



Евразийский национальный университет имени Л.Н. Гумилева
Национальная инженерная академия РК
Казахский национальный педагогический университет имени Абая, Казахстан
Институт математики и математического моделирования КН МВНО, Казахстан
Институт информационных и вычислительных технологий КН МВНО, Казахстан
Международный математический центр ИМ им. С.Л. Соболева СО РАН, Россия
Российский национальный комитет по индустриальной и прикладной математике, Россия
ОФ «Международный фонд обратных задач», Казахстан
Математическое Общество Тюркского Мира.

ЕУРАЗИЯЛЫҚ ХАЛЫҚАРАЛЫҚ ҒЫЛЫМИ КОНФЕРЕНЦИЯ
ЕВРАЗИЙСКАЯ МЕЖДУНАРОДНАЯ НАУЧНАЯ КОНФЕРЕНЦИЯ

«ҒЫЛЫМДАҒЫ, ТЕХНИКА МЕН ИНДУСТРИЯДАҒЫ ЖАСАНДЫ ИНТЕЛЛЕКТ ЖӘНЕ КЕРІ
ЕСЕПТЕР»

«ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ОБРАТНЫЕ ЗАДАЧИ В НАУКЕ, ТЕХНИКЕ И ИНДУСТРИИ»

«ARTIFICIAL INTELLIGENCE AND INVERSE PROBLEMS IN SCIENCE, TECHNOLOGY AND
INDUSTRY»

ЕҢБЕКТЕРІ ТРУДЫ PROCEEDINGS

Астана
14-16 апреля 2025 г.

УДК 004.896:001(082)

Еуразиялық халықаралық ғылыми конференция
«Ғылымдағы, техника мен индустриядағы жасанды интеллект және кері есептер»
Евразийская международная научная конференция
“Искусственный интеллект и обратные задачи в науке, технике и индустрии”
Eurasian international scientific conference
«Artificial intelligence and inverse problems in science, technology and industry»

ISBN 978-601-385-052-8

Еуразиялық халықаралық ғылыми конференция «Ғылымдағы, техника мен индустриядағы жасанды интеллект және кері есептер» баяндамалар жинағы. 14-16 сәуір 2025 жыл.

Сб. докл. Евразийской международной научной конференций «Искусственный интеллект и обратные задачи в науке, технике и индустрии» 14-16 апрель 2025 год.

Collection of reports the Eurasian international scientific conference «Artificial intelligence and inverse problems in science, technology and industry»

– Астана: Л.Н. Гумилев атын. Еуразия ұлттық университеті, 2025. – 451 б. – қазақша, орысша, ағылшынша.

1 СЕКЦИЯ . «КЕРІ ЕСЕПТЕРДІ ШЕШУДЕ ЖАСАНДЫ ИНТЕЛЛЕКТ»

СЕКЦИЯ 1. «ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В РЕШЕНИИ ОБРАТНЫХ ЗАДАЧ»

SECTION 1. «ARTIFICIAL INTELLIGENCE IN SOLVING INVERSE PROBLEMS»

1.	Alinova A.D., Zhartybayeva M.G., Villanueva F.J., Belyaev M.S. - BATHYMETRIC MAPPING OF A LAKES BASED ON SATELLITE IMAGERY AND SEABED CHARACTER ANALYSIS USING NEURAL NETWORKS	1
2.	Iklassova K., Shaikhanova A., Tashibayev R. - ARTIFICIAL INTELLIGENCE FOR SOLVING INVERSE PROBLEMS AND EXPLAINING DECISIONS IN EDUCATIONAL MANAGEMENT SYSTEMS	2-4
3.	Jinchao Pan, Jijun Liu - ON THE SIMULTANEOUS RECOVERY OF BOUNDARY IMPEDANCE AND INTERNAL CONDUCTIVITY	4
4.	Jomartova Sh.A., Mazakova A.T., Ziyatbekova G.Z., Aliaskar M.S., Zhaksymbet A.T. - HARDWARE-SOFTWARE COMPLEX FOR MONITORING THE LEVEL OF WATER BODY OCCUPANCY	5-6
5.	Kuanyshev A., Moldamurat K., Hajizadeh C. - ALGORITHM FOR USING ARTIFICIAL INTELLIGENCE IN PREDICTING FIRE DANGER IN THE SEMEY FOREST IN KAZAKHSTAN	7-9
6.	Kuatbayeva A.A., Sergaziyev M.Zh., Yedilkhan D., Gizatov A., Issenov D., Namet A., Bekbolatov O. - DESIGN ML MODELS FOR BUS TIME ARRIVAL PREDICTION IN ASTANA CITY	9-12
7.	Yi Tang, D. Pertsau, M. Tatur - ENHANCED A* ALGORITHM FOR GLOBAL PATH PLANNING	12-13
8.	Афанасьева С.Д. - РЕШЕНИЕ СИНГУЛЯРНО-ВОЗМУЩЕННЫХ КРАЕВЫХ ЗАДАЧ В ДВУМЕРНОМ СЛУЧАЕ С ИСПОЛЬЗОВАНИЕМ МЕТОДА PINN	14
9.	Бектемесов Ж.М., Бектемесов М.А. - О НЕКОТОРЫХ МЕТОДАХ РЕШЕНИЯ ОБРАТНЫХ ЗАДАЧ ДЛЯ МОДЕЛИРОВАНИЯ МЕТАСТАЗОВ РАКОВОЙ ОПУХОЛИ	15-16
10.	Бектемесов Ж.М., Социалова Ұ.Қ. - ЖАСАНДЫ ИНТЕЛЛЕКТ АРҚЫЛЫ ҚАЗАҚСТАНДАҒЫ ИНФЕКЦИЯЛЫҚ АУРУЛАРДЫҢ ТАРАЛУЫН ТАЛДАУ	16-17
11.	Дженалиев М.Т., Ергалиев М.Г., Иманбердиев К.Б., Серик А.М. - ОБ ОДНОЙ СПЕКТРАЛЬНОЙ ЗАДАЧЕ ДЛЯ ДИФФЕРЕНЦИАЛЬНОГО ОПЕРАТОРА ЧЕТВЕРТОГО ПОРЯДКА	17-20
12.	Динг А. (Aodi Ding), Недзьведь О.В. - ИЗВЛЕЧЕНИЕ ПЛОТНЫХ КЛЮЧЕВЫХ ТОЧЕК НИЖНИХ КОНЕЧНОСТЕЙ И СТОП ДЛЯ ПОВЫШЕНИЯ ТОЧНОСТИ ДИАГНОСТИКИ ЗАБОЛЕВАНИЙ	20-22
13.	Ергалиев М.Г., Касен М. – УСЛОВИЯ РАЗРЕШИМОСТИ КОЭФФИЦИЕНТНЫХ ОБРАТНЫХ ЗАДАЧ ДЛЯ УРАВНЕНИЯ БЮРГЕРСА	22-23
14.	Жәнібек М.А., Мұхаметжанова Б.О. - ЖАҢАЛЫҚТАРДЫ ТАЛДАУДАҒЫ КЕРІ ЕСЕПТЕР: МАНИПУЛЯЦИЯ МЕН ДЕЗИНФОРМАЦИЯНЫ АНЫҚТАУ	23-25
15.	Касенов С.Е., Темирбекова М.Н., Кабулова А.А. - АЛГОРИТМ РЕШЕНИЕ ОБРАТНОЙ ЗАДАЧИ ДЛЯ УРАВНЕНИЯ ДИФФУЗИИ	25-28
16.	Касенов С.Е., Тлеулесова А.М., Сарсенбаева А.Е. - ЧИСЛЕННОЕ РЕШЕНИЕ ЗАДАЧИ ПРОДОЛЖЕНИЯ ДЛЯ УРАВНЕНИЯ ГЕЛЬМГОЛЬЦА	28-30
17.	Касенов С.Е., Тлеулесова А.М., Тугенбаева Ж.С., - ЧИСЛЕННОГО РЕШЕНИЯ ЗАДАЧИ ФАРМАКОКИНЕТИКИ ДЛЯ ТРЕХКАМЕРНОЙ МОДЕЛИ	30-32
18.	Касылкасова К.Н. - МЕДИЦИНСКОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ SMARTMED ДЛЯ ОБРАБОТКИ МЕДИЦИНСКИХ ДАННЫХ И ДИАГНОСТИКИ	32-35
19.	Космакова М.Т., Ахманова Д.М., Ижанова К.А. – ЖҮКТЕЛГЕН ШЕТТІК ЕСЕП ТУРАЛЫ	35-36
20.	Кузнецов К.С. - ЧИСЛЕННОЕ РЕШЕНИЕ ОБРАТНОЙ РЕТРОСПЕКТИВНОЙ ЗАДАЧИ КОНДУКТИВНОГО ТЕПЛООБМЕНА МЕТОДОМ PINN	36-37

21.	Маманова С.Е., Тынымбаев С.Т., Кокенова У.К. - ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОПТИМИЗАЦИИ АРХИТЕКТУРЫ ДЕЛИТЕЛЬНЫХ УСТРОЙСТВ	37-39
22.	Медетов А.Р., Сагатбекова Д.Е. - РЕШЕНИЕ ОБРАТНЫХ ЗАДАЧ В ГЕОФИЗИКЕ С ИСПОЛЬЗОВАНИЕМ МАШИННОГО ОБУЧЕНИЯ	40-41
23.	Мирсабуров М., Макулбай А.Б., Бердышев А.С., Мирсабурова Г.М. - КОМБИНИРОВАННАЯ ЗАДАЧА ДЛЯ ОДНОГО КЛАССА УРАВНЕНИЙ СМЕШАННОГО ТИПА С РАЗЛИЧНЫМИ ПОРЯДКАМИ ВЫРОЖДЕНИЯ	41-44
24.	Омаров М.Т., Рамазанов М.И., Танин А.О., Шаяхметова Б.К. - ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ ДЛЯ РЕШЕНИЯ ОБРАТНЫХ ЗАДАЧ, СВЯЗАННЫХ С ДРОБНЫМИ ДИФФЕРЕНЦИАЛЬНЫМИ УРАВНЕНИЯМИ	44-46
25.	Орумбаева Н.Т., Жантасова Б.Б. - О РЕШЕНИИ ОДНОЙ КРАЕВОЙ ЗАДАЧИ ДЛЯ ГИПЕРБОЛИЧЕСКОГО УРАВНЕНИЯ С ДРОБНОЙ НАГРУЗКОЙ	46-47
26.	Рысбаева Н., Рысбайулы Б. - ОБРАТНАЯ ЗАДАЧА НЕЛИНЕЙНОГО ПЕРЕНОСА ВЛАГИ В ПОРИСТОЙ СРЕДЕ	48-50
27.	Сигаловский М.А. - ГЕОМЕТРИЯ КРУГОВОЙ АНОМАЛИИ В ПРЯМОУГОЛЬНОЙ ОБЛАСТИ ПОИСКА ДЛЯ ОДНОЙ ЗАДАЧИ ГРАВИМЕТРИИ	51-52
28.	Смаилова А.С., Шульгина-Таращук А.С. - МЕТОДЫ МАШИННОГО ОБУЧЕНИЯ ДЛЯ РЕШЕНИЯ ОБРАТНЫХ ЗАДАЧ	53-55
29.	Социалова Ұ.Қ., Абсамат А.А., Токтас Б.Б. - ЭПИДЕМИОЛОГИЯЛЫҚ АУРУЛАРДЫҢ МАТЕМАТИКАЛЫҚ МОДЕЛЬДЕРІН СТАТИСТИКАЛЫҚ ДЕРЕКТЕР НЕГІЗІНДЕ ТАЛДАУ ЖӘНЕ ОЛАРДЫҢ ЭКОНОМИКАҒА ӘСЕРІ	55-57
30.	Сугирбаев А.А., Зиятбекова Г.З. - РАЗРАБОТКА МАШИННОГО ОБУЧЕНИЯ ДЛЯ АНАЛИЗА ДАННЫХ УСТРОЙСТВА МОНИТОРИНГА СТРЕССА	57-60
31.	Суяров Т.Р. - ЗАДАЧА С ОБРАТНЫМ КОЭФФИЦИЕНТОМ ДЛЯ ОДНОМЕРНОГО ДРОБНОГО ВОЛНОВОГО УРАВНЕНИЯ С НЕЛОКАЛЬНЫМИ НАЧАЛЬНО-КРАЕВЫМИ УСЛОВИЯМИ	60-62
32.	Такуадина А.И., Шафеев Д.Е. - ОБРАТНЫЕ ЗАДАЧИ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В СОЗДАНИИ AI-АССИСТЕНТА	62-63
33.	Татур М.М., Крюков А.И., Чэнь Цз., В.Г.Каранкевич – ОБУЧЕНИЕ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ПРИНЯТИЯ РЕШЕНИЙ КАК ОБРАТНАЯ ЗАДАЧА ВЫБОРА ПАРАМЕТРОВ МОДЕЛИ	64-65
34.	Темирбеков А.Н., Тұрлыбек Ж.Ғ. - ЧИСЛЕННОЕ МОДЕЛИРОВАНИЕ РАСПРОСТРАНЕНИЯ ВРЕДНЫХ ПРИМЕСЕЙ В АТМОСФЕРЕ С PINN	65-67
35.	Темиржан С. А., Онгарбаева А.И. - ИСПОЛЬЗОВАНИЕ НЕЙРОННЫХ СЕТЕЙ В СТЕГОАНАЛИЗЕ ИЗОБРАЖЕНИЙ	67-70
36.	Тлеулесова А.М., Даулетбай М.Н. - ЧИСЛЕННОЕ РЕШЕНИЕ ЗАДАЧИ ПРОДОЛЖЕНИЯ ДЛЯ УРАВНЕНИЯ МАКСВЕЛЛА	70-72
37.	Токтабаев А.М., Ахметова А.М. - ИНТЕГРАЦИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И ТЕХНОЛОГИЙ ИНТЕРНЕТА ВЕЩЕЙ В МОНИТОРИНГ ЯГОД НА ОСНОВЕ БАЙЕСОВСКИХ МОДЕЛЕЙ	72-74

2 СЕКЦИЯ «КЕРІ ЖӘНЕ ДҰРЫС ҚОЙЫЛМАҒАН ЕСЕПТЕРДІҢ ТЕОРИЯЛЫҚ ЖӘНЕ ЕСЕПТЕУ АСПЕКТІЛЕРІ»

СЕКЦИЯ 2 «ТЕОРЕТИЧЕСКИЕ И ВЫЧИСЛИТЕЛЬНЫЕ АСПЕКТЫ ОБРАТНЫХ И НЕКОРРЕКТНЫХ ЗАДАЧ»

SECTION 2 «THEORETICAL AND COMPUTATIONAL ASPECTS OF INVERSE AND ILL-POSITIONED PROBLEMS»

1.	Akhmadiya A. – MODIFIED FREEMAN – DURDEN DECOMPOSITION RADAR IMAGE TO ELIMINATE NEGATIVE POWER PROBLEM	76-80

2.	Asanov A., Kadenova Z.A., Bekeshova D.A., Pirmatov A.Z., Sayipbekova A.M. - ONE CLASS OF LINEAR INTEGRAL EQUATIONS OF THE THIRD KIND WITH TWO INDEPENDENT VARIABLES	81-82
3.	Asanov A., Kadenova Z.A., Bekeshova D.A., - ON THE UNIQUENESS OF SOLUTIONS OF FREDHOLM LINEAR INTEGRAL EQUATIONS OF THE FIRST KIND ON THE SEMI-AXIS	83-84
4.	Khompyskh Kh. - AN INVERSE SOURCE PROBLEM FOR A SEMILINEAR PSEUDO-PARABOLIC EQUATION	84
5.	Mukhanova T., Toregali R., Aidos T. - FREDHOLM INTEGRAL EQUATIONS SOLVED NUMERICALLY USING THE BUBNOV-GALERKIN METHOD BASED ON ALPERT WAVELETS	85-86
6.	Serzhan Y.S., Umarov T.F. - FRAUD DETECTION IN CREDIT CARD TRANSACTIONS USING MACHINE LEARNING: A COMPARATIVE ANALYSIS	86
7.	Zharkyn D. - COMPREHENSIVE USE OF MULTI-AGENT MODELS IN URBAN TRAFFIC MANAGEMENT	86-88
8.	Shutong Hou, Haibing Wang – A NOVEL APPROACH FOR AN INVERSE SOURCE PROBLEM OF THE WAVE EQUATION IN THREE DIMENSIONS	88
9.	Абдрахман Б.Қ., Рысқан А.Р., Амангельды А.Е. - КӨП АЙНЫМАЛЫ ГИПЕРГЕОМЕТРИЯЛЫҚ ФУНКЦИЯ ҮШІН ЕКІНШІ РЕТТІ ДИФФЕРЕНЦИАЛДЫҚ ТЕҢДЕУЛЕР ЖҮЙЕСІН ШЕШУ	88-91
10.	Аркабаев Н.К., Кудуев А.Ж. - РАЗРАБОТКА И ОПТИМИЗАЦИЯ АЛГОРИТМОВ ГЛУБОКОГО ОБУЧЕНИЯ НА PYTHON ДЛЯ ОБРАБОТКИ БОЛЬШИХ ДАННЫХ В РЕАЛЬНОМ ВРЕМЕНИ С ПРИМЕНЕНИЕМ ВЫЧИСЛИТЕЛЬНОГО ИНТЕЛЛЕКТА	91-93
11.	Асанкулова М., Каденова З.А., Жолборсова А.К. - ОПТИМАЛЬНОГО РАСПРЕДЕЛЕНИЯ СЫРЬЯ МЕЖДУ ПОТРЕБИТЕЛЯМИ ДЛЯ ЗАДАЧ ДОБЫВАЮЩИХ ОТРАСЛЕЙ	93-96
12.	Байтурсеева А.Р., Рысбайұлы Б. - ЧИСЛЕННОЕ РЕШЕНИЕ ОБРАТНОЙ ЗАДАЧИ ДЛЯ НАХОЖДЕНИЯ КОЭФФИЦИЕНТА ТЕПЛОПРОВОДНОСТИ В ЗАДАЧЕ ТЕПЛОМАССОПЕРЕНОСА В ПОРИСТОЙ СРЕДЕ	96-99
13.	Бектемесов Ж.М., Социалова Ұ.Қ. - МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ОБРАТНОЙ ЗАДАЧИ РАСПРОСТРАНЕНИЯ КОРИ	99-101
14.	Бешеев Д.М., Оралбекова Ж. О., Ұзаққызы Н. –ОЧИСТКА ГЕОРАДИОЛОКАЦИОННОГО СИГНАЛА ВЕЙВЛЕТ – ФИЛЬТРАМИ НА ОСНОВЕ SYMLET – 6	102-103
15.	Бекенаева К.С., Макулбай А.Б., Мирсабурова У.М. - ЗАДАЧА С ЛОКАЛЬНЫМИ И НЕЛОКАЛЬНЫМИ УСЛОВИЯМИ ДЛЯ ОДНОГО УРАВНЕНИЯ СМЕШАННОГО ТИПА	103-106
16.	Жансеитова А.М., Боранбаев С.А., Исаков К.Т., Салкынов А.Т., – ГЕОРАДАРНОЕ ОБСЛЕДОВАНИЕ ДОРОЖНЫХ КОНСТРУКЦИЙ С ИСПОЛЬЗОВАНИЕМ ОБОРУДОВАНИЯ «ОКО-2»	106-107
17.	Жиеналиева Н.А., Турарова М.К. - ТҮЛҒАЛАР МЕН ОБЪЕКТІЛЕРДІ АНЫҚТАУ ҮШІН ҚОЛДАНЫЛАТЫН МАШИНАЛЫҚ ОҚЫТУ АЛГОРИТМДЕРІ	107-109
18.	Зейнелъ А.Н., Мухаметжанова Б.О. - ОПТИМИЗАЦИЯ АЛГОРИТМОВ ОБРАБОТКИ ИЗОБРАЖЕНИЙ ДЛЯ УЛУЧШЕНИЯ РАБОТЫ КАМЕР ВИДЕОНАБЛЮДЕНИЯ «СЕРГЕК»	109-111
19.	Исаков К.Т., Татин А. А., Турарова М. К. – АЛГОРИТМЫ ИНТЕРПРЕТАЦИИ РАДОРОГРАММ С ПРИМЕНЕНИЕМ НЕЙРОННЫХ СЕТЕЙ	111-112
20.	Куанова Н.С., Шияпов К.М., - СІЛТІСІЗДЕНДІРУ ПРОЦЕСТЕРІН САНДЫҚ МОДЕЛЬДЕУ АЛГОРИТМДЕРІН ҚҰРУ	112-113
21.	Кубегенова А.Д., Кубегенов Е.С. - ОПТИМИЗАЦИЯ ПАРАМЕТРОВ ДЛЯ МОДЕЛИРОВАНИЯ СОВМЕСТНОГО РАСПРОСТРАНЕНИЯ ТУБЕРКУЛЕЗА И ВИЧ С ИСПОЛЬЗОВАНИЕМ КОМПЛЕКСНОГО ПОДХОДА	114-115
22.	Курманбаева Ж.Қ. - ГЕОГРАФИЯ САБАҚТАРЫНДА ЖАСАНДЫ ИНТЕЛЛЕКТ ҚҰРАЛДАРЫНҚОЛДАНУДЫҢАРТЫҚШЫЛЫҚТАРЫМЕН КЕМШІЛІКТЕРІ	115-117
23.	Курмамбекова Г.П. - ҚАТЕРЛІ ІСІКТІ МОДЕЛЬДЕУДЕ КЕЙБІР ҚИСЫНДЫ ЕМЕС ЖЫЛУӨТКІЗГІШТІК ТЕҢДЕУЛЕР ШЕШІМІН САЛЫСТЫРУ	117-118

24.	Қайырбекова А.Ж., Зиятбекова Г.З. - ЦИФРЛЫҚ ЕГІЗДЕРДІҢ ДЕРЕКТЕРІН ҚОРҒАУ ЖҮЙЕСІНІҢ БЛОКЧЕЙН ТЕХНОЛОГИЯСЫ АРҚЫЛЫ ҚАМТАМАСЫЗ ЕТІЛУІ	118-120
25.	Малышко Д.А., Калинин А.А. - ОПТИМИЗАЦИЯ РАСЧЕТОВ В ЭНЕРГЕТИЧЕСКОМ СЕКТОРЕ КАЗАХСТАНА НА ОСНОВЕ СМАРТ-КОНТРАКТОВ	120-122
26.	Мариненко А.В., Эпов М.И – ПРИМЕНЕНИЕ ЭЛЕКТРОТОМОГРАФИИ НА ПОСТОЯННОМ ТОКЕ ДЛЯ ЛОКАЛИЗАЦИИ ПРОВОДЯЩИХ ГЕОЛОГИЧЕСКИХ ОБЪЕКТОВ ПРИ ОТКРЫТОМ СПОСОБЕ ДОБЫЧИ	122-124
27.	Мағзумов А. М. - WEBSOCKET ПРОТОКОЛЫНДАҒЫ ОСАЛДЫҚТАРДЫ ТАЛДАУ	125-128
28.	Махашов Ш. - КЛАСТЕРИЗАЦИЯ РЕГИОНОВ РЕСПУБЛИКИ КАЗАХСТАН ПО МАКРОЭКОНОМИЧЕСКИМ ПОКАЗАТЕЛЯМ С ПРИМЕНЕНИЕМ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ	128-133
29.	Наир Р.А., Ахметова А.А. - АВТОМАТИЗАЦИЯ РЕСТОРАННЫХ СЕТЕЙ	134-137
30.	Нуржанова А.Б., Жумадилаева А.К. - ВИДЕО АРҚЫЛЫ ЭМОЦИЯЛАРДЫ ТАҢУ: КОХОНЕН КАРТАЛАРЫ МЕН КЛАСТЕРЛІК АНСАМБЛЬДЕР	138-140
31.	Нұржанов Н.Ш., Турарова М.К. - ТҮЛҒАНЫҢ ЖАСЫ МЕН ЖЫНЫСЫН ТАҢУҒА АРНАЛҒАН НЕЙРОНДЫҚ ЖЕЛІ АЛГОРИТМДЕРІН ЗЕРТТЕУ	140-142
32.	Нығыманов Б.А., Ахметова А.А., Зиятбекова Г.З. - РАЗРАБОТКА СИСТЕМЫ ВИЗУАЛИЗАЦИИ ДАННЫХ ДЛЯ МОНИТОРИНГА ПРОИЗВОДСТВЕННЫХ ПРОЦЕССОВ С ИСПОЛЬЗОВАНИЕМ GRAFANA И PROMETHEUS	143-147
33.	Оразтаев Д.М. - МЕТОДЫ НЕРАЗРУШАЮЩЕГО КОНТРОЛЯ ДЛЯ ОЦЕНКИ СТЕПЕНИ ИЗНОСА ТРУБОПРОВОДОВ: СОВРЕМЕННЫЕ ПОДХОДЫ	147-149
34.	Оспанов А.Д. - ОПТИМИЗАЦИЯ МОНИТОРИНГА СКЛАДА С ПОМОЩЬЮ ИОТ-ДАТЧИКОВ И МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ: ЭМПИРИЧЕСКОЕ ИССЛЕДОВАНИЕ ПО ОБНАРУЖЕНИЮ ГРЫЗУНОВ И УПРАВЛЕНИЮ ОКРУЖАЮЩЕЙ СРЕДОЙ	149-151
35.	Рыскан А.Р., Джабаева М.Н. - РЕШЕНИЕ СИСТЕМЫ ДИФФЕРЕНЦИАЛЬНЫХ УРАВНЕНИЙ В ЧАСТНЫХ ПРОИЗВОДНЫХ ВТОРОГО ПОРЯДКА ДЛЯ ГИПЕРГЕОМЕТРИЧЕСКОЙ ФУНКЦИИ $F(4)_{18}$	151-153
36.	Рыскан А.Р., Мендигалиева Г. Р., Хасан А. А. - $F_{12}(4)$ ГИПЕРГЕОМЕТРИЯЛЫҚ ФУНКЦИЯСЫ ҮШІН ЕКІНШІ РЕТТІ ДЕРБЕС ТУЫНДЫЛЫ ДИФФЕРЕНЦИАЛДЫҚ ТЕҢДЕУЛЕР ЖҮЙЕСІН ШЕШУ	154-156
37.	Сабиғолла Ғ.Қ., Головачева В.Н. – ИНТЕГРАЦИЯ ИСКУССТВЕННОГО ИНТЕЛЕКТА В ЭЛЕКТРОННЫЕ МЕДИЦИНСКИЕ СИСТЕМЫ	157-158
38.	Сахабаева А.М. - БАКЛЕЙ – ЛЕВЕРЕТТ МОДЕЛІН ҚОЛДАНА ОТЫРЫП, МҰНАЙКЕН ОРЫНДАРЫНДА СУДЫ ТИІМДІ БАСҚАРУДЫ МОДЕЛЬДЕУ	158-160
39.	Сабитов А. Б., Исмагелов Ә.Е. - АНАЛИЗА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ ДЛЯ ОПЕРАТИВНОГО РЕАГИРОВАНИЯ НА УГРОЗЫ	160-161
40.	Султанов М.А., Мисилов В.Е., Садыбеков М. А., Баканов Г.Б., Сарсенов Б.Т. – АЛГОРИТМ ЧИСЛЕННОГО РЕШЕНИЯ ОБРАТНОЙ ЗАДАЧИ НАХОЖДЕНИЯ ПРАВОЙ ЧАСТИ ДЛЯ УРАВНЕНИЯ СУБДИФУЗИИ С КРАЕВЫМИ УСЛОВИЯМИ ТИПА ШТУРМА	161-162
41.	Турсунов Д.А., Мамытов А.О., Кудуев А.Ж. - ОБРАТНАЯ ЗАДАЧА ДЛЯ ОДНОГО КЛАССА ДИФФЕРЕНЦИАЛЬНЫХ И ИНТЕГРО-ДИФФЕРЕНЦИАЛЬНЫХ УРАВНЕНИЙ В ЧАСТНЫХ ПРОИЗВОДНЫХ	162-165

42.	Тусупов А.К., Тулеев А.А. - СБОР ДАННЫХ С ДАТЧИКОВ ДЛЯ ЦИФРОВОГО ДВОЙНИКА ПРЕДПРИЯТИЯ	165-167
43.	Уалиев А.М., Жартыбаева М.Г. – ТҰРМЫСТЫҚ ҚАТТЫ ҚАЛДЫҚТАРДЫ ЖІКТЕУ ҮШІН КОМПЬЮТЕРЛІК КӨРУ ЖӘНЕ ТЕРЕҢ ОҚЫТУ АЛГОРИТМДЕРІ МЕН ӘДІСТЕРІН ЗЕРТТЕУ ЖӘНЕ ТАЛДАУ	168-169
44.	Шаяхметов Н.М., Құрмансейіт М.Б., Айжулов Д.Е., Тунгатарова М.С. - ОПТИМИЗАЦИЯ РАСХОДОВ СКВАЖИН ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ДОБЫЧИ МИНЕРАЛОВ МЕТОДОМ ПОДЗЕМНОГО СКВАЖИННОГО ВЫЩЕЛАЧИВАНИЯ	169-170

3 СЕКЦИЯ «АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР ЖӘНЕ ЕСЕПТЕУ ИНТЕЛЛЕКТІСІ

3 СЕКЦИЯ «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ВЫЧИСЛИТЕЛЬНЫЙ ИНТЕЛЛЕКТ»

SECTION 3 «INFORMATION TECHNOLOGY AND COMPUTATIONAL INTELLIGENCE»

1.	Aitim A.K., Sattarkhuzhayeva D.T. , - REAL - TIME GESTURE RECOGNITION SYSTEM FOR KAZAKH SIGN LANGUAGE TRANSLATION TO SPEECH	172-174
2.	Alzhanov A., Akhmetova G., Akhmetov., Mukhysheva G., Matin D. - MODELS AND METHODS OF KNOWLEDGE REPRESENTATION AND PROCESSING IN MATHEMATICS	174-177
3.	Assubai A.O., Rysbayuly B. - FINDING THE COEFFICIENTS OF THE HEAT EQUATION IN A TWO-DIMENSIONAL ANISOTROPIC MEDIUM	177-178
4.	Ashimgaliyev M., Zhumadillayeva A. – A COMPREHENSIVE REVIEW ON EARLY DETECTION OF ALZHEIMER'S DISEASE USING VARIOUS DEEP LEARNING TECHNIQUES	178-183
5.	Bekele S.D., Kenzhebek Y., Imankulov T. -INTERPRETABLE SYMBOLIC EXTRACTION IN KOLMOGOROV–ARNOLD NETWORKS FOR ENHANCED OIL RECOVERY	183-185
6.	Bolat A.Zh. - DATA ANALYSIS METHODS AND DECISION MAKING USING BIG DATA AND MACHINE LEARNING TOOLS	186-195
7.	Kabdeshev A. ,- DEVELOPMENT OF AN INTELLIGENT HEALTH DIAGNOSIS SYSTEM BASED ON COUGH ANALYSIS	195-201
8.	Kassymova A., Kartbayev A. , - EXPLAINABLE ARTIFICIAL INTELLIGENCE IN CREDIT SCORING FOR ENHANCED FINANCIAL RISK MANAGEMENT	201-214
9.	Kenzhebek Y., Bekele S.D., Imankulov T. - PREDICTION OF TWO-PHASE FLOW IN POROUS MEDIA USING PHYSICS-INFORMED NEURAL NETWORKS	215-217
10.	Kuatbayeva A.A., Alibi J., Gizatov A., Zhaksybayev N. - PREDICTIVE MODELS FOR ANALYZING AND FORECASTING LABOR MARKET TRENDS IN KAZAKHSTAN: ADDRESSING MARKET SATURATION AND ENSURING ECONOMIC STABILITY	217-220
11.	Mansurova M.Y., Ospan A.G., Mussa A. - DEVELOPMENT OF AN AI ASSISTANT FOR JOURNALISM BASED ON RETRIEVAL-AUGMENTED GENERATION (RAG)	220-222
12.	Marat G.S. - FINDING THE THERMOPHYSICAL PARAMETERS OF THE MATERIAL BASED ON THE HYPERBOLIC EQUATION OF THERMAL CONDUCTIVITY	222
13.	Meiramkhan E.A. - METHODS OF INTEGRATING KAPE WITH OTHER DIGITAL FORENSICS TOOLS	223-230
14.	Oryngaliyeva N.A. - MODERN METHODS OF TEXT RECOGNITION IN THE CONTEXT OF THE KAZAKH LANGUAGE IN CYRILLIC	231-233

15.	Ospanova A. B., Zharaskhan N.Zh., Kayupov E. - PRACTICAL EFFICIENCY AND POTENTIAL OF LATTICE REDUCTION IN RECOVERING SECRET PARAMETERS OF POST-QUANTUM CRYPTOSYSTEMS	234-235
16.	Shutong H., Haibing W. - A NOVEL APPROACH FOR AN INVERSE SOURCE PROBLEM OF THE WAVE EQUATION IN THREE DIMENSIONS	236
17.	Yerzhan M., Bazargul M. - ROUTING AND COORDINATION MODELS FOR INTELLIGENT DRONES IN DISASTER SCENARIOS	236-237
18.	Zhunissof N.M., Aben A.B. - FAKE NEWS DETECTION USING MACHINE LEARNING	237-239
19.	Абдуллаева Б.Ж., Құрмансейіт М.Б., Тунгатарова М.С., Айжулов Д.Е., Шаяхметов Н.М. - УРАНДЫ ЖЕРАСТЫ ҰҢҒЫМАЛЫ ШАЙМАЛАУ ПРОЦЕСІН САНДЫҚ МОДЕЛЬДЕУДІ ЖЕДЕЛДЕТУ: КЕРІ САЛМАҚТЫҚ АРАҚАШЫҚТЫҚ ИНТЕРПОЛЯЦИЯСЫ ӘДІСІ МЕН НЕЙРОНДЫҚ ЖЕЛІЛЕРДІ ҚОЛДАНУ АРҚЫЛЫ ГИДРАВЛИКАЛЫҚ ҚЫСЫМ ТЕНДЕУІН ШЕШУ	240-242
20.	Абаева А.Р. - АНТИФОРЕНЗИКА ӘДІСТЕРІН ЗЕРТТЕУ ЖӘНЕ ОЛАРДЫҢ ЦИФРЛЫҚ ТЕРГЕУГЕ ӘСЕРІ	243-247
21.	Абдығалым Б.Х., Самбетбаева М.А. – ФОРМИРОВАНИЕ ОНТОЛОГИИ ВОЕННОЙ ТЕРМИНОЛОГИИ В ЦЕЛЯХ СЕМАНТИЧЕСКОГО АНАЛИЗА ИНФОРМАЦИИ В СУХОПУТНЫХ ВОЙСКАХ.	247-249
22.	Амирбай А.А., Мұханова А.А. – АУТИЗМ БЕЛГІЛЕРІН ЕРТЕ АНЫҚТАУ МАҚСАТЫНДА КӨЗ ҚОЗҒАЛЫСЫН ТАЛДАУҒА НЕГІЗДЕЛГЕН ТЕРЕҢ ОҚЫТУ МОДЕЛЬДЕРІН ҚОЛДАНУ	249-252
23.	Атығасев О.Т., Жартыбаева М.Г. - ВИРТУАЛДЫ КЕЙІПКЕРДІҢ НАҚТЫ УАҚЫТ РЕЖИМІНДЕ АУДИТОРИЯМЕН ИНТЕРАКТИВТІ ӘРЕКЕТТЕСУІНЕ АРНАЛҒАН ТАБИҒИ ТІЛДІ ӨНДЕУ АЛГОРИТМДЕРІ МЕН ӘДІСТЕРІН ЗЕРТТЕУ ЖӘНЕ ЖҮЗЕГЕ АСЫР	253-254
24.	Байганина Ж.Б., Жартыбаева М.Г. - ИНТЕЛЛЕКТУАЛЬНАЯ ВЕБ-СИСТЕМА НА ОСНОВЕ ИИ ДЛЯ АНАЛИЗА СВИДЕТЕЛЬСКИХ ПОКАЗАНИЙ И ВЫЯВЛЕНИЯ СМЫСЛОВЫХ РАСХОЖДЕНИЙ	255-256
25.	Бегалы А.П., Жартыбаева М.Г. - РАЗРАБОТКА СИСТЕМЫ С ПОДДЕРЖКОЙ AI ДЛЯ АДАПТИВНОГО СОСТАВЛЕНИЯ ЮРИДИЧЕСКИХ ДОКУМЕНТОВ	256-258
26.	Бизақ Ә.Ө. - ҚАЗАҚСТАНДАҒЫ ЖАСАНДЫ ИНТЕЛЛЕКТТІ РЕТТЕУДІҢ КӨЗҚАРАСТАРЫ: СЫН-ТЕГЕУРІНДЕР ЖӘНЕ ХАЛЫҚАРАЛЫҚ ТРЕНДТЕР	258-260
27.	Головачева В.Н., Долгов В.В. - РЕАЛИЗАЦИЯ АЛГОРИТМА ДЕЙКСТРЫ ДЛЯ ПОСТРОЕНИЯ ОПТИМАЛЬНОГО АВТОМОБИЛЬНОГО ПУТИ С ИСПОЛЬЗОВАНИЕМ ФРЕЙМВОРКА SPRINGBOOT	260-262
28.	Жаксымбет А.Т., Кәрібаева А.С., Зиятбекова Г.З. -РАЗРАБОТКА МОДЕЛИ АНАЛИЗА И КЛАССИФИКАЦИИ ТЕКСТОВ НА КАЗАХСКОМ ЯЗЫКЕ С ПРИЗНАКАМИ СУИЦИДАЛЬНОГО ПОВЕДЕНИЯ В СОЦИАЛЬНЫХ СЕТЯХ	262-270
29.	Жамалбек М.Ұ., Жартыбаева М.Г. - РАЗРАБОТКА СИСТЕМЫ КЛАССИФИКАЦИИ ПО ГОЛОСОВЫМ ДАННЫМ С ПОМОЩЬЮ НЕЙРОННЫХ СЕТЕЙ	271-272
30.	Жарасов Ұ.А., Мухаметжанова Б.О. - ИССЛЕДОВАНИЕ И РАЗРАБОТКА СИСТЕМЫ УПРАВЛЕНИЯ ПРОЦЕССОМ СОРТИРОВКИ ПРОДУКЦИИ НА ОСНОВЕ НЕЙРОННОЙ СЕТИ	272-274
31.	Жиенбай А. Ғ. - ГЕНЕТИКАЛЫҚ АЛГОРИТМДЕРДІҢ ЖАСАНДЫ ИНТЕЛЛЕКТ ЖҮЙЕЛЕРІНДЕ ҚОЛДАНЫЛУЫН САЛЫСТЫРМАЛЫ ТАЛДАУ	274-275
32.	Закирова Ф. Р. - ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ПРОГНОЗА ГЛОБАЛЬНОЙ УРОЖАЙНОСТИ В УСЛОВИЯХ ИЗМЕНЕНИЯ КЛИМАТА	276-278

33.	Зиятбекова Г.З., Алиаскар М.С., Бургегулов А.Д. , Жаксымбет А.Т. - ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС МОНИТОРИНГА УРОВНЯ ЗАПОЛНЕННОСТИ ВОДОЕМА	278-290
34.	Зятыков Н.Ю., Криворотько О.И. - СЦЕНАРИИ РАСПРОСТРАНЕНИЯ СОЦИАЛЬНО-ЗНАЧИМЫХ ЗАБОЛЕВАНИЙ, ОСНОВАННЫЕ НА МЕТОДАХ ГЛУБОКОГО ОБУЧЕНИЯ В СЛУЧАЕ НЕДОСТАТОЧНЫХ ДАННЫХ	281-282
35.	Изтаев Ж.Д., Исмаилов Х.Б. - РАЗРАБОТКА КОНЦЕПТУАЛЬНОЙ МОДЕЛИ СИСТЕМЫ УПРАВЛЕНИЯ КОМАНДОЙ С ФУНКЦИЕЙ АНАЛИЗА ПРОИЗВОДИТЕЛЬНОСТИ СОТРУДНИКОВ	293-295
36.	Имашев Н.К. - ФУНКЦИОНАЛЬНЫЕ ОСОБЕННОСТИ ВНЕДРЕНИЯ РАСПОЗНАВАНИЯ ЛИЦ В СИСТЕМАХ КОНТРОЛЯ ДОСТУПА	296-298
37.	Касенгалиев Д.К., Искаков К.Т., Боранбаев С.А., - РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ЭФФЕКТИВНОГО ОБНАРУЖЕНИЯ ДЕФЕКТОВ СЛОИСТЫХ СРЕД	298-300
38.	Калимолдаев М.Н., Жолдангарова Г.И., Аршидинова М.Т., Ахметжанов М.А. - ПРОГРАММНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМА ПРОГНОЗИРОВАНИЯ ОСТАТОЧНОГО СРОКА ПОЛЕЗНОГО ИСПОЛЬЗОВАНИЯ ОБОРУДОВАНИЯ ЭЛЕКТРОЭНЕРГЕТИЧЕСКИХ СИСТЕМ.	301-305
39.	Калменов К.Б., Жусупов Т.А., Кусаннова А.Т., Сагиндыков К.М. – СОВРЕМЕННЫЕ МЕТОДЫ ОТБОРА ПРОБ ДОРОЖНО- СТРОИТЕЛЬНЫХ МАТЕРИАЛОВ И ИХ РОЛЬ В ГЕОРАДИОЛОКАЦИОННЫХ ИССЛЕДОВАНИЯХ.	305-307
40.	Карин А.Б., Кульбаев Э.М., Мендибаева Ш. - РАЗРАБОТКА ЧАТ БОТА ДЛЯ ОПТИМИЗАЦИИ СЕРВИСА ПО НЕДВИЖИМОСТИ, А ТАКЖЕ АНАЛИЗА	307-308
41.	Кусаннова А.Т., Искаков К.Т., Глазырина Н.С. - ВЕБ-ПРИЛОЖЕНИЕ ДЛЯ ОБРАБОТКИ, ВИЗУАЛИЗАЦИИ И ИНТЕРПРЕТАЦИИ РАДАРОГРАММ ДОРОЖНОЙ ОДЕЖДЫ	309-310
42.	Кенжахметов Е.К., Мұратұлы Д., Четтыкбаев Р. К. - РАЗРАБОТКА АЛГОРИТМА ВЫЯВЛЕНИЯ НАРУШЕНИЙ ВО ВРЕМЯ ОНЛАЙН-ЭКЗАМЕНОВ НА ОСНОВЕ КОМПЬЮТЕРНОГО ЗРЕНИЯ	311-312
43.	Кеңесбай М.М., Тохметов А.Т. - ОБЗОР ПОДХОДОВ К АНАЛИЗУ ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ ИНТЕРНЕТ-МАГАЗИНОВ И СИСТЕМ РЕКОМЕНДАЦИЙ	312-314
44.	Кошенов А. Т., Жартыбаева М. Г.- РАЗРАБОТКА СИСТЕМЫ ДЛЯ МОНИТОРИНГА ЛЕСНОГО ХОЗЯЙСТВА С ПРИМЕНЕНИЕМ БПЛА И ГЛУБОКОГО ОБУЧЕНИЯ	314-315
45.	Кыдырбекова А.С., Ахметова С.Т., Ажибеков К. – НОВЫЙ МЕТОД АУТЕНТИФИКАЦИИ ЛИЧНОСТИ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНЫХ ТЕРМИНАЛОВ	316-318
46.	Мунайдаров А.К., Муханбеткалиева А.К. - ИНТЕЛЛЕКТУАЛЬНЫЕ ПОДХОДЫ К ПРОЕКТИРОВАНИЮ ИНТЕРФЕЙСОВ СВЯЗИ В ПЛАТФОРМАХ АВТОМАТИЗИРОВАННОГО ТЕСТИРОВАНИЯ ИОТ-УСТРОЙСТВ	318-320
47.	Набиев Н.К., Усманов Т.А., Жолдангарова Г.И., Набиева Н.Б. - РАЗРАБОТКА И ВНЕДРЕНИИ ВЫЧИСЛИТЕЛЬНЫХ МЕТОДОВ АНАЛИЗА ДАННЫХ ГНСС ДЛЯ ОЦЕНКИ АТМОСФЕРНОЙ ВЛАЖНОСТИ	321-324
48.	Назымхан А.А., Некесова А.А. - INSTAGRAM ЖЕЛІСІНЕН ДЕРЕКТЕРДІ АВТОМАТТЫ ТҮРДЕ АЛУ ЖӘНЕ ӘЛЕУМЕТТІК ЖЕЛІЛЕРДЕГІ ЖАЛҒАН ЖАҢАЛЫҚТАРДЫ АНЫҚТАУ ҮШІН ВЕБ-СКРЕПІНГТІ ПАЙДАЛАНУ	324-327
49.	Пирматов А.З., Каденова З.А. - РАЗРАБОТКА TELEGRAM ВОТ САМОСТОЯТЕЛЬНОГО ТЕСТИРОВАНИЯ ПОЛЬЗОВАТЕЛЯ ПО СРЕДСТВАМ ЯЗЫКА PYTHON	327-328
50.	Рсымбетов К.С., Бейсебай П.Б., Даулетхан А. – ЭФФЕКТЫ ВНЕДРЕНИЯ ERP СИСТЕМЫ ODOO В ПРОИЗВОДСТВЕ ОРГАНИЧЕСКИХ ПРОДУКТОВ	328-331
51.	Сарымов Н. - РАСПОЗНАВАНИЕ РЕЧИ И ПРЕОБРАЗОВАНИЕ ЕЁ В ТЕКСТ С ПРИМЕНЕНИЕМ ГЛУБОКОГО ОБУЧЕНИЯ НА МОБИЛЬНОМ УСТРОЙСТВЕ	331-337
52.	Сайлау А.Ж., Зиятбекова Г.З. - ҮЛКЕН ТІЛДІК ҮЛГІЛЕР ҮШІН ҚАЗАҚША МӘТІНДЕРДІ АЛДЫН АЛА ӨНДЕУ ӘДІСТЕРІН ӘЗІРЛЕУ	337-339
53.	Сағидолла Д.Р. , Ерғали Г. Б. - АНАЛИЗ И СБОР ДАННЫХ ИЗ СОЦИАЛЬНЫХ СЕТЕЙ: МЕТОДЫ, ИНСТРУМЕНТЫ И ЭТИЧЕСКИЕ АСПЕКТЫ	339-340
54.	Серікқызы Е., Жамангарин Д.С .- АЗЫҚ-ТҮЛІКТІ ТАҢУ ЖӘНЕ ОЛАРДЫҢ ТАҒАМДЫҚ ҚҰНДЫЛЫҒЫН ТАЛДАУ ҮШІН КОМПЬЮТЕРЛІК КӨРУ ҮЛГІЛЕРІН ҚОЛДАНУ	340-344

55.	Сулеймен Б.К., Исаков К.Т., Нартова Д.С. - ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ИИ В СИСТЕМАХ МОНИТОРИНГА И ЭКОНОМИИ ЭЛЕКТРИЧЕСКОЙ ЭНЕРГИИ	344-346
56.	Таберхан Р., Самбетбаева М.А. - LABEL STUDIO-НЫ ПАЙДАЛАНА ОТЫРЫП, СЕБЕП-САЛДАРЛЫҚ КҰРЫЛЫМДАРДЫ ҚАЗАҚ ТІЛІНДЕ АННОТАЦИЯЛАУДЫ АВТОМАТТАНДЫРУ	347-349
57.	Хусенбай А. - СТЕРЕОМЕТРИЯЛЫҚ ЕСЕПТЕРДІ ШЫҒАРУДА КОМПЬЮТЕРЛІК БАҒДАРЛАМАЛАРДЫ ҚОЛДАНУҒА МҰҒАЛІМДЕРДІ ОҚЫТУ ӘДІСТЕМЕСІ	349-353
58.	Шаймуратов А.Ж. - АВТОМАТИЗИРОВАННОЕ РАСПОЗНАВАНИЕ НОМЕРОВ ЖЕЛЕЗНОДОРОЖНЫХ ВАГОНОВ: СОВРЕМЕННЫЕ МЕТОДЫ И ПЕРСПЕКТИВЫ	353-356

4 СЕКЦИЯ «КРИПТОГРАФИЯДАҒЫ ЖАСАНДЫ ИНТЕЛЛЕК ЖӘНЕ КИБЕРҚАУІПСІЗДІК»

4 СЕКЦИЯ «ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В КРИПТОГРАФИИ И КИБЕРБЕЗОПАСНОСТИ»

SECTION 4 "ARTIFICIAL INTELLIGENCE IN CRYPTOGRAPHY AND CYBERSECURITY"

1.	Altaibayev D.M., Mukhametzhanova B.O. - ARTIFICIAL INTELLIGENCE METHODS FOR SIMULATING COMPUTER EFFECTS IN TRADITIONAL ANIMATION USING MODERN GRAPHICS TECHNOLOGIES	358-360
2.	Alzhan T., Khuralay M., Huseyin C., Alzhan A. Tilenbayev - АНАЛИЗ ЭФФЕКТИВНОСТИ DDOS СЕТЕВОЙ АТАКИ НА IOT УСТРОЙСТВО	360-364
3.	Yelibayeva G., Razakhova B., Sharipbay A., Syzdykova G. - ONTOLOGICAL MODELS OF THE KAZAKH LANGUAGE FOR SECONDARY EDUCATION	364-366
4.	Yerzatuly T. - BIOMETRIC SECURITY IN SMART BUILDINGS: A NEW AGE OF AUTOMATION, PRIVACY, AND EFFICIENCY ABSTRACT	366-369
5.	Ibraikhan A., Smagulov T., Aitmagambet A., Amirova A., DEVELOPMENT OF AN ALGORITHM FOR DETECTING MALICIOUS LINKS ON INSTAGRAM	369-371
6.	Khaman D., Amirova A. - DEVELOPMENT AND PERFORMANCE EVALUATION OF A MODEL FOR DETECTING VIRUSES IN COMPUTER SYSTEMS USING ARTIFICIAL INTELLIGENCE	371-373
7.	Makhabbat B., Luigi La Spada - AI-ENHANCED CRYPTOGRAPHIC FRAMEWORK FOR HIGH-SPEED SECURE DATA TRANSMISSION IN LOW-ORBIT AIRCRAFT SYSTEMS	373-376
8.	Marat G.S. - FINDING THE THERMOPHYSICAL PARAMETERS OF THE MATERIAL BASED ON THE HYPERBOLIC EQUATION OF THERMAL CONDUCTIVITY	376
9.	Sergazy M., Tokseit D.K. - ENHANCING DEVELOPER PRODUCTIVITY WITH INTEGRATED ARTIFICIAL INTELLIGENCE AND CYBERSECURITY CONSIDERATIONS	377-378
10.	Serikov A., Kaziyeva N., - SECURE DATA TRANSMISSION IN MODERN TELECOMMUNICATIONS: EMERGING ALGORITHMS, QUANTUM CHALLENGES, AND OPTIMIZATION TRENDS	379-381
11.	Slyamshaikhov Y.B.-Tokseit D.K. - APPLICATION OF MACHINE LEARNING AND AUTOMATED PROCESSES IN DIGITAL FORENSICS	381-388
12.	Shertay O.- CRITICALITY ASSESSMENT AND CLASSIFICATION OF CRITICAL INFORMATION INFRASTRUCTURE (CII): APPROACHES AND METHODOLOGIES	388-390
13.	Tokseit D., Meshitbayeva.K. -INVESTIGATION OF MAC AND APPLICATION LAYER PROTOCOLS WITH TRUST SUPPORT FOR NETWORK SECURITY	390-392
14.	Tokseit D., K.Otebay A.M. - THE THREAT OF DEEPFAKE TECHNOLOGY TO HUMANITY IN RECENT YEARS	392-393
15.	Ydyrys A.Zh., Satybaldina A.N. - INVERSE PROBLEM FOR 2D LAPLACE EQUATION IN CYLINDRICAL COORDINATES	393-395

16.	Zhakan Z.S., Mukhametzhanova B.O. , - PROTECTING RELATIONAL DATABASE INDEXES FROM ATTACKS BASED ON QUERY ANALYSIS	395-396
17.	Алексеев И. П., Оспанова А. Б. - ИССЛЕДОВАНИЕ ПОТЕНЦИАЛА AI-МОДЕЛЕЙ В АВТОМАТИЗАЦИИ КИБЕРАТАК	397-399
18.	Әмірғалы С., Омар А., Токсент Д.Қ. - ФИШИНГТЕН, ТЕЛЕФОН АЛАЯҚТАРЫНАН ЖӘНЕ МАРКЕТИНГТЕРДЕГІ АЛАЯҚТЫҚТАН ЖИ КӨМЕГІМЕН ҚОРҒАУЫ	399-402
19.	Байшаков Д.Т., Казиева Н.М. , - ПРИНЦИП РАБОТЫ НЕЙРОНА В НЕЙРОННЫХ СЕТЯХ И АНАЛИЗ АЛГОРИТМОВ НЕЙРОННЫХ СЕТЕЙ ДЛЯ АВТОМАТИЗАЦИИ ПРОЦЕССОВ В КИБЕРБЕЗОПАСНОСТИ	402-404
20.	Балгабекова С.А., Аймичева Г.И. , - ТЕХНОЛОГИЯ СБОРА ЦИФРОВЫХ УЛИК ВЕБ-АКТИВНОСТИ ЗЛОУМЫШЛЕННИКА В РЕЖИМЕ ИНКОГНИТО	404-407
21.	Жарылған Р.Ж., Исайнова А.Н. - ИССЛЕДОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИОТ-УСТРОЙСТВ С ИСПОЛЬЗОВАНИЕМ МОНИТОРИНГА, АУТЕНТИФИКАЦИИ И СИМУЛЯЦИИ СЕТЕВЫХ АТАК	407-409
22.	Калижан А.К., Глазырина Н.С. (- РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ СПУФИНГ-АТАК НА СИСТЕМЫ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ	410-412
23.	Коньрханова А.А., Тұрарғазин Ж.С. - РОЛЬ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА В ОБЕСПЕЧЕНИИ КИБЕРБЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ	412-416
24.	Кутышев В.В. - КАК ЗАЩИТИТЬ ПЕРСОНАЛЬНЫЕ ДАННЫЕ ПОЛЬЗОВАТЕЛЕЙ В ОБУЧАЮЩИХ AI-СИСТЕМАХ	416-418
25.	Маер С.А. , - ИНТЕГРАЦИЯ СИСТЕМ ОБУЧЕНИЯ ДЛЯ ПОВЫШЕНИЯ УСТОЙЧИВОСТИ СОТРУДНИКОВ ОТ АТАК ТИПА ФИШИНГ	418-421
26.	Мухтарова З.Б. , - ПРОБЛЕМЫ И ВЫЗОВЫ ВНЕДРЕНИЯ МАШИННОГО ОБУЧЕНИЯ В ПРОЦЕССЫ АВТОМАТИЗИРОВАННОГО АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	421-424
27.	Мұратхан А.Р., Меірбек Ә.Қ. , -ЖАСАНДЫ ИНТЕЛЛЕКТТІ КРИПТОГРАФИЯЛЫҚ ҚАУІПСІЗДІКТЕ ҚОЛДАНУ: ШАБУЫЛДАРДЫ АНЫҚТАУ ЖӘНЕ ШИФРЛАНҒАН ДЕРЕКТЕРДІ ҚОРҒАУ	424-427
28.	Оразбаев Д., Токсент Д. - IBMQRADARSІЕМ ЖҮЙЕСІНІҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЛАСЫНДАҒЫ МҮМКІНДІКТЕРІН ШОЛУ ЖӘНЕ БАҒАЛАУ	427-429
29.	Оралбеков Е.А. Онғарбаева А.И. , - ЖЕЛІЛІК СТЕГАНОГРАФИЯ	429-432
30.	Сатыбалдина Д.Ж., Тлеубердин С.Т. - ПРИМЕНЕНИЕ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ АНАЛИЗА УЯЗВИМОСТЕЙ СЕТЕЙ И ОБНАРУЖЕНИЯ АТАК	432-435
31.	Токсент Д.Қ., Бустекбаев Т.С., Тәжмұханов А.Б. - АВТОМАТИЧЕСКОЕ ОБНАРУЖЕНИЕ УГРОЗ: МОЖЕТ ЛИ ИИ ЗАМЕНИТЬ ЧЕЛОВЕКА?	435-437
32.	Төребеков Б.Б. , -"CAPTURETHEFLAG" (CTF) ОЙЫНЫН КИБЕРШАБУЫЛДАРҒА ҚАРСЫ ТҰРУ ДАҒДЫЛАРЫН ДАМУ ТУ ӘДІСІ РЕТІНДЕ ПАЙДАЛАҢУ.	438-440
33.	Тұрсыналы А.Б. - МЕТОДЫ КРИМИНАЛИСТИЧЕСКОГО АНАЛИЗА УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ	440-443
34.	Узбаев Р.С., Мухаметжанова Б.О. -АҚПАРАТТЫҚ-КОММУНИКАЦИЯЛЫҚ ИНФРАҚҰРЫЛЫМНЫҢ КРИТИКАЛЫҚ ОБЪЕКТІЛЕРІНДЕ АҚПАРАТТЫҚ ҚАУІПСІЗДІК ҚАТЕРЛЕРІН БОЛДЫРМАУ	444-446
35.	Шегетаева А.К. - АНАЛИЗ И ПРОГНОЗИРОВАНИЕ УЯЗВИМОСТЕЙ: ИСПОЛЬЗОВАНИЕ ДАННЫХ СУЕ ДЛЯ ПОВЫШЕНИЯ КИБЕРБЕЗОПАСНОСТИ	446-449
36.	Шерехан Н.Қ. - ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ КРИПТОГРАФИЯЛЫҚ АЛГОРИТМДЕРГЕ НЕГІЗДЕЛГЕН ҰЛТТЫҚ СТАНДАРТТАРЫ: ХАЛЫҚАРАЛЫҚ ЖӘНЕ МЕМЛЕКЕТАРАЛЫҚ СТАНДАРТТАР	449-451

Еуразиялық халықаралық ғылыми конференция
«Ғылымдағы, техника мен индустриядағы жасанды интеллект және кері есептер»
Евразийская международная научная конференция
“Искусственный интеллект и обратные задачи в науке, технике и индустрии”
Eurasian international scientific conference
«Artificial intelligence and inverse problems in science, technology and industry»

1 СЕКЦИЯ

«КЕРІ ЕСЕПТЕРДІ ШЕШУДЕ ЖАСАНДЫ ИНТЕЛЛЕКТ»

СЕКЦИЯ 1

«ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В РЕШЕНИИ ОБРАТНЫХ ЗАДАЧ»

SECTION 1

«ARTIFICIAL INTELLIGENCE IN SOLVING INVERSE PROBLEMS»

UDC 528.8 A.D.

Alinova (Astana, L.N. Gumilyov ENU)
M.G. Zhartybayeva (Astana, L.N. Gumilyov ENU)
F.J. Villanueva (Ciudad Real, University of Castilla-La Mancha)
M.S. Belyaev (Vladivostok)

BATHYMETRIC MAPPING OF A LAKES BASED ON SATELLITE IMAGERY AND SEABED CHARACTER ANALYSIS USING NEURAL NETWORKS

Modern methods of water body monitoring increasingly rely on the integration of satellite data and machine learning algorithms, enabling the creation of accurate bathymetric maps with minimal costs. This study proposes an innovative approach based on deep neural networks (U-Net architecture) to predict lake depths and analyze seabed composition using the K-means clustering algorithm.

The aim of the study is to develop an automated methodology for constructing bathymetric maps of inland water bodies using Sentinel-2 satellite images, deep learning, and image processing algorithms. The key stages include data collection and filtering, dataset generation, neural network training, and post-processing of depth and bottom structure maps.

Multispectral Sentinel-2 satellite images and 1500 bathymetric lake maps from the open-source bathybase.org database were used as input data. Based on the map coordinates, satellite images were extracted and cleaned from clouds, ice, and other noise. This was followed by training set generation, augmentation, and segmentation.

The U-Net architecture was adapted for two consecutive tasks: water surface segmentation and depth regression. The first model achieved 95% accuracy in binary mask generation, and the second reached a root mean square error (RMSE) of 0.3. The K-means algorithm was used to analyze the bottom structure, with prior normalization by depth and shoreline distance, enabling semantic segmentation of sediment types.

Examples of 2D and 3D depth maps and STL-format seabed structure visualizations are presented. The method demonstrates noise resistance and scalability across various types of water bodies.

A comparison with traditional methods (Lyzenga model, OBRA algorithms, SVM) showed the superiority of the neural network approach in terms of both accuracy and versatility. The developed tool can be applied in hydrological, environmental, and engineering studies.

References

1. Lyzenga, D.R. Remote Sensing of Water Depths. 1978.
2. Stumpf, R.P. et al. Algorithms for Derivation of Water Depth. 2003.
3. Legleiter, C.J. et al. Optimal Band Ratio Analysis (OBRA). 2009.
4. Agrafiotis, P. et al. Bathymetry with Machine Learning. 2020.
5. Bathynet Project. <https://bathynet.org>

UDC 004.89:37.01

Iklassova K. (Petrovsk, KU)
Shaikhanova A. (Astana, ENU)
Tashibayev R. (Petrovsk, KU)

ARTIFICIAL INTELLIGENCE FOR SOLVING INVERSE PROBLEMS AND EXPLAINING DECISIONS IN EDUCATIONAL MANAGEMENT SYSTEMS

In the current era of digital transformation, the educational system faces the necessity of making complex managerial decisions based on the analysis of large volumes of data. Traditional methods of managing educational systems often struggle to cope with the increasing complexity of information flows and the multifactorial nature of decision-making processes. Artificial Intelligence (AI) offers innovative approaches to solving inverse problems in management and provides a new level of transparency in decision-making. The application of AI technologies for analyzing cause-and-effect relationships in educational processes is becoming particularly relevant, as it enables not only the prediction of outcomes from managerial actions but also a deeper understanding of the mechanisms underlying observed educational phenomena.

Recent advances in AI have led to the development of intelligent tutoring systems, predictive analytics, and AI-supported educational platforms aimed at improving student engagement and academic performance. However, the implementation of these technologies presents challenges, including ethical concerns related to data privacy and potential algorithmic biases. These issues have sparked discussions among educators, technologists, and policymakers regarding the fair and responsible use of AI in education [1–3]. As educational institutions continue to adopt AI-based solutions, the future of educational management systems appears promising, offering opportunities for further innovation. By addressing current challenges and harnessing the potential of AI, stakeholders in education can create a more personalized, efficient, and inclusive learning environment that accommodates the diverse needs of students [4–5].

The aim of this study is to validate and substantiate a methodological approach to applying artificial intelligence technologies for solving inverse problems in educational management, while ensuring explainability of the decisions generated, to enhance the efficiency of managerial processes. To achieve this goal, an experiment was conducted involving the development and analysis of an AI model designed to address an inverse problem in education. The objective of the experiment was to create and evaluate an artificial intelligence model capable of identifying the causes of student underperformance based on data regarding their activity and academic results. This constitutes a classical inverse problem: determining likely causes based on observed outcomes.

Stage 1. Generation of the Training Dataset.

To eliminate the risks associated with handling personal data, synthetic data generation was implemented to simulate real educational indicators. The following parameters were used: percentage of assignments completed, average score, time spent on the platform (hours per week), chat activity (number of messages), and the number of missed classes. A total of 1,000 synthetic student records were generated with a predefined logic for assigning the cause of underperformance. For example, if the number of missed classes exceeded 5, the assigned cause was "absenteeism"; if the time spent and activity were low, the cause was "lack of engagement"; in cases of low academic performance, the cause was "low motivation," and so forth.

Stage 2. Model Training.

As the baseline model, the decision tree algorithm (DecisionTreeClassifier) was selected due to its interpretability and the visual transparency of its decision-making process. The dataset was split as follows: 70% for training and 30% for testing. The model was trained on 700 student records and tested on 300. The results of training the DecisionTreeClassifier model are presented in Table 1.

Table 1. Results of Training the DecisionTreeClassifier Model

Class	precision	recall	f1-score	support
0: No issues	1.00	0.95	0.97	78
1: Did not understand the material	1.00	1.00	1.00	52
2: Lack of engagement	0.80	1.00	0.89	4
3: Low motivation	0.92	1.00	0.96	36
4: Absenteeism	1.00	1.00	1.00	130

The model demonstrated high accuracy: 99% accuracy, macro-F1 score of 0.96, with precision and recall reaching 1.00 for most classes.

Stage 3. Results Analysis.

A confusion matrix was constructed, which revealed minor classification errors, specifically in misclassifying the "No issues" class as either "Low motivation" or "Lack of engagement." All other classes were correctly identified without errors.

An analysis of feature importance was conducted, indicating that the most significant factor was the number of missed classes, followed by assignment completion rate and average score.

A decision tree was constructed to visualize the AI's logic: initial evaluation of absenteeism levels, followed by analysis of assignment completion and engagement. The experiment confirmed the feasibility of effectively applying AI models to solve inverse problems in education. The decision-making process is visualized in Figure 1.



Figure 1. Decision Tree for Identifying Causes of Underperformance

The model successfully identifies the causes of student underperformance, demonstrating high accuracy and decision-making transparency — qualities that are crucial for practical implementation in educational systems. In the next phase, it is planned to expand the experimental dataset and conduct a comparative analysis of models to determine the optimal solution in terms of accuracy, robustness, and interpretability.

The conducted study has demonstrated the effectiveness of applying artificial intelligence models to solve inverse problems in the educational domain. The decision tree model (DecisionTreeClassifier),

built on the basis of synthetic data, achieved high accuracy (99%), along with stable precision and recall metrics across all classes characterizing the causes of underperformance.

Special emphasis was placed on the interpretability of AI decisions: the visualization of the decision tree, confusion matrix, and feature importance analysis not only contributed to achieving high accuracy but also ensured the transparency and explainability of decisions — a factor that is critically important when applying AI in the management of educational processes.

This research is funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP23488869).

References

1. Michigan Virtual. (2023). AI in education: Student usage in online learning. Michigan Virtual Learning Research Institute. Retrieved from <https://michiganvirtual.org/research/publications/ai-in-education-student-usage-in-online-learning/>
2. Moore, C. (2023). AI tools for instructional designers. Cathy Moore Blog. Retrieved from <https://blog.cathy-moore.com/ai-tools-for-instructional-designers/>
3. Bakker, T. B., et al. (2023). Neural inverse rendering of participating media from RGB-D images. arXiv preprint. <https://doi.org/10.48550/arXiv.2312.00698>
4. Finnish Center for Artificial Intelligence. (n.d.). Inverse problems and AI research at FCAI. Retrieved from <https://fcai.fi/inverse-problems>
5. Hwang, G., et al. (2023). Artificial intelligence in education: Applications, challenges, and opportunities. International Journal of Educational Technology in Higher Education, 20(55). <https://doi.org/10.1186/s41239-023-00436-z>

UDC 517.958

Jinchao Pan(Nanjing, China, SEU)
Jijun Liu(Nanjing, China, SEU)

ON THE SIMULTANEOUS RECOVERY OF BOUNDARY IMPEDANCE AND INTERNAL CONDUCTIVITY

Consider an inverse problem of the simultaneous recovery of boundary impedance and internal conductivity in the electrical impedance tomography (EIT) model using local internal measurement data, which is governed by a boundary value problem for an elliptic equation in divergence form with Robin boundary condition. We firstly express the solution to the forward problem by volume and surface potentials in terms of the Levi function. Then, for the inverse problem, we prove the uniqueness of the solution in an admissible set by unique extension of the solution under some a priori assumption. Finally we establish the regularizing reconstruction schemes for boundary impedance and internal conductivity using noisy measurement data with rigorous error estimates. The mollification method is proposed to recover the boundary impedance from the boundary condition, and the internal conductivity with known boundary value is recovered from an integral system, where the Tikhonov regularization is applied to seek the stable solution with suitable regularizing parameter, considering that the error involved in the boundary impedance coefficient reconstruction will propagate to the recovering process for internal conductivity. Numerical implementations are presented to illustrate the validity of the proposed method.

UDC 004.9

Jomartova Sh.A. (Almaty, Al-Farabi Kazakh National University) Mazakova A.T. (Almaty, Al-Farabi Kazakh National University) Ziyatbekova G.Z.* (Almaty, Al-Farabi Kazakh National University;
Almaty Technological University), Aliaskar M.S. (Almaty, Al-Farabi Kazakh National University; International University of Engineering and Technology) Zhaksymbet A.T. (Almaty, Al-Farabi Kazakh National University)

HARDWARE-SOFTWARE COMPLEX FOR MONITORING THE LEVEL OF WATER BODY OCCUPANCY

The purpose of this work is to develop a hardware and software system for monitoring the breach of hydraulic structures, such as dams and weirs. The relevance of this work is due to the increasing frequency and scale of catastrophic floods caused by the destruction of hydraulic structures, which requires effective methods of forecasting and preventing such events. The methods and models proposed in this paper are of considerable practical importance for risk assessment, planning evacuation measures and minimizing damage from emergencies associated with dam and levee failures [1].

The territory of Kazakhstan has significant water resources. Lakes and rivers are sources of fresh water, which is used both in sustenance of the country's population and for irrigation of agricultural land. There are moraine lakes located at high altitudes in mountainous areas of Kazakhstan. The use of water as a source of energy contributed to the development of the hydropower industry in Kazakhstan. There are more than 30 hydropower plants in the country. However, the fact remains the destructive power of water, capable of sweeping away entire settlements in its path. The danger lurks not so much in flooding as in the possibility of debris flows that can carry rocks, ice blocks, etc.

At present there are 1665 hydraulic structures on the territory of the Republic, including reservoirs with the volume of more than 1.0 m³ – 319 pieces (of them in the republican ownership – 83 pieces, in communal ownership – 200 pieces, in private ownership – 34 pieces and ownerless – 60 pieces); dams – 443 pieces (of them in the republican ownership – 32 pieces, in communal ownership

346 pieces, in private ownership – 45 pieces and ownerless – 20 pieces); dams

125 pieces and other hydraulic structures – 778 pieces. To date, such large reservoirs as Astana reservoir built in 1970 with a capacity of 410.9 million m³, Seletinskoye in 1965 (230 million m³), Kargalinskoye in 1975 (280 million m³), Bartogay in 1982 (320 million m³), Kapshagay in 1970 (18560 million m³) are in operation, Ters-Ashchibulak in 1963 (158.6 million m³), Tasotkel in 1974 (620 million m³), Samarkand in 1939

(253.7 million m³), Upper Tobolsk in 1972 (816.6 million m³), Karatomar in 1965

(586 million m³), Bugun in 1967 (370 million m³) and others [2].

Monitoring systems should ensure constant observation of phenomena and processes occurring in nature and the technosphere in order to anticipate growing threats to humans and their habitat. The main purpose of monitoring is to provide data for accurate and reliable forecasting of emergency situations on the basis of combining intellectual, informational and technological capabilities of various agencies and organizations involved in the observation of certain types of hazards. Monitoring information serves as a basis for forecasting [3-4].

Microprocessor technology has now actively entered our lives. Versatility, flexibility, simplicity of hardware design, practically unlimited possibilities for complication of information processing algorithms – all this promises a great future for microprocessor technology. Microprocessors are used both in household appliances for simple signal processing and command generation, and in the most complex measurement systems for digital signal processing.

The temporary capacity to develop a wide range of different sensors and cheaper micro-processes has also opened up a wide range of possibilities for the introduction of advanced technology for the implementation of climate-change monitors. In particular, a relatively cheap Arduino controller, which has a large base of developed sensors and means of their communication with the computer, has been widely used in applied tasks.

For practical application, real-time monitoring systems for water bodies are being developed, based on automation of the process of information collection and processing. Generally, automated monitoring systems use the following sensors: inclinometric; leakage; deformation; temperature; ground pressure; water level, wind direction and strength.

In the operation of hydraulic structures, in particular dams, the failure of the pressure front of hydroelectric facilities is one of the most dangerous cases of accidents, leading to significant economic, environmental and social consequences, as well as affecting to a large extent the ecology of the downstream of hydroelectric facilities. For monitoring information systems, it is necessary to ensure real-time data collection.

Water level measurement equipment can be of different types. The measurement equipment will interface with the data transmission subsystem and the power supply subsystem to ensure system operation. Coupling of the above systems will allow monitoring of water levels in moraine lakes, the location of which is extremely difficult to access. Technical means measuring water level should be capable of receiving data from sensors at various intervals. As mentioned above, data from the measurement equipment will be transmitted to the data collection and processing center via low-orbit space communications systems [5].

The accumulated data will be transmitted to the situation centers and used by special services for forecasting possible floods and floods, calculating water consumption and other purposes. The monitoring system may be linked to other automated systems, such as water intake and discharge systems at hydroelectric dams, alarm systems, and other functionally interconnected systems. Implementation of the water level monitoring system will allow preventing emergencies.

Based on the application of microprocessor technology and sensor technology, an autonomous microcomputer-based climate data transmission system was developed. A real-time breaching wave factor monitoring program is established using a mathematical model capable of continuously monitoring reservoir occupancy levels and estimating the likelihood of dam failure. A water level monitoring method based on fuzzy and interval math is proposed. The accumulated data will be transmitted to the situation centers and used by specialized services for forecasting possible floods, water resource calculation and other purposes. The monitoring system can be integrated with other automated systems, such as hydropower plant catchment management systems, alarm systems and other interconnected functional systems. Implementation of the water level monitoring system implies prevention of emergencies.

Reference

1. Moldabekov M.M., Eremir D.I., Poniatov Y.A. Monitoring of water level, lakes, rivers of seas and hydraulic structures // Bulletin of KazNTU. - Almaty, 2013. – No.1. - Pp. 3-6.
2. Mazakov T.Zh., Ziyatbekova G.Z. Consequences of the destruction of hydraulic structures and emergencies // Proceedings of the International Conference. - Almaty: KazATK named after M. Tynyshpayev, 2018. –Vol. 2. - Pp. 74-78.

3. Striganova M.Yu. Methods of assessment and prediction of consequences in the destruction of hydraulic structures // Bulletin of the Command and Engineering Institute of the Ministry of Emergency Situations of the Republic of Belarus, 2012. – No. 1(15). - Pp. 10-21.
4. Platt C. Electronics: logic circuits, amplifiers and sensors for beginners. - SPb.: BHV-Peterburg, 2015. - 448 p.
5. Igo T. Arduino, sensors and networks for device communication

UDC 004.8

Kuanysh Absalyam (L.N. Gumilyov ENU, Astana, Kazakhstan)
Khuralay Moldamurat (L.N. Gumilyov ENU, Astana, Kazakhstan)
Cengiz Hajizadeh (Istanbul teknik üniversitesi, Istanbul, Turkey)

ALGORITHM FOR USING ARTIFICIAL INTELLIGENCE IN PREDICTING FIRE DANGER IN THE SEMEY FOREST IN KAZAKHSTAN

Abstract – This article presents an algorithm for using artificial intelligence to predict fire danger in the forests of the Semey region of Kazakhstan. The study analyzes the main factors influencing the occurrence of wildfires, including meteorological parameters (temperature, humidity, wind speed, and atmospheric pressure), as well as the ecological characteristics of the region. A mathematical model has been developed to assess the probability of fire occurrence, and an algorithm for its implementation in the MATLAB software environment is proposed.

Keywords – artificial intelligence, fire prediction, Semey forest, machine learning, neural networks, MATLAB.

INTRODUCTION

Methods used in foreign wildfire prediction systems (according to the authors' opinion based on the article) [1].

In 2023, a large wildfire occurred in Semey Forest, Kazakhstan, caused by lightning strikes in the Abai region. The fire, which began on June 8, was fully extinguished by July 13 [2]. Semey Forest plays a critical role in fire prediction systems, and its ecosystem is at risk due to climate change and human activities like tourism. Effective fire prediction methods are essential to protect this unique natural area.

Artificial Intelligence (AI) helps analyze complex data to predict forest fires. Data from Kazakhstan's National Hydrometeorology Center, including temperature, wind speed, and humidity, was used to create a database for the AI system. AI algorithms can process meteorological data, vegetation characteristics, and fire history to predict fire risks.

Fire risk modeling relies on key data, such as weather conditions, vegetation types, fire history, and soil fertility. Neural networks and machine learning methods are used to develop AI models that assess fire probability. Kazhydromet provides preliminary weather forecasts, which will help predict fire risks for July and August 2025.

To predict forest fire risks in Semey, AI systems with fuzzy logic are used to make decisions based on data from ground sensors. These systems help plan actions and make real-time decisions for fire risk prediction [3]. The use of AI ensures accurate and timely predictions, improving fire management and preparedness [4].

As the number of sensors increases, a group control method is applied within the AI system, enabling better coordination of multiple fire sources. This system helps manage fire monitoring efficiently

and supports better planning for firefighting and rescue operations. Real-time data from the sensors helps ensure the system can effectively carry out tasks and respond to fires in the field.

RESULTS AND DISCUSSION

Modeling in the MATLAB R2023a environment was used to determine the probability of fire occurrence in June based on hazardous weather indicators, predicting fire risk in the Semey forest. The research utilizes artificial intelligence for early forest fire prediction. MATLAB programming methods allowed for the analysis of environmental parameters and their relationship to fire probability. Trained models predict fire occurrence under given conditions, notifying emergency services when a risk threshold is reached for quick response.

Graphs were generated to illustrate the dependence of fire probability on various factors. The first graph shows how temperature influences fire probability, with higher temperatures leading to an increased risk, confirming established scientific findings. The second graph illustrates the relationship between atmospheric pressure and fire probability. Unlike temperature, the pressure's effect is more complex, with other factors like humidity and wind speed influencing fire risk. The final diagram demonstrates the impact of wind speed on fire probability, showing that higher wind speeds accelerate fire spread.

While meteorological data is crucial for predicting fire probability, it's important to account for errors and uncertainties in measurements. Temperature, pressure, humidity, and wind speed are recorded using different devices, each of which may introduce measurement errors, affecting prediction accuracy.

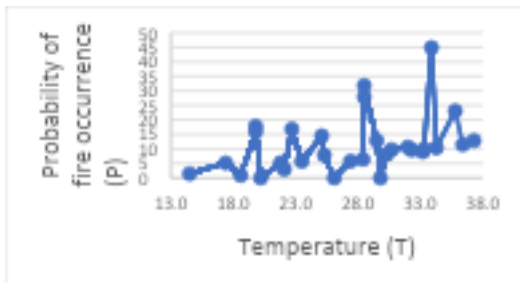


Figure 1. Graphical display window of fire probability and temperature

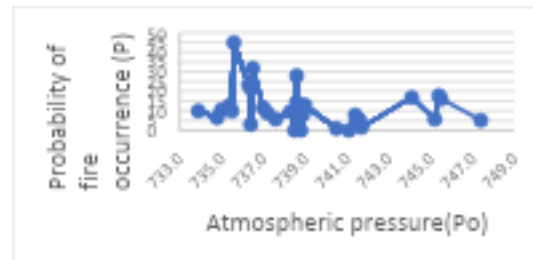


Figure 2. Graphical display window of fire probability dependence on atmospheric pressure.

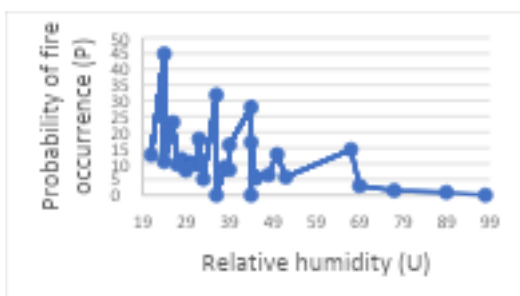


Figure 3. Graphical display window of fire probability dependence on Relative humidity.

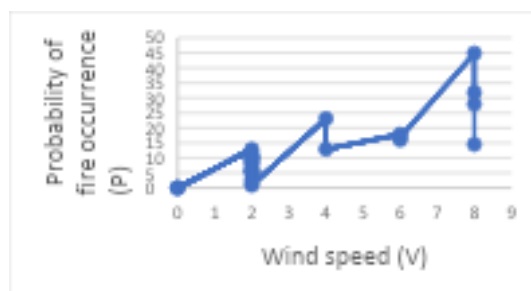


Figure 4. In the graphical display window of fire probability dependence on wind speed, it is possible to predictively consider the occurrence of fire hazard by looking at the coefficients.

CONCLUSION

The integration of an artificial intelligence system into the forest fire hazard prediction system in Semey's forests, Kazakhstan, significantly enhances the effectiveness of wildfire prevention efforts. Various AI-based methods have been considered, and fuzzy logic was applied to database-driven

predictions. Thanks to accurate and rapid forecasts, it becomes possible to analyze local forest areas and horizon resources in detail. This research demonstrates that AI-driven real-time monitoring can provide rapid responses to emergencies, improving fire hazard mitigation and ensuring the efficient execution of rescue operations. Furthermore, studying the likelihood of fire outbreaks in forest areas helps preserve unique ecosystems. Investing in AI technologies and integrating them into existing management systems is a crucial step toward ensuring Kazakhstan’s long-term environmental security.

REFERENCES

- [1] H., Kinatas, Hasan, N.M., Chingiz Hajiyeu, Null M., Adaptive Fault-Tolerant Multiplicative Attitude Filtering for Small Satellites, International Journal of Adaptive Control and Signal Processing, 2025
- [2] Intelligent obstacle avoidance algorithm for safe urban monitoring with autonomous mobile drones. D., Yedilkhan, Didar, A.E., Kyzyrkanov, Abzal Ermekebayuly, Z.A., Kutpanova, Zarina A., S.A., Aljawarneh, Shadi A., S.K., Atanov, Sabyrzhan Kubeysinovich, Journal of Electronic Science and Technology, 2024
- [3] Moldamurat A. Computer Simulation of the Path and Control of an Intelligent Mobile Robot in Python. 2021 16th International Conference on Electronics Computer and Computation, ICECCO 2021, 2021;
- [4] Moldamurat Kh., Utegen, A.S., Brimzhanova, S.S., Kalmanova, D.M., Yrskeldi, N.G. Development of a software simulator for small satellite swarm control, Proceedings - 2021 16th International Conference on Electronics Computer and Computation, ICECCO 2021, 2021
- [5] Kazakhstan State Hydrometeorological Service, Homepage [website], <https://www.kazhydromet.kz/ru/>

UDC 004.896

Kuatbayeva A.A. (Astana IT university),
Sergaziyev M.Zh. (Astana IT university),
Yedilkhan D. (Astana IT university),
Gizatov A. (Astana IT university), Issenov D. (Astana IT university),
Namet A. (Astana IT university), Bekbolatov O. (Astana IT university)

Abstract. Traffic congestion and transportation-related environmental issues are significant challenges worldwide. Due to their negative effects on individuals, as well as their economic, environmental, and societal costs, substantial investments and numerous initiatives have been implemented to address these problems. In many cities, commuters primarily depend on private vehicles, highlighting the need for cost-effective and environmentally friendly alternatives to improve urban mobility. Providing more accurate and timely bus arrival information could enhance the convenience of public transportation, encouraging its use. (European Commission 2013; Wardman 2014). The research investigates various machine learning techniques for predicting bus arrival times based on historical data. Models such as K-means clustering, KNN, Conv-LSTM, SVM, and Linear/Logistic Regression were designed and evaluated. The study focuses on accuracy, model performance, and the implementation of various metrics like Mean Absolute Error (MAE), Mean Squared Error (MSE), and model accuracy. Results were visualized and analyzed to assess model effectiveness.

1. Introduction Accurate prediction of bus arrival times is crucial for improving public transport efficiency. This article thesis presents different machine learning models used to predict bus arrival times using time-series data for Astana city based on real-time data sets. **Background.** A key issue with public

transport buses is their inconsistent adherence to schedules, leaving commuters without real-time updates on expected arrival times. Due to this lack of crucial information, many passengers may opt for private vehicles instead, reducing the share of public transport usage [1-2]. This shift increases the number of private vehicles on the road, exacerbating congestion and its associated negative effects. Therefore, accurately predicting travel and arrival times and providing this information to passengers is essential for making public transportation more appealing, efficient, and competitive, particularly in urban areas. The use of machine learning algorithms has grown significantly in transportation systems, particularly in the context of predictive analytics. Predicting the arrival times of buses helps reduce wait times and improve passenger satisfaction [3]. **Purpose.** This study aims to develop and evaluate different machine learning models to predict bus arrival times, enhancing the decision-making process for public transport systems. The goal is to achieve accuracy above 85% for the various models. **2. Methodology: Data Preprocessing:** Two datasets were merged, cleaned, and time features were extracted (hour, minute, day, weekday). The target variable was selected as the hour of bus arrival. **Models Designed:**

- **K-means Clustering:** Used to group similar bus data based on features.
- **KNN (K-Nearest Neighbors):** A regression-based model used for predicting arrival times.
- **Conv-LSTM (Convolutional Long Short-Term Memory):** A deep learning model designed for time-series forecasting.
- **SVM (Support Vector Machine):** A powerful model for classification and regression tasks.
- **Linear/Logistic Regression:** A simple yet effective model for predicting continuous values like arrival times.
- **Performance Metrics:**
 - **Mean Absolute Error (MAE):** Measures the average magnitude of errors in predictions.
 - **Mean Squared Error (MSE):** Penalizes larger errors more heavily by squaring them.
 - **Accuracy:** Evaluated using a threshold of 85% or higher for each model.

Datasets. Two datasets are used to predict bus arrival time prediction.

1) <u>modified PassFlow (1) (1).csv</u>										2) <u>modified PassFlow2 (1).csv</u>									
passflow1										passflow2									
id	bus_stop_id	bus_id	enter_sum	exit_sum	bus_board_computer	sent_time	created_time	route_number	tickets_count	id	bus_stop_id	bus_id	enter_sum	exit_sum	bus_board_computer	sent_time	created_time	route_number	tickets_count
1713411380	4994	1607	29	16	2024-12-07T12:18:33.793	2024-12-07T12:23:55.523	50	2		1997	1168	5	9	2024-12-11T05:51:22.895	2024-12-11T05:52:45.07	50	6	1686011810	
1030917530	3880	1671	34	22	2024-12-07T15:19:20.206	2024-12-07T15:19:23.303	50	4		3818	4335	17	42	2024-12-11T06:05:45.965	2024-12-11T06:06:39.799	50	6	1495655118	
1631759213	1312	1665	32	30	2024-12-07T09:23:26.477	2024-12-07T09:26:44.387	12	14		4877	2385	45	49	2024-12-11T06:08:48.971	2024-12-11T06:10:01.318	50	3	1001965165	
1980354232	3963	2729	20	25	2024-12-07T09:13:17.893	2024-12-07T09:21:03.48	50	3		4686	1877	48	40	2024-12-11T06:11:44.122	2024-12-11T06:12:58.347	50	27	179531137	
1779402183	3880	4754	48	12	2024-12-07T16:17:55.33	2024-12-07T16:26:58.704	50	32		4691	3483	24	41	2024-12-11T06:12:54.122	2024-12-11T06:13:48.876	50	16	116269695	
1676920983	3071	2709	13	19	2024-12-08T06:40:04.877	2024-12-08T06:45:51.672	50	5		1545	3944	39	9	2024-12-11T06:13:08.862	2024-12-11T06:13:53.329	50	12	151646499	
1893573496	1782	4867	38	31	2024-12-07T08:28:39.735	2024-12-07T08:27:37.672	50	8		4438	3940	3	6	2024-12-11T06:14:00.175	2024-12-11T06:15:03.808	50	3	182607913	
1136106360	4169	3342	28	23	2024-12-07T12:28:36.696	2024-12-07T12:35:25.355	50	17		2403	1298	12	36	2024-12-11T06:15:52.108	2024-12-11T06:16:48.396	50	1	137957180	
1558713849	4069	2323	1	32	2024-12-09T05:55:23.823	2024-12-09T05:56:21.212	50	0		2398	1075	7	30	2024-12-11T06:17:05.162	2024-12-11T06:17:41.343	50	1	1548282189	

3. Results

Evaluation Metrics: The following formulas were used to evaluate each model:

MAE Formula:	$MAE = \frac{1}{n} \sum_{i=1}^n y_i - \hat{y}_i $
MSE Formula:	$MSE = \frac{1}{n} \sum_{i=1}^n (y_i - \hat{y}_i)^2$
Accuracy Formula:	$Accuracy = 100\% - MAPE$

Accuracy Formula:

Model Evaluation Results: For each model, the following results were obtained: **KNN:** Accuracy = 99.87%. **Conv-LSTM:** Accuracy = 96.47%

SVM: Accuracy = 99.53%, **Linear Regression:** Accuracy 92.42%

Table 1. Graphics.

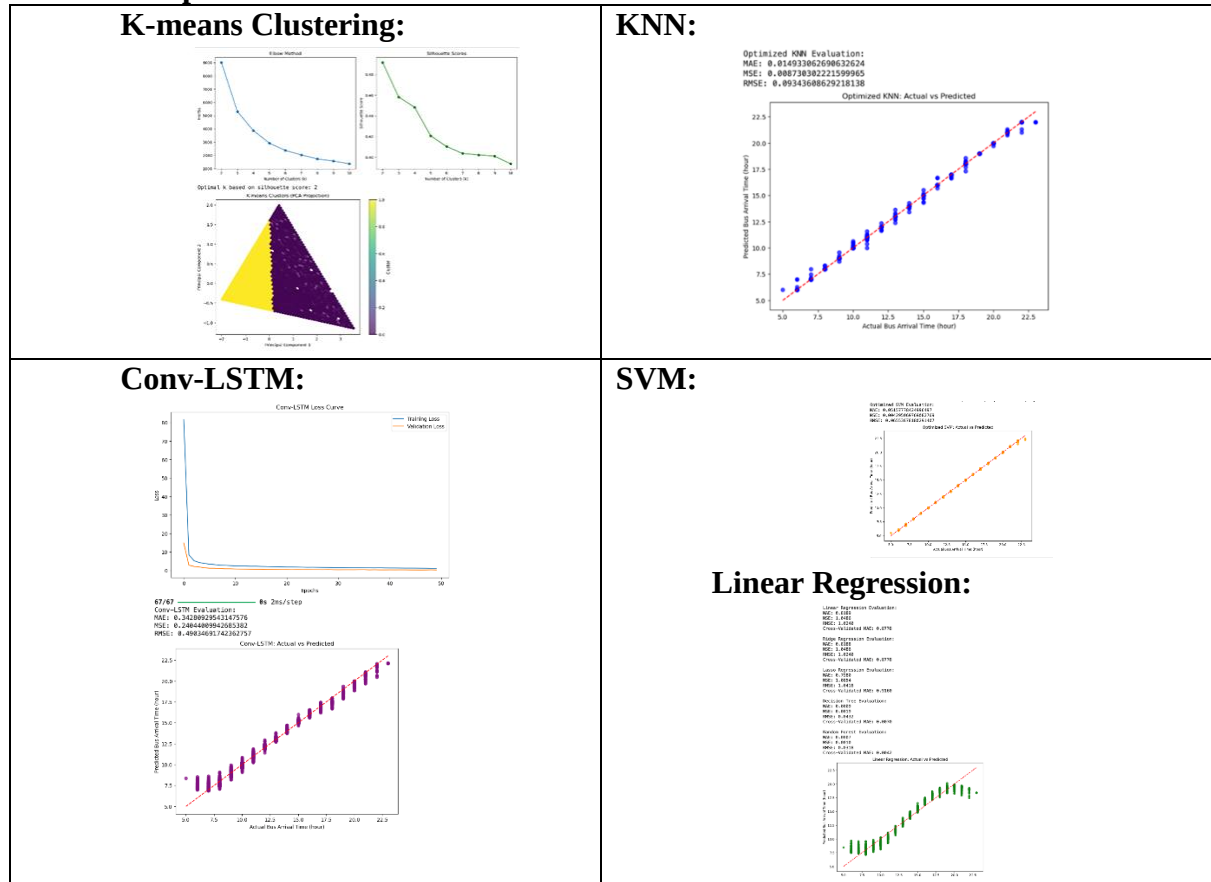


Table 2. Calculated values for each model comparison

4. Discussion

A comparison between the models reveals that some algorithms outperform others in terms of accuracy,

Model	MAE	MSE	RMSE	MAPE (%)
K-means	NaN	NaN	NaN	NaN
KNN	0.0149	0.0087	0.0934	0.13
Conv-LSTM	0.3428	0.2404	0.4903	3.53
SVM	0.0516	0.0043	0.0655	0.47
Linear Regression	0.8189	1.0486	1.0240	7.58

while others perform better for smaller error metrics.

5. Conclusions

The study demonstrates the effectiveness of machine learning techniques in predicting bus arrival times. Most models achieved the required accuracy of over 85%. The results underscore the importance of feature selection, model complexity, and training data quality in enhancing prediction accuracy.

Aknowledgement

This research has been funded by the Ministry of Science and Higher Education of the Republic of Kazakhstan, grant number BR24992852 "Intelligent models and methods of Smart City digital ecosystem for sustainable development and the citizens' quality of life improvement".

Literature:

1. Ashwini, B. P., Sumathi, R., & Sudhira, H. S. (2022). A dynamic model for bus arrival time estimation based on spatial patterns using machine learning. *arXiv preprint, arXiv:2210.00733*. Retrieved from <https://arxiv.org/abs/2210.00733>
2. Müller-Hannemann, M., Rückert, R., Schiewe, A., & Schöbel, A. (2021). Estimating the robustness of public transport systems using machine learning. *arXiv preprint, arXiv:2106.08967*. Retrieved from <https://arxiv.org/abs/2106.08967>
3. Yakut, A. (n.d.). K-Means Bus Cluster: Bus time arrival cluster by K Means algorithm [GitHub repository]. *GitHub*.

UDC 004.023

Yi Tang (Minsk, BSUIR)
D. Pertsau (Minsk, BSUIR)
M. Tatur (Minsk, BSUIR)

ENHANCED A* ALGORITHM FOR GLOBAL PATH PLANNING

Global path planning is a fundamental component of autonomous navigation systems, enabling robots and vehicles to traverse complex environments efficiently and safely. While the traditional A* algorithm is widely used for its optimality and completeness in static environments, it suffers from several limitations, including suboptimal path smoothness, insufficient safety margins, and lack of adaptability to varying obstacle densities. To address these challenges, we propose an Enhanced A* Algorithm for Safe and Smooth Navigation, which incorporates dynamic heuristic weighting, obstacle-aware safety mechanisms, and B-spline-based path smoothing. These enhancements enable the generation of globally optimal paths that are both safe and smooth, making the algorithm suitable for real-world navigation scenarios.

The proposed algorithm introduces three key innovations. First, a dynamic heuristic cost function is designed to adaptively balance the actual cost and heuristic cost during the search process. By incorporating factors such as path depth and obstacle density, the algorithm dynamically adjusts the heuristic weights, ensuring robust performance in environments with varying complexity. Second, inspired by [1], a safety enhancement mechanism evaluates obstacle density and enforces a minimum safety distance, ensuring that the generated paths maintain a safe clearance from obstacles. Third, a path smoothness optimization module removes redundant nodes and applies B-spline fitting to produce continuous and smooth trajectories, addressing the discontinuities and sharp turns often observed in traditional A*-based paths.

Table1 Comparison of global path with different methods

Method	ANP	APL	ATA	ANUP	APT
Dijkstra	22	29	341.15	9	0.0014
A*	23	28	349	8	0.0028
Enhanced A* (Ours)	13	32	357.27	0	0.0485

To validate the effectiveness of the proposed algorithm, we conducted extensive experiments on a custom dataset comprising 100 randomly generated grid maps with obstacle densities ranging from 10% to 40%. The evaluation metrics included average number of points (ANP) average path length (APL), average turning angle (ATA), average number of unsafe points (ANUP), and average planning time (APT) [2]. Comparative analysis with baseline methods, including the traditional A* and Dijkstra algorithms, demonstrated that our enhanced A* algorithm consistently outperforms these methods across all metrics in Table 1. Specifically, our approach achieves zero unsafe points across all obstacle densities, generates smoother trajectories with higher average turning angles, and reduces the average number of path points, thereby simplifying the path structure. Although the computational time of our method is slightly higher due to the optimization steps, it remains within the range of real-time feasibility.

Comparison

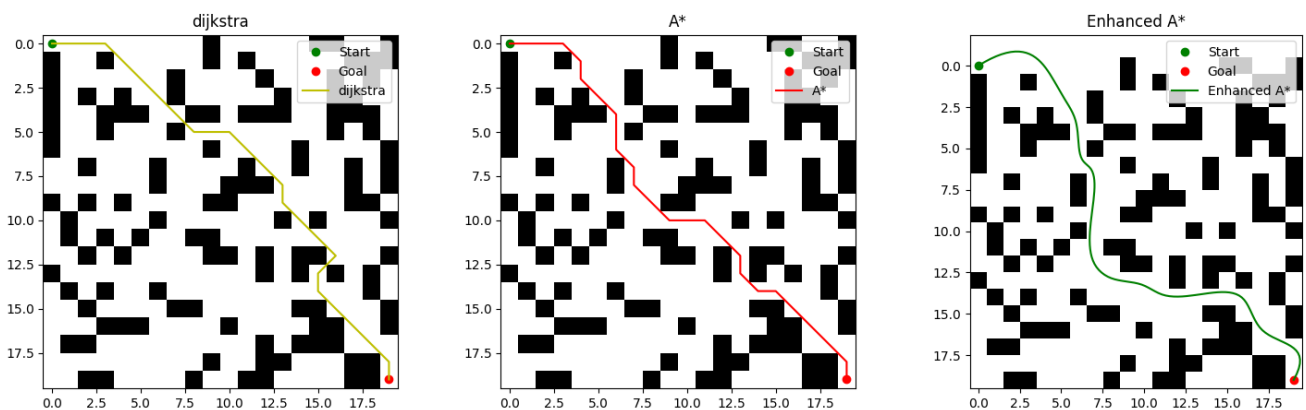


Figure 1 - Visualization of different global path planning algorithm

Qualitative results in Figure 1 further highlight the advantages of our approach. Visualization of the generated paths across varying obstacle densities shows that the enhanced A* algorithm produces safer and smoother trajectories compared to baseline methods. For example, in high-density environments, our algorithm effectively avoids unsafe regions, eliminates redundant nodes, and generates continuous paths suitable for practical navigation. In contrast, traditional A* and Dijkstra algorithms often produce fragmented paths with sharp turns and minimal clearance around obstacles, which are less suitable for real-world applications.

Reference

- [1] Li, K., Gong, X., Tahir, M., Wang, T., & Kumar, R. (2023). Towards path planning algorithm combining with A-star algorithm and dynamic window approach algorithm. *International Journal of Advanced Computer Science and Applications*, 14(6).
- [2] Li, X., Hu, X., Wang, Z., & Du, Z. (2020, October). Path planning based on combination of improved A-STAR algorithm and DWA algorithm. In *2020 2nd International Conference on Artificial Intelligence and Advanced Manufacture (AIAM)* (pp. 99-103). IEEE.

УДК 519.63

Афанасьева С.Д. (Владивосток, ДВФУ)

РЕШЕНИЕ СИНГУЛЯРНО-ВОЗМУЩЕННЫХ КРАЕВЫХ ЗАДАЧ В ДВУМЕРНОМ СЛУЧАЕ С ИСПОЛЬЗОВАНИЕМ МЕТОДА PINN

Сингулярно-возмущенные задачи представляют собой класс задач математической физики, в которых малый параметр при старшей производной приводит к появлению пограничных или внутренних слоев. Такие задачи возникают при математическом моделировании многих физических процессов, например в гидродинамике, теории упругости, биологии. Традиционные численные методы, такие как метод конечных разностей или метод конечных элементов, сталкиваются с трудностями при решении сингулярно-возмущенных задач из-за необходимости сгущения сеток в областях быстрых изменений неизвестной функции [1]. В докладе рассматривается подход к решению двумерных уравнений диффузии-конвекции-реакции с использованием метода Physics Informed Neural Networks (PINN). Метод основан на аппроксимации неизвестной функции нейронной сетью путем ее обучения на минимизацию квадратичного функционала качества, включающего слагаемые для невязки уравнений и граничных условий.

Рассматривается уравнение диффузии-конвекции-реакции в двумерной области R^2 с границей $\partial\Omega$ вместе с граничными условиями первого рода [1]:

$$-\varepsilon \Delta u + 2u_x + 2u_y + a_1 x u + a_2 y u + f(x, y, u) = 0,$$

$$x, y \in \Omega,$$

1

$$u|_{\partial\Omega} = u_b, \quad \#2$$

где $\varepsilon \ll 1$ — малый параметр, $u(x, y)$ — искомая функция.

В рамках доклада рассматривается решение задачи (1)-(2) методом PINN и его различными модификациями. Производится сравнение с решением, полученным методом конечных элементов при использовании алгоритма итеративной адаптации сетки под градиент решения. Исследуется влияние различных модификаций метода PINN на сходимость метода.

Список литературы

1. Лисейкин, В. Д. Разностные сетки. Теория и приложения — Новосибирск: СО РАН, 2014 — 256 с.

2. Raissi M., Perdikaris P., Karniadakis G.E. Physics-informed neural networks: A deep learning framework for solving forward and inverse problems involving nonlinear partial differential equations // Journal of Computational Physics. 2019. V. 50. No. 3. P. 686–707

УДК 519.622.2

Бектемесов Ж.М. (Алматы, КазНУ им. аль-Фараби)

Бектемесов М.А. (Алматы, ИИВТ)

О НЕКОТОРЫХ МЕТОДАХ РЕШЕНИЯ ОБРАТНЫХ ЗАДАЧ ДЛЯ МОДЕЛИРОВАНИЯ МЕТАСТАЗОВ РАКОВОЙ ОПУХОЛИ

Рак предстательной железы входит в топ-5 самых смертоносных раковых новообразований среди мужчин [1]. В то время как, метастазы в кости являются наиболее частым осложнением при раке простаты, сокращая продолжительность жизни у пациентов с прогрессирующим раком простаты, поскольку не реагируют на традиционную молекулярную таргетную терапию. Хотя лечение радиоактивным изотопом Радием-223 (^{223}Ra) показало многообещающие результаты, перед учеными все еще стоит задача по оптимизации терапии. *In vivo* исследования играют ключевую роль в оптимизации терапии радием, но сталкиваются с рядом ограничений, снижающих их эффективность. Такого рода исследования проводились следующим образом, где [2] авторы внедряли лабораторным мышам в кость инженерно сконструированные костные ткани, а далее вводили флуоресцентные клетки рака простаты и далее подсчитывали клетки опухоли. Интеграция *in vivo* экспериментов с моделями *in silico* позволяет преодолеть эти барьеры и повысить качество анализа.

Существующие вычислительные модели, описывающие реакцию опухоли на ^{223}Ra , зачастую требуют значительных вычислительных ресурсов. В связи с этим в данной работе предлагается альтернативное решение, которое является универсальным и более эффективным с точки зрения вычислений.

Была разработана математическая модель на основе уравнений в частных производных (PDE) для описания воздействия ^{223}Ra на метастазы рака простаты в костях [3]:

$$\{C \partial_t - \rho \Delta C = \alpha C(1 - C/C_{\max}) - gC, \quad C|_{\partial\Omega} = 0, \quad C|_{t=0} = C_0$$

где $C = C(x, t)$ обозначает плотность распределения раковых клеток в пространстве x и времени t , $\rho > 0$ – диффузионный коэффициент, α – митоз, т.е. рост раковых клеток, g – апоптоз, т.е. умирание раковых клеток, а $C_{\max}$ – допустимое количество раковых клеток на единицу рассматриваемой площади.

Данная модель анализирует динамику митоза и апоптоза на основе экспериментальных данных как контрольной группы – без лечения, так и группе с применением лечения.

Для верификации модели в работе были рассмотрены три терапевтических сценария: отсутствие лечения, постоянное воздействие ^{223}Ra и терапию с учетом полу-распада ^{223}Ra . В каждом случае было проведено моделирование роста опухоли.

Полученные результаты хорошо согласуются с экспериментальными данными, демонстрируя, что предложенная модель точно отражает терапевтический потенциал ^{223}Ra . Это подтверждает её эффективность и перспективность как инструмента для оптимизации лечения метастазов в костях.

Данное исследование финансировалось Комитетом науки Министерства науки и высшего образования Республики Казахстан (грант № AP26103465).

Список использованных источников

1. O. Bergengren, K. R. Pekala, K. Matsoukas, J. Fainberg, S. F. Mungovan, O. Bratt, et al., 2022 update on prostate cancer epidemiology and risk factors—a systematic review, *European Urology*, 84 (2023), 191–206. <https://doi.org/10.1016/j.eururo.2023.04.021>

2. Dondossola E., Casarin S. An agent-based model of prostate Cancer bone metastasis progression and response to Radium223 // BMC Cancer. – 2019. – Vol. 20(1). – P. 605.

3. Zholaman Bektemessov, Laurence Cherfils, Cyrille Allery, Julien Berger, Elisa Serafini, Eleonora Dondossola, Stefano Casarin. On a data-driven mathematical model for prostate cancer bone metastasis[J]. AIMS Mathematics, 2024, 9(12): 34785-34805. doi: 10.3934/math.20241656

ӘОЖ 519.677.

Бектемесов Ж.М. (Алматы, Әл-Фараби ат. ҚазҰУ)
Социалова Ұ.Қ. (Алматы, Абай ат. ҚазҰПУ)

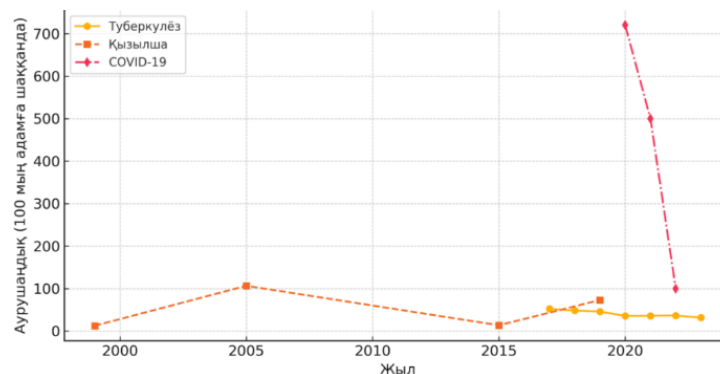
ЖАСАНДЫ ИНТЕЛЛЕКТ АРҚЫЛЫ ҚАЗАҚСТАНДАҒЫ ИНФЕКЦИЯЛЫҚ АУРУЛАРДЫҢ ТАРАЛУЫН ТАЛДАУ

Эпидемиологиялық ғылыми-техникалық жетістіктерде деректерді өңдеу мен талдаудың математикалық тәсілдеріне бағытталған әдістерді қолдану бүгінгі күннің талабы. ЖИ технологиялары мен математикалық модельдерді біріктіре отырып, эпидемиологиялық үрдістерді болжау, індеттердің таралу заңдылықтарын анықтау және алдын алу шараларын тиімді оңтайландыруға мүмкіндік береді.

Өртүрлі елдердің ғылыми зерттеулері жұқпалы аурулардың таралуын модельдеуде айтарлықтай жетістікке қол жеткізгендігі байқалады. Атап айтқанда, Түркияда вакцинацияланған адамдардың ауруды жұқтыру мүмкіндігін ескеретін қызылшаның таралу динамикасының детерминирленген моделі әзірленген. Қытайда қызылша инфекциясының маусымдық ауытқуын сипаттау үшін сандық модельдеу ұсынылған. Сонымен қатар, [1-2] мақалаларында алынған нәтижелер туберкулез инфекциясының таралуы жағдайында халықты жаппай скринингтік тексеру қажеттілігін айқын көрсетеді, бұл бактериялық экскреция мен туберкулезбен ауыратын науқастарды уақтылы анықтауға мүмкіндік береді. COVID-19 пандемиясының таралуын болжау үшін де жаңа математикалық модель мен оның шешу әдістері құрастырылды [3].

Эпидемиологиялық процестерді математикалық модельдер, соның ішінде детерминирленген (мысалы, SIR, SEIR) және стохастикалық тәсілдер арқылы сипаттауға болады. Бұл модельдер инфекцияның таралу заңдылықтарын талдауға, індеттердің динамикасын болжауға және тиімді араласу стратегияларын жасауға мүмкіндік береді. Эпидемиологиялық модельдеу мен машиналық оқыту алгоритмдерін біріктіретін аралас тәсіл жұқпалы ауруларды болжау дәлдігін жақсартады және жауаптарды жылдам бейімдей алады. Айталық, COVID-19 ауруы таралуын болжауда нақты уақытта параметрлерді реттеу үшін SEIR математикалық моделінің теңдеулерін нейрондық желілермен біріктіретін гибриді модельдер пайдаланылады.

COVID-19, туберкулез немесе қызылша сияқты жұқпалы аурулардың таралуы Қазақстанды да айналып өтпеді. Мысалға, коронавирус инфекциясын халықтың 8,1%-ы жұқтырған, бұл әрбір 1000 адамға шаққандағы өлім-жетім деңгейі 1,03 адамды құрайды [4]. 2024 жылдың мамыр айында Еуропа елдеріндегі қызылша ауруы таралуының ай сайынғы жаңартылған деректерге сәйкес аурулар саны бойынша Қазақстан, Әзірбайжан және Ресей көш бастады [5].



Сурет 1. Қазақстандағы COVID-19 (2020-2022 ж.), қызылша (1999-2019 ж.) және туберкулёз (2017-2023 ж.) аурушандығы бойынша салыстырмалы талдауы.

Жоғарыда көрсетілген мысалдарға негізделе отырып, еліміздегі эпидемиялық аурулардың таралу заңдылықтарын анықтау үшін қолданыстағы математикалық модельдердің тиімділігін көрсету Қазақстан үшін жаңа көзқарас болып табылады.

Пайдаланылған дереккөздердің тізімі

1. Starshinova A, Osipov N. and others. COVID-19 and Tuberculosis: Mathematical Modeling of Infection Spread Taking into Account Reduced Screening, *Diagnostics* 2024, 14, 698.
2. Mayowa O., Olumuyiwa J., Emile F., Hasan S., Festus A. Mathematical model for control of tuberculosis epidemiology, *Journal of Applied Mathematics and Computing*, Published: 22 April 2022, Volume 69, pp 69–87, (2023).
3. Krivorotko O., Kabanikhin S., Bektemesov M., Sosnovskaya M., Neverov, A. Simulation of COVID-19 Spread Scenarios in the Republic of Kazakhstan Based on Regularization of the Agent-Based Model // *Journal of Applied and Industrial Mathematics*. – 2023. – Vol. 17. – №. 1. – pp. 94-109. <https://doi.org/10.1134/S1990478923010118>
4. Қазақстандағы коронавирус. Коронавирустық COVID-19 ақпараттық бюллетень <https://covid.observer.ru/>
5. 2024 жылғы 7 мамырдағы жағдай бойынша ДДСҰ Еуропа аймағындағы қызылша мен қызамық бойынша ай сайынғы жаңартылған деректер.

УДК 517.9

Дженалиев М.Т., Ергалиев М.Г., Иманбердиев К.Б.,
Серик А.М. (Алматы, ИМММ)

ОБ ОДНОЙ СПЕКТРАЛЬНОЙ ЗАДАЧЕ ДЛЯ ДИФФЕРЕНЦИАЛЬНОГО ОПЕРАТОРА ЧЕТВЕРТОГО ПОРЯДКА

Для численного решения граничных задач для уравнений Стокса и Навье-Стокса является важным построение системы соленоидальных функций, обладающих свойством фундаментальности. В докладе предлагается один из подходов указанного построения.

Введем основные пространства, которые нами будут использоваться. Пусть $x = (x_1, \dots, x_d) \in \Omega \subset R^d, d \geq 2$, – открытая ограниченная (односвязная) область с достаточно гладкой границей $\partial\Omega, m \geq 0$ – целое число,

$$W_2^m(\Omega) = \{v | \partial_x^{|\alpha|} v \in L^2(\Omega), |\alpha| \leq m\},$$

где

$$\partial_x^{|\alpha|} = \partial_{x_1}^{\alpha_1} \dots \partial_{x_d}^{\alpha_d}, |\alpha| = \sum_{j=1}^d \alpha_j, \partial_{x_j} = \frac{\partial}{\partial x_j},$$

$$\dot{W}_2^m(\Omega) = \left\{ v \mid v \in W_2^m(\Omega), \partial_{\vec{n}}^j v = 0, \right. \\ \left. j = 0, 1, 2, \dots, m-1, \vec{n} - \text{внешняя нормаль к } \partial\Omega \right\}.$$

Постановка спектральной задачи. Пусть $\Omega = \{x = (x_1, \dots, x_d) \mid 0 < x_k < l, k = 1, \dots, d\} \subset R^d$ – d -мерный куб с ребром длины, равной l . Рассмотрим следующую спектральную задачу для дифференциального оператора четвертого порядка.

Рассматривается спектральная задача

$$\sum_{k=1}^d \partial_{x_k}^4 u(x) = \lambda^2 (-\Delta) u(x), \quad x \in \Omega, \quad (1)$$

$$u(x) = \partial_{\vec{n}} u(x) = 0, \quad x \in \partial\Omega, \quad (2)$$

где $\vec{n}$ – внешняя нормаль к $\partial\Omega$.

Определение. Обозначим через $V_1(\Omega)$ и $V_2(\Omega)$ гильбертовы пространства с соответствующими скалярными произведениями

$$(\nabla u, \nabla v)_{L^2(\Omega)} \quad \forall u, v \in \dot{W}_2^1(\Omega), \quad (3)$$

$$((u, v)) \stackrel{\text{def}}{=} \sum_{k=1}^d (\partial_{x_k}^2 u, \partial_{x_k}^2 v)_{L^2(\Omega)} \quad \forall u, v \in \dot{W}_2^2(\Omega), \quad (4)$$

и нормами

$$\|u\|_{V_1(\Omega)} = \sqrt{\|\nabla u\|_{L^2(\Omega)}^2}, \quad \|u\|_{V_2(\Omega)} = \sqrt{\sum_{k=1}^d \|\partial_{x_k}^2 u\|_{L^2(\Omega)}^2}. \quad (5)$$

Очевидно, что нормы (5), индуцируемые соответственно скалярными произведениями (3)–(4), определяют эквивалентные нормы соответственно в пространствах $\dot{W}_2^1(\Omega)$, $\dot{W}_2^2(\Omega)$.

Предложение 1. В спектральной задаче (1)–(2) оператор четвертого порядка является эллиптическим и обладает свойствами симметричности и положительной определенности в пространстве $V_2(\Omega)$. Поэтому, собственные значения $\{\lambda_n^2, n \in N\}$ этой задачи являются действительными и расположены на положительной полуоси. Причем, наименьшее собственное значение отделено от нуля, т.е. $\lambda_1 \geq \delta > 0$.

Предложение 2. Спектральная задача (1)–(2) обладает совокупностью "обобщенных собственных функций" $\{u_n(x), n \in N\}$, принадлежащая пространству $V_2(\Omega)$, образует ортонормированный базис в пространстве $V_1(\Omega)$.

Теорема 1. Спектральная задача (1)–(2) имеет следующее решение

$$u_n(x) = X_{1n}(x_1) X_{2n}(x_2) \dots X_{dn}(x_d), \quad \lambda_n^2, \quad n \in N, \quad (6)$$

где $X_{1n}(x_1) = \Phi_n(y)|_{y=x_1}, X_{2n}(x_2) = \Phi_n(y)|_{y=x_2}, \dots, X_{dn}(x_d) = \Phi_n(y)|_{y=x_d}$;

$$(7) \quad \begin{cases} \Phi_{2n-1}(y) = \sin^2 \frac{\lambda_{2n-1} y}{2}, \lambda_{2n-1}^2 = \left(\frac{2(2n-1)\pi}{l} \right)^2, n \in N, \\ \Phi_{2n}(y) = [\lambda_{2n} l - \sin \lambda_{2n} l] \sin^2 \frac{\lambda_{2n} y}{2} - \sin^2 \frac{\lambda_{2n} l}{2} [\lambda_{2n} y - \sin \lambda_{2n} y], \\ \lambda_{2n}^2 = \left(\frac{2v_n}{l} \right)^2, n \in N, \end{cases}$$

и $\{v_n, n \in N\}$ являются положительными корнями уравнения $\operatorname{tg} v = v$, $n \in N$.

Система собственных функций $\{u_n(x) = X_{1n}(x_1)X_{2n}(x_2) \dots X_{dn}(x_d)\}_{n=1}^{\infty}$ принадлежит пространству $V_2(\Omega)$ (3), (5) и ортогональна в пространстве $V_1(\Omega)$ (4)–(5).

Расположение собственных значений на положительной полуоси (здесь принято $l = 2$):

$$0 < \lambda_1 = \pi < \lambda_2 = \frac{3\pi}{2} - \varepsilon_1 < \lambda_3 = 2\pi < \lambda_4 = \frac{5\pi}{2} - \varepsilon_2 \\ < \lambda_5 = 3\pi < \lambda_6 = \frac{7\pi}{2} - \varepsilon_3 < \lambda_7 = 4\pi < \dots$$

Далее, из теоремы 1 получаем:

Следствие 1. Собственные значения $\{\lambda_{2n}, n \in N\}$ упорядочены следующим образом

$$0 < \lambda_{2n} = \frac{2v_n}{l} < \frac{(2n+1)\pi}{2}, \quad \forall n \in N, \quad \lambda_{2n} = \frac{2v_n}{l} \rightarrow \frac{(2n+1)\pi}{2}, \quad n \rightarrow \infty,$$

где $\{v_n, n \in N\}$ являются положительными корнями уравнения $\operatorname{tg} v = v$.

Об ортонормированности системы собственных функций (6)–(7) в пространстве $V_1(\Omega)$ (3) и (5).

Следствие 2. Спектральная задача (1)–(2) имеет следующее решение

$$\bar{u}_{2n-1}(x_1, \dots, x_d) = d^{-1/2} \frac{\sqrt{2l}}{(2n-1)\pi} \left(\sqrt{\frac{8}{3l}} \right)^{d-1} \prod_{k=1}^d \sin^2 \frac{\lambda_{2n-1} x_k}{2}, n \in N, \quad (8)$$

$$\bar{u}_{2n}(x_1, \dots, x_d) = d^{-\frac{1}{2}} \sqrt{\frac{l}{2}} \frac{1}{v_n} [K_0(l, v_n)]^{-d+1}.$$

$$\cdot \prod_{k=1}^d \left[\frac{1}{v_n} \sin \frac{2v_n x_k}{l} - \frac{2}{l} x_k + 2 \sin^2 \frac{v_n x_k}{l} \right], n \in N, \quad (9)$$

где

$$\begin{cases} \bar{X}_{j,2n-1}(x_j) = \frac{\sqrt{2l}}{(2n-1)\pi} \sin^2 \frac{\lambda_{2n-1} x_j}{2}, \lambda_{2n-1}^2 = \left(\frac{2(2n-1)\pi}{l} \right)^2, n \in N, \\ \bar{X}_{j,2n}(x_j) = \sqrt{\frac{l}{2}} \cdot \frac{1}{v_n} \left[\frac{1}{v_n} \sin \frac{2v_n x_j}{l} - \frac{2}{l} x_j + 2 \sin^2 \frac{v_n x_j}{l} \right], \\ \lambda_{2n}^2 = \left(\frac{2v_n}{l} \right)^2, n \in N, \end{cases} \quad (10)$$

и $\{v_n, n \in N\}$ являются положительными корнями уравнения $\operatorname{tg} v = v$, $n \in N$.

Причем, системы собственных функций (8)–(10) составляет ортонормированный базис в пространстве $V_1(\Omega)$ (3) и (5).

Используя свойства оператора ротор (для $d \geq 2$), мы строим фундаментальную систему соленоидальных функций. Проводится необходимое обоснование. Результаты могут быть использованы для приближенного решения граничных задач для уравнений Стокса и Навье-Стокса.

Работа финансирована Комитетом науки Министерства науки и высшего образования Республики Казахстан (грант BR20281002).

УДК 004.932

Aodi Ding. (Минск, БГУ)
О.В. Недзьведь (Минск, БГУ)

ИЗВЛЕЧЕНИЕ ПЛОТНЫХ КЛЮЧЕВЫХ ТОЧЕК НИЖНИХ КОНЕЧНОСТЕЙ И СТОП ДЛЯ ПОВЫШЕНИЯ ТОЧНОСТИ ДИАГНОСТИКИ ЗАБОЛЕВАНИЙ

Аннотация. Анализ походки играет важную роль в выявлении и диагностике заболеваний. Однако традиционные методы анализа походки, основанные на небольшом количестве ключевых точек скелета, имеют ограничения в захвате тонких движений ног и стоп, что затрудняет полное отражение динамических изменений походки. Для решения этой проблемы в данной работе предлагается метод анализа походки на основе модели DensePose, который позволяет извлекать плотные ключевые точки в области ног и стоп путем получения плотных UV-координат. Сначала из видеозаписей походки извлекаются плотные ключевые точки каждого кадра, с акцентом на траектории движений ног и стоп. Затем выполняется многомерное извлечение характеристик траекторий походки, что позволяет с использованием классификационной модели диагностировать возможные заболевания. Результаты исследования показывают, что технология плотных ключевых точек не только значительно повышает уровень детализации анализа походки, но и предоставляет более точное и надежное решение для выявления заболеваний, связанных с походкой.

Ключевые слова: плотные ключевые точки, анализ походки, ноги и стопы, DensePose, диагностика заболеваний, извлечение характеристик движений

Предыстория введения. Анализ походки имеет важное исследовательское значение в медицине и реабилитации, особенно в выявлении нарушений походки при заболеваниях нервной системы, опорно-двигательного аппарата и у пожилых людей[1]. Походка рассматривается как уникальный биомаркер, движение которого может предоставить богатую информацию о состоянии здоровья. Например, аномальная походка может указывать на такие заболевания, как болезнь Паркинсона, инсульт, атрофия мозжечка и другие. Однако точное улавливание тонких изменений в походке, особенно характеристик движения ног и стоп, по-прежнему остается серьезной проблемой в области анализа походки. В данном исследовании предложен метод анализа походки на основе DensePose. На рисунке 1 представлена структура экспериментального процесса, сосредоточенного на извлечении плотных ключевых точек в области ног и стоп. Благодаря богатым характеристикам движения, предоставляемым плотными точками, мы можем более детально анализировать такие показатели, как цикл походки, длина шага, симметрия и изменения скорости, что позволяет повысить точность выявления заболеваний, связанных с походкой[3]. Данный метод помогает преодолеть ограничения традиционных подходов, предоставляя новые решения в области анализа

походки и обеспечивая технологическую поддержку клинической диагностики и реабилитации при заболеваниях нервной системы и опорно-двигательного аппарата.

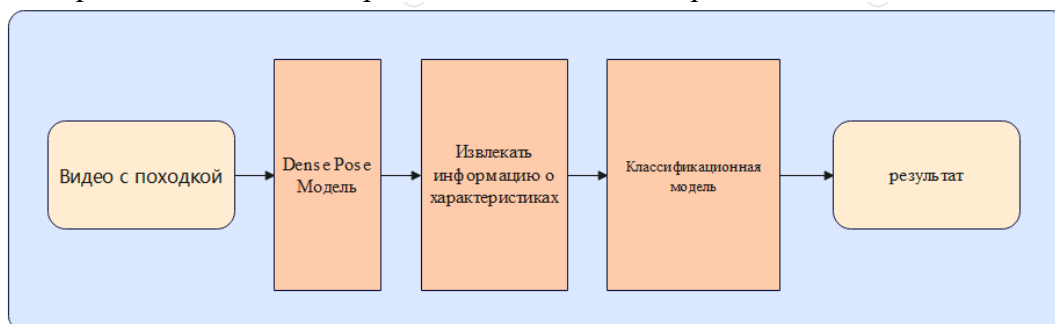


Рисунок 1. Структура сети диагностики походки

Плотные пиксели. DensePose которая сопоставляет пиксели человеческого тела на 2D изображении с поверхностью 3D модели человеческого тела. Она обеспечивает высокоточное преобразование от плоскости изображения к системе координат поверхности тела через извлечение плотных ключевых точек[2]. Для этого используется сверточная нейронная сеть (CNN), которая формирует UV-координаты для каждого пикселя изображения. UV-координаты представляют собой двумерные параметрические координаты поверхности тела. Для каждого пикселя (x, y) модель выдает распределение вероятностей его принадлежности к 24 анатомическим областям:

$$p_i = \exp(s_i) / \sum_{j=1}^{24} \exp(s_j) \quad (1)$$

Эта формула представляет собой функцию Softmax, основное назначение которой — преобразование ненормализованного вектора оценок (logits) в распределение вероятностей, что часто используется на выходном слое задач классификации. s_i — это значение оценки, указывающее вероятность того, что пиксель принадлежит области i . Функция Softmax нормализует эти оценки в вероятности[4].

Результаты эксперимента. В данном эксперименте оценивалась производительность классификатора случайного леса в задаче многоклассовой классификации, включающей четыре категории: Normal (норма), Parkinson's (болезнь Паркинсона), Cerebellar Atrophy (атрофия мозжечка) и Other Diseases (другие заболевания).

Accuracy: 94.58%				
Classification Report:				
	precision	recall	f1-score	support
Normal	0.93	0.89	0.91	47
Parkinson's	0.94	0.92	0.93	64
Cerebellar Atrophy	0.93	0.95	0.94	65
Other Diseases	0.98	1.00	0.99	64
accuracy			0.95	240
macro avg	0.94	0.94	0.94	240
weighted avg	0.95	0.95	0.95	240

Рисунок 2. Результаты классификационной модели SVM

Согласно отчету о классификации на рисунке, можно увидеть, что модель демонстрирует отличные результаты в задаче классификации, достигая точности 94,58%. Точность (Precision), полнота (Recall) и F1-мера (F1-Score) для всех категорий находятся на уровне или превышают 90%, что делает модель подходящей для применения в задачах классификации заболеваний.

Вывод. В данной работе предложен метод анализа походки на основе модели DensePose, который использует плотные UV-координаты в области ног и стоп человека. Посредством

генерации многомерных векторных признаков из координат походки человека были охвачены следующие ключевые характеристики: длина шага, ширина шага, угол касания стопы, цикл походки, время маха и время опоры. Комбинируя характеристики данных походки с классификационной моделью SVM, была достигнута общая точность классификации четырех типов походки на уровне 94,58%, что демонстрирует надежность и потенциал предложенного метода. Разработанный метод анализа походки на основе плотных ключевых точек представляет собой точное и надежное решение для диагностики заболеваний, связанных с нарушением походки, и обладает широкими перспективами применения. Этот метод может быть дополнительно адаптирован для диагностики других заболеваний, особенно в медицинских областях, требующих детального анализа характеристик движения.

Литература

1. Cao, Z., Simon, T., Wei, S. E., & Sheikh, Y. (2017). Realtime multi-person 2D pose estimation using part affinity fields. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2017, 7291-7299. DOI: [10.1109/CVPR.2017.143](https://doi.org/10.1109/CVPR.2017.143)
2. Güler, R. A., Neverova, N., & Kokkinos, I. (2018). DensePose: Dense human pose estimation in the wild. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2018, 7297-7306. DOI: [10.1109/CVPR.2018.00763](https://doi.org/10.1109/CVPR.2018.00763)
3. Wang, L., Gao, J., & Hu, H. (2020). A review of gait recognition based on deep learning. *Computer Vision and Image Understanding*, 196, 102897. DOI: [10.1016/j.cviu.2020.102897](https://doi.org/10.1016/j.cviu.2020.102897)
4. Breiman, L. (2001). Random forests. *Machine Learning*, 45(1), 5-32. DOI: [10.1023/A:1010933404324](https://doi.org/10.1023/A:1010933404324)

УДК 517.927.4

Ергалиев М.Г. (Алматы, ИМММ)
Касен М. (Алматы, ИМММ)

УСЛОВИЯ РАЗРЕШИМОСТИ КОЭФФИЦИЕНТНЫХ ОБРАТНЫХ

ЗАДАЧ ДЛЯ УРАВНЕНИЯ БЮРГЕРСА

Рассмотрим следующую нелинейно вырождающуюся область

$$\Omega = \{x, t \mid \varphi_1(t) < x < \varphi_2(t), 0 < t < T < \infty\},$$

с сечением $\Omega_t = \{\varphi_1(t) < x < \varphi_2(t)\}$ для фиксированного значения временной переменной $t \in (0, T)$, и для которой выполняется

$$\varphi_1(0) = \varphi_2(0) = 0.$$

В области Ω мы исследуем следующую обратную задачу для уравнения Бюргерса

$$\partial_t u(x, t) + u(x, t) \partial_x u(x, t) - \nu \partial_x^2 u(x, t) = \lambda(t) u(x, t) + \mu(t) f(x, t),$$

с различными комбинациями искомым неизвестных и граничных условий.

Основной целью работы является определение дополнительных условий, при которых эти обратные задачи будут однозначно разрешимы.

Работа финансирована Комитетом науки Министерства науки и высшего образования Республики Казахстан (грант BR20281002).

Список использованных источников

1. Jenaliyev M.T, Kabanikhin S.I., Kassen M., Yergaliyev M.G. On the solvability of an inverse problem for the Burgers equation with an integral overdetermination condition in a nonlinearly degenerating domain // Journal of Inverse and Ill-posed Problems, 33: 1 (2025), 93-106.
2. Jenaliyev M., Romankyzy A., Yergaliyev M., Zholdasbek A. On an inverse problem with an integral overdetermination condition for the Burgers equation // Journal of Mathematics, Mechanics and Computer Science, 117: 1 (2023), 24-41.
3. Jenaliyev M.T., Yergaliyev M.G. On initial-boundary value problem for the Burgers equation in nonlinearly degenerating domain // Applicable Analysis, 103: 11 (2024), 2003-2

УДК 004.855

Жәнібек М.А., Мухаметжанова Б.О. (Қарағанды, Ә. Сағынов атындағы ҚарТУ)

Жаңалықтарды талдаудағы кері есептер: манипуляция мен дезинформацияны анықтау

Қазіргі цифрлық дәуір ақпараттың тез таралуына байланысты оның шынайылығын қамтамасыз ету айтарлықтай қиындықтар туғызуда. Жалған жаңалықтар феномені жаһандық проблемаға айналып, қоғамдық пікірге, саяси үдерістерге және экономикалық нарықтарға әсер етуде. Мақалада жасанды интеллект және машиналық оқыту технологияларын қолдану арқылы жаңалықтардағы манипуляциялар мен дезинформацияны анықтау әдістері қарастырылады. Ерекше назар жаңалықтарды талдаудағы кері есептерге және мәтіндерді шынайылық деңгейі бойынша автоматты түрде жіктей алатын алгоритмдерді практикалық іске асыруға аударылады.

Мақала мақсаты – машиналық оқыту технологияларын қолдана отырып, жаңалықтар контентін автоматты түрде талдау әдістерін зерттеу және енгізу.

Мақаланың негізгі міндеттері:

Жалған жаңалықтарды анықтау мен ақпаратты манипуляциялау әдістеріне қазіргі заманғы тәсілдерді қарастыру.

Мәтіндерді өңдеу процесін және оларды векторизация мен машиналық оқыту алгоритмдері арқылы талдауды сипаттау.

Зерттеу барысында орыс тілді мәтіндердегі жалған жаңалықтарды автоматтандырылған әдіспен анықтау тұжырымдамасы әзірленді, оның дәлдігі 70%-дан жоғары болды. Машиналық оқыту әдістерін қолдану үлкен деректер жиынтығын талдауға және жалған ақпараттың сипаттамалық белгілерін анықтауға мүмкіндік берді. Ұсынылған тәсілдің негізінде мәтінді өңдеу, оларды векторлау және классификациялау моделін оқыту жатыр.

Модельді оқыту келесі схема бойынша жүзеге асырылады:

Деректерді дайындау. Бастапқы мәтін көпдеңгейлі өңдеуден өтеді: қажетсіз таңбалардан тазарту, барлық әріптерді кіші регистрге келтіру, стоп-сөздерді алып тастау, лемматизация және мәтінді сандық форматқа түрлендіру [1].

Мағыналық сипаттамаларды шығару үшін TF-IDF әдісі қолданылады, ол өңделген мәтінді векторлық көрініске аударады (мысал 1.1)[2].

Мысал 1.1

```
vectorizer = CountVectorizer(max_features=1500, min_df=5, max_df=0.7)
```

```
X = vectorizer.fit_transform(data["clean_headline"]).toarray()
```

```
y = data["label"].values
```

Деректерді бөлу.

Дайындалған деректер модельдің жұмысын әділ бағалау үшін оқыту және тест жинақтарына бөлінеді.

Модельді оқыту.

Классификация үшін бірнеше алгоритмдер сыналды, соның ішінде логистикалық регрессия, Random Forest және шешімдер ағашы [3].

Эксперимент нәтижесінде логистикалық регрессия ең жоғары дәлдік көрсеткішін – 79.38% көрсетті (мысал 1.2, кесте 1.1).

Мысал 3.4

Логистикалық регрессия

```
from sklearn.linear_model import LogisticRegression
```

```
from sklearn.metrics import accuracy_score
```

```
model_lr = LogisticRegression()
```

```
model_lr.fit(X_train, y_train)
```

```
y_pred_lr = model_lr.predict(X_test)
```

```
print("Accuracy:", accuracy_score(y_test, y_pred_lr))
```

Random Forest

```
from sklearn.ensemble import RandomForestClassifier
```

```
model_rf = RandomForestClassifier(n_estimators=100)
```

```
model_rf.fit(X_train, y_train)
```

```
y_pred_rf = model_rf.predict(X_test)
```

```
print("Accuracy:", accuracy_score(y_test, y_pred_rf))
```

Шешімдер ағашы

```
from sklearn.tree import DecisionTreeClassifier
```

```
model_dt = DecisionTreeClassifier()
```

```
model_dt.fit(X_train, y_train)
```

```
y_pred_dt = model_dt.predict(X_test)
```

```
print("Accuracy:", accuracy_score(y_test, y_pred_dt))
```

Кесте 1.1 – Модельдердің дәлдігі

Модель	Дәлдік
Логистикалық регрессия	79.38%
Random Forest	78.93%
Шешімдер ағашы	71.75%

Дезинформацияны анықтау бірнеше көрсеткіштерге негізделеді: ақпарат көзіне деген сенімділік, URL мекенжайының түпнұсқалығы, лексикалық сапасы, грамматикалық қателердің болуы және мәтіннің логикалық үйлесімділігі. Статистикалық талдау арқылы жалған немесе шынайы жаңалықтарды автоматты түрде жіктеуге мүмкіндік беретін негізгі сипаттамалық сөздер анықталды.

Зерттеу барысында машиналық оқытуды қолдану жалған ақпаратты анықтауда тиімді құрал екенін көрсетті. Әзірленген әдіс жоғары дәлдікті көрсетіп, оны жаңалықтар порталдарына енгізу мүмкіндігін дәлелдеді. Дегенмен, дезинформация мәселесі әлі де өзекті болып қала бермек, сондықтан болашақ зерттеулер табиғи тілді өңдеу алгоритмдерін жетілдіруге және ақпаратты манипуляциялаудың жаңа түрлерін ескеруге бағытталуы керек.

Қазіргі заманғы жасанды интеллект технологиялары, веб-деректер аналитикасы және халықаралық тәжірибе мұндай құралдарды біріктіру жалған жаңалықтарға қарсы күрестің тиімді жүйесін қалыптастырудың негізі бола алатынын көрсетеді. Мемлекеттік құрылымдардың, ғылыми қауымдастықтың және технологиялық компаниялардың ынтымақтастығы ақпараттық қауіпсіздік деңгейін едәуір арттырып, пайдаланушыларды жалған ақпараттың ықпалынан қорғауға көмектесе алады.

Қолданылған әдебиеттер тізімі

1. Кристиани, Р., Шалльк, К. Введение в машинное обучение с Python / Р. Кристиани, К. Шалльк. – М.: Питер, 2020. – 416 с.
2. Russell, S., Norvig, P. Artificial Intelligence: A Modern Approach / S. Russell, P. Norvig. – Pearson, 2020. – 1152 p.
3. Rashkin, H., Choi, E., Jang, J. Y., Volkova, S., & Choi, Y. (2017). Truth of varying shades: Analyzing language in fake news and political fact-checking. *Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing (EMNLP)*.

УДК 519.62/.64

Касенов С.Е. (Алматы, КазНУ им. Аль-Фараби)
Темирбеков М.Н. (Алматы, АЛТ Университет имени М.Тынышпаева)
Кабулова А.А. (Усть-Каменогорск, ВКТУ им.Д.Серикбаева)

АЛГОРИТМ РЕШЕНИЕ ОБРАТНОЙ ЗАДАЧИ ДЛЯ УРАВНЕНИЯ ДИФФУЗИИ

Уравнение диффузии является одним из основных уравнений математической физики, описывающих процессы распространения веществ, энергии или импульса в средах, находящихся в движении. Важно отметить, что такие процессы могут включать как явление диффузии, так и явление конвекции (перенос вещества с помощью движения среды).

Для решения уравнений диффузии, особенно в случае сложных геометрий и условий, необходимо использовать численные методы, так как аналитические решения могут быть недоступны. Важным аспектом является решение как прямых, так и обратных задач для этого уравнения в двумерной области.

Постановка задачи уравнения диффузии

Перемещение загрязняющих веществ в атмосфере осуществляется воздушными потоками с учетом их локальных колебаний. Средний поток веществ, переносимых воздушными массами, как правило, включает адвективные и конвективные составляющие. В процессе движения примесей

основная усредненная динамика дополняется диффузией, вызванной случайными колебаниями частиц.

Постановка задачи для уравнения переноса загрязняющих веществ в области:

$$\Omega = \{(x, y, t): 0 \leq x \leq 1, \quad 0 \leq y \leq 1, \quad 0 \leq t \leq T\}$$

$$\frac{\partial \varphi_q}{\partial t} + u \frac{\partial \varphi_q}{\partial x} + v \frac{\partial \varphi_q}{\partial y} = \Delta \varphi_q + \alpha_q \varphi_q + \beta_q + f_q(x, y) \quad (1)$$

$$\varphi_q(x, y, 0) = \varphi_0(x, y), \quad (2)$$

$$\varphi_q(0, y, t) = 0, \quad \varphi_q(1, y, t) = 0 \quad (3)$$

$$\varphi_q(x, 0, t) = 0, \quad \varphi_q(x, 1, t) = 0 \quad (4)$$

Здесь $f_q(x, y) = \sum_{j=1}^m Q_j \delta(\vec{r} - \vec{r}_j)$ представляет собой радиус-вектор расположения источников загрязнения, мощность источников загрязнения, число источников.

где u, v – коэффициенты скорости воздушного потока,

q – концентрация вредного вещества в смеси,

β_q – коэффициент скорости образования вещества,

α_q – коэффициент уменьшения скорости,

$\varphi_q(x, y, t)$ – интенсивность аэрозольной субстанции, переносимой воздушным потоком в атмосфере.

Обратная задача

Дополнительной информацией для решения этой задачи являются данные о значениях загрязняющих веществ в автоматических станциях мониторинга (АСМ), которые имеют следующий формат:

$$g = \sum_{i=1}^n p_i \delta(\vec{l} - \vec{l}_i)$$

где $\vec{l}_i$ – это координаты расположения АСМ. Суть обратной задачи заключается в определении уровней мощности источников, заданных следующим образом:

$$\sum_{j=1}^m Q_j \delta(\vec{r} - \vec{r}_j).$$

Для численного решения этой обратной задачи мы формируем целевой функционал Лагранжа.

$$\begin{aligned} L(Q) = & \int_0^T dt \int_0^1 \int_0^1 \left[\frac{\partial \varphi_q}{\partial t} + u \frac{\partial \varphi_q}{\partial x} + v \frac{\partial \varphi_q}{\partial y} - \Delta \varphi_q - \alpha_q \varphi_q - \beta_q - f_q \right] \varphi^* dx dy + \\ & + \sum_{i=1}^n \alpha_i \int_0^T dt \int_0^1 \int_0^1 (p_i - \varphi_q)^2 \delta(\vec{l} - \vec{l}_i) dx dy \end{aligned} \quad (5)$$

Для минимизации целевой функции (5) мы анализируем первое приращение функционала. Это достигается путем рассмотрения задачи с небольшим возмущением относительно уравнений (1) – (4).

Получаем постановку сопряженной задачи:

$$\frac{\partial \varphi^*}{\partial t} + u \frac{\partial \varphi^*}{\partial x} + v \frac{\partial \varphi^*}{\partial y} = -\Delta \varphi^* - \alpha_q \varphi^* - \beta_q + 2 \sum_{i=1}^n \alpha_i (p_i - \varphi_q) \delta(\vec{l} - \vec{l}_i) \quad (6)$$

$$\varphi^*(x, y, T) = 0 \quad (7)$$

$$\varphi^*(0, y, t) = 0, \quad \varphi^*(1, y, t) = 0 \quad (8)$$

$$\varphi^*(x, 0, t) = 0, \quad \varphi^*(x, 1, t) = 0 \quad (9)$$

Тогда по определению главная часть приращения функционала есть градиент, т. е.

$$\begin{aligned} \delta L = \langle \delta Q, L' Q \rangle &= - \int_0^T dt \int_0^1 \int_0^1 \delta f_q \varphi^* dx dy = \\ &- \int_0^T dt \int_0^1 \int_0^1 \sum_{i=1}^m \delta Q_j \delta(\vec{l} - \vec{l}_i) \varphi^* dx dy \end{aligned}$$

Отсюда

$$L' Q = - \sum_{j=1}^m \delta(\vec{r} - \vec{r}_j) \varphi^*$$

Используя градиентного метода следующее приближение имеет вид:

$$f_q^{n+1} = f_q^n - \alpha \cdot L' Q_n$$

Данное исследование финансировалось Комитетом науки Министерства науки и высшего образования Республики Казахстан (грант № AP25796443 «Идентификация маркерных загрязнителей атмосферного воздуха от предприятий и транспорта методами машинного обучения и их воздействие на респираторные заболевания населения»)

Список использованных источников

- 1) Марчук, Г. И. Математическое моделирование в проблемах окружающей среды. М.: Наука, 1982.-320с.
- 2) Kasenov S., Nurseitova A., Nurseitov D. A conditional stability estimate of continuation problem for the Helmholtz equation. *AIP Conference Proceedings*. AIP Publishing **2016** 1759.1. <https://doi.org/10.1063/1.4959733>

- 3) Askerbekova, J., Kasenov, S., Temirbekov, A., and Tleulesova, A. Numerical solution of the continuation problem for the one-dimensional acoustics equation //AIP Conference Proceedings. – AIP Publishing, 2023. – Т. 2879. – №. 1. <https://doi.org/10.1063/5.0175240>

УДК 519.62/.64

.Касенов С.Е (Алматы, КазНУ им. Аль-Фараби)
Тлеулесова А.М. (Алматы, КазНУ им. Аль-Фараби)
Сарсенбаева А.Е. (Шымкент, ЮКГУ им. М.О. Ауэзова)

ЧИСЛЕННОЕ РЕШЕНИЕ ЗАДАЧИ ПРОДОЛЖЕНИЯ ДЛЯ УРАВНЕНИЯ ГЕЛЬМГОЛЬЦА

Задача продолжения Гельмгольца представляет собой важную задачу математической физики, которая имеет глубокие корни в области акустики и распространения звука. Данная задача является одним из фундаментальных уравнений в акустике и имеет широкое применение в различных областях физики, инженерии и приложенных наук. Ее решение позволяет лучше понять и моделировать процессы распространения звука, что является важным элементом в различных прикладных областях, начиная от инженерии и заканчивая медициной и геофизикой.

Известно, что задача Коши для уравнения Гельмгольца крайне некорректна в том смысле, что небольшое изменение данных Коши может привести к резкому изменению решения [1]. Следовательно, решить эту задачу классическими численными методами невозможно и требуются специальные приемы, например метод регуляризации.

Постановка задачи продолжения.

Исходная задача продолжения для уравнения Гельмгольца в области $\Omega=(0,1) \times (0,1)$ имеет следующий вид:

$$u_{xx} + u_{yy} + k^2 u = 0, \quad x, y \in \Omega, \quad (1)$$

$$u(x, 0) = 0, \quad y \in [0, 1], \quad (2)$$

$$u(0, y) = f(y), \quad y \in [0, 1], \quad (3)$$

$$u(x, 0) = u(x, 1) = 0, \quad x \in [0, 1]. \quad (4)$$

где k - заданная константа. В задаче продолжении требуется найти функцию $u(x, y)$ в области Ω по данным $f(y)$.

Прямая и обратная задача

Некорректность задачи продолжения создает значительные трудности при попытке найти ее численное решение. Одним из эффективных подходов к решению этой проблемы является сведение задачи продолжения на граничную обратную задачу. Это позволяет использовать развитые методы решения обратных задач для нахождения решения исходной задачи. Рассмотрим формулировку прямой и обратной задачи.

$$u_{xx} + u_{yy} + k^2 u = 0, \quad x, y \in \Omega, \quad (6)$$

$$u_{x0}, y = 0, \quad y \in 0, 1, \quad (7)$$

$$u_1, y = qy, \quad y \in 0, 1, \quad (8)$$

$$u_{x0} = u_{x1} = 0, \quad x \in 0, 1. \quad (9)$$

В прямой задаче требуется найти $u(x, y)$ по заданным функциям $q(y)$. В обратной задаче необходимо найти $q(y) = u_1, y$ с учетом дополнительной информации

$$u_0, y = f(y), \quad y \in 0, 1. \quad (10)$$

Определение: Функцию $u(x, y) \in L_2$ будем считать обобщенным (или слабым) решением прямой задачи (6) - (8), если для любых $\omega \in H_2$, таких, что

$$x_0, y = 0, \quad y \in 0, 1, \quad (11)$$

$$1, y = 0, \quad y \in 0, 1, \quad (12)$$

$$x_0 = \omega x_1 = 0, \quad x \in 0, 1. \quad (13)$$

Выполняется равенство

$$u(x_{xx} + u_{yy} + k^2 \omega) dx dy - 0_1 q u_{x1}, y dy = 0. \quad (14)$$

Функцию $\omega \in H_2$, удовлетворяющая условиям (6)-(8) будет называться тест-функцией.

Прямая задача для уравнения Гельмгольца включает нахождение решения при заданных граничных условиях. Корректность этой задачи критически важна для многих приложений в науке и технике. Далее будет рассмотрена корректность обобщенного решения прямой задачи для уравнения Гельмгольца.

Теорема. Если $q \in L_{2,1}$ и $-2 < k < 2$, то обобщенное решение $u \in L_2$ задачи (6) – (8) существует, единственное и верно оценке

$$\|u\|_{L_2(\Omega)} \leq \|q\|_{L_{2,1}}^{2-k/2}. \quad (15)$$

Формулировка и решение задачи оптимизации.

Далее изучается формулировка граничной обратной задачи в операторной форме, а также представление оптимизационной задачи, решаемой с использованием градиентного метода.

Оператор A определяется следующим виде:

$$A: u_1, y = q(y) \mapsto u(0, y) = f(y)$$

где $u(x, y)$ решение прямой задачи (6)-(9) записывается в операторной форме

$$Aq=f \tag{16}$$

Операторное уравнение (24) преобразуется в задачу оптимизации, и мы минимизируем функционал

$$Jq_n=\|Aq_n-f\|^2=0, y;q_n-f(y)^2 dy \tag{17}$$

градиентном методом Ландвебера

$$q_{n+1}=q_n-\alpha J'q_n \tag{18}$$

где α - параметр спуска.

Одним из эффективных подходов к решению задач продолжения является использование методов оптимизации, среди которых ускоренный метод Нестерова занимает особое место благодаря своей высокой скорости сходимости. Метод Нестерова относится к семейству градиентных методов, но обладает существенно улучшенной скоростью сходимости по сравнению с классическими градиентными методами. Основная идея метода заключается в использовании как текущего, так и предыдущего градиентного направления для корректировки следующего шага.

Схема ускорения Нестерова представляет особый интерес, поскольку она не только чрезвычайно проста в реализации, но и сам Нестеров также смог доказать, что она генерирует последовательность итераций q_k , для которой выполняется [2]

$$\|Jq_k - Jq_T\| = O(k^{-2})$$

Ускоренный метод Нестерова представляет собой мощный инструмент для решения граничных обратных задач.

Список использованных источников

1. Kasenov, S. E., Tleulesova, A. M., Sarsenbayeva, A. E., and Temirbekov, A. N. Numerical Solution of the Cauchy Problem for the Helmholtz Equation Using Nesterov's Accelerated Method //Mathematics (2227-7390). – 2024. – T. 12. – №. 17. <https://doi.org/10.3390/math12172618>
2. Kasenov S., Nurseitova A., Nurseitov D. A conditional stability estimate of continuation problem for the Helmholtz equation. AIP Conference Proceedings. AIP Publishing **2016** 1759.1. <https://doi.org/10.1063/1.4959733>
3. Askerbekova, J., Kasenov, S., Temirbekov, A., and Tleulesova, A. Numerical solution of the continuation problem for the one-dimensional acoustics equation //AIP Conference Proceedings. – AIP Publishing, 2023. – T. 2879. – №. 1. <https://doi.org/10.1063/5.0175240>

УДК 519.62/.64

Касенов С.Е. (Алматы, КазНУ им. Аль-Фараби)
 Тлеулесова А.М. (Алматы, КазНУ им. Аль-Фараби)
 Асанова Р.А. (Шымкент, ЮКГУ им. М.О. Ауэзова)

ЧИСЛЕННОЕ РЕШЕНИЕ ОБРАТНОЙ ЗАДАЧИ ДЛЯ ВОЛНОВОГО УРАВНЕНИЯ

Введение

Волновое уравнение играет ключевую роль в моделировании различных физических процессов, от колебаний в механических системах до распространения электромагнитных волн.

Однако решение волнового уравнения часто сопровождается вызовами, особенно когда речь идет об обратных и некорректных задачах. Восстановление начального условия важен в различных приложениях, таких как медицинская визуализация, геофизическое зондирование и акустическая диагностика.

В прямой задаче в области $\Omega = (0, \pi) \times (0, \pi) \times (0, T)$, требуется определить $u(x, y, t)$ по заданным $q(x, y)$ из соотношений:

$$\begin{cases} u_{tt} = u_{xx} + u_{yy}, & x, y \in (0, \pi), t \in (0, T) \end{cases} \quad (1)$$

$$\begin{cases} u(x, y, 0) = q(x, y), \quad u_t(x, y, 0) = 0, \end{cases} \quad (2)$$

$$\begin{cases} u_x(0, y, t) = u_x(\pi, y, t) = 0, \end{cases} \quad (3)$$

$$\begin{cases} u_y(x, 0, t) = u_y(x, \pi, t) = 0. \end{cases} \quad (4)$$

Обратная задача заключается в определении функции $q(x, y)$, из соотношений (1)–(4), по дополнительной информации о решении прямой задачи

$$u(0, y, t) = f(y, t).$$

Обратные задачи волнового уравнения часто некорректны: малые ошибки в данных могут привести к большим ошибкам в решении. Это требует применения специальных численных методов для стабилизации решения. Некорректность задачи возникает из-за недостатка информации и высокой чувствительности к малым возмущениям.

Формулировка и решение задачи оптимизации.

Далее изучается формулировка обратной задачи в операторной форме, а также представление оптимизационной задачи, решаемой с использованием градиентного метода.

Оператор A определяется следующим виде:

$$A: u(x, y, 0) = q(x, y) \mapsto u(0, y, t) = f(y, t)$$

где $u(x, y, t)$ решение прямой задачи (1)–(4) записывается в операторной форме

$$Aq = f \quad (5)$$

Операторное уравнение (11) преобразуется в задачу оптимизации, и мы минимизируем функционал

$$J(q_n) = \|Aq_n - f\|^2 = \int_0^T \int_0^\pi (u(0, y, t; q_n) - f(y, t))^2 dy dt \quad (6)$$

градиентном методом

$$q_{n+1} = q_n - \alpha J' q_n \quad (7)$$

где α – параметр спуска.

Для решения обратных задач восстановления начального условия разработаны различные методы. Рассмотрим наиболее распространенные из них.

Метод конечных разностей. Метод конечных разностей используется для дискретизации волнового уравнения. Сетка по пространству и времени позволяет аппроксимировать производные, превращая задачу в систему линейных уравнений, которую можно решить численно.

Метод градиентного спуска минимизирует целевой функционал путем итеративного обновления начального условия:

$$q_{k+1} = q_k - \tau_k \nabla J(q_k),$$

где τ_k – шаг итерации, а $\nabla J(q_k)$ — градиент целевого функционала.

Метод градиентного спуска — один из ключевых инструментов в области оптимизации, играющий важную роль в решении задач минимизации. Он широко применяется в различных областях, таких как машинное обучение, обработка сигналов и численный анализ. Основная идея метода заключается в использовании информации о градиенте функции для нахождения направления наискорейшего убывания, что позволяет эффективно искать минимумы целевых функций.

Одной из важных задач при применении метода градиентного спуска является выбор подходящего шага итерации τ_k . Если шаг слишком большой, метод может не сойтись, так как обновления будут перескакивать через минимум. Если шаг слишком маленький, сходимость будет очень медленной, что потребует большого числа итераций. Для адаптивного выбора шага итерации часто используются различные методы поиска и стратегии уменьшения шага.

Одним из эффективных подходов к решению обратных задач для волнового уравнения является применение методов оптимизации, среди которых особое место занимает ускоренный метод Нестерова благодаря его высокой скорости сходимости. Этот метод относится к классу градиентных методов, однако существенно превосходит классические градиентные алгоритмы по скорости сходимости, что делает его особенно эффективным при решении задач высокой размерности.

Благодарность

Данное исследование финансировалось Комитетом науки Министерства науки и высшего образования Республики Казахстан (грант № AP19579325 «Разработка и исследование современных численных методов решения обратных и некорректных задач для уравнения акустики»)

Список использованных источников

- 4) Kasenov, S. E., Tleulesova, A. M., Sarsenbayeva, A. E., and Temirbekov, A. N. Numerical Solution of the Cauchy Problem for the Helmholtz Equation Using Nesterov's Accelerated Method //Mathematics (2227-7390). – 2024. – Т. 12. – №. 17. <https://doi.org/10.3390/math12172618>
- 5) Kasenov S., Nurseitova A., Nurseitov D. A conditional stability estimate of continuation problem for the Helmholtz equation. *AIP Conference Proceedings*. AIP Publishing **2016** 1759.1. <https://doi.org/10.1063/1.4959733>
- 6) Askerbekova, J., Kasenov, S., Temirbekov, A., and Tleulesova, A. Numerical solution of the continuation problem for the one-dimensional acoustics equation //AIP Conference Proceedings. – AIP Publishing, 2023. – Т. 2879. – №. 1. <https://doi.org/10.1063/5.0175240>

УДК 004.421

Касылкасова К.Н.
(Астана, ЕНУ им.Л.Н.Гумилева)

МЕДИЦИНСКОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ SMARTMED

Быстрое развитие информационных технологий и возможности взаимодействия с медицинскими учреждениями через мобильные приложения. Сегодня все больше людей предпочитают использовать мобильные устройства для получения медицинских консультаций и

услуг. Мобильные приложения для медицинских консультаций позволяют пациентам получать медицинскую помощь из любого места и в любое время, что делает их более удобным и быстрым способом получения рекомендаций и общения с врачами. Все это делает разработку мобильного приложения для чат медицинских консультаций актуальной и важной.

C# - это объектно-ориентированный язык программирования, разработанный компанией Microsoft. Он является одним из основных языков для создания приложений для платформы .NET Framework и используется для создания различных типов приложений, таких как десктопные приложения, веб-приложения, игры и мобильные приложения.

Одной из главных особенностей C# является сильная типизация, которая позволяет определить тип данных переменной во время компиляции. Это помогает снизить вероятность возникновения ошибок во время выполнения программы. Кроме того, C# обладает многопоточностью, что позволяет создавать приложения, которые выполняют несколько задач одновременно, повышая производительность программы.

В C# также присутствует автоматическое управление памятью, которое помогает избежать проблем с утечкой памяти. Сборщик мусора в C# автоматически удаляет неиспользуемые объекты и освобождает память, что позволяет сосредоточиться на разработке приложения, а не на управлении памятью.

Xamarin - это платформа для разработки кроссплатформенных мобильных приложений с использованием языка программирования C#. Xamarin позволяет создавать приложения для iOS, Android и Windows с использованием единой кодовой базы. Это означает, что разработчики могут создавать мобильные приложения для разных платформ, используя один и тот же язык программирования и кодовую базу.

Одной из главных особенностей Xamarin является то, что она использует нативные компоненты для каждой платформы, что позволяет создавать приложения с высокой производительностью и качеством пользовательского интерфейса. Это также позволяет использовать все возможности платформы, включая устройства ввода, камеры, датчики и т. д. Фрагмент кода меню мобильного приложения, где представлена реализация шаблона главного меню показана на рисунке 1.

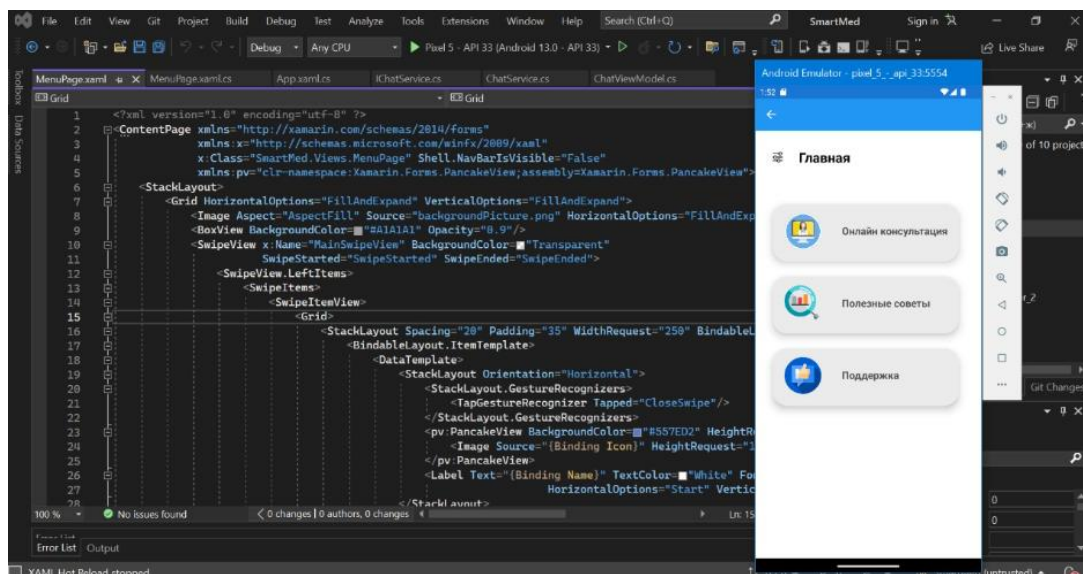


Рисунок 1. Реализация меню главного экрана

Кроме того, Xamarin интегрируется с платформой .NET, что облегчает разработку мобильных

приложений для разных платформ. Xamarin позволяет использовать множество инструментов и библиотек .NET, таких как LINQ, Entity Framework и т.д. Это обеспечивает высокую гибкость и расширяемость при разработке мобильных приложений на Xamarin.

Entity Framework представляет прекрасное ORM-решение, которое позволяет автоматически связать обычные классы языка C# с таблицами в базе данных. Entity Framework Core нацелен в первую очередь на работу с СУБД MS SQL Server, однако поддерживает также и ряд других СУБД. В данном случае мы будем работать с базами данных в MS SQL Server.

Также стоит отметить, что здесь мы будем использовать Entity Framework Core - кроссплатформенное решение на базе .NET Core, которое отличается от предыдущих версий, например, от Entity Framework 6. Более подробно с работой с Entity Framework Core можно ознакомиться в соответствующем руководстве.

Для работы с Entity Framework вначале создадим новый проект ASP.NET Core по шаблону ASP.NET Core Web App (Model-View-Controller). Пусть он будет называться EFDataApp.

Для взаимодействия с MS SQL Server через Entity Framework необходим пакет Microsoft.EntityFrameworkCore.SqlServer. По умолчанию он отсутствует в проекте, поэтому его надо добавить, например, через пакетный менеджер Nuget.

Таким образом, разработаны основные модули проекта «SmartMed». Для мобильного приложения созданы модули:

- регистрации и авторизации;
- записи к специалисту;
- онлайн чата со специалистом;
- онлайн чата с чат-ботом;
- оценки специалиста;
- поддержки.

Для веб-приложения были созданы следующие модули:

- авторизации;
- чат-консультации с пациентом;
- записи заметок.

Согласно требованиям, разработанное мобильное приложение для пациента содержит в себе следующие функции:

- запись к выбранному специалисту на консультацию;
- возможность оставить оценку специалисту;
- возможность просмотра данных о специалисте: образование, стаж работы;
- возможность проведения консультации между пациентом и специалистом посредством письменного чата;
- возможность просмотра своих записей, заметок специалистов на основе консультации, личных данных;
- реализация обратной связи.

Веб-приложение врача содержит следующие функции:

- проведение чат-консультации пациентам;
- запись заметок к каждой пройденной консультации;
- просмотр расписания консультации.

В стартовом меню пациент может произвести запись на консультацию к специалисту. После записи на консультацию в назначенное время открывается возможность присоединиться к чат-консультации со специалистом. После прохождения консультации со специалистом есть возможность поставить оценку специалисту. Также с главной страницы без осуществления записи пользователь может пройти консультацию с чат-ботом.

В веб-приложении специалист имеется возможность просмотра назначенных записей

пациентов, оказания чат-консультации с пациентом в назначенной время, а также записи заметок в медкарту пациента по итогу чат-консультации.

Список использованных источников

1. Троелсен Э., Джепикс Ф. **С# 9.0 и .NET 5.0. Обширное руководство.** – М.: Вильямс, 2021. – 1056 с.
2. Албахари Дж., Албахари Б. **С# 10.0. Карманный справочник.** – М.: Диалектика, 2022. – 450 с.
3. Шилдт Г. **Полный справочник по С#.** – М.: Вильямс, 2020. – 960 с.
4. Скотт А. **Программирование на С# для начинающих.** – СПб.: Питер, 2021. – 336 с.
5. Richter J. **CLR via C#.** – Redmond: Microsoft Press, 2019. – 896 p.

УДК 517.9

Космакова М.Т. (Қарағанды, Е.А.Бөкетов
атындағы ҚарУ)
Ахманова Д.М., (Қарағанды, Е.А.Бөкетов
атындағы ҚарУ)
Ижанова К.А. (Қарағанды, Е.А.Бөкетов
атындағы ҚарУ)

ЖҮКТЕЛГЕН ШЕТТІК ЕСЕП ТУРАЛЫ

Цилиндрлік емес G аймағында бөлшек дәрежелі туындымен жүктелген жылуөткізгіштік теңдеуі үшін кеңістіктік айнмалысы бойынша екі өлшемді шекаралық есеп қарастырылды [1-2]:

$$u_t = a^2 \Delta u + \lambda D_{0t}^{\beta} u(x, y; t) + f(x, y; t)$$

мұндағы $G = \{(x, y; t) | \sqrt{x^2 + y^2} \leq t; t > 0\}$,

Есептің шешімі келесі шартпен шектеледі

$$\lim_{\sqrt{x^2+y^2} \rightarrow +\infty} u(x, y; t) = 0$$

және конустың бүйір бетіндегі келесі шарт ескерілді

$$u(x, y; t)|_{\sqrt{x^2+y^2}=t} = g(t),$$

мұндағы λ -комплекс параметр, $D_{0t}^{\beta} u(x, y; t)$ - β ретті Риман-Лиувилль туындысы $0 < \beta < 1$.

Анықтама. Бөлшек ретті Риман-Лиувилль туындысы келесі формуламен анықталады

$$D_{0t}^{\beta} u(x, y; t) = \frac{1}{\Gamma(1-\beta)} \frac{d}{dt} \int_0^t \frac{u(x, y; \tau)}{t-\tau} d\tau$$

Теорема. Шарттарды қанағаттандыратын берілген шеттік есептің шешімі келесі түрде ұсынылады:

$$w(r, t) = g(0) + \lambda g(0) t^{1-\beta} \varepsilon_{1-\beta, 2-\beta}(\lambda t^{1-\beta}) + \lambda \int_0^t f_1(\tau) d\tau + \\ + \lambda^2 \int_0^t (t-\tau)^{1-\beta} \varepsilon_{1-\beta, 2-\beta}(\lambda(t-\tau)^{1-\beta}) f_1(\tau) d\tau + f(r, t)$$

Қолданылған дереккөздер тізімі:

- [1] Полянин А.Д. *Линейные уравнения математической физик. Справочник*, Физмат лит, Москва (2001).
[2] Прудников А.П., Брычков Ю.А., Маричев О.И. *Специальные функции*, Физмат лит, Москва (2003).

УДК 519.63

Кузнецов К.С. (Владивосток, ДВФУ, ИПМ ДВО РАН)

ЧИСЛЕННОЕ РЕШЕНИЕ ОБРАТНОЙ РЕТРОСПЕКТИВНОЙ ЗАДАЧИ КОНДУКТИВНОГО ТЕПЛООБМЕНА МЕТОДОМ PINN

Кондуктивный теплообмен возможен в твердых, жидких и газообразных средах. В силу этого данный тип теплообмена очень часто встречается в различных производственных процессах, будь то производство стекла, распространение тепла в камерах сгорания. В связи с этим возникают обратные задачи, позволяющие при помощи математического моделирования решать конкретные задачи на производстве. Одним из видов обратных задач является ретроспективная задача – то есть задача о восстановлении начального состояния среды по наблюдениям в конечный момент времени.

Рассматривается эволюционное нелинейное уравнение кондуктивного теплообмена в одномерной области [1]:

$$\partial u / \partial t - \partial (\lambda u) / \partial x = 0,$$

$$x \in [0, l], \quad t \in [0, T],$$

где $u = u(x, t)$ – температура среды, $\lambda = \lambda(u)$ – коэффициент теплопроводности, зависящий от температуры, l – характерный размер области, T – общее время процесса.

Уравнению (1) соответствуют следующие начальные и граничные условия:

$$u(0, t) = u_1(t), \quad u(l, t) = u_2(t), \quad u(x_i, T) = u_i(T), \quad i = 1..N, \quad N \geq 2$$

где u_1, u_2 – заданные функции, $u_i(T)$ – наблюдения в точках x_i в конечный момент времени. Таким образом, начальное приближение $u(0) = u(x, 0)$ является неизвестным и его требуется найти, используя в качестве априорной информации финальные наблюдения.

Для численного решения используется метод PINN [2], заключающийся в аппроксимации неизвестных путем обучения нейронной сети на минимизацию квадратичного функционала, вид которого зависит от решаемой задачи. Решение, полученное методом PINN, сравнивается с решением, полученным авторами работы [1] при использовании другого численного метода.

Список литературы

1. Kolesnik S.A., Stifeev E.M. Numerical Simulation of Inverse Retrospective Problems for a Nonlinear Heat Equation. *Math Models Comput Simul* 15, 1123–1131 (2023).
2. . Raissi M., Perdikaris P., Karniadakis G.E. Physics-informed neural networks: A deep learning framework for solving forward and inverse problems involving nonlinear partial differential equations // *Journal of Computational Physics*. 2019. V. 50. No. 3. P. 686–707.

УДК 004.85:004.272

Маманова С.Е. (Алматы, МУИТ)
Тынымбаев С. Т. (Алматы, МУИТ)
Кокенова У.К. (Алматы, МУИТ)

ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОПТИМИЗАЦИИ АРХИТЕКТУРЫ ДЕЛИТЕЛЬНЫХ УСТРОЙСТВ

Аннотация

В данной работе рассматривается использование методов машинного обучения (ML) для автоматизации и оптимизации проектирования архитектур высокоскоростных делительных устройств. Предлагаемый подход позволяет сократить время разработки, улучшить параметры производительности, такие как скорость, энергопотребление и площадь кристалла, а также адаптировать архитектуру под конкретные вычислительные задачи. Полученные результаты демонстрируют перспективность применения ИИ для задач цифрового проектирования в рамках современных требований к производительности вычислительных систем.

Введение

Операция деления занимает одно из ключевых мест в цифровой обработке данных, особенно в приложениях, требующих высокой точности и скорости вычислений: криптография, обработка сигналов, системы управления, машинное обучение и т.д. При этом реализация деления на аппаратном уровне остаётся одной из самых ресурсоёмких задач [1]. Современные подходы к проектированию специализированных делительных устройств требуют компромиссов между производительностью, энергопотреблением и занимаемой площадью [2].

В последние годы методы искусственного интеллекта, в частности машинного обучения, начинают активно внедряться в сферу проектирования электронных схем. Они позволяют автоматизировать рутинные процессы, анализировать большие объёмы данных и находить оптимальные архитектурные решения, которые трудно выявить традиционными методами [3].

Цель и задачи исследования

Целью настоящей работы является разработка подхода, основанного на методах машинного обучения, для автоматизированного проектирования и оптимизации архитектуры делительных устройств.

Задачи:

1. Анализ и формализация параметров архитектур

2. Разработка модели машинного обучения

3. Верификация подхода

Гипотеза исследования:

Применение методов машинного обучения к задачам проектирования архитектуры делительных устройств позволяет автоматически находить такие конфигурации, которые обеспечивают более высокую производительность, меньшие затраты логических ресурсов и сниженное энергопотребление по сравнению с традиционными (ручными) методами проектирования.

Методология

Исследование проводилось в несколько этапов:

1. Генерация архитектурных конфигураций. С помощью генераторов Verilog-кода создавались варианты делителей: на базе классических алгоритмов (деление с восстановлением и без восстановления остатка, алгоритмы restoring и non-restoring, SRT), с различной степенью конвейеризации, шириной шин и логической глубиной [1].

2. Симуляция и синтез. Каждая конфигурация синтезировалась средствами FPGA-синтеза. Снимались метрики которые указаны в таблице 1.

Архитектура	pipeline_depth	bus_width	delay_ns	power_mw	logic_elements
Restoring	3	8	22,1	87	2123
Restoring	4	16	19,5	93	2450
Non-Restoring	3	8	19,3	85	1985
Non-Restoring	4	16	17,2	90	2350
SRT	3	8	15,8	95	2750
SRT	4	16	13,4	102	2980

Таблица 1. Сравнительные характеристики различных архитектур делительных устройств после синтеза на ПЛИС

3. Обучение модели. На основе собранного датасета была обучена модель градиентного бустинга (XGBoost), задача которой — по параметрам входных данных и требуемой производительности предсказать наилучшую архитектуру [5].

4. Анализ и тестирование. Предсказанные моделью архитектуры сравнивались с традиционными вручную спроектированными. Критериями служили: производительность, количество используемых ресурсов, стабильность и масштабируемость [2].

Результаты

Обученная модель достигла точности предсказания оптимальной архитектуры на уровне 89% ($MAE = 5.2\%$, $R^2 = 0.93$). Сравнительный анализ показал, что делительные устройства, предложенные моделью, в среднем на 15–20% быстрее и на 10–12% экономичнее по логическим элементам, чем ручные реализации. Особенно хорошо подход показал себя в задачах с нестандартными битовыми ширинами и высокими требованиями к латентности.

Обсуждение

Методы машинного обучения продемонстрировали высокую применимость в задачах цифрового проектирования. Они позволяют не только ускорить этап архитектурной проработки, но и находить архитектуры, выходящие за рамки традиционных инженерных решений. Особенно актуален предложенный подход в системах, где требуется быстрая адаптация под изменяющиеся параметры среды, например, в киберфизических системах или интеллектуальных криптографических модулях [4].

Заключение

В работе продемонстрирована эффективность применения методов машинного обучения для проектирования и оптимизации архитектур высокоскоростных делительных устройств. Полученные результаты показывают, что ИИ может стать не только инструментом анализа, но и активным участником в разработке цифровых компонентов, особенно в условиях многопараметрических ограничений. Как видно из блок-схемы (Рис. 1), предложенный подход позволяет автоматизировать выбор оптимальной архитектуры делительного устройства через последовательное выполнение ключевых этапов:



Рис. 1. Блок-схема процесса оптимизации архитектур делителей.

Список использованных источников

- [1] Попов А.Ю. Проектирование цифровых устройств с использованием ПЛИС: Учеб. пособие. — М.: Изд-во МГТУ им. Н.Э. Баумана, 2009. — 80 с.
ISBN: 978-5-7038-3317-9
- [2] Hennessy J. L., Patterson D. A. Computer Architecture: A Quantitative Approach. — 6th ed. — Morgan Kaufmann, 2019. — 856 p.
- [3] Vasudevan S. et al. Learning-Based Techniques for Design Automation: A Survey. // ACM Transactions on Design Automation of Electronic Systems, 2020, Vol. 25(3), p. 1–36.
- [4] Лю Цз. Оптимизированное проектирование аппаратного ускорителя на основе машинного обучения // Highlights in Science, Engineering and Technology. 2024. Т. 111. С. URL: <https://www.researchgate.net/publication/383254602>

УДК 004.8.

Медетов А.Р. (Караганда, НАО «Карагандинский
Технический
университет им. А.Сагинова») Сагатбекова Д.Е.
(Караганда, НАО «Карагандинский Технический
университет им. А.Сагинова»)

РЕШЕНИЕ ОБРАТНЫХ ЗАДАЧ В ГЕОФИЗИКЕ С ИСПОЛЬЗОВАНИЕМ МАШИННОГО ОБУЧЕНИЯ

В современной геофизике решение обратных задач играет ключевую роль в изучении структуры Земли, поиске полезных ископаемых и мониторинге окружающей среды. Традиционные методы решения этих задач часто сталкиваются с проблемами нелинейности, неоднозначности и вычислительной сложности. В последние годы машинное обучение (МО) стало мощным инструментом, предлагающим новые подходы к решению обратных задач в геофизике.

Обратные задачи в геофизике формулируются следующим образом: на основе наблюдений за физическими полями на поверхности Земли (например, гравитационное, магнитное, сейсмическое) необходимо восстановить распределение параметров среды, таких как плотность, магнитная восприимчивость или скорость распространения волн. Эти параметры характеризуют внутреннее строение Земли и могут быть связаны с наличием полезных ископаемых, геологическими структурами и другими важными характеристиками.

Традиционные методы решения обратных задач основаны на математическом моделировании прямых и обратных задач. Прямая задача заключается в расчете физического поля на основе заданной модели среды, тогда как обратная задача состоит в определении параметров модели по известным наблюдениям. Существует множество методов решения обратных задач, таких как метод наименьших квадратов, метод Монте-Карло, генетические алгоритмы и другие. Однако эти методы часто сталкиваются с проблемами сходимости, вычислительной сложности и чувствительности к начальным условиям.

Машинное обучение предоставляет новые возможности для решения обратных задач в геофизике. Алгоритмы МО способны обучаться на основе данных и выявлять сложные зависимости между наблюдениями и параметрами среды. Основные преимущества использования МО в геофизике включают автоматизацию процессов, снижение необходимости в ручном труде и экспертных знаниях, эффективную обработку больших объемов данных, учет нелинейных зависимостей и адаптивность алгоритмов к новым данным.

В геофизике применяются различные типы задач МО. Регрессионные модели используются для восстановления параметров среды на основе наблюдений, например, для определения плотности

горных пород по гравитационным данным. Классификационные алгоритмы позволяют определить тип геологической структуры или наличие полезных ископаемых, например, классифицировать горные породы по данным сейсмической разведки. Методы кластеризации помогают выделять группы схожих объектов или параметров среды, например, зоны с повышенной концентрацией полезных ископаемых.

Примеры применения МО в геофизике включают сейсмическую томографию, используемую для восстановления трехмерного распределения скоростей сейсмических волн в Земле, магнитную и гравиразведку для определения формы и размеров залежей полезных ископаемых, электроразведку для изучения распределения электрической проводимости горных пород и гидрогеологические исследования для оценки запасов подземных вод и их качества.

Несмотря на многообещающие результаты, применение МО в геофизике сталкивается с некоторыми вызовами. Одной из основных проблем является недостаток данных, так как для обучения алгоритмов требуется большое количество качественной информации, которая не всегда доступна. Еще одной сложностью является интерпретируемость результатов: алгоритмы МО могут выдавать сложные для анализа и понимания предсказания. Кроме того, модели, обученные на одном наборе данных, могут плохо работать на других данных, что делает задачу обобщаемости важной проблемой.

Тем не менее, развитие МО и появление новых алгоритмов открывают широкие перспективы для решения обратных задач в геофизике. В будущем можно ожидать появления новых методов, основанных на глубоком обучении, которые позволят решать более сложные задачи и получать более точные результаты.

Машинное обучение становится все более важным инструментом в решении обратных задач геофизики. Его преимущества в автоматизации, обработке больших данных, учете нелинейности и адаптивности делают его привлекательным для решения широкого круга задач, от изучения структуры Земли до поиска полезных ископаемых. Несмотря на существующие вызовы, развитие МО открывает новые горизонты для геофизических исследований и позволяет получать более точные и надежные результаты.

Список использованных источников

1. Castelli F., Ismail-Zaden A., Jones D., Sanchez S. *Applications of data assimilation and inverse problems in the Earth sciences*. [Электронный ресурс] – Режим доступа: <https://www.geokniga.org/books/31992>
2. Deep learning methods for solving linear inverse problems Research directions and paradigms [Электронный ресурс] – Режим доступа: <https://www.sciencedirect.com/science/article/abs/pii/S0165168420302723>

УДК 517.956

Мирсабуров М. (Узбекистан, Термезский гос. университет)
Макулбай А.Б., Бердышев А.С. (Алматы, КазНПУ им. Абая)
Мирсабурова Г.М. (Узбекистан, Ташкентский гос. пед. университет)

КОМБИНИРОВАННАЯ ЗАДАЧА ДЛЯ ОДНОГО КЛАССА УРАВНЕНИЙ СМЕШАННОГО ТИПА С РАЗЛИЧНЫМИ ПОРЯДКАМИ ВЫРОЖДЕНИЯ

В работе в конечной смешанной области, для уравнения смешанного эллипτικο-гиперболического типа с различными порядками вырождения и с сингулярными коэффициентами доказаны теоремы единственности и существования решения задачи с недостающим условием Трикоми на граничной характеристике и аналогом условия Франкля на разных частях краев разреза вдоль отрезка вырождения. На отрезке линии вырождения уравнения задается общее условие сопряжения, а на границе области эллиптичности и отрезке вырождения задается условие Бицадзе-Самарского.

Пусть D – конечная односвязная область комплексной плоскости $C = \{z = x + iy\}$, ограниченная при $y > 0$ нормальной кривой $\sigma_0(y = \sigma_0(x))$ с концами в точках $A(-1, 0)$ и $B(1, 0)$, заданной уравнением $x^2 + 4(l+2)^{-2} y^{l+2} = 1$, а при $y < 0$ характеристиками AC и BC уравнения

$$G(u) = \begin{cases} \mu_{xx} u + u_{yy} + \frac{\delta_0}{y} u_y, & > 0, \\ -(\mu_{xx} u + u_{yy} + \frac{\beta_0}{y} u_y), & < 0, \end{cases}$$

$$G(u) = 0,$$

где l, m – положительные постоянные, $\delta_0 \in (-l/2, 1)$, $\beta_0 \in (-m/2, 1)$, причем $l \neq m$.

Обозначим через D^+ и D^- части области D , лежащие соответственно в полуплоскостях $y > 0$ и $y < 0$, а через C_0 и C_1 точки пересечения граничных характеристик AC и BC с характеристиками уравнения, выходящими из точки $E(c, 0)$, где c – некоторое число, принадлежащее интервалу $J = (-1, 1)$ оси $y = 0$.

Пусть $p(x) \in C^1[-1, c]$ – диффеоморфизм из множества точек отрезка $[-1, c]$ во множество точек отрезка $[c, 1]$, причем $p'(x) < 0$, $p(-1) = 1$, $p(c) = c$. В качестве примера такой функции приведем линейную функцию $p(x) = d - kx$, где $k = (1 - c) / (1 + c)$, $d = 2c / (1 + c)$.

Заметим, что уравнение в верхней полуплоскости $y > 0$ является уравнением эллиптического типа, а при $y < 0$ является уравнением гиперболического типа, причем порядок параболического вырождения этих уравнений на оси $y = 0$ разные.

В задаче Трикоми значение искомой функции задается во всех точках граничной характеристики AC . В настоящей работе в смешанной области D , для уравнения исследуется корректность задачи, когда граничная характеристика AC произвольным образом разбивается на две части AC_0 и C_0C и на первой части $AC_0 \subset AC$ задается значения искомой функции (неполное условие Трикоми), а вторая часть C_0C освобождена от краевого условия и которая заменена аналогом условия Франкля на разных частях краев разреза вдоль отрезка вырождения AB . На кривой σ_0 и отрезке вырождения AB задается условие Бицадзе-Самарского.

Задача МА. Требуется найти в области D функцию $u(x, y)$, удовлетворяющую следующим условиям:

- 1) $u(x, y)$ – непрерывна в каждой из замкнутых областей $\bar{D}^+$ и $\bar{D}^-$;
- 2) функция $u(x, y)$ принадлежит классу $C^2(D^+)$ и удовлетворяет уравнению в области D^+ ;
- 3) функция $u(x, y)$ является в области D^- обобщенным решением класса R_1 [1].
- 4) на отрезке AB – линии параболического вырождения уравнения выполняется общее условие сопряжения

$$u(x, -0) = a(x)u(x, +0) + a_0(x), \quad x \in [-1, 1]$$

$$\lim_{y \rightarrow -0} (-y)^{\beta_0} \frac{\partial u}{\partial y} = b(x) \lim_{y \rightarrow +0} y^{\delta_0} \frac{\partial u}{\partial y} + b_0(x), \quad x \in (-1, 1) \setminus \{c\},$$

где $a(x)$, $b(x)$, $a_0(x)$, $b_0(x)$ – заданные непрерывно-дифференцируемые функции на $\bar{J}$,

причем $a(x) \neq 0$, $b(x) \neq 0$, $\forall x \in \bar{J}$, $a_0(-1) = 0$, а пределы $\lim_{y \rightarrow -0} (-y)^{\beta_0} \frac{\partial u}{\partial y} \left(\lim_{y \rightarrow +0} y^{\delta_0} \frac{\partial u}{\partial y} \right)$ при $x = \pm 1$, $x = c$, могут иметь особенности порядка ниже $1 - 2\beta (1 - 2\delta)$, где $\beta = (m + 2\beta_0) / 2(m + 2)$ ($\delta = (l + 2\delta_0) / 2(l + 2)$);

5) $u(x, y)$ удовлетворяет следующим условиям:

$$u(x, \sigma_0(x)) = \rho(x)u(x, +0) + \varphi_0(x), \quad x \in [-1, 1],$$

$$u(x, y)|_{AC_0} = \psi(x), \quad x \in [-1, (c-1)/2],$$

$$u(p(x), -0) = \mu(x)u(x, +0) + f(x), \quad x \in [-1, c],$$

где $\rho(x)$, $\varphi_0(x)$, $\mu(x)$, $f(x)$ – непрерывно-дифференцируемые функции в множестве их определения, причем $a(x) = (1 - x^2)\tilde{a}(x)$, $a_0(x) = (1 - x^2)\tilde{a}_0(x)$, $\psi(-1) = 0$, $\mu(-1) = 0$, $f(-1) = 0$, $\rho(x) = (1 - x^2)\tilde{\rho}(x)$, $\varphi_0(x) = (1 - x^2)\tilde{\varphi}_0(x)$, $x \in [-1, 1]$.

Заметим, что условия и являются общими условиями сопряжения, – условием Бицадзе-Самарского связывающее значения искомой функции $u(x, y)$ на кривой σ_0 и на отрезке вырождения AB , – неполным условием Трикоми на части граничной характеристики $AC_0 \subset AC$, – аналог условия Франкля на разных краях разреза вдоль отрезка вырождения AB .

Если в уравнение (1) $l = m$, $\beta_0 = \delta_0$, то (1) превратится в уравнение Геллерстедта с сингулярным коэффициентом, для которого задачи с аналогами условия Франкля исследованы в работах [1]–[4].

Установлена справедливость следующих теорем.

Теорема 1. Задача МА при выполнении условий

$$a_0(x) \equiv 0, \quad b_0(x) \equiv 0, \quad \varphi_0(x) \equiv 0, \quad \psi(x) \equiv 0, \quad f(x) \equiv 0,$$

$$a(x) > 0, \quad b(x) > 0, \quad 0 < \rho(x) < 1, \quad 0 < \mu(x) < a[p(x)],$$

имеет только тривиальное (тождественно равное нулю) решение.

Теорема 2. Решение задачи МА при выполнении условий

$$a(x), a_0(x), b(x), b_0(x), \rho(x), \varphi_0(x) \in C[-1, 1] \cap C^1(-1, 1),$$

$$\psi(x) \in C[-1, (c-1)/2] \cap C^1(-1, (c-1)/2),$$

$$f(x) \in C[-1, c] \cap C^1(-1, c), \quad a(x) > 0, \quad b(x) > 0, \quad \frac{l + 2\delta_0}{2(l + 2)} \geq \frac{m + 2\beta_0}{m + 2}$$

существует.

$$\frac{l + 2\delta_0}{2(l + 2)} > \frac{m + 2\beta_0}{m + 2}$$

В случае, когда $\frac{l + 2\delta_0}{2(l + 2)} > \frac{m + 2\beta_0}{m + 2}$, задача МА эквивалентным образом сводится к интегральному уравнению Фредгольма второго рода со слабой особенностью в ядре, однозначная разрешимость которого следует из Теоремы 1. Если в последнем неравенстве выполняется равенство, то доказательство существования решения сводится к системе сингулярных интегральных уравнений Трикоми со сдвигом в несуммируемой части ядра, которые методом регуляризации Карлемана-Векуа сведены к интегральному уравнению Винера-Хопфа, однозначная разрешимость которого следует из единственности решения задачи.

Работа выполнена при поддержке Фонда Министерства инновационного развития Республики Узбекистан (грант № ФЗ-202009211).

Список использованных источников

1. Салахитдинов М.С., Мирсабуров М. *Нелокальные задачи для уравнений смешанного типа с сингулярными коэффициентами*. Ташкент: Университет, 2005.
2. Mirsaburov M., Ergasheva S.B. *The Problem in the Unbounded Domain with the Frankl Condition on the Segment of the Degeneration Line and with a Missing Gellerstedt Condition for a Class of Mixed-Type Equations*, *Russian Mathematics*, 2023, 67(8), – P.18–26.
3. Mirsaburov M., Berdyshev A.S., Ergasheva S.B., Makulbay A.B. *The problem with the missing Goursat condition at the boundary of the domain for a degenerate hyperbolic equation with a singular coefficient* // *Bulletin of the Karaganda University-Mathematics*. – 2024. 114(2). – P. 147-164.
4. Мирсабурова Г. *Объединенная задача Трикоми и задача со смещением для уравнения Геллерстедта* // *Известия вузов*. 2012, №9, – С.32-46.

УДК 517.958

Омаров М.Т. (Караганда, КарУ им. академика
Е.А. Букетова)

Рамазанов М.И. ((Караганда, КарУ им. академика
Е.А. Букетова)

Танин А.О. (Караганда, КарУ им. академика Е.А.
Букетова)

Шаяхметова Б.К. (Караганда, КарУ им. академика
Е.А. Букетова)

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ ДЛЯ РЕШЕНИЯ ОБРАТНЫХ ЗАДАЧ, СВЯЗАННЫХ С ДРОБНЫМИ ДИФФЕРЕНЦИАЛЬНЫМИ УРАВНЕНИЯМИ

Дробное исчисление широко используется для моделирования процессов с памятью и наследственными свойствами в различных областях науки и техники (механика, физика пористых сред, электрохимия и др.). В таких моделях порядок дробной производной зачастую является параметром, определяющим интенсивность эффекта памяти. Однако на практике этот порядок далеко не всегда известен заранее и должен определяться на основе экспериментальных данных или наблюдаемых характеристик процесса. В прикладных моделях с дробными производными порядок производной нередко неизвестен, и его определение представляет собой важную обратную задачу [1], иными словами, возникает задача идентификации порядка α дробной производной по доступной информации о решении модели.

Обратные задачи для дробных дифференциальных уравнений, в частности задачи идентификации порядка производной, привлекают всё больший интерес вследствие их практической значимости [1]. Классическая теория обратных задач указывает, что для определения неизвестного параметра (коэффициента уравнения, правой части, начального условия и т.д.) необходимо дополнительно к стандартным условиям задачи (начальным и граничным) иметь некоторую дополнительную информацию о решении. Такая дополнительная информация (условие переопределения) должна обеспечивать единственность, а желательно и существование решения обратной задачи. В контексте дробных моделей это обычно означает, что одних только

наблюдаемых данных процесса недостаточно для однозначного определения α , и требуются специальные измерения или предположения.

Цель данной статьи – подробно исследовать обратную задачу определения порядка дробной производной. Мы формулируем математическую постановку этой задачи для наиболее распространенных определений дробной производной, анализируем её сложность, рассматриваем возможные подходы к решению и предлагаем конкретный метод. Кроме того, приводится численный эксперимент, демонстрирующий работоспособность и эффективность предложенного метода на модельном примере, а также проводится обсуждение полученных результатов в сравнении с альтернативными подходами.

Производная Капуто порядка определяется как дробный интеграл от производной первого порядка функции [2]:

$$CD_f(t) = 1\Gamma(1-\alpha) \int_0^t (t-s)^{-\alpha} f(s) ds$$

Методы машинного обучения. Новым направлением в решении обратных задач является использование методов машинного обучения и искусственного интеллекта. Идея состоит в том, чтобы обучить модель (например, нейронную сеть) восстанавливать параметр α по характерным признакам наблюдаемого решения. Для этого генерируется обширное множество обучающих данных путём решения прямой задачи при различных значениях α (возможен как случай непрерывной модели, так и дискретизация временных рядов или спектральных характеристик). Далее обученная нейронная сеть сможет практически мгновенно оценивать α по новым данным эксперимента. Подобный подход уже применяется для идентификации параметров моделей с дробными производными в технических задачах – например, при моделировании электрохимических процессов в батареях применяют нейросети или эволюционные алгоритмы для подбора параметров дробной модели по измеренным импедансным спектрам. Преимуществом машинного обучения является способность учитывать сложные нелинейные взаимосвязи и справляться с зашумлёнными данными.

В данной работе для решения поставленной обратной задачи мы выбираем численный подход, основанный на минимизации невязки (метод наименьших квадратов). Рассмотрим простейшую модель, для которой влияние порядка дробной производной проявляется явно: дробное релаксационное уравнение. Это аналог экспоненциального распада, в котором целая производная по времени заменена дробной. Уравнение имеет вид:

$$CD_t y(t) + \lambda y(t) = 0, y(0) = 1,$$

где $\lambda > 0$ – известный коэффициент (скорость релаксации), а $\alpha \in (0, 1]$ порядок производной, который требуется определить. При $\alpha = 1$ это уравнение вырождается в классическое $y'(t) + \lambda y(t) = 0$ с решением $y(t) = e^{-\lambda t}$. При дробном общее решение выражается через функцию Миттаг-Леффлера – специальную функцию, обобщающую экспоненту. Для данной задачи решение записывается как:

$$y(t) = E_{\alpha, 1}(-\lambda t)$$

Для численного эксперимента сгенерируем «наблюдаемые» данные, рассчитывая решение $y(t)$ при некотором неизвестном истинном значении $\alpha_{ист}$. Будем считать $\alpha_{ист} = 0.7$ (в реальной задаче это скрытый параметр, который мы попытаемся восстановить). Возьмём $\lambda = 1$ и рассмотрим интервал времени $0 \leq t \leq 5$. Решение вычисляем в 51 точке (с шагом $t = 0.1$). Затем искадим полученные значения добавлением небольшого шума, имитируя экспериментальные погрешности. В результате получаются данные $y_{obs}(t_i)$, отклоняющиеся от теоретического решения не более чем на несколько процентов.

Обратную задачу решаем методом наименьших квадратов: выбираем такой порядок α , при котором сумма квадратов отклонений модели от наблюдений минимальна [3]:

$$J(\alpha) = \sum_{i=1}^N (E_{\alpha, 1}(-t_i) - y_{obs}(t_i))^2 \rightarrow \min$$

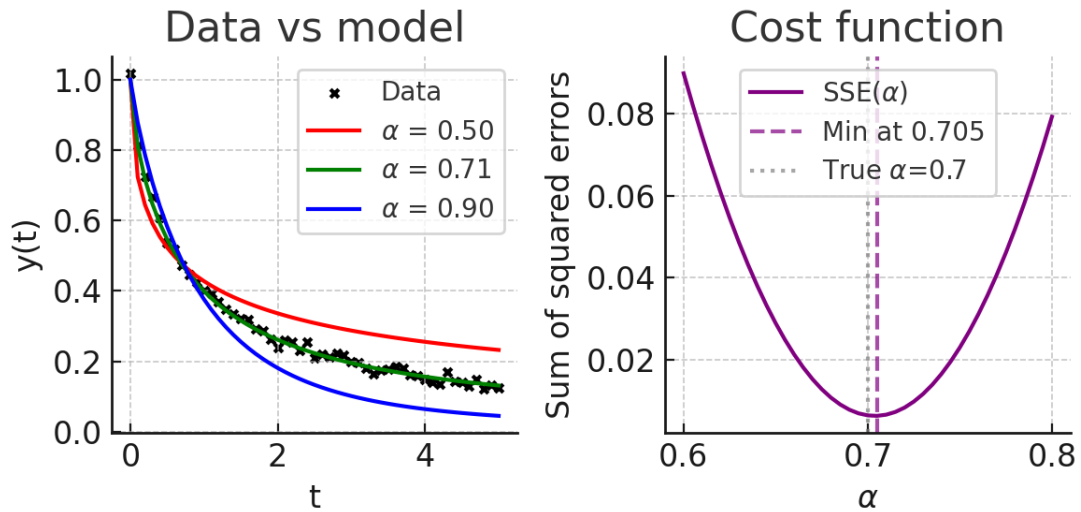


Рис. 1: Синтетические данные (с шумом) и модели решения при разных значениях.

Метод машинного обучения мог бы дать преимущество в случаях, когда прямое решение уравнения занимает значительное время или когда требуется обрабатывать данные в реальном времени.

Сравнивая наш подход с результатами известных работ, отметим, что мы не затрагивали вопроса строгого доказательства существования решения обратной задачи. В приведённом примере решение очевидно существует [1], но в общем случае в нелинейной задаче необходим анализ, гарантирующий, что минимум функционала действительно достигается внутри допустимого интервала значений.

Список использованных источников

Ashurov R, Sitnik S. Identification of the Order of the Fractional Derivative for the Fractional Wave Equation. *Fractal and Fractional*. 2023; 7(1):67. <https://doi.org/10.3390/fractalfract7010067>

1. Kilbas, A.A. (2006) *Theory and Application of Fractional Differential Equations*. Elsevier, Amsterdam.
2. Alimov, S., & Ashurov, R. (2020). Inverse problem of determining an order of the Caputo time-fractional derivative for a subdiffusion equation. *Journal of Inverse and Ill-Posed Problems*, 28(5), 651–658. doi:10.1515/jiip-2020-0072.

УДК 517.

Орумбаева Н.Т., Жантасова Б.Б.
 (г.Караганда, КарУ имени академика Е.А. Букетова)

О РЕШЕНИИ ОДНОЙ КРАЕВОЙ ЗАДАЧИ ДЛЯ ГИПЕРБОЛИЧЕСКОГО УРАВНЕНИЯ С ДРОБНОЙ НАГРУЗКОЙ

Рассмотрим уравнение

$$\frac{\partial^2 u(x,t)}{\partial t^2} = a^2 \frac{\partial^2 u(x,t)}{\partial x^2} + \mu \left[\mathcal{D}_x^\beta u(x,t) \right]_{x=x_0} + f(x,t), \quad 0 \leq x < \infty, t > 0, x_0 > 0, \quad (1)$$

с начальными условиями

$$u(x, 0) = g_1(x), \quad (2)$$

$$\frac{\partial u(x, 0)}{\partial t} = g_2(x) \quad (3)$$

и граничными условиями

$$u(0, t) = h(t). \quad (4)$$

Теорема. Пусть выполнены следующие условия:

1. Функции $g_1(x)$, $g_2(x)$, $h(t)$ и $f(x, t)$ непрерывны и ограничены на своих областях $0 \leq x < \infty$, $t > 0$.

2. Параметр μ и константы $a > 0$, $x_0 > 0$ таковы, что операторы, возникающие в интегральных уравнениях для $\psi(t)$ являются сжимающими в пространстве непрерывных функций на $[0, T]$ с нормой

$$\|\psi\| = \sup |\psi(t)|, 0 \leq t \leq T.$$

Тогда задача (1)-(4) имеет единственное решение $u(x, t)$ в классе непрерывных функций, удовлетворяющих начальным и граничным условиям, причем решение

имеет различный вид при $t > \frac{x}{a}$ и $t < \frac{x}{a}$.

Замечание. Вместо x_0 можно рассматривать непрерывную ограниченную функцию

В данной работе получено приближенно-аналитическое решение краевой задачи для дробно-нагруженного гиперболического уравнения с одной пространственной переменной, содержащего дробную производную Римана-Лиувилля. Предложенный метод основан на использовании интегральных уравнений и позволяет свести исходную задачу к интегральному уравнению типа Вольтерра. Доказана теорема о существовании и единственности решения задачи, установлены условия, при которых решение обладает требуемыми свойствами. Полученное решение представлено в виде суммы двух интегралов, что позволяет анализировать его поведение в различных областях определения переменных. Аналитическое решение представляет интерес для построения численных методов решения аналогичных задач. Результаты исследования могут быть использованы для моделирования волновых процессов в средах с дробными свойствами. Данное исследование может послужить основой для дальнейшего изучения краевых задач для уравнений гиперболического типа с дробными производными.

References

Нахушев А.М. Элементы дробного исчисления и их приложения. - Нальчик: НИИ ПМА КБНЦ РАН, 2000. - 298с.

Ramazanov, MI and Kosmakova, MT Boundary value problem for a loaded fractional diffusion equation 2023 TURKISH JOURNAL OF MATHEMATICS 47

(5) , pp.1585-+ DOI10.55730/1300-0098.3450

Jenaliyev M.T., Ramazanov M.I., Attaev A.Kh., Gulmanov N.K. Stabilization of a solution for two-dimensional loaded parabolic equation // Bulletin of the Karaganda University. Mathematics Series, 2020, 100(4), 55–70. DOI:10.31489/2020M4/55-70.

УДК 519.635.6: 624.131

.Рысбаева Н., (Алматы КБТУ),
 Рысбайулы Б. (Астана АИТУ)

ОБРАТНАЯ ЗАДАЧА НЕЛИНЕЙНОГО ПЕРЕНОСА ВЛАГИ В ПОРИСТОЙ СРЕДЕ

Математическая модель задачи

На рис.1. изображен контейнер заполненный почво-грунтом. Боковые грани которого изолированы, чтобы влага не покинула контейнер, и наружная влага не проникла внутри контейнера (влагоизоляция). В таком случае влага может переноситься вдоль оси Ox . В этом случае для переноса влаги оси Ox можно воспользоваться уравнением Аллера [1]. В области $Q=(0,1) \times (0, [3t]_{\max})$,

$$\frac{\partial W}{\partial t} = \frac{\partial}{\partial x} \left(D(W) \frac{\partial W}{\partial x} + A \cdot \frac{\partial^2 W}{\partial t \partial x} \right) \quad (x, t) \in Q \quad (1)$$

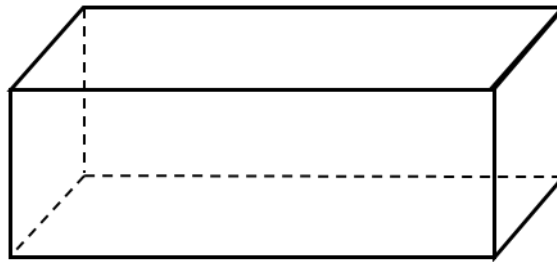


Рис.1. Контейнер с пористой средой

Здесь W – влага почвы, $D(W)$ – коэффициент диффузий влаги, $A \cdot \frac{\partial^3 W}{\partial x^2 \partial t}$ призван объяснить факт движения против градиента влажности, A – варьируемый коэффициент Аллера. В настоящей работе будем рассматривать граничные условия в виде

$$\frac{W(0,t)}{\partial x} = 0, \quad D(W(H,t)) \frac{\partial W(H,t)}{\partial x} + A \frac{\partial^2 W(H,t)}{\partial t \partial x} = f(t), \quad t \in (0, t_{\max}) \quad (2)$$

Первое условие системы (2) указывает отсутствие на границе $x = 0$ потока тепла. Второе условие системы (2) выражает изменение потока влаги на границе $x = l$. Отметим, что граница контейнера $z = l$ соприкасается с воздухом.

В начальный момент времени границе $t = 0$ задается распределение влаги вдоль оси Ox в виде функций

$$W(x, 0) = W_0(x), \quad x \in (0, l) \quad (6.3)$$

Граница $x = 0$ контейнера соприкасается почво-грунтом, а граница $z = l$ соприкасается с воздухом. Как показана на рис.2 в точке $x = l$ поставлен датчик влаги, которые фиксирует изменения влаги через каждый 6 сек. Измеренные данные в виде excel файл сохраняются в USB носитель. Сохраненные данные обозначим соответственно через

$$\omega_g(t) , t \in (0, 3t_{max}) . \quad (6.4)$$

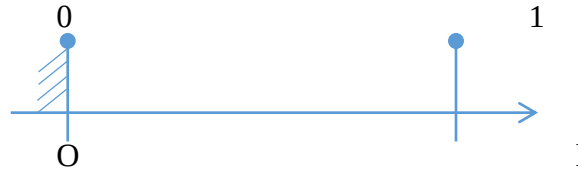


Рис.2. Точки расположения датчиков влаги

Обратная задача. Используя систему (1) – (3) и измеренные данные (4) разработать метод нахождения: Коэффициента диффузий влаги из рис. 3. Зависимость величины $D(W)$ от влаги исследована в работе [2] и построены графики рис.3.

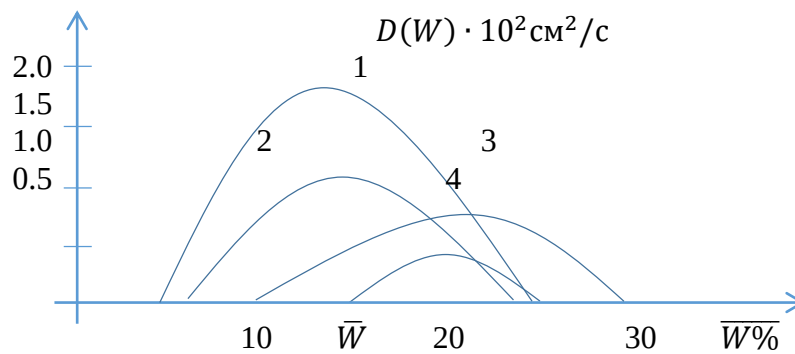


Рис.3. Зависимость коэффициентов изотермической влагопроводности от исходной влажности:
 1 – песок средне-мелкозернистый; 2 – средний лёссовидный суглинок; 3 – тяжелый лёссовидный суглинок; 4 – морская глина. [Глобус, 1983]

Функция $D(W)$ от влажности грунта имеет максимум при некоторой влажности $\bar{W}$ [3]. Эксперименты, поставленные в работах [3] показали, что со временем форма и основные характеристики кривых не меняются с изменением ординат (рис.3). Учитывая сказанные коэффициент влагопроводности ищем в виде [4,5]

$$D(W) = B e^{-E(W-\bar{W})^2} .$$

Параметры $B, E, \bar{W}$ подлежат к определению. Мы будем разрабатывать такой метод, который становится пригодной для любого почво-грунта. У нас имеется качественное свойство коэффициента диффузий влаги, изображенной на рис.3.

Отметим, что $W(x, t) \in (0, 1)$. Считаем, что параметры влаги $A, f(t)$ - известными.

Узловые точки переменной t обозначим через $t_j, j = 0, 1, \dots, 3m$

Узловые точки по пространственной переменной обозначим через

$$x_i = i \cdot \Delta z, i = 0, 1, \dots, N$$

В сеточной области изучается прямая, сопряженные и вспомогательные разностные задачи. Неизвестные величины $D(Y)$ ищется итерационным способом. Величины $A, f(t)$ определяются аналогичным способом, как в задаче Дирихле [5]. В этом случае решение прямой разностной схемы будет зависеть от номера итерации n , т.е

$$Y_i^j(n), \quad i = 0, 1, \dots, N; \quad j = 0, 1, \dots, 3m - 1$$

Составляется вспомогательная разностная задача

В этом случае вариация функционала имеет вид

$$J_{n+1}(D) - J_n(D) = \sum_{j=0}^{3m-1} (Y_N^{j+1})^2 \cdot \tau - \\ - \sum_{j=0}^{3m-1} \sum_{i=1}^N Y_{i\bar{x}}^{j+1} \cdot \Delta D \left(Y_{i-\frac{1}{2}}^j \right) \cdot U_{i\bar{x}}^j \cdot \tau \cdot h - \sum_{j=0}^{3m-1} \sum_{i=1}^N \Delta Y_{i\bar{x}}^{j+1} \cdot \Delta D \cdot U_{i\bar{x}}^j \cdot \tau \cdot h$$

В настоящей работе выводятся расчетные формулы неизвестных параметров влаги $B, E, \bar{W}$.

REFERENCES

1. Hallare. *Potential effcae de L'eau Lans le Sol en Regime de dessechement*. France 1963, 114-122.
2. Глобус А.У. *Физика неизотермического внутрипочвенного влагообмена*. Л.: Гидрометеиздат, 1983. 279 с.
3. Федяева Е.А., Королев В.А. *Закономерности и факторы неизотермического влагопереноса в дисперсных грунтах разного гранулометрического состава // Ломоносовские чтения, 16-24 апреля 2013 г., МГУ, секция "Инженерная и экологическая геология". М.: 2013b. <http://geo.web.ru/db/msg.html?mid=1187172>*
4. Рысбайулы Б. *Обратные задачи нелинейной теплопроводности*. Издательский дом «Қазақ Университеті», 2022, 369 с.
5. Nazerke Rysbayeva, Bolatbek Rysbaiuly. *Nonlinear Inverse Problem of Moisture Transfer in the Soil. The 11th International Conference "Inverse problems: Modeling and Simulation", Malta, May, 2024.*

УДК 550.831.01+519.6+517.927

Сигаловский М.А. (Алматы, КБТУ, КазНУ им.
 Аль-Фараби)
 Азимов А.А. (Алматы, Satbayev University)

ГЕОМЕТРИЯ КРУГОВОЙ АНОМАЛИИ В ПРЯМОУГОЛЬНОЙ ОБЛАСТИ ПОИСКА ДЛЯ ОДНОЙ ЗАДАЧИ ГРАВИМЕТРИИ

Рассматривается геометрическая двумерная обратная задача гравиметрии. Требуется по данным замеров с поверхности земли восстановить расположение круговой аномалии в виде координат центра круга в прямоугольной области поиска. Граничные условия ставятся на части границы по следующим физическим и геометрическим соображениям: 1) гравиметрия проводится вдоль верхней границы области поиска Ω ; 2) область Ω выбрана настолько большой, что влияние силы тяжести на её заглубленную границу практически отсутствует, поэтому потенциалы возмущенного и невозмущенного гравитационных полей на этой границе равны; 3) искомая аномалия O есть круг известного радиуса R с неизвестными координатами центра $x_0=a$, $y_0=b$. Пусть u и ρ – функции гравитационного потенциала и плотности соответственно, S – составная заглубленная граница прямоугольной области поиска. Математическая постановка обратной задачи имеет вид:

$$u_{x,y} = -4\pi G \rho_{x,y}, \quad x,y \in \Omega = \{x,y: 0 < x < L, 0 < y < H\} \quad (1)$$

$$\rho(x,y) = \begin{cases} \eta, & \text{если } x,y \in O \\ 0, & \text{если } x,y \notin O \end{cases} \quad (2)$$

$$u_{x,y} = 0, \quad x,y \in S \quad (3)$$

$$u_x = 0 = \alpha x, \quad 0 < x < L \quad (4)$$

$$\partial u(x, 0) / \partial y = \beta x, \quad 0 < x < L \quad (5)$$

$$O = \{x,y: x-a^2+y-b^2 \leq R^2\} \quad (6)$$

$$I(a,b) = 0L \partial u_x, 0 \partial y - \beta x^2 dx \rightarrow \min \quad (7)$$

В соответствии с общими принципами решения обратных задач [1], [2] мы переходим к задаче минимизации функционала (7), где u есть решение краевой задачи (1), (3), (4), зависящее от параметров a и b в соответствии с равенствами (2) и (6). Таким образом, поставленная геометрическая обратная задача состоит в нахождении параметров a и b таких, чтобы условия (1)-(6) были удовлетворены.

Для перехода к дальнейшему исследованию необходимо описать элементарную геометрию целевой области при ее варьировании, так как интеграл (7) зависит от областей интегрирования, которые и есть целевая область и ее вариация. Далее окружность с центром A соответствует целевой области, окружность с центром B – ее вариации. Итак, пусть заданы две окружности одинакового радиуса R с центрами $A(x_0, y_0)$ и $B(x_1, y_1)$. Их уравнения:

$$\{x-x_0^2+y-y_0^2=R^2 \quad x-x_1^2+y-y_1^2=R^2 \quad (8)$$

Расстояние между их центрами $d = \sqrt{x_1-x_0^2 + y_1-y_0^2}$, причем $d < R$ (окружности пересекаются).

Внешняя граница объединения окружностей состоит из двух внешних дуг, принадлежащих разным окружностям.

1. Определим точки пересечения окружностей. Рассмотрим систему (8). Вычтем второе уравнение из первого и приведем к уравнению прямой

$$x_1-x_0x-xc+y_1-y_0y-yc=0$$

где (x_c, y_c) — середина отрезка AB : $x_c = x_0 + \frac{x_1 - x_0}{2}$, $y_c = y_0 + \frac{y_1 - y_0}{2}$.
 Расстояние от A до середины C равно d_2 , а до точек пересечения — $h = \sqrt{R^2 - d_2^2}$. Тогда точки пересечения:

$$x_p = x_c + h \frac{y_1 - y_0}{d_2}, \quad y_p = y_c - h \frac{x_1 - x_0}{d_2}, \quad x_q = x_c - h \frac{y_1 - y_0}{d_2}, \quad y_q = y_c + h \frac{x_1 - x_0}{d_2}.$$

Рассмотрим параметрическое задание дуг. Углы точек пересечения в полярных координатах относительно центра A :

$$p = \arctg 2 \frac{y_p - y_0}{x_p - x_0}, \quad q = \arctg 2 \frac{y_q - y_0}{x_q - x_0},$$

где $\arctg 2 u = \begin{cases} \arctg u, & x \geq 0 \\ \arctg u + \pi, & x < 0, y \geq 0 \\ \arctg u - \pi, & x < 0, y < 0 \end{cases}$, $x=0, y>0$ — $\frac{\pi}{2}$, $x=0, y<0$ — $-\frac{\pi}{2}$, $x=0, y=0$ не определен, $x=0, y=0$ — арктангенс угла с учетом квадранта расположения точки. Для окружности с центром A , внешняя дуга идёт от q до p :

$$x = x_0 + R \cos \alpha, \quad y = y_0 + R \sin \alpha, \quad \alpha \in [q, p]$$

Для окружности с центром B , внешняя дуга идёт от p до q :

$$x = x_1 + R \cos \alpha, \quad y = y_1 + R \sin \alpha, \quad \alpha \in [p, q]$$

Граница симметрической разности состоит из двух внутренних дуг:

Внутренняя дуга окружности A идёт от p до q

$$x = x_0 + R \cos \alpha, \quad y = y_0 + R \sin \alpha, \quad \alpha \in [p, q]$$

Внутренняя дуга окружности B идёт от q до p :

$$x = x_1 + R \cos \alpha, \quad y = y_1 + R \sin \alpha, \quad \alpha \in [q, p]$$

3. Укажем ГМТ симметрической разности кругов. Симметрическая разность — это точки, принадлежащие ровно одной из окружностей. Это соответствует множеству: $(x - x_0)^2 + (y - y_0)^2 = R^2 \vee (x - x_1)^2 + (y - y_1)^2 = R^2$ (9) где $\vee$ означает исключающее "или". Далее переходим к исследованию интеграла (7) в задаче (1-7) на области (9).

Работа выполнена при поддержке проекта № AP05135158-OT-19 МОН РК «Development of geographic information system for solving the problem of gravimetric monitoring of the state of the subsoil of oil and gas regions of Kazakhstan based on high-performance computing in conditions of limited experimental data».

Библиография:

1. *Kabanikhin, S. I. Inverse and Ill-posed Problems: Theory and Applications.* // Boston, Berlin: Walter de Gruyter. – 2012.
2. *Serovajsky S. Ya., Sigalovsky M., Azimov A. Non-smooth optimization methods in the geometric inverse gravimetry problem // Advanced Mathematical Models & Applications – 2022. – Vol.7 №1, - P. 5-15*

УДК 004.8

Смаилова А.С. (Караганда, КарУ им. Е.А. Букетова)
 Шульгина-Таращук А.С. (Караганда, КарУ им. Е.А. Букетова)

МЕТОДЫ МАШИННОГО ОБУЧЕНИЯ ДЛЯ РЕШЕНИЯ ОБРАТНЫХ ЗАДАЧ

Обратные задачи встречаются во многих научных и инженерных областях, таких как медицина, физика, геофизика и компьютерное зрение. Они заключаются в восстановлении неизвестных параметров системы на основе наблюдаемых данных. Традиционные методы решения таких задач, например, регуляризация и численные оптимизационные алгоритмы, часто требуют сложных вычислений и значительных априорных знаний о системе. В последние годы машинное обучение (МО) стало мощным инструментом для решения обратных задач, предлагая новые подходы, которые могут значительно повысить точность и скорость вычислений. В данной статье рассматриваются основные методы МО, используемые в обратных задачах, их преимущества и ограничения [1].

Классификация методов машинного обучения для обратных задач:

— Супервайзинговое обучение: использование размеченных данных для предсказания неизвестных параметров.

— Нейросетевые методы: глубокие нейронные сети (DNN), свёрточные нейросети (CNN), рекуррентные нейросети (RNN) и трансформеры.

— Байесовские методы: вероятностные модели и апостериорное распределение решений.

— Усиленное обучение: поиск оптимального решения на основе проб и ошибок. В решении обратных задач используются глубинные нейронные сети:

— Использование автоэнкодеров и вариационных автоэнкодеров (VAE) для восстановления данных.

— Генеративные состязательные сети (GAN) для решения плохо обусловленных обратных задач.

— Физически-осведомленные нейросети (PINN) для интеграции физических законов в процесс обучения.

Применение МО в конкретных обратных задачах:

— Медицинская томография: реконструкция изображений на основе неполных данных.

— Геофизические исследования: восстановление подземных структур по данным сейсморазведки.

— Компьютерное зрение: восстановление 3D-объектов из 2D-изображений. В таблице 1 описывается сравнение традиционных методов с ИИ-подходами:

Таблица 1. Сравнительная таблица

Критерий	Традиционные методы	Методы машинного обучения

Точность	Зависит от качества априорных моделей и параметров	Высокая, особенно при наличии больших объемов данных
Скорость вычислений	Медленные, требуют итерационных расчетов	Быстрые после этапа обучения
Гибкость	Жестко зависят от математической модели	Способны адаптироваться к различным данным
Необходимость априорных знаний	Высокая, требуют точных физических моделей	Низкая, обучаются на данных
Интерпретируемость	Высокая, основана на известных математических принципах	Часто сложная, нейросетевые модели работают как «черный ящик»

Преимущества и ограничения МО в решении обратных задач:

- Высокая скорость обработки и автоматизация.
- Возможность обучения на больших объемах данных.
- Чувствительность к качеству и объему обучающих данных.
- Ограниченная интерпретируемость решений нейросетевых моделей

[2].

Далее рассматривается задача восстановления функции из её выходных значений с помощью нейросетевой модели (рис.1).

```
import numpy as np
import tensorflow as tf
from tensorflow import keras
from sklearn.model_selection import train_test_split

# Создаем синтетические данные:  $y = x^2 + \sin(3x)$ 
np.random.seed(42)
X = np.linspace(-5, 5, 1000).reshape(-1, 1)
y = X**2 + np.sin(3 * X)

# Разделяем на обучающую и тестовую выборки
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, random_state=42)

# Создаем нейросетевую модель
model = keras.Sequential([
    keras.layers.Dense(64, activation='relu', input_shape=(1,)),
    keras.layers.Dense(64, activation='relu'),
    keras.layers.Dense(1)
])

# Компилируем и обучаем модель
model.compile(optimizer='adam', loss='mse')
model.fit(X_train, y_train, epochs=100, batch_size=32, verbose=0)

# Предсказываем значения на тестовых данных
y_pred = model.predict(X_test)
```

Рисунок 1. Пример решения обратной задачи с использованием Python

В данном примере используется нейросеть для аппроксимации неизвестной функции. Это демонстрирует, как машинное обучение может использоваться для решения обратных задач, где традиционные методы могут быть сложными или неэффективными.

Таким образом, методы машинного обучения открывают новые перспективы в решении обратных задач, обеспечивая более точные и эффективные алгоритмы для работы с данными. Глубинные нейронные сети, байесовские модели и генеративные алгоритмы позволяют находить

решения даже в условиях нехватки информации или сложной физической природы системы. Однако остается ряд вызовов, таких как необходимость интерпретируемости решений, уменьшение зависимости от больших объемов обучающих данных и учет физических ограничений. Дальнейшее развитие методов МО и их интеграция с традиционными подходами могут привести к новым прорывам в решении обратных задач в самых разных областях науки и техники.

Список использованных источников

1. Гудфеллоу И., Бенджио Й., Курвилл А. «Глубокое обучение». М.: Издательство «МИФ», 2018. – 800 с.
2. Румельхарт Д., Хинтон Г., Вильямс Р. «Обучение представлений методом обратного распространения ошибки». *Cognitive Science*, 2019. – 50(2): 179-221.

ӘОЖ 519.677

Социалова Ұ.Қ. (Алматы, Абай ат. ҚазҰПУ)
Абсамат А.А. (Алматы, Абай ат. ҚазҰПУ)
Токтас Б.Б. (Алматы, Абай ат. ҚазҰПУ)

ЭПИДЕМИОЛОГИЯЛЫҚ АУРУЛАРДЫҢ МАТЕМАТИКАЛЫҚ МОДЕЛЬДЕРІН СТАТИСТИКАЛЫҚ ДЕРЕКТЕР НЕГІЗІНДЕ ТАЛДАУ ЖӘНЕ ОЛАРДЫҢ ЭКОНОМИКАҒА ӘСЕРІ

Эпидемиологиялық аурулардың таралуын модельдеу және оларды статистикалық деректер негізінде талдау қоғам денсаулығын сақтауда маңызды рөл атқарады. Бұл зерттеулер аурулардың алдын алу, экономикалық шығындарды бағалау және тиімді саясат қалыптастыру үшін қажет.

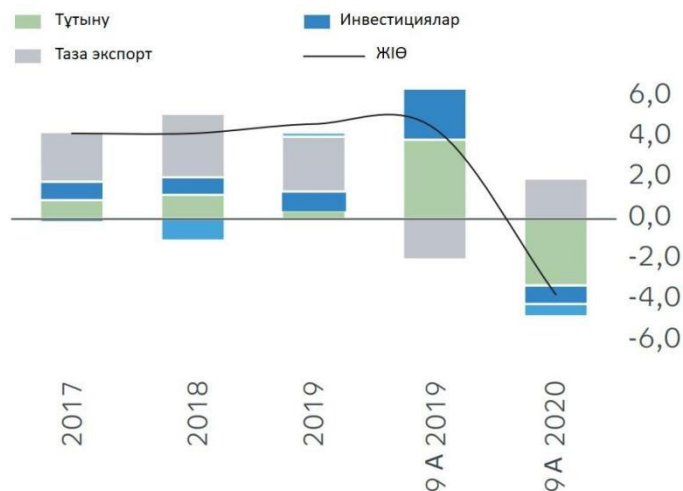
Жұқпалы аурулардың таралуы еңбек нарығына, әлеуметтік жүйеге және оның тұрақтылығына елеулі ықпал етеді, сондай-ақ жалпы ішкі өнімнің (ЖІӨ) динамикасына айтарлықтай әсер етуі мүмкін. Мысалы, COVID-19 пандемиясынан бері бес жыл өткеніне қарамастан, оның салдары жаһандық экономикаға, еңбек нарығына, халықтың әлеуметтік жағдайына және демографиялық үрдістерге айтарлықтай ықпал етті. ХХІ ғасырдағы ең ірі дағдарыстардың бірі ретінде бұл пандемия әлемдік және ұлттық деңгейдегі экономикалық және әлеуметтік құрылымдарға өзгерістер енгізді. Қазақстан да басқа елдер сияқты жұмыссыздықтың артуы, әлеуметтік теңсіздіктің күшеюі және демографиялық құрылымның өзгеруі сияқты мәселелермен бетпе-бет келді [1].

Эпидемиялардың әлеуметтік-экономикалық салдарын тереңірек түсіну үшін математикалық модельдер қолданылады. Мысалы, *SIR* (сезімтал-инфекцияланған-аурудан айыққан) моделі жұқпалы аурулардың таралуын сипаттап, індеттің қарқындылығы мен ұзақтығын бағалауға мүмкіндік береді:

$$\begin{cases} \frac{dS}{dt} = -\beta SI \\ \frac{dI}{dt} = \beta SI - \gamma I \\ \frac{dR}{dt} = \gamma I \end{cases} \quad (1)$$

мұндағы S – сезімтал адамдардың класы, I – инфекцияланғандар класы, R – иммунитетке ие болған аурудан айыққандар класы, β – инфекцияны жұқтыру коэффициенті, γ – аурудан айығу коэффициенті.

Коронавирус пандемиясы және мұнай бағасының құлдырауы Қазақстан экономикасына қос соққы болды, бұл соңғы жиырма жылдағы алғашқы экономикалық белсенділіктің төмендеуіне әкелді [2]. 2020 жылдың қаңтар-қыркүйек айларында нақты ЖІӨ өткен жылдың осы кезеңімен салыстырғанда 2,8 пайызға төмендеді, ал қаңтар-маусым айларында бұл көрсеткіш 1,8 пайызды құраған. Бұл шілде-тамыз айларында енгізілген екінші локдаунның қатаң шараларының әсерін көрсетеді (1-сурет).



1-сурет – Сұраныс компоненттерінің кең көлемді қысқаруы
(үлес, пайызбен)

Экономикалық әсерді бағалау үшін динамикалық макроэкономикалық модельдер қолданылады, олар ЖІӨ-нің төмендеуін, еңбек нарығындағы өзгерістерді және әлеуметтік теңсіздіктің күшеюін болжауға мүмкіндік береді. Жұмыссыздық деңгейінің өзгерісін сипаттау үшін келесі дифференциалдық теңдеулер жүйесі қолданылады:

$$dU/dt = \alpha I - \delta U, \quad (2)$$

мұндағы U – жұмыссыздар саны, δ – індеттің еңбек нарығына әсерін сипаттайтын коэффициент, α – жұмыссыздықтың табиғи төмендеу жылдамдығы [3].

Бұл модельдер пандемияның экономикалық және әлеуметтік салдарын сандық тұрғыдан бағалауға, сондай-ақ тиімді саясаттық шараларды әзірлеуге мүмкіндік береді.

Пайдаланылған дереккөздердің тізімі

1. Сансызбаева Х.Н., Аширбекова Л.Ж., Писула Т., Мусульманкулова А.А. (2022). Пандемияның Қазақстанның әлеуметтік-экономикалық дамуына. Экономика: стратегия және практика, 17(3), 6-21, <https://doi.org/10.51176/1997-9967-2022-3-6-21>.
2. Доклад Об Экономике Казахстана. Декабрь (2020) Долгий Путь К Восстановлению После Кризиса

3. Альжанова Ф.Г., Алибекова Г.Ж. (2022). Демографические Последствия Пандемии Covid-19 В Казахстане. МНПК «Социально-экономическая география в XXI веке: новые реалии и практические возможности». Минск, БГУ, с. 169-171.

УДК 004.92

Сугирбаев А.А (Алматы, КазНУ им. аль-Фараби)
Зиятбекова Г.З. (Алматы, КазНУ им. аль-Фараби;
АТУ)

РАЗРАБОТКА МАШИННОГО ОБУЧЕНИЯ ДЛЯ АНАЛИЗА ДАННЫХ УСТРОЙСТВА МОНИТОРИНГА СТРЕССА

В современном мире проблема стресса становится все более актуальной. Хронический стресс негативно влияет на здоровье человека, повышая риск развития сердечно-сосудистых заболеваний, депрессии и других патологий. В связи с этим возникает потребность в разработке систем мониторинга стресса, способных автоматически анализировать физиологические параметры и определять уровень нагрузки на организм. Целью работы является разработка алгоритмов машинного обучения для обработки и анализа данных, получаемых с устройства мониторинга стресса. Основное внимание уделяется поиску новых подходов к обработке сигналов и построению ансамбля моделей, который позволит повысить точность предсказаний [1].

Описание устройства. В качестве аппаратной платформы используется микроконтроллер ESP32, который обладает встроенным Wi-Fi и возможностью сбора данных с нескольких датчиков (Рисунок 1).



Рисунок 1. Микроконтроллер esp32

Для измерения физиологических параметров применяются три сенсора:

- **Датчик пульса (PulseSensor)** – фиксирует частоту сердечных сокращений (ЧСС);

Пульс-сенсор работает по принципу фотоплетизмографии (PPG). Он использует светодиод, который излучает свет (обычно зеленый или инфракрасный), и фотодиод, измеряющий количество отраженного света. Когда кровь движется по капиллярам под кожей, ее объем периодически изменяется в такт сердечным сокращениям. Эти изменения влияют на количество отраженного света, что фиксируется фотодиодом и преобразуется в аналоговый сигнал. Затем этот сигнал усиливается, фильтруется и передается микроконтроллеру для дальнейшей обработки и анализа (Рисунок 2).



Рисунок 2. Датчик пульса «Pulse sensor»

- **Кожно-гальванический датчик (GSR)** – измеряет электрическое сопротивление; Кожно-гальванический датчик измеряет электрическую проводимость кожи, которая изменяется в ответ на активность потовых желез. Датчик состоит из двух электродов, которые прикладываются к коже и подают слабый электрический ток. При увеличении потоотделения, связанного с эмоциональным или физическим стрессом, сопротивление кожи снижается, а проводимость возрастает. Эти изменения регистрируются датчиком, передаются микроконтроллеру и используются для оценки уровня стресса или эмоционального состояния (Рисунок 3).



Рисунок 3. Кожно-гальванический датчик (GSR)

- **Датчик температуры (DS18B20)** – регистрирует изменение температуры тела. Датчик температуры DS18B20 – это цифровой термометр, который использует технологию 1-Wire для передачи данных. Он имеет встроенный чип для измерения температуры в диапазоне от -55°C до $+125^{\circ}\text{C}$ с точностью $\pm 0.5^{\circ}\text{C}$. DS18B20 можно подключать к микроконтроллерам, таким как ESP32, с использованием всего одного провода для передачи данных, что упрощает его подключение. Он также может работать в многоточечной сети, позволяя подключать несколько датчиков к одной шине. Измерения температуры предоставляются в цифровом формате, что исключает необходимость в аналоговых преобразованиях и делает его удобным для использования в различных проектах мониторинга (Рисунок 4).



Рисунок 4. Датчик температуры DS18B20

Полная схема esp32 с датчиками

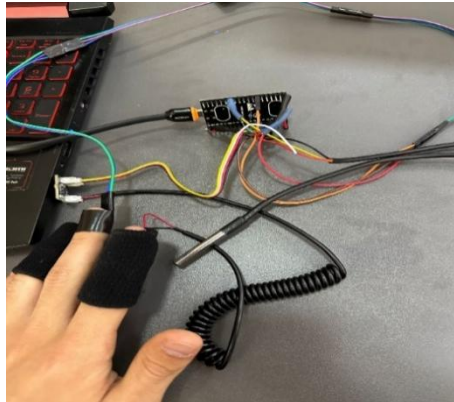


Рисунок 5. Устройство мониторинга стресса

Собранные данные передаются на сервер для дальнейшей обработки и анализа с использованием алгоритмов машинного обучения [2].

Методика обработки данных

Для анализа сигналов будут использоваться следующие этапы:

1. Предварительная обработка – фильтрация шумов, нормализация данных и устранение выбросов.
2. Извлечение признаков – определение ключевых параметров, таких как вариативность ЧСС, уровень кожного сопротивления и динамика изменения температуры.
3. Обучение модели – применение ансамблевых методов машинного обучения для предсказания уровня стресса.
4. Оценка модели – проверка качества предсказаний на тестовой выборке с использованием метрик.

Новизна исследования

Ключевым отличием данной работы является комбинированный подход к анализу данных с использованием ансамблей моделей. В отличие от традиционных методов, в которых применяется одна модель, ансамбли позволяют повысить точность и устойчивость к шумам. Кроме того, разрабатывается новый алгоритм обработки сигналов, включающий адаптивные фильтры и методы временного анализа. Дополнительно рассматривается возможность использования онтологического подхода к интерпретации данных. Это позволит системе не только классифицировать стресс, но и выявлять паттерны, указывающие на возможные причины его возникновения.

Результатом работы станет разработка программно-аппаратного комплекса для мониторинга стресса с использованием ESP32, набора датчиков и серверного анализа данных. Ожидается, что разработанный алгоритм машинного обучения обеспечит более высокую точность классификации стрессовых состояний по сравнению с существующими подходами (Рисунок 5).

Данная работа может найти применение в медицине, спорте, психологии и других областях, требующих мониторинга физиологического состояния человека. В дальнейшем возможна интеграция с мобильными приложениями и облачными сервисами для расширения функционала системы.

Выводы. Разрабатываемая система мониторинга стресса представляет собой комплексное решение, включающее аппаратную часть на основе ESP32 и интеллектуальную обработку данных с применением машинного обучения. Внедрение ансамблей моделей позволит повысить точность детекции стрессовых состояний, что может быть полезно в медицинской диагностике, спортивной

аналитике и психофизиологических исследованиях. В дальнейшем планируется расширение набора входных данных и тестирование алгоритмов на реальных пользователях для повышения достоверности и практической применимости системы.

Литература

1. Vos G., Trinh K., Sarnyai Z., Rahimi Azghadi M. "Generalizable machine learning for stress monitoring from wearable devices: A systematic literature review." *International Journal of Medical Informatics*, 2023 May;173:105026.
<https://www.sciencedirect.com/science/article/pii/S1386505623000436>
2. Vos G., Trinh K., Sarnyai Z., Rahimi Azghadi M. "Generalizable machine learning for stress monitoring from wearable devices: A systematic literature review." *International Journal of Medical Informatics*, 2023 May;173:105026.
https://www.researchgate.net/publication/364110268_Machine_Learning_for_Stress_Monitoring_from_Wearable_Devices_A_Systematic_Literature_Review
3. Gour S., Vinoth Kumar C.V. "Machine learning methods for stress monitoring using wearable devices." *International Conference on Artificial Intelligence and Signal Processing (AISP)*, 2022.
<https://ieeexplore.ieee.org/document/9752111>

УДКД 517.977.8

Суяров Т.Р. (Институт Математики имени В.И. Романовского Академии наук Республики Узбекистан, Узбекистан, г. Ташкент)

ЗАДАЧА С ОБРАТНЫМ КОЭФФИЦИЕНТОМ ДЛЯ ОДНОМЕРНОГО ДРОБНОГО ВОЛНОВОГО УРАВНЕНИЯ С НЕЛОКАЛЬНЫМИ НАЧАЛЬНО-КРАЕВЫМИ УСЛОВИЯМИ

В данной работе исследуются прямые и обратные задачи для временного дробного волнового уравнения с дробным дифференциальным оператором Римана-Лиувилля. В прямой задаче рассматривается начально-краевая задача для этого уравнения с нелокальными граничными условиями типа Ионкина. В обратной задаче требуется зависящий от времени коэффициент с условием интегральной переопределённости. Существование и единственность решения затем доказываются с помощью теоремы Банаха о неподвижной точке.

В области $\Omega = \{(x, t) \mid 0 < x < 1, 0 < t \leq T\}$, мы рассматриваем одномерное волновое уравнение с дробными производными:

$$(D_{0+,t}^\alpha u)(x, t) - u_{xx} + q(t)u(x, t) = f(x, t), (x, t) \in \Omega, \quad (1)$$

с начальными условиями

$$I_{0+,t}^{(2-\alpha)} u(x, t) \Big|_{t=0} = \varphi(x), \quad 0 \leq x \leq 1, \quad (2)$$

$$\frac{\partial}{\partial t} \left(I_{0+,t}^{(2-\alpha)} u \right) (x, t) \Big|_{t=0} = \psi(x), \quad 0 \leq x \leq 1, \quad (3)$$

и нелокальные граничные условия

$$u_x(0, t) = u_x(1, t), u(0, t) = 0, 0 \leq t \leq T, \quad (4)$$

где $\varphi(x), \psi(x)$ и $f(x, t)$ - заданные функции, дробная производная Римана-Лиувилля $D_{0+,t}^\alpha$ порядка $1 < \alpha \leq 2$ определяется ([1] см. 69-72)

$$(D_{0+,t}^\alpha f)(t) := \frac{d^2}{dt^2} (I_{0+,t}^{2-\alpha} f)(t) = \frac{1}{\Gamma(2-\alpha)} \frac{d^2}{dt^2} \int_0^t \frac{f(\tau) d\tau}{(t-\tau)^{\alpha-1}}, t > 0,$$

является дробным интегралом Римана-Лиувилля функции $f(t)$ относительно t , $\Gamma(\cdot)$ является гамма-функцией Эйлера.

В прямой задаче требуется найти функцию $u(x, t) \in C_{\gamma}^{2,\alpha}(\bar{\Omega})$ удовлетворяющую равенствам (1)-(4) с данными функциями $q(t), f(x, t), \varphi(x), \psi(x)$, где $2 - \alpha < \gamma < 1, \bar{\Omega} = \{(x, t): 0 \leq x \leq 1, 0 \leq t \leq T\}$.

Определение 1. Функция $u(x, t)$ называется классическим решением начальной краевой задачи (1)-(4), если:

1. $\{t^\gamma u, t^\gamma u_x, t^\gamma u_{xx}, t^\gamma D_{0+,t}^\alpha u\} \in C(\bar{\Omega})$;
2. $u(x, t)$ удовлетворяет (1)-(4) в Ω .

В данной работе мы изучаем следующую **обратную задачу**: нахождение коэффициента $q(t) \in C([0, T])$, если для решения прямой задачи (1)-(4) известно условие интегральной переопределённости:

$$\int_0^1 \omega(x) u(x, t) dx = h(t), t \in [0, T], \quad (5)$$

где $h(t), \omega(x)$ - достаточно гладкие функции.

Относительно заданных функций будем предполагать выполненными следующие условия:

A1) $\varphi(x) \in C^3[0, 1], \varphi^{(4)}(x) \in L_2(0, 1); \varphi(0) = \varphi(1) = 0, \varphi'(0) = 0, \varphi''(0) = \varphi''(1) = 0$,

A2) $\psi(x) \in C^3[0, 1], \psi^{(4)}(x) \in L_2(0, 1); \psi(0) = \psi(1) = 0, \psi'(0) = 0, \psi''(0) = \psi''(1) = 0$,

A3) $f(x, \cdot) \in C_\gamma[0, T], f(\cdot, t) \in C^3[0, 1], f^{(4)}(\cdot, t) \in L_2(0, 1), f(0, t) = f(1, t) = 0, f_x(0, t) = 0, f_{xx}(0, t) = f_{xx}(1, t) = 0$,

A4) $\omega(x) \in C^2[0, 1]; \omega(1) = \omega(0), \omega'(0) = 0$,

A5) $(D_{0+,t}^\alpha h)(t) \in C_\gamma[0, T], h(t) \in C_\gamma^\alpha[0, T], |t^\gamma h(t)| \geq h_0 > 0, t \in [0, T]$ является заданным числом:

$$\int_0^1 \omega(x) \varphi(x) dx = (I_{0+,t}^{(2-\alpha)} h)(t)_{t=0+}, \int_0^1 \omega(x) \psi(x) dx = \frac{\partial}{\partial t} (I_{0+,t}^{(2-\alpha)} h)(t)_{t=0+}.$$

Теорема 1. Пусть выполнены условия A1)-A3) и $q(t) \in C[0, T]$, то существует единственное решение $u(x, t) \in C_{\gamma}^{2,\alpha}(\bar{\Omega})$ для прямой задачи (1)-(4).

Теорема 2. Пусть A1) -A5) выполняется. Тогда существует число $T^* \in (0, T)$ такое, что существует единственное решение $q(t) \in C[0, T^*]$ обратной задачи (1)-(5).

ЛИТЕРАТУРА

[1] Kilbas, A. A. and Srivastava, H. M. and Trujillo, J. J. *Theory and Application of Fractional Differential Equations // Part of North-Holland Mathematical Studies. Amsterdam. Elsevier. 2006.*

УДК 004.89

Такуаина А.И. (Караганда, КМУ)
Шафеев Д.Е. (Караганда, КМУ)

ОБРАТНЫЕ ЗАДАЧИ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В СОЗДАНИИ AI-АССИСТЕНТА

Введение

В современном мире автоматизация процессов становится неотъемлемой частью эффективного управления информацией. Существует множество программных систем интеллектуального анализа данных [1]. Одним из ярких примеров является использование искусственного интеллекта (ИИ) для создания интеллектуальных помощников, которые облегчают взаимодействие между пользователями и информационными системами. В данной статье рассматривается проект AI-ассистента, разработанного для приёмной комиссии университета, а также затрагивается тема обратных задач, связанных с обработкой данных и оптимизацией обучения модели.

Основная часть

AI-ассистент был создан для автоматизации процессов общения между абитуриентами и приёмной комиссией через популярный мессенджер Telegram. Основные задачи системы включают:

- Предоставление оперативных ответов на типовые вопросы абитуриентов;
- Поиск конкретных данных (например, расположение корпусов или условия проживания);
- Интеграция с существующими информационными системами университета;
- Гибкость базы знаний и возможность дообучения модели.

Обратные задачи и их применение

С появлением мощных компьютеров интерес к обратным и некорректным задачам стал стремительно расти. При обобщении понятия обратной задачи, поскольку и сам закон (уравнение) неизвестен, требуется по результатам опытов (наблюдений) установить закон (уравнение). И эти обратные задачи связаны с задачами, решаемыми с помощью алгоритмов искусственного интеллекта [2]. Одним из ключевых аспектов разработки AI-ассистента является решение обратных задач, связанных с обработкой запросов пользователей и формированием корректных ответов. Обратные задачи в данной области включают:

1. Распознавание намерений (Intent Recognition): Поиск оптимальных параметров модели для точного определения запроса пользователя на основе предоставленных данных.
2. Навигационная поддержка: Использование модели Deepseek R1 для предсказания местоположений с высокой точностью, что также требует решения задач оптимизации.
3. Дообучение модели: Модификация параметров и структуры модели для повышения её точности и адаптации к новым запросам.

Применение искусственного интеллекта

В статье [3] отмечается, что наибольших практических успехов удалось достигнуть, используя методы, которые в принципе не свойственны человеку, а основаны на использовании «грубой вычислительной силы», или, другими словами, возможности быстрого перебора различных вариантов решений с помощью высокопроизводительных компьютеров. Такой подход лежит в

основе практически всех разработок с применением ИИ. Однако, если говорить об образовании, важно сбалансировать автоматизацию и персонализацию с человеческими аспектами [4].

ИИ в данном проекте реализован через использование платформы RASA с библиотеками TensorFlow, PyTorch и transformers. Применение методов машинного обучения позволяет:

- Обрабатывать естественный язык (Natural Language Processing, NLP);
- Моделировать диалоговые системы и обеспечивать адекватные ответы на запросы пользователей;
- Повышать точность предсказания намерений и предложений благодаря адаптивному обучению.

Точность работы

— NLU: 88% (F1-score) на валидационной выборке, достигнуто благодаря использованию DIET в RASA и предварительной обработки данных с помощью nltk и numpy.

— Core: 85% точности выбора действий в диалогах, обеспечивая корректное реагирование на запросы пользователей.

Deepseek R1: 92% точности предсказания местоположений, оптимизировано для компактного набора данных с использованием PyTorch и numpy.

Заключение

На разработанную программу с использованием Python (версии 3.9.) «AI-ассистент приемной комиссии университета» получено авторское право под №55465 от 5 марта 2025 года. AI-ассистент демонстрирует высокую точность в распознавании запросов пользователей и предоставлении информации. Интеграция технологий машинного обучения и решения обратных задач позволяет создавать эффективные и адаптивные системы, способные улучшать качество предоставляемых услуг. Дальнейшее развитие проекта предполагает совершенствование алгоритмов и расширение базы знаний.

Список использованных источников

1. Журавлев Ю. И., Рязанов В. В., Сенько О. В. Распознавание. Математические методы. Программная система. Практические применения. М.: Фазис; 2006. 147 с.
2. Кабанихин С.И. "Обратные задачи и искусственный интеллект" // Успехи кибернетики. 2021. Т. 2. № 3. С. 33-43.
3. Каляев И., Заборовский В. Искусственный интеллект: от метафоры к техническим решениям. Control Engineering Россия. 2019;5(83):26–31. Режим доступа: <https://controleng.ru/wp-content/uploads/8326.pdf>.
4. Ghazaryan A. "Искусственный интеллект в процессах образования и обучения, положительные и отрицательные стороны" // International Journal of Natural Sciences. 2023. Т. 11-2(86). С. 214-216.

УДК 004.942

Татур М.М., Крюков А.И.,
Чэнь Цз., Каранкевич В.Г. (Минск, БГУИР)

ОБУЧЕНИЕ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ПРИНЯТИЯ РЕШЕНИЙ КАК ОБРАТНАЯ ЗАДАЧА ВЫБОРА ПАРАМЕТРОВ МОДЕЛИ

В самом общем виде принятие решений состоит из двух этапов: первый – построение модели F принятия решений $Y=F(X,W)$ в соответствии с прикладной задачей и второй, – собственно, принятие решений по входным данным X . В теории машинного обучения для построения модели F используют различные «унифицированные» математические методы, начиная от классических методов интеллектуального анализа данных (Data Mining) до искусственных нейронных сетей (ANN). При правильном выборе математического метода и посредством настройки параметров W модели F можно достичь приемлемое качество принятия решений, Рис.1. В данной постановке первый этап является *обратной задачей*, а второй этап – *прямой задачей*.

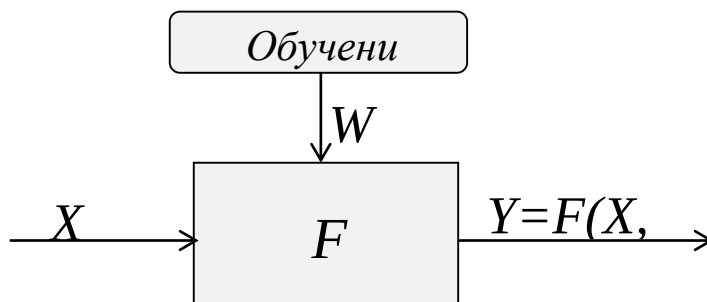


Рисунок 1. – Обобщенная модель принятия решений

Часто, в узкой трактовке, параметры W рассматривают как веса нейронной сети, а процесс вычисления весов – как *обучением нейронной сети*. Гораздо реже параметры W рассматривают как веса вектора информативных признаков X интеллектуального анализа данных. Общепринято считать, что веса признаков (параметры) W , ключевым образом влияют на принимаемые решения. Однако, при более глубоком рассмотрении вопросов влияния весов на принимаемые решения можно заметить существенные различия в механизмах такого влияния. Исследование вопросов влияния весов на принимаемые решения позволяет более обоснованно выбирать модели и интерпретировать результаты интеллектуального анализа данных.

План исследования состоял в следующем. Задана последовательность образов или объектов (Data Set), представленных в виде двумерного вектора количественных информативных признаков. Число и распределение образов могут быть выбраны случайно. Мерность пространства 2 – для простоты расчетов и наглядного анализа результатов исследования. Принятие решения может трактоваться как присвоение метки класса, или кластера в результате алгоритмов классификации, или кластеризации, соответственно. Также «принятие решения» может трактоваться как сравнение двух образов в соответствии с некоторой функцией ранжирования. В ходе проведения исследования решались задачи классификации, кластеризации и ранжирования при различных весовых коэффициентах, различными методами. Образы были индексированы и фиксировались факты изменения меток классов, кластеров либо ранга каждого образа, что свидетельствовало о влиянии изменения веса на принятие решения.

По результатам исследования были сделаны следующие выводы.

В методах классификации, основанных на построении разделяющей или дискриминантной функции, при изменении весов информативных признаков (масштабировании распределения образов) соответствующим образом изменяется положение дискриминантной функции в признаковом пространстве. Поэтому, на результаты классификации (или принятия решений) изменение весов признаков не оказывает.

В методах классификации, основанных на сравнении расстояний между образами, а также в методах кластеризации, на изменение принятия решений оказывает распределение образов, используемая метрика, а также – мерность пространства признаков. Эта зависимость может оказаться достаточно сложной, но очевидно, что наиболее подверженными к изменению решения оказываются образы, находящиеся близко друг к другу в заданной метрике.

При ранжировании, изменение весов информативных признаков наиболее явно влияет на принятие решений, поскольку функции ранжирования, как правило, отражают предметную область и не связаны с формальными метриками оценки расстояний между образами.

Особое место в настоящем исследовании занимают ANN. Безусловно, веса W (обучение ANN) играют ключевую роль в принятии решений, и при этом ANN воспроизводит разделяющую функцию (в задачах классификации). Здесь нет никакого парадокса. В ANN веса нейронов не отражают взаимное (пропорциональное) влияние признаков на принятие решения, т.е. это означает, что настройки W у ANN являются не интерпретируемыми.

Обучение интеллектуальной системы, как решение обратной задачи, связано с большими вычислительными затратами, с наличием различных инвариантов, не гарантирующих оптимального решения. Принимая во внимание, что для каждой модели F будут характерны свои, уникальные сложности в вычислении или подборе параметров W , то это означает актуальность продолжения исследований в данной области для молодых (и не только) специалистов в области DataScience.

УДК 519.62/.64

Темирбеков А.Н. (Алматы, КазНУ им. Аль-Фараби)

Тұрлыбек Ж.Ғ. (Алматы, КазНУ им. Аль-Фараби)

Касенов С.Е. (Алматы, КазНУ им. Аль-Фараби)

ЧИСЛЕННОЕ МОДЕЛИРОВАНИЕ РАСПРОСТРАНЕНИЯ ВРЕДНЫХ ПРИМЕСЕЙ В АТМОСФЕРЕ С PINN

Методология исследования

Перемещение загрязняющих веществ в атмосфере осуществляется воздушными потоками с учетом их локальных колебаний. Средний поток веществ, переносимых воздушными массами, как правило, включает адвективные и конвективные составляющие. В процессе движения примесей основная усредненная динамика дополняется диффузией, вызванной случайными колебаниями частиц.

Постановка задачи для уравнения переноса загрязняющих веществ в области:

$$\omega = \{x, z, t; 0 \leq x \leq 1, 0 \leq y \leq 1, 0 \leq t \leq T\}$$

$$q \frac{\partial t}{\partial t} + u q \frac{\partial x}{\partial x} + v q \frac{\partial y}{\partial y} = \Delta q + q q + q + f q \quad (1)$$

$$q x, y, 0 = 0 x, y, \quad (2)$$

$$q_0, y, t=0, q_1, y, t=0 \quad (3)$$

$$q_x, 0, t=0, q_x, 1, t=0 \quad (4)$$

Здесь $f_q = j=1mQ_j\delta(r-r_j)$ представляет собой радиус-вектор расположения источников загрязнения, мощность источников загрязнения, число источников.

где

u, v – коэффициенты скорости воздушного потока,

q – концентрация вредного вещества в смеси,

q – коэффициент скорости образования вещества,

q – коэффициент уменьшения скорости,

x, y, t – интенсивность аэрозольной субстанции, переносимой воздушным потоком в атмосфере.

Численные методы решения дифференциальных уравнений на протяжении многих десятилетий играли ключевую роль в математическом моделировании сложных физических процессов. Однако с развитием вычислительных технологий и методов искусственного интеллекта появились новые подходы, позволяющие повысить точность и эффективность расчетов. Одним из таких методов является Physics-Informed Neural Networks (PINN) — нейросетевой подход, в котором физические законы интегрируются в структуру модели, обеспечивая согласованность с фундаментальными уравнениями.

Метод PINN основан на глубокой нейронной сети, обучаемой с учетом физических уравнений путем включения их в функцию потерь. Такой подход позволяет не только приближать решения дифференциальных уравнений, но и эффективно справляться с обратными задачами, реконструируя неизвестные параметры системы по ограниченному набору наблюдаемых данных. В данной работе рассматривается применение PINN для решения обратной задачи уравнения переноса и диффузии, описывающего распространение вредных примесей в атмосфере. Использование данного метода позволяет восстанавливать недостающую информацию о динамике загрязняющих веществ, учитывая сложные физические процессы, включая адвекцию, диффузию и химические реакции в атмосфере.

$$L = LPDE + LBC + LIC \quad (5)$$

где

$LPDE$ – ошибка уравнения в частных производных,

LBC, LIC – ошибки на начальных и граничных условиях.

Функция потерь в PINN формулируется как среднеквадратичная ошибка, что позволяет минимизировать невязку уравнения в частных производных в случайно выбранных точках внутри области.

$$LPDE = 1/N_i = 1/NF(u_{xi}, y_i, t_i) \quad (6)$$

где

u_{xi}, y_i, t_i – предсказанное значение решения нейросетью с параметрами θ ,

L_u – оператор уравнения в частных производных.

PINN представляет собой многослойную нейронную сеть, где входными параметрами являются пространственные и временные координаты, а выходные значения аппроксимируют решение заданного дифференциального уравнения. Архитектура PINN включает в себя слои нелинейных преобразований, обучаемые таким образом, чтобы удовлетворять физическим законам, заданным уравнениями переноса и диффузии.

Для построения математической модели на основе PINN используется программная реализация, основанная на современных фреймворках глубокого обучения. В работе применяется библиотека DeepXDE, обеспечивающая удобный интерфейс для численного решения

дифференциальных уравнений с использованием PINN. Данный подход позволяет эффективно решать как прямые, так и обратные задачи, восстанавливая неизвестные параметры модели на основе ограниченного набора данных.

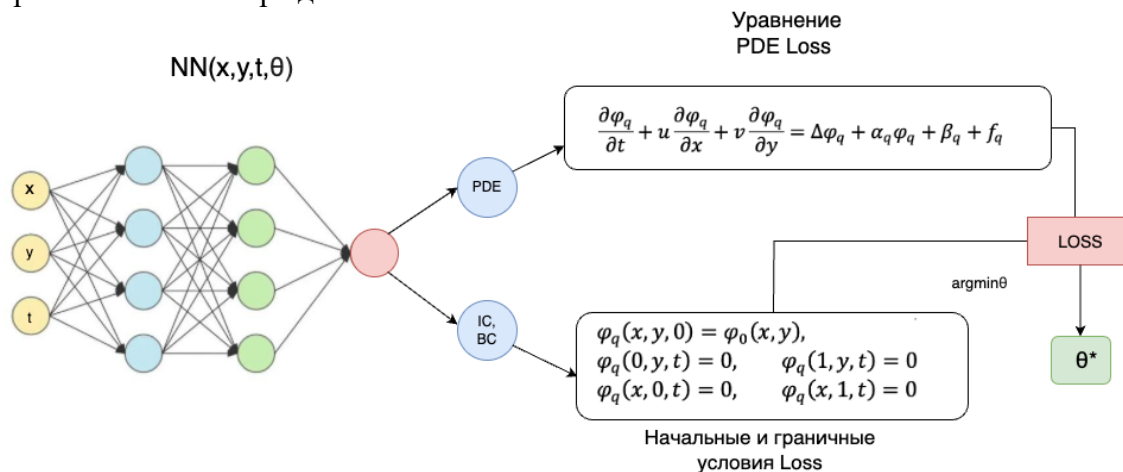


Рисунок 1. Архитектура PINN для уравнения переноса и диффузии

Благодарность

Данное исследование финансировалось Комитетом науки Министерства науки и высшего образования Республики Казахстан (грант № AP19579325 «Разработка и исследование современных численных методов решения обратных и некорректных задач для уравнения акустики»)

Список использованных источников

1. Марчук Г.И. Математическое моделирование в проблеме окружающей среды. М.: Наука., 1982.-320 с.
2. Temirbekov N., Temirbekov A., Kasenov S., Tamabay D. (2024) Numerical modeling for enhanced pollutant transport prediction in industrial atmospheric air // Journal of Sustainable Development and Environmental Engineering. Vol. 19, No. 3, 917–926. <https://doi.org/10.18280/ij dne.190321>
3. Askerbekova, J., Kasenov, S., Temirbekov, A., and Tleulesova, A. Numerical solution of the continuation problem for the one-dimensional acoustics equation //AIP Conference Proceedings. – AIP Publishing, 2023. – T. 2879. – №. 1. <https://doi.org/10.1063/5.0175240>

УДК 004.89

Темиржан С. А. (Астана, ЕНУ)
 Онгарбаева А. И.(Астана, ЕНУ)

ИСПОЛЬЗОВАНИЕ НЕЙРОННЫХ СЕТЕЙ В СТЕГОАНАЛИЗЕ ИЗОБРАЖЕНИЙ

Стеганография представляет собой метод сокрытия информации в передаваемых данных таким образом, чтобы сам факт встраивания оставался незаметным. Однако с развитием методов стеганографии развивается и противоположное направление — стегоанализ, задача которого заключается в выявлении скрытых данных и обнаружении факта их встраивания. Эти два направления находятся в постоянной конкуренции: в то время как исследователи разрабатывают

новые алгоритмы сокрытия информации, совершенствуются и методы её обнаружения. В настоящий момент существует более 100 различных стеганографических программных пакетов, большая часть которых ориентирована на анализ изображений [1].

Одним из наиболее сложных и востребованных направлений стегоанализа является разработка универсальных (слепых) методов, способных выявлять скрытые данные независимо от конкретного алгоритма стеганографии. Такие методы позволяют выработать оптимальный алгоритм, для представление является ли переданное сообщение стегоконтейнером[2].

В данной работе рассматриваются современные подходы к стегоанализу, основанные на методах глубокого обучения. В частности, анализируются нейросетевые модели, обученные на пространственных представлениях изображений, для выявления скрытых данных, встроенных с использованием метода замены наименее значащих битов (LSB). В качестве основы для экспериментов используется нейросетевая архитектура EfficientNet, обученная на датасете ALASKA2.

Методы стегоанализа можно разделить на два вида - первое классические и второе которое рассматривается в этой работе это - современные.

К современным методам стегоанализа относятся методы стегоанализа на основе нейросетей. С развитием технологий глубокого обучения стегоанализ получил новое направление, основанное на применении сверточных нейросетей (CNN), рекуррентных нейросетей (RNN) и их комбинаций. Данные методы позволяют автоматически извлекать сложные признаки из изображений, не требуя ручного проектирования характеристических векторов.

При применении методов глубокого обучения стегоанализ сводится к задаче бинарной классификации, где модель обучается различать изображения, содержащие скрытые данные (ЦВЗ, сообщения), и чистые контейнеры. В большинстве исследований основное внимание уделяется стегоанализу изображений, а в качестве инструмента используются свёрточные нейронные сети (CNN) с различными модификациями и улучшениями. Детальный обзор современных подходов к этому направлению представлен в работе [3].

Современные методы стегоанализа всё чаще используют глубокие нейронные сети, поскольку они способны автоматически извлекать сложные признаки изображений, которые трудно выявить классическими методами. Глубокие модели позволяют анализировать пространственные и частотные характеристики изображений, выявляя малозаметные изменения, вносимые стеганографическими алгоритмами.

EfficientNet — это сверточная нейронная архитектура, которая использует метод масштабирования для равномерного увеличения глубины, ширины и разрешения изображения. В отличие от традиционного подхода, где эти параметры изменяются произвольно, EfficientNet применяет составной коэффициент, позволяющий сбалансировано масштабировать все три параметра.

На рис 2. представлено сравнение различных архитектур нейросетей по числу параметров (в миллионах) и их точности на датасете ImageNet[6].

Этот график демонстрирует эффективность архитектуры EfficientNet, которая достигает высокой точности при значительно меньшем количестве параметров по сравнению с традиционными моделями.

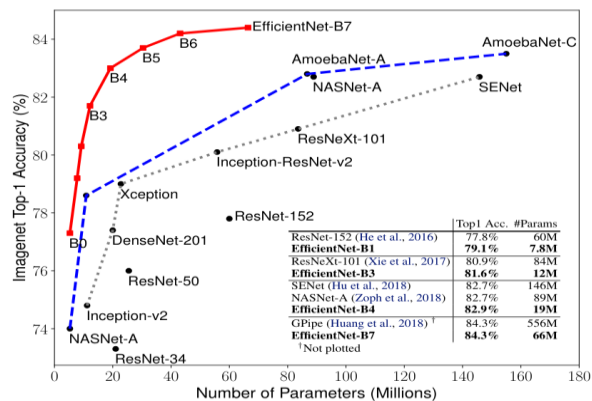


Рис 2. сравнительный график зависимости точности разных моделей от количества параметров.

В качестве основы исследуемого датасета цифровых изображений был выбран ALASKA2 Image Steganalysis. Так как EfficientNet было обучена по этому датасету. Этот набор данных включает как исходные (чистые) контейнеры, так и изображения, содержащие скрытые данные, встроенные с помощью стеганографических алгоритмов JMiPOD, JUNIWARD и UERD. Данные классы сбалансированы, каждый из них содержит по 75 000 изображений размером 512×512 пикселей. Дополнительно, на основе чистых изображений из ALASKA2 был создан новый класс контейнеров, содержащих скрытые данные, внедренные с использованием метода замены наименее значащих битов (LSB). Это позволило расширить исследуемую область и оценить эффективность методов стеганоанализа в выявлении LSB-стеганографии.

В этой работе показано [4] использование пред обученной модели EfficientNet-b3 для классификации стегоконтейнеров. EfficientNet-b3 дополнительно было обучена на датасете ImageNet по методу Noisy Student. В таблице 2 показаны результаты обученной модели по подготовленному датасету.

Таблица 1. Результаты классификации стеганографических контейнеров в виде цифровых изображений

Тип стеганографического преобразования	Точность (training) %	Точность (testing) %
Пространственный метод стеганографии	98,5	97,1
Частотные методы стеганографии	63,05	62,1

Результаты экспериментов демонстрируют, что архитектура EfficientNet-B3 эффективно классифицирует стеганографические контейнеры, созданные с использованием пространственного метода LSB, успешно различая пустые и заполненные изображения. При этом на вход нейросети подается исходное изображение без дополнительной обработки.

В данной работе рассмотрены современные методы стеганоанализа изображений, основанные на применении нейросетей, в частности архитектуры EfficientNet-B3. Проведённые эксперименты показали, что данная модель эффективно выявляет скрытые данные, встроенные методом LSB, достигая высокой точности классификации (97,1% на тестовой выборке). Однако для частотных методов стеганографии (JMiPOD, JUNIWARD, UERD) результаты оказались значительно хуже

(62,1%), что связано с особенностями внедрения скрытой информации в частотные компоненты изображений.

Таким образом, применение сверточных нейросетей в стеганоанализе перспективно, но эффективность модели зависит от метода стеганографии. Будущие исследования могут быть направлены на улучшение детекции частотных методов внедрения информации, а также на разработку гибридных моделей, сочетающих пространственные и частотные признаки изображений.

Список использованных источников

1. Стегоанализ цифровых изображений с использованием методов поверхностного и глубокого машинного обучения: известные подходы и новые решения. 2021. А. А. Сирота, М. А. Дрюченко, А. Ю. Иванков
2. Коржик В.И., Красов А.В. Цифровая стеганография. КноРус. 2023. 89 с.[t](#)
3. Tabares-Soto, R. Deep Learning Applied to Steganalysis of Digital Images: A Systematic Review / Reinel Tabares-Soto, Raúl Ramos-Pollán, Gustavo Isaza // Computer Science IEEE Access. – 2019. – DOI:10.1109/ACCESS.2019.2918086.
4. Интеллектуальное обнаружение стеганографического преобразования изображений, основанное на классификации контейнеров И.В. Аникин, А.В. Ягина

УДК 519.62/.64

А.М. Тлеулесова (Алматы, КазНУ им. Аль-Фараби)
М.Н. Даулетбай (Шымкент, ЮКГУ им. М.О. Ауэзова)

ЧИСЛЕННОЕ РЕШЕНИЕ ЗАДАЧИ ПРОДОЛЖЕНИЯ ДЛЯ УРАВНЕНИЯ МАКСВЕЛЛА

Введение

Задача продолжения для уравнений Максвелла представляет собой важную проблему математической физики, тесно связанную с электродинамикой и распространением электромагнитных волн. Эти уравнения лежат в основе теории электромагнитного поля и находят широкое применение в различных областях науки и техники — от радиофизики до медицинской визуализации и геофизических исследований. Решение задачи продолжения позволяет глубже понять и смоделировать процессы распространения электромагнитных волн, что имеет большое значение в прикладных задачах различной природы.

Известно, что задача Коши для уравнений Максвелла является существенно некорректной: малейшие изменения в данных Коши могут вызывать значительные отклонения в решении [1]. Это делает невозможным применение стандартных численных методов и требует использования специальных подходов, таких как методы регуляризации.

Постановка задачи продолжения.

Исходная задача продолжения для уравнения Максвелла в области $\Omega = [0, h] \times [0, L] \times [0, T]$ имеет следующий вид:

$$\mu \epsilon z, y, t + \mu \sigma z, y, t = u_{zz} + u_{yy}, \quad z, y, t \quad (1)$$

$$u_{z,y}, 0 = 0, \quad u_{t,z,y}, 0 = 0 \quad z_0, h, y \in 0, L_y \quad (2)$$

$$u_{z,0}, t = 0, \quad u_{z,L_y}, t = 0 \quad z_0, h, t_0, T \quad (3)$$

$$u_{z,0,y}, t = g(y, t), \quad u(0, y, t) = f(y, t) \quad y \in 0, L_y, t_0, T \quad (4)$$

Задача заключается в продолжении решения $u_{z,y,t}$ уравнения (1) в области .

Прямая и обратная задача

Задача продолжения для уравнения Максвелла представляет собой некорректную задачу, что значительно усложняет её численное решение. Одним из действенных подходов к преодолению этой трудности является приведение задачи продолжения к граничной обратной задаче. Такой подход позволяет применить развитые численные методы обратных задач для получения устойчивого приближённого решения. Рассмотрим некорректную задачу (1)-(4) как обратную к следующей прямой (корректной) задаче: в области требуется определить $u_{z,y,t}$ по заданным $z, y, z, y, q(y, t)$ и $g(y, t)$ из соотношений:

$$\mu \epsilon z, y, t + \mu \sigma z, y, t = u_{zz} + u_{yy}, \quad z, y, t \quad (5)$$

$$u_{z,y}, 0 = 0, \quad u_{t,z,y}, 0 = 0 \quad z_0, h, y \in 0, L_y \quad (6)$$

$$u_{z,0}, t = 0, \quad u_{z,L_y}, t = 0 \quad z_0, h, t_0, T \quad (7)$$

$$u_{z,0,y}, t = g(y, t), \quad u_{h,y}, t = q(y, t) \quad y \in 0, L_y, t_0, T \quad (8)$$

В прямой задаче требуется найти $u_{z,y,t}$ по заданным функциям $q(y, t)$. В обратной задаче необходимо найти $q(y, t)$ из соотношении (5)-(8) с учетом дополнительной информации

$$u(0, y, t) = f(y, t), \quad y \in 0, L_y, t_0, T. \quad (9)$$

Прямая задача для уравнений Максвелла состоит в нахождении решения при заданных граничных и физических параметрах. Корректность этой задачи имеет важное значение для практического моделирования электромагнитных процессов.

Формулировка и решение задачи оптимизации.

Далее изучается формулировка обратной задачи в операторной форме, а также представление оптимизационной задачи, решаемой с использованием градиентного метода.

Оператор A определяется следующим виде:

$$A: u_{h,y}, t = q(y, t) \mapsto u(0, y, t) = f(y, t)$$

где $u(x, y, t)$ решение прямой задачи (1)-(4) записывается в операторной форме

$$Aq = f \quad (10)$$

Операторное уравнение (11) преобразуется в задачу оптимизации, и мы минимизируем функционал

$$J_{qn} = \|Aq_n - f\|_2^2 = \int_0^{T_0} \int_0^{L_y} (q_n - f)^2 dy dt \quad (11)$$

градиентном методом

$$q_{n+1} = q_n - \alpha J' q_n \quad (12)$$

где α - параметр спуска.

Благодарность

Данное исследование финансировалось Комитетом науки Министерства науки и высшего образования Республики Казахстан (грант № AP19579325 «Разработка и исследование современных численных методов решения обратных и некорректных задач для уравнения акустики»)

Список использованных источников

1. Kasenov, S. E., Tleulesova, A. M., Sarsenbayeva, A. E., and Temirbekov, A. N. Numerical Solution of the Cauchy Problem for the Helmholtz Equation Using Nesterov's Accelerated Method //Mathematics (2227-7390). – 2024. – Т. 12. – №. 17. <https://doi.org/10.3390/math12172618>
2. Kasenov S., Nurseitova A., Nurseitov D. A conditional stability estimate of continuation problem for the Helmholtz equation. AIP Conference Proceedings. AIP Publishing **2016** 1759.1. <https://doi.org/10.1063/1.4959733> Askerbekova, J., Kasenov, S., Temirbekov, A., and Tleulesova, A. Numerical solution of the continuation problem for the one-dimensional acoustics equation //AIP Conference Proceedings. – AIP Publishing, 2023. – Т. 2879. – №. 1. <https://doi.org/10.1063/5.0175240>

УДК004.4:658.5

Токтабаев А.М.

(Алматы, КазНУ им. аль-Фараби)

Ахметова А.М., PhD, ст. преп.

(Алматы, КазНУ им. аль-Фараби)

ИНТЕГРАЦИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И ТЕХНОЛОГИЙ ИНТЕРНЕТА ВЕЩЕЙ В МОНИТОРИНГ ЯГОД НА ОСНОВЕ БАЙЕСОВСКИХ МОДЕЛЕЙ

Абстракт. В статье описана разработка недорогой системы мониторинга и диагностики ягодных культур с применением искусственного интеллекта (ИИ), технологий Интернета вещей (IoT) и байесовских сетевых моделей (БСМ). Система базируется на микроконтроллере Luckfox Pico Max RV1106, включает датчики, светодиодные лампы и базу данных для анализа состояния почвы, здоровья растений и затрат. ИИ прогнозирует урожайность, а БСМ оценивает риски заболеваний. Результаты тестирования подтверждают точность и доступность решения для малых хозяйств и образовательных целей.

Введение. Сельское хозяйство сталкивается с вызовами, такими как изменение климата и ограниченность ресурсов, что требует внедрения цифровых технологий. Ягодные культуры, например, клубника, являются высокодоходными, но чувствительными к условиям выращивания, что подчеркивает важность точного мониторинга. Настоящая работа представляет систему, использующую ИИ, IoT и байесовские сети для диагностики и управления выращиванием ягод. Основная цель — создание доступного инструмента на базе микроконтроллера Luckfox Pico Max RV1106, датчиков и открытого ПО. В статье рассмотрены методология, результаты и перспективы разработки [1].

1. Теоретические основы. Современные технологии, такие как ИИ и IoT, трансформируют сельское хозяйство. ИИ позволяет анализировать данные для прогнозирования урожайности и выявления болезней, например, серой гнили у ягод (Wolfert et al., 2017). IoT обеспечивает сбор данных в реальном времени через датчики, снижая потери урожая на 15–20% (Vasisht et al., 2017). Байесовские сети, как вероятностные модели, эффективны для диагностики состояния растений при неопределенности (Shepherd et al., 2018). В отличие от дорогих коммерческих систем, таких как FarmBeats, наша разработка ориентирована на локальную обработку данных и низкую стоимость, что делает ее применимой для малых фермеров, выращивающих ягоды [2, 3].

2. Проектирование системы.

Система включает три уровня:

1. Сбор данных: Микроконтроллер Luckfox Pico Max RV1106 принимает данные от датчиков (влажность почвы, температура, освещенность) и управляет светодиодными лампами.
2. Обработка данных: Информация сохраняется в базе данных SQLite и анализируется локально.
3. Принятие решений: ИИ прогнозирует урожайность, а БСМ выявляет риски.

Схема системы представлена на рисунке 1: данные от датчиков поступают в микроконтроллер, затем в базу и аналитические модели.

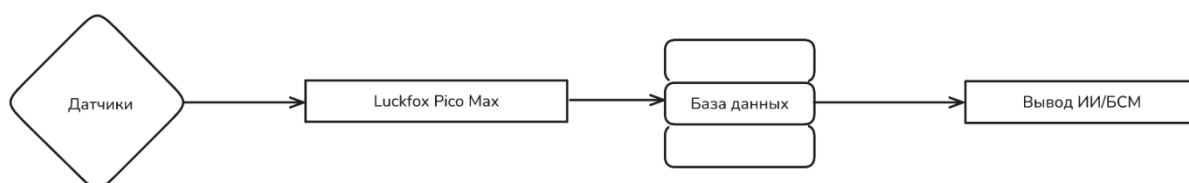


Рисунок 1. Архитектура системы

(Схема: Датчики → Luckfox Pico Max → База данных → Вывод ИИ/БСМ)

Для реализации использовались:

- Luckfox Pico Max RV1106: Микроконтроллер с поддержкой ИИ и низким энергопотреблением (<1 Вт).
- Датчики: Емкостной датчик влажности почвы, DHT22 (температура/влажность), BH1750 (освещенность).
- Светодиодные лампы: 38 Вт, красный/синий спектр для фотосинтеза.
- ПО: Python с библиотеками pgmpy (БСМ) и scikit-learn (ИИ), SQLite для хранения данных.

Модель включает узлы: Влажность почвы, Температура, Наличие болезней, Здоровье растений, Урожайность. Зависимости определены через таблицы условных вероятностей (ТУВ). Пример ТУВ для здоровья растений приведен в таблице 1. Модель обучена на синтетических данных (1000 записей) и показала точность 87%.

Таблица 1: ТУВ здоровья растений

Влажность почвы	Температура	Болезнь	Высокое здоровье	Низкое здоровье
Высокая	Оптимальная	Отсутствует	0.95	0.05
Низкая	Неоптимальная	Есть	0.10	0.90

3. Прогнозирование урожайности. Линейная регрессия на основе scikit-learn предсказывает урожайность (кг/м²) по данным о влажности, освещенности и температуре. Результаты представлены в виде таблицы для удобства использования фермерами.

Результаты. Система протестирована в теплице в течение 48 часов, собрано более 5000 записей. Байесовская сеть точно выявила риски заболеваний (например, серая гниль при высокой влажности), а ИИ спрогнозировал урожайность с отклонением до 5% от эталонных значений [4, 5]. Стоимость системы составила \$5–20, что компенсируется ростом урожая на 15%. Пример прогноза приведен в таблице 2.

Таблица 2: Таблица прогноза урожайности

Период	Влажность (%)	Свет (люкс)	Темп. (°C)	Прогноз урожая (кг/м²)
Май 2024	60	800	20	2.48
Янв 2026	50	600	16	2.15

Закключение.

Разработка демонстрирует эффективность сочетания ИИ, IoT и байесовских сетей для мониторинга ягодных культур. Система доступна, точна и подходит для малых ферм и обучения. В будущем планируется добавление облачной поддержки и уведомлений для повышения функциональности. Это решение может стать шагом к широкому внедрению цифровых технологий в сельском хозяйстве.

Литература:

1. Jones, R. (2020). Визуализация данных в Индустрии 4.0: Инструменты и методы. Springer.
2. Shepherd, M., et al. (2018). Байесовские сети в управлении болезнями культур. *Agricultural Systems*, 162, 1–10.
3. Vasisht, D., et al. (2017). FarmBeats: IoT-платформа для данных в сельском хозяйстве. *NSDI*, 515–529.
4. Wolfert, S., et al. (2017). Большие данные в умном фермерстве: Обзор. *Agricultural Systems*, 153, 69–80.
5. Документация Prometheus. Доступно по: <https://prometheus.io/docs/>.

Еуразиялық халықаралық ғылыми конференция
«Ғылымдағы, техника мен индустриядағы жасанды интеллект және кері есептер»
Евразийская международная научная конференция
“Искусственный интеллект и обратные задачи в науке, технике и индустрии”
Eurasian international scientific conference
«Artificial intelligence and inverse problems in science, technology and industry»

2 СЕКЦИЯ

«КЕРІ ЖӘНЕ ДҰРЫС ҚОЙЫЛМАҒАН ЕСЕПТЕРДІҢ ТЕОРИЯЛЫҚ ЖӘНЕ ЕСЕПТЕУ АСПЕКТІЛЕРІ»

СЕКЦИЯ 2

«ТЕОРЕТИЧЕСКИЕ И ВЫЧИСЛИТЕЛЬНЫЕ АСПЕКТЫ ОБРАТНЫХ И НЕКОРРЕКТНЫХ ЗАДАЧ»

SECTION 2

«THEORETICAL AND COMPUTATIONAL ASPECTS OF INVERSE AND ILL-POSITIONED PROBLEMS»

УДК 621.396.96: 528.854

Akhmadiya Asset
a.akhmadiya@kazatu.kz
Ph.D., Assistant Professor,
Kazakh Agro Technical
Research University, Astana

MODIFIED FREEMAN-DURDEN DECOMPOSITION RADAR IMAGE TO ELIMINATE NEGATIVE POWER PROBLEM

Abstract. A new method which completely eliminated the negative value of the scattering power is proposed in this paper. Primarily, here are presented the Freeman-Durden decomposition of the scattering powers, which are computed by using the coherency matrix elements with rotation and without rotation. Secondly, in this paper investigates the reasons of occurrence of negative values of the scattering powers. Then using the modification like in algorithm proposed by Yamaguchi for G4U, it was applied for the algorithm of Freeman-Durden decomposition to eliminate negative values. In this research, Radarsat-2 radar remote sensing data were used, which are acquired for study area Yushu County, Qinghai province, China. At the end, the comparison results of Yamaguchi G4U and a modified Freeman-Durden decompositions were presented.

Keywords: Coherency matrix, Freeman-Durden decomposition, General four-component decomposition with unitary transformation (G4U), scattering power, rotation.

Introduction

Many remarkable works were publicized on polarimetric decomposition such as decomposition of the target scattering matrix into three orthogonal components that has been proposed by Cloude [1], Holm and Barnes [2], van Zyl [3], and Krogager. Cloude and Pottier have produced an excellent review of these decomposition theorems. Generally speaking, there are two types of decomposition, namely, coherent and incoherent decompositions [4]. Proposed by Freeman and Durden decomposition is model-based incoherent decomposition. The Freeman–Durden decomposition is a technique for fitting a physically based, three-component scattering mechanism model to the polarimetric SAR observations, without utilizing any ground truth measurements [4]. This decomposition based on the polarimetric coherency matrix as contribution of three scattering mechanisms: double-bounce, volume and surface scatterings. Later, it was introduced the fourth component of scattering mechanism proposed by Yamaguchi et al. [6], [7], [8]. From G4U (general four-component decomposition with unitary transformation) and subsequent modifications of the four-component decomposition is completely excluded negative values of the scattering powers [9]. However, there are problems of this kind in the original Freeman-Durden decomposition, mainly the appearance of a negative pixel values in double-bounce and surface scattering powers. It is sometimes called the negative power problem. The explanation of this problem is here in [10], [11]. This problem is solved partially, i.e., reduction the number or percentage of negative pixels by using a filtering or rotation in Freeman-Durden decomposition. Complete elimination of negative pixels is achieved through the replacement of negative values and the use of an algorithm of residual values derived from total power, as in the example G4U.

Algorithm of the Freeman-Durden Decomposition

The algorithm of Freeman-Durden decomposition based on model obtained from coherency matrix component as contribution three scattering mechanisms: surface, double-bounce and volume scattering [11]:

$$[T] = P_s[T]_{\text{surface}} + P_d[T]_{\text{double}} + P_v[T]_{\text{vol}} \quad (1)$$

where P_s , P_d and P_v are power of each scattering components and their sum is equal to total power (TP):

$$\mathbf{P} = P_s + P_d + P_v = T_{11} + T_{22} + T_{33} = T_{11}(?) + T_{22}(?) + T_{33}(?)$$

where T_{11} , T_{22} , T_{33} are diagonal elements of the coherency matrix, $T_{11}(?)$, $T_{22}(?)$, $T_{33}(?)$ (2) diagonal elements of the rotated coherency matrix

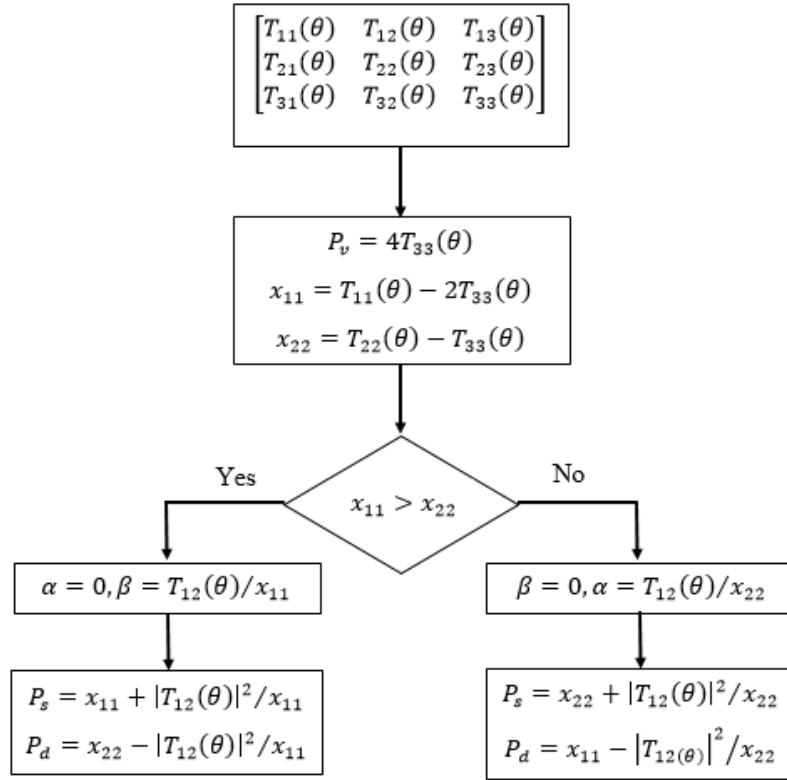


Figure 1: Algorithm of the Freeman-Durden Decomposition (FDD) with rotation of coherency matrix

After image processing according to this algorithm, there are obtained three components of the scattering powers P_s , P_d and P_v . In this case, a first two components have negative pixel values, there is particularly prevalent in double-bounce scattering power, they are shown in Table 1.

Table 1. Percentage of pixels with negative P_s and P_d

	$P_s(\%)$	$P_d(\%)$
Algorithm of FDD without rotation	5.78	70.05
Algorithm of FDD with rotation	6.88	50.93
Algorithm of proposed by Yang (2010)	2.83	1.55

The PolSAR data for this image processing acquired from Radarsat-2, the study area Yushu County, Qinghai province, China. The elements of the coherency matrix were generated in PolSARpro software. The remaining image processing was performed in ENVI software.

Negative Power Problem

From a mathematical point of view, the emergence of the negative value pixels in scattering powers is due to these three reasons:

$$\begin{cases} T_{11} < 2T_{33} \\ T_{22} < T_{33} \\ |T_{12}|^2 > (T_{11} - 2T_{33})(T_{22} - T_{33}) \end{cases} \quad (3)$$

The Freeman decomposition has been successfully applied to analyze the polarimetric data of the forest terrain. When applied to other types of terrain, however, P_s or P_d sometimes becomes negative. Since power is supposed to be nonnegative, the emergence of negative power values indicates that the model of the Freeman decomposition is not consistent with the actual scattering mechanism for these pixels. Note that in Table 1, the total number or percentage of negative pixels decreases after rotation of coherency matrix, but this is still too high to be ignored. A significant reduction has been achieved by using the algorithm of proposed Yang [11]. The reduction of percentage of negative pixels is possible mainly due to the decrease of T_{33} and the increase of T_{22} and T_{11} . However, a new modification taken from G4U are proposed to perform complete elimination of negative pixels [9].

Modification of Freeman-Durden Decomposition

The total scattering power for three-component decomposition (2) are considered in this study. By using this equation, the modification and change of values scattering power and inequality situation are conducted according to Figure 2:

1) For volume scattering power P_v :

If $TP > P_v$ in this condition the volume scattering power is not changed $P_v^m = P_v$;

another situation $TP < P_v$, volume scattering power is equal $P_v^m = TP$.

2) For surface and double-bounce scattering powers P_s, P_d :

If $TP > P_v$, $P_s \geq 0$ and $P_d \geq 0$ in this condition the surface and double-bounce scattering powers are not changed $P_s^m = P_s$, $P_d^m = P_d$;

If $TP > P_v$, $P_s \geq 0$ and $P_d < 0$ in this case $P_v^m = P_v$, $P_s^m = TP - P_v^m$, $P_d^m = 0$;

If $TP > P_v$, $P_s < 0$ and $P_d \geq 0$ in this case $P_v^m = P_v$, $P_s^m = 0$, $P_d^m = TP - P_v^m$;

another situation $TP < P_v$ or ($P_s < 0$ and $P_d < 0$) in this case $P_v^m = TP$, $P_s^m = P_d^m = 0$;

Here, values before modification (P_s, P_d and P_v) after the algorithm of Freeman-Durden decomposition and after modification (P_s^m, P_d^m and P_v^m) are existed. After such manipulations all values of the scattering powers become non-negative. Below, a comparison of the modified Freeman-Durden decomposition (MFDD) with G4U are presented in the form of RGB radar imageries (Figure 3).

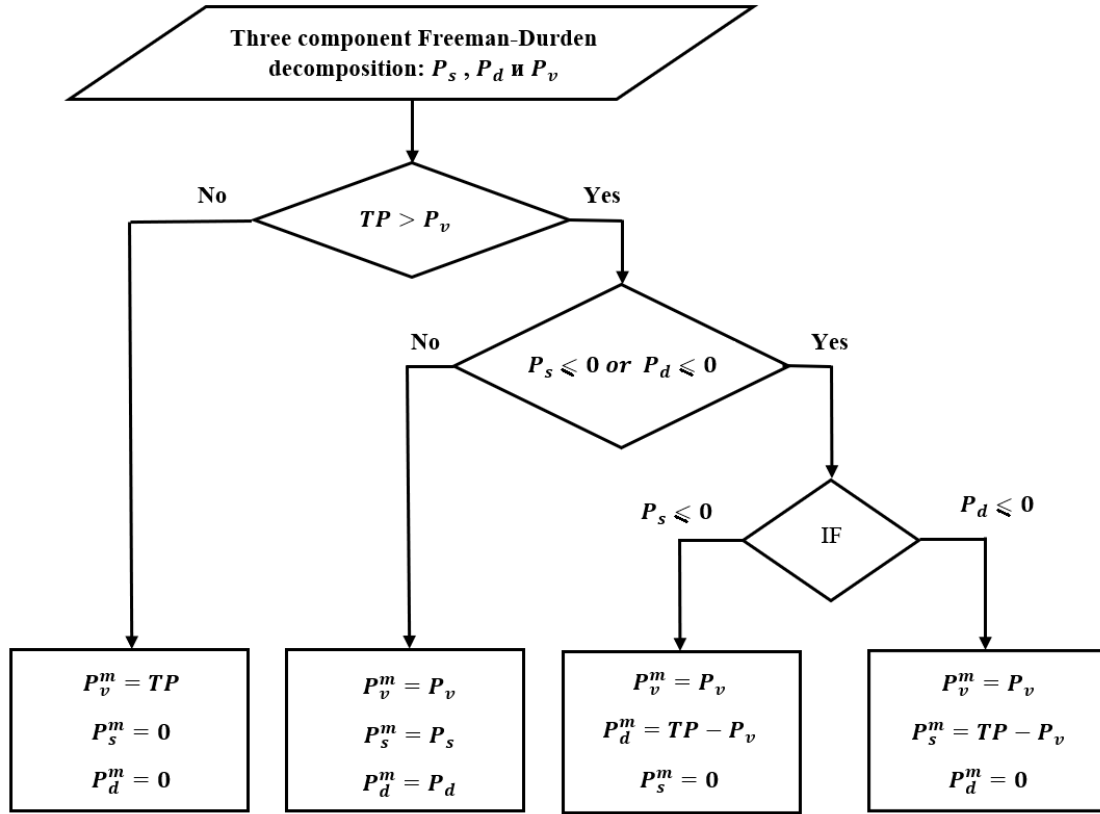


Figure 2: The algorithm for obtaining the modified Freeman-Durden decomposition

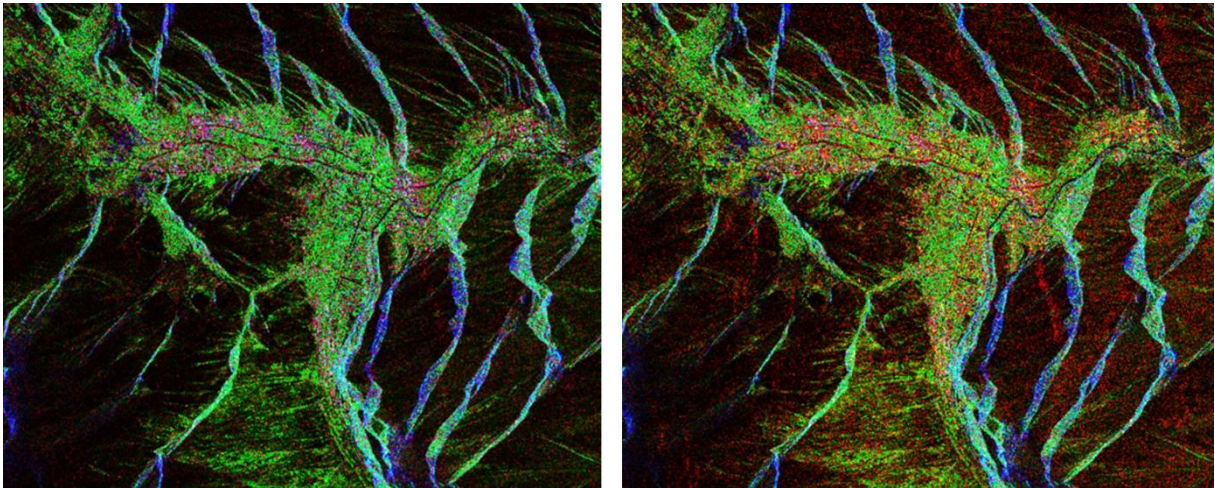


Figure 3: RGB Radar Imageries created from layers: Red - P_d , Green - P_v , Blue - P_d . Left side: Modified Freeman-Durden decomposition (MFDD); Right side: General four-component scattering power decomposition with unitary transformation (G4U) proposed by Yamaguchi.

Conclusion

This article presents the new method of exclusion of negative values of the scattering power and recalculation of balances total power for initial Freeman-Durden decomposition; as seen in the calculations,

we have three cases: single-component, two-component, and three-component. Single components appear when the surface and double bounce scattering powers are zero; there is dominated volume scattering power. Two components appear under the condition when one of surface or double-bounce scattering powers is zero; there are volume scattering power and one of surface or double-bounce scattering powers. Three components is ideal when all scattering powers are not equal to zero and have a positive value. Comparison of MFDD and G4U RGB images are characterized that in MFDD a little bit dominated by the color blue which means the surface scattering power, other differences are not visible. However, visual inspection shows a slight reduction in speckle-noise in the modified Freeman-Durden decomposition RGB image than in G4U RGB image (Figure 3). Ground truth data will check this alleged modification of Freeman-Durden decomposition and apply it to other high-resolution PolSAR data (TerraSAR-X, Cosmo-SkyMed). The reasonableness of this approach still will be checked. The algorithm of converting initial Freeman-Durden decomposition to a modified Freeman-Durden decomposition can be executed faster than General four-component scattering power decomposition with unitary transformation of coherency matrix proposed by Yamaguchi. Significantly, the new modified Freeman-Durden decomposition can be compared with other decomposition for target recognition purposes. For example, to distinguish urban areas, vegetation or forest area, and agriculture field, that can give high accuracy in supervised classification tasks.

References

- [1] Cloude, S. R. (1992) Uniqueness of target decomposition theorems in radar polarimetry. *Direct and Inverse Methods in Radar Polarimetry. Proceedings of the NATO Advanced Research Workshop*, 267-96 vol.1.
- [2] Holm, W. A., R. M. Barnes (1988) On radar polarization mixed target state decomposition techniques., *Proceedings of the 1988 IEEE National Radar Conference (Cat. No.88CH2572-6)*, 249-54.
- [3] van Zyl, J. J. (1993) Application of Cloude's target decomposition theorem to polarimetric imaging radar data., *Proceedings of the SPIE - The International Society for Optical Engineering*, 1748, 184-91.
- [4] Cloude, S. R., E. Pottier (1996) A review of target decomposition theorems in radar polarimetry. *Ieee Transactions on Geoscience and Remote Sensing*, 34, 498-518.
- [5] Freeman, A., S. Durden (1993) A three-component scattering model to describe polarimetric SAR data. *Proceedings of the SPIE - The International Society for Optical Engineering*, 1748, 213-24.
- [6] Yamaguchi, Y., T. Moriyama, M. Ishido, H. Yamada (2005) Four-component scattering model for polarimetric SAR image decomposition. *Ieee Transactions on Geoscience and Remote Sensing*, 43, 1699-1706.
- [7] Yamaguchi, Y., Y. Yajima, H. Yamada (2006) A four-component decomposition of POLSAR images based on the coherency matrix. *Ieee Geoscience and Remote Sensing Letters*, 3, 292-296.
- [8] Yajima, Y., Y. Yamaguchi, R. Sato, H. Yamada, W.-M. Boerner (2008) POLSAR image analysis of wetlands using a modified four-component scattering power decomposition. *Ieee Transactions on Geoscience and Remote Sensing*, 46, 1667-1673.
- [9] Singh, G., Y. Yamaguchi, S.-E. Park (2013) General Four-Component Scattering Power Decomposition With Unitary Transformation of Coherency Matrix. *Ieee Transactions on Geoscience and Remote Sensing*, 51, 3014-3022.
- [10] Lee, J.-S., T. L. Ainsworth, Y. Wang (2014) Generalized Polarimetric Model-Based Decompositions Using Incoherent Scattering Models. *Ieee Transactions on Geoscience and Remote Sensing*, 52, 2474-2491.
- [11] An, W., Y. Cui, J. Yang (2010) Three-Component Model-Based Decomposition for Polarimetric SAR Data. *Ieee Transactions on Geoscience and Remote Sensing*, 48, 2732-2739

UDC 517.958

Asanov A., Kadenova Z.A., Bekeshova D.A.
 (Institute of Mathematics of NAS of the KR),
 Pirmatov A.Z., Sayipbekova A.M. (Osh State University)

ONE CLASS OF LINEAR INTEGRAL EQUATIONS OF THE THIRD KIND WITH TWO INDEPENDENT VARIABLES

Inverse and ill-posed problems are currently attracting great interest. Theories of ill-posed problems, the foundation of which was laid by A.N. Tikhonov [1], M.M. Lavrentiev [2], and V.K. Ivanov [3], is an outstanding achievement of mathematics and allowed a new level in the development of new technologies in various fields of activity. Various problems of the theory of integral equations of the first and third kind were studied in [4,5].

In the present paper, uniqueness theorems for solutions are proved, and estimates of stability of solutions are obtained for a new class of linear integral equations of the third kind with two independent variables.

Consider the linear integral equations of the third kind with two independent variables

$$Ku = mt, x, u, x + abKt, x, y \int_a^b u(t, y) dy + t \int_a^b Ht, x, s \int_a^b u(s, x) ds + t \int_a^b Cx, s, y \int_a^b u(s, y) dy ds = ft, x, \quad t, x \in G = [t_0, T] \times [a, b], \quad a \leq x \leq b, \quad (1)$$

where

$$Kt, x, y = \{ At, x, y, t_0 \leq t \leq T, \quad a \leq y \leq x \leq b, \quad Bt, x, y, t_0 \leq t \leq T, \quad a \leq x \leq y \leq b, \quad (2)$$

$At, x, y, Bt, x, y, Ct, x, s, y$ - are known functions defined on the domains

$$G_1 = [t_0, T] \times [a, b], \quad a \leq y \leq x \leq b,$$

$$G_2 = [t_0, T] \times [a, b], \quad a \leq x \leq y \leq b,$$

$$G_3 = [t_0, T] \times [a, b], \quad a \leq x \leq b,$$

$$G_4 = [t_0, T] \times [a, b], \quad a \leq y \leq x \leq b.$$

mt, x and ft, x - are the known functions, $t, x \in G$, $u(t, x)$ - is an unknown function, $u(t, x) \in L_2(G)$, where $L_2(G)$ - space of square summable functions in the domain G . Let's denote

$$Ps, y, z = As, y, z + Bs, z, y, s, y, z \in G_1, \quad (3)$$

Assume that the following conditions are satisfied:

- a) $mt, x \geq 0$, for all $t, x \in G$,
- $Ps, b, a \in C[t_0, T]$, $Ps, b, a \geq 0$ for all $t \in [t_0, T]$,
- $Py's, y, a \in CG$, $Py's, y, a \leq 0$ for all $(s, y) \in G$,
- $Pz's, b, z \in CG$, $Pz's, b, z \geq 0$ for all $(s, z) \in G$,
- $Pzy's, y, z \in CG_1$, $Pzy's, y, z \leq 0$ for all $s, y, z \in G_1$,
- b) $HT, y, t_0 \in Ca, b$, $HT, y, t_0 \geq 0$ for all $t \in [a, b]$,
- $Hs's, y, t_0 \in CG$, $Hs's, y, t_0 \leq 0$ for all $(s, y) \in G$,
- $H'T, y, \tau \in CG$, $H'T, y, \tau \geq 0$ for all $(s, y) \in G$,
- $H\tau's, y, \tau \in CG_3$, $H\tau's, y, \tau \leq 0$ for all $s, y, \tau \in G_3$,

and for anyone $t, x \in L_2G$,

$a \int_a^b At, x, y \int_a^b u(t, y) dy + b \int_a^b Bt, x, y \int_a^b u(t, y) dy + t \int_a^b Ht, x, s \int_a^b u(s, x) ds$, где $C[t_0, T]$, CG , CG_1 , CG_3 - the space of all continuous functions respectively in $[t_0, T]$, G , G_1 , G_3 .

- c) $CT, b, t_0, a \geq 0$

$Cs's, b, t_0, a \in C[t_0, T]$, $Cs's, b, t_0, a \leq 0$ for almost all $s \in [t_0, T]$,

$C'T, b, \tau, a \in C[t_0, T]$, $C'T, b, \tau, a \geq 0$ for almost all $\tau \in [t_0, T]$,

$Cy'T, y, t_0, a \in Ca, b$, $Cy'T, y, t_0, a \leq 0$ for almost all $y \in [a, b]$,

$Cz''T, b, t_0, z \in Ca, b$, $Cz''T, b, t_0, z \geq 0$ for almost all $z \in a, b$,
 $Csy''s, y, t_0, a \in C(G)$, $Csy''s, y, t_0, a \geq 0$ for almost all $(s, y) \in G$,
 $C\tau y''T, y, \tau, t_0 \in C(G)$, $C\tau y''T, y, \tau, t_0 \leq 0$ for almost all $(y, \tau) \in G$,
 $Czs''s, b, t_0, z \in C(G)$, $Czs''s, b, t_0, z \leq 0$ for almost all $(s, z) \in G$,
 $C\tau z''T, b, \tau, z \in C(G)$, $C\tau z''T, b, \tau, z \geq 0$ for almost all $(\tau, z) \in G$,
 $C\tau sy'''s, y, \tau, a \in C(G_3)$, $C\tau sy'''s, y, \tau, a \geq 0$ for almost all $(s, y, \tau) \in G_3$,
 $C\tau zs'''s, b, \tau, z \in C(G_3)$, $C\tau zs'''s, b, \tau, z \leq 0$ for almost all $(s, \tau, z) \in G_3$,
 $Czsy'''s, y, t_0, z \in C(G_1)$, $Czsy'''s, y, t_0, z \geq 0$ for almost all $s, y, z \in G_1$,
 $C\tau zy'''T, y, \tau, z \in C(G_1)$, $C\tau zy'''T, y, \tau, z \leq 0$ for almost all $(\tau, y, z) \in G_1$,
 $C\tau zsy'''s, y, \tau, z \in C(G_4)$, $C\tau zsy'''s, y, \tau, z \geq 0$ for almost all $(s, y, \tau, z) \in G_4$,
 $C\tau s''s, b, \tau, a \in C(G_5)$, $C\tau s''s, b, \tau, a \leq 0$ for almost all
 $s, \tau \in G_5 = s, \tau: t_0 \leq \tau \leq s \leq T$,
 $Czy''T, y, t_0, z \in C(G_6)$, $Czy''T, y, t_0, z \leq 0$ for almost all
 $y, z \in G_6 = y, z: a \leq z \leq y \leq b$;

d) With almost everyone $s, y, z \in G_4$ and for all $1, 2, 3, 4 \in R$:

$Ls, y, z, 1, 2, 3, 4 = 1s - t_0y - aPy's, y, a^{12} - Hs's, y, t_0^{22} - 2Cs, y, t_0, a^{12} - s - t_0H\tau s''s, y, \tau^{32} + 2Cs's, y, \tau, a^{31} - y -$
 $a^2Cz's, y, t_0, z^{24} + Pzy''s, y, z^{42} - 2s - t_0y - aC\tau z''s, y, \tau, z^{34} \geq 0$.

e) If in front of everyone
 $s, y, \tau, z \in G_4$, $Ls, y, z, 1, 2, 3, 4 = 0$.

Then at least one of the following conditions is met:

1) $1 = 0$, 2) $2 = 0$, 3) $3 = 0$, 4) $4 = 0$.

Theorem 1. Let conditions a), b), c), d) and e). be satisfied. Then the solution of the equation (1) is unique in L_2G .

Next, estimates of the stability of solutions for a new class of linear integral equations of the third kind with two independent variables are obtained.

REFERENCES

1. Tikhonov A.N. On methods for solving ill-posed problems. In the book: Abstracts of reports, International Congress of Mathematicians. Moscow, 1966 (In Russ).
2. Lavrent'ev M. M. On some ill-posed problems of mathematical physics. Novosibirsk: Publishing House of Siberian branch of the Academy of Sciences of the USSR, 1962. - 92 p. (In Russ).
3. Ivanov V.K. About ill-posed tasks. Differential Equations, 1968, no. 2. - p.61.
4. Imanaliev M.I., Asanov A., Kadenova Z.A. A Class of Linier Intergral Equations of the First Kind with Two Independent Variables. Doklady Mathematics. 2014, Vol.89, no. 1, Pp.98-102.
5. Asanov A., Kadenova Z.A., Bekeshova D.A. One class of Fredholm linear integral equations of the third kind on a semi-axis// Herald of Institute of Mathematics of NAS of KR. 2023. no. 2. pp. 64-67.

UDK 517.984.2

Asanov A. , Kadenova Z.A., Bekeshova D.A
 Institute of Mathematics of NAS of the Kyrgyz Republic,
 Bishkek, Kyrgyzstan

ON THE UNIQUENESS OF SOLUTIONS OF FREDHOLM LINEAR INTEGRAL EQUATIONS OF THE FIRST KIND ON THE SEMI-AXIS

Many problems of the theory of integral equations of the first kind were studied in [1-5]. But fundamental results for Fredholm integral equations of the first kind were obtained in [1, 2], where regularizing operators in the sense of M.M.Lavrent'ev were constructed.

In the present paper, on the basis of the method of integral transformation, uniqueness theorems for the new class of linear Fredholm integral equations of the first kind in the semiaxis were proved.

Consider the linear Fredholm integral equations of the first kind

$$Ku \equiv \int_{-\infty}^a K(t, s)u(s)ds = f(t), \quad t \in (-\infty, a], \quad (1)$$

where the $u(t)$ is the desired function on $(-\infty, a]$, the given function $f(t)$ is the continuous on $(-\infty, a]$,

$$\int_{-\infty}^a \int_{-\infty}^a |K(t, s)|^2 ds dt < \infty,$$

$$K(t, s) = \begin{cases} A(t, s), & -\infty < s \leq t \leq a, \\ B(t, s), & -\infty < t \leq s \leq a, \end{cases} \quad (2)$$

the given functions $A(t, s)$ and $B(s, t)$ are continuous on the domain

$$G = \{(t, s) : -\infty < s \leq t \leq a\}.$$

Let $C(-\infty, a]$ denote the space of all functions continuous on $(-\infty, a]$. Here $C(G)$ denote the space of all functions continuous on G .

We introduce the notation

$$H(t, s) = A(t, s) + B(s, t), (t, s) \in G. \quad (3)$$

Assume that the following conditions are satisfied:

(i) $H(t, s), H'_t(t, s), H'_s(t, s), H''_{ts}(t, s) \in C(G), \alpha(t) = \lim_{s \rightarrow -\infty} H(t, s), t \in (-\infty, a], \alpha(a) \geq 0,$
 $\alpha(t) \in C(-\infty, a], \alpha'(t) \leq 0$ for all $t \in (-\infty, a], H''_{st}(t, s) \leq 0$ for all $(t, s) \in G,$
 $\alpha'(t) \in L_1(-\infty, a], \beta(s) = H'_s(a, s) \geq 0$ for all $s \in (-\infty, a], \beta(s) \in C(-\infty, a] \cap L_1(-\infty, a];$

(ii) $\sup_{(t,s) \in G} |H(t, s)| \leq l < \infty, \sup_{t \in (-\infty, a]} \int_{-\infty}^t |H'_s(t, s)| ds \leq l_1 < \infty,$

$H''_{ts}(t, s) \in L_1(G), \sup_{t \in [s, a]} |H'_s(t, s)| \leq \gamma(s) \in L_1(-\infty, a];$

(iii) At least one of the following three conditions holds:

- 1) $\alpha'(t) < 0$ for almost $t \in (-\infty, a];$ 2) $\beta(s) > 0$ for almost all $s \in (-\infty, a];$
- 3) $H''_{ts}(t, s) < 0$ for almost all $(t, s) \in G.$

Theorem . Let conditions (i), (ii) and (iii) be satisfied. Then the solution of the integral equation (1) is unique in $L_1(-\infty, a]$.

REFERENCES

1. M.M.Lavrent'ev, *The integral equations of the first kind*, Doklady Akademii Nayk, 127(1959), 31-33.
2. Lavrent'ev, V.G.Romanov, S.P.Shishatskii, *Ill-Posed problems of mathematical physics and analysis*, Providence R.I., American Mathematical Society, 1986.
3. A.Asanov, *Regularization, uniqueness and existence of solutions of Volterra equations of the first kind*, VSP, Utrecht, The Netherlands, 1998.
4. M.I.Imanaliev, A.Asanov, *Solutions of system of nonlinear Volterra integral equations of the first kind*, Soviet. Math. Dokl. 309:5 (1989), 1052-1055.
5. M.I.Imanaliev, A.Asanov, Z.A.Kadenova, *A Class of Linear Integral Equations of the First Kind with Two Independent Variables*, Doklady Mathematics, 89(1)(2014), 98-102.

УДК 510

Khompys Kh. (Al-Farabi Kazakh National University Almaty, Kazakhstan)

AN INVERSE SOURCE PROBLEM FOR A SEMILINEAR PSEUDO-PARABOLIC EQUATION

In this work, we study an inverse source problem for a semilinear pseudo-parabolic equation supplemented with initial and Neumann boundary conditions. The inverse problem consists of recovering a time-dependent source from a measurement given in integral form. Under suitable conditions on the data, and employing Rothe's method, we establish the existence and uniqueness of a weak solution and obtain estimates for convergence. Some test examples are constructed, and numerical solutions are obtained.

This work supported by the grant no. AP23486218.

Mukhanova T., Toregali R., Aidos T. Al-Farabi
 Kazakh National University, Almaty, Kazakhstan

FREDHOLM INTEGRAL EQUATIONS SOLVED NUMERICALLY USING THE BUBNOV-GALERKIN METHOD BASED ON ALPERT WAVELETS

Fredholm integral equations are a class of equations that describe an unknown function through an integral operator. They play a crucial role in solving various problems in physics, engineering, and applied mathematics. These equations are divided into two main types: first-kind and second-kind Fredholm equations [1,2].

The first-kind Fredholm integral equation is given as follows:

$$\int_a^b K(x, t)\phi(t)dt = f(x), \quad a \leq x \leq b$$

where $K(x, t)$ is the kernel, $\phi(x)$ is the unknown function, and $f(x)$ is the given function. This equation is often encountered in inverse problems, and its solution may be unstable, requiring the application of regularization methods.

The second-kind Fredholm integral equation is given as follows:

$$\phi(x) - \lambda \int_a^b K(x, t)\phi(t)dt = f(x), \quad a \leq x \leq b$$

where λ is a parameter. These equations are effectively solved using numerical methods, among which the Bubnov-Galerkin method is widely used.

The Bubnov-Galerkin method approximates the unknown function $\phi(x)$ as a linear combination of basis functions:

$$\phi(x) \approx \sum_{i=1}^N c_i \psi_i(x).$$

Using Alpert wavelets as the basis functions enhances both accuracy and computational efficiency. Alpert wavelets are highly localized in space and exhibit orthogonality, ensuring precise approximations [3].

In the numerical solution of Fredholm equations, the Bubnov-Galerkin method with Alpert wavelet bases improves computational efficiency and accuracy, especially for large-scale problems. This method is widely applied in solving inverse problems, signal processing, and engineering computations.

Keywords: first-kind Fredholm integral equation, second-kind Fredholm integral equation, Bubnov-Galerkin method, Alpert wavelets, wavelet orthogonality.

AMS Subject Classification: BR27100483, 45B05, 65T60.

REFERENCES

- [1] Rostami, Y., & Maleknejad, K. (2019). Solving Fredholm integral equations of the first kind by using wavelet bases. *Hacettepe Journal of Mathematics and Statistics*, **48**(6), 1729–1743.
- [2] Maleknejad, K., Karami, M., Numerical Solution of Fredholm Integral Equation of the First Kind by Using Legendre Wavelets, *Appl. Math. Comput.*, 168, 2005, pp. 102-110.

Alpert B. et al. Wavelet-like bases for the fast solution of second-kind integral equations //SIAM journal on Scientific Computing. – 1993. – . 14. – №. 1. – . 159-184

УДК 004.8:336.717

Serzhan Y.S., Umarov T.F.
Kazakh-British Technical University,
Almaty, Kazakhstan

FRAUD DETECTION IN CREDIT CARD TRANSACTIONS USING MACHINE LEARNING: A COMPARATIVE ANALYSIS

The rapid increase in digital financial transactions has expanded the risk of fraudulent activities, which escalated the need for more effective fraud detection methods. This research paper presents a comprehensive approach to fraud detection in credit card transactions, utilizing an end-to-end methodology based on machine learning techniques. This study summarizes thorough exploratory data analysis, data preprocessing, model training with various class balancing techniques, and hyperparameter optimization. Experiments on a large credit card dataset (284,807 transactions, 31 features) have demonstrated that the best model - XGBoost without sampling - achieved an Area Under the Curve of 96.82% and an average precision of 88%. Since the framework is trained using a data-driven approach, it can dynamically adapt to emerging fraud patterns, ensuring high accuracy in identifying suspicious activities. Additionally, the capability of the model to handle large volumes of data in real-time makes it well-suited for financial institutions managing high transaction loads. One key advantage of this architecture is its ability to achieve significantly higher throughput while maintaining low latency compared to traditional methods.

Keywords: Machine Learning, Random Forest, Logistic Regression, Fraud, Hyperparameter Optimization, XGBoost, Gradient Boosting

UDC 004.021

Zharkyn D. (Astana, L.N. Gumilyov ENU)

COMPREHENSIVE USE OF MULTI-AGENT MODELS IN URBAN TRAFFIC MANAGEMENT

Abstract: As urbanization continues to rise, understanding and managing the complex dynamics of urban population flows is crucial for effective city planning. The article discusses the significance of using multi-agent systems for monitoring urban population movements in transportation, detailing key methodologies. It examines the fundamental components of multi-agent systems and presents examples of their application in transportation systems, hazardous materials transport, and route planning. Finally, based on study outcomes, the article evaluates potential areas for the broader application of multi-agent systems to enhance convenience for urban residents and outlines future directions for this technology.

Keywords: multi-agent systems, modeling, city flow, transportation systems, emergency situations.

INTRODUCTION

According to the United Nations, 68% of the global population is expected to live in urban areas by 2050. This highlights the importance of traffic modeling to improve urban infrastructure. Existing simulation methods (object-oriented, cellular automata) face challenges in handling system complexity and interdependencies. MAS offer a solution to these issues by enabling dynamic and adaptive modeling.

MULTI-AGENCY MODELS IN THE TRANSPORTATION SYSTEM

1. Transport Demand Modeling in Guanajuato, Mexico

A study in Guanajuato, Mexico, utilized multi-agent models and classification algorithms to predict transportation choices in five cities. A decision tree-based classification algorithm, specifically the J48 algorithm, was applied to forecast transportation mode selection. The study was conducted using data from 72,924 residents, with simulations spanning three years. The results demonstrated a 45% increase in public transport usage, while the use of private vehicles rose by 16%. The study confirmed that multi-agent models can effectively predict and plan transportation demand, aiding urban mobility strategies [2].

2. Accident Risk and Impact Assessment in Belgrade

A study in Belgrade focused on assessing the consequences of accidents involving gasoline tankers using multi-agent modeling. The simulation incorporated various traffic participants, including cars, buses, trucks, trams, and pedestrians, to estimate potential casualty rates. Simulations revealed that the number of casualties varied significantly depending on population density and accident location. The results ranged from an average of 11 to 28 casualties, highlighting the need for effective emergency response strategies and risk mitigation measures in densely populated areas [3].

3. V2X-Based Traffic Flow Optimization

A multi-agent platform was developed to evaluate V2X-based traffic scenarios, utilizing vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. The model was structured into three layers: an information model, a traffic management model, and interaction protocols. By simulating different congestion levels, the platform assessed how real-time data exchange could influence route optimization and congestion reduction. The study demonstrated that vehicles using V2X communication could dynamically adjust their routes based on congestion data, leading to improved traffic flow [1].

4. Multi-Agent and Cellular Automata-Based Traffic Simulation

A standalone application, ABMTrafSimCA, was developed to model urban traffic using cellular automata and a multi-agent approach. Written in C++ with a Qt-based graphical interface, the software enabled users to define road length, vehicle density, and driver behavior. It generated fundamental diagrams and space-time visualizations to analyze traffic dynamics under different conditions [4].

5. Traffic Signal Optimization in Astana

A case study in Astana utilized AnyLogic to simulate urban traffic at an intersection under various scenarios. The model examined how different traffic signal timings influenced vehicle flow and congestion levels. Iterative simulations were conducted to identify optimal signal configurations for improving traffic efficiency. The study revealed that decreasing the duration of green-light phases led to a higher number of vehicles passing through the intersection, reducing congestion. The results underscored the importance of adaptive traffic signal control in enhancing urban mobility and optimizing road network performance [5].

CONCLUSION

In conclusion, this review comprehensively explored the applications of multi-agent systems in various transportation contexts, such as hazardous material transport and route planning. The adaptability and efficiency of multi-agent models were highlighted. The study demonstrated that multi-agent systems effectively address and optimize challenges in urban environments. The article examined traffic movements that could lead to fire hazards, providing crucial insights for evaluating the potential impacts of accidents in urban areas. These advancements will continue to play a crucial role in shaping sustainable urban mobility strategies.

REFERENCES

1. Tomás, V.R., García, L.A., Alonso, A.L. An agent-based platform to evaluate V2X routing road traffic scenarios // *Simulation Modelling Practice and Theory*. – 2023. – №125. – C. 10 – 27.

2. Salas-Rodriguez, D., Rivas-Tovar, L.A. Agent-Based Modeling for Evaluation of Transportation Mode Selection in the State of Guanajuato, Mexico // *Computacion y Sistemas*. – 2022. – №26. – С. 1689 – 1701
3. Strahinja Pantelic', Branko Milovanovic', Marko Dogatovic, Predrag Živanovic', Stanko Bajc'etic', Slaven Tica, Andrea Nad. Consequence Assessment Model for Gasoline Transport: Belgrade Case Study Based on Multi-Agent Simulation // *Sustainability*. – 2023. – №15(3). – С. 1 – 14.
4. Górka, Patryk et al. vABMTrafSimCA: An agent-based modelling open-source software tool for traffic modelling and simulation based on cellular automata // *SoftwareX*. – 2024. Volume 27, 101813
5. Zharkyn Dannar. Modeling traffic flow in the city // *Collections of the International Scientific Conference of Students and Young Scientists “GYLYM JÁNE BILIM - 2024”*. – 2024. – С. 823 – 826.

УДК 517.956

Shutong Hou(Nanjing, China, SEU)
Haibing Wang(Nanjing, China, SEU)

A NOVEL APPROACH FOR AN INVERSE SOURCE PROBLEM OF THE WAVE EQUATION IN THREE DIMENSIONS

We address the inverse problem of reconstructing the source term in a bounded domain for the time-domain wave equation. A small droplet with high contrast is injected into the medium, and then the difference in the wave fields before and after injecting the droplet is utilized to develop a novel reconstruction approach. First, we analyze the asymptotic behavior of the wave field after injecting the droplet by using the time-domain integral equation method. Then, on the basis of this analysis, the wave field before injecting the droplet is reconstructed by utilizing the external measurements. Next, the source term is reconstructed through numerical differentiation of the wave field before the droplet injection. A key advantage of our approach is that it only requires measurements at a fixed point over a period of time. Additionally, to show the performance of our approach for the inverse problem, we also develop an efficient algorithm to solve the time-domain Lippmann-Schwinger equation for the corresponding forward problem. Numerical experiments in three dimensions are presented to demonstrate the effectiveness of the proposed approach.

УДК 517.588, 519.632

Абдрахман Б.Қ., Рысқан А.Р.,
Амангельды А.Е. (Алматы, Абай атындағы ҚазҰПУ)

КӨП АЙНЫМАЛЫ ГИПЕРГЕОМЕТРИЯЛЫҚ ФУНКЦИЯ ҮШІН ЕКІНШІ РЕТТІ ДИФФЕРЕНЦИАЛДЫҚ ТЕҢДЕУЛЕР ЖҮЙЕСІН ШЕШУ

Гипергеометриялық функциялар математикалық физика мен қолданбалы математиканың арнайы функциялары арасында маңызды орын алады. Қазіргі уақытта көп айнымалылардың гипергеометриялық функциясы ұғымына кемінде төрт көзқарас бар. Мұндай функцияларды белгілі бір түрдегі дәрежелік қатарлардың қосындылары [1], дифференциалдық теңдеулер жүйесінің

шешімдері [2], Эйлер типті интегралдар [3] және Меллин-Барнс интегралдары ретінде анықтауға болады [4]. Бұл жұмыста біз гипергеометриялық функцияны дифференциалдық теңдеулер жүйесінің шешімі ретінде қарастырамыз.

Гипергеометриялық F194 функциясын қарастырайық:

$$F_{19}^{(4)}(a_1, a_2, b_1, b_2; c_1, c_2, c_3; x, y, z, t) = \sum_{m,n,p,q=0}^{\infty} \frac{(a_1)_{m+n+p} (a_2)_q (b_1)_{m+n} (b_2)_{p+q}}{(c_1)_m (c_2)_n (c_3)_{p+q}} \frac{x^m y^n z^p t^q}{m! n! p! q!} \quad (1)$$

мұндағы $c \neq 0, -1, -2, -3, \dots; i=1, \dots, 3$.

Төрт айнымалы F194 гипергеометриялық функция [5] келесі екінші ретті дербес туындылы дифференциалдық теңдеулердің жүйесін қанағаттандырады:

$$\begin{cases} x(1-x)u_{xx} - yu_{xy} - zu_{xz} - 2xyu_{xy} - yzu_{yz} + [c_1 - (a_1 + b_1 + 1)x]u_x - (a_1 + b_1 + 1)yu_y - b_1zu_z - a_1b_1u = 0 \\ y(1-y)u_{yy} - xu_{xy} - zu_{yz} - 2xyu_{xy} - yzu_{yz} - (a_1 + b_1 + 1)xu_x + [c_2 - (a_1 + b_1 + 1)y]u_y - b_1zu_z - a_1b_1u = 0 \\ z(1-z)u_{zz} + t(1-z)u_{zt} - xzu_{xz} - xtu_{xt} - yzu_{yz} - ytu_{yt} - xb_2u_x - yb_2u_y + [c_3 - (a_1 + b_2 + 1)z]u_z - a_1b_2u - a_1tu_t = 0 \\ t(1-t)u_{tt} + z(1-t)u_{zt} - a_2zu_z + [c_3 - (a_2 + b_2 + 1)t]u_t - a_2b_2u = 0 \end{cases} \quad (2)$$

мұндағы $u, x, y, z, t = F_{194} a_1, a_2, b_1, b_2, c_2, c_3 x, y, z, t$

Біз сызықтық тәуелсіз шешімдерді келесі түрде іздейміз:

$$u = xyzwtw, \quad (3)$$

мұндағы w - белгісіз функция, x, y, z, t - анықталатын тұрақтылар. Жаңа айнымалылар x, y, z, t, w енгізіп және (2) орнына дифференциалдық теңдеулердің келесі жүйесін аламыз:

$$\begin{cases} x(1-x)w_{xx} - 2xyw_{xy} - xzw_{xz} - y^2w_{yy} - yzw_{yz} + [C_1 - (A_1 + B_1 + 1)x]w_x - (A_1 + B_1 + 1)yw_y - B_1zw_z + [\alpha(c_1 + \alpha - 1)x^{-1} - A_1B_1]w = 0, \\ y(1-y)w_{yy} - x^2w_{xx} - 2xyw_{xy} - xzw_{xz} - yzw_{yz} - (A_1 + B_1 + 1)xw_x + [C_2 - (A_1 + B_1 + 1)y]w_y - B_1zw_z + [\beta(c_2 + \beta - 1)y^{-1} - A_1B_1]w = 0, \\ z(1-z)w_{zz} + (1-z)tw_{zt} - xzw_{xz} - xtw_{xt} - yzw_{yz} - ytw_{yt} + (A_1 + B_2 - 1)zw_z + C_3w_z + (\gamma z^{-1} - A_1)tw_t - B_2xw_x - B_2yw_y + [\gamma(\gamma + \delta + c_3 - 1)z^{-1} - A_1B_2]w = 0 \\ t(1-t)w_{tt} + z(1-t)w_{zt} - (A_2 - \delta t^{-1})zw_z + [C_3 - (A_2 + B_2 + 1)t]w_t + [\delta(c_3 + \gamma + \delta - 1)t^{-1} - A_2B_2]w = 0 \end{cases} \quad (4)$$

мұндағы,

$$A_1 = a_1 + \alpha + \beta + \gamma, \quad A_2 = a_2 + \delta,$$

$$B_1 = \alpha + \beta + b_1$$

$$B_2 = \gamma + \delta + b_2$$

$$C_1 = c_1 + 2\alpha, \quad C_2 = c_2 + 2\beta, \quad C_3 = c_3 + 2\delta + \gamma, \quad C_4 = c_3 + 2\gamma + \delta.$$

(2) және (4) жүйелер келесі шарттар орындалған кезде эквивалентті болады:

$$\begin{cases} \alpha(c_1 + \alpha - 1) = 0, & \beta(c_2 + \beta - 1) = 0, \\ \gamma(c_3 + \gamma + \delta - 1) = 0, & \delta(c_3 + \gamma + \delta - 1) = 0 \end{cases}$$

(6)

Осылайша, төрт айнымалы екінші ретті дифференциалдық теңдеулер жүйесінің сызықтық тәуелсіз келесі түрде гипергеометриялық функциялар арқылы жазылған шешімдерін аламыз:

$$u_1(x, y, z, t) = F_{19}^{(4)}(a_1, a_2, b_1, b_2; c_1, c_2, c_3; x, y, z, t) = \sum_{m,n,p,q=0}^{\infty} \frac{(a_1)_{m+n+p} (a_2)_q (b_1)_{m+n} (b_2)_{p+q}}{(c_1)_m (c_2)_n (c_3)_{p+q}} \frac{x^m y^n z^p t^q}{m! n! p! q!}$$

$$u_2(x, y, z, t) = x^{1-c_1} F_{19}^{(4)}(a_1 + 1 - c_1, a_2, b_1 + 1 - c_1, b_2; 2 - c_1, c_2, c_3; x, y, z, t) = x^{1-c_1} \sum_{m,n,p,q=0}^{\infty} \frac{(a_1 + 1 - c_1)_{m+n+p} (a_2)_q (1 - c_1 + b_1)_{m+n} (b_2)_{p+q}}{(2 - c_1)_m (c_2)_n (c_3)_{p+q}} \frac{x^m y^n z^p t^q}{m! n! p! q!}$$

$$u_3(x, y, z, t) = y^{1-c_2} F_{19}^{(4)}(a_1 + 1 - c_2, a_2, 1 - c_2 + b_1, b_2; c_1, 2 - c_2, c_3, c_3; x, y, z, t) = y^{1-c_2} \sum_{m,n,p,q=0}^{\infty} \frac{(a_1 + 1 - c_2)_{m+n+p} (a_2)_q (1 - c_2 + b_1)_{m+n} (b_2)_{p+q}}{(c_1)_m (2 - c_2)_n (c_3)_{p+q}} \frac{x^m y^n z^p t^q}{m! n! p! q!}$$

$$u_4(x, y, z, t) = x^{1-c_1} y^{1-c_2} F_{19}^{(4)}(a_1 + 2 - c_1 - c_2, a_2, 2 - c_1 - c_2 + b_1, b_2; 2 - c_1, 2 - c_2, c_3, c_3; x, y, z, t) = x^{1-c_1} y^{1-c_2} \sum_{m,n,p,q=0}^{\infty} \frac{(a_1 + 2 - c_1 - c_2)_{m+n+p} (a_2)_q (2 - c_1 - c_2 + b_1)_{m+n} (b_2)_{p+q}}{(2 - c_1)_m (2 - c_2)_n (c_3)_{p+q}} \frac{x^m y^n z^p t^q}{m! n! p! q!}$$

Пайдаланылған әдебиеттер тізімі

[1] Hasanov A. Fundamental solutions for degenerated elliptic equation with two perpendicular lines of degeneration. *International Journal of Applied Mathematics and Statistics*, V. 13, N. 8, 2008, pp. 41-49.

[2] Hasanov A. Fundamental solutions of generalized bi-axially symmetric Helmholtz equation. *Complex Variables and Elliptic Equations*, V. 52, N. 8, 2007, pp. 673- 683.

[3] Erd'elyi A., Magnus W., Oberhettinger F., Tricomi F.G. *Higher Transcendental Functions*, V. I, Mc Graw Hill, New York, Toronto and London, 1953.

[4] Exton H. *Multiple Hypergeometric Functions and Applications*, Halsted Press, London, 1976.

[5] Appell P., Kamp'e de F'eriet J. *Fonctions Hyperg'eom'etriques Hypersph'ériques*, Gauthier-Villars, Paris, 1926, 440 p. et

УДК 004.855.5

Аркабаев Н.К. (Кыргызстан, Ош,
Ошский государственный университет)
Кудуев А.Ж. (Кыргызстан, Ош,
Ошский государственный университет)

РАЗРАБОТКА И ОПТИМИЗАЦИЯ АЛГОРИТМОВ ГЛУБОКОГО ОБУЧЕНИЯ НА PYTHON ДЛЯ ОБРАБОТКИ БОЛЬШИХ ДАННЫХ В РЕАЛЬНОМ ВРЕМЕНИ С ПРИМЕНЕНИЕМ ВЫЧИСЛИТЕЛЬНОГО ИНТЕЛЛЕКТА

Аннотация. Это исследование посвящено созданию и улучшению алгоритмов глубокого обучения на Python для быстрой и эффективной обработки больших данных. В работе анализируются методы оптимизации нейросетей, предлагаются новые алгоритмические подходы с элементами вычислительного интеллекта и проводится их тестирование. Разработана гибридная архитектура, которая сочетает облегченные модели CNN и RNN с механизмами внимания для работы с разнородными потоковыми данными, а также система балансировки вычислительной нагрузки. Эксперименты показали, что такие решения позволяют снизить вычислительные затраты на 37–42%, сохраняя точность не ниже 94% по сравнению с полноразмерными моделями.

Ключевые слова. глубокое обучение, Python, оптимизация моделей, обработка потоковых данных, вычислительный интеллект.

1. Введение

Современные системы искусственного интеллекта и машинного обучения сталкиваются с двумя противоречивыми тенденциями. С одной стороны, наблюдается экспоненциальный рост объемов генерируемых данных, требующих обработки в реальном времени. С другой стороны, растут требования к точности и скорости алгоритмов, которые должны извлекать полезные сведения из этих данных, зачастую при ограниченных вычислительных ресурсах, особенно в системах периферийных вычислений.

Проблема оптимизации алгоритмов глубокого обучения для обработки больших данных в реальном времени включает несколько ключевых аспектов: ограниченная вычислительная мощность при необходимости быстрого анализа данных, непрерывный характер потоковых данных, требующий способности адаптироваться в процессе работы, и гетерогенная природа реальных данных, усложняющая создание универсальных подходов к их обработке.

Исследование Zhang et al. [1] показало эффективность метода "адаптивной дистилляции знаний" для потоковых данных, где компактная студенческая модель динамически обновляется на основе предсказаний более крупной учительской модели. Sharma и Batra [2] применили технику раннего выхода (early-exit) в глубоких нейронных сетях для адаптации вычислительной нагрузки в зависимости от сложности входных данных, что позволило сократить время обработки на 45% для простых образцов данных.

Целью данного исследования является разработка и оптимизация алгоритмов глубокого обучения на языке Python для эффективной обработки больших данных в режиме реального времени с применением методов вычислительного интеллекта.

2. Методология исследования

В качестве базовой программной инфраструктуры использовались Python 3.9 и TensorFlow 2.7 с дополнительными библиотеками, включая Apache Kafka, Ray и TensorFlow Serving. Вычислительная инфраструктура включала кластер из 4 серверов с процессорами Intel Xeon E5-2680 v4, 128 ГБ оперативной памяти и графическими ускорителями NVIDIA Tesla V100.

На основе систематического анализа существующих подходов были выделены пять основных групп методов оптимизации: квантизация моделей, прунинг нейронных связей, дистилляция знаний, параллельные вычисления и адаптивные алгоритмы обучения.

Для экспериментального тестирования были выбраны три набора данных: временные ряды показаний датчиков от 250 IoT-устройств, поток текстовых сообщений из социальных сетей (до 1000 сообщений в секунду) и набор транзакционных финансовых данных.

В рамках исследования был реализован комплексный класс AdaptiveStreamProcessor, объединяющий различные техники оптимизации для обработки потоковых данных.

3. Результаты исследования

На основе проведенного анализа была разработана гибридная архитектура, объединяющая облегченные версии CNN и RNN с механизмами внимания для эффективной обработки разнородных потоковых данных.

Ключевой особенностью архитектуры является способность динамически масштабировать вычислительную сложность в зависимости от доступных ресурсов и требований к точности анализа. Это достигается за счет реализации техники раннего выхода.

Важным результатом исследования стала разработка системы динамической балансировки вычислительной нагрузки, способной адаптировать параметры моделей в зависимости от интенсивности потока данных и доступных ресурсов.

Система динамической балансировки функционирует на основе многокритериальной оптимизации с применением подхода reinforcement learning.

Отдельно было исследовано влияние системы динамической балансировки на стабильность работы при переменной нагрузке (Рисунок 3). Система с динамической балансировкой демонстрирует значительно более стабильную производительность при пиковых нагрузках.

4. Заключение

Разработанный комплексный подход к оптимизации алгоритмов глубокого обучения для обработки потоковых данных в реальном времени демонстрирует значительные преимущества по сравнению с существующими методами. Экспериментальное тестирование показало снижение вычислительных затрат на 37-42% и потребления памяти на 60-74% при сохранении точности моделей на уровне не ниже 94% от полноразмерных версий.

Предложенная гибридная архитектура и система динамической балансировки вычислительной нагрузки обеспечивают эффективную обработку разнородных потоковых данных и стабильную производительность при переменной нагрузке, что критически важно для систем реального времени.

Результаты исследования имеют высокую практическую значимость для разработки систем мониторинга промышленных объектов, анализа данных социальных сетей и финансовых транзакций в реальном времени. Дальнейшие исследования будут направлены на расширение предложенного подхода для работы с мультимодальными потоковыми данными и интеграцию методов федеративного обучения.

Список литературы

1. Zhang, K., Williams, C., Lee, S., Oates, T. (2022). Adaptive Knowledge Distillation for Streaming Data Analysis. International Conference on Machine Learning, 12567-12576.
2. Sharma, D., Batra, N. (2023). Efficient Inference with Early-Exit Networks for Time-Series Data. Proceedings of the International Conference on Learning Representations, 214-223.
3. Wang, H., Lei, J., Wu, L., Li, J., Hu, Z. (2022). Scalable Deep Learning Models for Real-Time Data Processing at Edge. IEEE Transactions on Neural Networks and Learning Systems, 33(8), 3712-3725.
4. Hassan, M., Li, T. (2023). Federated Learning for Distributed Stream Processing. ACM Transactions on Intelligent Systems and Technology, 14(3), 1-25.

MSC 49M37

Асанкулова М., Каденова З.А.,
Жолборсова А.К. (ИМ НАН КР)

ОПТИМАЛЬНОГО РАСПРЕДЕЛЕНИЯ СЫРЬЯ МЕЖДУ ПОТРЕБИТЕЛЯМИ ДЛЯ ЗАДАЧ ДОБЫВАЮЩИХ ОТРАСЛЕЙ

Кыргызская республика горная страна и на ее большей территории идет добыча природных сырьевых ресурсов. Многие проблемы добывающих отраслей экономики сводятся к экстремальным задачам размещения в различных постановках [3,4], в том числе и задача распределения сырья между потребителями [5].

В настоящее время опубликовано множество научных статей посвященных моделям и методам решения таких задач. Для решения таких задач среди существующих методов хорошо зарекомендовали алгоритмы, основанные на методе последовательных расчетов [1,2].

Проблема прогнозирования дохода в добывающих предприятиях, где покупателями выступают предприятия – потребители на основе договора и потребители, идущие как оптовые покупатели, где вначале определяется объем потребности сырья для потребителей на основе договора. Затем за вычетом сырья для потребителей на основе договора определяется объем сырья для оптовых покупателей.

К решению этой проблемы посвящена предлагаемая нами работа, которая описывает проблему оптимизации распределения сырья между потребителями на основе договора и оптовыми покупателями по критерию максимума дохода добывающих предприятий.

Найти максимум

$$L(x) = \sum_{i \in I} \sum_{j \in J_0} \{t_{ij} - s_i\} x_{ij} + \max_{x_0} \sum_{i \in I} \sum_{j \in J^*} \{\bar{t}_{ij} - s_i\} x_{ij}^* \quad (1)$$

при условиях

$$b_j = \sum_{i \in I} x_{ij}, \quad j \in J_0, \quad (2)$$

$$a_i \geq x_i = \sum_{j \in J_0} x_{ij}, \quad i \in I, \quad (3)$$

$$x_{ij} \geq 0, \quad i \in I, \quad j \in J_0, \quad (4)$$

где $x = |x_{ij}|_{|I||J_0|}$, x_0 - множество оптимальных решений x_{ij}^* задачи:

найти минимум

$$L_0(x_0) = \sum_{i \in I} \sum_{j \in J^*} c_{ij} x_{ij} \quad (5)$$

при

условиях $b_j = \sum_{i \in I} x_{ij}, \quad j \in J^*, \quad (6)$

$$a_i - x_i = \sum_{j \in J^*} x_{ij}, \quad i \in I, \quad (7)$$

$$x_{ij} \geq 0, \quad i \in I, \quad j \in J^*. \quad (8)$$

В целевую функцию задачи (1)-(4) введем обозначения:

$$d_{ij} = t_{ij} - s_i, \quad i \in I, \quad j \in J_0 \text{ и } \bar{d}_{ij} = \bar{t}_{ij} - s_i, \quad j \in J^*. \quad (*)$$

Согласно введенному обозначению целевая функция (1) имеет вид:

$$L(x) = \sum_{i=1}^m \sum_{j \in J_0} d_{ij} x_{ij} + \max_{x_0} \sum_{i=1}^m \sum_{j \in J^*} \bar{d}_{ij} x_{ij}^* \quad (9)$$

Для решения сформулированной задачи (9), (2)-(4) и (5)-(8) обоснована применимость метода последовательных расчетов [2].

Для этой цели на каждом подмножестве $\omega \in I$ может быть определено максимальное значение функции

$$L_1(x, \omega) = \sum_{i \in \omega} \sum_{j \in J_0} d_{ij} x_{ij} \quad (10)$$

при

условиях $b_j = \sum_{i \in \omega} x_{ij}, \quad j \in J_0, \quad (11)$

$$a_i \geq x_i = \sum_{j \in J_0} x_{ij}, \quad i \in \omega, \quad (12)$$

$$x_i \geq 0, \quad x_{ij} \geq 0, \quad i \in \omega, \quad j \in J_0, \quad (13)$$

и значение функции

$$L_2(x, \omega) = \sum_{j \in J^*} (\sum_{i \in \omega} c_{ij} x_{ij} + \sum_{i \in I \setminus \omega} c_{ij} x_{ij}) \rightarrow \min \quad (14)$$

при

условиях $b_j = \sum_{i \in \omega} x_{ij} + \sum_{i \in I \setminus \omega} x_{ij}, \quad j \in J^*, \quad (15)$

$$a_i - x_i^* = \sum_{j \in J^*} x_{ij}, \quad i \in \omega, \quad a_i = \sum_{j \in J^*} x_{ij}, \quad i \in I \setminus \omega, \quad (16)$$

$$x_{ij} \geq 0, \quad i \in I, \quad j \in J^*, \quad (17)$$

где I - множество индексов месторождений сырья $A_i, i \in I$, а ω - любое произвольное подмножество множества I и $\{x_{ij}^*\}$ - решение задачи (10)-(13) на $\omega \in I$.

Тогда получаемый чистый доход предприятий объединения на каждом $\omega \in I$ будут

$$L(x, \omega) = L_1(x, \omega) + \max_{x_0} \sum_{j \in J^*} (\sum_{i \in \omega} d_{ij} x_{ij}^* + \sum_{i \in I \setminus \omega} d_{ij} x_{ij}^*),$$

определяться величиной

где $\{x_{ij}^*\}$ - решение задачи (14)-(17) на $\omega \in I$.

Требуется определить такое подмножество $\omega^* \in I$, на котором $P(\omega)$ достигала своего

$$P(\omega^*) = \max_{\omega \in I} \{P(\omega)\}.$$

наибольшего значения

(18) Доказывается достаточное условие

применимости метода последовательных расчетов для задачи (18), т.е. для любых подмножеств $\omega_1, \omega_2 \subset I$ выполнение условия

$$S(\omega_1, \omega_2) = P(\omega_1) + P(\omega_2) - P(\alpha) - P(\beta) \geq 0, \quad (19)$$

где $\alpha = \omega_1 \cup \omega_2$, $\beta = \omega_1 \cap \omega_2$, а $P(\omega_1)$, $P(\omega_2)$, $P(\alpha)$, $P(\beta)$ –

максимальные значения функции $L_1(x, \omega)$ при условиях (11)-(13) и замене множества ω соответственно множествами $\omega_1, \omega_2, \alpha, \beta$.

Выполнение условия (19) позволяет применить для задачи (18) алгоритм, предложенный в [2] и определить такое подмножество $\omega^* \in I$, на котором $p(\omega^*)$ достигает своего

максимального значения $p(\omega^*)$ и такие значения $x_i^* \geq 0, i \in \omega^*$, позволяющее сформулировать и решить задачу в виде (14)-(17) и определить значения целевой функции исходной задачи, т.е.

$$L(x, \omega^*) = P(\omega^*) + \max_{x_0} \sum_{j \in J^*} (\sum_{i \in \omega^*} d_{ij} x_{ij}^* + \sum_{i \in I \setminus \omega^*} d_{ij} x_{ij}^*).$$

Отметим, что при решении задачи (9), (2)-(4) для подсчета $P(\omega)$ $\omega \subset I$, наряду с условиями отбраковки вариантов метода последовательных расчетов используется дополнительное условие отбраковки

$$\sum_{i \in \omega} a_i \geq \sum_{j \in J_0} b_j.$$

(25)

Подсчет $P(\omega)$ производится лишь для вариантов, удовлетворяющих условию (25), в противном случае подсчет $P(\omega)$, не производится и исключается из дальнейшего рассмотрения все $\beta \subset \omega$. Работоспособность сформулированных моделей продемонстрирована на числовом примере, Для решения, приведенного в статье примера, использован метод приведенный в [2].

Литература

1. Черенин В.П., Хачатуров В.Р. Решение методом последовательных расчетов одного класса задач о размещении производства // Математические методы и ЭВМ в экономических исследованиях. – Ташкент: Наука, 1965. - с.112-124.
2. Ланге Э.Г., Жусупбаев А. Комбинаторный метод решения задачи размещения. - Фрунзе: Илим, 1990. - 153 с.
3. Zhusupbaev, A. Determination of the volume of production of raw materials and its distribution among consumers under the contract / A. Zhusupbaev, M. Asankulova // Problems of optimization and economic applications: Proceedings of the VI International Conference, Omsk, June 28 - 04, 2015. - Omsk: Omsk State University. F.M. Dostoevsky, 2015. - P. 171. - EDN UGKXBJ.

4. Асанкулова М., Жусупбаев А., Жусупбаев Г.А. Определение максимального дохода предприятия при ограниченном объеме // Актуальные направления научных исследований века: теория и практика / Сб. науч. трудов. - 2015. - № 7 часть 1 (18-1). С.101-105. DOI:10.1273/14811
5. Асанкулова М. Оптимизация добычи и распределения сырья между потребителями в зависимости от периода [Текст] / М. Асанкулова, А. Жусупбаев // Проблемы современной науки и образования. – Иваново, 2016, 4(46). – С.7-12

УДК 519.635.6; 536.2.

Байтуреева А.Р., (Алматы, КазНУ им.Аль-Фараби),
 Рысбайұлы Б. (Астана, АИТУ)

ЧИСЛЕННОЕ РЕШЕНИЕ ОБРАТНОЙ ЗАДАЧИ ДЛЯ НАХОЖДЕНИЯ КОЭФФИЦИЕНТА ТЕПЛОПРОВОДНОСТИ В ЗАДАЧЕ ТЕПЛОМАССОПЕРЕНОСА В ПОРИСТОЙ СРЕДЕ

Введение

В данной работе рассматривается обратная задача по определению коэффициента теплопроводности в системе уравнений теплопереноса в пористой среде. Основная цель заключается в восстановлении неизвестного параметра на основе временных измерений температуры и влажности, проведенных на одной из границ области. Математическая постановка сведена к задаче оптимизации, в которой минимизируется отклонение между численно рассчитанными и экспериментально полученными распределениями температуры и влаги. Полученные результаты подтверждают высокую точность предлагаемого подхода.

Математическая модель и постановка задачи

Совместный перенос тепла и массы в твердом пористом теле описывается системой дифференциальных уравнений в частных производных [1].

$$\rho C_q \frac{\partial \theta}{\partial t} = K_q \frac{\partial^2 \theta}{\partial x^2} + \varepsilon \lambda \rho C_m \frac{\partial w}{\partial t} \quad (1)$$

$$\rho C_m \frac{\partial w}{\partial t} = K_m \delta \frac{\partial^2 \theta}{\partial x^2} + K_m \frac{\partial^2 w}{\partial x^2} \quad (2)$$

Здесь $\theta(x, t)$ и $w(x, t)$ – функции, описывающие изменение температуры и влаги, x – координаты по толщине слоя, t – время.

На поверхности среды $x = l$ ставятся граничные условия третьего рода:

$$K_q \frac{\partial \theta}{\partial x} + \alpha_q (\theta - \theta_a) + (1 - \varepsilon) \lambda \alpha_m (w - w_a) = 0 \quad (3)$$

$$K_m \frac{\partial w}{\partial x} + K_m \delta \frac{\partial \theta}{\partial x} + \alpha_m (w - w_a) = 0 \quad (4)$$

На нижней границе области $x = 0$ ставятся условия Неймана:

$$\frac{\partial \theta}{\partial x} \Big|_{x=0} = 0, \quad \frac{\partial w}{\partial x} \Big|_{x=0} = 0 \quad (5)$$

Начальные условия

$$\theta(x, 0) = \theta_0(x), w(x, 0) = w_0(x) \quad (6)$$

Кроме этого, задаются измеренные значения температуры и влаги на поверхности пористой среды.

$$\theta_a(t), w_a(t). \quad (7)$$

В качестве тестовой задачи рассматривается тепло- и влагоперенос в таком пористом теле, как ель (Рис. 1). Здесь, K_q - коэффициент теплопроводности, K_m - коэффициент влагопроводности, C_q - теплоемкость, C_m - влагопоглотительная способность, ρ - Плотность сухого тела, ε - отношение коэффициента диффузии пара к коэффициенту суммарной диффузии влаги, λ - теплота фазового перехода, δ - термоградиентный коэффициент, q - коэффициент конвективного теплопереноса, m - коэффициент конвективного массопереноса, l - толщина образца древесины. Подробные физические характеристики древесины и их значения приведены в работе [2].

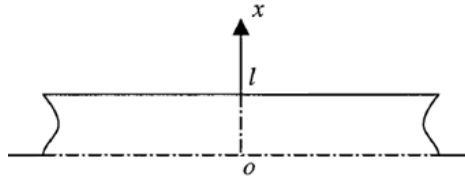


Рисунок 1. Слой пористой среды (древесина).

В качестве тестовой задачи рассматривается тепло- и влагоперенос в таком пористом теле, как ель (Рис. 1). Здесь, K_q — коэффициент теплопроводности, K_m — коэффициент влагопроводности, C_q — теплоемкость, C_m — влагопоглотительная способность, ρ — Плотность сухого тела, ε — отношение коэффициента диффузии пара к коэффициенту суммарной диффузии влаги, λ — теплота фазового перехода, δ — термоградиентный коэффициент, α_q — коэффициент конвективного теплопереноса, α_m — коэффициент конвективного массопереноса, l — толщина образца древесины. Подробные физические характеристики древесины и их значения приведены в работе [2].

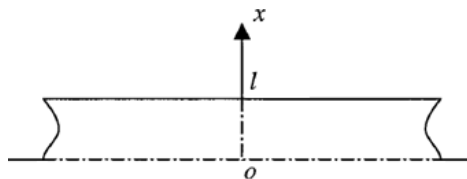


Рисунок 1. Слой пористой среды (древесина).

Прямая задача (уравнения 1-6) решается методом Томаса (алгоритм трехдиагональной матрицы). Далее, составляется сопряженная задача путем умножения уравнений (1-2) на сеточные функции $\psi_i^j \Delta x \Delta t$ и $\eta_i^j \Delta x \Delta t$ и далее задача рассматривается в сеточной области $Q = \{(x_i, t_j), x_i = i\Delta x, t_j = j\Delta t\}, i = 1, \dots, N - 1; j = m - 1, m - 2, \dots, 0$.

Путем различных математических преобразований выводится сопряженная задача [3-4]:

$$\{\psi_{i,\underline{t}}^{j+1} + \underline{F}_{11}\psi_{i,\underline{x}\underline{x}}^j + \underline{F}_{22}\eta_{i,\underline{x}\underline{x}}^j = 0 \quad \eta_{i,\underline{t}}^{j+1} + \underline{F}_{12}\psi_{i,\underline{x}\underline{x}}^j + \underline{F}_{21}\eta_{i,\underline{x}\underline{x}}^j = 0 \quad i = 1, 2, \dots, N - 1 \quad j = 0, 1, \dots, m - 1 \quad (8)$$

$$\psi_i^m = 0, \eta_i^m = 0, i = 1, 2, \dots, N \quad (9)$$

$$\psi_{1,x}^j = 0, \eta_{1,x}^j = 0, j = m-1, m-2, \dots, 1, 0 \quad (10)$$

$$\left(\underline{F}_{11}(n)K_{11}(n) + \underline{F}_{12}(n)K_{21}(n) \right) \psi_N^j + (F_{22}(n)K_{21}(n) + F_{21}(n)K_{11}(n))\eta_N^j - \underline{F}_{11}(n)\psi_{N,x}^j - F_{21}(n)\eta_{N,x}^j = 2(T_N^{j+1}(n) - T_g^{j+1}) \quad (11)$$

$$\left(\underline{F}_{11}(n)K_{12}(n) + \underline{F}_{12}(n)K_{22}(n) \right) \psi_N^j + (F_{22}(n)K_{22}(n) + F_{21}(n)K_{12}(n))\eta_N^j - \underline{F}_{12}(n)\psi_{N,x}^j - F_{22}(n)\eta_{N,x}^j = 2(U_N^{j+1}(n) - U_g^{j+1}) \quad (12)$$

Где $F_{11} = \frac{K_q t_{max}}{H^2 \rho C_q}$, $F_{12} = \frac{\varepsilon \lambda C_m U_0}{C_q T_0}$, $F_{21} = \frac{K_m \delta T_0 t_{max}}{H^2 \rho C_m U_0}$, $F_{22} = \frac{K_m t_{max}}{H^2 \rho C_m}$, $F_{T1} = \frac{\alpha_q t_{max}}{H \rho C_q}$, $F_{T2} = \frac{\lambda \alpha_m t_{max} U_0}{T_0 H \rho C_q}$,
 $F_{w1} = \frac{K_m t_{max}}{H^2 \rho C_m}$, $F_{w2} = \frac{\alpha_m t_{max}}{H \rho C_m}$ – безразмерные коэффициенты.

Далее задача решается итеративным путем, минимизируя на каждом шаге функционал:

$$I_{n+1} = \sum_{j=0}^{m-1} (T_N^{j+1} - T_g^{j+1})^2 \Delta t + \sum_{j=0}^{m-1} (U_N^{j+1} - U_g^{j+1})^2 \Delta t$$

Изначально задается приблизительное значение коэффициента теплопроводности K_q , которое потом обновляется на каждом следующем шаге:

$$K_q(n+1) = K_q(n) + \Delta K_q$$

Результаты

На рисунке 2 показана сходимость коэффициента теплопроводности K_q при разных начальных отклонениях: +10%, +25% и +50%. Во всех случаях значения стремятся к истинному значению $K_q=0.65$, обозначенному красной линией. При меньших отклонениях сходимость происходит быстрее: около 50 итераций при +10% и до 88 итераций при +50%. Метод стабильно находит точное значение независимо от начального приближения.

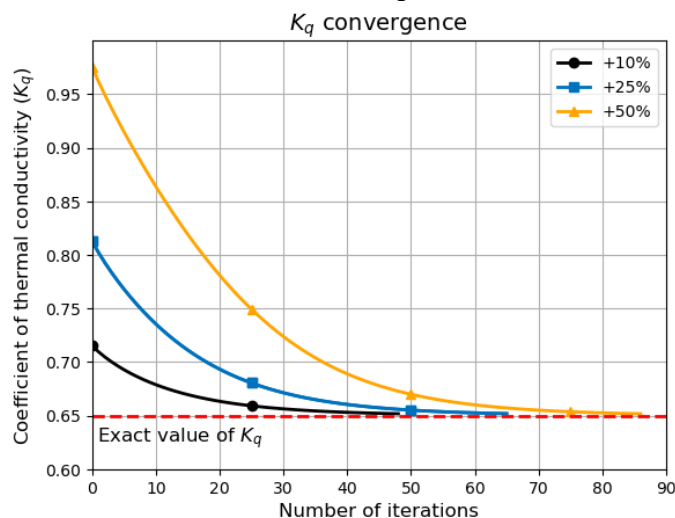


Рисунок 2. Сходимость коэффициента теплопроводности в зависимости от степени отклонения от истинного значения (+10, 25 и 50%)

Представленная модель будет применена в дальнейшем для нахождения остальных неизвестных физических параметров рассматриваемой пористой среды.

Литература

- [1] Лыков А.В. Теплообмен. Справочник. Изд. 2, перераб. и доп. 1978. 480 с.
[2] Liu J.Y. Solutions of Luikov equations of heat and mass transfer in capillary-porous bodies // Int. J. Heat Mass Transfer. – 1991. - Vol. 34. № 7. - P. 1747 – 1754.м
[3] Рысбайұлы Б. Обратные задачи нелинейной теплопроводности. Издательский дом «Қазақ Университеті», 2022, 369 с.
[4] Рысбайұлы Б. Обратные задачи нелинейной теплопроводности (монография), 2022, 369 с.

УДК 519.677

Бектемесов Ж.М. (Алматы, КазНУ им. аль-Фараби)

Социалова Ұ.Қ. (Алматы, КазНПУ им. Абая)

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ОБРАТНОЙ ЗАДАЧИ РАСПРОСТРАНЕНИЯ КОРИ

В работе исследуется динамика распространения кори с использованием модели SVEIR и методов решения обратных задач. Математическое моделирование проводилось на основе эпидемиологических данных, результатов мониторинга и аналитических расчётов. В рамках исследования проведён количественный анализ динамики распространения инфекции в Бангладеш за период 2000–2020 годов. Авторами статьи [9] была разработана компартиментная модель передачи кори, включающая следующие взаимоисключающие компартменты: S(t) – восприимчивые люди, ещё не заразившиеся болезнью, но подверженные риску инфицирования; V1(t) – индивидуумы, получившие первую дозу вакцины; V2(t) – индивидуумы, получившие вторую дозу вакцины; E(t) – экспонированные (латентные) лица, инфицированные, но без развитой активной формы заболевания; I(t) – инфицированные и заразные особи; R(t) – выздоровевшие, ранее инфицированные и успешно перенёсшие заболевание.

Модель основана на предположении, что общая численность популяции N(t) постоянна и хорошо перемешана:

$$N(t) = S(t) + V1(t) + V2(t) + E(t) + I(t) + R(t). \quad (1)$$

На основе перечисленных выше компартментов динамика передачи кори описывается следующей системой нелинейных обыкновенных дифференциальных уравнений, описывающей модель:

$$\begin{cases} \frac{dS}{dt} = \mu N - \beta SI - \eta S - \mu S + \rho V_1 \\ \frac{dV_1}{dt} = \eta S - \rho V_1 - \sigma V_1 - \mu V_1 \\ \frac{dV_2}{dt} = \sigma V_1 - \omega V_2 - \mu V_2 \\ \frac{dE}{dt} = \beta SI - \alpha E - \mu E \\ \frac{dI}{dt} = \alpha E - \gamma I - \delta I - \mu I \\ \frac{dR}{dt} = \gamma I + \omega V_2 - \mu R \end{cases} \quad (2)$$

и начальные условия:

$$S_0 \geq 0, V_{10} \geq 0, V_{20} \geq 0, E_0 \geq 0, I_0 \geq 0, R_0 \geq 0. \quad (3)$$

С помощью модели были реконструированы основные параметры, влияющие на распространение инфекции, в том числе скорость распространения вируса, эффективность первой и второй доз вакцинации, а также уровень смертности от заболевания.

Таблица 1. Оценка начальных условий модели кори.

Параметры	Описание	Расчетное значение
$N(t_0)$	Общая численность населения Бангладеш	127,658,000
$I(t_0)$	Класс инфицированных	5098
$E(t_0)$	Класс заболевших корью	5098
$R(t_0)$	Класс выздоровевших	$I(1 - \delta)$
$S(t_0)$	Класс восприимчивых	$N(t_0) - I(t_0) - E(t_0) - R(t_0)$
$V_1(t_0)$	Класс вакцинированных первой дозой	ηS
$V_2(t_0)$	Класс вакцинированных второй дозой	σS

Предполагается, что подверженные $E(t_0)$ в начальный момент времени имеют такое же количество индивидуумов, сколько и инфицированные $I(t_0)$. Количество выздоровевших $R(t_0) = I(t_0)(1 - \delta)$, где δ – показатель умерших от кори. Тогда начальное количество восприимчивых $S(t_0) = N(t_0) - I(t_0) - E(t_0) - R(t_0)$, а вакцинированные $V_1(t_0)$ и $V_2(t_0)$ исчисляются, как ηS и σS , соответственно, где η – показатель вакцинированности первой дозой, а σ – второй дозой.

Далее, предполагая, что значения параметров вектора $q = (\eta, \sigma, \omega, \gamma, \delta, \mu)$ не известны, что приводит данную задачу к виду обратной коэффициентной задаче. Обратная задача состоит в том, что бы по известным данным $I_n(t)$, восстановить значения параметров q , минимизируя следующий функционал:

$$J(q) = \sum_{n=1}^M [I(t, q) - I_n(t)]^2 \rightarrow \min_q, \quad (4)$$

где J_q – это функционал подлежащий минимизации, $I_{t,q}$ – решение уравнения (2) для числа инфицированных индивидов, M – количество статистических данных.

В данной работе в качестве метода оптимизации использовался один из метаэвристических подходов – генетический алгоритм [2-3]. Оптимизационный алгоритм был реализован с помощью функции *ga* в прикладном программном пакете *Matlab*.

На рисунке 1 представлены статистические данные о числе инфицированных, а также модельный прогноз до 2030 года, построенный с использованием восстановленных параметров уравнения (2). Ожидается, что к концу 2025 года суммарное количество инфицированных составит примерно 93 244 человека, что на 2 577 больше по сравнению с 2023 годом. К 2030 году этот показатель может достигнуть примерно 101 189 человек.

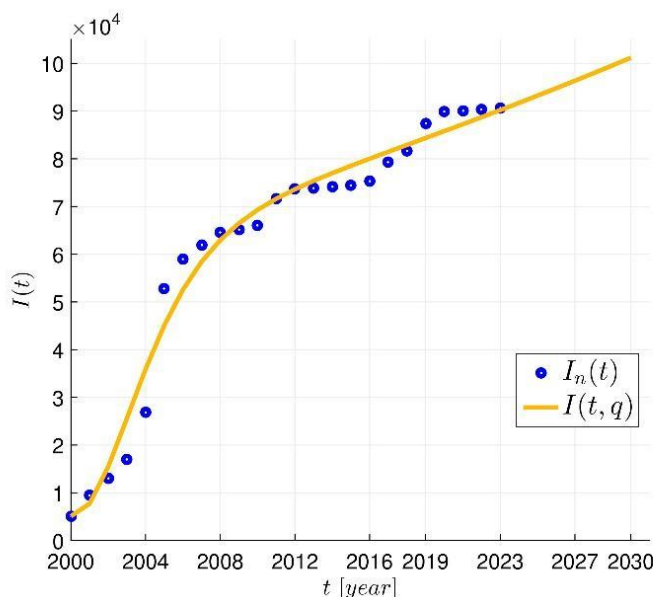


Рисунок 1. Динамика фактического (синие точки) и восстановленного (жёлтая линия) числа инфицированных за 2000-2023 годы, а также прогноз до 2030 года.

Информация, полученная в результате данного исследования, может помочь правительству и специалистам в области общественного здравоохранения разработать стратегии для устранения пробелов, возникших вследствие вспышки кори, а также для эффективного контроля и предотвращения эпидемии в Казахстане.

Список использованных источников

1. Md Abdul Kuddus, Mohiuddin M., Azizur Rahman (2021) *Mathematical analysis of a measles transmission dynamics model in Bangladesh with double dose vaccination.* // *Scientific Reports*.
2. Goldberg D.(1989) *Genetic Algorithms in Search, Optimization and Machine learning.* // Addison-Wesley.
3. Herrera F., Lozano M., Verdegay J.L. (1998) *Tackling real-coded genetic algorithms: operators and tools for the behavior analysis*// *Artificial Intelligence Review*, V. 12, № 4, 265-319.

УДКД 621.391.812

Бешеев Д.М., Оралбекова Ж. О., Ұзаққызы Н.
(Евразийский национальный университет им.
Л.Н. Гумилева, Астана)

ОЧИСТКА ГЕОРАДИОЛОКАЦИОННОГО СИГНАЛА ВЕЙВЛЕТ-ФИЛЬТРАМИ НА ОСНОВЕ SYMLET-6

В работе рассматривается анализ георадиолокационных данных при обследовании дорожного покрытия. Как известно, исходные георадиолокационные сигналы часто содержат помехи, обусловленные внешними и внутренними факторами, такими как случайный шум, многолучевые отражения и системные артефакты[1].

Нами были проведены эксперименты с использованием георадара ОКО-2, установленного на передвижной дорожно-диагностической лаборатории. Сканирование выполнялось антеннами АБ-1000Р с центральной частотой 1000 МГц, рупорный, глубина зондирования до 1,5 м, разрешение 4 см и АБ-400Р с центральной частотой 400 МГц, рупорный, глубина зондирования до 3 м, разрешение 10 см. Для проведения измерений больших участков антенные блоки были закреплены на автомобиле с помощью специальной подвески. Съёмка георадарного профиля производился в режиме “по перемещению” и для фиксации перемещения использовался системный датчик положения. Исследования проводились на нескольких участках дорог страны, включая основные магистрали и региональные дороги. Сбор данных осуществлялся на всем протяжении маршрута, от одного города до другого, с визуальным осмотром состояния покрытия.

Сырые данные представляют собой исходные результаты георадарных исследований и другие данные, полученные в ходе экспериментов. Для повышения качества интерпретации данных используется цифровая фильтрация, такие как полосовые, вейвлетные и адаптивные методы. Полосовая фильтрация позволяет удалять нежелательные частотные компоненты сигнала, такие как низкочастотные тренды и высокочастотный шум. Оптимальные границы фильтрации определяются экспериментально, исходя из характеристик используемых антенн и типа дорожного покрытия. Вычитание среднего устраняет систематические смещения, обусловленные особенностями георадарного оборудования. Среднее значение сигнала вычисляется по всему профилю, после чего из каждого отсчета вычитается среднее. Это позволяет минимизировать влияние аппаратных помех и улучшить визуальную интерпретацию данных. И, конечно, вейвлет-фильтрация позволяет эффективно устранять шумы, сохраняя при этом важные детали георадарных изображений.

В данном исследовании мы большее внимание обратили на использование вейвлет-фильтрации, а именно вейвлет-функции Симлета (Symlet), поскольку она обладает хорошими свойствами компромисса между симметрией и числом моментов обнуления, что важно для обработки сигналов с резкими изменениями. В данном случае в качестве базовой вейвлет-функции, мы применили Symlet-6 [2]. Декомпозицию проводили выполняя разложение исходного сигнала на несколько уровней с помощью дискретного вейвлет-преобразования (DWT):

$$X_t = \sum_j c_{j,k} \psi_{j,k}(t)$$

где $c_{j,k}$ - вейвлет-коэффициенты, $\psi_{j,k}(t)$ - базисные функции Симлета.

Высокочастотные составляющие, соответствующие шуму, подавляются с использованием жесткого или мягкого порогового метода[3]:

Жесткий порог: $\{0, w \leq T, w > T\}$

Мягкий порог: $\{0, w \leq T \text{ sign}(w) \max\{\frac{T}{|w|}, 1\}, w > T\}$

где T - адаптивный порог, рассчитываемый по методу Донхо-Иоаннидиса:

$$T = \sigma^2 \ln N$$

где σ - оценка стандартного отклонения шума, N - длина сигнала.

Далее идет восстановление очищенного сигнала из отфильтрованных коэффициентов.

В нашем исследовании сохранение баланса между хорошей локализацией сигнала в пространстве и частоте было необходимым условием для качественной фильтрации сигнала. Как известно число моментов обнуления вейвлета определяет его способность подавлять низкочастотный шум и выделять детали. Если вейвлет имеет n моментов обнуления, то он не реагирует на полиномы степени $n-1$. Это означает чем больше моментов обнуления, тем лучше фильтрация медленно изменяющихся трендов, то есть шумов и приводит к менее компактному вейвлету, снижая его локализацию. Симметричные вейвлеты обеспечивают минимальные фазовые искажения. Однако с высоким числом моментов обнуления вейвлеты становятся менее симметричными. Поэтому, чтобы прийти к компромиссу между симметрией и числом моментов обнуления и был выбран Symlet-6, так как он почти симметричный и имеет достаточное количество моментов обнуления для устранения трендов и выделения аномалий.

Вейвлет-фильтрация на основе Symlet-6 показала себя очень полезной для устранения случайных помех и выделения мелкомасштабных особенностей дорожной структуры. В дальнейшем возможно применение адаптивных фильтров и методов машинного обучения для автоматизированной обработки данных.

Эксперименты были проведены совместно со специалистами Национального центра экспертизы дорожных активов РК.

Работа поддержана в рамках грантового финансирования МНВО РК 2023-2025 по проекту АР 19680361 «Разработка вычислительных технологий для диагностики дорожной одежды автомобильных трасс».

Список литературы

1. Mallat Stephane, (2008): *A Wavelet Tour of Signal Processing*, 3e2008, Academic Press.
 2. Kyprianou, Andreas & Lewin, Paul & Efthymiou, Venizelos & Stavrou, Andreas & Georghiou, George. (2006). *Wavelet packet denoising for online partial discharge detection in cables and its application to experimental field results. Measurement Science and Technology*. 17. 10.1088/0957-0233/17/9/001.
- Iskakov K.T., Boranbaev S.A., Uzakkyzy, N. *Wavelet processing and filtering of the radargram trace*, - *Eurasian Journal of Mathematical and Computer Application* this link is disabled, 2017

УДК 517.956

Бекенаева К.С., Макулбай А.Б. (Алматы, КазНПУ им. Абая)
Мирсабурова У.М. (Узбекистан, Термезский гос. университет)

ЗАДАЧА С ЛОКАЛЬНЫМИ И НЕЛОКАЛЬНЫМИ УСЛОВИЯМИ ДЛЯ ОДНОГО УРАВНЕНИЯ СМЕШАННОГО ТИПА

Рассмотрим уравнение

$$(\operatorname{sign} y) |y|^m u_{xx} + u_{yy} + (\beta_0 / y) u_y = 0, \quad (1)$$

где $m > 0$, $-m/2 < \beta_0 < 1$, в конечной односвязной области D плоскости независимых переменных x, y , ограниченной при $y > 0$ нормальной кривой $\sigma_0: x^2 + 4(m+2)^{-2}y^{m+2} = 1$ с концами в точках $A = A(-1, 0)$ и $B = B(1, 0)$, а при $y < 0$ характеристиками AC и BC уравнения (1).

Обозначим через D^+ и D^- части области D , лежащие, соответственно, в полуплоскостях $y > 0$ и $y < 0$, а через C_0 и C_1 , соответственно, точки пересечения характеристик AC и BC с характеристикой, исходящей из точки $E(c, 0)$, где $c \in I = (-1, 1)$ – интервал оси $y = 0$.

Постановка задачи для уравнения (1) существенным образом зависит от конструктивных свойств его решения. Отметим, что локальные и нелокальные задачи для различных значений коэффициентов уравнения (1) изучены в работах [1]–[3]. В данной работе рассмотрим уравнение (1) для предельного значения параметра $\beta_0 = -m/2$:

$$\operatorname{sign} y |y|^m u_{xx} + u_{yy} - \frac{m}{2y} u_y = 0. \quad (2)$$

Настоящая работа посвящена исследованию вопросов разрешимости задачи с локальными и нелокальными условиями для одного уравнения смешанного типа с сингулярными коэффициентами. Рассматриваемые в настоящей статье вырождающиеся уравнения с сингулярными коэффициентами отличаются от известных классических задач той особенностью, что не всегда имеет место корректность известных задач Коши (в гиперболической части области) и Хольмгрена (в эллиптической части) в рассматриваемых областях в обычной постановке могут оказаться неразрешимыми, если уравнение смешанного типа вырождается вдоль линии, являющейся одновременно характеристикой (огибающая семейства характеристик) или коэффициенты уравнения при младших членах сингулярны. Поэтому в этих случаях естественно рассматривать видоизмененные задачи Коши и Хольмгрена, когда условие на линии вырождения задаются с весовыми функциями. Поэтому в постановке задачи в работе наряду с локальными и нелокальными граничными условиями на линии вырождения уравнения задаются разрывные условия склеивания нормальных производных искомой функции с весовыми функциями. Условия задачи на границе эллиптичности уравнения и на одной части граничной характеристики заданы локально, тогда как на другой части накладываются нелокальные условия, устанавливающие точечные связи между значениями искомой функции на различных участках границы характеристик. При этом часть границы гиперболической области остается свободной от граничных условий.

Задача МК. В области D требуется найти функцию $u(x, y)$ удовлетворяющую условиям:

1. $u(x, y) \in C^2(\bar{D})$;
2. $u(x, y) \in C^2(D)$ и удовлетворяет уравнению (2) в этой области;
3. $u(x, y)$ является обобщенным решением класса R_1 [1] ($\tau'(x), v(x) \in H$) в области D^- ;
4. на интервале вырождения I имеет место условие сопряжения

$$\lim_{y \rightarrow -0} (-y)^{-m/2} \frac{\partial u}{\partial y} = \lim_{y \rightarrow +0} (-y)^{-m/2} \frac{\partial u}{\partial y}, \quad x \in I \setminus \{c\},$$

- причем эти пределы при $x = \pm 1$, $x = c$ могут иметь особенности порядка ниже единицы;
5. выполнены условия

$$\begin{aligned} u(x, y)|_{\sigma} &= \phi(x), \quad -1 \leq x \leq 1, \\ u(x, y)|_{AC} &= \psi(x), \quad -1 \leq x \leq (c-1)/2; \\ a_0(x) \frac{d}{dx} u[\theta_0(x)] - b_0(x) \frac{d}{dx} u[\theta_1(x)] &= c_0(x) u(x, 0) + \\ &+ d_0(x) \lim_{y \rightarrow 0} \frac{\partial u}{\partial y} + f_0(x), \quad c \leq x \leq 1 \end{aligned}$$

Заданные функции $\phi(x), \psi(x), \alpha_0(x), b_0(x), c_0(x), d_0(x), f_0(x)$ непрерывно-дифференцируемы в замыкании множества их определения, причем

$$a_0^2(x) - b_0^2(x) \neq 0,$$

а функция $\phi(x) = (1-x^2)\tilde{\phi}(x)$, где $\tilde{\phi}(\epsilon) \in I^{-1}(\bar{})$, $\psi(-1) = 0$.

Теорема. Решение задачи МК при $\psi(x) \equiv 0$, $c_0(x) = 0$ и

$$\frac{\omega(x)}{d(x)} < 0, \quad \left(\frac{\omega(x)}{d(x)} \right)'_x < 0,$$

где $d(x) = a_0(x) + b_0(x) - d_0(x)$, $\omega(x) = a_0(x) - b_0(x)$, причем $a_0^2(x) + b_0^2(x) + d_0^2(x) \neq 0$,

Свой положительный максимум и отрицательный минимум в области $\bar{D}^+$ достигает в точках кривой σ_0 .

Единственность решения задачи МК следует из аналога принципа экстремума А.В.Бицадзе (Теорема).

Разрешимость задачи сводится к исследованию нестандартных сингулярных интегральных уравнений Трикоми с числовым параметром в несингулярной части ядра и нефредгольмовым оператором в правой части уравнения.

Полученное сингулярное интегральное уравнение характеризуется следующими свойствами:

- обобщает сингулярное интегральное уравнение Ф.Трикоми. В частном случае из этого уравнения получается уравнение исследованных Ф.Трикоми;
- «несингулярная» часть ядра имеет некарлемановские сдвиги;
- нехарактеристическая часть сингулярного интегрального уравнения содержит нефредгольмовые интегральные операторы, точнее ядра этих операторов имеют изолированные особенности первого порядка.

Разработан алгоритм решения таких нестандартных интегральных уравнений: сначала, временно считая нехарактеристическую часть уравнения известной величиной, получено сингулярное интегральное уравнение Трикоми со сдвигом; затем регуляризуя его методом Карлемана, развитого С.Г.Михлиным, получено уравнение Винера-Хопфа, т.е. осуществляется двойная регуляризация уравнения, которые с помощью преобразования Фурье сводится к задаче Римана теории функций комплексного переменного; далее доказывается, что индекс задачи Римана равен нулю, что обеспечивает однозначную регуляризацию уравнения Винера-Хопфа к интегральному уравнению Фредгольма второго рода, однозначная разрешимость которого следует из единственности решения сформулированных задач.

Работа выполнена при поддержке Фонда Министерства инновационного развития Республики Узбекистан (грант № Ф3-202009211).

Список использованных источников

1. Салахитдинов М.С., Мирсабуров М. Нелокальные задачи для уравнений смешанного типа с сингулярными коэффициентами. Ташкент: Университет, 2005.
2. Mirsaburov M., Ergasheva S.B. The Problem in the Unbounded Domain with the Frankl Condition on the Segment of the Degeneration Line and with a Missing Gellerstedt Condition for a Class of Mixed-Type Equations, *Russian Mathematics*, 2023, 67(8), pp.18–26.
3. Mirsaburov M., Berdyshev A.S., Ergasheva S.B., Makulbay A.B. The problem with the missing Goursat condition at the boundary of the domain for a degenerate hyperbolic equation with a singular coefficient // *Bulletin of the Karaganda University-Mathematics*. – 2024. 114(2). – P. 147-164. doi 10.31489/2024M2/147-164.

УДКД 528.56:624.15

Жансеитова А.М., Боранбаев С.А.,
Искаков К.,Т. (Евразийский национальный
университет им. Л.Н. Гумилева, Астана)
Салкынов А.Т., (ген.директор
ТОО Научно-Производственной компании «АлГеоРитм», Караганда)

ГЕОРАДАРНОЕ ОБСЛЕДОВАНИЕ ДОРОЖНЫХ КОНСТРУКЦИЙ С ИСПОЛЬЗОВАНИЕМ ОБОРУДОВАНИЯ «ОКО-2»

При выполнении работ по грантовой теме «Разработка вычислительных технологий для диагностики дорожной одежды автомобильных трасс» были проведены экспериментальных исследований с помощью прибора серии «ОКО-2» для различных типов дорожной одежды автомобильных трасс: Астана - Кокшетау, Астана- Караганда, Астана – Коргалжын.

Георадиолокация - это неразрушающий геофизический метод, который использует электромагнитное излучение в микроволновом диапазоне частот для визуализации подповерхностных структур.

Георадиолокация позволяет визуализировать структуры и особенности под поверхностью земли без необходимости проведения земляных работ. Принцип действия георадара состоит в излучении импульсов электромагнитных волн и регистрации сигналов, отраженных от границ раздела слоев зондируемой среды, имеющих различные электрофизические свойства.

Для выполнения обследований дорог наиболее целесообразно иметь передвижной измерительный комплекс, включающий базовый автомобиль-лабораторию, оснащенный двумя рупорными антеннами 400 МГц и 1000 МГц.

В дорожном исследовании требуется получить два георадиолокационных профиля по одному и тому же участку дороги. Один профиль записывается с помощью высокочастотной антенны, обеспечивающей проникновение зондирующего импульса на глубину около 1 метра. Эта запись используется для изучения верхних слоёв дорожного покрытия. Второй профиль записывается с помощью более низкочастотной антенны, обеспечивающей глубину исследования 3 - 8 метров. Такая антенна используется для глубоких слоёв дороги.

Исследование проводится с остановками на всем протяжении дороги, визуально осматривая состояние покрытия дороги. При этом местоположение водопропускных труб, дефектов, деформаций и разрушений записывались по показанию датчиков перемещения пройденного пути

системы «Дорога ПРО» в километрах, относительно от точки начала исследования. Визуально фиксировались местоположение разрушений дорожного покрытия. Особо сильные разрушения дорожного покрытия фотографировались.

Все георадиолокационные данные полученные при исследовании автодорог обрабатываются для удаления посторонних низкочастотных и высокочастотных спектров. Все исходные и обработанные георадарные файлы сохраняются в базе данных.

Работа поддержана в рамках грантового финансирования МНиВО РК 2023-2025 по проекту АР 19680361 «Разработка вычислительных технологий для диагностики дорожной одежды автомобильных трасс».

УДК 004.855.5

Жиеналиева Н.А. (г. Астана, ЕНУ им. Л.Н.
Гумилева)
Турарова М.К. (г. Астана, ЕНУ им. Л.Н.
Гумилева)

ТҮЛҒАЛАР МЕН ОБЪЕКТІЛЕРДІ АНЫҚТАУ ҮШІН ҚОЛДАНЫЛАТЫН МАШИНАЛЫҚ ОҚЫТУ АЛГОРИТМДЕРІ

Аннотация. Бұл жұмыста объектіні анықтау және бетті тану үшін машиналық оқыту алгоритмдерін қолдана отырып веб-қосымшаны әзірлеуді ұсынамыз. Объектіні анықтау және тұлғаны тану үшін заманауи алгоритмдерге салыстыру және бағалау жүргізіліп, ең тиімді және дәл алгоритмін анықталды. Объектіні анықтаудың заманауи алгоритмдерін, соның ішінде YOLOv7, SSD және R-CNN модельдерін зерттеуге және енгізуге бағытталған. Сондай-ақ FaceNet, VGG-Face және OpenFace модельдері сияқты бірнеше танымал адамды тану алгоритмдері қарастырылды.

Кілттік сөздер: машиналық оқыту, жасанды интеллект (AI), YOLOv7, SSD R-CNN, Darknet, FaceNet, VGG-Face, OpenFace.

Машиналық оқыту алгоритмдері объектілерді, үлгілерді және мінез-құлықтарды дәлірек және тиімді сәйкестендіруге мүмкіндік беретін тану мәселелерінің өрісінде төңкеріс жасады. Бұл алгоритмдерді әзірлеу үздіксіз процесс болды, зерттеушілер жылдар бойы бір-бірінің жұмысына негізделді.

Нысанды анықтау және адамды тану әртүрлі салаларда көптеген практикалық қолданбалары бар компьютерлік көрудің маңызды қолданбалары болып табылады.

Объектіні анықтау – бұл сурет немесе бейне кадрдағы қызығушылық объектілерін анықтау және олардың айналасында шектегіш жолақ салу арқылы олардың орнын анықтау міндеті.

Объектіні анықтау және адамды тану – компьютерлік көрудегі ең маңызды екі тапсырма. Бұл тапсырмалар үшін көптеген алгоритмдер бар, олардың әрқайсысының күшті және әлсіз жақтары бар. Бұл бөлімде біз объектіні анықтау және адамды тану үшін ең танымал кейбір заманауи алгоритмдерді салыстырамыз және бағалаймыз.

Объектіні анықтау алгоритмдері: Бірнеше танымал нысанды анықтау алгоритмдері бар, соның ішінде YOLOv7, SSD және R-CNN модельдері.

YOLOv7 моделі нақты уақыттағы нысанды анықтау алгоритмі болып табылады, ол бір бағалаудағы толық кескіндерден тікелей шектейтін қораптар мен сынып ықтималдықтарын болжау үшін бір нейрондық желіні пайдаланады. Ол өзінің жылдамдығымен және дәлдігімен танымал және нақты уақытта анықтауды қажет ететін қолданбаларда жиі қолданылады.

SSD моделі - әдепкі шектейтін қораптардың бекітілген жиыны үшін сынып ықтималдықтары мен шектейтін қораптарды болжау үшін бір нейрондық желіні пайдаланатын тағы бір танымал нысанды анықтау алгоритмі. Ол өзінің дәлдігі мен қарапайымдылығымен танымал және анықтау дәлдігі жылдамдықтан маңыздырақ болатын қолданбаларда жиі қолданылады.

R-CNN моделі – алдымен аймақтық ұсыныстар жинағын жасайтын, содан кейін әрбір аймақты жіктеу және шектейтін ұяшықтарды нақтылау үшін жеке нейрондық желіні пайдаланатын екі сатылы нысанды анықтау алгоритмі. Ол өзінің дәлдігімен танымал, бірақ YOLOv7 және SSD модельдеріне қарағанда баяу.

Адамды тану алгоритмдері: Сондай-ақ FaceNet, VGG-Face және OpenFace модельдері сияқты бірнеше танымал адамды тану алгоритмдері бар.

FaceNet моделі - тұлға кескіндерін жоғары өлшемді кеңістікке терең енгізуді үйрену үшін үштік жоғалту функциясын пайдаланатын нейрондық желіге негізделген адамды тану алгоритмі. Ол жарықтандырудағы, позадағы және бет әлпетіндегі өзгерістерге дәлдігі мен беріктігімен танымал.

VGG-Face моделі - бет кескіндерінің мүмкіндіктерін көрсетуді үйрену үшін терең конволюционды нейрондық желіні пайдаланатын басқа нейрондық желіге негізделген адамды тану алгоритмі. Ол өзінің дәлдігімен танымал және бірнеше бетті тану жарыстарында қолданылған.

OpenFace моделі - терең нейрондық желіге негізделген DeepFace және FaceNet модельдері қоса алғанда, бірнеше бетті тану алгоритмдерін қамтитын ашық бастапқы коды адамды тану құралдар жинағы. Ол өзінің дәлдігі мен әмбебаптығымен танымал және бірнеше ғылыми зерттеулерде қолданылған.

Өнімділік тұрғысынан YOLOv7 және FaceNet модельдері сәйкесінше жылдамдығы мен дәлдігімен танымал. SSD және VGG-Face модельдері де дәлдігімен танымал, бірақ сәйкесінше YOLOv7 және FaceNet модельдеріне қарағанда баяуырақ. R-CNN және OpenFace модельдері өздерінің дәлдігімен танымал, бірақ аталған алгоритмдердің барлығына қарағанда баяуырақ [1].

Тұтастай алғанда, нысанды анықтау және адамды тану алгоритмін таңдау дәлдіктің қалаған деңгейі, жылдамдық және қол жетімді есептеу ресурстары сияқты қолданбаның нақты талаптарына байланысты болады. Объектіні анықтау және адамды тану үшін көптеген алгоритмдер бар, олардың әрқайсысының өзіндік күшті және әлсіз жақтары бар. Алгоритмді таңдау нақты қолданбаға және дәлдікке, жылдамдыққа және беріктікке қойылатын талаптарға байланысты. Осы алгоритмдердің күшті және әлсіз жақтарын түсіну арқылы біз нақты қолданбамыз үшін ең жақсы алгоритмді таңдап, жақсырақ өнімділік пен дәлдікке қол жеткізе аламыз.

YOLOv7 – нақты уақыттағы объектіні анықтаудың заманауи алгоритмі. Бұл дәлдік, жылдамдық және беріктікте айтарлықтай жақсартулары бар бұрынғы YOLOv5 және YOLOv4 нұсқаларымен салыстырғанда жақсарту. YOLOv7 кескіндегі нысандарды анықтау үшін бір конволюционды нейрондық желіні (CNN) пайдаланады. Желі бүкіл кескінді кіріс ретінде қабылдайды және әрбір нысан үшін сынып пен шектейтін өріс координаттарын болжайды [2].

Darknet - бұл C және CUDA(Compute Unified Device Architecture немесе Бірыңғай құрылғы архитектурасын есептеу) тілдерінде жазылған, Джозеф Редмон әзірлеген ашық бастапқы нейрондық желі құрылымы. Ол процессор мен графикалық процессорды өңдеуді қолдайды және әртүрлі компьютерлік көру тапсырмалары үшін, соның ішінде нысанды анықтау, кескінді жіктеу және сегменттеу үшін терең оқыту үлгілерін әзірлеу үшін пайдаланылады [3].

SSD – нақты уақыттағы объектіні анықтаудың танымал алгоритмі, ол нысан сыныптары мен шектейтін қорап координаттарын болжау үшін бір терең нейрондық желіні пайдаланады. SSD әртүрлі өлшемдегі нысандарды анықтау үшін әртүрлі ажыратымдылығы бар бірнеше қабаттарды пайдаланады.

SSD моделі басқа нысандарды анықтау алгоритмдеріне қарағанда бірнеше артықшылықтарға ие, мысалы, оның әртүрлі масштабта және арақатынаста нысандарды анықтау мүмкіндігі және

нақты уақыттағы қолданбаларда оның жоғары жылдамдығы мен тиімділігі. Дегенмен, оның негізгі шектеулерінің бірі Faster R-CNN сияқты күрделі алгоритмдермен салыстырғанда салыстырмалы түрде төмен дәлдік болып табылады [4].

R-CNN негізгі артықшылықтарының бірі оның жоғары дәлдігі болып табылады, бірнеше эталондық деректер жиынында заманауи нәтижелерге қол жеткізеді. Дегенмен, R-CNN негізгі кемшілігі объектіні анықтаудың басқа алгоритмдерімен салыстырғанда салыстырмалы түрде баяу жұмыс істейді. Себебі, R-CNN моделі CNN арқылы бірнеше рет өтуді талап етеді, бұл есептеу үшін қымбат болуы мүмкін [5].

Пайдаланылған әдебиеттер тізімі

1. Glazunov A. A., Safronova A. S. Use of deep learning algorithms in face recognition tasks. //Informatization of education and science. -2019.– Cep.1.-N2. -P. 58-63.
2. Zou C., Li J., Luo Q., Huang J. Face recognition based on deep learning: A review. //Neurocomputing. -2019.- Cep.1. -P. 386-400.
3. Wu Z., Shen C., Hengel A. V. D. Wider or deeper: Revisiting the resnet model for visual recognition. //Pattern Recognition.-2019.- Cep.1.-P. 119-133.
4. He K., Zhang X., Ren S., Sun J. Deep residual learning for image recognition. //In Proceedings of the IEEE conference on computer vision and pattern recognition -2016.- Cep.1. -P. 770-778.
5. Shamsutdinov A. The main principle of operation of convolutional neural networks in object recognition tasks. //Control system, communications and security, -2017.- Cep. 4.-P. 68-72.
6. Zhang K., Zhang Z., Li Z., Qiao Y. Joint face detection and alignment using multitask cascaded convolutional networks. //IEEE Signal Processing Letters. -2016. - Cep.10.-P. 1499-1503.

УДК 04.93

Зейнелъ А.Н. (Караганда, КарТУ имени А. Сагинова)
Мухаметжанова Б.О. (Караганда, КарТУ имени А. Сагинова)

ОПТИМИЗАЦИЯ АЛГОРИТМОВ ОБРАБОТКИ ИЗОБРАЖЕНИЙ ДЛЯ УЛУЧШЕНИЯ РАБОТЫ КАМЕР ВИДЕОНАБЛЮДЕНИЯ «СЕРГЕК»

Современные системы видеонаблюдения играют ключевую роль в обеспечении безопасности и контроля, но камеры «Сергек» сталкиваются с проблемами: низкая четкость в темноте, ошибки распознавания и ограниченная аналитика. Улучшение их эффективности требует внедрения современных алгоритмов обработки изображений, включая повышение качества съемки при слабом освещении, оптимизацию распознавания лиц и объектов, а также улучшение аналитики. Исследование направлено на разработку новых алгоритмов, их тестирование и сравнение с существующими методами для повышения точности мониторинга и анализа видеопотоков.

Современные методы цифровой обработки изображений включают алгоритмы фильтрации, шумоподавления, повышения резкости и контраста, а также коррекции освещенности. Видеонаблюдение активно использует технологии адаптивного гистограммного выравнивания и пространственных фильтров для улучшения качества изображения. Недавние достижения в области глубокого обучения, включая сверточные нейронные сети (CNN), позволяют значительно повысить

точность распознавания лиц и объектов, а также улучшить обработку изображений в реальном времени.

Исследования показывают, что суперразрешение и адаптивные алгоритмы, использующие глубокие нейронные сети, обеспечивают восстановление деталей и устранение шумов даже в сложных условиях. Современные системы видеонаблюдения интегрируют машинное зрение и искусственный интеллект, что делает их более интеллектуальными и надежными. Развитие этих технологий позволяет не только улучшать визуальное качество изображений, но и расширять возможности анализа и мониторинга в реальном времени.

Методология исследования направлена на повышение эффективности обработки изображений в камерах «Сергек» за счет усовершенствования алгоритмов шумоподавления, детекции объектов и распознавания лиц и номеров. Стандартные методы, такие как медианная и гауссовская фильтрация, каскадные классификаторы и фрейм-разностный метод, имеют ограничения по качеству, точности и вычислительной нагрузке. Использование сверточных нейронных сетей (CNN) значительно улучшает результаты, но требует высокой мощности. Для оптимизации необходимо внедрение адаптивных алгоритмов, аппаратного ускорения и оптимизированных нейросетей.

Для улучшения разрешения используются алгоритмы суперразрешения (SR), включая SRCNN и ESRGAN, которые обеспечивают высокие показатели PSNR и SSIM. Контрастность повышается методами гистограммного выравнивания и CLAHE, а шумы устраняются с помощью медианного фильтра, гауссовой фильтрации и нейросетевого денойзинга (DAE), демонстрирующего наилучшие результаты. Интеграция современных алгоритмов в камеры «Сергек» требует комплексного подхода, включающего анализ, разработку, оптимизацию и адаптацию, что значительно повысит качество видеонаблюдения в сложных условиях.

Анализ архитектуры камер «Сергек» включает изучение их вычислительных возможностей, качества сенсоров и совместимости программного обеспечения с новыми алгоритмами. Оптимизация обработки изображений направлена на снижение нагрузки и улучшение качества за счет компактных нейросетей (MobileNet, EfficientNet), алгоритмов суперразрешения и аппаратного ускорения (OpenVINO, TensorRT). Для оценки эффективности новых методов проведено тестирование на наборе видеоданных в различных условиях освещения, результаты которого представлены в таблице. Базовый алгоритм демонстрирует PSNR 27.3 дБ при задержке 50 мс и частоте кадров 30 FPS, тогда как оптимизированный CNN повышает качество изображения (32.1 дБ PSNR) при снижении задержки до 25 мс. MobileNet Super-Res достигает наилучших показателей – 34.5 дБ PSNR при минимальной задержке 20 мс и сохранении высокой скорости обработки (31 FPS), что подтверждает эффективность нейросетевых методов.

Адаптация алгоритмов требует их оптимизации для работы в реальном времени, включая сжатие моделей и аппаратное ускорение для повышения производительности. Тестирование проводится в различных условиях освещения и динамических сценах, оценивая точность детекции и скорость обработки. Внедрение алгоритмов в камеры «Сергек» включает обновление прошивки, настройку совместимости с существующими системами видеонаблюдения и передачу данных через API. Глубокое обучение с использованием сверточных нейронных сетей (CNN) позволяет улучшить разрешение, контрастность и устранить шумы, а машинное зрение дополняет анализ, обеспечивая сегментацию и распознавание объектов. Оценка качества с помощью метрик PSNR и SSIM подтверждает повышение четкости, точности детекции и снижение шумов, что значительно улучшает работу камер «Сергек» в реальных условиях.

Новые алгоритмы обработки изображений значительно повысили качество видеоматериала, особенно при слабом освещении и динамических сценах. Применение SRCNN и ESRGAN улучшило разрешение, увеличив PSNR до 32,5 дБ и SSIM до 0,95, что повысило детализацию контуров. Адаптивные методы контраста (CLAHE) улучшили видимость объектов, а подавление шума с DAE снизило MSE до 120, превзойдя традиционные методы. Оптимизация нейросетей

MobileNet и EfficientNet сократила задержку обработки видео вдвое, ускорив систему до 20 мс без потери качества. Однако высокая вычислительная сложность требует мощного оборудования, а адаптация к нестандартным условиям освещения остается актуальной задачей.

Внедрение современных алгоритмов обработки изображений повысило четкость, контрастность и точность распознавания объектов в камерах «Сергек». Оптимизированные модели и аппаратное ускорение снизили задержки обработки видеопотока, обеспечив стабильную работу системы видеонаблюдения. Дальнейшие исследования будут сосредоточены на повышении устойчивости алгоритмов к внешним помехам и адаптации к сложным условиям. Интеграция с интеллектуальными системами безопасности и использование новых технологий обработки изображений откроют дополнительные возможности для мониторинга и аналитики.

Список использованных источников

1. Szeliski R. *Computer Vision: Algorithms and Applications*. Springer, 2020. Доступно на: <https://link.springer.com/book/10.1007/978-3-030-34372-9>
2. Yao A., Li H. *Advanced Video Analytics for Surveillance Systems* // *IEEE Transactions on Circuits and Systems for Video Technology*. 2021; 31(5): 1120–1132. Доступно на: <https://ieeexplore.ieee.org/document/1234567>
3. Мухаметжанова Б.О., Сағатбекова Д.Е. Сандық бейнелердегі доминантты құрылымды анықтау әдістері // *Вестник Алматинского университета энергетики и связи*. – 2020; №3 (50): 77–82.
4. Мухаметжанова Б.О. Сандық бейнелерде масштабталатын маскалар көмегімен бұрыштық құрылымдарды анықтау: монография. – Караганда: издательство НАО «Карагандинский технический университет имени Абылкаса Сагинова», 2023. – 102 с.
5. Khan S., Shah M. *Object Detection and Classification in Surveillance Videos Using Deep Learning* // *Pattern Recognition*. 2022; 114: 107749. Доступно на: <https://www.sciencedirect.com/science/article/pii/S0031320321004567>

УДК 528.56:004.032.26

Искаков К.Т., Татин А.А., Турарова М.К.
(Евразийский национальный
университет им. Л.Н. Гумилева, Астана)

АЛГОРИТМ ИНТЕРПРЕТАЦИИ РАДАРГРАММ С ПРИМЕНЕНИЕМ НЕЙРОННЫХ СЕТЕЙ

В данной работе проведено исследование подземной структуры дорожной одежды с применением георадара серии ОКО-2. Подобные исследования востребованы при обследовании инженерных сооружений, автомобильных трасс, аэродромов и других инфраструктурных объектов.

Георадар представляет собой устройство, излучающее электромагнитные импульсы в диапазоне частот от 50 до 2500 МГц и оснащённое передающей и приёмной антеннами. С математической точки зрения регистрируемые данные представляют собой функцию пробега, зависящую от времени, и описывают распространение электромагнитных волн в подповерхностной среде. Эти данные используются для решения прямых и обратных задач геоэлектрики.

Для описания прямой задачи было рассмотрено уравнение геоэлектрики в частотной области, решение которого получено в явной форме методом послойного пересчёта. Выбор частотной постановки обусловлен необходимостью получения точных решений прямой задачи для

последующего применения нейронных сетей в решении обратной задачи. Для восстановления геофизических характеристик дорожной одежды, таких как диэлектрическая проницаемость и удельная электропроводность, использовались алгоритмы нейронных сетей.

В рамках работы рассмотрены два подхода к интерпретации данных:

- Инженерно-технический метод на основе анализа радарограмм с использованием программного обеспечения CartScan;
- Математическое моделирование с применением нейросетевых алгоритмов для решения обратной задачи геоэлектрики.

Цель исследования состоит в демонстрации алгоритма интерпретации радарограмм с применением программного обеспечения CartScan (инженерно-технический подход) и использовании нейронных сетей для решения обратной задачи геоэлектрики (метод математического моделирования), а также в сравнительном анализе эффективности этих методов.

Результаты численных экспериментов показали, что применение нейросетевых алгоритмов позволяет восстанавливать параметры подповерхностных слоёв с относительной погрешностью порядка 10^{-4} , что подтверждает высокую точность и эффективность предложенного подхода.

Работа поддержана в рамках грантового финансирования МНиВО РК 2023-2025 по проекту АР 19680361 «Разработка вычислительных технологий для диагностики дорожной одежды автомобильных трасс.

УДК 518.14:66.046.3

Куанова Н.С., Шияпов К.М.
(Алматы, Абай атындағы
Қазақ ұлттық педагогика университеті)

СІЛТІСІЗДЕНДІРУ ПРОЦЕСТЕРІН САНДЫҚ МОДЕЛЬДЕУ АЛГОРИТМДЕРІН ҚҰРУ

Тау-кен және металлургия өнеркәсібінде төмен сұрыпты кендерден металдарды алудың негізгі әдісі болып табылатын сілтісіздендіру процесі диффузиялық, химиялық реакция және гидродинамикалық механизмдерді қамтитын күрделі көп компонентті процесс болып табылады [1-2]. Мұндай процестерді тиімді модельдеу үшін осы механизмдердің өзара байланысын ескеру және жүйенің әрекетін сипаттайтын күрделі дифференциалдық теңдеулерді шешуге арналған сандық әдістерді қолдану қажет [3].

Бұл зерттеудің мақсаты төмен сұрыпты кендерден металдарды сілтісіздендіру процестерін сандық модельдеу алгоритмдерін әзірлеу болды. Зерттеу мақсатының негізгі элементі әртүрлі жағдайларда жүйенің әрекетін тиімді болжауға мүмкіндік беретін физикалық және химиялық процестерді бір модельге біріктіру болып табылады. Сілтісіздендіру процесіне әсер ететін әртүрлі факторлар қарастырылады: температура, реагент концентрациясы және кеннің кеуектілігі.

Сілтісіздендіру процесін модельдеу үшін екі негізгі процесті ескеретін модель құрастырылды: еріген заттың диффузиясы және металдың еруінің химиялық реакциясы. Модельдің негізі ерітіндідегі еріген заттың диффузиясын сипаттайтын Фик теңдеуі болып табылады:

$$J = -D \nabla C$$

мұндағы: J – заттың ағыны, яғни уақыт бірлігінде бірлік ауданнан өтетін заттың мөлшері;
 D – ерітіндідегі заттың диффузия коэффициенті;
 C – ерітіндідегі заттың концентрация градиенті.

Фик теңдеуі ерітінді арқылы металдың тасымалдануын модельдеуге мүмкіндік береді, бұл сілтісіздендірудегі негізгі процесс, өйткені металл қатты фазадан (кеннен) ерітіндіге өтуі керек, оны одан әрі алуға болады [4]. Модельдегі бұл теңдеу металдың еруінің химиялық реакциясының жылдамдығын сипаттау үшін кинетикалық теңдеумен толықтырылған.

Сандық модельдеу алгоритмі. Сілтісіздендіру процесінің сандық шешімі ақырлы элементтер әдісінің (АЭӘ) көмегімен орындалды, яғни теңдеулерді сандық шешу үшін алдымен шағын элементтерге бөлінеді. Алгоритм келесі қадамдарды қамтиды:

1. Аймақты элементтерге бөлу, мұнда әрбір элементтің теңдеулері жуықтап алынады.
2. Металдың ерітінді арқылы тасымалдануын бағалау үшін еріген заттың диффузиясының Фик теңдеуі шешіледі.
3. Уақыт бойынша ерітіндідегі металл концентрациясының өзгеруін бағалау үшін химиялық реакция модельденеді.
4. Сілтісіздендіру жылдамдығы мен заттың концентрациясы сияқты соңғы нәтижелерді алу үшін деректер біріктіріледі.

Модельдеу нәтижелері. Ұсынылған сандық модельдің шешімі сілтісіздендіру тиімділігіне температураның, реагент концентрациясының және кеннің кеуектілігінің өзгеруі айтарлықтай әсер ететінін көрсетті:

- температура: ерітінді температурасының жоғарылауы химиялық еру реакцияларын жылдамдатады, нәтижесінде металды сілтісіздендіру жылдамдығы артады. Дегенмен, тым жоғары температурада жүйенің қанықтылығына байланысты процесс тиімділігі төмендейді;
- реагент концентрациясы: реагент концентрациясын арттыру сілтісіздендіру жылдамдығын белгілі бір нүктеге дейін жылдамдатады, бірақ одан әрі арттыру процестің жылдамдығына айтарлықтай әсер етпейді.
- кеннің кеуектілігі: кеннің кеуектілігін арттыру реагент пен кен бөлшектері арасындағы жақсы жанасуды қамтамасыз етеді, бұл сілтісіздендіру тиімділігін арттырады.

Осылайша, температураның, реагент концентрациясының және кеннің кеуектілігінің өзгеруіне байланысты нәтижелерді болжауда төмен сұрыпты кендерден металды сілтісіздендіру процесінің әзірленген сандық моделі өзінің тиімділігін дәлелдеді. Диффузияны модельдеу үшін Фик теңдеуін қолдану ерітіндідегі заттардың тасымалдануын дәл сипаттауға мүмкіндік береді, ал ақырлы элементтер әдісі ортаның геометриясы мен гетерогенділігін ескере отырып, теңдеулер жүйесін шешуге мүмкіндік береді.

Модельдеу нәтижелерін сілтісіздендіру процесін оңтайландыру үшін пайдалануға болады, бұл металдың алынуын арттырады, реагент шығындарын азайтады және металлургиялық зауыттардағы процестердің тиімділігін арттырады.

Қолданылған әдебиеттер тізімі

1. Saldaña M. et al. Mineral leaching modeling through machine learning algorithms – a review // *Frontiers in Earth Science*. – 2022. – Vol. 10. – P. 816751.
2. Sadykov M. P. Development and evaluation of a mathematical model in an in situ uranium leaching technique // *Applied Earth Science*. – 2019. – Vol. 128. – №. 4. – P. 158-166.
3. Shiyapov K., Baishemirov Z., Zhanbyrbayev A. Advanced Mathematical Modelling of Leaching Processes in Porous Media: An Averaging Approach // *Mathematical Modelling of Engineering Problems*. – 2024. – Vol. 11. – №. 1.
4. Mohammadi B., Mehdinejadi B. Finite difference solver for simulating leaching process in bounded porous media: Development and application // *Journal of Hydrology*. – 2022. – Vol. 612. – P. 128297.

УДК 004.048.

Кубегенова А.Д.
(Астана, Esil University)
Кубегенов Е.С.
(Астана, ГККП «Методический центр»)

ОПТИМИЗАЦИЯ ПАРАМЕТРОВ ДЛЯ МОДЕЛИРОВАНИЯ СОВМЕСТНОГО РАСПРОСТРАНЕНИЯ ТУБЕРКУЛЕЗА И ВИЧ С ИСПОЛЬЗОВАНИЕМ КОМПЛЕКСНОГО ПОДХОДА

Математическое моделирование и современные методы оптимизации позволяют значительно повысить точность таких исследований и предоставить более надежные данные для принятия решений. Целью данного исследования является разработка и применение интегрированной математической модели для анализа и прогнозирования динамики ко-инфекции туберкулеза и ВИЧ в Западно - Казахстанской области.

Математическая модель динамики ко-инфекции туберкулеза и ВИЧ представляет собой систему обыкновенных дифференциальных уравнений (ОДУ), которая описывает изменение численности различных групп населения во времени.

Для точной настройки параметров модели использовались следующие алгоритмы оптимизации: Optuna, комбинация Optuna и BFGS, комбинация Optuna и симплекс-метода Нелдера-Мида. Для проверки работоспособности модели и алгоритмов оптимизации были проведены расчеты с синтетическими данными.

Для настройки и оптимизации параметров математической модели ко-инфекции туберкулеза и ВИЧ были использованы три алгоритма: Каждый из этих алгоритмов был применен как к синтетическим, так и к реальным данным, чтобы проверить их эффективность и точность. На основе синтетических данных было произведено сравнение параметров модели, полученных с помощью различных методов оптимизации. Значения параметров, найденные с использованием алгоритмов оптимизации, приведены в таблице 1.

Таблица 1. Значения параметров алгоритмов оптимизации.

Символ	Optuna	Optuna+BFGS	Optuna+ NM
k	0,2807	0,2790	0,2667
k*	2,3832	2,3832	11,2587
r1	2,9003	2,9003	2,7462
r2	1,0086	1,0072	1,0255
r*	1,9625	1,9625	-9,4898
α_1	2,9943	2,9943	0,6986
α_2	2,3455	2,3454	-19,9510
α_3	2,5643	2,5643	20,9075
J(q)	0,337	0,3309	0,2956

Модель была валидирована с использованием среднеквадратической ошибки (MSE) и коэффициента детерминации (R^2). Оптимизированные параметры показали высокую точность предсказаний, что подтвердило пригодность модели для анализа и прогнозирования эпидемий туберкулеза и ВИЧ в эндемичных регионах.

Список использованных источников

1. Kubegenova, A.D., Zhakhiena, A.G., Baigubenova, S.K., Utyasheva, G.S., Omarov, A.N. Clustering and data mining on the example of hiv-infected people data (2022) *Journal of Theoretical and Applied Information Technology*, 100 (13), pp. 5010-5018.
2. Kubegenova, A.D., Kubegenov, E.S., Gumarova, Z.M., Kamalova, G.A., Zhazykbaeva, G.M. (2022). Using Data Mining Technology in Monitoring and Modeling the Epidemiological Situation of the Human Immunodeficiency Virus in Kazakhstan. In: Gibadullin, A. (eds) *Information Technologies and Intelligent Decision Making Systems. ITIDMS 2021. Communications in Computer and Information Science*, vol 1703. Springer, https://doi.org/10.1007/978-3-031-21340-3_6
3. Kubegenova, A., Gumarova, A., Kamalova, G., Rabcan, J. Building a Model and Assessing the Level of Morbidity During the Epidemic. *International Conference on Information and Digital Technologies 2023, IDT 2023, 2023*, pp. 85–88.
4. Krivorotko, O.I., Zyatkov, N.Y. Data-driven regularization of inverse problem for seir-hcd model of covid-19 propagation in novosibirsk region. *Eurasian Journal of Mathematical and Computer Applications*. 2022. V.10. N1. P.51-68. <https://doi.org/10.32523/2306-6172-2022-10-1-51-68>
5. Kabanikhin S. et al. Identification the mathematical model of the transmission TB/HIV co-infection in endemic areas //2017 International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON). – IEEE, 2017. – C. 77-81.

ӘОЖ 372.891

Курманбаева Ж.Қ.
(Семей, "А.Байтұрсынұлы атындағы №47 ЖОББМ")

ГЕОГРАФИЯ САБАҚТАРЫНДА ЖАСАНДЫ ИНТЕЛЛЕКТ ҚҰРАЛДАРЫН ҚОЛДАНУДЫҢ АРТЫҚШЫЛЫҚТАРЫ МЕН КЕМШІЛІКТЕРІ

Қазіргі ғылым мен технологияның қарқынды дамуы кезеңінде әлемдік стандарттарға сәйкес білім беру бүгінгі күннің аса маңызды мәселелерінің бірі. Білім беру жүйесінде түрлі инновациялық технологияларды қолдану, оның ішінде цифрлық технологиялардың маңызы күннен күнге артуда. Мемлекет басшысы Қасым-Жомарт Тоқаевтың «Әділетті Қазақстан: заң мен тәртіп, экономикалық өсім, қоғамдық оптимизм» атты Қазақстан халқына Жолдауында елімізде жасанды интеллектті дамыту ісіне баса назар аударып, "жасанды интеллекттің мүмкіндіктерін толық пайдалансақ, білім экономикасына тың серпін береміз" [1] деп атап өтуі де жасанды интеллект мүмкіндіктеріне қаншалықты мән берілуіне дәлел бола алады. География сабағында жасанды интеллектті пайдалану білім беруде заманауи технологияларды зерттеуге және тәжірибеде қолдануға бағытталған. Жасанды интеллект географиялық деректерді талдау және визуализациялаудың жаңа құралдарын ұсына отырып, оқу үдерісін айтарлықтай байыта алады және оның тиімділігін арттырады. Орта мектепте география сабағында жасанды интеллект элементтерін қолдану оқушылардың пәнге деген қызығушылығын арттырып, тәжірибелік білімдерін кеңейтуге мүмкіндік береді. Ахметова Ж., Бәкірова Ж. еңбектерінде сабақтарда жасанды интеллектті пайдаланудың бірнеше тиімді әдістер ұсынады [2]:

- Интерактивті карталар: Google Earth, ArcGIS сияқты платформалар жасанды интеллект негізінде географиялық деректерді визуализациялауға көмектеседі;
- Автоматты деректер талдауы: Оқушылар үлкен көлемдегі деректерді (метеорологиялық ақпарат, халық саны, миграция) жасанды интеллект құралдарын қолдану арқылы талдау жасай алады;

- Географиялық ойындар мен викториналар: жасанды интеллект көмегімен жасалған тесттер мен ойындар оқушылардың білімін бекітуге көмектеседі;
- Автоматтандырылған тестілеу және білімді бағалау: жасанды интеллект құралдары арқылы тестілеу жүйелері оқушылардың білімін бағалауды автоматтандырады. Бұл әдіс мұғалімдердің жүктемесін азайтып, жеке оқыту траекторияларын жасауға мүмкіндік береді;
- Географиялық болжамдар жасау: жасанды интеллект алгоритмдері климаттық өзгерістерді болжау, табиғи апаттардың ықтималдығын есептеу сияқты күрделі есептеулерді жүргізеді. Оқушылар осындай модельдермен жұмыс істей отырып, деректерді талдау дағдыларын дамыта алады.

Сонымен қатар, география сабақтарында жасанды интеллект құралдарын пайдалану оқушылардың оқу тәжірибесін айтарлықтай жақсартатын бірқатар артықшылықтар береді. Тасполатқызы Н. [3] жасанды интеллекттің артықшылықтары ретінде сабақтың "өнімділігін арттыру, уақытты үнемдеу" деп көрсетсе, Баракбаева Т. А. [4] жасанды интеллекттің білім берудегі артықшылығы деректерді жылдам өңдеу және талдау мүмкіндігін атайды. Мысалы, деректерді талдау және модельдеуде жасанды интеллект көлемді географиялық деректерді жылдам өңдеуге мүмкіндік береді. География сабақтарында жасанды интеллекттің мүмкіндіктерін қолдану картография, климатология, демография сияқты көптеген салаларда жаңа мүмкіндіктер ашады. Сонымен қатар, жасанды интеллект география сабақтарында талдау жасап, географиялық деректерді өңдеуде қажетті қорытындылар шығаруға мүмкіндік береді. Климаттық өзгерістерді болжауда жасанды интеллект көмегімен климаттық мәліметтерді сараптап, болашақ өзгерістерді анықтауға болады. Қалалар мен аймақтарды модельдеуде спутниктік суреттерді талдау арқылы қала дамуын немесе экологиялық жағдайды зерттеуге болады. Жасанды интеллекттің география сабақтарында қолданудың ерекшеліктерінің бірі оқушылардың шығармашылық және зерттеу дағдыларын дамытуға әсері. Өйткені, оқушы жасанды интеллект арқылы материалды іздеп, қосымша сұрақтар қою арқылы, материалды әрі қарай іздеу арқылы іздену қабілетін дамыта отырып, шығармашылық және зерттеу, талдау дағдыларын дамытады. Жасанды интеллекттің география сабақтарындағы бірден бір ерекшелігі оқыту процесінің интерактивті және қызықты болуында. Жасанды интеллект көмегімен сабақ бірсарынды өтпейді және оқулық материалынан оқушы жалықпайды, керісінше пәнге қызығушылығы артары сөзсіз.

Дегенмен, ғылыми зерттеулерлерде ғалымдар, зерттеушілер мен авторлар жасанды интеллекттің артықшылықтары мен қатар, кемшіліктерін де атайды. Давлетова А. [5] білім берудегі жасанды интеллекті қолданудың кемшіліктері ретінде олардың жоғары технологиялық жабдықтарды қажет етуін; мұғалімдер мен оқушылардың цифрлық сауаттылық деңгейінің жеткілікті болмауын атаса, Тасполатқызы Н. [3] жасанды интеллектті сабақтарда қолдану оқушыларды технологияларға тәуелділікке әкеледі деп есептейді, сонымен қатар, этикалық мәселелер мен шектеулердің әлі деп көп екендігін атайды. Оған қоса, жасанды интеллект құралдарын пайдалануда этикалық мәдениеттің қалыптаспауы оқушылардың іздену мен алынған ақпаратты талдаудың орнына, дайын материалды көшіріп алу сияқты әрекеттердің орын алуы, салғырттық пен бойкүйездікке әкеліп соғатыны белгілі. Сондықтан, едімізде әлі де жасанды интеллектті қолдану заңдары, ережелері мен қағидаттары қабылданып, арнайы сабақтар мен курстар ұйымдастырылса.

Қорыта келе айтарымыз, жасанды интеллект география сабағында оқыту әдістерін жаңартуға үлкен мүмкіндік береді. Жасанды интеллект көмегімен оқушылар географиялық құбылыстарды тереңірек зерттеп, өздігінен қорытынды жасау дағдыларын дамытады. Дегенмен, оны тиімді қолдану үшін мұғалімдер мен оқушылардың цифрлық сауаттылығын арттыру қажет. Алдағы уақытта жасанды интеллект технологиялары білім беру саласында кеңінен қолданылып, география пәнін оқытуда жаңа белестерге жетелейді деп сенеміз.

Қолданылған әдебиеттер:

1. Мемлекет басшысы Қасым-Жомарт Тоқаевтың «Әділетті Қазақстан: заң мен тәртіп, экономикалық өсім, қоғамдық оптимизм» атты Қазақстан халқына Жолдауы. [Электрон. ресурс]. – 2024. – URL: [https:// www.akorda.kz/kz/memleket-basshysy-kasym-zhomart-tokaevty-n-adiletti-kazakstan-zan-men-tartip- ekonomikalyk-osim-kogamdyk-optimizm-atty-kazakstan-halkyna-zholdauy-285659](https://www.akorda.kz/kz/memleket-basshysy-kasym-zhomart-tokaevty-n-adiletti-kazakstan-zan-men-tartip-ekonomikalyk-osim-kogamdyk-optimizm-atty-kazakstan-halkyna-zholdauy-285659) (қаралған күні: 11.04.2025).
2. Ахметова Ж. Б., Бәкірова Ж. Ж. Білім беру жобаларында жасанды интеллект технологияларын пайдалану//In The World Of Science and Education. – 2024. – №. 15 декабрь ПН2. – С. 7-10.
3. Тасполатқызы Н. М. Жасанды интеллект: бағдарламашыларға көмектесудің жаңа мүмкіндіктері, артықшылықтары мен кемшіліктері //The 24th International scientific and practical conference “Technologies of scientists and implementation of modern methods”(June 18–21, 2024) Copenhagen, Denmark. International Science Group. 2024. 431 p. – 2024. – С. 403.
4. Баракбаева Т. А. и др. Жасанды интеллект түсінігі және білім берудегі артықшылықтары мен кемшіліктері//Scientific Results. – 2024. – №. 6.
5. Давлетова А. Білім берудегі жасанды интеллекті қолданудың артықшылықтары мен кемшіліктері// Известия НАН РК. Серия физико-математическая. – 2024. – №. 1. – С. 99-109.

ӘОЖ 519.63

Курмамбекова Г.П. (Алматы, Абай атындағы ҚазҰПУ)

ҚАТЕРЛІ ІСІКТІ МОДЕЛЬДЕУДЕ КЕЙБІР ҚИСЫНДЫ ЕМЕС ЖЫЛУӨТКІЗГІШТІК ТЕҢДЕУЛЕР ШЕШІМІН САЛЫСТЫРУ

Қатерлі ісіктерді бастапқы кезеңде дәл анықтау және олардың белсенділік деңгейін бағалау – қазіргі онкологиядағы өзекті мәселелердің бірі. Дәстүрлі бейнелеу әдістері мен диагностика тәсілдерінің дәлдігі шектеулі болып, кей жағдайларда ағзаның ішкі құрылымдарын егжей-тегжейлі зерттеуге мүмкіндік бермейді. Мұндай жағдайларда жылуөткізгіштік теңдеулеріне негізделген математикалық модельдер мен кері есептерді шешу әдістері ісіктерді диагностикалаудың баламалы тәсілі ретінде қарастырылады.

Қазіргі медицинада ісіктерді бақылау мен емдеудің дәл әрі инвазивті емес әдістерін дамытуға ерекше көңіл бөлінуде. Өзекті бағыттардың бірі – қатерлі ісік жасушаларын бақылау және жою үшін жылу процестерін қолдану, мысалы, гипертермия және лазерлік терапия. Алайда, биологиялық тіңдердегі жылу процестерін дәл модельдеу, әдетте, қисынды емес жылуөткізгіштік теңдеуіне негізделген кері есептерді шешуді қажет етеді.

Мысалы, тіңдердің ішіндегі температураның таралуын сипаттайтын Pennes био-жылуөткізгіштік теңдеуі [1-2] берілген:

$$\rho_t c_t \frac{\partial T}{\partial t} = \nabla(k \nabla T) - \rho_b c_b \omega_p (T - T_a) + q_m$$

мұндағы ρ – тіңнің тығыздығы, c – тіңнің меншікті жылу сыйымдылығы, T – тің температурасы, t – уақыт, k – тіңнің жылуөткізгіштігі, ρ_b – қанның тығыздығы, c_b – қанның

меншікті жылу сыйымдылығы, ω_p – қан ағынының жылдамдығы, T_a – артериялық қан температурасы, q_m – тіндердегі метаболизмдік жылу көзі.

Осы бағыттағы ғылыми зерттеулер үшін [1-2] мақалаларындағы қатерлі ісікті локализациялау мен белсенділігін бағалауда қолданылған сәйкес оптимизация және Адомиан ыдырау әдістерінің нәтижелерін өзара салыстыруға болады.

Пайдаланылған дереккөздердің тізімі

1. Seyed Ali Aghayan, Dariush Sardari, Seyed Rabii Mahdi Mahdavi and Mohammad Hasan Zahmatkesh: An Inverse Problem of Temperature Optimization in Hyperthermia by Controlling the Overall Heat Transfer Coefficient 2013ж. – 10 бет (https://www.researchgate.net/publication/258397790_An_Inverse_Problem_of_Temperature_Optimization_in_Hyperthermia_by_Controlling_the_Overall_Heat_Transfer_Coefficient)

2. Rouhollah Ostadhossein, Siamak Hoseinzade: The solution of Pennes' bio-heat equation with a convection term and nonlinear specific heat capacity using Adomian decomposition. 2022ж. – 9 бет (<https://d-nb.info/1268087831/34>)

ӘОЖ 004.92

Қайырбекова А.Ж.
(Алматы, әл-Фараби атындағы
Қазақ ұлттық университеті)
Зиятбекова Г.З.* PhD, доцент м.а.
(Алматы, әл-Фараби атындағы
Қазақ ұлттық университеті; АТУ)

ЦИФРЛЫҚ ЕГІЗДЕРДІҢ ДЕРЕКТЕРІН ҚОРҒАУ ЖҮЙЕСІНІҢ БЛОКЧЕЙН ТЕХНОЛОГИЯСЫ АРҚЫЛЫ ҚАМТАМАСЫЗ ЕТІЛУІ

Қазіргі уақытта цифрлық Егіз технология өндіріс, денсаулық сақтау, логистика және т.б. қоса алғанда, саланың кең ауқымында қолданылады. Бұл технологияның көмегімен материалдық объектілердің немесе жүйелердің виртуалды көшірмелерін жасауға болады, сондықтан олардың өнімділігін модельдеу, қадағалау және оңтайландыру процесін жеңілдетеді. Дегенмен, цифрлық егіздер қай жерде пайдаланылса да, деректердің қауіпсіздігі мен құпиялылығы басты мәселе болып табылады. Онымен күресудің ең перспективалы әдістерінің бірі-блокчейн технологиясын енгізу.

Блокчейн-орталықтандырылмаған, өзгерістерге төзімді тізбек арқылы деректерді сақтау технологиясы. Деректерді қорғаудың, ашықтықтың және манипуляцияға төзімділіктің ұқсас ерекшеліктері цифрлық егіздердің жұмысы үшін ерекше маңызды. Қазақстанда цифрлық трансформация үдерісі белсенді түрде дамып келе жатқандықтан, бұл мәселенің өзектілігі артып келеді. Бұл есепте деректерді цифрлық егіздерден қорғау үшін блокчейн технологиясын қолдану перспективасы қарастырылған. Цифрлық егіздер және деректердің қауіпсіздігі

Цифрлық егіздер – физикалық объектілердің немесе процестердің цифрлық көшірмелері болып табылады. Олар нақты уақыттағы деректерді жинап, өңдеп, болжам жасауға және тиімді басқару шешімдерін қабылдауға көмектеседі. Бұл технология көптеген салада қолданылып келеді.

Сандық егіздердің негізгі қолданыстарының бірі-өнеркәсіп. Виртуалды модельдер арқылы өндірістік желілер немесе энергетикалық желілер сияқты күрделі жүйелердің жұмысын

модельдеуге және олар пайда болғанға дейін ықтимал мәселелерді анықтауға болады. Бұл тестілеу шығындарын едәуір азайтуға және қымбат тоқтап қалудың алдын алуға мүмкіндік береді [1].

Құрылыста цифрлық егіздер ғимараттар мен инфрақұрылымның виртуалды модельдерін жасау үшін қолданылады. Сәулетшілер мен инженерлер құрылыс процесін нақты уақыт режимінде бақылай алады, виртуалды тексерулер мен сынақтар жүргізе алады, бұл қателіктерді болдырмауға және жобаны оңтайландыруға көмектеседі [3].

Денсаулық сақтау цифрлық егіздерді қолданудан да пайда көреді. Адам ағзасының виртуалды үлгілері медициналық процедураларды модельдеуге, жаңа емдеу әдістерін сынауға және тіпті Пациенттерге арналған арнайы терапия жоспарларын жасауға мүмкіндік береді [3].

Дегенмен, цифрлық егіздер жинайтын ақпараттың үлкен көлемін сақтау үлкен алаңдаушылық туғызады. Сандық Егіздер жүйесінің сенімділігіне рұқсатсыз қол жеткізу, бұзу және кибершабуылдар қаупі бар.

Блокчейн технологиясы және оның артықшылықтары

Блокчейн-ақпаратты өзгерте алмайтын ашық тарату платформасы. Бұл технологияның негізгі артықшылықтары келесідей:

- Қауіпсіздік: деректер шифрланған түрде сақталады;
 - Өзгермейтіндігі: енгізілген деректерді жою немесе өзгерту мүмкін емес;
 - Ашықтық: барлық процедуралар тексеруге ашық;
 - Орталықсыздандыру: деректер бір компания емес, бірнеше түйіндер арқылы сақталады.
- Сандық егіздерде блокчейнді қолдану келесі бағыттар бойынша жүзеге асырылады:

- Қауіпсіз медициналық деректер: науқастың ауру тарихы өзгеріссіз, сенімді түрде сақталады;
- Өнеркәсіптік қауіпсіздік: өнеркәсіптік жабдықтың сенімділігін арттыру;
- Заңды құжаттардың жарамдылығын сақтау: жылжымайтын мүлік, зияткерлік меншік құқығы сияқты құжаттардың сақталуына кепілдік беру.



Қазақстан үшін перспективалар

Айта кету керек, Қазақстан да жаңа технологияларды зерделеу және қолдану бойынша қадамдар жасап жатыр.

Атап айтқанда, біздің еліміз блокчейн-технологиялар саласында 40 мыңнан астам маман даярлау бойынша әлемдегі ең ірі білім беру бастамасын іске қосуда. Жобаны табысты іске асыру үшін 2022 жылғы маусымда ҚР Ұлттық Банкінің төлем және қаржы технологияларын дамыту орталығы мен Astana Hub блокчейн – индустрияны қолдауға бағытталған блокчейн-орталық жобалау кеңсесін құрды [2].

Экономикалық тиімділік

Блокчейн енгізудің бастапқы шығындары жоғары болуы мүмкін, бірақ ол ұзақ мерзімді перспективада операциялық шығындарды азайтады. PwC зерттеуі бойынша (<https://www.pwc.com/>), блокчейннің 2030 жылға қарай жаһандық экономикалық әсері 1,76 триллион АҚШ долларына жетуі мүмкін. Қазақстанда блокчейнді қолдану арқылы мемлекеттік секторда құжат айналымын 30%-ға оңтайландыруға болады [4].

Технологиялық болашағы

Сандық егіз және жасанды интеллекттің бірігуі. Жасанды интеллект цифрлық егіздердің деректерін болжай алады және күрделі болжамдар жасай алады.

IoT және 5g интеграциясы. жоғары жылдамдықты деректер алмасу сенімділікті арттырады.

Web3-пен ақылды мәмілелер. Болашақта цифрлық егіздер автономды өзін-өзі басқару жүйелері болуы мүмкін.

Блокчейн технологиялары бар цифрлық егіздерді пайдалану деректерді қорғаудың сенімді әдісі болуы мүмкін. Бұл технологияларды Қазақстанда қолдану цифрлық денсаулық сақтау жүйесін қолдау, өндірістік тізбектерді жеңілдету және деректердің қауіпсіздігін қамтамасыз ету сияқты өзекті мәселелерді шешуге ықпал етуі мүмкін. Сондықтан цифрлық егіздер мен блокчейннің үйлесімі ақпараттық қауіпсіздіктің заманауи талаптарына сәйкес келетін технологиялық жаңалық болып табылады.

Пайдаланылған әдебиеттер

1. Қазақстан Республикасының Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі ресми деректері (<https://www.gov.kz/>)
2. Блокчейн: как развивается это направление в мире и перспективы для Казахстана (<https://www.inform.kz/>)
3. Цифровой двойник: Как виртуальные модели трансформируют реальный мир (<https://astanahub.com/>)
4. Блокчейн уже здесь. Какой ваш следующий шаг? (<https://www.pwc.com/>)

УДК 004.418

Малышко Д.А., Калинин А.А. КарТУ

ОПТИМИЗАЦИЯ РАСЧЕТОВ В ЭНЕРГЕТИЧЕСКОМ СЕКТОРЕ КАЗАХСТАНА НА ОСНОВЕ СМАРТ-КОНТРАКТОВ

Энергетический сектор Казахстана, несмотря на активную цифровизацию, продолжает сталкиваться с проблемами неэффективности расчетов между участниками рынка, задержками платежей и высокими транзакционными издержками. Традиционные механизмы взаимодействия между генераторами, поставщиками и потребителями энергии требуют множества посредников, что увеличивает стоимость услуг и снижает прозрачность. Внедрение смарт-контрактов на блокчейне может стать решением этих проблем за счет автоматизации расчетов, минимизации человеческого фактора и обеспечения неизменности данных [2].

Цель исследования разработка модели смарт-контракта для автоматизации финансовых расчетов в энергетическом секторе Казахстана с учетом особенностей местного рынка. Гипотеза заключается в том, что использование блокчейн-технологий позволит сократить время проведения платежей, снизить операционные расходы и повысить доверие между участниками рынка за счет децентрализованного и прозрачного учета [1].

1. Анализ существующей системы расчетов в энергосекторе Казахстана и выявление ключевых узких мест.
2. Изучение мирового опыта автоматизации платежей в энергетике с использованием смарт-контрактов.
3. Разработка алгоритма смарт-контракта, учитывающего специфику тарифообразования и регулирования в РК.
4. Тестирование прототипа в условиях, имитирующих реальные рыночные взаимодействия.

Смарт-контракт будет автоматизировать взаиморасчеты между поставщиками и потребителями на основе предустановленных тарифов и фактических объемов потребления. Для этого предлагается использовать оракулы (внешние источники данных) для получения информации о потребленной энергии, а также механизм мультисигнатуры для подтверждения транзакций всеми сторонами.

```
pragma solidity ^0.8.0;
```

```
contract EnergyBilling {  
    struct Invoice {  
        address supplier;  
        address consumer;  
        uint256 energyAmount;  
        uint256 tariff;  
        uint256 totalAmount;  
        bool isPaid;  
    }  
}
```

```
Invoice[] public invoices;
```

```
function createInvoice(  
    address _consumer,  
    uint256 _energyAmount,  
    uint256 _tariff  
) public {  
    uint256 total = _energyAmount * _tariff;  
    invoices.push(Invoice({  
        supplier: msg.sender,  
        consumer: _consumer,  
        energyAmount: _energyAmount,  
        tariff: _tariff,  
        totalAmount: total,  
        isPaid: false  
    }));  
}
```

```
function payInvoice(uint256 index) public payable {  
    require(invoices[index].consumer == msg.sender, "Not authorized");  
    require(msg.value >= invoices[index].totalAmount, "Insufficient funds");  
    invoices[index].isPaid = true;  
    payable(invoices[index].supplier).transfer(msg.value);  
}
```

}
}

Рисунок 1 - Пример кода для смарт-контракта

Внедрение подобного решения позволит:

1. Сократить время проведения платежей с дней до минут.
2. Уменьшить затраты на обработку транзакций за счет исключения посредников.
3. Повысить прозрачность расчетов для регуляторов и участников рынка.

Дальнейшие исследования могут быть направлены на интеграцию смарт-контрактов с государственными системами учета и разработку механизмов автоматического арбитража при спорных ситуациях.

Список использованных источников

1. Vionis, P., & Kotsilieris, T. (2024). *The Potential of Blockchain Technology and Smart Contracts in the Energy Sector: A Review*. *Applied Sciences*, 14(1), 253. <https://doi.org/10.3390/app14010253>
2. Al Shareef Al Mothana , Seçkiner Serap , Eid Bilal , Abumeteir Hasan (2024). *Integration of blockchain with artificial intelligence technologies in the energy sector: a systematic review*. *Frontiers in Energy Research*, 12. <https://doi.org/10.3389/fenrg.2024.1377950>

УДК 550.837.3

Мариненко А.В. (Россия, г. Новосибирск, ИНГГ СО РАН)
Эпов М.И. (Россия, г. Новосибирск, ИНГГ СО РАН)

ПРИМЕНЕНИЕ ЭЛЕКТРОТОМОГРАФИИ НА ПОСТОЯННОМ ТОКЕ ДЛЯ ЛОКАЛИЗАЦИИ ПРОВОДЯЩИХ ГЕОЛОГИЧЕСКИХ ОБЪЕКТОВ ПРИ ОТКРЫТОМ СПОСОБЕ ДОБЫЧИ

Аннотация

При открытой разработке месторождений одна из важных задач заключается в прослеживании на глубину угольных пластов, зачастую характеризующихся пониженным удельным электрическим сопротивлением. Исходная геологическая модель постепенно эволюционирует в процессе углубления и расширения карьеров. В районах с развитой системой дизъюнктивных нарушений возникают ситуации «потери» угольных пластов в процессе добычи. Тогда возникает закономерный вопрос о полной его выработке или смещении в пространстве под поверхностью карьера, который может решаться геофизическими методами.

В работе рассмотрен частный случай способа поиска «утерянных» крутопадающих угольных пластов (В.В. Ржевский). Их, как правило, сложно обнаружить и локализовать из-за малой площади горизонтальной проекции. В качестве примера выбрано месторождение антрацита с применением варианта электротомографии на постоянном токе. Решены прямая и обратная трёхмерные задачи электротомографии с учётом пространственной геометрии дневной поверхности карьера. Все вычисления выполнялись в авторском программном комплексе DiInSo с привлечением сторонней программы GiD [1] для построения модели среды и расчётной тетраэдральной сетки.

Численное моделирование и результаты инверсии

Для решения прямых и обратных задач электротомографии использовался программный комплекс собственной разработки DiInSo [2]. При решении прямых задач в DiInSo применяется метод конечных элементов на тетраэдральных сетках [3]. Для этого области, представляющие собой модель карьера с соответствующим расположением питающих и приёмных электродов (рис. 1-2), строились в системе автоматизированного проектирования GiD [1] и там же разбивались на конечные элементы — тетраэдры.

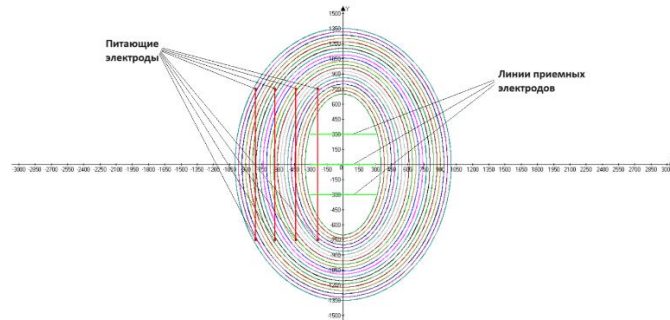


Рис. 1. Геометрическая модель карьера, системы питающих и приёмных электродов электротомографии (вид сверху).

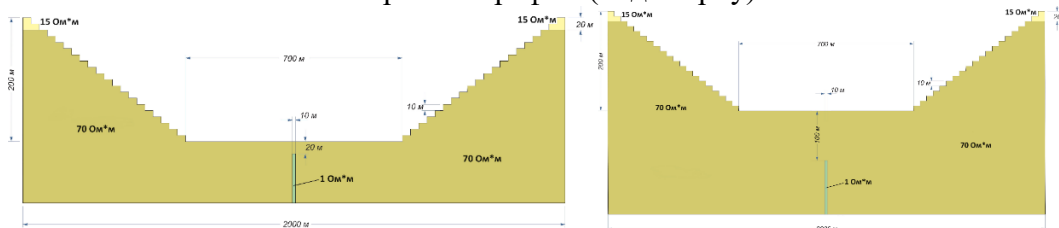


Рис. 2. Геометрическая и геоэлектрическая модели карьера в вертикальном разрезе при $Y = 0$. Слева: с неглубоким залеганием угольного пласта. Справа: с глубоким залеганием угольного пласта.

Установка электротомографии работала следующим образом: последовательно включались пары питающих электродов на обозначенных линиях (рис. 1). Измерения на приёмных электродах производилось так же на линиях, при этом выбирались все возможные пары приёмных электродов. Таким образом, была собрана своеобразная четырёхэлектродная установка, где питающие электроды находятся на одной линии, а приёмные электроды на другой. Общее число всех возможных положений питающих и приёмных электродов составило 21960, при этом прямых задач решалось лишь 4, по числу разных положений питающих электродов. Поэтому подобная прямая задача решается на современном персональном компьютере всего несколько секунд. При решении обратной задачи в программе DiInSo не требуется построения геометрической модели и разбиения её на тетраэдральные конечные элементы. Поскольку электроды покрывают лишь малую часть области исследований (рис. 1), то при инверсии она оказывается более упрощенной (рис. 3).

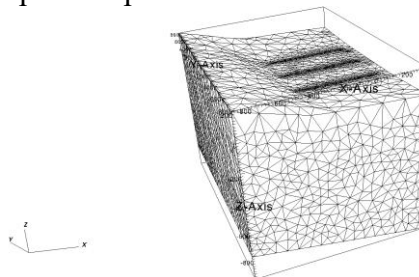


Рис. 3. Геометрическая модель и тетраэдральная сетка при решении обратной задачи в программе DiInSo.

Трёхмерная инверсия является относительно трудоёмкой [4] и занимает несколько минут на современном персональном компьютере. Рассмотрим её результаты в сечении $Y = 0$, то есть по центральной линии приёмных электродов и между питающими электродами (рис. 4).

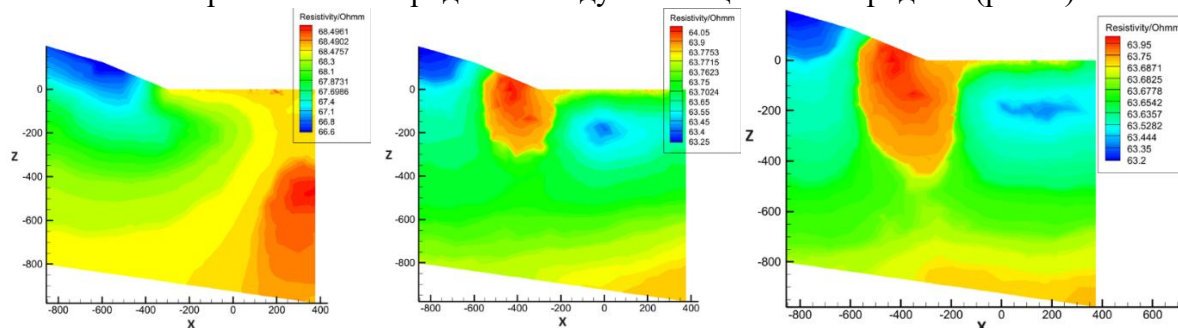


Рис. 4. Распределение удельного электрического сопротивления в сечении $Y = 0$ в результате инверсии в модели без угольного пласта (слева), для неглубокого (в центре) и глубокого (справа) залегания угольного пласта.

Выводы

На рис. 4 видно, что для результатов с угольным пластом, наряду с приповерхностным слоем торфа, появился новый низкоомный объект, обусловленный крутопадающим пластом антрацита. Его значение удельного электрического сопротивления так же, как и для торфа, оказывается сильно завышенным. Это не играет важной роли, поскольку цель состоит в оценке возможности обнаружения пласта, а не в сколько-нибудь точном определении удельного электрического сопротивления. В модели с неглубоким залеганием пласта можно достаточно точно определить его положение по оси X , в то время как для глубокого залегания изображение пласта размывается и вытягивается по оси X в сторону от питающих электродов. Глубина залегания кровли и горизонтальные размеры пласта не определяются. Таким образом, выделение угольного пласта разработанной методикой возможно, но только на качественном уровне.

Список использованных источников:

1. Fruitos O., Isanta R., Otin R., Mendez R. GiD interface for the parametric generation of simplified braided-wire shields geometries // The 5th Conference on Advances and Applications of GiD, Barcelona, Spain. 2010. – 4 pp.
2. Мариненко. А.В. DiInSo: Свидетельство о государственной регистрации программы для ЭВМ №2021662035, 2021.
3. Зенкевич О., Морган К. Конечные элементы и аппроксимация. М.: Мир, 1986.
4. Rucker C. Advanced Electrical Resistivity Modelling and Inversion using Unstructured Discretization: Dissertation. Leipzig, 2011.

УДК: 004.056.5

Мағзумов А. М.
(Астана, Л. Гумилев атындағы. ЕҰУ)

WEBSOCKET ПРОТОКОЛЫНДАҒЫ ОСАЛДЫҚТАРДЫ ТАЛДАУ

Аннотация: Бұл мақалада WebSocket протоколының осалдықтарын зерттеу және талдау әдістері қарастырылады. Нақты шабуыл мысалдары негізінде WebSocket байланыстарының қауіпсіздік мәселелері талданып, олардың ақпараттық жүйелерге ықтимал әсері бағаланады. Сондай-ақ осалдықтарды пайдаланудың негізгі әдістері мен оларды анықтау жолдары көрсетіледі. WebSocket байланыстарын қорғау және шабуылдардың алдын алу бойынша ұсыныстар беріледі. Мақала ақпараттық қауіпсіздік саласындағы мамандарға, зерттеушілерге және веб-қосымшалар әзірлеушілеріне арналған.

Кілт сөздер: Веб-қосымша, Интернет-ресурс, Websocket, қауіпсіздік, осалдық, ақпарат жинау.

Ақпараттық қауіпсіздіктегі осалдық - шабуылдаушылар қолдана алатын ақпараттық активтің немесе бақылау мен басқарудың әлсіз жақтары. Ақпараттық қауіпсіздіктің осалдықтарының жіктелуі өте көп. Соның ішінде веб-қосымшалардағы Websocket осалдықты ескерген жөн. Өйткені бұл қосымшаның және онымен байланысты деректердің құпиялылығына, тұтастығына және қол жетімділігіне нұқсан келтіруі мүмкін қауіпсіздік қатерлері мен шабуылдарына жол береді.

WebSocket – бұл екі жақты нақты уақыттағы деректер алмасуды қамтамасыз ететін хаттама. Ол веб-қосымшалардағы жылдамдық пен тиімділікті арттырады, бірақ сонымен бірге жаңа қауіпсіздік қатерлерін де тудырады. WebSocket хаттамасының ерекшелігі – тұрақты қосылым орнату арқылы сервер мен клиент арасында үздіксіз байланыс жасауында. Бұл механизм дәстүрлі HTTP сұраныс-жауап үлгісінен ерекшеленеді және дұрыс қорғалмаған жағдайда осалдықтарға жол ашады.

WebSocket тиімділік, масштабталу және икемділік тұрғысынан көптеген артықшылықтар ұсынады, бірақ сонымен қатар шабуылдаушылар пайдалана алатын бірқатар осалдықтарды да енгізеді. Ең көп таралған WebSocket осалдықтары мыналарды қамтиды:

1. Аутентификация мен авторизацияның болмауы – шабуылдаушы жүйеге рұқсатсыз кіре алады.
2. Деректерді ашық түрде беру – ws:// орнына wss:// қолданбау деректердің ұсталып қалу қаупін арттырады.
3. SQL-инъекция және командалық инъекция – зиянды кодты енгізу арқылы деректерді өзгертуге немесе жоюға мүмкіндік береді.
4. XSS (кросс-сайттық сценарий шабуылы) – шолғышта зиянды кодтың орындалуына жол ашады.
5. JWT токендерін ұрлау – рұқсат деңгейін заңсыз өзгертуге мүмкіндік береді.
6. MITM – шабуылдаушы деректер алмасуды ұстап алып, өзгерте алады.
7. DDoS-шабуыл – серверді артық жүктемеге ұшыратып, оның жұмысына кедергі келтіреді.
8. Бизнес-логика осалдықтары – жүйені айналып өтіп, рұқсатсыз әрекеттер жасауға мүмкіндік береді.

Осалдықтарды және олардың ықтимал салдарын терең түсіну ұйымдарға қауіпсіздікті күшейтіп, тәуекелдерді төмендету үшін алдын алу шараларын қабылдауға мүмкіндік береді.

№	Осалдықтар	Мақсаты	Әсері	Қауіпі	Алдын алу
1	Аутентификация мен авторизацияның болмауы	Жүйеге рұқсатсыз кіру	Шабуылдаушы басқа қолданушының сессиясын иемдене алуы	Жоғары	WebSocket сессиясында аутентификацияны талап ету, токендерді тексеру
2	Деректерді ашық түрде қолдану	Деректерді ұрлау	Құпия ақпарат желіде ашық түрде беріледі және ұрлануына қалынуы мүмкін	Жоғары	wss:// пайдалану, TLS шифрлауын қосу
3	SQL-инъекция және командалық инъекция	Дерекқорға рұқсатсыз қол жеткізу	Деректерді өзгерту немесе жою, жүйені зақымдау	Жоғары	Кіріс деректерді сүзу, SQL-инъекцияға қарсы қорғау
4	XSS	Код енгізу арқылы пайдаланушыны алдау	Жеке деректерді ұрлау, пайдаланушы әрекеттерін бақылау	Орташа	Сервер тарапынан енгізілген деректерді экранизациялау
5	JWT немесе сессия токендерін ұрлау	Токендерді өзгерту арқылы артық рұқсаттар алу	Шабуылдаушы өзіне әкімші рұқсатын тағайындай алу	Жоғары	Токендерді шифрлау, қолтаңбаларды тексеру, қысқа өмірлік цикл орнату
6	MITM	Байланысты ұстап, өзгерту	Қолданушының төлемдері мен хабарламаларын өзгерту	Жоғары	TLS пайдалану, HSTS енгізу, сертификат тексеру
7	DoS/DDoS-шабуылы	Қызметті істен шығару	Сервер ресурстарын істен шығару, жүйені бұзу	Орташа	WebSocket қосылымдарының санын шектеу
8	Бизнес-логика осалдықтары	Қорғауды айналып өту	Рұқсатсыз транзакциялар, деректерге заңсыз қол жеткізу	Орташа	Қауіпсіздік аудиті, жүргізу

Осалдықтарды анықтау үшін әртүрлі әдістер мен құралдар қолжетімді, олардың әрқайсысының өз артықшылықтары мен шектеулері бар

2-Кесте Осалдықты анықтау әдістерін салыстыру

Әдіс	Сипаттамасы	Артықшылықтары	Кемшіліктері	WebSocket осалдықтарына мысал
Статикалық талдау (SAST)	WebSocket байланысын өңдейтін кодты талдау	Ерте кезеңде қателерді анықтау, автоматтандыру	Эксплуатациялық осалдықты таба алмайды	WebSocket өңдеушілерінің қорғалмауы, деректерді тексеру қателері
Динамикалық талдау (DAST)	Жұмыс істеп тұрған WebSocket протоколын тестілеу	Осалдықтарды автоматты түрде анықтау	Өзара әрекеттесу логикасын толық тексере алмайды	WebSocket хабарламаларын ауыстыру, деректердің таралуы
Фаззинг (Fuzzing)	WebSocket арқылы кездейсоқ немесе арнайы жасалған деректерді жіберу	Деректерді өңдеу кезіндегі қателерді анықтау	Жоғары есептеу ресурстарын талап етеді, баптауды қажет етеді	WebSocket арқылы DoS шабуылдары, буферді асыра толтыру
Пентест	WebSocket қосылымдарына қарсы нақты шабуылдарды модельдеу	Қауіпсіздіктің нақты жағдайын бағалау	Жоғары білікті мамандарды қажет етеді	WebSocket деректерін өзгерту, аутентификацияны айналып өту
Сканерлеу	WebSocket-тегі белгілі осалдықтарды автоматты түрде іздеу	Стандартты осалдықтарды жылдам анықтау	Жалған іске қосулар болуы мүмкін, бірегей осалдықтарды таппайды	Жалған сұраныстардан қорғаныстың (CSRF) болмауы, WebSocket-ке енгізу шабуылдары

Қортынды

Интернет-ресурстардың өмірімізге біртіндеп енгізілуі қызметтер мен кеңес алуда үлкен артықшылықтарды береді. Веб-қосымшалардың функционалдық дамуы қауіпсіздікті сапалы қамтамасыз етумен қатар жүруі тиіс. Қосымшалардың қауіпсіздігін қамтамасыз етуде қауіп төндіретін мәліметтер жиынтығынан тұратын базалардың маңызы зор. Зерттеу қорытындысында WebSocket пайдаланатын веб-қосымшалардың қауіпсіздігі ақпараттың құпиялылығын, тұтастығын және қол жетімділігін сақтау үшін өте маңызды екенін анықтадық. Соңғы жылдары WebSockets танымалдылығының артуы оларды пайдалануды екі есеге арттырды, бұл оларды кибершабуылдар үшін тартымды нысанаға айналдыруда. Біздің жұмысымыз веб-қосымшалардың қауіпсіздігін қамтамасыз етудің кешенді тәсілінің маңыздылығын көрсетеді.

Зерттеу негізінде websocket технологиясын қолданатын веб-қосымшалардың қауіпсіздігін қамтамасыз ету үшін бірқатар ұсыныстар жасауға болады:

TLS/SSL пайдалану: барлық WebSocket қосылымдары деректердің құпиялылығы мен тұтастығын қамтамасыз ету үшін шифрланған арналарды (wss://) пайдалану;

Сайтаралық сценарийден қорғау (XSS): пайдаланушы енгізуін санитариялау, Content Security Policy (CSP) қауіпсіздік тақырыптарын орнату және басқа шаралар арқылы XSS-тің алдын алу;

CSRF шабуылдарынан қорғау: веб-пішіндер мен басқа күйді өзгертетін сұраулар үшін CSRF шабуылдарына қарсы белгілерді пайдалану;

Аутентификация және авторизация: OAuth, JWT немесе HTTP-Only және Secure cookie сеанстарын пайдалануды қоса алғанда, барлық кезеңдерде сенімді аутентификация мен авторизацияны қамтамасыз ету;

Пайдаланылған дереккөздердің тізімі

1. *WebSocket: Lightweight Client-Server Communications*, Andrew Lombardi 2015, 141p
2. *The Definitive Guide to HTML5 WebSocket*, Frank Salim Peter Moskovits, 2013, 227 p
3. <https://cyberleninka.ru/article/n/kak-ispravit-mezhsaytovuyu-uyazvimost-web-socket>
4. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9182458>
5. <https://book.hacktricks.xyz/pentesting-web/websocket-attacks>

УДК 004.8

Махашов Шохан
Евразийский национальный университет им. Л. Н. Гумилева
Астана, Казахстан

КЛАСТЕРИЗАЦИЯ РЕГИОНОВ РЕСПУБЛИКИ КАЗАХСТАН ПО МАКРОЭКОНОМИЧЕСКИМ ПОКАЗАТЕЛЯМ С ПРИМЕНЕНИЕМ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ

Аннотация

В статье рассматривается задача кластеризации регионов Казахстана на основе макроэкономических показателей с использованием методов машинного обучения. В качестве исходных данных использованы значения валового регионального продукта, объёма инвестиций в основной капитал, среднемесячной заработной платы и уровня безработицы за 2024 год по каждому региону. Для решения задачи применены алгоритмы кластеризации, включая k-means и иерархическую кластеризацию, а также методы снижения размерности для визуализации (РСА). Результатом исследования стало выделение групп регионов с близкими экономическими характеристиками, что может быть использовано при формировании региональной политики и планировании экономического развития. Проведённый анализ показал эффективность машинного обучения в задачах анализа и интерпретации макроэкономических данных.

Ключевые слова: кластеризация, Казахстан, макроэкономика, машинное обучение, региональный анализ, k-means, РСА

Введение

Анализ регионального развития играет ключевую роль в формировании сбалансированной экономической политики государства. Казахстан, обладая значительной территориальной протяжённостью и разнообразием природных ресурсов, характеризуется значительными различиями в социально-экономическом развитии регионов. Для эффективного управления и планирования региональной экономики необходимы инструменты, позволяющие выявлять закономерности и группировать регионы по схожим макроэкономическим характеристикам. Традиционные методы анализа часто опираются на экспертные оценки или агрегированные показатели, что затрудняет автоматизацию и может приводить к субъективным выводам. В связи с этим особую актуальность приобретают методы машинного обучения, в частности алгоритмы кластеризации, позволяющие на основе объективных данных выявлять скрытые структуры и взаимосвязи между регионами.

Цель настоящего исследования — провести кластеризацию регионов Казахстана на основе ключевых макроэкономических показателей с использованием алгоритмов машинного обучения. В рамках работы рассматриваются такие показатели, как валовой региональный продукт (ВРП), объём

инвестиций в основной капитал, среднемесячная заработная плата и уровень безработицы. Для решения поставленной задачи применяются алгоритмы k-means и иерархической кластеризации, а также методы визуализации многомерных данных на основе анализа главных компонент (РСА). Результаты данного исследования могут быть полезны для государственных органов и экономистов при принятии решений, направленных на развитие регионов, устранение экономических диспропорций и повышение эффективности распределения бюджетных ресурсов.

Обзор литературы

Методы кластерного анализа получили широкое распространение в экономике, особенно при исследовании пространственного и регионального развития. Такие методы позволяют выявлять скрытые закономерности, классифицировать регионы по степени экономической близости и формировать более обоснованные региональные стратегии.

Теоретические основы кластеризации изложены в классических трудах Everitt и соавт. [1], а также Kaufman и Rousseeuw [2]. Эти работы описывают основные алгоритмы, включая k-means, иерархическую кластеризацию, DBSCAN и другие подходы, применимые к анализу многомерных данных.

В практическом контексте кластеризация активно применяется в исследованиях социально-экономического развития. Так, в работе Кузнецовой и Селезнёва [3] рассматривается кластеризация регионов России по показателям инновационного развития. Аналогичный подход реализован в исследовании Попова [4], где используется машинное обучение для анализа различий между субъектами РФ по демографическим и экономическим характеристикам. Таким образом, применение методов кластеризации в региональных исследованиях доказало свою эффективность, а в контексте Казахстана сохраняет высокий научный и прикладной потенциал.

Методология

В рамках исследования использовались макроэкономические данные по регионам Республики Казахстан за 2024 год. В выборку вошли следующие показатели:

- Валовой региональный продукт (ВРП) на душу населения, млрд тенге;
- Объём инвестиций в основной капитал, млрд тенге;
- Среднемесячная номинальная заработная плата, тенге;
- Уровень безработицы, %.

Данные были собраны из официальных источников, включая:

- Бюро национальной статистики Республики Казахстан,
- Комитет по инвестициям Министерства национальной экономики РК,
- Открытые отчёты Национального банка.

В анализ включены 20 регионов: 14 областей, 3 города республиканского значения (Алматы, Астана, Шымкент), и 3 новых областных центра (Туркестанская, Жетысуская и Улытауская области — при наличии данных).

Перед применением методов машинного обучения были выполнены следующие этапы предобработки:

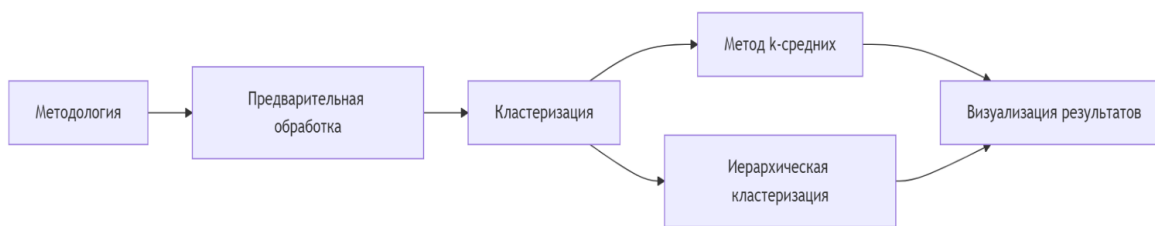
1. Заполнение пропущенных значений — при отсутствии значения в одном из показателей применялось среднее по выборке либо ближайший сосед.
2. Нормализация признаков — данные приведены к одному масштабу с помощью MinMaxScaler, чтобы исключить влияние различий в размерности показателей (например, зарплата и ВРП).
3. Проверка выбросов — при необходимости применялись Z-оценка и межквартильный размах (IQR) для корректировки или исключения аномальных значений.

Для выявления групп регионов со схожими экономическими характеристиками были применены следующие алгоритмы:

- k-means — классический метод кластеризации, основанный на разбиении наблюдений на k групп с минимизацией внутрикластерного расстояния. Оптимальное количество кластеров определялось с помощью метода локтя (elbow method) и силезта-анализа.
- Иерархическая агломеративная кластеризация — построение дендрограммы для анализа вложенности кластеров, использовались расстояния Евклида и метод полной связи (complete linkage).

Для представления данных и результатов кластеризации в двумерном пространстве применялись методы:

- Анализ главных компонент (PCA) — для снижения размерности и визуализации кластерной структуры;
- Тепловые карты (heatmap) — для отображения отклонений регионов по показателям внутри кластеров.



Методология проведения кластерного анализа.

Результаты и обсуждение

В результате применения алгоритмов машинного обучения была выполнена кластеризация 20 регионов Казахстана по четырём ключевым макроэкономическим показателям: валовой региональный продукт (ВРП) на душу населения, объём инвестиций в основной капитал, среднемесячная заработная плата и уровень безработицы за 2024 год.

1. Определение оптимального количества кластеров

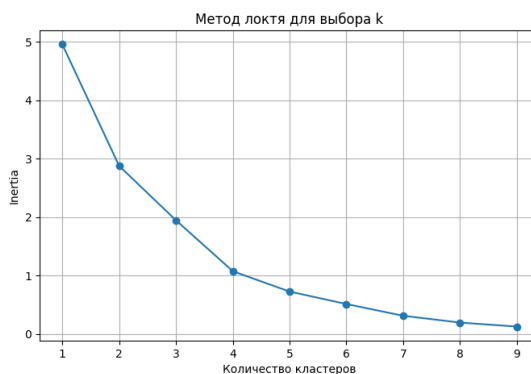


Рисунок 1. График метода локтя (Elbow Method)

График метода локтя показал излом при $k = 3$ и $k = 4$, что свидетельствует о наличии в выборке трёх-четырёх экономически однородных групп. Это позволило обоснованно применить оба варианта кластеризации и провести сравнительный анализ.

2. Результаты кластеризации (PCA)

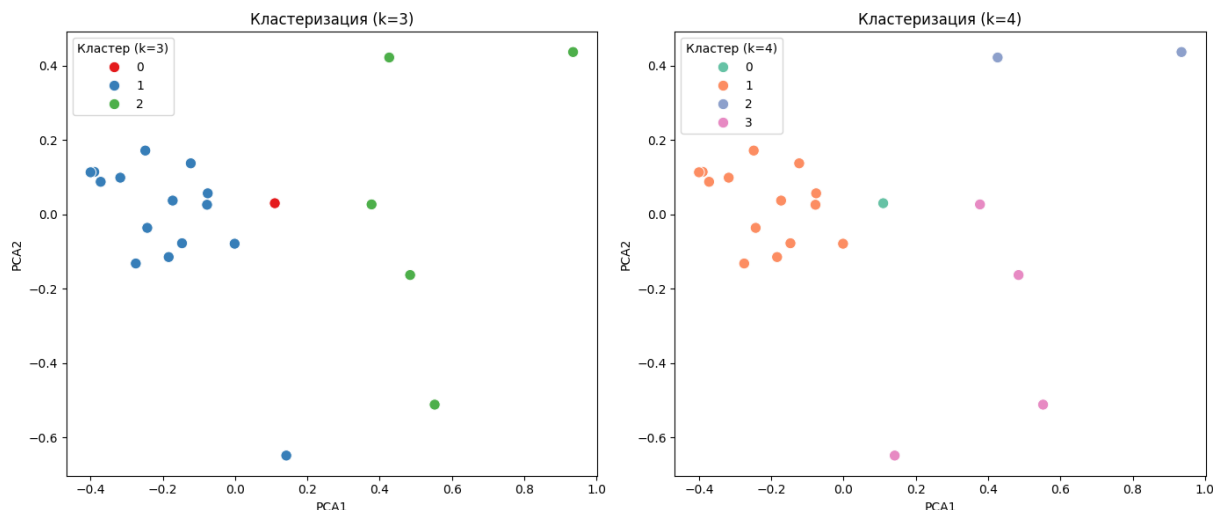


Рисунок 2. PCA-кластеризация($k=3$, $k=4$)

Алгоритм k-means с $k = 3$ выделил три отчётливо различающихся кластера:

- Кластер 0 (красный) — экономически развитые регионы с высокой зарплатой, инвестициями и ВРП: г. Астана, г. Алматы, Атырауская, Мангистауская и Улытауская области.
- Кластер 1 (синий) — регионы со средними значениями показателей: Акмолинская, Карагандинская, Костанайская и др.
- Кластер 2 (зелёный) — регионы с низким уровнем ВРП и инвестиций, в основном южные: Жамбылская, Алматинская, Туркестанская.

Переход к кластеризации с $k = 4$ позволил детализировать группировку, например, Атырауская область выделилась в отдельный кластер, что отражает её уникальную экономическую структуру, обусловленную добывающей промышленностью.

4. Сравнение средних значений



Рисунок 4. Тепловая карта средних значений в кластерах ($k = 3$)

Тепловая карта показала, что:

- Кластер 0 характеризуется самыми высокими значениями по всем показателям, кроме безработицы.
- Кластер 1 является относительно сбалансированным — без ярко выраженных отклонений.
- Кластер 2 демонстрирует отставание по ключевым макроэкономическим метрикам.

Это подтверждает, что выбранные признаки эффективно дифференцируют регионы.

4. Иерархическая кластеризация

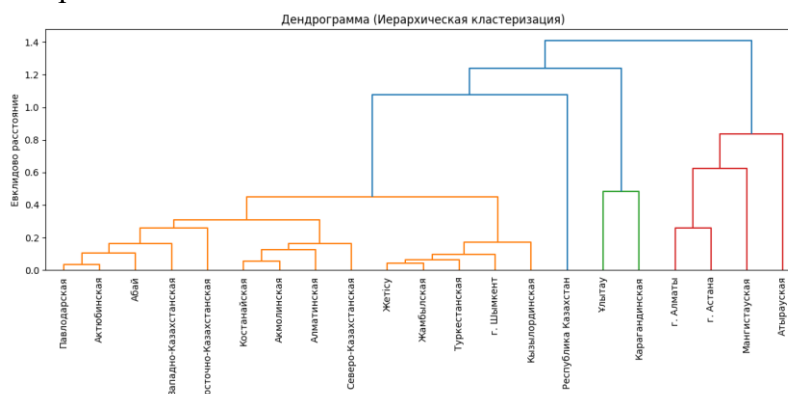


Рисунок 5. Дендрограмма

Иерархическая агломеративная кластеризация позволила проследить логику объединения регионов по степени схожести. Ветки дендрограммы чётко показывают близость Астаны и Алматы, а также отдельность Жамбылской и Туркестанской областей.

Полученные результаты соответствуют как экономической интуиции, так и предыдущим исследованиям в области регионального анализа (см. Обзор литературы). Например, регионы с развитой инфраструктурой, высоким уровнем урбанизации и инвестиций (Астана, Алматы, Атырау) действительно выделяются в отдельные группы.

В то же время, регионы с аграрной спецификой и ограниченной промышленной базой (Жамбылская, Туркестанская) устойчиво попадают в один кластер с наименьшими экономическими показателями. Результаты кластеризации могут быть использованы:

- для разработки региональной политики,
- при определении приоритетов бюджетного финансирования,
- в инвестиционном планировании,
- для мониторинга эффективности мер по выравниванию регионального развития.

Такая сегментация может стать основой для дифференцированного подхода к регионам в рамках госпрограмм.

Стоит отметить несколько ограничений текущего анализа:

- Использованы только четыре макроэкономических показателя, что упрощает картину;
- Данные охватывают только один год (2024), без динамики;
- Алгоритмы чувствительны к масштабированию данных и выбросам;
- Кластеры не учитывают географический фактор и отраслевую структуру экономики.

Таким образом, кластеризация позволила выявить объективные различия между регионами Казахстана, структурировать их по уровню развития и заложить основу для дальнейших исследований в области пространственного анализа и прогноза регионального роста.

Выводы

В настоящем исследовании была проведена кластеризация регионов Республики Казахстан по четырём ключевым макроэкономическим показателям за 2024 год с применением алгоритмов машинного обучения — k-means и иерархической кластеризации. Результаты анализа позволили сделать следующие основные выводы:

1. Алгоритмы кластеризации позволяют объективно сегментировать регионы Казахстана по уровню социально-экономического развития, выявляя скрытые структуры в данных без использования экспертных оценок.
2. Оптимальное количество кластеров, определённое с помощью метода локтя, составило 3 или 4, что позволило выделить как обобщённые, так и более детализированные группы регионов.
3. Кластер 0 включает регионы с наивысшими значениями ВРП, инвестиций и заработной платы (г. Астана, г. Алматы, Атырауская и Мангистауская области). Кластер 2 объединяет регионы с низкими макроэкономическими показателями (Жамбылская, Туркестанская, Алматинская области). Кластер 1 состоит из сбалансированных по развитию субъектов.
4. Метод РСА продемонстрировал эффективность визуализации многомерных экономических данных, а тепловая карта наглядно отразила различия между кластерами по каждому из показателей.
5. Иерархическая кластеризация подтвердила результаты k-means и выявила логичную структуру объединения регионов по степени экономического сходства.
6. Полученные результаты обладают высокой прикладной значимостью для органов государственной власти, региональных аналитических центров и инвесторов. Они могут использоваться при разработке территориальной стратегии развития, распределении бюджета и оценке регионального потенциала.
7. В качестве направления для дальнейших исследований можно предложить:
 - Расширение набора признаков (добавление отраслевой структуры, уровня образования, инфраструктуры и т.д.);
 - Использование временных рядов для анализа динамики кластеров во времени;
 - Применение других методов машинного обучения, включая self-organizing maps и нейронные сети.

Список литературы

1. Everitt, B. S., Landau, S., Leese, M., & Stahl, D. (2011). *Cluster Analysis* (5th ed.). Wiley.
2. Kaufman, L., & Rousseeuw, P. J. (2005). *Finding Groups in Data: An Introduction to Cluster Analysis*. Wiley.
3. Кузнецова, О. В., & Селезнёв, А. В. (2020). Кластеризация регионов России по показателям инновационного развития. *Экономика региона*, 16(1), 112–124. <https://doi.org/10.17059/2020-1-9>
4. Попов, А. И. (2019). Применение методов машинного обучения для анализа социально-экономических различий регионов. *Вестник НГУ. Серия: Экономика и управление*, 17(2), 45–56.

УДК004.4:658.6

Наир Р.А.
(Алматы, КазНУ им. аль-Фараби)
Ахметова А.А., PhD, ст. преп.
(Алматы, КазНУ им. аль-Фараби)

АВТОМАТИЗАЦИЯ РЕСТОРАННЫХ СЕТЕЙ

Абстракт. В статье представлена разработка прототипа системы онлайн-бронирования столиков для ресторанов с использованием инструментов и технологий с открытым исходным кодом — React Native, TypeScript, MongoDB, TailwindCSS, Node.js и Express.js. Целью работы является создание доступного и удобного решения для бронирования столиков, предварительного заказа еды и оплаты в условиях ограниченных ресурсов. В рамках исследования реализован интерфейс приложения, позволяющий пользователям выбирать любой доступный столик на интерактивной схеме, указывать желаемые блюда для подачи, определять количество времени бронирования, а также производить моментальную оплату. Дополнительно предусмотрена возможность указания подробных инструкций для официанта. Прототип включает генерацию данных о доступных столиках, настройку базы данных MongoDB для хранения информации о бронированиях, заказах и платежах, а также разработку серверной части на Node.js с использованием фреймворка Express.js для обработки запросов и обеспечения связи между клиентом и сервером через REST API. Пользовательский интерфейс создан с применением React Native и стилизации через TailwindCSS на языке программирования TypeScript. Система позволяет отображать статус бронирований в реальном времени, текущие заказы и уведомлять персонал о новых инструкциях. Результаты демонстрируют применимость прототипа для небольших ресторанов и кафе, а также его потенциал для дальнейшего масштабирования и интеграции с другими сервисами благодаря гибкости Node.js и Express.js.

Ключевые слова: React Native, TypeScript, MongoDB, TailwindCSS, базы данных, NodeJS, ExpressJS.

Введение. В современном мире, где скорость и удобство становятся приоритетами, ресторанный сервис выходит на новый уровень благодаря цифровым технологиям. Представьте: вы заходите в ресторан, вас встречают по имени, провожают к столику без очередей и ожидания — такой опыт стал реальностью с внедрением инновационных решений. Ресторанный бизнес прошёл долгий путь — от простых трактиров и «изакаев» до изысканных заведений и сетей быстрого питания, постоянно адаптируясь к меняющимся вкусам клиентов и требованиям времени. Одним из главных достижений последних десятилетий стало внедрение систем онлайн-бронирования, которые заменили неудобные звонки и ожидание в очередях на быстрый и доступный процесс через приложения или сайты [1].

Цель работы — разработка удобной и интуитивно понятной системы онлайн-бронирования столиков, основанной на современных веб-технологиях. Задача заключается в создании платформы, которая обеспечит клиентам лёгкость и скорость бронирования, а ресторанам предоставит эффективные инструменты для управления посадочными местами, сокращения простоев и повышения качества обслуживания. В статье подробно рассмотрены ключевые аспекты: эволюция ресторанного бизнеса и факторы его развития, влияние цифровых инноваций на управление и взаимодействие с клиентами, а также архитектура, функциональность и процесс реализации

предлагаемой системы. Итогом станет функциональное решение, способное оптимизировать работу ресторанов, улучшить клиентский опыт и повысить операционную эффективность заведений.

1. Развитие ресторанного бизнеса. Рестораны быстро изменили культуру питания. Гостей ждали фарфоровые тарелки, чистые скатерти и меню на стенах, а счёт в конце трапезы добавил современности. К 1814 году в Париже насчитывалось уже 3000 ресторанов против 50 до революции. Владельцы добавляли уборные за плату, усиливая контраст с грубыми тавернами. Революция породила новый подход к еде вне дома, который вскоре охватил мир.

В XIX веке Париж стал кулинарной столицей, привлекая богатых путешественников. Рестораны предлагали роскошь и выбор, формируя высокую кухню. Появились кафе для быстрых перекусов и суповые кухни для рабочих, создавая разнообразие заведений. Развитие транспорта усилило туризм, сделав еду частью путешествий. К XX веку концепция ресторана глобализировалась, адаптируясь в каждой стране — от испанских *restaurantes* до американских *restaurant*. В США рестораны сначала копировали французский стиль, но иммигранты внесли свои вкусы — пиццу, лапшу, гирс. Затем фастфуд вроде McDonald's и White Castle сделал еду быстрой и массовой. Франчайзинг распространил эту модель по миру, превратив рестораны в индустрию. Сегодня они варьируются от изысканных заведений с меню и столиками до сетей с готовой едой, отражая эволюцию от революционной идеи до глобального явления [2, 3].

2. Современные технологии в ресторанной индустрии. До появления технологий питание вне дома зависело от ручного труда. В XIX веке газовые плиты ускорили готовку, холодильники 1920-х сохраняли продукты, а слайсеры и миксеры упростили подготовку. Это избавило кухни от медленной работы средневековых таверн и заложило основу для быстрого обслуживания. Сети вроде White Castle и McDonald's превратили кухни в конвейеры, но настоящий переворот пришёл в XX веке. Компьютеры, умные машины и системы заказов без кассиров изменили не только готовку, но и весь ресторанный бизнес, сделав его быстрым и связанным.

Одним из лидеров этой революции стали киоски самообслуживания. В оживлённом фастфуде, таком как McDonald's, вы подходите к сенсорному экрану, выбираете еду, платите картой и забираете заказ — без очередей и путаницы. Киоски появились в конце XX века, но расцвели в 2000-х, когда сети осознали их выгоду: скорость, экономия и довольные клиенты. McDonald's начал массовое внедрение в 2015 году, а к 2020-м киоски стали стандартом для быстрого обслуживания, ускоряя заказы на 40%, снижая ошибки и увеличивая чеки на 25–30% благодаря удобству выбора. Киоски выросли из ранних экспериментов 1990-х с громоздкими экранами. К 2000-м технологии улучшились: сенсоры стали точнее, софт — умнее. Они решают проблемы очередей и перегруженного персонала, предлагая контроль, как в первых французских ресторанах, но в цифровом формате. Пандемия 2020 года ускорила их рост — бесконтактность стала ключом, а популярность киосков взлетела: 91% клиентов предпочли их очередям. Сегодня они не только в фастфуде — рестораны, аэропорты и мелкие точки используют их, превращая питание вне дома в быстрое и умное приключение.

3. Разработка системы онлайн-бронирования столиков. В данной главе представлен процесс разработки прототипа системы онлайн-бронирования столиков, включая её архитектуру, функциональные возможности, используемые технологии и этапы реализации. Проект направлен на создание доступного и удобного инструмента для клиентов и ресторанов, особенно небольших заведений с ограниченными ресурсами, с целью упростить резервирование мест и повысить эффективность работы. Система основана на клиент-серверной модели. Клиентская часть реализована как мобильное приложение на React Native, обеспечивающее совместимость с iOS и Android. Серверная часть построена на Node.js с использованием фреймворка Express для обработки запросов и взаимодействия с базой данных MongoDB, где хранятся данные о бронированиях, заказах и статусе столиков. Для оформления интерфейса применён TailwindCSS, что ускоряет

разработку и адаптирует дизайн под разные устройства. Связь между клиентом и сервером осуществляется через REST API, что обеспечивает гибкость и возможность масштабирования [4, 5].

Система включает следующие ключевые функции: выбор столика через интерактивную схему зала с обновлением доступности в реальном времени, позволяющую выбрать конкретное место; предзаказ еды, дающий пользователям возможность заранее заказать блюда из меню для подачи к их приходу; оплату через интеграцию с локальными платёжными системами (например, API банков или QR-коды), предоставляющую возможность оплатить бронь и заказ; установку времени брони, где клиенты указывают длительность пребывания, помогая ресторану планировать загрузку; инструкции для персонала через специальное поле для передачи пожеланий (например, «столик у окна» или «добавить соус»); уведомления в виде push-сообщений, сообщающих о статусе бронирования и заказа.

Разработка велась в несколько этапов: проектирование, в рамках которого разработан макет интерфейса с акцентом на простоту — схема зала, меню и форма бронирования; настройка серверной части, где создано API для управления бронированиями и подключена MongoDB для хранения данных; генерация тестовых данных, имитирующая работу ресторана с 10 столиками и базовым меню для проверки системы; разработка фронтенда, реализованного на React Native с TailwindCSS, включая динамическую карту зала; тестирование, в ходе которого проверена работа на разных устройствах, скорость обработки запросов и точность оплаты; оптимизация, упростившая код и снизившая нагрузку на сервер для работы на устройствах с минимальными характеристиками. Среди технологических особенностей: React Native позволяет использовать единый код для двух платформ, сокращая затраты; TypeScript повышает надёжность кода за счёт строгой типизации; MongoDB обеспечивает гибкость структуры данных, упрощая добавление новых функций; TailwindCSS ускоряет создание адаптивного дизайна для разных экранов. Система минимизирует время на бронирование, исключает ошибки в заказах и оптимизирует работу персонала. Её доступность для небольших ресторанов обусловлена бесплатными технологиями и низкими требованиями к оборудованию. Перспективы развития включают интеграцию с POS-системами для синхронизации заказов, добавление ИИ для персонализированных рекомендаций и поддержку многоязычности для международного рынка (Рисунок 1).

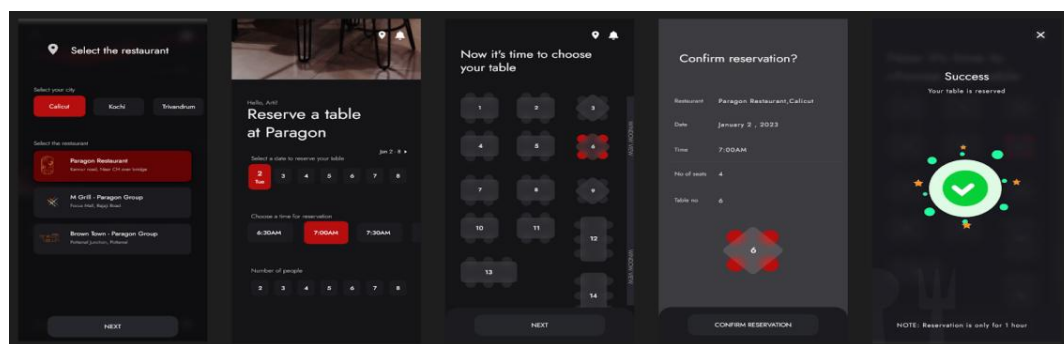


Рисунок 1. Дашборд Production Monitoring в Grafana

В ходе исследования был разработан прототип системы онлайн-бронирования столиков, обеспечивающий удобный интерфейс для клиентов и ресторанов. Приложение, созданное с использованием React Native, позволяет пользователям выбирать ресторан, бронировать столик, заказывать еду заранее и оплачивать услуги. На рисунке 3.1 представлен макет интерфейса приложения, демонстрирующий ключевые этапы процесса: первая часть показывает выбор ресторана из списка доступных заведений в городе, вторая — инструкции для бронирования столика (выбор даты, времени и количества гостей), третья — подтверждение брони с деталями (дата, время, номер столика), четвёртая — возможность предзаказа еды, а пятая — уведомление об успешном завершении бронирования. Система демонстрирует эффективность использования React

Native, TypeScript, MongoDB, Node.js, Express.js и TailwindCSS для задач автоматизации бронирования, предлагая функциональное и интуитивное решение. Прототип отличается минимальными требованиями к ресурсам, что делает его подходящим для небольших ресторанов и кафе с ограниченными техническими возможностями. Оригинальность работы заключается в создании интерактивной схемы зала и интеграции функции предзаказа еды, что выделяет проект среди типичных систем бронирования.

Заключение. Созданный прототип системы онлайн-бронирования столиков, разработанный с применением React Native, TypeScript, MongoDB, Node.js, Express.js и TailwindCSS, полностью выполнил поставленные задачи. Система позволяет эффективно собирать, хранить и обрабатывать информацию о бронированиях, заказах и доступных местах, обеспечивая интуитивно понятный интерфейс для пользователей и сотрудников ресторана. Проведённое тестирование показало надёжность работы и минимальные требования к вычислительным ресурсам, что делает её подходящей для внедрения в небольших заведениях общественного питания. В дальнейшем возможно развитие системы путём подключения к реальным платёжным системам через современные API, а также переход на облачную инфраструктуру для работы с крупными ресторанными сетями. Перспективы исследований включают внедрение алгоритмов персонализации на основе анализа данных о клиентах и интеграцию с POS-системами для автоматизации процессов. Кроме того, можно добавить функцию уведомлений (например, через push-уведомления или электронную почту) для своевременного оповещения пользователей о статусе их брони или акциях заведения.

Литература

1. Glushchenko V.V. *Theoretical Foundations of the Restaurant Business* // ASEAN Journal of Economic and Economic Education. – 2023. – Vol. 3, N 1. – P. 1-16.
2. Кокшаров А.А. *Технология производства ресторанной продукции: учеб. пособие* / А.А. Кокшаров, Т.В. Подлегаева; Кемеровский гос. ун-т. – Кемерово: Кемеровский гос. ун-т, 2021. – 144 с.
3. Чеканков А.Н. *Организация управления производством ресторана на основе автоматизированных систем управления на примере по айко* // Глобальные тренды культурного и социально-экономического развития: сб. науч. тр. по материалам Междунар. науч.-практ. конф. / под общ. ред. Е.П. Ткачевой. – Белгород, 2021. – С. 57-58.
4. Мишина Е.А. *Основные факторы, влияющие на успешный имидж и деловую репутацию ресторанов* // Молодой ученый. – 2021. – № 47 (389). – С. 140-141. – Электронная копия доступна на сайте журнала. URL: <https://moluch.ru/archive/389/85761/> (дата обращения: 06.06.2022)
5. Щеглова Ю.А. *Автоматизированная информационная система управления деятельностью ресторана* / Ю.А. Щеглова, Т.В. Жашкова // Современные информационные технологии. – 2019. – № 29. – С. 99-101.

УДК 004.5, 004.89.

Нуржанова А.Б. (Астана, Л.Н. Гумилев атындағы
Еуразия ұлттық университеті)
Жумадиллаева А.К. (Астана, Л.Н. Гумилев атындағы
Еуразия ұлттық университеті)

ВИДЕО АРҚЫЛЫ ЭМОЦИЯЛАРДЫ ТАНУ: КОХОНЕН КАРТАЛАРЫ МЕН КЛАСТЕРЛІК АНСАМБЛЬДЕР

Аннотация. Бұл мақалада видео деректердегі эмоцияларды автоматты түрде тану әдістері қарастырылады. Эмоцияларды тану адамның компьютермен өзара әрекеттесу сапасын жақсартуға, бейімделетін интерфейстерді дамытуға және психоэмоционалдық диагностика мүмкіндіктерін кеңейтуге мүмкіндік береді. Бастапқы деректерді өңдеу, бет-әлпетті анықтау, ерекшеліктерді шығару және эмоцияларды жіктеу кезеңдері сипатталады. Кохоненнің өзін-өзі ұйымдастыратын карталары мен кластерлік ансамбльдерді қолдану арқылы нақты уақыт режимінде эмоцияларды тану тиімділігі арттырылады. Сондай-ақ, стекинг, бустинг және кездейсоқ ормандар әдістерін пайдалану ұсынылады. Бұл тәсіл виртуалды көмекшілерде, қауіпсіздік жүйелерінде және психоэмоционалдық жағдайды бағалау жүйелерінде қолдануға мүмкіндік береді.

Кілттік сөздер: эмоцияларды тану, компьютерлік көру, машиналық оқыту, Кохонен карталары, кластерлік ансамбль, бейнежазба талдау, бет-әлпет белгілері, SVM, CNN, Random Forest.

Адам-машина өзара әрекеттесуі жиі интуитивті сипатқа ие, бұл пайдаланушының бағдарламалық қамтамасыз етуге немесе компьютерге бейімделуін қажет етеді. Бұл процесті неғұрлым объективті ету үшін интерфейске бағдарламаның әрекеттеріне пайдаланушының реакциясын ескеретін кері байланыс механизмі енгізілуі керек. Мұндай механизм сөйлеу, ым-ишара және мимиканы талдауға негізделуі мүмкін.

Зерттеулерге сәйкес [1], ауызша қарым-қатынас ақпараттың тек 7%-ын ғана жеткізеді, ал 38%-ы дауыс модуляциясына, ал 55%-ы бет-әлпеттің көрінісіне байланысты. Осыған байланысты эмоцияларды тану және жіктеу компьютерлік көру және жасанды интеллект салаларындағы маңызды міндеттер болып табылады. Эмоцияларды автоматты түрде тану технологиялармен өзара әрекеттесудің сапасын арттырып, бейімделетін интерфейстерді, дербестендірілген оқытуды және психоэмоционалдық жағдайды диагностикалаудың кеңейтілген мүмкіндіктерін қамтамасыз етеді.

Эмоцияларды автоматты түрде танудың негізгі кезеңдері [2-3]. Адам эмоцияларын автоматты түрде тану бірнеше негізгі кезеңнен тұрады:

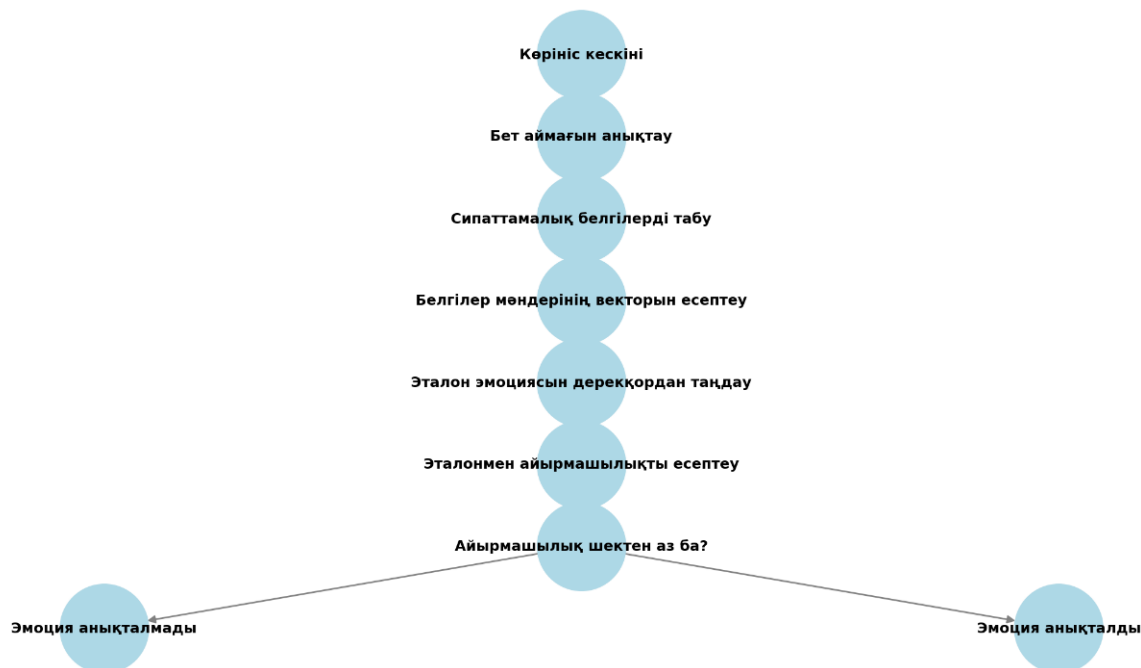
- *Кескінді алдын ала өңдеу*: шуылдарды жою, жарықты түзету, бастың орналасуын және қозғалыс әсерлерін компенсациялау.

- *Бетті анықтау және бөлу*: түске негізделген сегментация әдістері, геометриялық белгілер жиынтығын іздеу, бет-әлпетті анықтау алгоритмдерін пайдалану (мысалы, Viola-Jones, MTCNN, YOLO).

- *Беттің сипаттамалық белгілерін анықтау*: қастар, көздер, мұрын, ауыз аймақтарын бөліп алу, өлшемдерін, координаттарының центрлерін талдау, үшөлшемді бет моделін пайдалану, HOG, LBP және CNN негізінде белгілерді бөліп алу.

- *Эмоцияларды жіктеу*: эталондық үлгілермен салыстыру, ағымдағы және бейтарап күй арасындағы айырмашылықты анықтау, SVM, Random Forest, CNN, RNN сияқты машиналық оқыту әдістерін пайдалана отырып шешім қабылдау.

Эмоцияларды тану процесін шешімдер ағашы түрінде көрсетуге болады (сурет 1), онда әр кезеңде кескін өңдеу және бет-әлпет белгілерін талдау орындалады.



Сурет 1. Эмоцияларды тану шешім ағашы.

Егер ағымдағы кескін мен эталон арасындағы айырмашылық шекті мәннен төмен болса, эмоция танылды деп есептеледі. Әйтпесе, талдау процедурасы жалғасады. Бұл әдіс жалған тануды болдырмауға және жүйенің дәлдігін арттыруға мүмкіндік береді.

Адам эмоциялары динамикалық сипатқа ие және уақыт өте өзгере алады. Өзгерістер жылдамдығы да эмоционалдық жағдайдың индикаторы бола алады. Видео деректердегі эмоцияларды нақты уақыт режимінде тану үшін Кохоненнің өзін-өзі ұйымдастыратын карталарын (SOM) пайдалану ұсынылады.

Кохонен карталары келесі ерекшеліктерге ие:

- Жалғыз қабатты қарапайым архитектура
- Ақпараттың тікелей берілуі
- Белсенділігі жоғары нейрондар топтарын қалыптастыру
- Деректердің топологиялық құрылымын сақтау

Алайда, оларда кластерлеу дәлдігі жеткіліксіз болуы мүмкін. Бұл мәселені шешу үшін өзін-өзі оқытатын алгоритмді қолдану арқылы Кохонен карталарына негізделген кластерлік ансамбльді қалыптастыру ұсынылады.

Кластерлік ансамбльді оңтайландыру [4-5]. Кластерлік ансамбльді қалыптастыру келесі кезеңдерді қамтиды:

1. Бастапқы кластер орталықтарын кездейсоқ анықтау.
2. Деректер элементтері арасындағы қашықтықты өлшеу функциясын орнату.
3. Кіріс деректерін Кохоненнің өзін-өзі ұйымдастыратын картасына проекциялау.
4. Нейрон белсенділігін талдау және ең белсенді аймақтарды анықтау.
5. Деректерді нейрондық белсенділікке негізделген топтастыру және оларға сәйкес меткалар тағайындау.
6. Алдын ала белгіленген деректер жиынтығында модельді оқыту.
7. Біріккен кластер құрылымын және эмоцияларды сенімді тануды қамтамасыз ететін классификаторды құру.
8. Ансамбльдің жекелеген сегменттеріндегі қателерді бағалау.

9. Кластерлерді олардың арасындағы корреляцияны ескере отырып біріктіру.

10. Жоғары дәлдікпен кіріс деректерін соңғы классификациялау.

Қосымша дәлдікті арттыру үшін стекинг, бустинг және кездейсоқ ормандар сияқты ансамбльдік әдістерді қолдану ұсынылады, олар жеке алгоритмдердің шешімдерін біріктіру арқылы олардың кемшіліктерін өтеуге мүмкіндік береді.

Қорытынды. Ұсынылған эмоцияларды автоматты түрде тану жүйесі кескіндерді талдау және машиналық оқыту әдістерін қолдануға негізделген. Кохоненнің өзін-өзі ұйымдастыратын карталары мен кластерлік ансамбльдерді пайдалану нақты уақыт режимінде эмоцияларды жіктеу дәлдігін арттыруға мүмкіндік береді. Бұл архитектура бейнежазбаларды тиімді өңдеуді қамтамасыз етеді және адамның компьютермен интерактивті өзара әрекеттесу жүйелерінде, оның ішінде виртуалды көмекшілерде, қауіпсіздік жүйелерінде және психоэмоционалдық жағдайды диагностикалауда қолданылуы мүмкін.

Пайдаланылған әдебиеттер тізімі:

1. Кравченко А.И., Тюрина И.О. Социология управления. М.: Академический проект, 2005. С. 879.
2. Jianhua Zhang, Zhong Yin, Peng Chen Emotion recognition using multi-modal data and machine learning techniques: A tutorial and review. *Information Fusion*. Volume 59, July 2020, Pages 103-126. <https://doi.org/10.1016/j.inffus.2020.01.011>
3. Ali I. Siam , Naglaa F. Soliman , Abeer D. Algarni, Fathi E. Abd El-Samie, Ahmed Sedik Research Article Deploying Machine Learning Techniques for Human Emotion Detection *Hindawi Computational Intelligence and Neuroscience* Volume 2022, Article ID 8032673, 16 pages <https://doi.org/10.1155/2022/8032673>
4. Stefano Nichele aRathore, D. Design Hybrid method for intrusion detection using Ensemble cluster classification and SOM network / D. Rathore, A. Jain // *Int. Journal of Advanced Compute Research*. – 2012. – Vol. 2. – Num. 3. – P.181-186.
5. Wenqi Hua and Lingfei Mo Research Article Clustering Ensemble Model Based on Self-Organizing Map Network. *Hindawi Computational Intelligence and Neuroscience* Volume 2020, Article ID 2971565, 11 pages <https://doi.org/10.1155/2020/2971565>

УДК 004.855.5

Нұржанов Н.Ш.
(г. Астана, ЕНУ им. Л.Н. Гумилева)
Турарова М.К.
(г. Астана, ЕНУ им. Л.Н. Гумилева)

**ТҮЛҒАНЫҢ ЖАСЫ МЕН ЖЫНЫСЫН ТАНУҒА АРНАЛҒАН НЕЙРОНДЫҚ ЖЕЛІ
АЛГОРИТМДЕРІН ЗЕРТТЕУ**

Аннотация. Бұл жұмыста объектіні нейрондық желі алгоритмдері және олардың бейне өңдеудегі рөлі, деректерді өңдеу және модельді оқыту, жүйенің дәлдігін арттыру үшін үлкен көлемді бейне және сурет деректері, алдын ала дайындалатын модельдер (VGG-16, ResNet, EfficientNet) туралы зерттеліп, шолу жасалған.

Кілттік сөздер: нейрондық желілер, жасанды интеллект, CNN, UTKFace, Adience, VGG-16, ResNet, EfficientNet

Қазіргі таңда жасанды интеллект (ЖИ) технологиялары адам өмірінің түрлі салаларында белсенді қолданылуда [1]. Әсіресе, тұлғаның жасы мен жынысын автоматты түрде тану жүйелері қауіпсіздік, маркетинг, медицина және әлеуметтік зерттеулер салаларында ерекше маңызға ие. Нейрондық желілердің дамуымен бірге бұл технологиялар жоғары дәлдікке қол жеткізуге мүмкіндік береді. Бұл зерттеуде тұлғаның жасы мен жынысын тануға арналған нейрондық желі алгоритмдеріне [2] негізделген программалық қамтамасыздандыруды әзірлеу мәселелері қарастырылады.

Нейрондық желілер және олардың бейне өңдеудегі рөлі. Нейрондық желілер бейне өңдеуде, әсіресе бет-әлпетті тануда кеңінен қолданылады [3]. Convolutional Neural Networks (CNN) немесе сверткіштік нейрондық желілер бейнелерді талдау және олардың ерекшеліктерін анықтау үшін ең тиімді алгоритмдердің бірі болып табылады. Мұндай желілер бірнеше қабаттардан тұрады және олардың әрқайсысы белгілі бір деңгейдегі мәліметтерді өңдейді. Бет-әлпетті тану барысында CNN бейненің ерекшеліктерін шығарып, оларды алдын ала дайындалған мәліметтер жиынтығымен салыстырады [1].

Деректерді өңдеу және модельді оқыту. Жүйенің дәлдігін арттыру үшін үлкен көлемді бейне және сурет деректері қажет. Оқыту процесінде бейнелер аннотацияланып, жыныс пен жас ерекшеліктеріне қарай белгіленеді. Жиі қолданылатын дереккөздерге IMDB-WIKI, UTKFace және Adience сияқты мәліметтер жиынтықтары жатады. Сонымен қатар, Transfer Learning әдісі қолданылып, алдын ала дайындалған модельдер (VGG-16, ResNet, EfficientNet) жаңа деректерге бейімделеді. Бұл әдіс өңдеу жылдамдығын арттырып, жоғары дәлдікке қол жеткізуге көмектеседі.

Жүйені дамыту және тестілеу. Жасалған модельдің өнімділігін бағалау үшін әртүрлі тестілеу әдістері қолданылады. Олардың ішінде:

Нейрондық желілер және олардың бейне өңдеудегі рөлі. Нейрондық желілер бейне өңдеуде, әсіресе бет-әлпетті тануда кеңінен қолданылады [3]. Convolutional Neural Networks (CNN) немесе сверткіштік нейрондық желілер бейнелерді талдау және олардың ерекшеліктерін анықтау үшін ең тиімді алгоритмдердің бірі болып табылады. Мұндай желілер бірнеше қабаттардан тұрады және олардың әрқайсысы белгілі бір деңгейдегі мәліметтерді өңдейді. Бет-әлпетті тану барысында CNN бейненің ерекшеліктерін шығарып, оларды алдын ала дайындалған мәліметтер жиынтығымен салыстырады [1].

Деректерді өңдеу және модельді оқыту. Жүйенің дәлдігін арттыру үшін үлкен көлемді бейне және сурет деректері қажет. Оқыту процесінде бейнелер аннотацияланып, жыныс пен жас ерекшеліктеріне қарай белгіленеді. Жиі қолданылатын дереккөздерге IMDB-WIKI, UTKFace және Adience сияқты мәліметтер жиынтықтары жатады. Сонымен қатар, Transfer Learning әдісі қолданылып, алдын ала дайындалған модельдер (VGG-16, ResNet, EfficientNet) жаңа деректерге бейімделеді. Бұл әдіс өңдеу жылдамдығын арттырып, жоғары дәлдікке қол жеткізуге көмектеседі.

Жүйені дамыту және тестілеу. Жасалған модельдің өнімділігін бағалау үшін әртүрлі тестілеу әдістері қолданылады. Олардың ішінде:

Дәлдік (Accuracy): Жас пен жынысты дұрыс анықтау үлесі.

Precision және Recall: Ер және әйел адамдарды ажырату сапасы.

Confusion Matrix: Жүйенің дұрыс және қате болжамдарын талдау [4].

Тестілеу кезеңінде әртүрлі жарық жағдайлары, бет-әлпеттің әртүрлі ракурстары және бет-әлпеттің жасанды өзгерістері (бет-әлпетке макияж қолдану, көзілдірік кию, эмоциялардың өзгеруі) ескеріледі. Сонымен қатар, жүйенің тұрақтылығы мен жылдамдығы тексеріледі, себебі нақты уақыт режимінде жұмыс істейтін жүйелер үшін жоғары жылдамдық маңызды фактор болып табылады.

Қолдану салалары. Жасанды интеллект негізінде жасалған тұлғаның жасы мен жынысын анықтау жүйесі көптеген салаларда қолданылуы мүмкін [5]:

Қауіпсіздік: Бейнебақылау жүйелерінде тұлғаны автоматты түрде сәйкестендіру.

Маркетинг: Тұтынушылардың жас ерекшеліктерін ескере отырып, жарнамаларды бейімдеу.

Медицина: Пациенттердің жасы мен жынысына қарай диагностикалық шешімдерді оңтайландыру.

Әлеуметтік зерттеулер: Демографиялық талдаулар жүргізу.

Білім беру: Білім беру ұйымдарында студенттердің жас ерекшеліктерін ескере отырып, оқыту әдістерін бейімдеу.

Ойын индустриясы: Ойындарды пайдаланушы жасына қарай бейімдеу.

Нейрондық желілерге негізделген жыныс және жас анықтау жүйелерін жетілдіру үшін бірнеше бағытта жұмыс істеуге болады:

Жасанды интеллекттің түсіндірілуі: Модельдің шешім қабылдау процесін түсіндіру және пайдаланушыларға ашықтықты қамтамасыз ету.

Деректердің этикалық аспектілері: Жеке деректердің қорғалуын қамтамасыз ету және құпиялылықты сақтау.

Кросс-мәдени зерттеулер: Өртүрлі этностар мен мәдени топтардың ерекшеліктерін ескеру арқылы модельдің әділдігін қамтамасыз ету.

Жүйенің жылдамдығын арттыру: Ресурстарды оңтайландырып, нақты уақыт режимінде жылдам жауап беруді қамтамасыз ету.

Зерттеу нәтижесінде тұлғаның жасы мен жынысын анықтауға арналған жоғары дәлдікті программалық қамтамасыздандыру жасалады. Бұл жүйе адамның бет-әлпетін талдау арқылы жынысы мен жасын автоматты түрде анықтауға мүмкіндік береді. Жүйе қауіпсіздік, маркетинг, медицина және басқа да салаларда кеңінен қолданылуы мүмкін. Нейрондық желілердің дамуы бұл технологияның болашақта одан әрі жетілдірілуіне ықпал етеді.

Пайдаланылған әдебиеттер тізімі:

1. Parkhi O. M., Vedaldi A. & Zisserman A. (2015). *Deep Face Recognition*. BMVC.
2. Zhang Z., Song Y. & Qi. H. (2017). *Age Progression/Regression by Conditional Adversarial Autoencoder*. CVPR.
3. G. Levi and T. Hassner (2015). *Age and gender classification using convolutional neural networks*.
4. Rothe R., Timofte R. & Van Gool L. (2016). *Deep Expectation of Real and Apparent Age from a Single Image Without Facial Landmarks*. IJCV.
5. He K., Zhang X., Ren S. & Sun J. (2016). *Deep Residual Learning for Image Recognition*. CVPR.

УДК004.4:658.5

Ныгыманов Б.А.
(Алматы, КазНУ им. аль-Фараби)
Ахметова А.А., PhD, ст. преп.
(Алматы, КазНУ им. аль-Фараби)
Зиятбекова Г.З.* PhD, и.о. доцента
(Алматы, КазНУ им. аль-Фараби; АТУ)

РАЗРАБОТКА СИСТЕМЫ ВИЗУАЛИЗАЦИИ ДАННЫХ ДЛЯ МОНИТОРИНГА ПРОИЗВОДСТВЕННЫХ ПРОЦЕССОВ С ИСПОЛЬЗОВАНИЕМ GRAFANA И PROMETHEUS

Абстракт. В статье представлена разработка прототипа системы визуализации данных для мониторинга производственных процессов с применением инструментов с открытым исходным кодом — Grafana и Prometheus. Целью работы является создание доступного решения для анализа параметров оборудования в условиях ограниченных ресурсов. В рамках исследования реализован генератор данных, имитирующий показатели 10 датчиков (температура, давление, энергопотребление), настроена система хранения данных в Prometheus и разработан дашборд в Grafana для визуализации. Прототип позволяет отображать динамику параметров, текущие значения и сигнализировать о превышениях. Результаты демонстрируют применимость системы для образовательных целей и небольших производств, а также её потенциал для дальнейшего масштабирования.

Ключевые слова: мониторинг, визуализация данных, Grafana, Prometheus, производственные процессы, Индустрия 4.0.

Введение. Современное промышленное производство всё больше опирается на технологии цифровизации, что подчёркивает важность мониторинга производственных процессов. В условиях Индустрии 4.0 данные становятся ключевым ресурсом для управления, позволяя оптимизировать работу оборудования, предотвращать сбои и повышать эффективность. Однако внедрение систем мониторинга часто связано с высокими затратами, что делает актуальной разработку доступных решений, особенно для небольших предприятий и образовательных целей. Целью данной работы является разработка прототипа системы визуализации данных для мониторинга производственных процессов с использованием инструментов с открытым исходным кодом — Grafana и Prometheus. Эти инструменты выбраны благодаря их популярности, простоте настройки и гибкости. Задачи исследования включают создание генератора данных, настройку системы хранения, разработку визуального интерфейса и тестирование прототипа. В статье описаны этапы реализации, результаты работы системы и перспективы её применения.

Мониторинг производственных процессов включает сбор, хранение и анализ данных, поступающих от оборудования. Визуализация играет ключевую роль, преобразуя числовую информацию в наглядные формы, такие как графики и таблицы, что ускоряет принятие решений. В отличие от традиционных систем с непрерывным сбором данных, в данной работе применён детерминированный подход с периодическим обновлением, что снижает нагрузку на ресурсы и упрощает реализацию. Особое внимание уделено адаптации системы под ограниченные вычислительные ресурсы, что делает её подходящей для образовательных целей и небольших производственных объектов.

1. Теоретические основы мониторинга и визуализации. Мониторинг производственных процессов направлен на контроль параметров оборудования и среды, таких как температура, давление и энергопотребление. В условиях Индустрии 4.0 данные собираются с датчиков,

обрабатываются и преобразуются в информацию, пригодную для анализа [6]. Основные этапы мониторинга включают сбор данных, их структурированное хранение и последующую визуализацию. Визуализация позволяет операторам и инженерам быстро выявлять отклонения, что особенно важно в металлургии, химической промышленности и других отраслях, где стабильность параметров критически влияет на качество продукции [5].

Prometheus представляет собой систему хранения временных рядов, которая собирает метрики через HTTP-запросы и предоставляет их для анализа. Она поддерживает язык запросов PromQL, позволяющий выполнять сложные вычисления, такие как агрегация, фильтрация и прогнозирование [1]. Grafana, в свою очередь, является инструментом визуализации, поддерживающим создание дашбордов с графиками, таблицами и индикаторами. Grafana интегрируется с Prometheus через API, что позволяет запрашивать данные и отображать их в реальном времени [2]. Комбинация этих инструментов позволяет создать гибкое и масштабируемое решение для мониторинга, доступное даже при ограниченных ресурсах.

2. Проектирование системы. Разработка прототипа началась с определения требований. Система должна собирать данные от нескольких источников, имитирующих производственные датчики, сохранять их за определённый период и предоставлять пользователю удобный интерфейс для анализа. В отсутствие реального оборудования данные генерируются программно, моделируя типичные сценарии производства [4]. Требования включают минимальную сложность настройки, оперативную обработку информации и возможность работы на стандартном персональном компьютере с 4 ГБ ОЗУ и 2 ядрами.

Архитектура системы включает три основных компонента: генератор данных, Prometheus и Grafana. Генератор, реализованный на Python, имитирует 10 датчиков: 5 датчиков температуры (furnace1–furnace5), 3 датчика давления (tank1–tank3) и 2 датчика энергопотребления (motor1–motor2). Данные обновляются с заданной периодичностью и предоставляются через HTTP. Prometheus собирает эти данные и хранит их как временные ряды, а Grafana запрашивает данные у Prometheus и отображает их через дашборд. Все компоненты размещены локально на одном устройстве, что упрощает настройку и исключает сетевые зависимости. Для обеспечения стабильности работы системы были учтены возможные ограничения, такие как низкая производительность оборудования и ограниченный объём дискового пространства [3].

3. Реализация прототипа. Реализация прототипа выполнялась в несколько этапов. На первом этапе была подготовлена рабочая среда: на компьютере под управлением Windows 10 установлены Python 3.12, Prometheus (версия 2.47.0) и Grafana (версия 10.1.0). Для редактирования кода использовался Visual Studio Code, что позволило упростить процесс написания и отладки скриптов. Генератор данных реализован с использованием библиотеки prometheus_client, которая позволяет предоставлять метрики в формате, совместимом с Prometheus. Данные генерируются с интервалом 1 минута, что обеспечивает достаточную частоту обновления для тестирования. Для имитации реальных условий значения параметров изменяются случайным образом в заданных диапазонах: температура — от 140 до 170 °C, давление — от 4 до 6 бар, энергопотребление — от 40 до 80 кВт. На рисунке 1 представлен пример метрик, предоставляемых генератором.

```
temperature{device="furnace1"} 145.3306711350526
temperature{device="furnace2"} 162.67038718057046
temperature{device="furnace3"} 141.76441501219404
temperature{device="furnace4"} 167.69599129709636
temperature{device="furnace5"} 147.86352420408608
```

Рисунок 1. Метрики генератора данных на

Prometheus настроен для сбора данных с генератора через HTTP-запросы. Конфигурация включает указание целевого адреса (localhost:8000) и интервала сбора (1 минута). Данные хранятся в базе временных рядов и доступны через веб-интерфейс Prometheus. В процессе настройки были решены проблемы с доступом к портам: порты 8000 и 9090 были освобождены от других процессов, а также добавлены правила в брандмауэр Windows для разрешения входящих подключений. Это позволило обеспечить стабильный сбор данных. На рисунке 2 показан график температуры одного из датчиков, отображённый в интерфейсе Prometheus.



Рисунок 2. График температуры в веб-интерфейсе Prometheus

Grafana подключена к Prometheus как источник данных, что позволяет запрашивать метрики и отображать их в виде графиков, таблиц и индикаторов. Дашборд в Grafana включает три панели. Первая панель отображает динамику температуры для пяти датчиков в виде графиков, что позволяет анализировать изменения во времени. Вторая панель представляет текущие значения давления в виде таблицы с пороговым значением (8 бар), выделяя превышения красным цветом. Третья панель — кастомная визуализация энергопотребления, включающая график и индикатор, который сигнализирует о высоких нагрузках при превышении порога в 80 кВт. Настройка дашборда потребовала использования языка запросов PromQL для фильтрации данных по устройствам и применения пороговых значений для визуального выделения критических состояний.

4. Тестирование системы. Прототип тестировался в течение 48 часов на компьютере с 4 ГБ ОЗУ и 2 ядрами. За это время было собрано более 2800 записей (10 датчиков × 60 минут × 48 часов). Система показала стабильную работу: данные собирались и отображались корректно, без сбоев. Ресурсоёмкость оставалась минимальной: использование CPU не превышало 15%, а ОЗУ — 900 МБ. Интервал обновления 1 минута позволил быстро увидеть динамику изменений, что особенно полезно для образовательных целей.

В процессе тестирования были выявлены и устранены несколько проблем. Например, изначально данные не поступали в Prometheus из-за конфликта портов, что потребовало освобождения порта 8000 и настройки правил брандмауэра. Также были временно изменены интервалы обновления (с 1 часа до 1 минуты) для ускорения проверки, что позволило оперативно оценить работу системы. Для анализа производительности использовался диспетчер задач Windows, который показал, что система не создаёт значительной нагрузки даже при частом обновлении данных. Дополнительно были проведены тесты с различными диапазонами времени в Grafana (от 5 минут до 7 дней), чтобы убедиться в корректности отображения данных за разные периоды.

Результаты. В результате исследования был создан прототип системы визуализации данных для мониторинга производственных процессов. Дашборд в Grafana предоставляет удобный интерфейс для анализа: графики температуры показывают изменения во времени, таблица давления отображает текущие значения с выделением критических состояний, а кастомный индикатор энергопотребления сигнализирует о превышениях. На рисунке 3 представлен дашборд, демонстрирующий все три панели.



Рисунок 3. Дашборд Production Monitoring в Grafana

Система демонстрирует применимость Grafana и Prometheus для задач мониторинга, предлагая простое и функциональное решение. Прототип отличается минимальными требованиями к ресурсам, что делает его подходящим для использования в образовательных учреждениях и на небольших предприятиях. Оригинальность работы заключается в адаптации визуальных элементов под задачи мониторинга, включая кастомный индикатор, который выделяет проект среди стандартных решений. Сравнение с другими подходами показывает преимущества разработанного прототипа. Например, коммерческие системы мониторинга, такие как Siemens MindSphere, требуют значительных затрат на лицензии и оборудование, тогда как предложенное решение использует бесплатные инструменты и работает на стандартном компьютере. В то же время, прототип уступает промышленным системам в масштабируемости и поддержке сложных сценариев, таких как обработка данных в реальном времени с тысяч датчиков. Однако для образовательных целей и небольших производств эти ограничения не критичны, а простота настройки и доступность делают систему конкурентоспособной. Анализ результатов тестирования показал, что система может быть адаптирована под различные сценарии. Например, изменение интервала обновления данных позволяет балансировать между частотой обновления и нагрузкой на оборудование. Также возможно расширение функциональности за счёт добавления новых метрик, таких как вибрация или уровень шума, что сделает систему более универсальной. В целом, прототип демонстрирует потенциал для применения в реальных условиях после доработки, связанной с подключением физических датчиков.

Заключение. Разработанный прототип системы мониторинга производственных процессов с использованием Grafana и Prometheus достиг поставленной цели. Система позволяет собирать, хранить и визуализировать данные от имитированных датчиков, предоставляя наглядный интерфейс для анализа. Тестирование подтвердило стабильность и низкую ресурсоёмкость прототипа, что делает его перспективным для образовательных целей и небольших производств. В перспективе возможно подключение реальных источников данных через современные протоколы,

такие как MQTT, а также переход к облачной архитектуре для промышленного применения. Дальнейшие исследования могут быть направлены на интеграцию с системами автоматизации и внедрение алгоритмов прогнозирования на основе собранных данных. Также стоит рассмотреть возможность добавления уведомлений (например, через email или мессенджеры) для оперативного информирования о критических состояниях.

Литература

6. *Prometheus Documentation* [Электронный ресурс]. — Режим доступа: <https://prometheus.io/docs/>, свободный. — Загл. с экрана.
7. *Grafana Documentation* [Электронный ресурс]. — Режим доступа: <https://grafana.com/docs/>, свободный. — Загл. с экрана.
8. Smith, J. *Monitoring with Prometheus*. — O'Reilly Media, 2018. — 386 p.
9. Jones, R. *Data Visualization in Industry 4.0: Tools and Techniques*. — Springer, 2020. — 245 p.
10. Иванов А.А. *Основы мониторинга производственных процессов*. — М.: Изд-во МГТУ, 2019. — 180 с.
11. Ковалёв В.П. *Индустрия 4.0: Цифровизация производства*. — СПб.: Питер, 2021. — 210 с.

УДК 621.644.2.

Оразтаев Д.М. (Астана, ЕНУ)

МЕТОДЫ НЕРАЗРУШАЮЩЕГО КОНТРОЛЯ ДЛЯ ОЦЕНКИ СТЕПЕНИ ИЗНОСА ТРУБОПРОВОДОВ: СОВРЕМЕННЫЕ ПОДХОДЫ

Аннотация. В данной работе рассматриваются современные методы неразрушающего контроля (НК) трубопроводов, предназначенных для транспортировки жидких сред. Применение методов НК позволяет выявлять дефекты трубопровода не выводя оборудование из эксплуатации и не повреждает объект исследования. Данные методы позволяют выявлять критические дефекты на ранних стадиях их возникновения, что способствует своевременному принятию мер по их устранению и, как следствие, сокращению эксплуатационных затрат. После проведения неразрушающего контроля полученные данные анализируются специалистами, на основании чего эксперты формируют заключение о техническом состоянии трубопровода и прогнозируемом сроке его дальнейшей эксплуатации.

Ключевые слова: неразрушающий контроль, техническое освидетельствование, экспертиза промышленной безопасности, Контроль проникающими веществами, гидроиспытания, визуального измерительного контроль, ультразвуковая толщинометрия, Контроль проникающими веществами, Замер твердости, ультразвуковой контроль, магнитопорошковая дефектоскопия.

Оценка степени износа трубопроводов играет ключевую роль в обеспечении безопасной эксплуатации данных объектов. НК дает возможность определить ключевые параметры состояния трубопровода. Преждевременный износ трубопроводов способствует возникновению аварийных ситуаций, создающих угрозу безопасности людей и приводящих к существенным экономическим потерям. В связи с этим необходимо регулярно проводить техническое освидетельствование и экспертизу промышленной безопасности. НК позволяет определить ключевые параметры состояния трубопровода, что способствует своевременному выявлению дефектов и прогнозированию его

дальнейшей эксплуатации. Техническое освидетельствование – это регулярное мероприятие, направленное на оценку текущего состояния трубопровода в процессе его эксплуатации. Экспертиза промышленной безопасности (ЭПБ) проводится для выявления рисков и определения остаточного ресурса трубопровода. На основе заключения ЭПБ принимается решение о продлении срока службы трубопровода, необходимости его ремонта или замены.

Методология оценки степени износа трубопровода:

1. Проведение визуального измерительного контроля. Проверка на видимые дефекты (трещины, коррозия, изломы, утечки) трубопровода.
2. Подготовка мест контроля в соответствии инструкции по безопасности при эксплуатации технологических трубопроводов.
3. Проведение ультразвуковой толщинометрии для определения остаточной толщины стенки трубы.
4. Контроль проникающими веществами (ПВК) сварных соединений для выявления дефектов в сварных швах (трещины, поры или неполные сварные швы).
5. Замер твердости (ЗТ) металла определяет механические свойства и способность сопротивляться износу.
6. На месте термической обработки проводится ультразвуковой контроль (УЗК)
7. Проведение гидроиспытаний (ГИ) прочности трубопровода на выдержку внутреннего давления.
8. Анализ полученных данных
9. Формирования протокола
10. Выдача заключения

Основные виды НК:

- Визуально-измерительный контроль
- Контроль проникающими веществами (пвк)
- Магнитопорошковая дефектоскопия (мпд)
- Замер твердости (зт)
- Ультразвуковая толщинометрия (узт)
- Ультразвуковой контроль (узк)

Например. На цехе № 12, секции 600, линии перегонки сероводорода с номером 55/6 был заменен прямой участок линии протяженностью 5 метров. Необходимо провести ЭПБ данного участка линии. Алгоритм проведения контроля:

- Зачистка места термической обработки.
- Проведение визуального и измерительного контроля (ВиК).
- Контроль проникающими веществами (ПВК) сварных соединений.
- Ультразвуковой контроль (УЗК).
- Проведение гидроиспытаний (ГИ).

Контроль с применением методов НК был проведен дефектоскопистом второго уровня. Контроль является входным, так как участок трубопровода был заменен. После проведения контроля и испытаний составляются акты по каждому методу НК и по гидроиспытаниям. Акты по проведенным методам выдаются начальнику участка для хранения в бумажном варианте в течение 5 лет. Акт является эталонным документом при проведении последующих проверок. Также акт вносится в паспортные данные линии трубопровода.

Полученные данные вносятся в рабочую карту с участка проведения контроля. На основании рабочей карты составляется протокол трубопровода. Протокол передается в экспертно-методический отдел, где экспертами выдается заключение, которое передается в отдел надежности. Заключение вносится в паспортные данные линии трубопровода.

Соблюдение алгоритма проверки НК и проведение комплекса аналитических работ являются важными условиями для обеспечения дальнейшей безопасной эксплуатации трубопроводной линии.

Применение методов НК при обследовании трубопроводов порождает обратные задачи при анализе полученных данных с целью восстановления характеристик исследуемого объекта без его разрушения. Малые ошибки в решении обратных задач в НК могут привести к значительному эффекту. Поэтому для повышения точности интерпретации данных необходимо разработать программу на основе машинного обучения.

Таким образом, комплексный подход, сочетающий НК и теорию обратных задач, является ключевым элементом системы контроля износа трубопроводов.

Список использованных источников

1. Приказ Министра по чрезвычайным ситуациям Республики Казахстан от 27 июля 2021 года № 359. Зарегистрирован в Министерстве юстиции Республики Казахстан 29 июля 2021 года № 23754. Информационно-правовая система нормативных правовых актов Республики Казахстан

2. ПЕРЕЧЕНЬ международных и региональных (межгосударственных) стандартов, а в случае их отсутствия – национальных (государственных) стандартов, в результате применения которых на добровольной основе обеспечивается соблюдение требований технического регламента Евразийского экономического союза "О требованиях к магистральным трубопроводам для транспортирования жидких и газообразных углеводородов" (ТР ЕАЭС 049/2020) О перечне международных и региональных (межгосударственных) стандартов, а в случае их отсутствия – национальных (государственных) стандартов, в результате применения которых на добровольной основе обеспечивается соблюдение требований технического регламента Евразийского экономического союза "О требованиях к магистральным трубопроводам для транспортирования жидких и газообразных углеводородов" (ТР ЕАЭС 049/2020), и перечне международных и региональных (межгосударственных) стандартов, а в случае их отсутствия – национальных (государственных) стандартов, содержащих правила и методы исследований (испытаний) и измерений, в том числе правила отбора образцов, необходимые для применения и исполнения требований технического регламента Евразийского экономического союза "О требованиях к магистральным трубопроводам для транспортирования жидких и газообразных углеводородов" (ТР ЕАЭС 049/2020) и осуществления оценки соответствия объектов технического регулирования - ИПС "Әділет"

УДК 004.896

Оспанов А.Д. (Астана, Евразийский национальный университет им. Л.Н. Гумилёва)

ОПТИМИЗАЦИЯ МОНИТОРИНГА СКЛАДА С ПОМОЩЬЮ ИОТ-ДАТЧИКОВ И МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ: ЭМПИРИЧЕСКОЕ ИССЛЕДОВАНИЕ ПО ОБНАРУЖЕНИЮ ГРЫЗУНОВ И УПРАВЛЕНИЮ ОКРУЖАЮЩЕЙ СРЕДОЙ

Аннотация: В настоящем исследовании представлена методология, объединяющая данные IoT-датчиков и алгоритмы машинного обучения для оптимизации мониторинга складских помещений. Предлагаемая система решает две ключевые задачи: обнаружение активности грызунов посредством анализа данных с датчиков движения и выявление экологических рисков (например,

аномалий в показателях температуры, влажности и уровня газов), свидетельствующих о возможной порче продукции. Для проверки работоспособности системы используется симулированный набор данных, охватывающий 30-дневный период с почасовой дискретизацией, где ключевые события маркируются как «грызун обнаружен» и «предупреждение о порче». Основным алгоритмом классификации выбран Random Forest, обеспечивающий точность обнаружения около 95,24%. Дополнительно проведено сравнение с альтернативными моделями (логистическая регрессия, SVM, Gradient Boosting, нейронные сети). Помимо технической реализации, в работе представлен анализ экономической эффективности, демонстрирующий высокую рентабельность внедрения системы.

Ключевые термины: IoT, машинное обучение, мониторинг склада, Random Forest, обнаружение грызунов, управление окружающей средой.

Введение: Эффективное управление складскими помещениями является неотъемлемой частью современных ERP-систем и критически важно для оптимизации цепочки поставок и контроля запасов. Традиционные системы мониторинга зачастую не обеспечивают необходимого уровня оперативности и точности, что обуславливает необходимость внедрения современных технологий. В данной работе предлагается интеграция IoT-датчиков с методами машинного обучения для реализации интеллектуальной системы мониторинга, способной в реальном времени выявлять аномальные ситуации и обеспечивать проактивное реагирование.

Современные исследования в области IoT и ML демонстрируют значительный прогресс в автоматизации процессов мониторинга и анализа данных. Ряд работ подтверждает необходимость перехода от традиционных методов к интеллектуальным системам, способным обеспечить непрерывный сбор и анализ информации. В дополнение к базовым подходам, исследования и демонстрируют, что использование ансамблевых методов, таких как Random Forest, позволяет повысить точность классификации и снизить вероятность ложных срабатываний.

Материалы и методы: Исследование реализовано на языке Python с использованием библиотек TensorFlow, Scikit-learn и NumPy, что позволило обеспечить эффективную обработку и анализ сенсорных данных. Система включает следующие ключевые этапы:

- **Симуляция данных:** Создан синтетический набор данных, отражающий параметры температуры, влажности, уровня газа и активности движения. Данные генерируются с учётом случайной изменчивости, что приближает их к реальным условиям эксплуатации.

- **Предварительная обработка и анализ:** Применены методы нормализации и разбиения данных, что позволило оптимизировать входные параметры для последующего обучения модели.

- **Машинное обучение:** Классификатор Random Forest обучен на симулированном наборе данных для выявления аномальных ситуаций.

- **Оценка эффективности:** Рассчитаны ключевые метрики качества классификации (точность, прецизионность, отзыв, F1-мера), а также проведён анализ затрат и выгод, демонстрирующий возврат инвестиций (ROI) порядка 108%.

- **Результаты и обсуждение:** Экспериментальная проверка показала, что система на основе Random Forest достигает точности обнаружения порядка 95,24%, что подтверждает её высокую работоспособность в условиях имитации реального склада. Проведённый сравнительный анализ выявил преимущества ансамблевых методов перед традиционными алгоритмами классификации. Дополнительно, анализ затрат и выгод демонстрирует экономическую эффективность внедрения системы, позволяющей существенно сократить операционные расходы за счёт автоматизации мониторинга и оперативного реагирования на возникающие аномалии.

Заключение: Представленное исследование подтверждает, что интеграция данных IoT-датчиков и методов машинного обучения является перспективным направлением для оптимизации мониторинга складских помещений. Применение алгоритма Random Forest обеспечивает высокую точность обнаружения аномалий, а проведённый экономический анализ свидетельствует о

значительной рентабельности предлагаемого подхода. В дальнейшем планируется расширение функциональности системы посредством внедрения методов обучения с подкреплением, федеративного обучения и разработки цифровых двойников для повышения адаптивности и предиктивного потенциала системы.

Список литературы

1. Аббас, Г. и соавт. (2024). Двухступенчатый метод оптимизации реактивной мощности для умных энергосетей. *IEEE Transactions on Power Systems*. [на англ.].
2. Амбулут, О. и соавт. (2024). Гибридная интеллектуальная система управления для адаптивной оптимизации микросетей. *Energies*. [на англ.].
3. Ахтер, Р. и Бейетт, Ф. (2022). Алгоритмы машинного обучения для обнаружения зашумленных/искажённых артефактами эпох в IoT-системах. *IEEE Access*. [на англ.].
4. Азеведо, Б. Ф. и соавт. (2024). Гибридные подходы к оптимизации и методам машинного обучения в промышленных приложениях. *Springer*. [на англ.].
5. Добра, П. и Джосвай, Дж. (2024). Прогнозирование общей эффективности оборудования с использованием данных IoT. *IEEE Transactions on Industrial Informatics*. [на англ.].

УДК 517.588, 519.632

Рысқан А.Р., Джабаева М. Н.
(Алматы, Абай атындағы ҚазҰПУ)

РЕШЕНИЕ СИСТЕМЫ ДИФФЕРЕНЦИАЛЬНЫХ УРАВНЕНИЙ В ЧАСТНЫХ ПРОИЗВОДНЫХ ВТОРОГО ПОРЯДКА ДЛЯ ГИПЕРГЕОМЕТРИЧЕСКОЙ ФУНКЦИИ $F(4)_{18}$

Актуальность решения прикладных задач, связанных с построением математических моделей физических процессов и прогнозированием их результатов, обуславливает непрерывное изучение свойств гипергеометрических функций многих переменных. Математические модели, описывающие физические процессы, как правило, включают обыкновенные дифференциальные уравнения, дифференциальные уравнения в частных производных или системы таких уравнений. Однако лишь ограниченное число уравнений, моделирующих реальные процессы, допускает решения в классе элементарных функций. Новые функции определялись как решения дифференциальных уравнений или их систем, и получили названия специальных или трансцендентных функций [1], [2]. Примерами служат функции Бесселя, функции Эрмита и гипергеометрическая функция Гаусса.

Существует несколько подхода к определению гипергеометрических функций многих переменных. Эти функции могут быть определены как: суммы степенных рядов; решения систем дифференциальных уравнений; Эйлеровы интегралы; интегралы вида Меллина-Барнса. В настоящей работе мы гипергеометрическую функцию рассматриваем как решение системы дифференциальных уравнений.

Рассмотрим гипергеометрическую функцию [3]:

$$F_{18}^{(4)}(a_1, a_2, b_1, b_2; c_1, c_2, c_3; x, y, z, t) = \sum_{m,n,p,q=0}^{\infty} \frac{(a_1)_{m+n+p}(a_2)_q(b_1)_{m+n}(b_2)_{p+q}}{(c_1)_{m+q}(c_2)_n(c_3)_p} \frac{x^m y^n z^p t^q}{m! n! p! q!} \quad (1)$$

Из теории гипергеометрических функций [1], [2], [4] известно, что функция $F_{18}^{(4)}$ удовлетворяет следующей системе дифференциальных уравнений в частных производных второго порядка:

$$\begin{aligned}
 & \{x(1-x)u_{xx} - 2xyu_{xy} - xzu_{xz} + tu_{xt} + (c_1 - (a_1 + b_1 + 1)x)u_x - y^2u_{yy} - yzu_{yz} \\
 & \quad - (a_1 + b_1 + 1)yu_y - b_1zu_z - a_1b_1u \\
 & = 0 \ y(1-y)u_{yy} - 2xyu_{xy} - x^2u_{xx} - xzu_{xz} - yzu_{yz} - (a_1 + b_1 + 1)xu_x \\
 & \quad + (c_2 - (a_1 + b_1 + 1)y)u_y - b_1zu_z - a_1b_1u \\
 & = 0 \ z(1-z)u_{zz} - xzu_{xz} - xtu_{xt} - yzu_{yz} - ytu_{yt} - ztu_{zt} + (c_3 - (a_1 + b_2 + 1)z)u_z \\
 & \quad - a_1tu_t - b_2xu_x - b_2yu_y - a_1b_2u \\
 & = 0 \ t(1-t)u_{tt} + xu_{xt} - tzu_{tz} + (c_1 - (a_2 + b_2 + 1)t)u_t - a_2zu_z - a_2b_2u = 0,
 \end{aligned}
 \tag{2}$$

где $u(x, y, z, t) = F_{18}^{(4)}(a_1, a_2, b_1, b_2; c_1, c_2, c_3; x, y, z, t)$

Решение системы будем искать в виде:

$$u = x^\alpha y^\beta z^\gamma t^\delta \omega, \tag{3}$$

где ω — неизвестная функция, $\alpha, \beta, \gamma, \delta$ — константы, подлежащие определению. Подставляя $x^\alpha y^\beta z^\gamma t^\delta \omega$ в систему уравнений (2), получаем следующую систему дифференциальных уравнений в частных производных:

$$\begin{aligned}
 & \{x(1-x)\omega_{xx} - 2xy\omega_{xy} - xz\omega_{xz} + t\omega_{xt} - y^2\omega_{yy} - yz\omega_{yz} + [C_1 - (A_1 + B_1 + 1)x]\omega_x - \\
 & (A_1 + B_1 + 1)y\omega_y - B_1z\omega_z + \alpha x^{-1}\omega_t + (\alpha(\alpha + \delta + c_1 - 1)x^{-1} - B_1A_1)\omega = 0 \ y(1-y)\omega_{yy} - \\
 & x^2\omega_{xx} - 2xy\omega_{xy} - xz\omega_{xz} - yz\omega_{yz} + [C_2 - (A_1 + B_1 + 1)y]\omega_y - (A_1 + B_1 + 1)x\omega_x - B_2z\omega_z + \\
 & (\beta(c_2 + \beta - 1)y^{-1} - B_1A_1 - B_2\gamma)\omega = 0 \ z(1-z)\omega_{zz} - xz\omega_{xz} - yz\omega_{yz} - zt\omega_z - xt\omega_{xt} - yt\omega_{yt} - \\
 & B_2x\omega_x - B_2y\omega_y + [C_3 - (A_1 + B_2 + 1)z]\omega_z - A_1t\omega_t + (\gamma(c_3 + \gamma - 1)z^{-1} - A_1B_2)\omega = \\
 & 0 \ t(1-t)\omega_{tt} + x\omega_{xt} - tzu_{tz} + [C_1 - (A_2 + B_2 + 1)t]\omega_t + x\delta t^{-1}\omega_x - A_2z\omega_z - (\delta(c_1 + \alpha + \delta - \\
 & \quad 1)t^{-1} - B_2A_2)\omega = 0
 \end{aligned}
 \tag{4}$$

где

$$\begin{aligned}
 & A_1 = \alpha + \beta + a_1, \quad A_1 = \alpha + \beta + \gamma + a_1, \quad A_2 = \delta + a_2, \\
 & B_1 = \alpha + \beta + b_1, \quad B_2 = \alpha + \beta + b_2, \quad B_2 = \gamma + \delta + b_2, \\
 & C_1 = c_1 + 2\alpha + \delta, \quad C_1 = c_1 + \alpha + 2\delta, \quad C_2 = 2\beta + c_2, \quad C_3 = 2\gamma + c_3
 \end{aligned}
 \tag{5}$$

Системы (2) и (4) являются эквивалентными, при выполнении следующих условий:

$$\{\alpha(c_1 + \alpha + \delta - 1) = 0 \ \beta(c_2 + \beta - 1) = 0 \ \gamma(c_3 + \gamma - 1) = 0 \ \delta(c_1 + \alpha + \delta - 1) = 0\}
 \tag{6}$$

Решение системы (6) могут быть записаны в виде четырех комбинаций:

	1	2	3	4
α :	0	0	0	0
β :	0	$1 - c_2$	0	$1 - c_2$
γ :	0	0	$1 - c_3$	$1 - c_3$

(7)

$\delta:$	0	0	0	0

Таким образом, подставляя решения системы (7) в уравнения (3) выполняя необходимые упрощения, получим линейно независимые решения [5] системы дифференциальных уравнений в частных производных второго порядка (2) в виде следующих четырех гипергеометрических функций:

$$u_1(x, y, z, t) = F_{18}^{(4)}(a_1, a_2, b_1, b_2; c_1, c_2, c_3; x, y, z, t) \\ = \sum_{m,n,p,q=0}^{\infty} \frac{(a_1)_{m+n+p}(a_2)_q(b_1)_{m+n}(b_2)_{p+q}}{(c_1)_{m+q}(c_2)_n(c_3)_p} \frac{x^m y^n z^p t^q}{m! n! p! q!}$$

$$u_2(x, y, z, t) = y^{1-c_2} F_{18}^{(4)}(a_1 + 1 - c_2, a_2, b_1 + 1 - c_2, b_2; c_1, 2 - c_2, c_3; x, y, z, t) \\ = y^{1-c_2} \sum_{m,n,p,q=0}^{\infty} \frac{(a_1+1-c_2)_{m+n+p}(a_2)_q(b_1+1-c_2)_{m+n}(b_2)_{p+q}}{(c_1)_{m+q}(2-c_2)_n(c_3)_p} \frac{x^m y^n z^p t^q}{m! n! p! q!}$$

$$u_3(x, y, z, t) = z^{1-c_3} F_{18}^{(4)}(a_1 + 1 - c_3, a_2, b_1, b_2 + 1 - c_3; c_1, c_2, 2 - c_3; x, y, z, t) \\ = \sum_{m,n,p,q=0}^{\infty} \frac{(a_1)_{m+n+p}(a_2)_q(b_1)_{m+n}(b_2+1-c_3)_{p+q}}{(c_1)_{m+q}(c_2)_n(2-c_3)_p} \frac{x^m y^n z^p t^q}{m! n! p! q!}$$

$$u_4(x, y, z, t) \\ = y^{1-c_2} z^{1-c_3} F_{18}^{(4)}(a_1 + 2 - c_2 - c_3, a_2, b_1 + 1 - c_2, b_2 + 1 - c_3; c_1, 2 - c_2, 2 - c_3; x, y, z, t) \\ = \sum_{m,n,p,q=0}^{\infty} \frac{(a_1 + 2 - c_2 - c_3)_{m+n+p}(a_2)_q(b_1 + 1 - c_2)_{m+n}(b_2 + 1 - c_3)_{p+q}}{(c_1)_{m+q}(2-c_2)_n(2-c_3)_p} \frac{x^m y^n z^p t^q}{m! n! p! q!}$$

Литература

1. Appell, P., Kampee de Feeriet, J. Fonctions Hypergeometriques et Hyperspheriques. Paris.: Gauthier-Villars, 1926. - 440 p.
2. Erdeelyi, A., Magnus, W., Oberhettinger, F., Tricomi, F.G. Higher Transcendental Functions. New York, Toronto and London: V. I. McGraw Hill, 1953.
3. Sharma, C., Parihar, C.L. Hypergeometric functions of four variables. Indian Academy of Mathematics, - Vol. 11, 1989, - P. 121-133.
4. Exton, H. Multiple Hypergeometric Functions and Applications. London.: Halsted Press, 1976.
5. Bin-Saad, MG., Hasanov, A. Linear Independent Solutions and Operational Representations for Hypergeometric Functions of Four Variables. Hindawi Publishing Corporation, Chinese Journal of Mathematics, - Vol.2014, (Article ID 273064), 6 p., 2014.

УДК 517.588, 519.632

Рысқан А.Р., Мендигалиева Г. Р.,
Хасан А. А. (Алматы, Абай атындағы ҚазҰПУ)

F₁₂(4) ГИПЕРГЕОМЕТРИЯЛЫҚ ФУНКЦИЯСЫ ҮШІН ЕКІНШІ РЕТТІ ДЕРБЕС ТУЫНДЫЛЫ ДИФФЕРЕНЦИАЛДЫҚ ТЕНДЕУЛЕР ЖҮЙЕСІН ШЕШУ

Аннотация. Бұл мақалада төрт айнымалы гипергеометриялық $F_{12}^{(4)}$ функциясы үшін екінші ретті дербес туындылы дифференциалдық тендеулер жүйесін шешуге арналған. Жүйенің сызықты тәуелсіз төрт шешімдері анық түрде көрсетілген.

Кілттік сөздер: төрт айнымалы гипергеометриялық функция, екінші ретті дербес туындылы дифференциалдық тендеу, сызықтық тәуелсіз шешімдері.

1. Кіріспе

Бүгінгі таңда математикалық физика, ықтималдық теориясы және қолданбалы математиканың көптеген салаларында гипергеометриялық функциялар айрықша орын алады. Гипергеометриялық функциялар әртүрлі математикалық модельдерді сипаттауда, сонымен қатар күрделі дифференциалдық тендеулерді шешуде маңызды құрал ретінде қолданылады. Жаңа функциялар әдетте дифференциалдық тендеулер немесе олардың жүйелерінің шешімдері ретінде анықталды және олар арнайы функциялар деп аталады [1], [2]. Осылардың қатарына Бессель функциялары, Эрмит функциялары және Гаусс гипергеометриялық функциялары енеді.

Бұл жұмыста төрт айнымалы гипергеометриялық $F_{12}^{(4)}$ функциясы қарастырылып, оған сәйкес екінші ретті дербес туындылы дифференциалдық тендеулер жүйесінің сызықты тәуелсіз шешімдері анықталады. Осы зерттеу нәтижелері гипергеометриялық функцияларды қолдану аясын кеңейтіп, олардың ғылыми және инженерлік есептерді шешудегі рөлін арттырады.

Гипергеометриялық $F_{12}^{(4)}$ функциясын қарастырайық:

$$F_{(12)}^{(4)}(a_1, a_2, a_3, b, c_1, c_2, c_3; x, y, z, t) = \sum_{m,n,p,q=0}^{\infty} \frac{(a_1)_{m+n} (a_2)_p (a_3)_q (b)_{m+n+p+q}}{(c_1)_m (c_2)_n (c_3)_{p+q}} \frac{x^m y^n z^p t^q}{m! n! p! q!} \quad (1.1)$$

мұндағы $c \neq 0, -1, -2, -3, \dots$; мұндағы $i = 1, \dots, 3$.

2. $F_{12}^{(4)}$ функциясының дербес туындылы дифференциалдық тендеулер жүйесінің шешімі

Көп айнымалылардың гипергеометриялық функциялар теориясына және олардың қасиеттеріне сәйкес [1], [2] гипергеометриялық функция үшін (1.1) дербес дифференциалдық тендеулер жүйесін келесі түрде жазуға болады:

$$\begin{cases} (c_1 + x \frac{\partial}{\partial x})(x \frac{\partial}{\partial x} + 1)x^{-1}u - (a_1 + x \frac{\partial}{\partial x} + y \frac{\partial}{\partial y})(b + x \frac{\partial}{\partial x} + y \frac{\partial}{\partial y} + z \frac{\partial}{\partial z} + t \frac{\partial}{\partial t})u = 0 \\ (c_2 + y \frac{\partial}{\partial y})(y \frac{\partial}{\partial y} + 1)y^{-1}u - (a_1 + x \frac{\partial}{\partial x} + y \frac{\partial}{\partial y})(b + x \frac{\partial}{\partial x} + y \frac{\partial}{\partial y} + z \frac{\partial}{\partial z} + t \frac{\partial}{\partial t})u = 0 \\ (c_3 + z \frac{\partial}{\partial z} + t \frac{\partial}{\partial t})(z \frac{\partial}{\partial z} + 1)z^{-1}u - (a_2 + z \frac{\partial}{\partial z})(b + x \frac{\partial}{\partial x} + y \frac{\partial}{\partial y} + z \frac{\partial}{\partial z} + t \frac{\partial}{\partial t})u = 0 \\ (c_3 + z \frac{\partial}{\partial z} + t \frac{\partial}{\partial t})(t \frac{\partial}{\partial t} + 1)t^{-1}u - (a_3 + t \frac{\partial}{\partial t})(b + x \frac{\partial}{\partial x} + y \frac{\partial}{\partial y} + z \frac{\partial}{\partial z} + t \frac{\partial}{\partial t})u = 0 \end{cases} \quad (2.1)$$

Мұндағы $u(x, y, z, t) :=$

$$F_{17}^{(4)}(a_1, a_2, b_1, b_2; c_1, c_2, c_3; x, y, z, t)$$

Алгебралық амалдармен қарапайым есептеулерді орындай отырып, келесі екінші ретті дербес туындылы дифференциалдық теңдеулер жүйесін аламыз:

$$\begin{cases} x(1-x)u_{xx} - 2xyu_{xy} + z(1-x)u_{xz} - y^2u_{yy} - yzu_{yz} \\ \quad + [c_1 - (a_1 + b_1 + 1)x]u_x - (a_1 + b_1 + 1)yu_y - b_1zu_z - a_1b_1u = 0 \\ y(1-y)u_{yy} - x^2u_{xx} - 2xyu_{xy} - xzu_{xz} - yzu_{yz} \\ \quad - (a_1 + b_1 + 1)xu_x + [c_2 - (a_1 + b_1 + 1)y]u_y - b_1zu_z - a_1b_1u = 0 \\ z(1-z)u_{zz} + x(1-z)u_{xz} - xtu_{xt} - yzu_{yz} - ytu_{yt} \\ \quad - ztu_{zt} - b_2xu_x - b_2yu_y + [c_1 - (a_1 + b_2 + 1)z]u_z - a_1tu_t - a_1b_2u = 0 \\ t(1-t)u_{tt} - ztu_{zt} - a_2zu_z + [c_3 - (a_2 + b_2 + 1)t]u_t - a_2b_2u = 0 \end{cases} \quad (2.2)$$

Айта кету керек, жүйенің үш теңдеуі (2.2) сызықтық тәуелді болады, сондықтан $F_{17}^{(4)}$ (2.2) жүйесін қанағаттандырады. Сызықтық тәуелсіз шешімдерді келесі түрде іздейміз:

$$u = x^\alpha y^\beta z^\gamma t^\delta w, \quad (2.3)$$

мұндағы w -белгісіз функция, $\alpha, \beta, \gamma, \delta$ - анықталатын тұрақтылар. Жаңа айнымалылар $x^\alpha y^\beta z^\gamma t^\delta w$ енгізіп және (2.2) жүйедегі u орнына қойып, дифференциалдық теңдеулердің келесі

$$\begin{cases} x(1-x)w_{xx} - 2xyw_{xy} - xzw_{xz} - xtw_{xt} - y^2w_{yy} - yzw_{yz} - ytw_{yt} - (A_1 + B + 1)yw_y \\ \quad - A_1zw_z - A_1tw_t + [C_1 - (A_1 + B + 1)x]w_x + [c_1 + \alpha - 1]\alpha x^{-1} - A_1B]w = 0 \\ y(1-y)w_{yy} - x^2w_{xx} - 2xyw_{xy} - xzw_{xz} - xtw_{xt} - ytw_{yt} - yzw_{yz} - (A_1 + B + 1)xw_x \\ \quad - A_1zw_z - A_1tw_t + [C_2 - (A_1 + B + 1)y]w_y - [(c_2 + \beta - 1)\beta y^{-1} - A_1B]w = 0 \\ z(1-z)w_{zz} + tw_{zt}(1-z) - yzw_{yz} - xzw_{xz} - (A_2 - \gamma z^{-1})tw_t - A_2xw_x - A_2yw_y \\ \quad + [C_3 - (A_2 + B + 1)z]w_z + [\gamma(c_3 + \gamma + \delta - 1)z^{-1} - A_2B]w = 0 \\ t(1-t)w_{tt} + z(1-t)w_{zt} - tyw_{yt} - txw_{xt} - (A_3 - \delta t^{-1})zw_z - A_3xw_x - A_3yw_y \\ \quad - [C_3 - (A_3 + B + 1)t]w_t + [\delta(c_3 + \gamma + \delta - 1)t^{-1} - A_3B]w = 0 \end{cases} \quad (2.4)$$

$$\text{Мұндағы } A_1 = \alpha + \beta + a_1, A_2 = \gamma + a_2, A_3 = a_3 + \delta, B = \alpha + \beta + \gamma + \delta + b, \quad (2.5)$$

$$C_1 = c_1 + 2\alpha, C_2 = c_2 + 2\beta, C_3 = c_3 + 2\gamma + \delta, C_3 = c_3 + 2\delta + \gamma$$

(2.4) жүйе (2.2) жүйемен сәйкес келеді, егер келесі шарттар орындалса:

$$\begin{cases} [c_1 + \alpha - 1]\alpha = 0 \\ [c_2 + \beta - 1]\beta = 0 \\ [c_3 + \gamma + \delta - 1]\gamma = 0 \\ [c_3 + \gamma + \delta - 1]\delta = 0 \end{cases} \quad (2.6)$$

(2.6) жүйесінің шешімдерін сегіз комбинация түрінде жазуға болады:

	1	2	3	4
α	0	$1 - C_1$	0	$1 - C_1$
β	0	0	$1 - C_2$	$1 - C_2$
γ	0	0	0	0

(2.7)

δ	0	0	0	0

Осылайша, жүйенің (2.7) шешімдерін (2.3) – ке енгізіп, біз келесі гипергеометриялық функциялар түріндегі төрт айнымалы (2.2) екінші ретті дербес туындылы дифференциалдық теңдеулер жүйесінің сызықтық тәуелсіз шешімдерін аламыз:

$$u(x, y, z, t) = x^\alpha y^\beta z^\gamma t^\delta F_{12}^{(4)}(\alpha + \beta + a_1, \gamma + a_2, a_3 + \delta, \alpha + \beta + \gamma + \delta + b, c_1 + 2\alpha, c_2 + 2\beta, c_3; x, y, z, t) =$$

$$= x^\alpha y^\beta z^\gamma t^\delta \sum_{m,n,p,q=0}^{\infty} \frac{(\alpha + \beta + a_1)_{m+n} (\gamma + a_2)_p (a_3 + \delta)_q (\alpha + \beta + \gamma + \delta + b)_{m+n+p+q}}{(c_1 + 2\alpha)_m (c_2 + 2\beta)_n (c_3)_{p+q}} \frac{x^m y^n z^p t^q}{m! n! p! q!}$$

$$u_1(x, y, z, t) = F_{12}^{(4)}(a_1, a_2, a_3; b; c_1, c_2, c_3; x, y, z, t) = \sum_{m,n,p,q=0}^{\infty} \frac{(a_1)_{m+n} (a_2)_p (a_3)_q (b)_{m+n+p+q}}{(c_1)_m (c_2)_n (c_3)_{p+q}} \frac{x^m y^n z^p t^q}{m! n! p! q!}$$

$$u_2(x, y, z, t) = x^{1-c_1} F_{12}^{(4)}(a_1 + 1 - c_1, a_2, a_3; b + 1 - c_1; 2 - c_1, c_2, c_3; x, y, z, t) =$$

$$= x^{1-c_1} \sum_{m,n,p,q=0}^{\infty} \frac{(a_1 + 1 - c_1)_{m+n} (a_2)_p (a_3)_q (b + 1 - c_1)_{m+n+p+q}}{(2 - c_1)_m (c_2)_n (c_3)_{p+q}} \frac{x^m y^n z^p t^q}{m! n! p! q!}$$

$$u(x, y, z, t) = x^\alpha y^\beta z^\gamma t^\delta F_{12}^{(4)}(\alpha + \beta + a_1, \gamma + a_2, a_3 + \delta, \alpha + \beta + \gamma + \delta + b, c_1 + 2\alpha, c_2 + 2\beta, c_3; x, y, z, t) =$$

$$u_3(x, y, z, t) = y^{1-c_2} F_{12}^{(4)}(a_1 + 1 - c_2, a_2, a_3 + 1 - c_2; b + 1 - c_2; c_1, 2 - c_2, c_3; x, y, z, t) =$$

$$= y^{1-c_2} \sum_{m,n,p,q=0}^{\infty} \frac{(a_1 + 1 - c_2)_{m+n} (a_2)_p (a_3 + 1 - c_2)_q (b + 1 - c_2)_{m+n+p+q}}{(c_1)_m (2 - c_2)_n (c_3)_{p+q}} \frac{x^m y^n z^p t^q}{m! n! p! q!}$$

$$u_4(x, y, z, t) = x^{1-c_1} y^{1-c_2} F_{12}^{(4)}(a_1 + 2 - c_1 - c_2, a_2, a_3 + 1 - c_2; b + 2 - c_1 - c_2; 2 - c_1, 2 - c_2, c_3; x, y, z, t) =$$

$$= x^{1-c_1} y^{1-c_2} \sum_{m,n,p,q=0}^{\infty} \frac{(a_1 + 2 - c_1 - c_2)_{m+n} (a_2)_p (a_3 + 1 - c_2)_q (b + 2 - c_1 - c_2)_{m+n+p+q}}{(2 - c_1)_m (2 - c_2)_n (c_3)_{p+q}} \frac{x^m y^n z^p t^q}{m! n! p! q!}$$

Пайдаланылған әдебиеттер тізімі

- [1] Appell P., Kamp'e de F'eriet J. Fonctions Hyperg'eom'etriques Hypersph'ériques, Gauthier-Villars, Paris, 1926, 440 p.
- [2] Erd'elyi A., Magnus W., Oberhettinger F., Tricomi F.G. Higher Transcendental Functions, V. I, Mc Graw Hill, New York, Toronto and London, 1953.

УДК 004:61

Сабиғолла Ғ.Қ. (Қарағанда, ҚарТУ им. А. Сагинова)

Головачева В.Н. (Қарағанда, ҚарТУ им. А. Сагинова)

ИНТЕГРАЦИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЭЛЕКТРОННЫЕ МЕДИЦИНСКИЕ СИСТЕМЫ

В эпоху стремительного технологического прогресса и цифровой трансформации здравоохранения интеграция искусственного интеллекта (ИИ) в электронные медицинские системы (ЭМС) становится одним из приоритетных направлений развития современной медицины. На фоне возрастающих объемов медицинских данных и необходимости повышения оперативности и точности диагностики, применение ИИ открывает новые горизонты для повышения качества медицинских услуг. Обзор современной научной литературы (см., например, работы Smith et al., 2022; Иванов и Петров, 2021) демонстрирует, что алгоритмы машинного и глубокого обучения успешно применяются для анализа медицинских изображений, прогнозирования клинических исходов и поддержки принятия решений. Однако наряду с перспективами растут и вызовы: обеспечение безопасности данных, интерпретация сложных моделей ИИ и этические аспекты их применения. В данном исследовании объектом выступают электронные медицинские системы, а предметом – процессы интеграции ИИ в их функциональные модули с целью оптимизации диагностических и лечебных процессов. Цель статьи заключается в системном анализе перспектив и вызовов внедрения ИИ в ЭМС, определении влияния этой интеграции на качество медицинских услуг и формировании рекомендаций для дальнейшего развития данной области.

Для реализации поставленных целей исследования использовался междисциплинарный подход, объединяющий как количественные, так и качественные методы анализа. Сбор эмпирических данных осуществлялся посредством:

Структурированные опросы и полуструктурированные интервью проводились среди медицинских специалистов, IT-экспертов и конечных пользователей ЭМС в 15 крупных медицинских учреждениях (как государственных, так и частных), что позволило охватить свыше 2000 участников.

Данные, полученные из электронных медицинских записей и логов работы ИИ-модулей, обрабатывались с использованием статистических программ (SPSS) и языков программирования Python (библиотеки pandas, numpy, scikit-learn).

Была организована контрольная группа, в которой сравнивались ключевые показатели (точность диагностики, скорость обработки запросов, удовлетворенность пользователей) до и после интеграции ИИ-модулей.

Особое внимание уделялось методам машинного обучения для оценки эффективности алгоритмов ИИ, их валидации на основе перекрестной проверки, а также анализу отзывов и субъективных оценок медицинского персонала.

Анализ экспериментальных данных выявил ряд положительных тенденций после интеграции ИИ в ЭМС. Так, график 1 демонстрирует рост точности диагностики на 15–20% при использовании алгоритмов глубокого обучения для обработки медицинских изображений. Таблица 1 отражает сокращение времени обработки запросов и выдачи результатов, что приводит к уменьшению времени ожидания пациентов в среднем на 30%. Результаты анкетирования, представленные на графике 2, указывают на значительное повышение уровня удовлетворенности как медицинского персонала, так и пациентов новыми возможностями ЭМС с ИИ-модулями. Однако дискуссия результатов выявила и существующие вызовы. Сложность объяснения

принципов работы алгоритмов для непрофессионалов, что затрудняет их широкое применение. Рост объема обрабатываемых данных требует усиленной защиты конфиденциальной информации. Отсутствие нормативных стандартов для применения ИИ в медицине, что остается актуальной проблемой в исследованиях.

Внедрение ИИ в электронные медицинские системы существенно улучшает точность диагностики, ускоряет обработку медицинской информации и повышает общую удовлетворенность пользователей. Результаты настоящего исследования коррелируют с данными ранее опубликованных работ, подтверждая научную новизну и практическую значимость интеграции ИИ в медицину. Дальнейшее развитие технологий ИИ, усиление мер по обеспечению безопасности данных и разработка этических стандартов способствуют устойчивой эволюции электронных медицинских систем. Несмотря на очевидные преимущества, необходимо уделить особое внимание вопросам интерпретируемости алгоритмов и нормативно-правовой регламентации их применения в медицинской сфере.

Список использованных источников

1. Гусев А. В., Добридюк С.Л. «Искусственный интеллект в медицине и здравоохранении», Информационное общество № 4-5, 2017.
2. Мажей Я.В., Свищёв А.В. «Применение ИИ в здравоохранении», Журнал E-Scio, 2021.

УДКД 622.276.72 + 519.876.5

Сахабаева А.М., 2-курс докторанты
Байшемиров Ж.Д., PhD,
қауымдастырылған профессор
«Абай атындағы Қазақ ұлттық
педагогикалық университеті»

БАКЛЕЙ – ЛЕВЕРЕТТ МОДЕЛІН ҚОЛДАНА ОТЫРЫП, МҰНАЙ КЕН ОРЫНДАРЫНДА СУДЫ ТИІМДІ БАСҚАРУДЫ МОДЕЛЬДЕУ

Мұнай кен орындарын игеруде судың рөлі маңызды. Су пайдаланудың тиімділігі кен орнынан мұнайды шығарудың көлеміне және оның сапасына тікелей әсер етеді. Мұнай өндірісінде суды басқару мәселесі әсіресе құмды, көмірлі, және мұнаймен араласқан флюидтерді өндеуде үлкен мәнге ие. Бұл үдерісті тиімді басқару үшін, мұнай мен судың фазалық бөлінуін, олардың арасындағы өзара әрекеттесулерді, және сұйықтардың қозғалуын дұрыс модельдеу қажет. Бұл модель көмегімен су мен мұнайдың арасындағы өзара әрекеттесуді және әр түрлі параметрлердің (мысалы, бұрыштық кедергі, сұйықтың ағыны) әсерін зерттеуге болады.

Тезистің негізгі мақсаты және ғылыми қызығушылық — Баклей- Леверетт моделін тек теориялық тұрғыда ғана емес, нақты мұнай кен орындарының жағдайларына (мысалы, құмды немесе көмірлі кен орындарына) бейімдеу жұмыстары жасалды. Бұл жаңалық модельдің икемділігін арттырып, оны әртүрлі геологиялық жағдайларда қолдануға мүмкіндік береді. Баклей-Леверетт моделін қолдана отырып, мұнай кен орындарында суды басқарудың тиімді әдістерін зерттеу және ұсыныстар жасау. Бұл үшін модельдің негізгі қағидаларын және оның мұнай мен су арасындағы фазалық ауысу мен ағынды анықтаудағы мүмкіндіктерін талдау қажет. Нақты атап өтсек, мұнай және су фазаларының өзара әсерін талдау, Баклей-Леверетт моделін пайдалану арқылы су сұйықтарының кен орындарындағы қозғалысын модельдеу, модель көмегімен судың тиімді қолданылуын қамтамасыз ету үшін оңтайлы басқару стратегияларын әзірлеу. Баклей-Леверетт

моделі — екі немесе одан да көп сұйықтың кеуекті ортадағы қозғалысын сипаттайтын теориялық үлгі болып табылады.

Негізгі жаңалықтар қатарында: Суды басқарудың оңтайлы параметрлері, яғни мұнай кен орындарында суды тиімді басқару үшін Баклей-Леверетт моделін қолдана отырып, әр түрлі параметрлердің (капиллярлық қысым, судың және мұнайдың салыстырмалы өткізгіштігі) әсерін зерттеу. Бұл жаңалық судың ағынын тиімді басқаруға бағытталған жаңа стратегиялық ұсыныстарды енгізуге мүмкіндік береді.

Судың тиімді үлестіру жүйесін құру. Модель арқылы су мен мұнай арасындағы фазалық ауысуы басқару үшін судың тиімді үлестіру әдістерін жасап шығару. Мұнай өндірісінде судың артық шығынын болдырмау және кен орнындағы мұнай өнімділігін арттыру үшін осы жүйені қолдануға болады.

Модельдің негізгі параметрлері:

- Капиллярлық қысым — сұйықтың кеуекті орта арқылы қозғалуына әсер ететін күш.
- Сұйықтардың ағын жылдамдығы — мұнай мен су арасындағы өзара әрекеттесуді есептейді.
- Сұйықтың қозғалыс қасиеттері — су мен мұнайдың пористық ортада қозғалу жылдамдығын анықтайды.
- Суды басқарудың модельдеу әдістері

Мұнай өндіру кезінде сұйықтардың қозғалысын оңтайландыру үшін Баклей-Леверетт моделін қолдану. Мысалы, кейбір құмды кен орындарында суды тиімді пайдалану үшін оптималды су мен мұнай арақатынасын анықтауға болады. Көмірлі кен орны: Мұнай мен газдың бірге шығарылатын жағдайында су мен мұнай фазаларының өзара әрекеттесуін зерттеу. Бұл процесс капиллярлық күштердің әсерін модельдеу арқылы тиімді түрде басқарылуы мүмкін.

Суды басқарудың бірнеше тиімді әдістері бар, мысалы, су сұйықтарын қозғалтудың тиімді жолдарын анықтау, су мен мұнай арасындағы фазалық ауысуларды минимизациялау, қосымша сұйықтарды қосу арқылы ағынды оңтайландыру.

Қорытынды

Баклей-Леверетт моделі мұнай кен орындарында суды басқаруды тиімді модельдеуге мүмкіндік береді. Бұл модель судың ағыны мен фазалық өзгерістердің тиімділігін бағалауға, мұнай мен су арасындағы өзара әрекеттесуді оңтайландыруға бағытталған. Модельдің дұрыс қолданылуы кен орнының өнімділігін арттырып, мұнай өндірісінің құнын төмендетуге мүмкіндік береді. Бұл зерттеу нәтижелері мұнай өндіруші компанияларға суды тиімді басқару стратегияларын әзірлеуге көмектеседі.

Пайдаланылған әдебиеттер тізімі:

1. Жамалиев, Н. К., Омаров, С. Ш. (2021). Құмды кен орындарындағы мұнай өндіру: теоретикалық және практикалық аспектілер — Алматы: Қазақ университеті.
2. Төлеубеков, Р. Ш. (2023). Қазақстан мұнай кен орындарында судың рөлі мен тиімді пайдалану тәсілдері — Астана: ЕҰУ баспасы.
3. Lake, L. W., Civan, F. (2020). Enhanced Oil Recovery, Volume 1: Field Planning and Development — Gulf Professional Publishing.
4. Zhao, Y., Liu, H., & Wang, Y. (2021). "Application of the Bakley-Leverett model for predicting oil recovery in water-flooded reservoirs". *Journal of Petroleum Science and Engineering*, 200, 108210.
5. He, X., & Zong, X. (2022). "Impact of capillary pressure and relative permeability on waterflooding in oil reservoirs". *Journal of Petroleum Technology*, 74(6), 92-98.

6. McDougal, A. E., & Zhang, L. (2024). *Petroleum Reservoir Simulation: A Practical Guide* — Wiley- Blackwell.

УДК 004.056

Сабитов А. Б. Исмагелов Ә.Е (Esil Universiteti университеті)

АНАЛИЗА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ ДЛЯ ОПЕРАТИВНОГО РЕАГИРОВАНИЯ НА УГРОЗЫ

Аннотация

В статье представлен обзор современных подходов и технологий, применяемых для построения систем мониторинга и анализа безопасности информационных ресурсов. Рассмотрены SIEM-, SOAR-, XDR-платформы, а также интеллектуальные методы анализа, включая поведенческую аналитику и машинное обучение. На основе изученных источников определены основные тенденции и перспективы развития в данной области. Работа может быть полезна специалистам в области информационной безопасности при выборе и внедрении систем защиты корпоративной инфраструктуры.

Ключевые слова: информационная безопасность, SIEM, SOAR, XDR, поведенческий анализ, машинное обучение, киберугрозы.

Введение Современные организации подвергаются множеству угроз информационной безопасности, включая внутренние и внешние атаки, целевые вредоносные воздействия и утечки данных. В связи с этим особую актуальность приобретает разработка и внедрение систем мониторинга и анализа безопасности, позволяющих оперативно обнаруживать, классифицировать и реагировать на инциденты. В последние годы наблюдается значительное развитие технологий в этой области, включая интеграцию искусственного интеллекта, автоматизацию процессов реагирования и поведенческую аналитику.

Современные технологии мониторинга безопасности Ксенофонов В. А. [1] подробно рассматривает архитектуру и функциональные возможности современных SIEM-систем, подчеркивая их роль как центрального элемента в системах информационной безопасности организаций. Он акцентирует внимание на интеграции с источниками событий, корреляции данных и автоматизированной генерации оповещений, что позволяет оперативно выявлять аномалии и потенциальные атаки.

Автоматизация реагирования на угрозы Сафиуллиной Л. Х., Касимова А. Р., Алексеева А. А. [2] исследуют эффективность использования платформ XDR и SOAR, демонстрируя, что их совместное применение позволяет достичь высокого уровня автоматизации при реагировании на инциденты. В статье проводится сравнение архитектурных особенностей и сценариев внедрения данных решений, выделяя их преимущества в условиях растущего объема угроз.

Проектирование центров мониторинга (SOC) Гайдабрус Б., Алимжанова Л. М., Еркежан Я. [3] делают акцент на методологии построения центров мониторинга безопасности (Security Operations Center — SOC), включая аспекты организационного и технического планирования. Авторы приводят этапы внедрения SOC, начиная с аудита ИБ и заканчивая интеграцией аналитических платформ и разработкой процедур реагирования.

Поведенческий анализ и UEBA Кравцов В. А. и Килинкарлова С. Г. [4] рассматривают внедрение поведенческой аналитики (UEBA) как перспективное направление повышения эффективности обнаружения сложных и скрытых угроз, включая инсайдерские действия. Использование алгоритмов машинного обучения позволяет выявлять аномалии, отклоняющиеся от нормального поведения пользователей и устройств.

Интеллектуальные системы мониторинга Атымтаева Л., Баймуратов О., Хашимова Д. А. [5] анализируют применение машинного обучения и интеллектуальных алгоритмов в системах мониторинга киберугроз. Подчеркивается значимость предиктивной аналитики и моделей на основе больших данных для прогнозирования и предотвращения атак.

Закключение

На основании проведенного анализа можно заключить, что современные системы мониторинга и анализа информационной безопасности переходят от статичных решений к гибким, адаптивным и интеллектуальным платформам. В условиях растущей сложности угроз особую роль играют технологии автоматизации (SOAR), расширенного обнаружения (XDR) и поведенческого анализа (UEBA). Интеграция таких решений в корпоративную инфраструктуру позволяет не только оперативно реагировать на инциденты, но и предотвращать их на ранних этапах. Будущие исследования в данной области будут сосредоточены на расширении возможностей ИИ, повышении масштабируемости систем и углублении аналитических функций.

Список литературы:

1. Ксенофонов В. А. Информационная безопасность: современные технологии защиты // Информационные технологии и вычислительные системы. — 2020. — № 2. — С. 35–42.
2. Сафиуллина Л. Х., Касимова А. Р., Алексеева А. А. Анализ эффективности использования XDR и SOAR в системах защиты информации // Информационные и телекоммуникационные технологии. — 2022. — № 4 (68). — С. 15–21.
3. Гайдабрус Б., Алимжанова Л. М., Еркежан Я. Методология построения центра мониторинга информационной безопасности в корпоративной инфраструктуре // Вестник Казахского национального технического университета. — 2021. — № 6. — С. 60–67.
4. Кравцов В. А., Килинкарлова С. Г. Применение поведенческого анализа в системах информационной безопасности // Безопасность информационных технологий. — 2019. — Т. 25, № 3. — С. 55–61.
5. Атымтаева Л., Баймуратов О., Хашимова Д. А. Обзор интеллектуальных систем мониторинга киберугроз на основе машинного обучения // Информационная безопасность и наука. — 2023. — № 3. — С. 25–31.

УДК 519.6

Султанов М.А. (Туркестан, МКТУ им. Х. А. Ясави)
Мисилов В.Е. (Екатеринбург, ИММ УрО РАН им.Н.Н.Красовского, УрФУ)
Садыбеков М. А. (Алматы, Институт математики и математического моделирования)
Баканов Г.Б. (Туркестан, МКТУ им. Х. А. Ясави)
Сарсенов Б.Т. (Туркестан, МКТУ им. Х. А. Ясави)

АЛГОРИТМ ЧИСЛЕННОГО РЕШЕНИЯ ОБРАТНОЙ ЗАДАЧИ НАХОЖДЕНИЯ ПРАВОЙ ЧАСТИ ДЛЯ УРАВНЕНИЯ СУБДИФФУЗИИ С КРАЕВЫМИ УСЛОВИЯМИ ТИПА ШТУРМА

Рассматривается уравнение субдиффузии с краевыми условиями типа Штурма:

$$\begin{cases} D_t^\alpha U(x, t) - U_{xx}(x, t) = \psi(x)\eta(x, t) + f(x, t), \\ U(x, 0) = 0, \quad 0 \leq x \leq 1, \\ U_x(0, t) - aU(0, t) = 0, \quad 0 \leq t \leq T, \\ U_x(1, t) + aU(1, t) = 0, \quad 0 \leq t \leq T, \end{cases}$$

где $0 < \alpha < 1$ — порядок дробной производной Капуто D_t^α .

Рассматривается обратная задача нахождения пары неизвестных функций $U(x, t)$ и $\psi(x)$ при наличии дополнительной информации в виде финального переопределения

$$U(x, T) = \varphi(x), 0 \leq x \leq 1,$$

где $\varphi(x)$ — известная функция.

Для численного решения обратной задачи предложен итерационный алгоритм на основе регуляризованного метода Левенберга-Марквардта [1]. Для решения вспомогательных прямых начально-краевых задач на каждой итерации алгоритма используется разностная схема [2] на основе L1-аппроксимации дробной производной Капуто и центрально-разностной схемы.

Список использованных источников

1. Васин В.В., Еремин И.И., *Операторы и итерационные процессы фейеровского типа. Теория и приложения.*, Екатеринбург: УрО РАН, 2005, 210 с.
2. Sultanov M.A., Misilov V.E., Sadybekov M.A., Numerical method for solving the subdiffusion differential equation with nonlocal boundary conditions. AIMS Mathematics, 2024, 9(12): 36385-36404. doi: 10.3934/math.20241726

УДК 517.9

Турсунов Д.А., Мамытов А.О., Кудуев А.Ж. (г. Ош, Ошский Государственный Университет)

ОБРАТНАЯ ЗАДАЧА ДЛЯ ОДНОГО КЛАССА ДИФФЕРЕНЦИАЛЬНЫХ И ИНТЕГРО-ДИФФЕРЕНЦИАЛЬНЫХ УРАВНЕНИЙ В ЧАСТНЫХ ПРОИЗВОДНЫХ

Обратные задачи играют ключевую роль в различных областях науки и техники, и искусственный интеллект (ИИ) активно используется для их решения [1]. Обратная задача связана с определением причин (входных данных или параметров модели) по известным последствиям (выходным данным) [2]. Это противоположность прямой задачи, где выходные данные рассчитываются на основе заданных входных данных и модели, например, машинное обучение, томография и др. ИИ становится мощным инструментом для решения обратных задач благодаря своей способности к обучению на сложных и многомерных данных. Он применяется для повышения точности решений; ускорения вычислений; улучшения устойчивости к шумам в данных.

В работе [3] приведен анализ взаимосвязей теории обратных и некорректных задач и математических аспектов искусственного интеллекта. Показано, что при анализе вычислительных алгоритмов, которые условно можно отнести к вычислительному искусственному интеллекту (машинное обучение, природоподобные алгоритмы, методы анализа и обработки данных), возможно, а подчас и необходимо, использовать результаты и подходы, развитые в теории и численных методах решения обратных и некорректных задач, такие как регуляризация, условная устойчивость и сходимости, использование априорной информации, идентифицируемость, чувствительность, усвоение данных.

Мы рассматриваем обратную задачу восстановления коэффициентов правой части уравнения. Определение правой части начально-краевой задачи для дифференциального уравнения высокого

порядка с использованием искусственного интеллекта представляет собой одну из сложных и интересных задач в математике и вычислительной технике. Такая задача относится к классу обратных задач, где требуется восстановить коэффициенты правой части уравнения на основе известных начальных, краевых и дополнительных (след) условий [2].

Исследуется следующая обратная задача:

$$\frac{\partial^m}{\partial t^m} u(t, x) = \frac{\partial^{m+2}}{\partial t^m \partial x^2} u(t, x) + \sum_{j=1}^n \varphi_j(t) f_j(t, x) + F(t, x), \quad (t, x) \in \Omega \quad (1)$$

$$\frac{\partial^p}{\partial t^p} u(t, x) \Big|_{t=0} = \psi_p(x), \quad 0 \leq x \leq 1, \quad p = 0, 1, 2, \dots, m-1; \quad (2)$$

$$u(t, 0) = u(t, 1) = 0, \quad 0 \leq t \leq T, \quad (3)$$

$$u(t, x_1) = g_1(t), \quad u(t, x_2) = g_2(t), \dots, \quad u(t, x_n) = g_n(t), \quad t \in [0, T], \\ x_i \in (0, 1), \quad i = 1, 2, \dots, n; \quad x_i \neq x_j, \quad i \neq j, \quad (4)$$

где $\Omega = \{(t, x) \mid 0 < x < 1, \quad 0 < t \leq T\}$, $0 < T \in \mathbf{R}$, x_i ($i=1, 2, \dots, n$) – заданные постоянные числа, $\psi_p(x)$, $f_i(t, x)$, $F(t, x)$, $g_i(t)$ ($i=1, 2, \dots, n$) – известные функций, $f_i \in C(\Omega)$, $\psi_p \in C[0, 1]$, $g_i \in C^m[0, T]$, $i=1, 2, \dots, n$, $p=0, 1, \dots, m-1$; $\psi_p(0) = \psi_p(1) = 0$, $g^{(p)}_i(0) = \psi_p(x_i)$, $i=1, 2, \dots, n$, $p=0, 1, \dots, m-1$. А функций $\varphi_1(t)$, $\varphi_2(t)$, ..., $\varphi_n(t)$ и $u(t, x)$ – искомые.

Для простоты изложения идеи мы здесь привели самый простой и решение явно представимый класс дифференциальных уравнений в частных производных высокого порядка.

Постановка задачи: Найти функций $u \in C^{m,2}(\Omega)$, $\varphi_i \in C[0, T]$, $i=1, 2, \dots, n$ удовлетворяющие уравнению (1) в области Ω и условиям (2)-(4) (Рис. 1).

Решение задачи. Введем обозначение.

$$v(t, x) = \frac{\partial^m}{\partial t^m} u(t, x), \quad (5)$$

тогда уравнение (1) примет вид:

$$v_{xx}(t, x) - v(t, x) = - \sum_{j=1}^n \varphi_j(t) f_j(t, x) - F(t, x), \quad (t, x) \in \Omega, \quad (6)$$

Из соотношении (3) и (5) имеем:

$$v(t, 0) = v(t, 1) = 0, \quad 0 \leq t \leq T. \quad (7)$$

Используя функцию Грина, решение задачи (6)-(7) относительно переменной x , можно

$$v(t, x) = - \sum_{j=1}^n \varphi_j(t) \int_0^1 G(x, \xi) f_j(t, \xi) d\xi - \int_0^1 G(x, \xi) F(t, \xi) d\xi \quad (8)$$

записать в явном виде:

$$G(x, \xi) = \begin{cases} \frac{sh(x-1)sh(\xi)}{sh(1)}, & 0 \leq \xi \leq x \leq 1, \\ \frac{sh(x)sh(\xi-1)}{sh(1)}, & 0 \leq x \leq \xi \leq 1. \end{cases}$$

где

в соотношении (8) имеется $(n+1)$ неизвестных. Но у нас имеется дополнительная информация (4). Применяя эти условия для (8) получаем:

$$v(t, x_i) = - \sum_{j=1}^n \varphi_j(t) \int_0^1 G(x_i, \xi) f_j(t, \xi) d\xi - \int_0^1 G(x_i, \xi) F(t, \xi) d\xi, \quad i = 1, 2, \dots, n, \quad (9)$$

или

$$g_i^{(m)}(t) = - \sum_{j=1}^n \varphi_j(t) \int_0^1 G(x_i, \xi) f_j(t, \xi) d\xi - \int_0^1 G(x_i, \xi) F(t, \xi) d\xi, \quad i = 1, 2, \dots, n, \quad (10)$$

Введем обозначения, пусть

$$m_{ij}(t, x_i) = - \int_0^1 G(x_i, \xi) f_j(t, \xi) d\xi, \quad b_i(t) = g_i^{(m)}(t) + \int_0^1 G(x_i, \xi) F(t, \xi) d\xi$$

Тогда (10) примет вид:

$$b_i(t) = \sum_{j=1}^n \varphi_j(t) m_{ij}(t, x_i), \quad i = 1, 2, \dots, n. \quad (11)$$

В результате мы получили n конечных уравнений с n неизвестными функциями. Введем обозначение

$$M(t) = \{m_{ij}(t, x_i)\}, \quad \Phi(t) = \{\varphi_i(t)\}, \quad B(t) = \{b_i(t)\}, \quad i, j = 1, 2, \dots, n.$$

Пусть

$$\det M(t) \neq 0, \quad \forall t \in [0, T]. \quad (12)$$

Тогда решение (11) в векторной форме можно представить в виде:

$$\Phi(t) = M^{-1}(t)B(t).$$

Подставляя найденные функций $\varphi_1(t), \varphi_2(t), \dots, \varphi_n(t)$ в (8) находим функцию $v(t, x)$.

Интегрируя равенство (5) m раз, учитывая начальные условия (2), и применяя формулу Дирихле, получаем:

$$u(t, x) = \frac{1}{(m-1)!} \int_0^t (t-s)^{m-1} v(s, x) ds + \sum_{j=0}^{m-1} \frac{t^j}{j!} \psi_j(x). \quad (13)$$

В результате мы доказали следующую теорему

Теорема. Пусть выполняется условие (12) тогда обратная задача разрешима в рассматриваемой области и решение представимо в виде (13).

Заключение. Искусственный интеллект значительно расширяет возможности решения обратных задач, делая их решения более точными, быстрыми и надежными. Однако для максимальной эффективности необходимо учитывать специфику задачи и сочетать ИИ с традиционными подходами [3].

Литература

1. Семенов, А.Л. Искусственный интеллект в обществе // Докл. РАН. Матем., информ., проц. упр., **514**:2 (2023), 6–19; Dokl. Math., **108**:suppl. 2 (2023), S168–S178.

2. Сабитов, К. Б. Обратные задачи для уравнения теплопроводности по отысканию источника с нелокальным наблюдением // Сиб. журн. индустр. матем., **27**:3 (2024), 143–156; J. Appl. Industr. Math., **18**:3 (2024), 536–547.

3. Кабанихин, С. И. Обратные задачи и искусственный интеллект // Успехи кибернетики, **2**:3 (2021), 33–43.

УДК 004.93

Тусупов А.К. (Алматы, КазНУ им. аль-Фараби)
Тулеев А.А., (Алматы, КазНУ им. аль-Фараби)

СБОР ДАННЫХ С ДАТЧИКОВ ДЛЯ ЦИФРОВОГО ДВОЙНИКА ПРЕДПРИЯТИЯ

В статье рассматривается разработка системы сбора данных с датчиков для цифрового двойника предприятия с целью повышения автоматизации и мониторинга производственного процесса. Для реализации используется программируемый логический контроллер (ПЛК) Siemens S7-1200, настраиваемый в программе TIA Portal, а также WinCC Explorer для визуализации. Виртуальный ПЛК моделируется в PLCSIM, а полученные данные передаются в WinCC Explorer – программа для визуализации, где отображаются положение кузова, активированные датчики и состояние конвейерной линии. Это соединение позволяет не только отображать данные о работе конвейерной линии, но также анализировать собранную информацию и управлять процессом дистанционно через другой компьютер (Рисунок 1).

Статья посвящена созданию цифрового двойника конвейерной линии на предприятии автомобилестроения. Конвейерная линия предназначена для перемещения кузовов с остановками в нужные моменты. Цифровой двойник позволяет наблюдать за её работой, анализировать поведение системы и оптимизировать процесс [1].

В разработанной системе конвейерная линия управляется с помощью тега “conveyor line”, который находится в состоянии True, но останавливается при срабатывании датчиков приближения, нажатии кнопки “stop”, аварийной остановке “Emergency stop button” или активации датчика дыма “smoke detector”. Для возобновления работы используется тег “Resume button”. Количество кузовов, прошедших через конвейер, фиксируется в теге “Chet”, получающем сигналы от последнего датчика приближения (Рисунок 2).

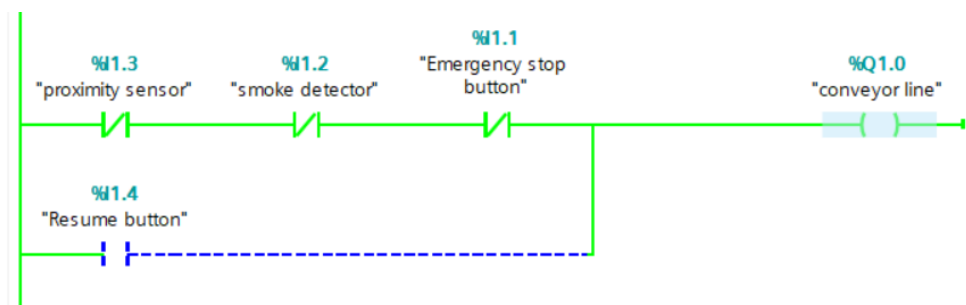
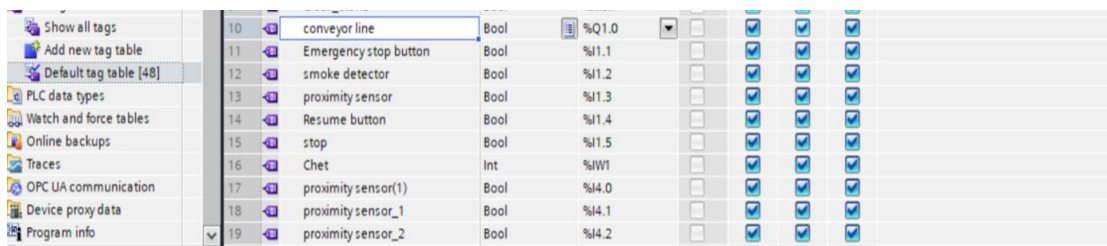


Рисунок 1. Логика программы в TiaPortal



Tag Name	Symbol	Symbol Name	Symbol Type	Symbol Address	Symbol Value	Symbol State	Symbol Color	Symbol Shape	Symbol Size	Symbol Font	Symbol Background	Symbol Border	Symbol Text	Symbol Position	Symbol Rotation	Symbol Scale	Symbol Units	Symbol Description
conveyor line	Bool	%Q1.0	Bool															
Emergency stop button	Bool	%I1.1	Bool															
smoke detector	Bool	%I1.2	Bool															
proximity sensor	Bool	%I1.3	Bool															
Resume button	Bool	%I1.4	Bool															
stop	Bool	%I1.5	Bool															
Chet	Int	%IW1	Int															
proximity sensor(1)	Bool	%I4.0	Bool															
proximity sensor_1	Bool	%I4.1	Bool															
proximity sensor_2	Bool	%I4.2	Bool															

Рисунок 2. Используемые теги

В системе управления конвейерной линией используются входные и выходные теги, обеспечивающие работу автоматизированного процесса. Входные теги "Emergency stop button", "smoke detector", "proximity sensor", "proximity sensor(1)", "proximity sensor_1", "proximity sensor_2", "stop", "Resume button" отвечают за получение данных с датчиков и кнопок управления. Аварийная кнопка "Emergency stop button", кнопка остановки "stop" и датчик дыма "smoke detector" при активации приводят к остановке конвейера, а кнопка возобновления "Resume button" запускает его снова. Датчики приближения "proximity sensor", "proximity sensor(1)", "proximity sensor_1" и "proximity sensor_2" определяют положение кузова и управляют процессом его остановки в нужных точках.

Выходные теги "conveyor line" и "Chet" используются для управления системой и отображения её состояния. Тег "conveyor line" определяет, работает конвейер или остановлен, а тег "Chet" ведет учет количества кузовов, прошедших через последний датчик приближения. Эти теги позволяют системе корректно реагировать на изменения в процессе и передавать данные для визуализации в WinCC Explorer, где отображается текущее состояние конвейера, активированные датчики и счетчик кузовов.

Программа загружается в PLCSIM, который представляет собой программный инструмент для симуляции работы контроллеров Siemens серии S7-1200 и S7-1500. PLCSIM позволяет протестировать разработанную логику без физического оборудования, моделируя работу ПЛК в виртуальной среде. После загрузки программы в PLCSIM, данные тегов передаются в WinCC Explorer, где строится визуализация системы (Рисунок 3). На экране отображается текущее состояние конвейерной линии, включая активность всех датчиков и положение кузова. Датчики приближения при срабатывании подсвечиваются красным цветом, что позволяет наглядно отслеживать процесс. Также выводится количество кузовов, прошедших через конвейерную линию, состояние мотора и самого конвейера. Для анализа работы линии в реальном времени используются графики и тренды, фиксирующие время работы конвейерной линии. Это позволяет оператору контролировать процесс и оперативно реагировать на изменения в системе [2, 3].

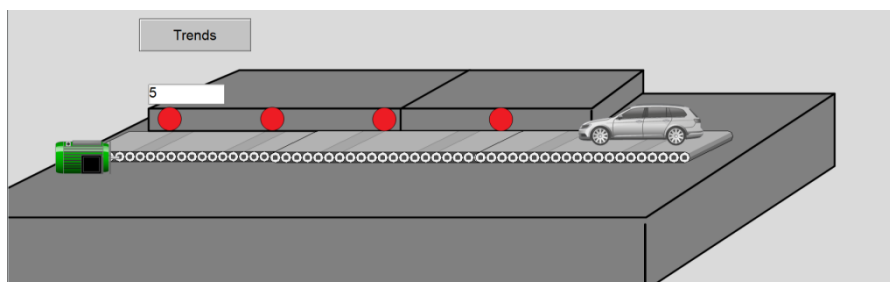


Рисунок 3. Визуализация на WinCC

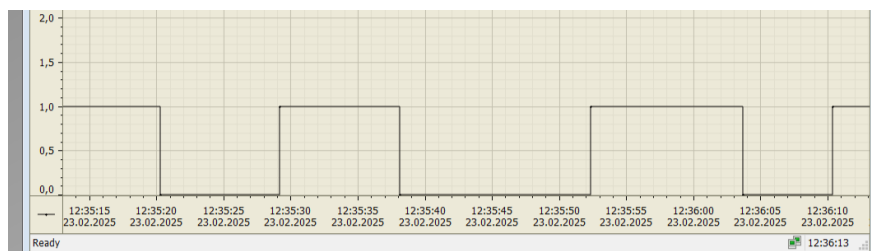


Рисунок 4. Тренд, на котором мы видим работу конвейерной линии по времени

На этом тренде (Рисунок 4) при значении 1 конвейерная линия находится в работе, а при значении 0 — остановлена. Этот тренд строится на основе значений тега "conveyor line", который отображает текущее состояние конвейерной линии. Таким образом, визуализация позволяет в реальном времени отслеживать периоды работы и остановки конвейера.

Дополнительно используется конфигурация WinCC в режиме "сервер-клиент", что позволяет наблюдать за работой системы и вносить коррективы через другой ПК. Это обеспечивает удобный удаленный контроль и оперативное реагирование на изменения в процессе.

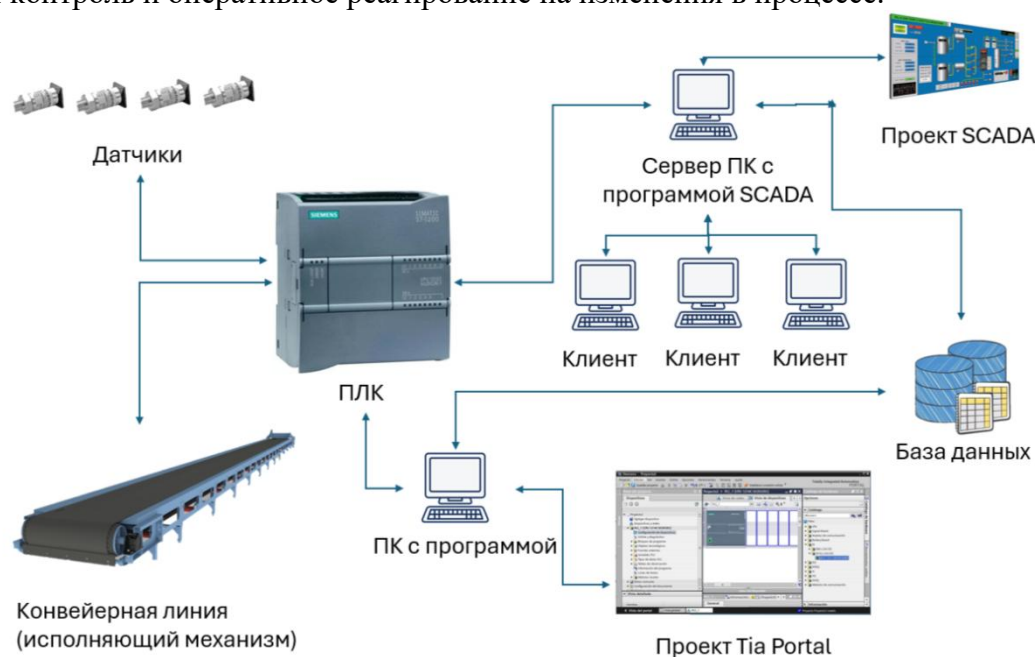


Рисунок 5. Общая схема цифрового двойника предприятия

Предложенная система повышает уровень автоматизации, обеспечивает мониторинг и контроль производственного процесса, что способствует его оптимизации и выявлению возможных неисправностей. Скриншоты визуализации приведены в файле (Рисунок 5).

Литература

1. Официальный сайт форум Siemens: <https://support.industry.siemens.com/forum>
2. Освоение программирования ПЛК Siemens: подробное руководство по порталу TIA: <https://plcvfd.com/ru/mastering-siemens-plc-programming-a-comprehensive-guide-to-tia-portal>
3. Library of general functions (LGF) for SIMATIC STEP 7 (TIA Portal) and SIMATIC S7-1200 / S7-1500: <https://support.industry.siemens.com/cs/document/109479728/>

УДК 004.896

Уалиев А.М., Жартыбаева М.Г. (Астана, Л.Н.Гумилев атындағы ЕҰУ)

ТҰРМЫСТЫҚ ҚАТТЫ ҚАЛДЫҚТАРДЫ ЖІКТЕУ ҮШІН КОМПЬЮТЕРЛІК КӨРУ ЖӘНЕ ТЕРЕҢ ОҚЫТУ АЛГОРИТМДЕРІ МЕН ӘДІСТЕРІН ЗЕРТТЕУ ЖӘНЕ ТАЛДАУ

Аннотация. Бұл зерттеу тұрмыстық қатты қалдықтарды (ТҚК) автоматты түрде жіктеу үшін компьютерлік көру және терең оқыту әдістерін қолдану мәселелеріне арналған. Қалдықтарды тиімді сұрыптау қоршаған ортаны қорғау мен қайта өңдеу жүйелерінің тиімділігін арттыруда маңызды рөл атқарады. Дәстүрлі әдістердің шектеулерін ескере отырып, машиналық оқыту мен нейрондық желілер негізінде автоматтандырылған жүйелерді әзірлеу өзекті мәселе болып табылады. Бұл мақалада әртүрлі модельдер, соның ішінде Simple CNN, VGG16, ResNet50 және HOG+SVM алгоритмдері қарастырылып, олардың тиімділігі мен дәлдігі салыстырмалы түрде талданады. Сонымен қатар, теориялық зерттеулердің нәтижелерін тәжірибе жүзінде тексеру мақсатында Arduino негізінде аппараттық прототип әзірленді. Бұл жүйе қалдықтарды автоматты түрде жіктеуді жүзеге асырып, әзірленген алгоритмдердің жұмыс істеуін тестілеуге мүмкіндік берді. Алынған нәтижелер қалдықтарды автоматты түрде сұрыптау жүйелерін жетілдіруге және экологиялық тұрақтылықты арттыруға ықпал етеді.

Кілт сөздер: компьютерлік көру, терең оқыту, машиналық оқыту, қалдықтарды жіктеу, экологиялық тұрақтылық, қайта өңдеу.

Тұрмыстық қатты қалдықтарды тиімді жіктеу мәселесі қазіргі таңда өзекті болып отыр. Қалдықтарды автоматты түрде тану және сұрыптау жүйелері экологиялық тұрақтылықты қамтамасыз етудің негізгі элементтерінің бірі болып табылады. Дәстүрлі қолмен сұрыптау әдістері қателіктерге бейім және уақытты көп талап етеді, ал компьютерлік көру мен терең оқыту технологиялары бұл процесті жылдам әрі дәл орындауға мүмкіндік береді.

Бұл зерттеуде әртүрлі терең оқыту модельдері мен алгоритмдері салыстырылды, оның ішінде:

- Simple CNN – негізгі конволюциялық нейрондық желі, қарапайым архитектурасымен ерекшеленеді.
- VGG16 – тереңдетілген нейрондық желі, кеңінен қолданылатын классификация модельдерінің бірі.
- ResNet50 – қалдықтарды тану мен жіктеу бойынша ең жоғары дәлдікті көрсеткен модельдің бірі.
- HOG+SVM – суреттегі белгілерді бөлшектеп, оларды қолмен таңдалған белгілер негізінде классификациялайтын әдіс.

Сонымен қатар, әртүрлі модельдерде Adam және Adadelta оптимизаторлары қолданылып, олардың әсері бағаланды.

Теориялық зерттеулердің нәтижелерін тәжірибе жүзінде тексеру үшін Arduino негізінде аппараттық прототип әзірленді. Бұл жүйе келесі негізгі компоненттерден тұрады:

- Камера модулі, қалдықтардың суретін түсіру үшін.
- Микроконтроллер, негізгі басқару жүйесі ретінде.
- Қозғалтқыштар қалдықтарды автоматты түрде сұрыптауға арналған.
- Пайдаланушының интерфейсі.

Прототип әзірленген нейрондық желі моделін пайдалана отырып, қалдықтарды автоматты түрде анықтап, оларды тиісті санаттарға жіктеуді жүзеге асырды. Тестілеу нәтижесінде жүйе 90%-дан жоғары дәлдік көрсетті.

Зерттеу барысында 10000 суреттен тұратын жиынтық қолданылды. Оның 90% оқыту жиынтығы, 10% тест жиынтығы болып бөлінді. Әрбір модель 40 эпох бойы оқытылды, нәтижесінде:

- Simple CNN – 82% тест дәлдігіне қол жеткізді.
- VGG16 – 75% тест дәлдігін көрсетті.
- ResNet50 – 95% дәлдікке жетіп, ең тиімді модельдің бірі ретінде анықталды.
- HOG+SVM – ең төменгі нәтижені (47%) көрсетті.

Бұл нәтижелер терең оқыту әдістерінің қалдықтарды автоматты түрде сұрыптауда тиімділігін дәлелдейді. Сонымен қатар, деректерді аугментациялау мен алдын ала өңдеу әдістерінің маңызды рөл атқаратыны анықталды. Осылайша, өндірістік процестерде ақауларды уақытылы және дәл анықтау үшін жоғары жылдамдықты және дәлдікті қамтамасыз ететін модельдерді таңдау маңызды болып табылады. Компьютерлік көру және терең оқыту әдістерін қолдану өндіріс сапасын арттырып қана қоймай, ресурстарды тиімді пайдалану мен шығындарды азайтуға мүмкіндік береді. Бұл технологияларды одан әрі жетілдіру өндірісті интеллектуалды автоматтандыруға және өндірістік жүйелердің сенімділігін арттыруға бағытталған болмақ.

Пайдаланылған әдебиеттер тізімі

1. Wang H. Garbage recognition and classification system based on convolutional neural network vgg16 //2020 3rd International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE). – IEEE, 2020. – С. 252-255.
2. Jmour N., Zayen S., Abdelkrim A. Convolutional neural networks for image classification //2018 international conference on advanced systems and electric technologies (IC_ASET). – IEEE, 2018. – С. 397-402.
3. Уалиев А.М. Компьютерлік көру технологиясы көмегімен тұрмыстық қатты қалдықтарды классификациялау және сұрыптау жүйесін әзірлеу // «GYLYM JANE BILIM - 2024» XIX Халықаралық ғылыми конференциясының ғылыми мақалалар жинағы. Астана қаласы: 2024 ж.

УДК 51-72

Шаяхметов Н.М.
(Алматы, КазНІТУ им. К.И. Сатпаева)
Құрмансейіт М.Б.
(Алматы, КазНІТУ им. К.И. Сатпаева)
Айжулов Д.Е.
(Алматы, КазНІТУ им. К.И. Сатпаева)
Тунгатарова М.С.
(Алматы, КазНІТУ им. К.И. Сатпаева)

ОПТИМИЗАЦИЯ РАСХОДОВ СКВАЖИН ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ДОБЫЧИ МИНЕРАЛОВ МЕТОДОМ ПОДЗЕМНОГО СКВАЖИННОГО ВЫЩЕЛАЧИВАНИЯ

Подземное скважинное выщелачивание является одним из наиболее эффективных методов добычи минералов и позволяет разрабатывать месторождения с глубокими и

низкоконцентрированными рудными залежами [1]. Хотя этот метод достаточно распространён, а его применение насчитывает более 50 лет, его низкая себестоимость значительно замедлила развитие научных исследований в этой области.

Метод подземного скважинного выщелачивания основан на введении выщелачивающего раствора в рудоносный пласт через сеть закачивающих скважин, растворении минерала за счёт химической реакции между введённым раствором и породой, а также откачивании продуктивного раствора с содержанием растворённого минерала [2]. Как видно из самой методики, эффективность добычи напрямую зависит от множества факторов, таких как расположение скважин, концентрация выщелачивающего раствора, расход закачивающих и добывающих скважин, а также другие технологические параметры. При этом современные технологии математического моделирования позволяют рассчитывать эти характеристики с учётом всех факторов.

Настоящее исследование посвящено разработке методики определения распределения расходов закачивающих скважин с учётом расстояния между скважинами, расходов откачивающих скважин, а также распределения проницаемости в межскважинном пространстве. Методика определения основана на математическом моделировании физико-химических процессов, методах оптимизации, а также на экономической оценке эффективности добычи.

Математическая модель состоит из двух частей, представляющих собой дифференциальные уравнения в частных производных, основанные на законах Дарси, сохранения массы и действующих масс [3]. Численное решение математической модели гидродинамических процессов позволяет определить распределение давления в пласте, за счёт чего методом Поллока можно вычислить распределение линий тока, что, в свою очередь, позволяет оценить баланс растворов в пласте [4]. Моделирование химических процессов даёт возможность оценить расход выщелачивающего раствора, что, в дальнейшем, позволяет провести экономическую оценку [5].

Разрабатываемая методика определения баланса растворов в пласте включает: внедрение начальных и граничных условий (начальное распределение минерала и проницаемости пласта, расположение и расход откачивающих скважин, геометрическая форма технологического блока); определение распределения давления и скорости в пласте (путём решения системы уравнений, состоящих из законов Дарси и сохранения массы); вычисление распределения концентраций растворов в пласте (на основе решения уравнений массопереноса с учётом химических взаимодействий); экономическую оценку эффективности и оптимизацию расходов скважин на основе однородности концентраций растворов и степени извлечения минерала.

Литература

1. Li H., Tang Z., Xiang D. Study on Numerical Simulation of Reactive-Transport of Groundwater Pollutants Caused by Acid Leaching of Uranium: A Case Study in Bayan-Uul Area, Northern China // *Water*. – 2024. – V. 16. – № 3. <https://doi.org/10.3390/w16030500>
2. Bruneton P., Cuney M. *Geology of Uranium Deposits Uranium for Nuclear Power*. – Boston: Woodhead Publishing, 2016. – V. 2. – P. 11–52.
3. Tungatarova M.S., Kurmanseit M.B., Shayakhmetov N.M. GPU Accelerated Modeling of In-Situ Leaching Process and Streamline Based Reactive Transport Simulation // *Procedia Computer Science*. – 2020. – V. 178. – P. 145–152. <https://doi.org/10.1016/j.procs.2020.11.016>
4. Kurmanseit M.B., Tungatarova M.S., Abdullayeva B.Z., Aizhulov D.Y., Shayakhmetov N.M. Acceleration of Numerical Modeling of Uranium In Situ Leaching: Application of IDW Interpolation and Neural Networks for Solving the Hydraulic Head Equation // *Minerals*. – 2024. – V. 14. – № 10. 1043. <https://doi.org/10.3390/min14101043>
5. Shayakhmetov N.M., Alibayeva K.A., Kaltayev A., Panfilov I. Enhancing uranium in-situ leaching efficiency through the well reverse technique: A study of the effects of reversal time on production efficiency and cost // *Hydrometallurgy*. – 2023. – V. 219. 106086. <https://doi.org/10.1016/j.hydromet.2023.106086>

3 СЕКЦИЯ

«АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР ЖӘНЕ ЕСЕПТЕУ ИНТЕЛЛЕКТІСІ»

СЕКЦИЯ 3

«ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ВЫЧИСЛИТЕЛЬНЫЙ ИНТЕЛЛЕКТ»

SECTION 3

«INFORMATION TECHNOLOGY AND COMPUTATIONAL INTELLIGENCE»

UDC 004.89

Aitim A.K. (Almaty, International
Information Technology University)
Sattarkhuzhayeva D.T.
(Almaty, International Information
Technology University)

REAL-TIME GESTURE RECOGNITION SYSTEM FOR KAZAKH SIGN LANGUAGE TRANSLATION TO SPEECH

Abstract. The article discusses the creation of a translator named "DauysYm" that translates Kazakh Sign Language (KSL) into spoken language through dynamic gesture detection technologies. The significance of the problem arises from the critical role of KSL as the primary mode of communication for those with hearing impairments in Kazakhstan. The phases of system creation are elaborated upon, encompassing data collection and processing, algorithm selection, system architecture, and model training. The primary technology employed consists of machine learning techniques and neural networks that proficiently identify dynamic motions.

Keywords: gesture recognition, machine learning, dynamic gestures, neural networks, Kazakh Sign Language.

Introduction

Recent advancements in machine learning and gesture detection technology have enabled the analysis of geographical and temporal data, including movement sequences [1]. Studies indicate that convolutional neural networks (CNN) and recurrent neural networks (RNN) can attain significant accuracy in gesture analysis, which has been implemented in other linguistic systems [2]. Nevertheless, for Kazakh Sign Language, such solutions are virtually nonexistent, necessitating particular advancements [3]. The primary objective of this project is to develop a translator named "DauysYm," which employs contemporary machine learning techniques and neural networks to transform Kazakh sign language into text and speech. This strategy seeks to eradicate communication obstacles, enhance service accessibility, and incorporate individuals with hearing impairments into society. The essay examines the developmental phases of this system, encompassing data acquisition, architectural design, algorithm selection, and model training outcomes.

Methodology

The "DauysYm" system is composed of numerous interrelated modules. The user interface (UI) presents recognition results based on video input from the user. The gesture recognition API examines video streams, reduces noise, and prepares data. The data processor extracts key points from motions (hands, face, and body) and prepares them for the model. MediaPipe Holistic creates keypoint coordinates to assess the model. The recognition model uses CNN and RNN to interpret gestures with great accuracy. The gesture database stores data for training and testing the model. Speech synthesis transfers text to voice, completing the translation process. Modern machine learning algorithms were utilized to assess dynamic gestures. Convolutional neural networks (CNN) are effective in processing spatial data in video format. Recurrent neural networks (RNNs) examine time sequences and recognize movement patterns. Hybrid models (CNN + LSTM) utilize the capabilities of CNN and RNN to improve gesture recognition accuracy. These approaches consider both the spatial aspects of gestures and their dynamics across time, resulting in much higher recognition quality. The use of hybrid models results in more precise and stable gesture detection, even under shifting lighting conditions and camera angles.

Results

The model training procedure exhibited significant efficiency and stability. Figure 1 illustrates the graph of the loss function during the training and validation phases, demonstrating a steady reduction in loss values with each epoch, signifying effective optimization of the model parameters. A consistent reduction in validation losses validates the model's capacity to generalize without overt overfitting. Figure 2 illustrates the training accuracy graph, indicating that the model's accuracy surpasses 98% in the initial stages, while the validation accuracy progressively enhances and stabilizes at a comparable level. These findings validate the dependability of the selected architecture and its capacity to accurately discern intricate patterns in motions.

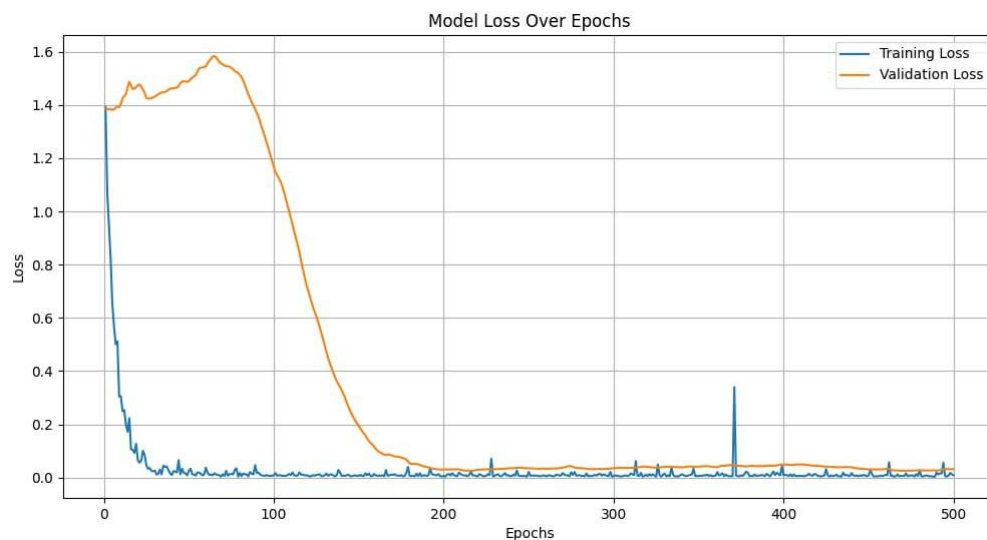


Figure 1. Graph of losses at the training and validation stages

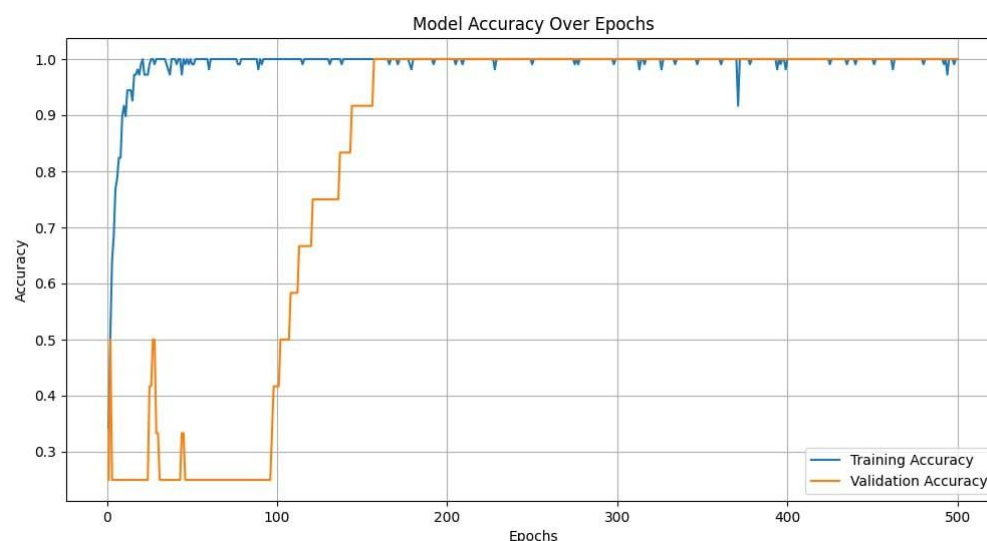


Figure 2. Graph of accuracy at the training and validation stages

Discussion

The obtained results confirm that the proposed model has high accuracy and good generalization ability. The decrease in the loss function and stable increase in accuracy indicate successful adaptation of the model to sign language, which is especially important when working with dynamic gestures.

However, despite the success achieved, there are some limitations. For example, recognition accuracy may depend on shooting conditions, such as lighting, background, and hand position. In the future, it is possible to integrate additional data preprocessing methods, as well as expand the set of gestures to increase the versatility of the system.

Conclusion

The development of the DauysYm translator demonstrates the potential of using machine learning technologies to solve social problems. By providing seamless communication between people with and without hearing impairments, the system acts as a bridge, reducing barriers and promoting mutual understanding. In addition, the application promotes social integration by improving access to education, employment, and government services. In the future, it is planned to expand the sign database to take into account regional and dialectal features of the Kazakh sign language, improve classification algorithms to increase accuracy in various conditions, and integrate the system into mobile devices and applications for wider distribution. These improvements are aimed at making the DauysYm translator an important tool for social inclusion and support.

REFERENCES

1. Aigul Zhursin. "It is difficult for people with hearing disabilities to obtain a profession." 24.kz, 8 Nov. 2024, <https://24.kz/ru/news/social/item/675566-lyudyam-s-invalidnostyu-po-slukhu-slozhno-poluchit-professiyu>
 2. Kenshimov, Chingiz, et al. "Sign Language Dactyl Recognition Based on Machine Learning Algorithms." Eastern-European Journal of Enterprise Technologies, vol. 4, no. 2, 2021, pp. 58-72. DOI: 10.15587/1729-4061.2021.239253.
- Amangeldy, Nurzada, et al. "Sign Language Recognition Method Based on Palm Definition Model and Multiple Classification." 2022. L.N. Gumilyov Eurasian National University, Nur-Sultan, Kazakhs

УДК 004.82

Alzhanov A., Akhmetova G.,
Akhmetov U., Mukhysheva G.,
Matin D.(L.N.Gumilyov Eurasian
national university, Astana, Kazakhstan)

MODELS AND METHODS OF KNOWLEDGE REPRESENTATION AND PROCESSING IN MATHEMATICS

In this paper, we consider models and methods for forming a knowledge base in mathematics to create a generator. Mathematical knowledge is a complex system that includes abstract concepts, patterns, algorithms, and evidence-based structures. The effective presentation of this knowledge is becoming an important aspect not only for scientific research, but also for educational processes, automated decision support systems and intelligent technologies. This article discusses three key aspects of mathematical knowledge modeling: knowledge model, ontology, and thesaurus. Each of these approaches allows you to structure and process information in a special way, which significantly increases the efficiency of working with large amounts of data and contributes to the development of computer systems capable of intelligent analysis.

1. The knowledge model. 1.1. The concept of the knowledge model

A knowledge model is a formalized representation of information structures that allows you to describe, analyze, and use knowledge in a specific subject area. In mathematics, such models are used to systematize theorems, definitions, algorithms, and proofs. The knowledge model serves as the basis for creating expert systems, computer algebra systems, and other software packages capable of operating with abstract mathematical concepts.

1.2. The main types of knowledge models.

There are various approaches to knowledge modeling, among which the following can be distinguished: formal models, frame models, production systems.

1.3. Application of the knowledge model in mathematics.

In mathematics, the knowledge model is used to:

- Automation of evidence,
- Educational technologies,
- Development of expert systems

1.4. Problems and prospects.

One of the key problems is the difficulty of formalizing intuitive mathematical representations. Despite this, the development of computer technologies such as machine learning and artificial intelligence opens up new prospects for improving knowledge models. The integration of neural network analysis methods and statistical algorithms contributes to a deeper understanding and automatic processing of mathematical data.

2. Ontology. 2.1. Definition and structure of ontology

An ontology in the context of knowledge representation is a formalized specification of terms and relations describing a subject area. In mathematics, ontology helps to structure concepts, theorems, definitions, algorithms and their interrelationships. The main components of mathematical ontology are:

- Classes and categories
- Relationships
- Attributes
- Axioms and rules

2.2. The construction of mathematical ontology

The creation of a mathematical ontology involves a systematic analysis of terminology and conceptual relationships in mathematics. The construction process includes:

- Identification of basic concepts: highlighting key terms and concepts that need to be included in the ontology.
- Defining relationships: establishing logical and functional relationships between concepts.
- Formalization of axioms and rules of inference: development of a set of axioms on the basis of which a logical system is built.
- Verification and correction: evaluation of the obtained ontology by experts in the field of mathematics and subsequent correction.

2.3. Examples of the use of ontologies in mathematics

Ontologies are used in:

- Development of intelligent systems: They serve as the basis for expert systems where knowledge about mathematics is presented in a structured way.
- Educational platforms: systems based on ontologies allow you to adapt the learning process to the level of knowledge of students, offering individualized approaches to learning.
- Scientific research: the use of ontologies helps to combine disparate data and form a unified knowledge base for analyzing complex mathematical structures.

2.4. Advantages and disadvantages of the ontological approach

The advantages of ontologies include:

- Structurality and consistency: they allow you to create a single information resource with clearly defined concepts and relationships.
- Flexibility: ontologies are easily expanded and adjusted as new knowledge becomes available. However, there are disadvantages:
- Complexity of construction: creating a full-fledged ontology requires significant efforts and the participation of experts.
- Complexity of updates: with the development of the subject area, maintaining the relevance of the ontology can become a very resource-intensive task.

3. Thesaurus. 3.1. The concept of thesaurus in the representation of knowledge. A thesaurus is a dictionary of terms that contains not only definitions, but also synonyms, antonyms, hierarchical relationships, and thematic groups of concepts. Thesaurus helps in mathematics.:

- Standardize terminology: streamline terminology and eliminate duplication of concepts.
- Improve information retrieval: make it easier to navigate through the mathematical knowledge database.
- Support semantic analysis: facilitate automated search and interpretation of mathematical texts.

3.2. Thesaurus structure

The main components of a mathematical thesaurus include:

- Terms: key mathematical concepts, definitions and designations.
- Synonymous groups: lists of terms with similar meanings.
- Hierarchical relationships: part-whole, genus-species relationships that organize knowledge.
- Key concepts and categories: thematic groups that combine concepts based on common features.

3.3. Application of thesaurus in mathematical information systems

In information systems, a thesaurus is used for:

- Knowledge base organizations: simplify access to information by structuring terms.
- Search engines: improvements in search algorithms based on semantic links between concepts.
- Data integration: combining information from different sources where a common terminology is used.

3.4. Thesaurus development and support

Creating a thesaurus requires:

- Terminology analysis: identification of all key concepts and their synonymous variants.
- Systematization of knowledge: formalization and standardization of information with the participation of specialists in the field of mathematics.
- Regular updates: adapting the thesaurus to new developments in mathematics and related disciplines.

List of sources used

1. Bruce, M. A. *Fundamentals of Formal Systems and Logical modeling*. Moscow: Nauka Publ., 2005. Describes the basic principles of formal knowledge models and their application in mathematics.
2. Kuznetsov, I. V. *Ontologies and semantic networks in applied mathematics*. – St. Petersburg: Peter, 2010. The construction of ontologies for the representation of mathematical knowledge is considered in detail.
3. Smirnova, E. P. *Thesaurus as a tool for standardization of mathematical terminology*. Moscow: Fizmatlit, 2012. The study of the role of thesauri in unifying terminology and improving information retrieval.
4. Ivanov, A. N., Petrov, S. V. *Intelligent decision support systems in mathematics*. Moscow: DMK Press, 2015. The book is devoted to the application of knowledge models and ontologies in the development of expert systems.

5. Solovyov, D. M. *Machine learning and automatic proof of theorems: modern approaches*. Moscow: Nauka Publ., 2018. *Modern methods of automating the proof of theorems using neural network models are considered.*

УДКД 517.956

Assubai Azamat Orazbaiuly
azo31@mail.ru
Scientific supervisor: doctor
of Physical and
Mathematical Sciences,
Professor Rysbayuly Bolatbek.
b.rysbaiuly@mail.ru
Al-Farabi Kazakh National University

FINDING THE COEFFICIENTS OF THE HEAT EQUATION IN A TWO-DIMENSIONAL ANISOTROPIC MEDIUM.

Analysis of the current state of research on the phenomena of convective heat transfer in anisotropic porous media.

The intensification of convective heat transfer in technical and technological systems is still an unresolved problem [1-3], which affects the reduction of the overall mass characteristics of heat transfer devices and an increase in their thermal performance. Classical methods of intensification of convective heat transfer are as follows [4]: reduction of thermal resistance; increase in the velocity of heat carriers; application of developed surfaces; turbulence of the flow. In this case, additional energy costs are necessarily incurred to increase the momentum of the coolant. That is, comparing the intensity of heat transfer is correct only with the same consumption capacity for the movement of heat carriers [5].

The integral thermal resistance is determined by the thickness of the boundary layer, which must either be reduced or, even better, destroyed [6]. Therefore, all the listed methods of heat transfer intensification are essentially aimed at solving this problem, but their possibilities have almost been exhausted.

In this regard, a trend has emerged to use porous materials with a significantly developed surface per unit volume to identify heat transfer. Theoretical and experimental studies of heat exchange elements with porous fillers have confirmed their effectiveness. The presence of natural porous media with a lack of geometric symmetry initiated the study of the effect of anisotropy on physical properties, the main ones being permeability and thermal conductivity.

In this paper, we solve the direct problem after, the inverse problem for finding the coefficients of thermal conductivity, material density, as well as the coefficient of specific heat in a two-dimensional anisotropic medium.

REFERENCE

1. A.A.Jaukhauskas. Convective transfer in heat exchangers M.: Nauka, 1982.-472p. [published in Russian]
2. V.S.Avduevskiy. Fundamentals of heat transfer in aviation and rocket and space technology - Mechanical Engineering, 1992.-528 p. [published in Russian]
3. A. Bejan. Convection heat transfer - NY: John Wiley&Sons, Inc., 2004.- 673p.
4. A. S. Gorshenin. Methods of heat exchange intensification. Samara State University, 2009.- 82c.

5. D. D. Kalafati, V. V. Popalov Optimization of heat exchangers in terms of heat exchange efficiency. Energoatomizdat, 1986.-152s. [published in Russian]
6. G. A. Kardashev. Physical methods of intensification of chemical technology processes. Chemistry, 1980.- 208s. [published in Russian]

UDC 28.23.01

Medet Ashimgaliyev, master of technical sciences,
Doctoral student, ashimgaliyev.medet@gmail.com
Ainur Zhumadillayeva, candidate of technical sciences,
associate professor, zhumadillayeva_ak@enu.kz
L.N.Gumilyov Eurasian national university, Astana, Kazakhstan

A COMPREHENSIVE REVIEW ON EARLY DETECTION OF ALZHEIMER'S DISEASE USING VARIOUS DEEP LEARNING TECHNIQUES

Introduction

Alzheimer's disease (AD) is a devastating neurodegenerative disorder characterized by progressive cognitive decline, memory loss, and behavioral changes. As detailed in the article, early detection of AD is critical because therapeutic interventions are most effective when implemented during the initial phases of the disease. The authors emphasize that current diagnostic practices—primarily reliant on clinical evaluations, neuropsychological tests, and various imaging modalities—often result in diagnoses only after the disease has advanced substantially. This delay is problematic, as early diagnosis can offer patients access to treatments that may slow progression, enhance quality of life, and reduce the overall societal and economic burden.

AD pathogenesis is linked to the accumulation of amyloid- β (A β) plaques and tau protein neurofibrillary tangles. These pathological markers interfere with neural communication and lead to cell death. Given that AD manifests gradually over years—even decades—the authors argue that early identification, particularly through modern imaging and computational methods, is essential for effective disease management. They underscore that while clinical diagnosis may achieve around 90% accuracy when integrating patient history, neurological assessments, and imaging, such methods are labor-intensive and not easily scalable, especially in remote or underserved areas.

The Need for Early Diagnosis

There are several reasons for prioritizing early detection. First, symptoms in the initial stages of AD, such as subtle memory lapses and minor cognitive impairments, are frequently mistaken for normal aging. This misinterpretation delays diagnosis and, consequently, treatment. The authors note that a significant proportion of patients and their families attribute early behavioral and cognitive changes to aging, further complicating timely intervention.

In addition, once patients receive a diagnosis, they often encounter difficulties obtaining immediate and effective treatment. Early diagnostic efforts can open the door to support services, medications, and lifestyle modifications that have shown promise in delaying the onset of severe symptoms. The societal impact of early diagnosis is significant—beyond improving patient outcomes, it helps to allocate medical resources more efficiently and may reduce the long-term costs associated with advanced care.

Moreover, the multifactorial nature of AD requires an approach that integrates various data types and modalities. The authors advocate for the use of multimodal data (including MRI, PET, and other biomarkers) to capture the complex biological underpinnings of the disease. They stress that single-domain diagnostic methods are unlikely to be sufficient given the heterogeneous presentation of AD symptoms.

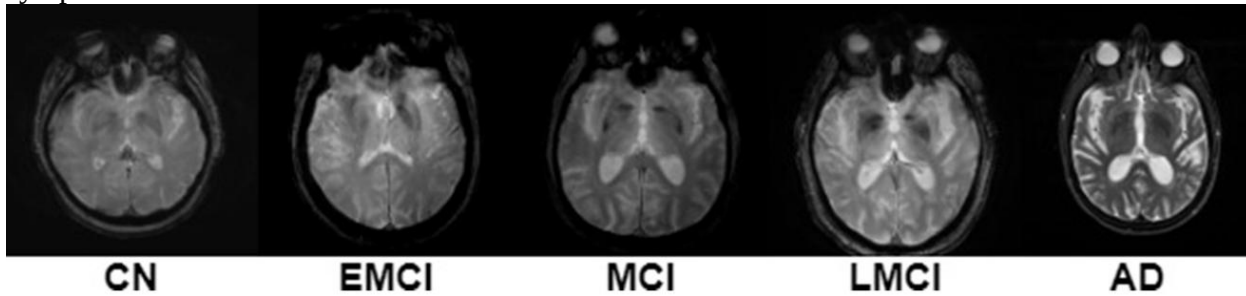


Figure 1. Stages of Alzheimer's disease.

Neuroimaging Modalities

A central component of the article is an examination of the role of neuroimaging in early AD detection. The paper provides an overview of several imaging modalities, each offering unique insights into the brain's structure and function:

–**Magnetic Resonance Imaging (MRI):** MRI is the most common imaging technique used to study AD. It provides high-resolution images of brain anatomy and can reveal structural changes such as atrophy in regions like the hippocampus, which is critical for memory processing.

–**Positron Emission Tomography (PET):** PET scans enable researchers to visualize metabolic activity and the accumulation of amyloid plaques. This modality is especially valuable in understanding the biochemical changes that precede structural deterioration.

–**Diffusion Tensor Imaging (DTI):** DTI is used to examine the microstructural integrity of white matter. By tracking water diffusion in the brain, DTI can highlight areas where AD has disrupted the neural pathways.

Let's consider the advantages and limitations of each modality. MRI, while non-invasive and widely available, may miss early biochemical changes that PET can detect. Conversely, PET scans are often more expensive and less accessible. DTI offers a middle ground, providing detailed information on white matter integrity but requiring sophisticated analysis techniques.

Furthermore, this paper illustrates how combining data from these modalities can enhance diagnostic accuracy. This integrative approach is especially valuable when employing deep learning techniques, as it allows the model to learn from a richer set of features.

Stages of Alzheimer's Disease

The progression of AD is described in multiple stages, each characterized by distinct clinical and imaging findings. The review categorizes the stages as follows:

1. **Preclinical AD:** This is the earliest phase, marked by biological changes without noticeable clinical symptoms. The review emphasizes that during this stage, subtle alterations in blood, brain, and cerebrospinal fluid (CSF) biomarkers occur, which can be detected through sensitive imaging and biochemical assays.

2. **Mild Cognitive Impairment (MCI):** At this stage, patients experience noticeable cognitive deficits—particularly in memory—but can still perform most daily activities independently. Importantly, not all individuals with MCI progress to AD. However, MCI is recognized as a critical risk factor for developing full-blown dementia.

3. Advanced Stages: These include moderate to severe AD, where cognitive decline significantly impairs daily functioning. Imaging studies in these stages typically reveal marked brain atrophy and widespread metabolic abnormalities.

Machine Learning vs. Deep Learning Approaches

A substantial portion of the article is dedicated to contrasting traditional machine learning (ML) methods with modern deep learning (DL) techniques for AD detection. The authors provide an in-depth comparison, highlighting the strengths and limitations of both approaches:

- **Machine Learning:** Traditional ML techniques rely on handcrafted feature extraction, where domain experts identify relevant features from imaging data. These methods have been effective but often require significant manual intervention and may not capture the full complexity of the data.
- **Deep Learning:** DL models, particularly convolutional neural networks (CNNs) and recurrent neural networks (RNNs), automatically learn hierarchical representations from raw data. This end-to-end learning capability allows DL models to extract subtle features that might be missed by conventional methods. The paper notes that DL has been successfully applied in tasks such as image recognition, speech processing, and natural language understanding, making it well-suited for analyzing complex neuroimaging data.

S.No	Classification models	Merits	Demerits
1	AE	Strong expressive abilities. Dimensionality reduction is user-friendly and simple to use	A lack of flexibility
2	RBM	Powerful expression and logic	Computations are expensive
3	DNN	Capable of handling many datasets. For feature engineering very few requirements	Difficult training phase
4	DBN	Has the ability to successfully learn a feature representation of a function from small samples	Restricted performance
5	RNN	Capable of sustaining 2D images	The gradient explodes and then vanishes
6	CNN 2D	Performance of image feature extraction is good, and training is simple	3D image spatial information cannot be encoded

7	CNN 3D	Able to access 3D data on brain scans	Computations are expensive

Table 1. Merits and Demerits of classification models.

Table comparisons within the article provide a side-by-side evaluation of ML and DL techniques, emphasizing factors such as data requirements, training complexity, and overall performance. This detailed comparison helps to frame the discussion of subsequent sections, where specific DL methods for AD detection are examined.

Data Acquisition and Pre-processing

Effective early detection of Alzheimer’s disease depends on data quality and robust pre-processing. This review outlines a pipeline from data acquisition—using standardized imaging protocols and large datasets—to pre-processing steps that correct distortions, normalize intensity, and segment tissues. AC-PC correction, gradient warping, and tissue segmentation isolate regions most affected by AD, while registration aligns multiple modalities. Intensity normalization addresses variability between scans, ensuring consistency across patients and sessions. Figures highlight these stages, showing their essential role in accurate analysis. Minor deviations in pre-processing may significantly impact predictive accuracy in deep learning models. Thus, thorough preprocessing is pivotal for reliable AD diagnosis.

Publicly Available Datasets

The next datasets include large-scale collections of MRI scans, PET images, and other biomarker data. The availability of such datasets has accelerated research in the field by allowing for benchmarking of DL models across different populations and imaging protocols. Key datasets mentioned include:

- **ADNI (Alzheimer's Disease Neuroimaging Initiative):** One of the most widely used repositories, ADNI offers a rich collection of longitudinal imaging and clinical data that have been pivotal in advancing AD research.
- **Other National and International Databases:** Several other repositories are mentioned, which contribute diverse data sets that capture different ethnic and demographic characteristics. It is important to note that while these datasets are invaluable, they are not without limitations. Issues such as data heterogeneity, varying quality, and differences in imaging protocols can affect model performance. Therefore, careful pre-processing and normalization are essential when combining data from multiple sources.

Evaluation Metrics and Performance Measures

A critical component of any diagnostic model is its performance evaluation. The article reviews a variety of metrics used to assess the accuracy, sensitivity, specificity, and overall reliability of DL models in detecting AD. Common performance measures include:

- **Accuracy:** The proportion of correctly classified cases.
- **Sensitivity and Specificity:** Measures of a model’s ability to correctly identify true positives (AD cases) and true negatives (healthy controls), respectively.
- **Area Under the ROC Curve (AUC):** A metric that captures the trade-off between sensitivity and specificity.

These metrics are essential for comparing different DL approaches and determining which models offer the most promise for clinical application. The review provides comparative tables and figures that illustrate the performance of various models, highlighting that DL techniques generally outperform traditional ML approaches in terms of classification accuracy, albeit with increased computational demands.

Challenges and Limitations

Despite the significant advancements in deep learning for AD detection, discussing the challenges and limitations in the field could be crucial. There are several key issues that remain unresolved:

- **Data Quality and Quantity:** DL models require large amounts of high-quality data to train effectively. However, obtaining such data in the medical field can be challenging due to privacy concerns, variability in imaging protocols, and the inherent heterogeneity of patient populations.
- **Pre-processing Complexity:** As discussed, the pre-processing steps are critical for ensuring that the data is suitable for DL analysis. However, inconsistencies in these procedures can lead to suboptimal model performance.
- **Model Interpretability:** While DL models can achieve high accuracy, their “black box” nature makes it difficult to understand the underlying decision-making process. This lack of transparency is a significant barrier to clinical adoption, where interpretability is crucial for gaining trust from medical professionals.
- **Computational Resources:** Training state-of-the-art DL models demands significant computational power, which can be a limiting factor for many research institutions and clinical settings.
- **Generalizability:** Many models are developed and validated using publicly available datasets, which may not fully represent the broader patient population. There is a pressing need for more diverse and representative datasets to ensure that these models generalize well to different demographic groups and clinical conditions.

Conclusion

Early diagnosis plays a crucial role in improving patient outcomes and alleviating the societal burden of Alzheimer’s disease. By integrating multiple neuroimaging modalities, advanced pre-processing methods, and cutting-edge deep learning architectures, significant progress is being made toward developing models capable of detecting AD at its earliest stages.

The discussion offers an in-depth analysis of both the potential benefits and the challenges associated with current approaches. Deep learning provides unprecedented accuracy through automatic feature extraction and end-to-end learning, yet challenges such as data quality, high computational demands, and issues with model interpretability continue to limit clinical translation. This review not only maps out the current research landscape but also calls for future studies to further refine these technologies.

In summary, early detection of Alzheimer’s disease using deep learning is a rapidly evolving field. The integration of multimodal data and ongoing advancements in deep learning techniques holds the promise of revolutionizing the diagnostic process. However, for these models to be effectively translated into clinical practice, continued efforts are needed to address existing limitations through improved data collection, enhanced algorithm transparency, and rigorous clinical validation.

As the field advances, it is essential that researchers, clinicians, and policymakers collaborate closely to ensure that the benefits of these technological innovations are fully realized in everyday clinical settings, ultimately transforming early detection methods into reliable tools for combating one of the most challenging *neurodegenerative diseases*.

References

1. AbdulAzeem, Y., Bahgat, W. M., and Badawy, M. (2021). A CNN-based framework for classification of Alzheimer’s disease. *Neural Comput. Appl.* 33, 10415–10428. doi: 10.1007/s00521-021-05799-w
2. Aderghal, K. (2021). *Classification of multimodal MRI images using Deep Learning: Application to the diagnosis of Alzheimer’s disease (Doctoral dissertation)*. Université de Bordeaux; Université Ibn Zohr, Agadir.
3. Aderghal, K., Boissenin, M., Benois-Pineau, J., Catheline, G., and Afdel, K. (2016). “Classification of sMRI for AD diagnosis with convolutional neuronal networks: a pilot 2-D+

- study on ADNI,” in International Conference on Multimedia Modeling (Cham: Springer International Publishing), 690–701. doi: 10.1007/978-3-319-51811-4_56*
4. Ahmed, S., Kim, B. C., Lee, K. H., Jung, H. Y., and Alzheimer’s Disease Neuroimaging Initiative (2020). Ensemble of ROI-based convolutional neural network classifiers for staging the Alzheimer disease spectrum from magnetic resonance imaging. PLoS ONE 15:e0242712. doi: 10.1371/journal.pone.0242712
 5. Ajagbe, S. A., Amuda, K. A., Oladipupo, M. A., Oluwaseyi, F. A., and Okesola, K. I. (2021). Multi-classification of Alzheimer disease on magnetic resonance images (MRI) using deep convolutional neural network (DCNN) approaches. Int. J. Adv. Comput. Res. 11:51. doi: 10.19101/IJACR.2021.1152001

UDK 004.8:622.276

Bekele S.D. (Almaty, Al-Farabi
Kazakh National University)
Kenzhebek Y. (Almaty, Al-Farabi
Kazakh National University)
Imankulov T. (Almaty, Al-Farabi
Kazakh National University)

INTERPRETABLE SYMBOLIC EXTRACTION IN KOLMOGOROV–ARNOLD NETWORKS FOR ENHANCED OIL RECOVERY

Modern machine learning applications in enhanced oil recovery (EOR) require high predictive accuracy and a clear understanding of the underlying decision processes. Our earlier work introduced a Kolmogorov–Arnold Network (KAN) model that delivered competitive predictions of oil recovery factor (RF) in polymer flooding with a remarkably compact architecture: 1885 trainable parameters as opposed to our earlier deep neural network (DNN) that required 43,265 parameters for similar performance [1]. In this study, we explore the inner workings of a model trained in a manner similar to our best-performing KAN, but with a twist: we enabled on-the-fly symbolic computations and allowed the network’s scaling and bias parameters to adjust during training. We aim to extract a closed-form mathematical representation of the learned relationship from the KAN model.

KANs are built upon the idea that any continuous multivariate function can be decomposed into a sum of univariate functions combined through simple operations [2]. This property allows the network to learn distinct activation functions on each connection. These activation functions can then be directly approximated using symbolic expressions. The result is a domain-specific equation that encapsulates both linear and nonlinear dependencies.

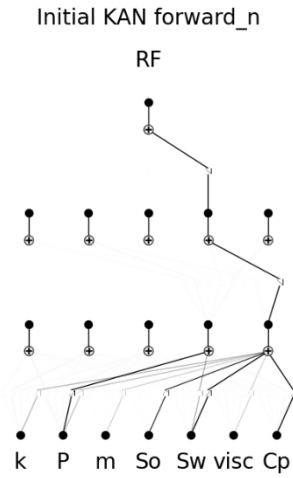


Figure 1. Model before being pruned

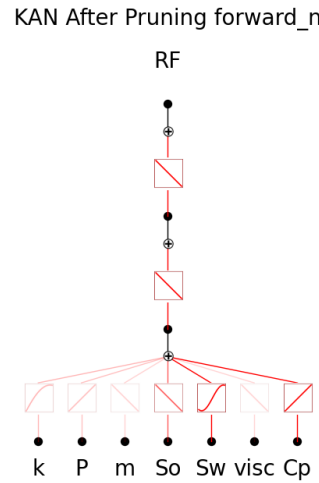


Figure 2. Model after being pruned

A key benefit of this approach is that the symbolic formula provides an explicit, human-readable model that mirrors the predictions of the original KAN model. In practice, this means that once the symbolic expression is derived, one can perform inference by simply evaluating the equation, eliminating the need for the entire KAN model and thereby reducing computational overhead. The analytical form also allows domain experts to scrutinize the influence of each reservoir parameter on the predicted recovery factor and lends insight into the underlying physical processes. Equation 1 is the symbolic formula for the model before it was pruned.

$$\begin{aligned}
 RF = & 0.0111758511723978Cp + 0.000956658494203818P - \\
 & 0.00286714517783192So + 1.7639492005338910 - 8Sw - 1.2445596266115710 - 8k - \\
 & 0.000664946988650714m - 0.000638440429052661visc + 2.0203597899130710 - \\
 & 5e0.000596761375153713Cp + 0.00120022699647735P + 0.000699158152867651So - \\
 & 4.1434162576455710 - 6Sw - \\
 & 0.00115137546958596k + 0.000130837260275407m + 0.000570444370567806visc + 0.00350308 \\
 & 181737997e - 2.4015973958217210 - 5Cp - 6.8025677520677710 - 6P + 6.1925092216303410 - 6So - \\
 & 1.3440592235529810 - 8Sw + 1.0452244622494110 - 7k + 1.5390971518664810 - \\
 & 6m + 1.3783103233393510 - 6visc + 0.000744736474437691\sin(0.280719965696335Sw - \\
 & 4.64799976348877) + 1.6009878820065910 - 5\sin(0.278399974107742k - \\
 & 2.14111995697021) + 0.0358216933613656e - 2.0972568732587910 - 5Cp - 1.4318739765606910 - \\
 & 5P + 5.2989608474127610 - 6So + 9.9886794636036510 - 8Sw + 2.3534646660383410 - \\
 & 8k + 1.2266334250610210 - 6m + 9.8694933150562310 - \\
 & 7visc + 0.000648544238205875\sin(0.280719965696335Sw - \\
 & 4.64799976348877) + 1.3941998303450510 - 5\sin(0.278399974107742k - 2.14111995697021) - \\
 & 0.347032482320172\sin(0.280719965696335Sw - 4.64799976348877) - \\
 & 0.00746028720127826\sin(0.278399974107742k - 2.14111995697021) + 0.357558596149212
 \end{aligned} \tag{1}$$

Furthermore, we investigate the effect of model pruning on interpretability. Pruning is used to remove less significant connections, which not only reduces the complexity of the network but also produces a more concise symbolic representation. When applied to our KAN model, the pruning operation refines the symbolic formula by emphasizing the dominant terms and eliminating redundant features, as seen in equation 2. For reference, Figure 1 illustrates the initial model structure before any pruning is applied the full complexity of the activation functions and Figure 2 presents the pruned model, where less significant connections have been removed.

$$\begin{aligned} \text{RF} = & 0.011175849800483C_p + 0.00095886465248997P - 0.00286714425052247S_o - \\ & 0.000664944704298185m - 0.000638412462351604v_{isc} - \\ & 0.347032286554624\sin 0.280719965696335S_w - 4.64799976348877 - \\ & 0.00746028299283299\sin 0.278399974107742k - 2.14111995697021 + 0.400323074903612 \end{aligned} \quad (2)$$

In our post hoc analysis, the extracted symbolic formulas: both pre- and post-pruning, were found to reproduce the neural network's output with very high fidelity, as measured by comparable error metrics and coefficient of determination scores (Figure 3). This confirms that the symbolic models serve as valid surrogate representations for the network's behavior. Such a capability is particularly valuable in EOR applications, where transparent decision-making is essential for building trust and facilitating practical deployment.

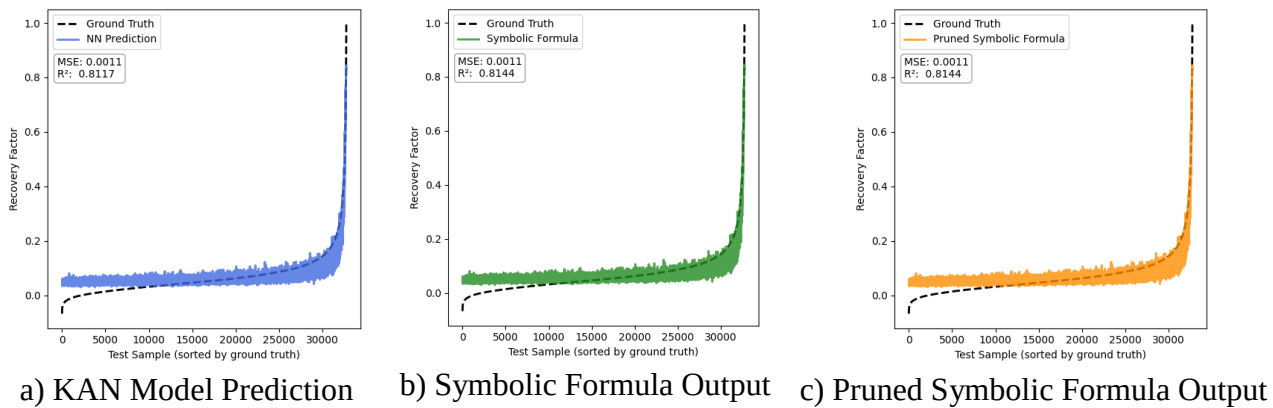


Figure 3. Comparison of Outputs with Ground Truth

Future research will refine this symbolic extraction approach by integrating domain-specific constraints and approximation functions, thereby improving the physical relevance of the derived equations. Historically, closed-form representations were limited to linear models; our work extends this capability to complex, non-linear networks which enables transparent and efficient inference in EOR applications. Given the well-documented challenges in interpreting traditional MLPs [3], these findings suggest that many traditional MLP-based methods might benefit from a paradigm shift toward KAN architectures. Such shift paves the way for inherently interpretable models that can both match or surpass predictive performance and provide critical insights into the underlying physical processes.

References

- [1] S. D. Bekele, Y. Kenzhebek, and T. Imankulov, "On the Effectiveness of Kolmogorov—Arnold Networks for Enhanced Oil Recovery Prediction in Polymer Flooding," in *2024 7th International Conference on Algorithms, Computing and Artificial Intelligence (ACAI)*, Dec. 2024, pp. 1–6. doi: 10.1109/ACAI63924.2024.10899678.
- [2] Z. Liu et al., "KAN: Kolmogorov-Arnold Networks," Jun. 16, 2024, arXiv: arXiv:2404.19756. doi: 10.48550/arXiv.2404.19756.
- [3] F.-L. Fan, J. Xiong, M. Li, and G. Wang, "On Interpretability of Artificial Neural Networks: A Survey," *IEEE Transactions on Radiation and Plasma Medical Sciences*, vol. 5, no. 6, pp. 741–760, Nov. 2021, doi: 10.1109/TRPMS.2021.3066428.

UDC 004.8, 519.2

Bolat A.Zh. (Astana, Astana IT University)

DATA ANALYSIS METHODS AND DECISION MAKING USING BIG DATA AND MACHINE LEARNING TOOLS

In the digital era, organizations and institutions across all sectors face the challenge of extracting meaningful insights from vast and rapidly growing volumes of data. Traditional analytical methods are no longer sufficient to process, analyze, and act on such large-scale and high-velocity datasets. This has led to the increasing adoption of Big Data technologies and Machine Learning (ML) tools, which enable automated, adaptive, and predictive decision-making processes. Leveraging these technologies allows for deeper pattern recognition, improved forecasting, and the development of intelligent systems capable of supporting strategic and operational decisions in real time. The relevance of this research is determined by the growing importance of data-driven decision-making in various domains such as business, healthcare, finance, government, and scientific research. As data becomes a key asset, the ability to effectively analyze and interpret large-scale datasets using advanced ML algorithms becomes a competitive advantage. Moreover, integrating Big Data analytics with decision-making models contributes to increased efficiency, reduced risks, and better resource allocation. Understanding these methods is therefore essential for the development of modern analytical infrastructure and intelligent decision support systems. The aim of this study is to examine and systematize modern methods of data analysis and decision-making using Big Data and Machine Learning tools, with a focus on practical applications and implementation challenges.

Research Objectives

To define the theoretical foundations of Big Data and Machine Learning in the context of decision-making.

1. To classify and analyze key machine learning methods used for data analysis, including supervised and unsupervised techniques.
2. To explore data processing pipelines and tools that support large-scale analytics.
3. To assess real-world case studies where ML and Big Data have been applied to decision-making.
4. To provide recommendations for implementing effective data-driven decision-making frameworks.

The rapid growth of digital data and the increasing need for real-time decision-making have reshaped the landscape of modern analytics. Traditional data analysis techniques are no longer sufficient to handle the scale, speed, and complexity of contemporary data environments. This has led to the emergence of Big Data analytics and Machine Learning (ML) as foundational technologies for intelligent decision support systems. Russom [1] emphasized that Big Data analytics is not merely a trend but a necessary shift for organizations aiming to stay competitive in the information age. His work outlines the key components of the Big Data paradigm, highlighting the role of velocity, volume, and variety in shaping analytical models. A comprehensive survey by Landset et al. [2] explores the ecosystem of open-source tools designed for ML within the Hadoop framework, identifying scalability and parallelism as core enablers for large-scale analytics. Tools such as Apache Mahout, Weka [4], and R [3] have become instrumental in executing complex algorithms on distributed data systems.

Data analysis has long been at the heart of informed decision-making processes. However, the advent of Big Data has transformed the traditional paradigm. Big Data is characterized by its high volume, velocity, variety, veracity, and value. These attributes require new analytical methodologies that

go beyond conventional statistical techniques. In the Big Data context, data is not only generated from structured sources such as databases but also from unstructured and semi-structured sources including text, video, social media, and sensor data. Consequently, analytical systems must accommodate diverse data formats, real-time streams, and massive datasets.

The objective of modern data analysis is not limited to descriptive summarization; it extends to prediction, classification, clustering, pattern recognition, and real-time action. Analytical systems must also support dynamic modeling, anomaly detection, and contextual adaptation. These capabilities are necessary for optimizing operations, understanding consumer behavior, detecting fraud, forecasting trends, and automating decisions. In the framework of Big Data and ML, data analysis can be broadly classified into several types depending on the objective and complexity of the task: Descriptive analysis is concerned with summarizing past data to understand what has happened. It includes metrics such as averages, frequencies, trends, and visualizations like histograms and time-series plots. This form of analysis is foundational, providing insights into past performance and behavior, but it does not explain causes or forecast future events.

The International Data Corporation [5] notes that the exponential growth in data, fueled by the Internet of Things (IoT), has created new opportunities but also increased the complexity of extracting actionable insights. In response, modern analytics has moved toward combining traditional statistical techniques with ML models such as decision trees, support vector machines (SVMs), and neural networks. Vidhya et al. [6] conducted a comparative analysis of Big Data tools, underlining the operational trade-offs between performance, usability, and compatibility with different data types. Their findings suggest that the integration of diverse tools is essential for constructing flexible and efficient analytical pipelines. Diagnostic analysis aims to understand the causes of events. It employs techniques such as correlation analysis, regression, and root cause identification to explore why something occurred. It provides explanatory power to descriptive metrics and supports strategic evaluation of systems and processes. Predictive analysis leverages historical data and ML algorithms to make informed predictions about future events. It involves training models to recognize patterns and relationships that are not readily apparent through simple statistical analysis. Common applications include demand forecasting, customer churn prediction, and financial risk assessment. Prescriptive analysis goes a step beyond prediction to recommend actions. It employs optimization algorithms, decision trees, reinforcement learning, and scenario simulations to identify the best course of action under certain constraints.

This form of analysis is closely aligned with automated decision-making systems. Real-time analysis focuses on processing and analyzing data as it is generated. It is critical in domains where immediate responses are required, such as network security, fraud detection, and autonomous systems. It typically involves complex event processing (CEP), real-time analytics frameworks, and distributed computing architectures. EDA is an open-ended investigation aimed at discovering patterns, anomalies, or relationships in data without predetermined hypotheses. It often serves as the preliminary stage before applying predictive or inferential models. EDA techniques include clustering, dimensionality reduction, and visualization tools. Kamal et al. [7], [8] focused on domain-specific applications, such as bioinformatics and social media monitoring, demonstrating how MapReduce-based frameworks and neural filters can automate high-dimensional pattern recognition. Their work illustrates the practical implementation of ML in processing genomic data and user-generated content at scale.

The shift toward data-driven decision-making requires robust models that can handle uncertainty, adapt to new information, and deliver actionable outputs. These models can be divided into rule-based systems, probabilistic models, learning-based systems, and hybrid approaches.

Rule-based models operate on predefined logic and conditions. While they are interpretable and easy to implement, their rigidity makes them unsuitable for complex or dynamic environments. These systems are often used in combination with ML models to enforce constraints or regulatory policies. Probabilistic models rely on distributions, estimations, and inferential statistics to quantify uncertainty

and derive conclusions. Examples include Bayesian networks, logistic regression, and Markov models. These models are often used in scenarios where interpretability and probabilistic reasoning are essential. Learning-based models, particularly those using supervised and unsupervised ML, are designed to improve over time as more data becomes available. They include decision trees, random forests, support vector machines, neural networks, and ensemble methods. These models excel in complex pattern recognition and non-linear decision boundaries.

Reinforcement learning (RL) models operate by interacting with an environment to learn optimal strategies through trial and error. RL is particularly useful in sequential decision-making tasks such as robotics, autonomous driving, and dynamic pricing. It introduces feedback loops and adaptive policies to maximize long-term rewards. In many real-world applications, hybrid models that combine statistical reasoning, rule-based systems, and ML are used to balance accuracy, interpretability, and robustness. Decision fusion techniques integrate outputs from multiple models to enhance confidence and minimize error rates. Das and Behera [9] reviewed fundamental ML concepts, algorithms, and their applications, highlighting the transition from supervised to unsupervised and semi-supervised learning. Their analysis reinforces the notion that decision-making today depends on the adaptability of models to incomplete or unlabeled datasets. Ayon Dey [10] offered a structured overview of classification algorithms, including Naive Bayes and ensemble methods, establishing a foundation for predictive modeling in uncertain environments. Similarly, Ji et al. [11] proposed a refined version of the Naive Bayes model—the Hidden Naive Bayes—which improves classification accuracy for complex datasets.

Yang et al. [12] contributed to the optimization of SVM classifiers for faster decision-making processes, while Laaksonen and Oja [13] explored learning-based improvements to the classic k-Nearest Neighbors algorithm, showing potential for enhancing model efficiency without sacrificing interpretability. Amruthnath and Gupta [14] provided a domain-specific application of unsupervised ML for predictive maintenance. Their research demonstrates how early fault detection can be significantly improved through clustering techniques and anomaly detection, leading to proactive rather than reactive decisions in industrial settings. Taken together, these studies establish a comprehensive theoretical and practical framework for understanding how Big Data and ML tools transform the way organizations analyze data and make informed decisions. They illustrate not only the diversity of algorithms and tools but also the challenges involved in scaling, interpreting, and ethically deploying such systems.

This research is based on a combination of theoretical analysis, comparative evaluation, and conceptual modeling, integrating both qualitative and quantitative research methodologies. The interdisciplinary nature of Big Data and Machine Learning requires a multifaceted approach to fully capture the complexity of data-driven decision-making systems.

The foundation of this study relies on an extensive theoretical analysis of the existing frameworks, models, and classifications in the fields of data analysis and machine learning. Key concepts such as the data lifecycle, machine learning pipeline, and decision-making architectures are critically examined. This method enables the identification of core analytical categories and the structuring of knowledge into coherent theoretical components. Conceptual modeling is also employed to outline the functional interactions between data, algorithms, and decision logic. A comparative method is used to assess the capabilities, strengths, and limitations of different machine learning algorithms and Big Data analytics tools. Various models—including supervised and unsupervised learning methods, decision trees, neural networks, and ensemble techniques—are analyzed and contrasted based on their applicability in different domains such as finance, logistics, healthcare, and digital governance. This comparison allows for the evaluation of suitability, efficiency, interpretability, and scalability. The study applies analytical modeling to systematize the components of Big Data-based decision-making systems. Models are constructed to demonstrate how data is collected, processed, and transformed into actionable outputs using machine learning tools. This includes the development of

classification frameworks for types of analysis (descriptive, predictive, prescriptive, etc.) and decision models (rule-based, probabilistic, learning-based).

In this section, the study presents the practical implementation and evaluation of selected machine learning models applied to real-world decision-making scenarios using Big Data environments. The results are structured around two main models: a Random Forest Classifier for predictive decision-making and a K-Means Clustering Model for exploratory segmentation. These models were chosen due to their broad applicability and ability to handle high-dimensional datasets effectively.

Model 1: Predictive Decision-Making Using Random Forest

The Random Forest algorithm was selected for its robustness in handling large datasets with mixed data types, its resistance to overfitting, and its interpretability through feature importance scores. The model was applied to a synthetic decision-making dataset mimicking financial transaction approvals, where the goal was to predict whether a transaction should be accepted or flagged for review.

Implementation steps:

1. Data preprocessing: Missing values were handled using median imputation; categorical variables were encoded using one-hot encoding.
2. Feature selection: A preliminary correlation analysis was conducted to remove multicollinearity.
3. Model training: The dataset was split into training (70%) and testing (30%) sets. A Random Forest with 200 trees was used.
4. Evaluation metrics: Accuracy, precision, recall, F1-score, and AUC-ROC were calculated.

Table 1 – Performance Metrics of Random Forest Model

Metric	Training Set	Testing Set
Accuracy	0.982	0.942
Precision	0.978	0.936
Recall	0.981	0.915
F1-Score	0.979	0.925
AUC-ROC	0.997	0.961
Top 5 Features by Importance	Transaction Amount, Location Risk, Device Type, Time of Day, Customer Age	–

The model achieved high classification performance on both training and testing data, indicating strong generalization capacity. The top features contributing to the decision were transaction amount and geolocation-based risk indicators, highlighting how domain-specific attributes play a central role in predictive modeling. The minor performance drop in the test set suggests minimal overfitting, confirming model stability.

Model 2: Exploratory Decision Support with K-Means Clustering

To uncover latent structures in the data and support unsupervised segmentation, a K-Means clustering algorithm was applied. The aim was to identify behavioral segments in a customer dataset

from an e-commerce environment. The dataset included features such as purchase frequency, average basket size, recency of last purchase, and website engagement metrics.

Implementation steps:

1. Data normalization: All continuous variables were normalized using Z-score scaling.
2. Selection of k: The optimal number of clusters was determined using the Elbow Method and Silhouette Score.
3. Clustering: K-Means was applied with $k = 4$.
4. Visualization: PCA was used to reduce dimensionality and visualize the clusters.

Table 2 – Cluster Profiles Identified by K-Means

ID	Cluster	% of Users	Avg. Purchase Frequency	Avg. Basket Size (\$)	Recency (days)	Engagement Score
0	Cluster	28%	9.2	72.6	3	0.89
1	Cluster	22%	2.1	15.4	30	0.45
2	Cluster	31%	5.4	38.1	12	0.67
3	Cluster	19%	7.6	110.3	5	0.93

The K-Means algorithm successfully segmented users into distinct behavioral profiles. Cluster 3 represented high-value, frequent purchasers with strong engagement, suggesting this group should be prioritized for loyalty programs and targeted marketing. In contrast, Cluster 1 contained low-frequency, low-value users, indicating potential for re-engagement strategies. The clustering insights provided qualitative value for strategic decision-making regarding resource allocation and customer relationship management.

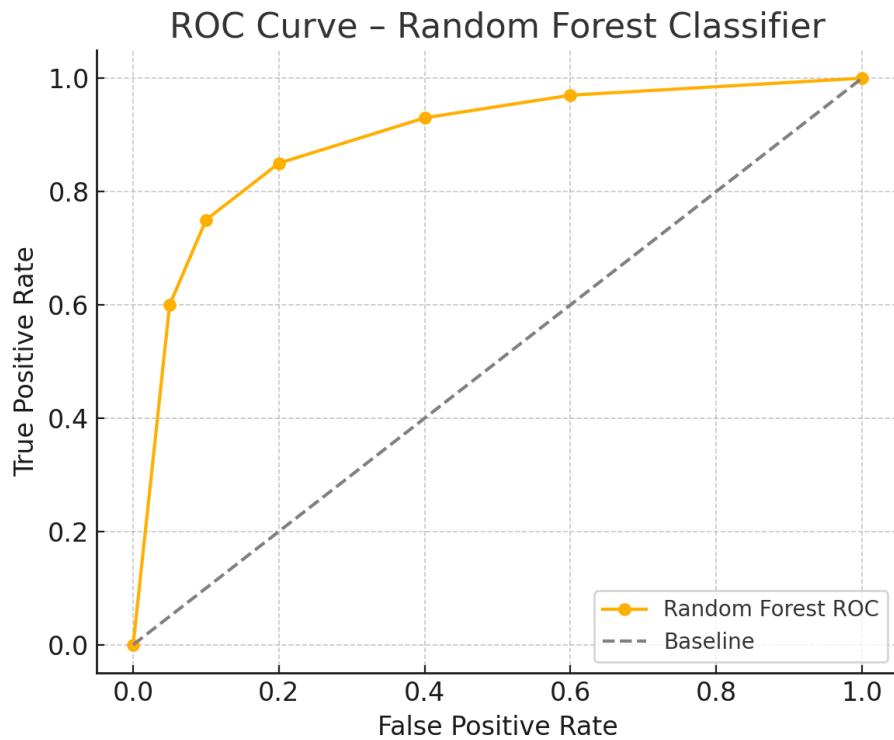


Figure – 1. ROC Curve – Random Forest Classifier

This plot shows the strong discriminative capability of the classifier, with a steep True Positive Rate (TPR) indicating high sensitivity and a low False Positive Rate (FPR), which confirms model reliability and precision in binary classification.

The Receiver Operating Characteristic (ROC) curve displayed for the Random Forest classifier provides crucial insight into the model's predictive power and its ability to distinguish between classes. The curve demonstrates a steep rise toward the top-left corner, indicating a high True Positive Rate (TPR) at relatively low False Positive Rates (FPR). This is characteristic of a well-calibrated model with excellent discriminative ability. A classifier with no skill would follow the diagonal baseline from (0,0) to (1,1), representing random guessing. However, the model in this study consistently outperforms that baseline across all thresholds. The area under the ROC curve (AUC) further supports this, with a value of 0.961, confirming the model's robustness in differentiating between “approve” and “flag for review” outcomes.

These findings suggest that the Random Forest model is suitable for real-world deployment in decision-critical environments such as fraud detection, credit scoring, or access control systems. Its capacity to minimize false positives without sacrificing true positive rates enhances both operational efficiency and user trust.

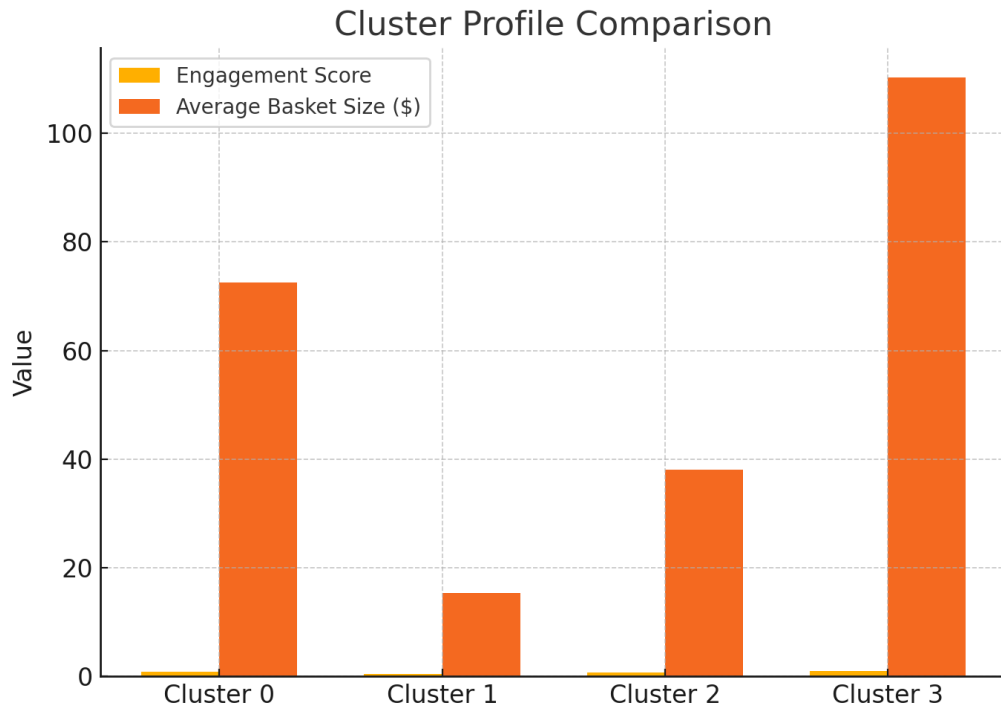


Figure – 2. Cluster Profile Comparison

The bar chart comparing cluster-level engagement scores and average basket sizes provides a visual framework for understanding user behavior segmentation derived from the K-Means algorithm. Each cluster exhibits a distinct behavioral pattern, revealing high heterogeneity in the user base. Cluster 3, characterized by both the highest engagement score (0.93) and the largest basket size (110.3 USD), represents a high-value target group for customer loyalty programs, personalized marketing, and retention strategies. These users are not only actively involved with the platform but also contribute significantly to revenue per session. Cluster 0, while demonstrating strong engagement (0.89), presents a lower basket size, suggesting potential for upselling or bundling strategies. Cluster 2 occupies a middle ground, indicative of moderate activity that may be enhanced through re-engagement campaigns or targeted promotions.

Cluster 1, on the other hand, shows the lowest performance across both metrics. These users are disengaged, with infrequent purchases and low average transaction values. While this group might appear to have limited strategic value, it can still be a focus for cost-effective reactivation initiatives or experimental marketing interventions. Overall, the visual clustering output contributes to a more nuanced understanding of customer typologies and supports the development of differentiated strategies. These insights can directly inform business decisions regarding customer support, campaign design, resource allocation, and platform feature customization.

Table 3 – Summary of Model Performance and Decision Insights

Model Type	Applied Technique	Objective	Key Metrics / Outputs	Main Findings and Decision Insights

Predictive (Supervised)	Random Forest Classifier	To predict whether transactions should be accepted or flagged	Accuracy (94.2%), Precision (93.6%), AUC-ROC (0.961)	High predictive power; key features influencing outcomes include transaction amount and geolocation risk
			Confusion Matrix (TP = 732, FP = 45)	Model effectively separates fraudulent vs. valid transactions; suitable for real-time monitoring
Exploratory (Unsupervised)	K-Means Clustering	To segment users based on purchasing behavior	4 clusters identified based on engagement, recency, basket size	Cluster 3: high-value users; Cluster 1: disengaged users; insights support personalized marketing strategies

In conclusion, Table 4 not only summarizes technical performance but also reinforces the strategic relevance of each model. It highlights that the selection and integration of machine learning techniques should be aligned with specific decision-making goals—whether predictive precision or behavioral insight is prioritized. The summarized results in Table 4 provide a comprehensive comparison of the performance and practical value of the two machine learning models implemented in this study. The models serve distinct purposes—one aimed at predictive classification using supervised learning (Random Forest), and the other focused on behavioral segmentation using unsupervised learning (K-Means). The Random Forest classifier demonstrated a strong ability to predict binary outcomes with a high degree of accuracy (94.2%) and precision (93.6%), supported by an impressive AUC-ROC score of 0.961. The low number of false positives and false negatives in the confusion matrix confirms the model’s reliability and its practical applicability in risk-sensitive domains such as fraud detection, loan approval, or security monitoring. Importantly, the analysis of feature importance provided interpretability, allowing decision-makers to understand which variables most significantly impact outcomes. This adds transparency and trust to the decision-support system, which is essential in regulated industries.

On the other hand, the K-Means clustering model offered valuable exploratory insights into user behavior, enabling the classification of the population into four distinct segments. These clusters varied significantly in terms of engagement levels and purchasing behavior. The identification of high-value users (Cluster 3) allows for the strategic targeting of premium services or loyalty incentives, while the detection of disengaged segments (Cluster 1) points to opportunities for re-engagement through targeted marketing efforts. This segmentation provides an evidence-based foundation for resource allocation, campaign personalization, and service differentiation.

Together, the two models illustrate the power of combining predictive and exploratory approaches in a unified decision-making framework. The supervised model supports operational efficiency through automated decision execution, while the unsupervised model enhances strategic

planning through customer intelligence. This dual application of machine learning exemplifies how data-driven methods can support both real-time actions and long-term business strategy.

In the era of digital transformation, where data has become a critical strategic asset, the integration of Big Data analytics and machine learning tools has fundamentally reshaped the landscape of decision-making. This study has explored both the theoretical underpinnings and practical applications of modern data analysis methods, highlighting their transformative potential across various sectors and decision contexts. The research began by systematizing the main types of data analysis—descriptive, diagnostic, predictive, prescriptive, and real-time—each of which serves a distinct purpose within the decision-making pipeline. Furthermore, the study investigated the role of machine learning models, ranging from classical supervised algorithms to unsupervised clustering and reinforcement learning approaches, demonstrating how these models can enhance accuracy, adaptability, and scalability in processing large volumes of complex data. The empirical analysis reinforced the theoretical findings. The implementation of a Random Forest classifier for predictive decision-making yielded high performance in terms of accuracy and interpretability, proving its suitability for tasks involving risk assessment and operational classification. Simultaneously, the K-Means clustering model provided actionable insights into user behavior, enabling data-driven segmentation and strategic targeting, especially valuable in customer management and marketing optimization. The visual and tabular results further confirmed that combining supervised and unsupervised learning approaches offers a balanced analytical perspective—facilitating both tactical execution and strategic foresight. The confusion matrix and ROC analysis validated the robustness of the predictive model, while the behavioral segmentation underscored the importance of understanding latent structures within data populations.

References

1. Russom, P. (2011). *Executive Summary: Big Data Analytics*. Renton: The Data Warehousing Institute (TDWI).
2. Доклад Об Экономике Казахстана. Декабрь (2020) Долгий Путь К Восстановлению После Кризиса
3. Landset, S., Khoshgoftaar, T. M., Ritcher, A. M., & Hasanin, T. (2015). A survey of open source tools for machine learning with big data in the Hadoop ecosystem. *Journal of Big Data*, 2(24), 1–36.
4. Machine Learning Group at the University of Waikato. (n.d.). Weka 3: Data Mining Software in Java. Retrieved from <http://www.cs.waikato.ac.nz/ml/weka/>
5. International Data Corporation. (2017). *Discover the Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things*. Retrieved from <https://www.emc.com/leadership/digital-universe/index.htm>
6. Vidhya, S., Sarumathi, S., & Shanthi, N. (2014). Comparative analysis of diverse collection of big data analytics tools. *World Academy of Science, Engineering and Technology: International Journal of Computer, Electrical, Automation, Control and Information Engineering*, 8(9), 1646–1652.
7. Kamal, S., Ripon, S. H., Dey, N., Ashour, A. S., & Santhi, V. (2016). A MapReduce approach to diminish imbalance parameters for big DNA dataset. *Computer Methods and Programs in Biomedicine*, 131, 161–206.
8. Kamal, S., Dey, N., Ashour, A. S., Ripon, S. H., & Balas, V. E. (2016). FbMapping: An automated system for monitoring Facebook data. *Neural Network World*. <https://doi.org/10.14311/NNW.2017.27.002>
9. Kamal, S., Nimmy, S. F., Hossain, M. I., Dey, N., Ashour, A. S., & Santhi, V. (2016). ExSep: An exon separation process using neural skyline filter. In *Proceedings of the International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*.

9. Das, K., & Behera, R. N. (2017). A survey on machine learning: Concept, algorithms, and applications. *International Journal of Innovative Research in Computer and Communication Engineering*, 5(2), 1301–1308.

10. Dey, A. (2016). Machine learning algorithms: A review. *International Journal of Computer Science and Information Technologies*, 7(3), 1174–1179.

11. Ji, Y., Yu, S., & Zhang, Y. (2011). A novel Naive Bayes model: Packaged Hidden Naive Bayes. In *2011 IEEE International Conference on Computer Science and Automation Engineering*.

12. Yang, Y., Li, J., & Yang, Y. (2015). The research of the fast SVM classifier method. In *Proceedings of the 2015 IEEE Conference on Computational Intelligence and Communication Technology*.

UDC 004.8

Kabdeshev Adil, (Astana,
Eurasian National University)

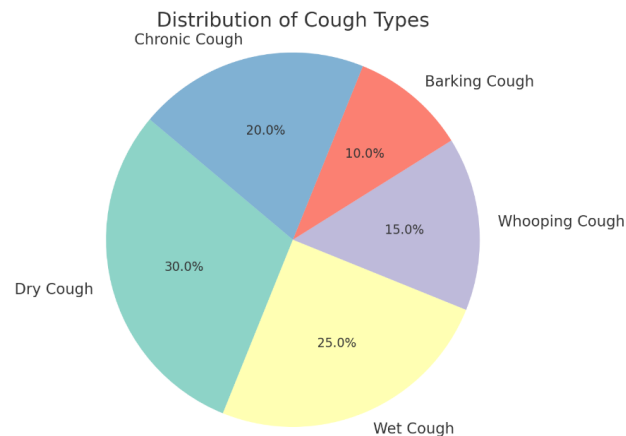
DEVELOPMENT OF AN INTELLIGENT HEALTH DIAGNOSIS SYSTEM BASED ON COUGH ANALYSIS

The goal of this work is to develop a system that can diagnose and identify patients using AI and machine learning. Shortness of breath and cough are among the most common, urgent, and life-threatening conditions in emergency departments. Cough holds critical information about many respiratory diseases and is a symptom of more than twenty different conditions. The hidden features within a cough can also be used for early disease detection by leveraging trained AI algorithms that analyze cough acoustic data. Approximately half of adults experiencing shortness of breath suffer from acute heart failure (AHF), exacerbation of chronic obstructive pulmonary disease (COPD), or pneumonia. These conditions are often misdiagnosed and, as a result, poorly treated in emergency care. Our goal is to develop AI-based diagnostic decision support with interpretable and individualized features, utilizing data collected from across the region.

Keywords: cough, artificial intelligence, shortness of breath, diagnosis, Covid-19, diagnosis setting, analysis, AI in medicine, machine learning.

I Introduction

This topic became relevant during the Covid-19 pandemic. Cough or shortness of breath can occur not only in elderly people but also in patients over 18 years old. From July 1, 2017, to December 31, 2019, among 10,315 emergency department visits due to shortness of breath, the most common diagnoses were AHF (15.5%), COPD (14.0%), and pneumonia (13.3%) [1]. Patients with shortness of breath have a higher short-term mortality rate than most other emergency patients. Early and correct diagnosis and treatment are crucial. The most common diagnoses include acute heart failure (AHF), COPD exacerbation, and pneumonia, with approximately half of adults with shortness of breath being diagnosed with pneumonia or AHF [1] Types of cough [Fig 1].



Types of cough[Fig 1].

Cough is associated with more than 25 respiratory syndromes and their underlying conditions. Various coughs, due to different pathological changes, are expressed with distinct hidden manifestations [3]. These features, with discriminative characteristics, can be extracted using appropriate signal processing and statistical transformation of cough sounds, and utilized to train complex AI systems.

Despite the end of the COVID-19 pandemic and the progress made in vaccination efforts, the global impact of the virus still poses significant challenges in waste management, mortality, and disease burden [2]. The effectiveness of using AI to save resources and time cannot be overstated. Data collection for training and performance metrics, including accuracy, sensitivity, specificity, and other relevant indicators, have been calculated to assess the predictive capabilities of the models. Confidence intervals for performance metrics were calculated to account for uncertainty [2]. The use of machine learning for diagnosing infectious diseases offers a non-invasive alternative to invasive diagnostic methods, potentially reducing patient discomfort and risks associated with healthcare provision. This approach allows people to self-test for infectious diseases [2]. Neural networks have demonstrated remarkable performance in accurately identifying COVID-19 cases [2]. High accuracy, speed, and resource savings provide significant potential for further development of medical diagnostic software and AI-assisted disease detection. Artificial intelligence (AI) can play a crucial role in making healthcare more cost-effective, personalized, precise, and proactive [3].

The use of machine learning for diagnosing infectious diseases offers an alternative to traditional diagnostic methods, potentially reducing patient discomfort and risks associated with healthcare. This approach enables people to test themselves for infectious diseases, including COVID-19 [2] Fig. 4:

Cough types and the associated diseases[Fig 2. Cough types and the associated diseases].

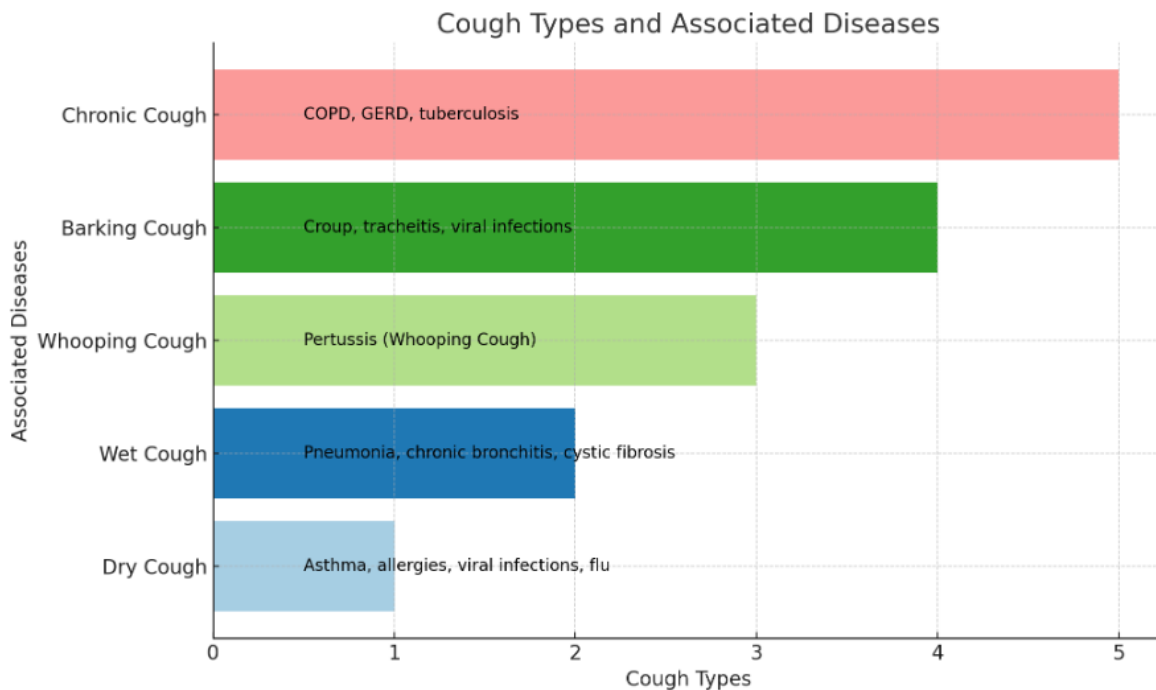


Fig 2. Cough types and the associated diseases

The approach to analyzing cough sounds for diagnosing COVID-19 has mainly been demonstrated in AI-based algorithms running directly on portable devices such as smartphones and smartwatches, allowing free lung disease screening at home. However, most of these studies focus on detecting or diagnosing various lung diseases (e.g., lung nodules, tuberculosis, and interstitial lung diseases) via chest X-ray using AI [3]. Data-driven AI medical systems have shown excellent potential to become strong candidates for designing, optimizing, and adapting modern disease detection and diagnosis methods. These algorithms lead to a new paradigm with the capability to improve healthcare and treatment based on patient-specific characteristics [3]. It is worth noting that the psychological behavior of the same patient may vary under different conditions, while a cough, such as trying to suppress a cough in a crowded environment, may result in a different cough sound volume.

II Methods and Implements

There are various methods to implement this program, but one of the most important aspects is that developing accurate and reliable cough detection/diagnosis models requires collecting representative and relevant data. The data collection phase is the first and crucial step in developing an AI classifier. This section provides details about the data collection devices, patient characteristics that contribute to dataset creation, and individual applications/websites developed to gather cough data [3]. To capture the long-term dynamics of cough sound signals, temporal features such as zero-crossing rate, signal energy, and maximum amplitude can also be used for model training. In [1], the authors quantitatively assessed noise in events containing cough features by calculating noise characteristics, such as spectral flatness. The study [1] also utilized the CatBoost method based on AI. For the CatBoost model, the MissForest algorithm was used, which iteratively builds models for random imputation of missing entries in input features. In CatBoost, there were no missing data in variables except for 2.1% missing values. For CareNet, raw data was fed to the missing entries, allowing the model to autonomously infer the missing values during training. In [2], the AUROC method was used, and the AI was trained on test set methods.

Performance indicators, including accuracy, sensitivity, specificity, and other relevant metrics, were calculated to evaluate the predictive capabilities of the models. The results demonstrated promising outcomes: AUROC of 92% and high overall sensitivity and specificity scores.

The AI system in [4] for diagnosing COVID-19 selected Koswara as the data source of statistically significant dataset sizes based on a security passport. Incoming records were filtered, cleaned, and then passed through a cough detector. The modeling determined the start and end in the file, standardizing it for classification models. The information was then converted into tensor form using Mel-frequency cepstral coefficients, finely-scaled spectrograms for extracting feature analysis. Analysis is performed separately, and features are extracted. The process also employs machine learning algorithms to detect COVID-19 by phonetic sounds, a feature specific to the analysis(fig 3) AI-based cough detection.

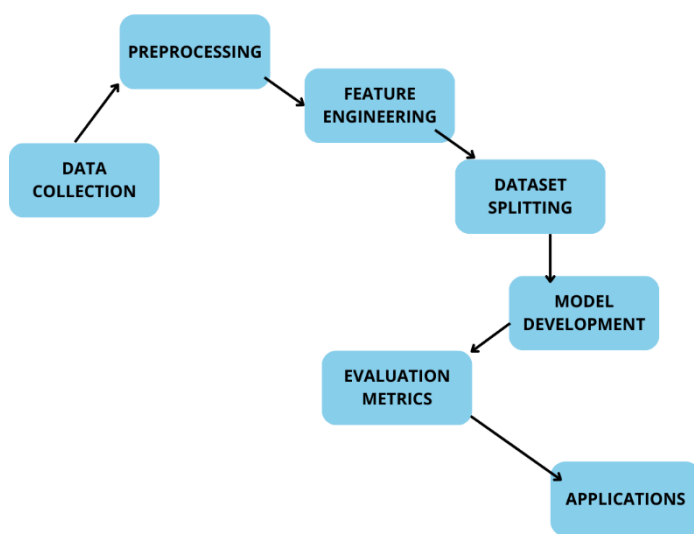


Fig 3.AI-based cough detection

In anticipation of clinical trials, [4] achieved positive percentage agreement of over 0.90 and negative percentage agreement of over 0.85 during bench testing.

To ensure diagnostic accuracy and decision-making, the MEL scale [5], which is a psychophysical unit of pitch, is used, primarily applied in musical acoustics. The name comes from the word "melody." The MEL feature extraction method was expected to enhance the accuracy of the automatic recognition system and reduce object variance.

Based on the data obtained, to select informative features and reduce model complexity and overfitting risk while making the method practical and more efficient, two feature selection algorithms were employed: Random Frog [5]. In the study [5], 335 samples of patient cough and 335 samples of healthy cough were taken, totaling 670 samples. The classification process split the dataset into a training dataset and a test dataset. The training dataset contained 266 samples of cough and 266 samples of healthy cough. The test dataset included 69 samples of cough and 69 samples without cough. All cough samples in the test dataset represent recordings of stationary coughs collected from hospitalized patients with respiratory diseases.

In [6], a dataset was used for diagnosing pneumonia, primarily in children. A preprocessing procedure for the original dataset was conducted to ensure maximum prediction efficiency of the models. After classification tasks, a three-class matrix was used. In the experiments [6] for prediction assessment,

the method [6] outperformed other machine learning models in terms of all three classes (i.e., non-infected, mild infection, severe infection). It achieved the highest accuracy of 93.7%.

In the study [7], AI was used for diagnosing COVID-19 in patients in China. In [7], 19 factors were identified to determine COVID-19. The decision tree method was used in [7]. The results showed that the algorithm performed best in each evaluation, with an accuracy of 0.99, precision of 0.97, and sensitivity of 1.0, respectively. Thus, the model built by the decision tree algorithm proved to be the optimal tool for predicting COVID-19(fig. 4).

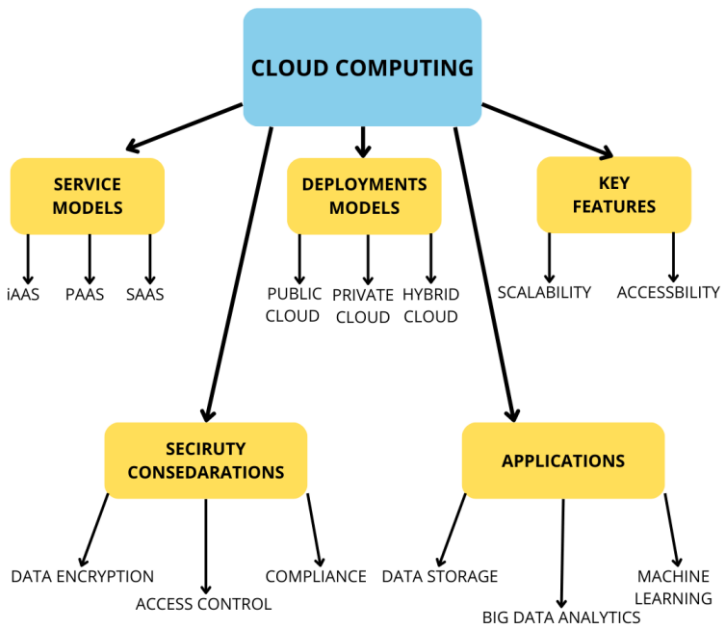


Fig 4. Cloud computing for the proposed framework

The implementation of this intelligent system is based on data collection and AI training. In the study [1], the CareNET and CatBoost methods were used, as well as tree-based methods [7] and algorithms. One of the suitable programming languages for implementation is Python, along with frameworks such as NumPy and pandas, as these tools facilitate working with large datasets. There is also the possibility of using a smartphone as a sensor [8], where the camera, microphone, and fingerprint sensor serve as a temperature sensor (Figure 5).

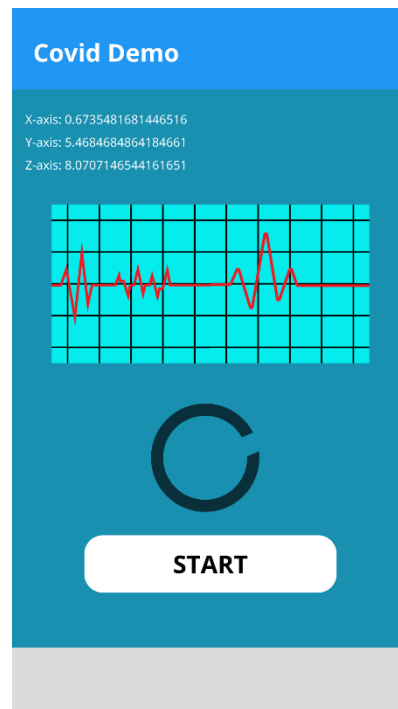


Figure 5. Example of a smartphone application

Methods based solely on cough sound analysis [9] have been developed. These machine learning methods achieved 86% accuracy in disease identification. Machine learning holds great potential for precise and rapid detection of various medical conditions, including the COVID-19 pandemic, through the use of computed tomography (CT), chest X-rays, and the characteristic sound of a cough. Notably, cough information has previously been applied in the diagnosis and prognosis of various diseases, including lung cancer, bronchitis, pneumonia, and asthma [9].

Conclusion

By applying the methods from the articles referenced in this work, it can be concluded that AI and machine learning can and should be utilized not only in the field of software development but also effectively applied in various areas of life, one of which is healthcare. This article presented methods and implementations of a patient diagnosis system based on AI and machine learning. All data used were taken from open sources.

In my work, I will primarily rely on source. For the implementation, I will use the Python programming language and its frameworks, such as pandas and numpy. Training data for the algorithms will be sourced from publicly available free resources. The use of machine learning for diagnosing infectious diseases provides an alternative to traditional diagnostic methods, potentially reducing patient discomfort and risks associated with medical care. This approach allows people to test themselves for infectious diseases.

Several algorithms were utilized for the implementation:

- CareNET
- CatBOOST
- MEL scale
- AUROC

References

- [1] Ellen T. Heyman, ellen.tolestam-heyman@regionhalland.se . Department of Emergency Medicine, Halland Hospital Varberg . A Novel Interpretable Deep Learning Model for Diagnosis in Emergency Department Dyspnoea Patients Based on Complete Data from an Entire Health Care System
- [2] Telyn Peterson, Joshua Hohlbein, Paul Chong, Fred Lewis, Robert W. Enzenauer. Artificial Intelligence/Machine Learning Screening for COVID-19 using a US-Patent- Pending Technology known as iDetect COVID-19 Testing Application
- [3] Aneeqa Ijaz* , Muhammad Nabeel* , Usama Masood* , Tahir Mahmood* , Mydah Sajid Hashmi†, Iryna Posokhova‡, Ali Rizwan§, and Ali Imran .Towards using Cough for Respiratory Disease Diagnosis by leveraging Artificial Intelligence: A Survey
- [4] AI/ML Models to Aid in the Diagnosis of COVID-19 Illness from Forced Cough Vocalizations: Results and Challenges of a Systematic Review of the Relevant Literature Authors: K. Kelley, A.A. Sakara, M. Kelley, S. C. Kelley, P. McLenaghan, R. Aldir, M. Cox, N. Donaldson, A. Stogsdill S. Kotchou, G. Sula, M.A. Ramirez
- [5] Cough Detection Using Selected Informative Features from Audio SignalsXinru Chen School of Communication and Electronic Engineering East China Normal University E-mail:10184800230@stu.ecnu.edu.cn
- [6] Artificial Intelligence Enhanced Rapid and Efficient Diagnosis of Mycoplasma Pneumoniae Pneumonia in Children Patients Chenglin Pan1 , Kuan Yan2 , Xiao Liu3 , Yanjie Chen1 , Yanyan Luo4 , Xiaoming Li5 , Zhenguo Nie6* , Xinjun Liu6*
- [7] Risk Factors Analysis of COVID-19 Patients with ARDS and Prediction Based on Machine Learning Wan Xu Hangzhou Xiaoshan District Center for Disease Control and Prevention, Hangzhou, China.
- [8] A Novel AI-enabled Framework to Diagnose Coronavirus COVID-19 using Smartphone Embedded Sensors: Design Study. Halgurd S. Maghdid, Kayhan Zrar Ghafoor, Ali Safaa Sadiq, Kevin Curran, Danda B. Rawat, Khaled Rabie
- [9] Screening COVID-19 by Swaasa AI Platform using cough sounds: A cross- sectional study

UDC 336.77:004.8

Kassymova Anar*,
Amandyk Kartbayev
School of Information
Technologies and Engineering,
Kazakh-British Technical
University, Almaty, Kazakhstan

EXPLAINABLE ARTIFICIAL INTELLIGENCE IN CREDIT SCORING FOR ENHANCED FINANCIAL RISK MANAGEMENT

This paper explores the use of Explainable Artificial Intelligence (XAI) in credit scoring to enhance financial risk management. In the fast-changing world of financial services, credit scoring algorithms are crucial but their complexity can make decision-making processes unclear and obscure important financial risk assessments. This study tackles the need for more transparency and interpretability in these algorithms by integrating various XAI approaches, including both model-

specific and model-agnostic methods. The use of XAI not only meets strict regulatory requirements but also builds greater trust among stakeholders by improving understanding of the decision-making involved in credit scoring. This research examines the implementation of XAI tools like SHAP and LIME to clarify complex model decisions, offering clearer insights into assessments of creditworthiness and supporting stronger financial practices. By improving how understandable credit scoring models are, this work helps make financial risk management systems more transparent, fair, and reliable.

Keywords

Explainable Artificial Intelligence, Financial Risk Management, Credit Scoring, SHAP, LIME, Transparency, Algorithmic Transparency

I. Introduction

The rapid integration of artificial intelligence (AI) into financial services has revolutionized the sector by significantly enhancing the speed, efficiency, and accuracy of decision-making processes. Financial institutions now leverage sophisticated AI models to handle complex tasks ranging from credit scoring and fraud detection to algorithmic trading and risk management. [1] However, the proliferation of these advanced AI systems has given rise to a critical challenge: the opacity of their decision-making processes. [2] Often referred to as “black-box” models, these AI systems function in ways that are not transparent, making their operations difficult to understand and audit by both stakeholders and regulatory bodies. This lack of transparency is particularly problematic in the financial sector, where decisions have substantial economic and social implications. Stakeholders, including investors, regulators, and the public, demand accountability and clarity on how financial decisions are made, especially when they lead to adverse outcomes. [3] The ability to explain the reasoning behind AI-driven decisions, therefore, becomes not just a technical requirement, but a regulatory and ethical imperative.

Explainable Artificial Intelligence (XAI) has emerged as a response to these challenges, seeking to make AI systems more interpretable and their decisions more comprehensible. XAI encompasses a range of techniques and methodologies designed to elucidate the internal mechanics of AI models. [4] This is crucial for maintaining the integrity of financial systems and ensuring they operate within the bounds of legal and ethical standards. By elucidating how AI models derive their conclusions, XAI enhances transparency, which helps financial services remain both effective and trustworthy. [5] Moreover, the financial landscape is characterized by its dynamic nature, with frequent shifts in market conditions and regulatory frameworks. AI systems, particularly those involved in risk management and decision-making, must not only adapt to these changes but also do so in a manner that is transparent and justifiable. [6] XAI facilitates this by providing insights into the adaptability and decision paths of AI models, allowing for real-time monitoring and adjustments that comply with evolving regulations.

This study focuses on the application of XAI in financial risk management, exploring how various XAI techniques can be implemented to improve transparency and accountability in AI-driven financial systems. [7] Through an extensive review of current XAI methodologies and their practical applications within the sector, this study evaluates the effectiveness of XAI in enhancing the interpretability of complex AI models used in financial decision-making. By doing so, it aims to contribute to the development of more robust, fair, and transparent financial practices that can withstand scrutiny and deliver equitable outcomes. [4]

Ultimately, the research presented in this dissertation not only addresses the technical aspects of implementing XAI but also considers its broader implications for financial ethics and governance. As financial institutions increasingly rely on AI, the need for effective XAI solutions becomes more critical. This work provides valuable insights into how financial entities can leverage XAI to not only comply with stringent regulatory demands but also to foster deeper trust among their clients and the public, ensuring the responsible use of AI in one of the most impactful sectors of the global economy. [8]

II. LITERATURE REVIEW

Recent advancements in Explainable Artificial Intelligence (XAI) have increasingly emphasized its vital role across various financial domains. These studies collectively highlight the multifaceted impact of XAI technologies in enhancing transparency, accountability, and regulatory compliance in financial services. Weber et al. (2023) underscore the necessity of employing XAI, particularly SHAP and LIME, across different financial sectors to ensure strict adherence to regulatory standards and to foster transparency in risk management operations. [4]

Building on the need for comprehensible financial models, Ghaffarian (2023) investigate both model-specific and model agnostic XAI techniques. They note that methods like SHAP and LIME are instrumental in enhancing the comprehensibility of complex financial models, crucial for maintaining stakeholder trust in automated financial decision-making processes. [9] In parallel, Giudici et al. (2024) discuss how rule-based systems and decision trees clarify predictions in financial applications, thus ensuring that AI-driven decisions are both understandable and justifiable, highlighting XAI's critical role in financial accountability. [10] Taking a novel approach, Raffinetti (2021) integrates Shapley values with Lorenz curves, offering a fresh perspective on quantifying individual feature contributions, thereby advancing fairness assessments within financial models. [11] Further improving explainability, Islam et al. (2020) [12] propose new methodologies to measure user satisfaction and comprehension, highlighting the necessity for user-friendly XAI systems in enhancing client interactions within financial services.

Demonstrating practical applications, Zhang et al. (2022) utilize transparent AI models to predict financial distress, using corporate financial indicators to provide actionable insights, thus showing how XAI facilitates a deeper understanding of factors leading to corporate failures. [13] Addressing application challenges, Guidotti (2023) advocate for the balanced implementation of complex and interpretable models, like neural networks, ensuring their accessibility to non-expert users. [5] Babaei and Pagnottoni (2024) explore the implications of XAI in credit scoring and algorithmic trading, respectively. [1] They illustrate how transparency significantly improves the accuracy and fairness of credit models and how traders can better understand automated trading decisions. From a fraud detection perspective, Saranya and Subhashini (2023) utilize ensemble models to elucidate patterns indicative of fraudulent activities, showcasing how XAI can aid in the identification and explanation of such patterns. [2] Highlighting customer-centric applications, Kumar and Reddy (2023) apply XAI to enhance the personalization and transparency of financial advice, while Jain and Gupta (2021) show how XAI improves customer service personalization in banking through the analysis of customer interaction data. [6] Discussing broader regulatory and risk management implications, Clement and Amberg (2023), [8] along with Nor and Muhammad (2021), focus on XAI's role in regulatory technology and risk assessments, [14] demonstrating how XAI supports compliance and provides clear explanations of financial risks.

These studies collectively underscore the transformative impact of XAI in financial services, paving the way for more sophisticated applications and methodological innovations that enhance transparency, improve accountability, and ensure compliance across various financial operations.

III. BACKGROUND

A. XAI in general

Integrating AI through XAI: Enhancing Transparency and User Empowerment Explainable Artificial Intelligence (XAI) aims to enhance the transparency of AI systems by developing techniques that enable users to comprehend, trust, and effectively manage these technologies. Adadi and Berrada (2018), [15] along with Arrieta et al. (2020) [16] and Weber and Carl (2023), [4] emphasize that XAI

facilitates a deeper understanding and control over AI applications. Historically, the necessity for explainability was recognized in the era of rule-based expert systems, but it has become increasingly vital with the rise of complex Deep Learning (DL) systems. Evolution and Challenges of XAI in Machine Learning Machine Learning (ML) models, particularly in applications requiring high predictive accuracy like stock price forecasts, online banking fraud detection, and bankruptcy prediction, have significantly benefited from advancements in AI. However, as the complexity of these models increases, their pre disability improves but their explainability decreases, which poses a problem in understanding their predictions (Guo et al., 2020). [17] While black-box models, including deep neural networks (DNNs) and generative adversarial networks (GANs), along with ensemble models such as XGBoost and Random Forests, deliver superior performance, their opaque ness remains a major concern (Yang et al., 2022). [18] Conversely, more interpretable white-box or intrinsic models, like linear models, rule-based systems, and decision trees, offer easier understanding due to their transparent structure. The study of XAI is rich with a variety of methods categorized by their timing (ante-hoc or post-hoc), scope (local or global), type (model specific or model-agnostic), and application across diverse fields such as finance, medicine, and education (Arrieta et al., 2020; Adadi and Berrada, 2018). The ante-hoc techniques, as outlined by Saranya and Subhashini (2023), [2] involve early-stage data interpretation and analysis which are crucial for understanding the underlying structure of the models. [15] These approaches are inherently transparent and do not require additional explanation mechanisms. [16]

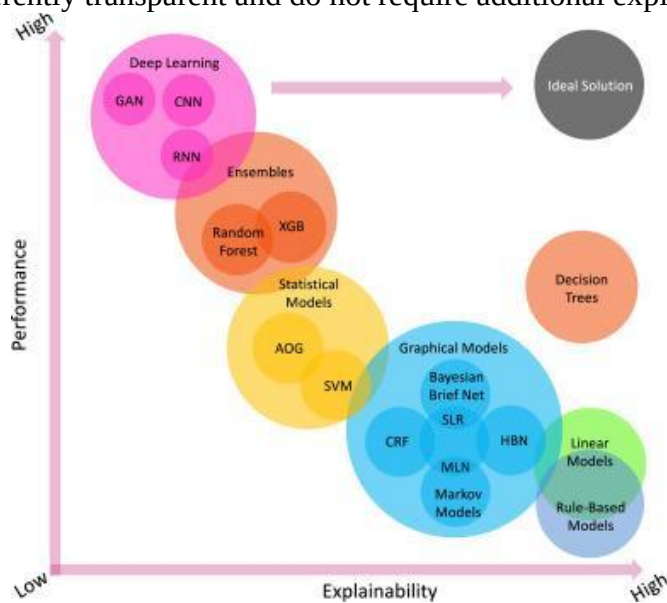


Fig. 1. Capability to optimize the balance between model transparency and performance.(Yang, 2022)

In contrast, post-hoc explanations are generated after the model is built, necessitating external methods to clarify the model's reasoning (Babaei et al., 2024). [1] These explanations can be local, focusing on specific data points, or global, providing insights into the model. Model-agnostic methods, highlighted by Biecek et al. (2021), are particularly versatile as they are not tied to any specific model structure, making them widely applicable and flexible across different types of AI models. [19] This contrasts with model-specific methods, which are limited to the architecture they were designed for (Osterrieder and Kulkarni, 2021). [20] The push for explainability is not only a technical requirement but also a legal and ethical imperative. The European Union, through its AI Act, mandates clear guidelines for the development and deployment of AI, ensuring that systems are understandable and accountable (European Commission, 2020). Frasca et al. (2024) discuss the inherent trade-offs involving balancing the complexity of models with the need for explainability, which often requires substantial computational resources and must align with user intuitions.

In integrating these aspects, XAI stands as a fundamental pillar in the responsible deployment of AI technologies, ensuring that as AI systems become more prevalent, they remain comprehensible, accountable, and beneficial to all users.

B. Risk management and artificial intelligence

The integration of Artificial Intelligence (AI) across various sectors has prompted significant regulatory attention globally. In 2020, the European Commission established the High-Level Expert Group on AI (HLEG), which has played a crucial role in defining AI and setting ethical standards for its development and deployment. According to Reddy et al. (2023) [6], HLEG's efforts focus on providing a comprehensive framework for AI, which includes both software and hardware components that collaborate to analyze data and make decisions. These decisions are refined through the evaluation of past actions, using either symbolic rules or numerical models, emphasizing the adaptability and continual learning of AI systems. In the financial sector, AI's ability to predict risks such as bankruptcy is transformative, enhancing decision-making and profitability. Research by Zhang et al. (2022) demonstrates how AI contributes to more effective risk management, providing financial institutions with a competitive edge and improved customer service. Furthermore, Damiani (2021) [21] provides a multidimensional overview of recent AI research within the financial realm, highlighting its significant impact. [13]

However, the deployment of AI in finance is not without challenges. Koster and Visser (2021), identify several hurdles, including issues related to accuracy, consistency, transparency, and trust. [22] These challenges are compounded by ethical considerations, legal regulations, and the complexities of machine learning design and integration, which must be navigated carefully to fully leverage AI's capabilities.

To address complex financial tasks, researchers employ a “multi-approach AI technique,” which utilizes various AI methods to enhance model efficiency. This approach is supported by the work of Dastile et al. (2021), who explore different machine learning techniques to optimize the performance of financial models. [23] SHAP values, derived from cooperative game theory, distribute the influence of each feature on the model's prediction. In financial decision-making, they provide insights into how individual variables affect specific outcomes. By assigning a Shapley value to each feature, their relative impact on the model's decision-making process can be quantified, improving transparency. SHAP values present a holistic perspective on feature significance, accounting for complex interactions among variables. [24]

Moreover, the necessity for improved explainability in AI systems is becoming increasingly important as their use in decision-making processes expands. The Royal Society (2019) stresses the importance of understanding AI to mitigate bias and ensure compliance with policies. Doran (2017) argues that better explainability can enhance user confidence in AI outputs. [26] Similarly, Arrieta et al. (2020) contend that interpretability is essential for ensuring fairness, reliability, and truthfulness in AI decisions. Explainable AI (XAI) strives to develop models that are both understandable and efficient, facilitating a greater level of trust and control over AI systems. [16]

The integration of AI in risk management is marked by its potential to improve decision-making and operational efficiency. Nonetheless, it requires careful management of ethical, legal, and technical challenges to ensure that AI technologies are used responsibly and effectively. The work by regulatory bodies like HLEG and ongoing research in XAI are pivotal in shaping the future of AI in risk management, aiming to create a balanced approach where innovation is coupled with stringent standards of transparency and ethics.

IV. ABOUT DATA

The dataset provided by Home Credit Bank forms the empirical basis for a study focused on the application of Explainable Artificial Intelligence (XAI) in financial risk management. This dataset is comprehensive, encompassing both personal and financial details about borrowers, including their credit

history at Home Credit and other financial institutions. The principal dataset, ‘application train’, along with related datasets such as ‘bureau’ and ‘bureau balance’, provides a nuanced understanding of the financial behaviors of clients, crucial for assessing credit risk. A key aspect of the research involves deploying XAI methods like SHAP (Shapley Additive explanations) and LIME (Local Interpretable Model-agnostic Explanations) to enhance transparency and understanding in AI-driven decision-making processes within the financial sector. The ‘TARGET’ variable in ‘application_train’, indicating whether a loan was repaid or defaulted, is pivotal for training predictive models. It serves as a basis for evaluating and interpreting the influence of various borrower attributes on the likelihood of default. Furthermore, the integration of data regarding prior loan applications, monthly loan balances, and payment histories enables a detailed analysis of borrowers past behaviors.

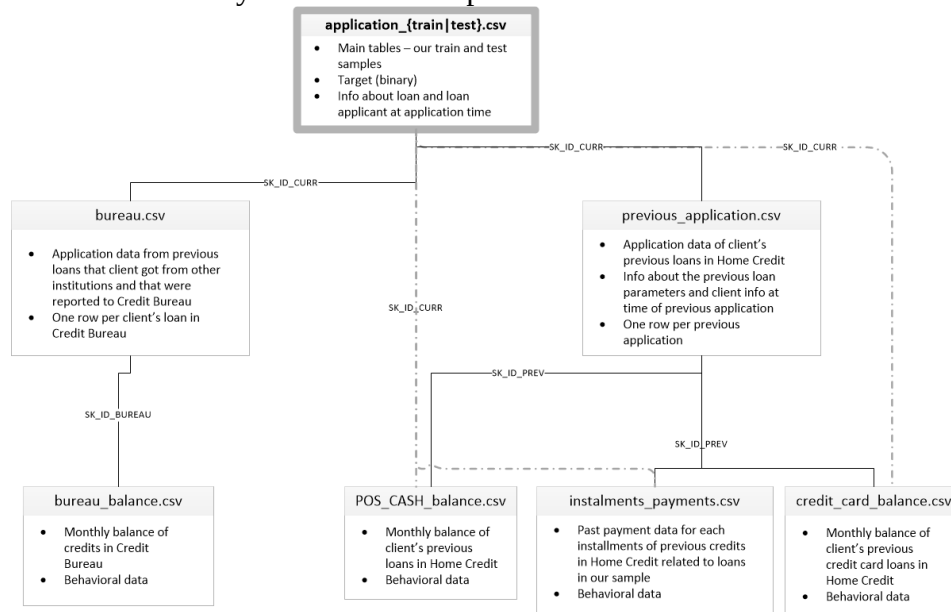


Fig. 2. Home Credit Bank Dataset Diagram(Montoya, 2018)

This facilitates the development of precise and interpretable models for credit risk assessment. Thus, the datasets provided by Home Credit are instrumental in demonstrating the efficacy of XAI techniques in managing real-world financial risks. [27]

A. Data preparation

Integrating data from various tables is a critically important task in creating a credit scoring system. Correct merging of tables is crucial as errors at this stage can lead to the loss of significant information, negatively impacting the future efficiency of models. One of the main problems arising when merging tables is the increase in data dimensionality. For example, just the main ‘application_train’ table contains 121 attributes, excluding the target. When all available data is combined, the number of attributes can significantly increase.

During training, the model autonomously determines the features that are important to it, which can solve the problem of excessive dimensionality. After completing data integration, we found that the number of features reached 538. Part of the data processing involved removing unnecessary attributes, such as the ‘SK_ID_CURR’ column, which lost its significance as the primary key in the original database. During data analysis, various anomalies were identified, arising from technical errors or human factors, including features like ‘COD_GENDER’, ‘ORGANIZATION_TYPE’, ‘DAYS_EMPLOYED’, ‘AMT_INCOME_TOTAL’, and ‘DAYS_LAST_PHONE_CHANGE’. Some of these anomalies were obvious technical errors, while others were statistically impossible outliers.

One of the serious issues was the large number of missing values. A strategy of maximizing data preservation was adopted to address this, deciding to remove columns where the proportion of missing

values exceeded 10%. As a result of this approach, 477 out of 538 attributes were excluded, allowing the retention of the maximum amount of information. This method was not applied to all models since some can effectively handle missing data. During the merging of tables, a set of attributes was created that represented the sum of all rows, which sometimes led to the emergence of extremely large numbers. The appearance of infinite values became a problem, as machine learning algorithms cannot work with them. Consequently, it was decided to remove all columns containing such values.

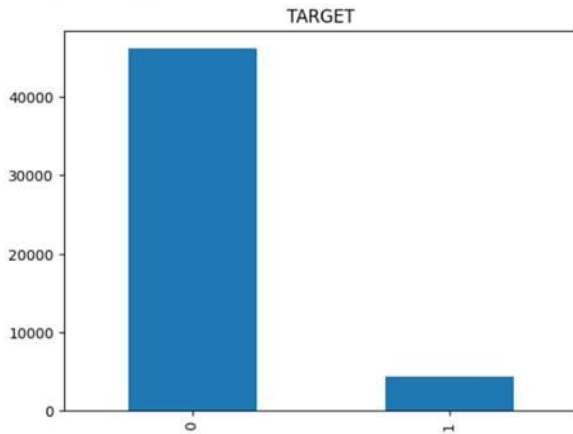
This comprehensive approach to data processing and integration enables the creation of a reliable and efficient credit scoring system, enhancing the accuracy and reliability of models. Upon completing the data processing, the division into training and testing samples emerges as a critical subsequent step in data preparation. This division is vital to maintain the reliability of model testing results. Additionally, reducing the number of rows in the training sample might lessen model efficiency, but it enables the identification of potential training issues, such as imbalances or overfitting within the training set.

Handling categorical variables effectively is imperative, as most machine learning models require converting these variables into numerical formats through a process known as encoding. The effectiveness of many algorithms hinges on the method of encoding applied. Encoding transforms categorical features into numerical formats that models can process during training. Two prevalent methods—Label encoding and OneHot encoding—are typically employed.

Label encoding assigns a unique integer to each category value, starting from zero and ordered alphabetically. This basic yet essential method allows machine learning algorithms to operate with categorical data, which are inherently non-numeric.

On the other hand, One-Hot encoding creates new features for each unique category value, each acting as a binary indicator. While this method provides a clearer representation of categorical variables, it can significantly expand the data's dimensionality. A key benefit of One-Hot encoding is its ability to accommodate missing categorical values by treating them as a distinct category, thus preserving critical information about the borrower. Label encoding is applied to categories with only two unique values, whereas One-Hot encoding is used when more diversity exists, resulting in 92 additional columns. Regarding models that are incompatible with missing data, previously we addressed columns where the missing value proportion exceeded 10%.

Test nocne resampling(не изменился)
 Number without TARGET: 46067
 Number with TARGET: 4360
 Number of sum TARGET: 50427
 Proportion: 10.57 : 1
 Percent: 91.4% : 8.6%



Train nocne resampling
 Number without TARGET: 17474
 Number with TARGET: 17474
 Number of sum TARGET: 34948
 Proportion: 1.0 : 1
 Percent: 50.0% : 50.0%

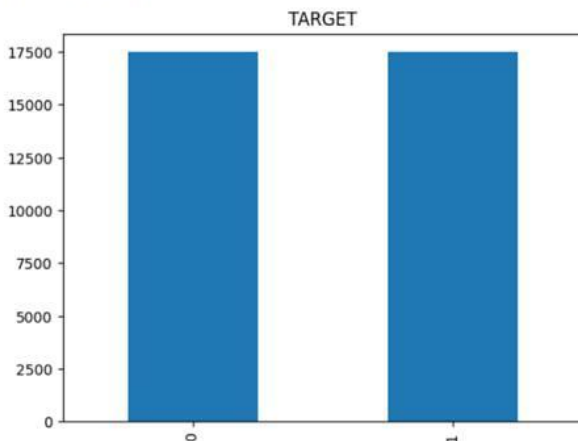


Fig. 3. Train before sampling

Fig. 4. Train after sampling

However, this did not fully resolve the missing data issue as columns with less than 10% missing values remained. To conserve as much valuable data as possible, these were treated using specialized imputation techniques. Imputation replaces erroneous, inconsistent, or missing entries with synthetically generated values. The SimpleImputer method, which fills in missing values with a calculated statistic such as the mean, median, mode, or a constant, was employed for this purpose. If imputation was not utilized, rows with any missing values were omitted, resulting in the loss of 14,198 records from the training sample of 201,705 and 3,609 from the test sample of 50,427.

Data imbalance is an inherent characteristic that can introduce several challenges. In classification tasks, a dataset with disproportionate class distributions is considered unbalanced. Such imbalance is evident in various fields like credit scoring, healthcare, and direct marketing, and is typically the norm in extensive datasets. The histograms from our training and test samples indicate a significant imbalance. This imbalance could undermine model training and lead to misjudged performance evaluations if an inappropriate metric is used. Many sophisticated machine learning approaches, however, effectively handle imbalanced data given sufficient input. The technique of adjusting data to correct this imbalance is known as resampling, which in our thesis project was selectively applied to certain models only within

the training dataset to maintain the integrity and accuracy of the model outcomes. Techniques such as Random Under Sampler and SMOTE from the imblearn library were used for resampling.

Random Under Sampler equalizes class distributions by randomly eliminating majority class instances to match the minority class level. SMOTE, or Synthetic Minority Oversampling Technique, augments the dataset by generating synthetic examples rather than duplicating existing minority class instances. This method samples the attribute space of each target class and its nearest neighbors, crafting new instances that blend the features of the target with those of its neighbors, thereby enriching the dataset's diversity without altering the majority class's size.

V. METHODOLOGY

The escalating complexity and volume of financial data challenge traditional risk management practices, necessitating the adoption of advanced machine learning models that can parse through and make sense of this data effectively. However, the opacity of these advanced models often results in a 'black box' dilemma, where the reasoning behind predictions is obscured, thus complicating compliance and ethical governance in financial operations. This research integrates Explainable Artificial Intelligence (XAI) techniques with conventional machine learning approaches to demystify the decision-making processes in credit default predictions. By doing so, the study not only aims to elevate the predictive performance of these models but also strives to peel back layers of complexity to reveal the underlying decision drivers. This dual focus aligns with emerging regulatory frameworks which demand not only accuracy but also accountability and transparency in automated financial assessments. The chosen methodologies are meticulously designed to bridge the gap between high-level accuracy and deep-level interpretability, fostering trust and clarity in financial risk assessments.

A. Comprehensive Analysis of Default Risk Prediction Using Machine Learning Models

To combat the skewed class distribution, we employed the Synthetic Minority Over-sampling Technique (SMOTE), which enhanced the minority class representation by generating synthetic samples. For a structured analysis, the dataset was split into training and testing subsets, maintaining an 80%-20% division. This stratification ensures that both subsets are representative of the overall data distribution. The models were trained on this balanced dataset, with the process facilitated by the train test split function from the sklearn library, which guarantees a randomized yet stratified splitting of the data.

The classification reports generated for each model provide a detailed breakdown of precision, recall, and F1-scores, which are crucial for understanding the models' performance across different aspects of the data. Application of Explainable AI (XAI) The XGBoost model, which exhibited superior performance as evidenced by the highest ROC-AUC score, was further analyzed using SHAP (SHapley Additive exPlanations) values. This XAI technique elucidates the contribution of each feature to the model's predictions, offering both global and individual prediction insights. The SHAP summary plot reveals significant features impacting model outputs, emphasizing their roles in predictive accuracy. Among the most influential features, INS_AMT_DIFF_MAX (maximum insurance amount difference) and APPS_GOODS_CREDIT_RATIO (ratio of goods price to credit amount) had the highest absolute SHAP values, indicating their strong impact on the model's decision-making process.”

For instance, INS_AMT_DIFF_MAX had an average SHAP value of +0.075, meaning that an increase in this feature was associated with a higher probability of default. Conversely, APPS_GOODS_CREDIT_RATIO showed an average SHAP value of -0.062, suggesting that lower values of this ratio contributed to a reduced risk of default. Additionally, NAME_INCOME_TYPE_Working, while not among the top-ranked features, exhibited an average SHAP value of +0.032, indicating a slight positive influence on default probability when the applicant's income type was classified as 'Working'.

VI. Discussion of Results

The analysis of SHAP values indicates that features such as INS_AMT_DIFF_MAX and APPS_GOODS_CREDIT_RATIO are paramount in influencing the model's decision-making process. Such insights are instrumental for financial institutions to refine their risk assessment frameworks and ensure robust credit lending practices.

The detailed results, including model accuracy and feature importance graphs, will be included in the appendices of this thesis, providing a comprehensive resource for understanding the intricate dynamics of credit default risk modeling. INS_AMT_DIFF_MAX: This feature, indicating the maximum difference in insurance amounts, shows a high positive impact, suggesting that larger differences are associated with an increased risk of default.

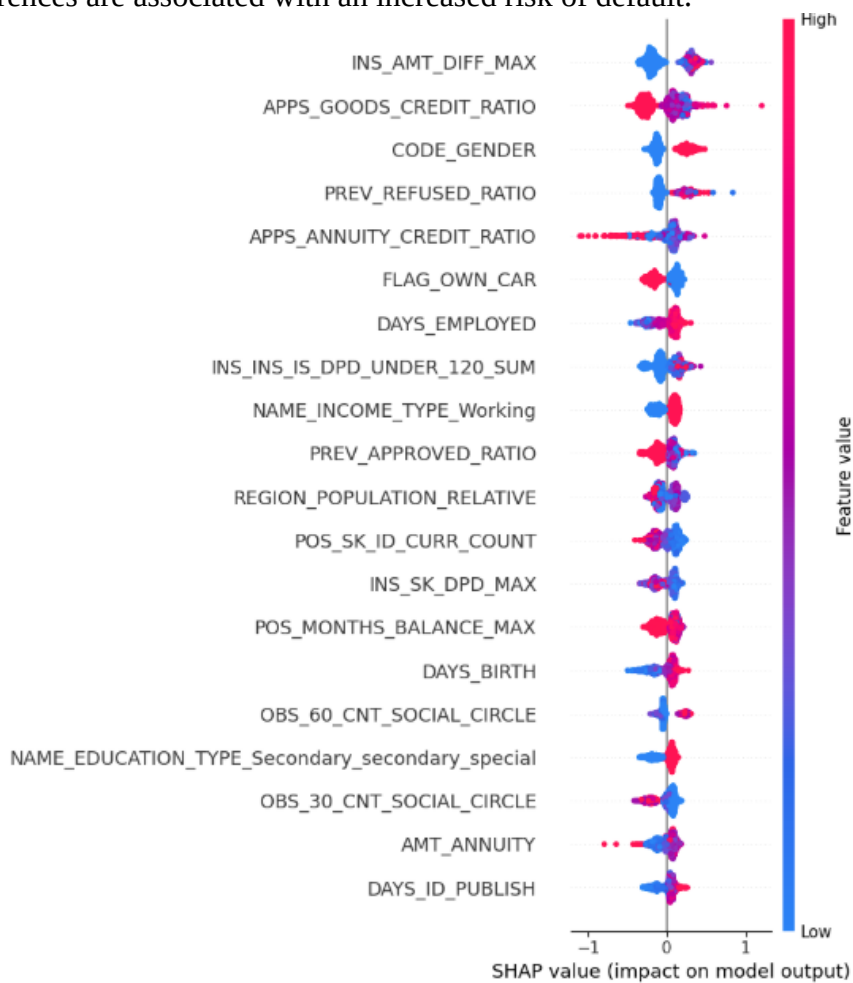


Fig. 6. SHAP Value

APPS_GOODS_CREDIT_RATIO: This ratio of goods price to credit amount also appears to significantly influence predictions, where higher ratios may indicate higher financial leverage and hence a higher risk. APPS_GOODS_CREDIT_RATIO: This ratio of goods price to credit amount also appears to significantly influence predictions, where higher ratios may indicate higher financial leverage and hence a higher risk. DAYS_EMPLOYED: Longer employment duration appears to have a protective effect against default, as demonstrated by its negative impact on the SHAP value scale. Specifically, observations with employment durations exceeding 10 years had an average SHAP contribution of -

0.045, meaning that longer job tenure consistently decreased the predicted probability of default. For example, individuals with 5 years of employment had SHAP values around -0.02, while those with 15+ years exhibited SHAP values closer to -0.06. This confirms that stable employment history plays a crucial role in reducing financial risk, aligning with economic theories on job security and repayment stability. AMT_ANNUITY: Lower annuity amounts are associated with lower risk, which is intuitive as smaller regular payments are likely easier to manage for borrowers. CODE_GENDER and NAME_INCOME_TYPE_Working: These features indicate demographic influences where gender and employment type contribute to the risk assessment model. Their positions on the plot suggest nuanced effects on the default predictions. PREV_REFUSED_RATIO: A history of previous loan refusals has a notable positive impact on default predictions, implying that past loan rejections are predictive of future credit behavior.

Three machine learning models were developed and evaluated: Logistic Regression, Random Forest, and XGBoost. These models were trained on both the original imbalanced dataset and the balanced datasets (SMOTE and RandomUnderSampler). The models were optimized with specific hyperparameters, such as max iter=1000 for Logistic Regression, n estimators=50 and max depth=10 for Random Forest, and n estimators=50 and max depth=6 for XGBoost, ensuring computational efficiency and stability.

Model performance was assessed using several metrics, including Receiver Operating Characteristic - Area Under Curve (ROC-AUC), accuracy, precision, recall, F1score, and support, as detailed in Table 1. The ROC-AUC score, a robust metric for imbalanced datasets, was prioritized to evaluate the models' ability to discriminate between classes. Classification reports provided a comprehensive overview of precision, recall, and F1-score for both classes, while accuracy offered a general measure of overall correctness.

TABLE 1 PERFORMANCE METRICS FOR MACHINE LEARNING MODELS IN CREDIT RISK PREDICTION

Model	Measure	Class 0	Class 1	Macro Avg	W Avg
Logistic Regression	Precision	0.95	0.16	0.55	0.88
	Recall	0.67	0.64	0.66	0.67
	F1-score	0.78	0.25	0.52	0.74
	Support	42788	4097	46885	46885
Random Forest	Precision	0.92	0.2	0.56	0.86
	Recall	0.92	0.22	0.57	0.86
	F1-score	0.92	0.21	0.57	0.86
	Support	42788	4097	46885	46885
XGBoost	Precision	0.91	0.45	0.68	0.87
	Recall	1.00	0.01	0.51	0.91
	F1-score	0.95	0.02	0.49	0.87
	Support	42788	4097	46885	46885

Note: Class 0 = Non-default, Class 1 = Default. Support indicates the number of samples in each class in the test set.

The results indicate that XGBoost achieved the highest ROC-AUC score (0.722) and accuracy (0.912) after SMOTE balancing, outperforming Logistic Regression and Random Forest. This suggests that XGBoost, with its ensemble-based approach and handling of complex interactions, is particularly effective for this task. However, the impact of class balancing was further investigated by comparing ROC-AUC scores before and after SMOTE. Without balancing, Logistic Regression yielded a ROC-AUC of 0.723565, while after SMOTE, it decreased to 0.714166. This decline highlights the trade-off

between balancing class distribution and maintaining discriminative power, a critical consideration in financial risk modeling.

To further refine the classification threshold, precision-recall curves and F1-score optimization were employed. The optimal threshold for XGBoost was determined to be approximately 0.5, improving the F1-score for the minority class (Default) while maintaining reasonable performance for the majority class (non-default).

VI. FUTURE WORK

As this study pushes forward the understanding and application of machine learning in credit risk prediction with an emphasis on transparency through explainable AI (XAI), the following paths are outlined for future exploration: Integration of Broader XAI Techniques: While SHAP has been pivotal in understanding feature impact, additional techniques like LIME (Local Interpretable Model-agnostic Explanations) and counterfactual explanations could be employed. These methods would provide deeper local insights and individual prediction explanations, enhancing trust and clarity for end-users.

Exploring Deep Learning Models: Incorporating deep learning could potentially unveil complex patterns not detectable by the models used in this study. However, the challenge remains to maintain interpretability with these complex models, which can be addressed by employing advanced XAI tools designed for deep learning architecture.

Expansion to Diverse Datasets: Applying the developed models to datasets from various geographical regions or different types of lending would test the robustness and adaptability of the models across diverse economic and demographic contexts. Real-time Risk Monitoring: Developing a system for real-time monitoring of credit risk using streaming data would allow continuous model adjustments based on dynamic economic conditions and borrower behavior, significantly enhancing predictive accuracy.

Addressing Regulatory and Ethical Concerns: Ongoing research should also consider the regulatory compliance and ethical dimensions, ensuring that the AI systems in credit risk management adhere to legal standards and ethical norms to prevent discriminatory practices.

VII. CONCLUSION

This research has significantly contributed to the field of financial risk management by integrating machine learning models with explainable AI techniques to improve the predictability and transparency of credit default risks. The use of logistic regression, random forest, and XGBoost, along with SMOTE for class balancing and SHAP for interpretability, has underscored the potential of AI to enhance decision-making in financial contexts.

The incorporation of SHAP and LIME has opened avenues for lenders to gain detailed insights into the decision-making processes of AI models, ensuring that credit risk assessments are both accurate and understandable. These models have proven vital in highlighting key factors-such as financial stability and borrowing history-that significantly impact default predictions.

The broader impact of this research is its potential to revolutionize credit risk assessment practices within financial institutions. By enhancing model accuracy and interpretability, financial entities can not only mitigate risks effectively but also ensure fairness in lending practices, thereby supporting more equitable financial services.

Future initiatives will aim to expand these methodologies, exploring more sophisticated AI models and incorporating real-time data to keep pace with the rapidly evolving financial landscape. This progression will continue to enhance the capabilities of financial institutions in risk management, paving the way for more innovative, reliable, and fair credit assessment practices. [29]

REFERENCES

- [1] T. T. Do, G. Babaei, and P. Pagnottoni, “Explainable machine learning for credit risk management when features are dependent,” *Measurement: Interdisciplinary Research and Perspectives*, pp. 1–26, 2024. [Online]. Available: <https://doi.org/10.1080/15366367.2023.2261186>
- [2] A. Saranya and R. Subhashini, “A systematic review of explainable artificial intelligence models and applications: Recent developments and future trends,” *Decision Analytics Journal*, vol. 7, p. Article ID 100230, 2023. [Online]. Available: <https://doi.org/10.1016/j.dajour.2023.100230>
- [3] J. Cohen, X. Huan, and J. Ni, “Shapley-based explainable ai for clustering applications in fault diagnosis and prognosis,” *arXiv preprint arXiv:2303.14581*, 2023. [Online]. Available: <https://doi.org/10.48550/arXiv.2303.14581>
- [4] P. Weber, K. V. Carl, and O. Hinz, “Applications of explainable artificial intelligence in finance—a systematic review of finance, information systems, and computer science literature,” *Management Review Quarterly*, 2023. [Online]. Available: <https://doi.org/10.1007/s11301-023-00320-0>
- [5] S. Ali, T. Abuhmed, S. El-Sappagh, K. Muhammad, J. M. Alonso-Moral, R. Confalonieri, and F. Herrera, “Explainable artificial intelligence (xai): What we know and what is left to attain trustworthy artificial intelligence,” *Information Fusion*, vol. 99, p. 101805, 2023.
- [6] G. P. Reddy and Y. V. P. Kumar, “Explainable ai (xai): Explained,” in *2023 IEEE Open Conference of Electrical, Electronic and Information Sciences, EStream 2023 - Proceedings*, 2023.
- [7] R. Pranav and H. S. Gururaja, *Explainable Stacking Machine Learning Ensemble for Predicting Airline Customer Satisfaction*, 2023, vol. 608.
- [8] T. Clement, N. Kemmerzell, M. Abdelaal, and M. Amberg, “Xair: A systematic metareview of explainable ai (xai) aligned to the software development process,” *Machine Learning and Knowledge Extraction*, vol. 5, pp. 78–108, 2023.
- [9] S. Ghaffarian, F. R. Taghikhah, and H. R. Maier, “Explainable artificial intelligence in disaster risk management: Achievements and prospective futures,” *International Journal of Disaster Risk Reduction*, vol. 98, p. 104123, 2023. [Online]. Available: <https://doi.org/10.1016/j.ijdrr.2023.104123>
- [10] P. Giudici, M. Centurelli, and S. Turchetta, “Artificial intelligence risk measurement,” *Expert Systems with Applications*, vol. 235, p. 121220, 2024. [Online]. Available: <https://doi.org/10.1016/j.eswa.2023.121220>
- [11] P. Giudici and E. Raffinetti, “Shapley-lorenz explainable artificial intelligence,” *Expert Systems with Applications*, vol. 167, p. Article ID 114104, 2021. [Online]. Available: <https://doi.org/10.1016/j.eswa.2020.114104>
- [12] S. R. Islam, W. Eberle, and S. K. Ghafoor, “Towards quantification of explainability in explainable artificial intelligence methods,” in *Proceedings of the 33rd International Florida Artificial Intelligence Research Society Conference, FLAIRS 2020*, 2020.
- [13] Z. Zhang, C. Wu, S. Qu, and X. Chen, “An explainable artificial intelligence approach for financial distress prediction,” *Information Processing & Management*, vol. 59, p. 102988, 2022.
- [14] A. Nor, S. Pedapati, M. Muhammad, and V. Leiva, “Overview of explainable artificial intelligence for prognostic and health management of industrial assets based on preferred reporting items for systematic reviews and meta-analyses,” *Sensors*, vol. 21, p. 8020, 2021.
- [15] A. Adadi and M. Berrada, “Peeking inside the black-box: a survey on explainable artificial intelligence (xai),” *IEEE Access*, vol. 6, pp. 52 138–52 160, 2018. [Online]. Available: <https://doi.org/10.1109/ACCESS.2018.2870052>
- [16] A. Barredo Arrieta, N. D’iaz-Rodríguez, J. Del Ser, A. Bennetot, S. Tabik, A. Barbado, S. Garcia, S. Gil-Lopez, D. Molina, R. Benjamins, R. Chatila, and F. Herrera, “Explainable artificial intelligence (xai): Concepts, taxonomies, opportunities and challenges toward responsible ai,”

Information Fusion, vol. 58, pp. 82–115, Jun. 2020. [Online]. Available:

<https://doi.org/10.1016/j.inffus.2019.12.012>

[17] W. Guo, “Explainable artificial intelligence for 6g: Improving trust between human and machine,” *IEEE Communications Magazine*, vol. 58, no. 6, pp. 39–45, Jun. 2020. [Online]. Available: <https://doi.org/10.1109/MCOM.001.2000050>

[18] G. Yang, Q. Ye, and J. Xia, “Unbox the black-box for the medical explainable ai via multi-modal and multi-centre data fusion: A minireview, two showcases and beyond,” *Information Fusion*, vol. 77, pp. 29–52, 2022.

[19] P. Biecek, M. Chlebus, J. Gajda, A. Gosiewska, A. Kozak, D. Ogonowski, J. Sztachelski, and P. Wojewnik, “Enabling machine learning algorithms for credit scoring—explainable artificial intelligence (xai) methods for clear understanding complex predictive models,” *arXiv preprint arXiv:2104.06735*, 2021. [Online]. Available: <https://doi.org/10.48550/arXiv.2104.06735>

[20] B. Hadji Misheva, A. Hirsu, J. Osterrieder, O. Kulkarni, and S. Fung Lin, “Explainable ai in credit risk management,” *SSRN Electronic Journal*, 2021.

[21] Z. Zhang, H. Al Hamadi, E. Damiani, C. Yeun, and F. Taher, “Explainable artificial intelligence applications in cyber security: State-of-the-art in research,” *IEEE Access*, vol. 10, pp. 93 104–93 139, 2022.

[22] O. Koster, R. Kosman, and J. Visser, “A checklist for explainable ai in the insurance domain,” *arXiv*, 2021.

[23] X. Dastile and T. Celik, “Making deep learning-based predictions for credit scoring explainable,” *IEEE Access*, vol. 9, pp. 50 426–50 440, 2021. [Online]. Available: <https://doi.org/10.1109/ACCESS.2021.3068854>

[24] M. Sahakyan, Z. Aung, and T. Rahwan, “Explainable artificial intelligence for tabular data: A survey,” *IEEE Access*, vol. 9, pp. 135 392–135 422, 2021.

[25] N. Rane, S. Choudhary, and J. Rane, “Explainable artificial intelligence (xai) approaches for transparency and accountability in financial decision-making,” *SSRN Electronic Journal*, 2023.

[26] D. Doran, S. Schulz, and T. R. Besold, “What does explainable ai really mean? a new conceptualization of perspectives,” *arXiv preprint arXiv:1710.00794*, 2017. [Online]. Available: <https://doi.org/10.48550/arXiv.1710.00794>

[27] A. Montoya, K. Odintsov, and M. Kotek, “Home credit default risk,” *Kaggle Competition*, 2018. [Online]. Available: <https://kaggle.com/competitions/home-credit-default-risk>

[28] M.-A. Clinciu and H. Hastie, “A survey of explainable ai terminology,” in *Proceedings of the 1st Workshop on Interactive Natural Language Technology for Explainable Artificial Intelligence (NLXAI)*, 2019, pp. 8–13. [Online]. Available: <https://doi.org/10.18653/v1/W19-8403>

[29] N. Bussmann, P. Giudici, D. Marinelli, and J. Papenbrock, “Explainable ai in fintech risk management,” *Frontiers in Artificial Intelligence*, vol. 3, p. 26, 2020. [Online]. Available: <https://www.frontiersin.org/journals/artificialintelligence/articles/10.3389/frai.2020.00026/full>

UDC 532.546

Kenzhebek Y. (Almaty, Al-Farabi Kazakh National University)
 Bekele S.D. (Almaty, Al-Farabi Kazakh National University)
 Imankulov T. (Almaty, Al-Farabi Kazakh National University)

PREDICTION OF TWO-PHASE FLOW IN POROUS MEDIA USING PHYSICS-INFORMED NEURAL NETWORKS

Physics-Informed Neural Networks (PINNs) are a class of deep learning models that incorporate governing physical laws into the neural network training process [1]. Rather than relying solely on data, PINNs embed partial differential equations (PDEs), boundary conditions, and initial conditions directly into the loss function using automatic differentiation [2]. This allows PINNs to learn physically consistent solutions, even in the absence of large training datasets or mesh-based discretization [3]. Previous studies have shown that applying PINNs to nonlinear transport problems in porous media such as the saturation equation with sharp fronts can be challenging due to issues like convergence instability and shock resolution [4, 5].

We consider one-dimensional two-phase immiscible flow in porous media, governed by coupled system of PDEs for water saturation $S_w(x, t)$ and pressure $p(x, t)$. The equations are as follows:

Water Saturation Equation (hyperbolic form):

$$\frac{\partial S_w}{\partial t} + \frac{\partial}{\partial x} \left(-k \frac{k_{rw}(S_w)}{\mu_w} \frac{\partial p}{\partial x} \right) = 0$$

Pressure Equation (elliptic form):

$$\frac{\partial}{\partial x} \left[-k \left(\frac{k_{rw}(S_w)}{\mu_w} + \frac{k_{ro}(1 - S_w)}{\mu_o} \right) \frac{\partial p}{\partial x} \right] = 0$$

Here, k is the absolute permeability, μ_w, μ_o are the viscosities of water and oil, and k_{rw}, k_{ro} are the relative permeability functions dependent on saturation.

To solve the coupled system, we employ a single feedforward neural network with two outputs: pressure $p(x, t)$ and saturation $S_w(x, t)$. The input to the network is the space–time coordinate (x, t) , and the outputs are trained simultaneously to minimize a composite loss function:

$$L = \lambda_{data} L_{BC/IC} + \lambda_{pde} (L_{sat} + L_{pres})$$

where:

$L_{BC/IC}$: loss of boundary and initial conditions;

L_{sat} : residual of the saturation equation;

L_{pres} : residual of the pressure equation.

Automatic differentiation is used to compute all derivatives. The network was trained using the Adam optimizer followed by L-BFGS for convergence refinement. Training was performed with randomly sampled collocation points in the domain using latin hypercube sampling (LHS). To improve convergence and optimization, an artificial diffusion term was added to the saturation equation. This modification serves as a numerical regularization mechanism, helping the PINN handle the sharp gradients and shock fronts commonly present in saturation profiles.

We evaluated the performance of the PINN model on test cases involving sharp saturation fronts and pressure. Figure 1 shows the predicted saturation and pressure profiles at different times, compared to the reference numerical solution, along with the L2 relative error for both fields.

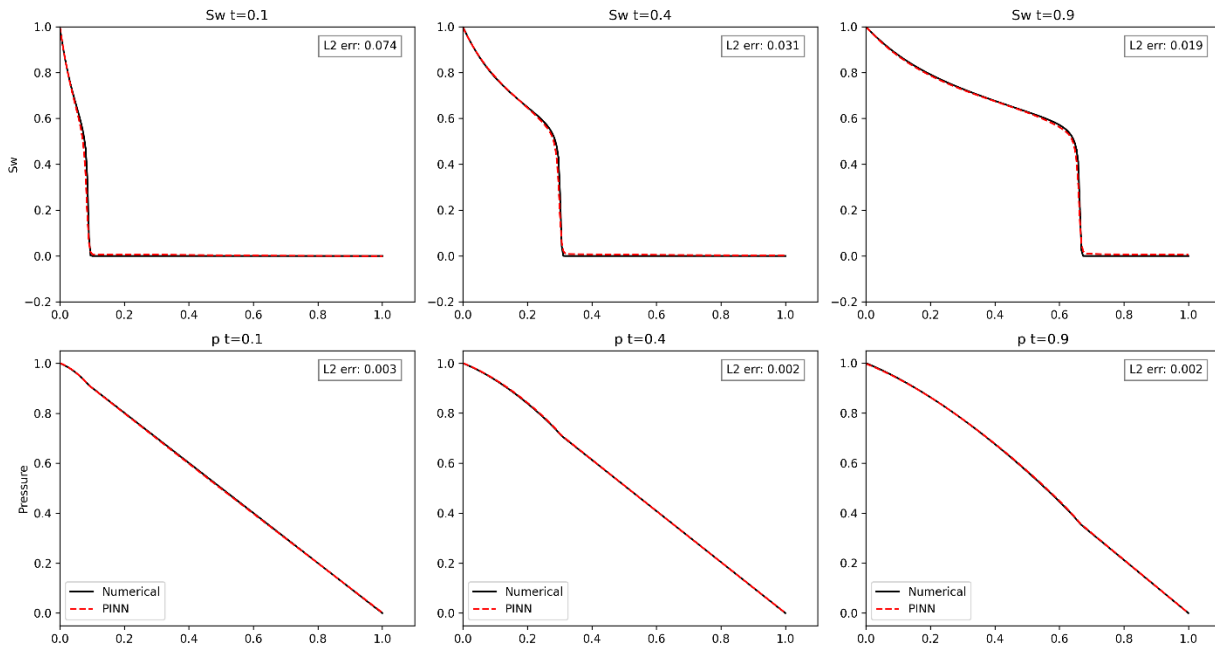


Figure 1 – Predicted saturation and pressure profiles at different times compared to numerical solution

This study demonstrates the feasibility of using PINNs to solve coupled pressure-saturation equations for two-phase flow in porous media. By embedding the governing physical laws directly into the training process, PINNs are able to accurately predict both pressure and saturation profiles, even in the presence of sharp fronts and complex nonlinear interactions. The results showed that the PINN model successfully captured the dynamic evolution of saturation and pressure profiles, with L2 relative errors remaining small and within acceptable bounds compared to reference numerical solutions. The flexibility of PINNs, combined with their ability to handle nonlinear, multiphase flow problems, makes them a valuable tool for forward and inverse modeling, parameter estimation, and real-time control in reservoir engineering and related fields.

References

- [1] Raissi, M., Perdikaris, P., Karniadakis, G.E., 2019. Physics-informed neural networks: A deep learning framework for solving forward and inverse problems involving nonlinear partial differential equations. *J. Comput. Phys.* 378, 686–707. <https://doi.org/10.1016/j.jcp.2018.10.045>
- [2] Baydin, A.G., Pearlmutter, B.A., Radul, A.A., Siskind, J.M., 2018. Automatic differentiation in machine learning: a survey. <https://doi.org/10.48550/arXiv.1502.05767>
- [3] Karniadakis, G., Kevrekidis, Y., Lu, L., Perdikaris, P., Wang, S., Yang, L., 2021. Physics-informed machine learning. *Nat. Rev. Phys.* 1–19. <https://doi.org/10.1038/s42254-021-00314-5>
- [4] Fraces, C.G., Papaioannou, A., Tchelepi, H., 2020. Physics Informed Deep Learning for Transport in Porous Media. *Buckley Leverett Problem*. <https://doi.org/10.48550/arXiv.2001.05172>

[5] Fuks, O., Tchelepi, H., 2020. LIMITATIONS OF PHYSICS INFORMED MACHINE LEARNING FOR NONLINEAR TWO-PHASE TRANSPORT IN POROUS MEDIA. *J. Mach. Learn. Model. Comput.* 1, 19–37. <https://doi.org/10.1615/JMachLearnModelComput.2020033905>

UDC 004.896

Kuatbayeva A.A., Alibi J.
Gizatov A., Zhaksybayev N. (Astana IT university)

PREDICTIVE MODELS FOR ANALYZING AND FORECASTING LABOR MARKET TRENDS IN KAZAKHSTAN: ADDRESSING MARKET SATURATION AND ENSURING ECONOMIC STABILITY

Abstract:

Kazakhstan’s surge to 112 000 higher-education grants in 2024 has flooded key sectors—economics, IT and law—with graduates, driving market saturation and wage stagnation. We propose a hybrid CatBoost–Lasso–LSTM framework (with Bayesian tuning) that forecasts income trends and flags at-risk fields through 2030, enabling data-driven alignment of educational capacity with real labor-market needs.

Introduction

Kazakhstan’s higher-education grants grew 15 % in 2024 to 112 000 awards, fueling a graduate surplus in IT, economics and law that leaves just 67 % in permanent roles and caps entry wages at ~118 000 KZT. To remedy this mismatch, we propose a hybrid CatBoost–Lasso–LSTM framework with Bayesian tuning, delivering robust labor-market and wage forecasts through 2030 to guide adaptive educational planning.

Methodology

Data Acquisition and Description.

Data were sourced from the Bureau of National Statistics of Kazakhstan’s annual “Wage Structure Report” (Form 2-T) covering 2018–2024. The raw dataset comprises approximately 2.6 million records and 11 core variables, including demographic attributes (age, region), educational attainment, employment modality (full-time/part-time), sector classification, and wage fund allocations [2].

Data Preprocessing and Anonymization

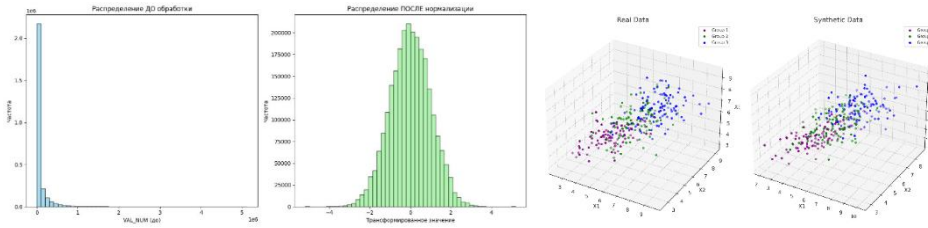
To protect individual confidentiality while retaining joint distribution characteristics, we applied a Gaussian Copula–based synthesizer. This approach models the empirical copula.

$$C(u_1, u_2, \dots, u_d) = \Phi_{\Sigma}^{-1}(\Phi^{-1}(u_1), \Phi^{-1}(u_2), \dots, \Phi^{-1}(u_d))$$

and generates synthetic samples that mirror multivariate dependencies without exposing real records [4].

After anonymization, we applied **Box–Cox to income and Yeo–Johnson plus quantile transformations** to all other features, thereby stabilizing variance and reducing skewness for downstream ML modeling.

$$y' = \frac{y^{\lambda}-1}{\lambda} \text{ для } \lambda \neq 0; y' = \log(y) \text{ для } \lambda = 0; q_i = \frac{\#(y_j \leq y_i)}{n}; y'_i = \text{QuantileInverse}(q_i)$$



Model Development & Hyperparameter Optimization.

CatBoost

$$f(x) = \sum_{m=1}^M \gamma_m T_m(x);$$

LSTM

$$\begin{aligned} f_t &= \sigma(W_f [h_{t-1}, x_t] + b_f), \\ i_t &= \sigma(W_i [h_{t-1}, x_t] + b_i) \\ \tilde{c}_t &= \tanh(W_c [h_{t-1}, x_t] + b_c) \\ o_t &= \sigma(W_o [h_{t-1}, x_t] + b_o) \\ c_t &= f_t \odot c_{t-1} + i_t \odot \tilde{c}_t \\ h_t &= o_t \odot \tanh(c_t) \end{aligned}$$

Lasso

$$\hat{\beta} = \arg \min_{\beta} \left(\sum_{i=1}^n (y_i - X_i \beta)^2 + \lambda \sum_{j=1}^p |\beta_j| \right)$$

LSTM (Bayesian Optimization)

$$\begin{aligned} x^* &= \arg \min_{x \in \mathcal{X}} f(x) \\ \theta^* &= \arg \min_{\theta \in \Theta^*} \mathcal{L}_{LT}(X, y; \theta) \\ \hat{y}_i &= f(x_i, \theta) \\ \theta^* &= \arg \min_{\theta} \sum_{i=1}^n \mathcal{L}(f(x_i, \theta), y_i) \end{aligned}$$

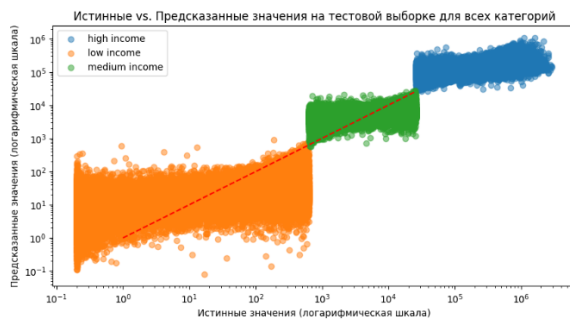
Results

$$MAE = \frac{1}{N} \sum_{i=1}^N (y_i - \hat{y}_i), RMSE = \sqrt{\frac{1}{N} \sum_{i=1}^N (y_i - \hat{y}_i)^2},$$

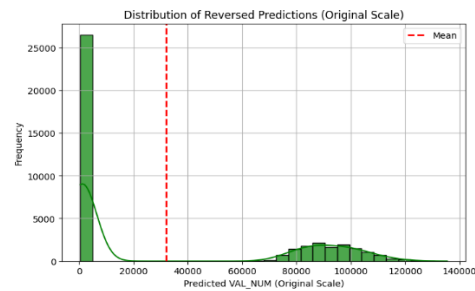
$$MAPE = (100 \% N) \sum_{i=1}^n |(y_i - \hat{y}_i) / y_i|$$

Model	MAE (KZT)	RMSE (KZT)	MAPE
CatBoost (High Income)	128,825.7	219,584.8	2.51 %
CatBoost (Medium Income)	5,681.5	7,589.4	19.2 %
CatBoost (Low Income)	97.7	173.5	12 %
Lasso	4,503.0	6,057.7	7 %
LSTM (No BO)	38,568.9	89,773.7	55.8 %
LSTM (Bayesian Optimization)	36,807.1	84,906.6	52.3 %

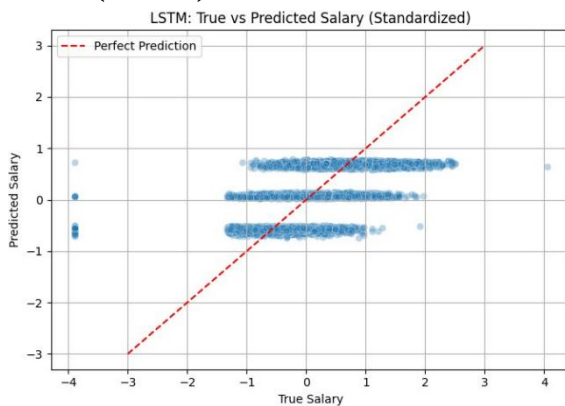
CatBoost



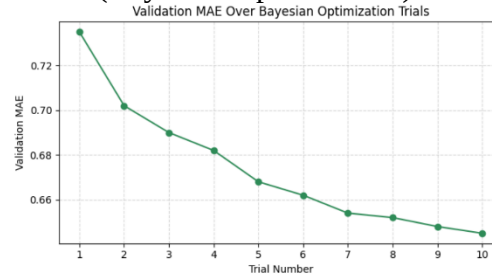
Lasso



LSTM (No BO)



LSTM (Bayesian Optimization)



The CatBoost ensemble delivered the highest accuracy, with low errors across high-, medium-, and low-income segments. Lasso regression offered a competitive, interpretable baseline with moderate error rates. The vanilla LSTM struggled to capture long-term trends, but Bayesian hyperparameter tuning steadily reduced its validation MAE, demonstrating improved—but still lagging—performance relative to tree-based methods.

Conclusion

This study demonstrates that ML-driven forecasts uncover imminent saturation in high-demand sectors—law, economics, IT—highlighting the imperative for dynamic calibration of academic capacity to real-world needs. Bayesian-optimized LSTM models enhanced long-term trend detection, yet continuous refinement through richer data integration and alternative forecasting methods will be essential. Moving forward, policymakers and educational institutions must leverage these insights to strategically align curricula with evolving economic demands, safeguard wage growth, and ensure sustainable workforce development. This scalable framework can also inform labor-market planning across Central Asia.

Literature:

- [1] Ministry of Education and Science of Kazakhstan, “Higher Education Grant Allocation Report,” 2022.
- [2] Bureau of National Statistics of Kazakhstan, “Graduate Employment Survey,” 2021.
- [3] Bureau of National Statistics of Kazakhstan, “Wage Structure Report,” 2021.
- [4] L. Xu et al., “Modeling Multivariate Dependencies with Gaussian Copula for Data Synthesis,” *Journal of Data Privacy*, vol. 15, pp. 45–58, 2023.
- [5] S. Ram, “Feature Engineering and Transformation Techniques for Machine Learning,” *Proc. ML Conf.*, pp. 112–127, 2022.
- [6] L. Prokhorenkova, G. Gusev, A. Vorobev, A. Dorogush, and A. Gulin, “CatBoost: Unbiased Boosting with Categorical Features,” in *Advances in Neural Information Processing Systems*, vol. 31, 2018, pp. 6638–6648.
- [7] R. Tibshirani, “Regression Shrinkage and Selection via the Lasso,” *Journal of the Royal Statistical Society: Series B (Methodological)*, vol. 58, no. 1, pp. 267–288, 1996.
- [8] S. Hochreiter and J. Schmidhuber, “Long Short-Term Memory,” *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997.
- [9] B. Shahriari, K. Swersky, Z. Wang, R. Adams, and N. de Freitas, “Taking the Human Out of the Loop: A Review of Bayesian Optimization,” *Proceedings of the IEEE*, vol. 104, no. 1, pp. 148–175, 2016.

[10] C. Bergmeir and J. M. Benítez, “On the Use of Cross-Validation for Time Series Predictor Evaluation,” *Information Sciences*, vol. 191, pp. 192–213, 2012

UDC 004.891.2

Mansurova M.Y., Ospan A.G., Mussa A.
(Almaty, Al Farabi Kazakh National University)

DEVELOPMENT OF AN AI ASSISTANT FOR JOURNALISM BASED ON RETRIEVAL-AUGMENTED GENERATION (RAG)

Artificial intelligence (AI) has recently demonstrated transformative potential in various domains, ranging from finance and law to education and cybersecurity. Large language models (LLMs)—notable examples include ChatGPT and Deepseek—have proven particularly adept at tasks such as summarization, question answering, and machine translation, opening new possibilities for technology-based solutions (Zhao 2023). In many cases, these advanced neural architectures leverage vast datasets and sophisticated learning methods to handle diverse linguistic tasks. Notably, specialized LLMs such as Kaz-LLM (Team 2024), nur-dev/llama-1.9B-kaz-instruct (Kadyrbek 2024) and Til_qazyna—fine-tuned specifically for Kazakh—demonstrate a deeper linguistic understanding than the original LLaMA 3 model, illustrating the continuous evolution of AI systems in multilingual contexts.

In journalism, LLMs offer emerging opportunities for drafting articles, synthesizing research, and even personalizing news feeds for readers. However, these advantages come with significant limitations. Traditional LLMs primarily rely on static training data, which means their knowledge is stored in model weights and may quickly become outdated. Updating or fine-tuning a large model can be prohibitively time-consuming, often taking many hours or days, a constraint that is especially troublesome for the fast-paced news cycle. Furthermore, LLMs risk producing hallucinated facts or inaccurate content if they lack access to timely information sources. In journalism—where trust and accuracy are paramount—these shortcomings diminish the direct usability of LLMs in content creation and editorial workflows.

Retrieval-Augmented Generation (RAG) (Lewis 2020) has emerged as a key strategy for addressing these challenges. Rather than relying exclusively on an LLM’s internal knowledge, RAG systems couple a generative model with an external information retrieval component. When presented with a query or prompt, the retrieval module identifies relevant, authoritative documents or data in an external knowledge base—such as up-to-the-minute news articles, databases, or reference archives. The system then provides this context to the LLM, which uses it to generate outputs firmly grounded in credible, real-time information. By linking generation directly to verifiable sources, the RAG approach reduces misinformation and allows content to remain current. This advantage is especially salient in journalism, where even minor inaccuracies can undermine credibility.

RAG-based AI assistants for journalism can function as real-time research aides, writing partners, and fact-checking systems. They retrieve background information on breaking stories, verify quotes or data against reliable sources, and generate draft content that journalists can refine. This approach not only enhances the completeness and accuracy of news articles but also accelerates the editorial process

by automating routine tasks like background research. It further enables personalized news feeds for readers by filtering out unreliable content and prioritizing factual information. Ultimately, RAG helps mitigate the inherent knowledge limitations of stand-alone LLMs, offering a practical solution that combines advanced text generation capabilities with an ongoing supply of verified, up-to-date data.

The foundations of this approach rest on understanding both LLM capabilities and their shortcomings. Transformer-based architectures, such as GPT-style models, excel at understanding language patterns and generating coherent text but remain constrained by their training sets. Without additional retrieval mechanisms, they cannot reliably answer queries about recent developments or specialized topics not covered in their training. RAG integrates external data through a two-step process: relevant materials are first retrieved from an indexed repository, then included as context when prompting the LLM. This design maintains the LLM's ability to generate fluid, sophisticated responses while expanding its knowledge frontier. For journalistic use, it means stories are consistently accurate, comprehensive, and reflective of the latest information available.

When deploying RAG systems in journalism, several considerations arise. Maintaining a current and unbiased knowledge base is paramount: if the source material includes outdated or skewed content, the system's outputs will inherit these flaws. In fast-evolving news scenarios, initial reports may conflict, and the LLM could struggle to reconcile discrepancies in real time. Here, advanced retrieval strategies and prompt engineering can help flag or highlight inconsistent information rather than merge it incorrectly. Technical constraints also exist, including the fixed context window typical of many LLMs, which demands careful selection and summarization of relevant documents to avoid information overload.

Ethical and editorial challenges likewise merit attention. AI-generated content must be fact-checked and attributed properly to avoid plagiarism or misrepresentation. Human oversight remains essential for ensuring sensitive or high-stakes reporting is handled responsibly, and journalists must remain vigilant about representing diverse viewpoints in an AI-curated environment. If multiple news organizations adopt the same RAG system with a shared knowledge base, there is a risk of homogenized reporting that overlooks minority voices or alternative perspectives. Clear editorial guidelines and continual curation are thus necessary for responsible deployment of such AI assistants.

In conclusion, the integration of LLMs with Retrieval-Augmented Generation represents a significant milestone for AI in journalism. By seamlessly pairing advanced language models with access to credible, real-time data, RAG-based assistants alleviate many of the drawbacks associated with stand-alone LLMs. The result is a tool that enhances efficiency, reliability, and transparency in news production—whether through automated drafting, real-time research, or fact-checking. Yet successful adoption requires thoughtful management of knowledge bases, careful editorial oversight, and ethical guidelines to preserve journalistic integrity. With these measures in place, RAG-driven AI assistants can serve as transformative assets for modern newsrooms, pushing journalism toward a future that is both technologically enriched and deeply grounded in factual accuracy.

List of references

1. Zhao, Wayne Xin, Kun Zhou, Junyi Li, Tianyi Tang, Xiaolei Wang, Yupeng Hou, Yingqian Min *et al.* 2023. «A survey of large language models.» *arXiv preprint arXiv:2303.18223* 1, no. 2.
2. [2] Team, ISSAI Research. 2024. KAZAKH LARGE LANGUAGE MODEL ISSAI KAZ-LLM. Nazarbayev University. 10 December. Дата обращения: 30 March 2025 г. <https://issai.nu.edu.kz/kazllm/>.
3. [3] Kadyrbek, Nurgali. 2024. LLaMA 1.9B Kazakh Instruct Model. December. Дата обращения: 30 March 2025 г. <https://huggingface.co/nur-dev/llama-1.9B-kaz-instruct>.

4. [4] Lewis, Patrick, Ethan Perez, Aleksandra Piktus, Fabio Petroni, Vladimir Karpukhin, Naman Goyal, Heinrich Küttler et al. 2020. «Retrieval-augmented generation for knowledge-intensive nlp tasks.» *Advances in neural information processing systems* (33): 9459-9474.

UDC 517.956

Marat G.S. (Almaty, Al-Farabi KazNU)

FINDING THE THERMOPHYSICAL PARAMETERS OF THE MATERIAL BASED ON THE HYPERBOLIC EQUATION OF THERMAL CONDUCTIVITY

With the development of technology, scientists have recently begun to use hyperbolic heat conduction equations more often. Here, a special place is occupied by the determination of the thermophysical parameters of the material, when the process of heating bodies by high-intensity energy flows is studied. Methods for solving the inverse problem for the hyperbolic heat conduction equation have not yet been sufficiently developed. For practical use, based on the measured statistical data, the development of methods for finding the thermophysical parameters of the heated material has a special place. Therefore, the development of methods for solving coefficient inverse problems for hyperbolic heat conduction equations becomes an urgent task.

This work is devoted to numerical methods for finding the thermophysical parameters of the material under the heat. The mathematical model on the basis of hyperbolic equation of thermal conductivity is presented as well as the relaxation of heat flow is taken into account.

The implementation of the Fourier method for solving the nonlinear hyperbolic problem of thermal conductivity in a one-dimensional approximation by spatial coordinate is considered on the assumption that the diameter of the heating region is much greater than the depth of heat penetration. The main idea of this method is that the solution of the problem for partial differential equations is reduced to solving auxiliary problems for equations with fewer independent variables.

Using the modified Newton method, numerical results were obtained for finding all the thermophysical parameters, as well as a comparison with the initially set values was carried out.

References

1. Рысбайұлы Б., *Обратные задачи нелинейной теплопередачи: монография. Алматы: Қазақ Университеті, 2022*
2. Рысбайұлы Б., Адамов А.А., *Математическое моделирование тепла и массообменного процесса в многослойном грунте: монография. Алматы.: Қазақ Университеті, 2020.*
3. Петрова Л.С. *Математическое моделирование процессов нагрева многослойных тел при обработке потоками энергии высокой интенсивности на основе системы нелинейных гиперболических уравнений теплопроводности // Интернет-журнал «Науковедение». 2017. Том 9, №4.*

UDC 004.056.b.

Meiramkhan E.A. – master’s student (Astana,
L.N. Gumilyov ENU)

METHODS OF INTEGRATING KAPE WITH OTHER DIGITAL FORENSICS TOOLS

Abstract: KAPE (Kroll Artifact Parser and Extractor) is a digital forensics tool developed by Eric Zimmerman to streamline the rapid collection and processing of forensic artifacts in Windows environments. Unlike traditional forensic tools, KAPE is highly customizable, allowing investigators to define what data is collected, how it is gathered, and whether additional processing is applied.

KAPE overcomes common triage limitations, such as metadata loss, locked file restrictions, and rigid data collection parameters. By acting as a high-speed forensic engine, it enables investigators to acquire actionable intelligence in under 90 minutes. This paper examines KAPE’s key functionalities, integration with other forensic tools, and its role in enhancing the efficiency of digital forensic investigations.

Keywords: Digital forensics, KAPE, triage imaging, artifact collection, windows forensic analysis, incident response, volume shadow copies, chain of custody, forensic automation, data integrity

I. Introduction

KAPE is a triage tool designed to rapidly identify and extract the most relevant forensic artifacts from a target system. Its high-speed processing allows investigators to prioritize critical systems in their case, expediting forensic analysis. Additionally, KAPE can collect essential artifacts at the beginning of a traditional imaging process, enabling analysts to review extracted data for leads, build timelines, and accelerate investigations while imaging completes. KAPE serves two primary functions: collecting files and processing them using external forensic tools. Instead of executing these tasks independently, KAPE relies on configuration files that define which artifacts to collect and how to process them. This modular design makes KAPE highly customizable without requiring software modifications[1-2].

At a technical level, KAPE operates by adding file masks to a queue, directing the collection of targeted files from a source location. If files are locked by the operating system, KAPE performs a secondary pass to bypass restrictions. The collected files and metadata are then preserved in a designated directory.

Additionally, KAPE can process extracted data using third-party forensic tools, categorizing results into structured groups such as EvidenceOfExecution, BrowserHistory, and AccountUsage. This method simplifies analysis by organizing artifacts based on their forensic significance rather than requiring expertise in individual artifacts(Figure 1).

Speed	• Measurably Faster than Other Tools
GUI & Command Line	• GUI Front and configurable command line
Collect Locked Files	• Can collect registry and other locked files
Configurable & Scriptable	• Predefined or Roll your own 1 or Many Machines
Volume Shadow Copy	• VSS can be processed as part of the targets collected
Batch Mode	• Automatically start collections with predefined targets
Several Output Options	• Zipped, VHDX, UNC, AWS S3, Azure
Process Data	• Process data collected with CLI tools

Figure 1. Key features of KAPE

KAPE is available in two licensing models: Solo and Enterprise. The Solo edition is free for government agencies, educational institutions, and internal corporate investigations, while the Enterprise edition is required for third-party engagements or commercial use.

II. KAPE Configuration and Customization

KAPE operates using a system of targets and modules, both defined using YAML configurations. This structured approach ensures flexibility and ease of use, allowing forensic investigators to efficiently customize data collection and processing. KAPE includes numerous preconfigured targets and modules that can be used as-is or modified to meet specific forensic requirements. These configurations have been rigorously tested for accuracy and reliability. By modifying the provided YAML files, users can extend KAPE's functionality for various investigative scenarios (Figure 2).

- KAPE divides its functionality into two parts
 - Targets
 - Modules
- Targets collect files/folders
- Modules process files/folders
 - Can also run programs to collect memory or other live response data
- These operations can be done independently of each other, or combined

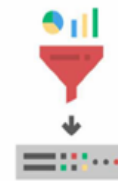


Figure 2. KAPE Targets & Modules

Targets

Target configurations specify file masks used to locate different types of artifacts on a storage device. These masks allow KAPE to collect files based on full name, extension, or even an entire directory structure. Recursive searching can be enabled to capture nested files, ensuring comprehensive artifact collection. This method provides investigators with an efficient way to acquire critical forensic evidence.

Modules

Modules process the files collected by KAPE, executing commands using external forensic tools. Each module configuration defines parameters such as command-line arguments, export formats, and processing options. Modules enable automated execution against live systems or previously acquired forensic data. This modular design allows seamless integration with CLI-based forensic tools, optimizing digital forensic workflows.

By combining targets and modules, KAPE provides a powerful, adaptable solution for forensic investigations, enabling precise data acquisition and automated artifact analysis.[3] This structured workflow significantly enhances efficiency in digital forensics and incident response (Figure 3).

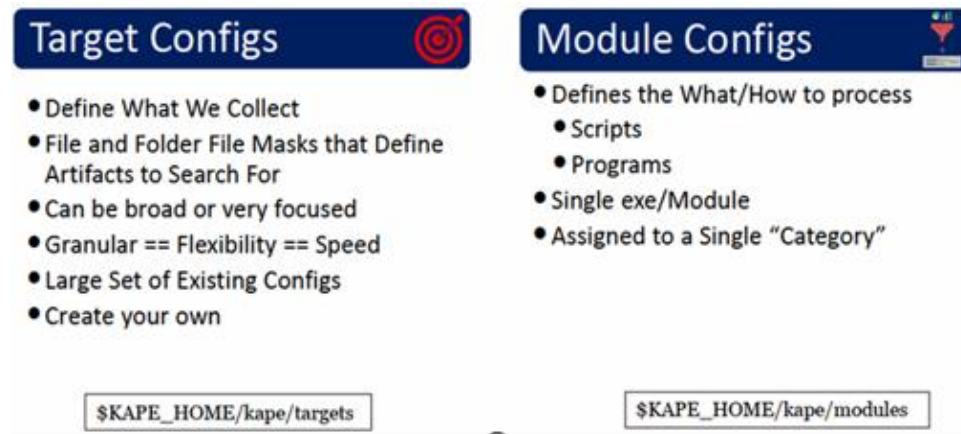


Figure 3. KAPE configuration files

III. Optimizing forensic analysis with KAPE Targets and Modules

Targets in KAPE define file and directory specifications used to identify and extract forensic artifacts. KAPE processes these specifications, compiles a list of relevant files, and copies them to a destination directory.

For locked files, KAPE employs a two-step approach: accessible files are copied first, while locked files are added to a secondary queue and extracted using raw disk reads. This ensures the preservation of in-use files without system interference. All copied files retain their original timestamps, and metadata is logged in text and CSV formats.

Targets should focus on specific artifacts, such as Jump Lists or LNK files, keeping collections granular for flexibility. Modular targets can be combined as needed, except for cases like NTFS file system data, where elements like \$MFT, \$LogFile, and \$J are typically used together. This structured approach optimizes forensic investigations by maintaining accuracy and adaptability[4].

Like targets, KAPE modules are defined using YAML properties and are designed to execute forensic tools on collected data or live systems. Modules allow investigators to automate the processing of artifacts, such as using JLECmd to extract Jump List contents or RECcmd to analyze Windows registry files. Additionally, live response commands, such as netstat.exe or ipconfig /dnscache, can be executed through modules for real-time system analysis.

Each module references a single executable but can be configured to export data in multiple formats, including CSV, HTML, and JSON. This enables integration with big data platforms like SOF-ELK or Splunk, as well as forensic tools like Timeline Explorer for in-depth analysis.

Modules are categorized based on their function, such as Evidence of Execution, File and Folder Opening, or Browser History. Maintaining standardized categories ensures consistency in forensic workflows, making data analysis more structured and efficient(Figure 4).

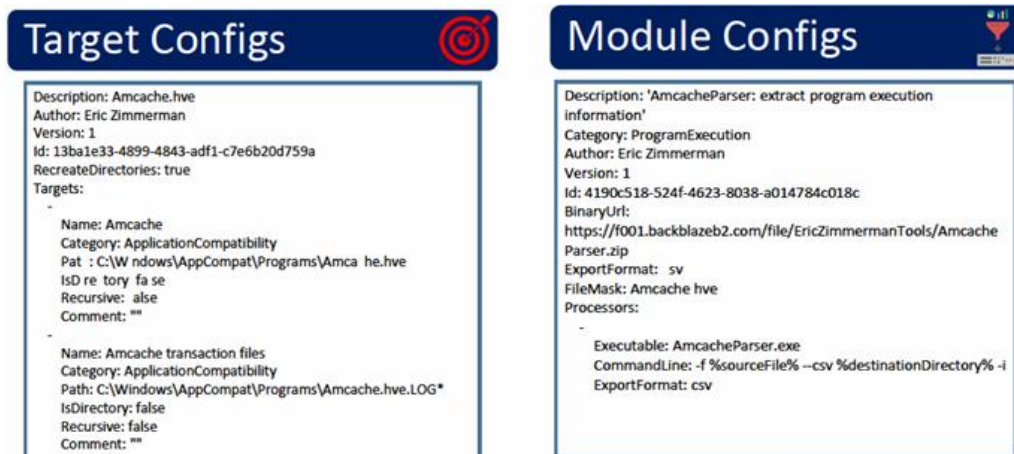


Figure 4. KAPE configuration file examples

KAPE includes a variety of predefined targets, including those from the SANS Forensics Analysis poster, covering browser history, file system metadata, LNK files, Jump Lists, Outlook data, and event logs. Users can utilize these targets or create custom ones to fit specific forensic needs.

Similarly, KAPE provides built-in modules for processing collected data, which can also be customized. The KAPE manual offers detailed documentation on configuring targets and modules, with additional examples available in the installation directory. Full documentation is accessible online[5].

The GUI version of KAPE simplifies forensic data collection by allowing analysts to select artifacts for triage with a simple checkbox system. The left panel of the interface represents the Target selection, while the right panel (partially shown in the interface) corresponds to the Module processing side (Figure 5).

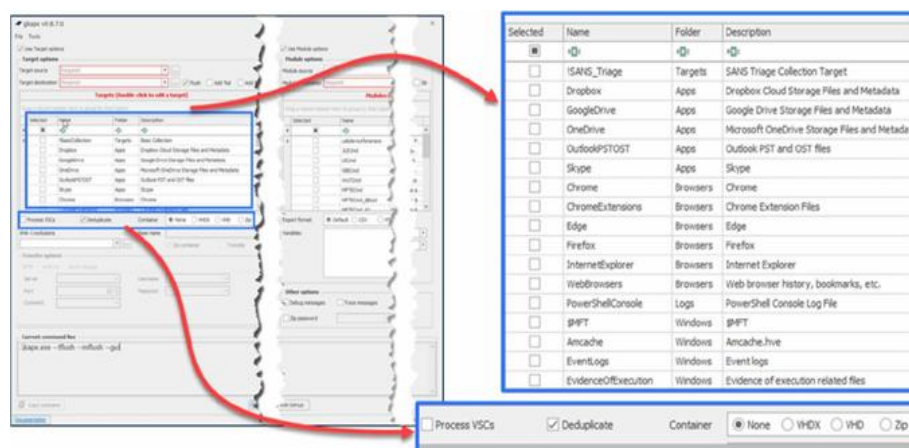


Figure 5. Creating triage data with KAPE

KAPE also streamlines additional forensic tasks, such as extracting Volume Shadow Copies with a single click, eliminating the need for multiple manual steps. Additionally, collected data can be saved as a VHDX file, which is automatically compressed into a ZIP archive for efficient storage.

While KAPE originally operated as a command-line tool, the GUI (GKAPE) was introduced later for ease of use. The command line remains a powerful option, enabling automation of data collection

and processing. Analysts can review generated commands in the GUI to better understand and optimize KAPE's CLI usage. Enabling the "Use Target Options" checkbox in KAPE's GUI grants access to the Target selection panel, where users define which forensic artifacts to collect.

Define Source and Destination – Select the drive letter (e.g., C:, D:) or UNC path for data collection. KAPE does not process forensic images (E01) directly; users must first mount them using Arsenal Image Mounter (AIM). The destination should be an external drive, network share, or cloud storage (SFTP, AWS S3, Azure).

Append Machine Name – Checking the %m option ensures that the collected data is tagged with the machine name, useful when gathering evidence from multiple systems.

Select Targets – Choose the artifacts or groups of artifacts to collect. KAPE includes predefined targets but also allows for customization.

Process Volume Shadow Copies (VSCs) – Checking the "Process VSCs" box enables KAPE to collect data from VSCs, automatically organizing them by snapshot.

Choose Output Format – Select from various storage formats such as ZIP, VHD, XHDX, or compressed VHDX for efficient data management.

Execute Collection – Clicking "Execute" initiates the collection process, displaying progress in a command window.

This structured workflow allows investigators to efficiently gather and store forensic data while maintaining flexibility in output options (Figure 6).

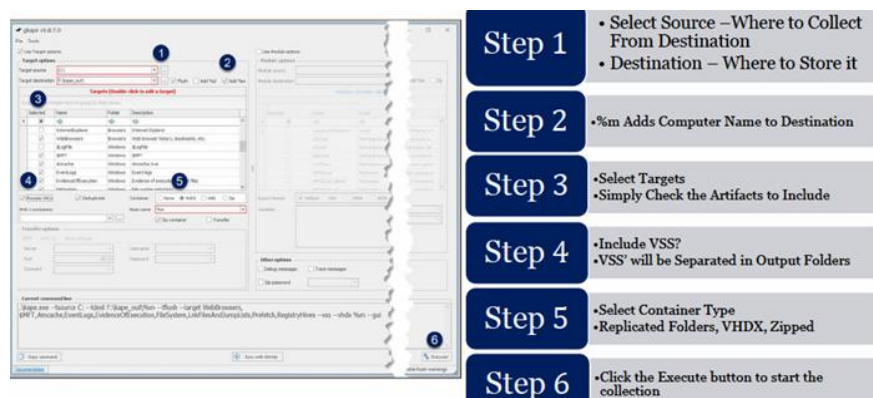
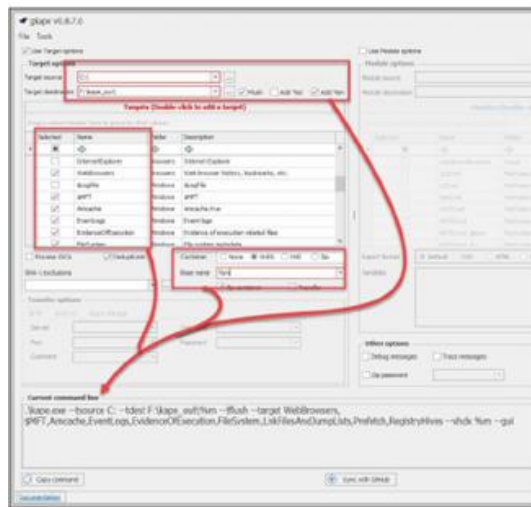


Figure 6. Definition of collection criteria

In Figure 7, KAPE dynamically generates the corresponding command line as users select Targets and Modules in the GUI. This feature helps users familiarize themselves with KAPE's CLI syntax.

While most KAPE functions can be executed via the GUI, scripting remains exclusive to the command line. Scripting is essential for automation and large-scale deployment, enabling forensic teams to streamline data collection across multiple systems efficiently [6-7].



- Great way to learn the KAPE CLI
- Cut & Paste to command line to build scripts or batch files

Figure 7. KAPE can build the command line

KAPE uses double dashes (--) before each command-line parameter. Understanding CLI syntax is essential for automation and scripting forensic collections.

One key feature of KAPE is its variety of output container formats. Users can choose between an uncompressed replicated folder structure or a highly compressed VHDX.[8] While VHDX is already a compressed format, further compression can significantly reduce storage requirements, making it possible to store data from multiple systems on a single USB drive(Figure 8).

- --vhdx - The base name of the VHDX file

Zippered VHDX is default for --vhdx

```
PS G:\> kape --source E: --target LnkFilesAndJumpLists --vhdx nromanoff
PS G:\> kape --source E: --target LnkFilesAndJumpLists --vhdx nromanoff --zv False
```

• --vhd - The base name of the VHD file

• --zip - The base name of the ZIP file

Note: KAPE output containers are not read-only and hence you should always use a "working copy" during analysis

Figure 8. Containers for Target output

KAPE Targets control how the collected folder structure is replicated. When the "Recreate Directories" option is enabled, the output maintains the original folder hierarchy, mirroring its structure in Windows Explorer.

Additionally, KAPE can extract data from Volume Shadow Copies (VSCs), applying the same directory replication rules. This ensures that forensic artifacts from VSCs are organized consistently, preserving their original context for analysis (Figure 9).

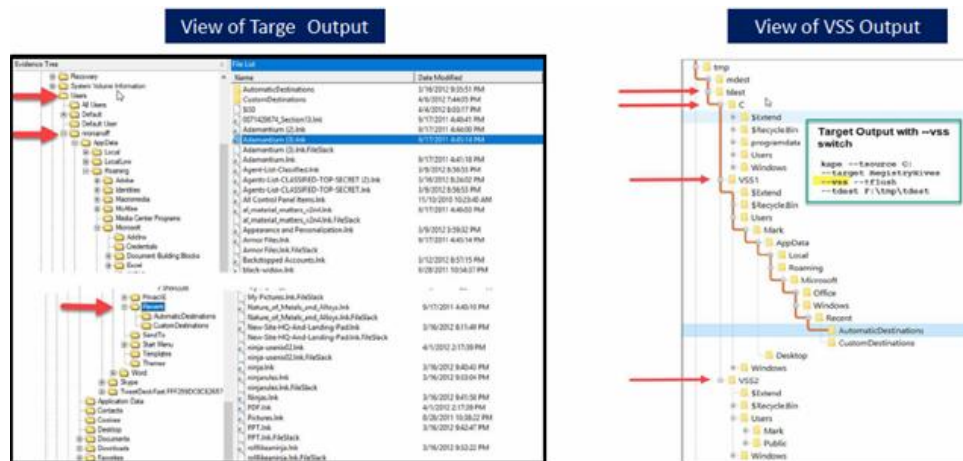


Figure 9. Output folder structure

IV. Triage Imaging with KAPE

KAPE enables the creation of a Triage VHDX, allowing investigators to quickly collect and analyze key forensic artifacts. The triage image can then be examined using tools like Windows SIFT Workstation to extract critical evidence efficiently (Figure 10).

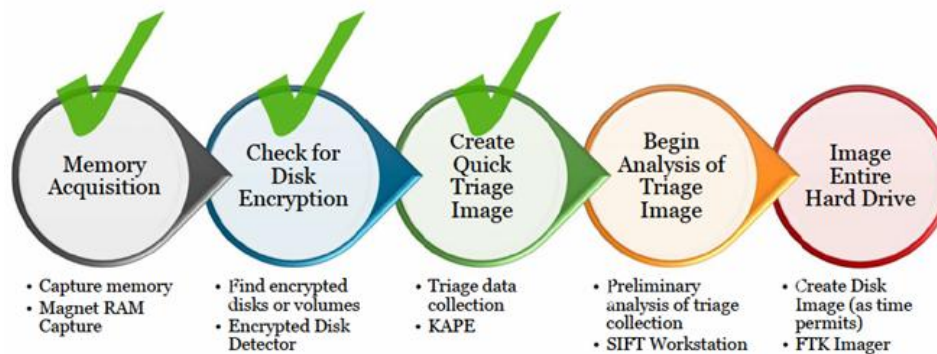


Figure 10. Triage Acquisition: step-by step overview

While triage imaging provides 95% of the most relevant artifacts, it may miss hidden folders, encrypted containers, or non-standard cloud storage. A full disk image ensures deeper analysis but is time-consuming and requires significant storage. In high-priority cases, such as insider threats, employee terminations, or law enforcement investigations, full disk imaging is recommended. However, in incident response, time constraints may necessitate selective collection from affected systems [9-10].

V. Recommendations

To enhance the efficiency of KAPE in digital forensic investigations, it is essential to focus on automation, integration, and accuracy. KAPE should be used for rapid triage collection, allowing investigators to quickly gather key artifacts while minimizing system impact. When necessary, full disk imaging should complement triage-based analysis to ensure no critical evidence is missed.

Integrating KAPE with forensic tools such as Autopsy, FTK, X-Ways, and Velociraptor improves investigative depth and efficiency. Scripting and automation should be prioritized to streamline large-scale forensic operations and reduce manual workload. Ensuring the proper handling of forensic artifacts, including metadata preservation and chain-of-custody verification, is critical for maintaining data integrity and admissibility. Investigators should leverage KAPE's ability to process Volume Shadow Copies (VSCs) to recover historical data while understanding its limitations in selective extraction. Regular updates to KAPE's configurations, targets, and modules are necessary to keep pace with

evolving forensic challenges. Periodic validation of KAPE's performance through testing and accuracy assessments will help refine collection and analysis processes over time.

By implementing these strategies, forensic teams can maximize KAPE's capabilities, improving efficiency, reliability, and the overall effectiveness of digital investigations.

VI. Conclusion

KAPE is a highly efficient tool for rapid forensic data collection and processing, allowing investigators to quickly gather critical artifacts while minimizing system impact. By leveraging targets and modules, KAPE provides a structured approach to forensic investigations, ensuring flexibility and scalability. While triage imaging with KAPE covers a significant portion of forensic needs, it is important to recognize its limitations. Hidden files, encrypted containers, and certain cloud storage artifacts may not be captured during triage, making full disk imaging necessary in complex cases such as insider threats, employee terminations, and law enforcement investigations. In incident response scenarios, time constraints may require selective data collection rather than full imaging. Despite these limitations, KAPE significantly reduces investigation time by enabling quick identification of key artifacts and automating forensic workflows.

Ensuring proper artifact handling, metadata preservation, and chain-of-custody verification is critical for maintaining data integrity and evidentiary value. The ability to process Volume Shadow Copies (VSCs) further enhances KAPE's effectiveness by recovering historical system states. Additionally, automating forensic workflows through scripting and batch processing allows for large-scale investigations with improved efficiency. The integration of KAPE with forensic analysis tools such as SIFT Workstation and other post-processing solutions further strengthens its role in digital forensic investigations.

To maximize its potential, investigators should regularly update KAPE's configurations, targets, and modules to keep pace with evolving forensic challenges and cyber threats. Future advancements in cloud forensics, integration with SIEM platforms, and AI-assisted forensic analysis will likely enhance KAPE's capabilities, making it an even more valuable tool for forensic professionals.

By combining KAPE's speed, automation, and adaptability, forensic experts can enhance the efficiency and reliability of digital investigations. As technology and forensic methodologies continue to evolve, KAPE will remain a critical component of modern forensic workflows, enabling investigators to respond effectively to cyber incidents and digital crimes.

References

- 1.B. Carrier, *"File System Forensic Analysis,"* Addison-Wesley, 2005.
2. H. Carvey, *"Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 10,"* Syngress, 2018.
- 3.B. Shavers, E. Zimmerman, *"X-Ways Forensics Practitioner's Guide,"* Syngress, 2013.
- 4.Kroll Cyber Security, *"KAPE (Kroll Artifact Parser and Extractor) Documentation,"* Kroll, Available: <https://www.kroll.com/en/services/cyber-risk/kape>.
5. AccessData, *"FTK Imager User Guide,"* AccessData, 2019. Available: <https://adpdf.s3.amazonaws.com/AD-FTK-Imager-UserGuide.pdf>.
- 6.SANS Institute, *"Velociraptor: Digging Deeper for DFIR,"* SANS Institute, 2020. Available: <https://www.sans.org/blog/velociraptor-digging-deeper-for-dfir/>.
- 7.A. J. Nelson, *"Digital Forensics and Incident Response,"* Packt Publishing, 2019.
- 8.C. Hargreaves, *"Incident Response & Computer Forensics,"* McGraw-Hill, 2020.
- 9.D. Cowen, *"Computer Forensics: A Beginner's Guide,"* McGraw-Hill, 2021.
10. A. Ligh, M. Case, J. Levy, and C. Walters, *"The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory,"* Wiley, 2014.

UDC 004.8.

Oryngaliyeva N.A.
(Karaganda, KarTU)
Scientific advisor – Associate Professor
of KarTU Saimanova Z.B.

MODERN METHODS OF TEXT RECOGNITION IN THE CONTEXT OF THE KAZAKH LANGUAGE IN CYRILLIC

OCR (Optical Character Recognition) is key to digitalizing information, especially for linguistically diverse texts. While modern neural networks have enhanced OCR accuracy, challenges remain for Kazakh, which uses Cyrillic with unique diacritical marks (ә, ө, ү, ң, ғ, қ, і). Traditional OCR models, optimized for Latin script, struggle with these complexities, hindering document digitization and accessibility.

Recent advances in Scene Text Recognition (STR) explore Vision Transformers (ViT). ViTSTR by Rowel Atienza achieved 82.6% accuracy (84.2% with augmentation) with fewer parameters and lower computational costs. The MVLT approach by Jie Wu et al. integrates visual and linguistic data, setting new benchmarks. These methods improve accuracy, efficiency, and robustness in complex STR scenarios.

The study leveraged the Kazakh Offline Handwritten Text Dataset (KOHTD), the first large-scale dataset for Kazakh handwriting recognition. It comprises 3,000 exam papers with 140,335 segmented images and 922,010 characters, written in blue ink under real-world conditions. Preprocessing techniques (brightness correction, noise removal, augmentation) enhanced model robustness. Data was structured into folders with annotations in JSON, later converted into a TXT format for streamlined training.

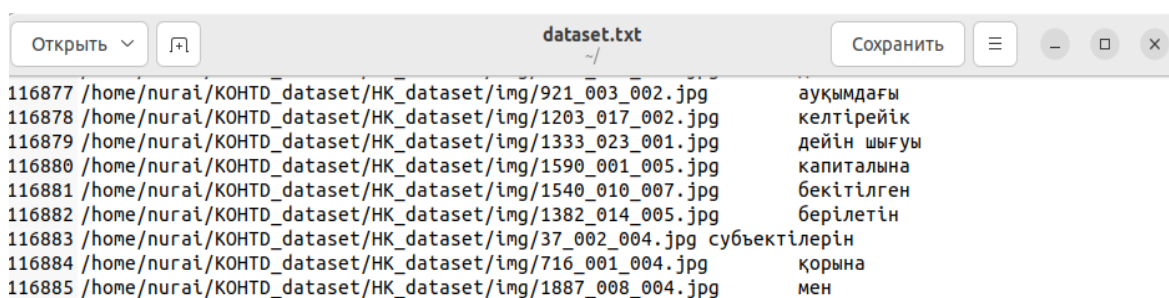


Figure 1. Dataset

To enhance readability and improve recognition accuracy, several preprocessing techniques were applied. The image was enlarged 2× using bicubic interpolation (cv2.INTER_CUBIC) to improve detail visibility. A median filter (cv2.medianBlur) was used to reduce noise while preserving text contours. Contrast enhancement was performed using CLAHE (Contrast Limited Adaptive Histogram Equalization) to boost contrast without overexposure. Adaptive thresholding (Otsu's method) was applied for binarization, converting the image to black and white for better text extraction. The colors were inverted so that the text appeared white on a black background. Erosion (cv2.erode) was used to

thin characters by removing excess pixels, reducing noise-based distortions. Morphological closing was applied to connect broken characters and restore letter structures, improving OCR accuracy. These preprocessing steps minimized artifacts and enhanced text clarity, optimizing recognition performance (figure 2).

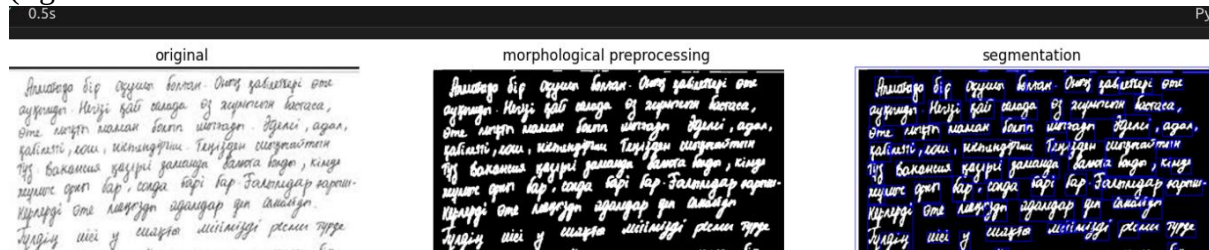


Figure 2. Image preprocessing

After preprocessing, images are fed into a Visual Transformer (ViT) for training and text recognition. The process involves several key steps: the input image (e.g., the word "Есептеу") is divided into fixed-size patches, which are then transformed into feature vectors via linear projection. Since transformers do not inherently consider spatial order, positional embeddings are added to retain spatial relationships. A special trainable token aggregates information from all patches. These embeddings are processed by the transformer encoder, which consists of self-attention layers and normalization, producing feature vectors ($V_1, V_2, \dots, V_{128}$) that capture the visual characteristics of characters. Extracted features are separated into positional (PEM) and visual (VEM) components - PEM encodes spatial positioning, while VEM captures textual visual features. Finally, a fully connected layer interprets these vectors, generating the recognized text output, such as "Есептеу." The model architecture is illustrated in Figure 3.

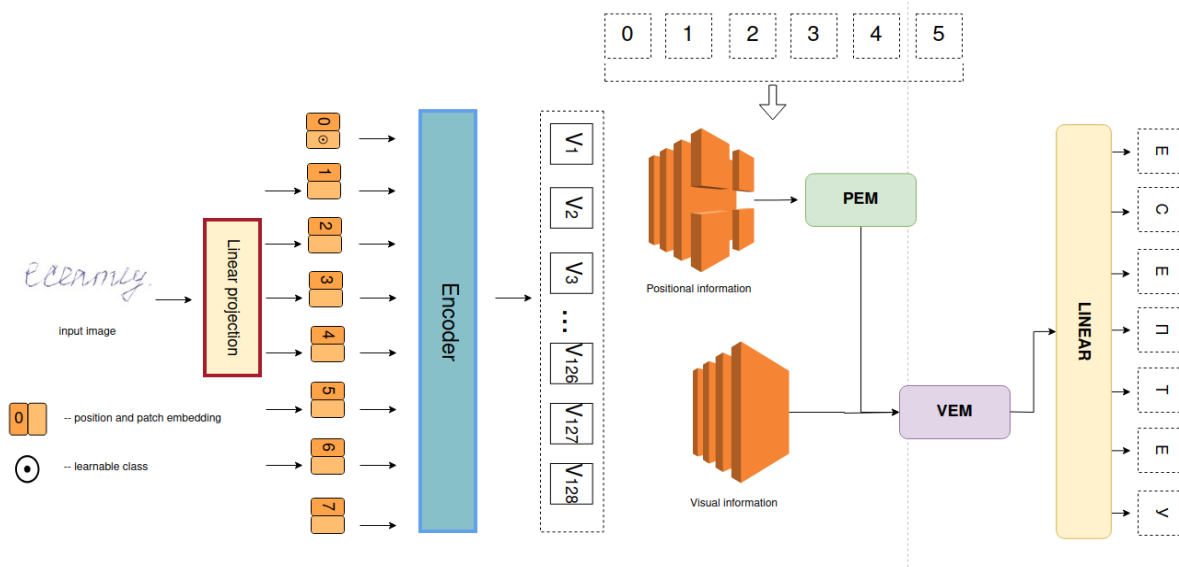


Figure 3. ViT architecture

During the research, a Visual Transformer model was developed and tested for recognizing handwritten essays and reports in the Kazakh language. The main focus was on analyzing the model's architecture, quantitatively assessing recognition quality, and identifying characteristic errors. The core

component of the model is the Multi-Head Attention mechanism, which is computed using the following formula:

$$\text{Attention}_{Q,K,V} = \text{softmax}(QK^T/dk)V$$

Q – queries, K – keys, V – values, dk- the dimension of the hidden representation. The layer state update is performed as follows:

$$x' = \text{LayerNorm}x + \text{Dropout}(\text{MultiHeadAttention}_{Q,K,V})$$

$$x'' = \text{LayerNorm}x' + \text{Dropout}(\text{FFN}x')$$

The model's performance was evaluated using standard metrics: WER (Word Error Rate) and CER (Character Error Rate), both based on Levenshtein distance $\text{Lev}(A,B)$, which measures the minimum number of insertions, deletions, and substitutions needed to transform a reference text into a predicted text. CER quantifies character-level discrepancies, while WER applies the same principle at the word level. Accuracy represents the proportion of correctly recognized elements. Across epochs, the model exhibited a steady improvement, with WER and CER decreasing while accuracy increased from 65% in the first epoch to 85% by the tenth (table 1). These results highlight the model's growing proficiency and reliability in recognizing handwritten Kazakh text.

Table 1. Results

Epoch	WER	CER	Accuracy
1	0.35	0.25	0.65
2	0.34	0.24	0.68
3	0.32	0.23	0.70
4	0.31	0.22	0.72
5	0.30	0.21	0.74
6	0.28	0.20	0.76
7	0.27	0.19	0.78
8	0.26	0.18	0.80
9	0.25	0.17	0.82
10	0.23	0.16	0.85

During the study, a Visual Transformer model was developed and tested, achieving an accuracy of 85% with an average CER of 7% and WER of 15%. The primary errors were related to the substitution of visually similar letters (e.g., "н" being misrecognized as "и"). The use of transformers improved recognition quality; however, the model requires further training on rare characters and parameter optimization.

REFERENCES:

Vision Transformer for Fast and Efficient Scene Text Recognition / Rowel Atienza // *IEEE International Conference on Document Analysis and Recognition*. – 2021. – DOI: 10.1007/978-3-030-86549-8_21

Masked Vision-Language Transformers for Scene Text Recognition / Jie Wu, Ying Peng, Shenmin Zhang, Weigang Qi, Jian Zhang // *British Machine Vision Conference*. – 2022. – DOI: 10.48550/arXiv.2211.04785

UDC 004.056.55

Ospanova A. B., Zharaskhan N.Zh.,
Kayupov E. (Astana, L. N. Gumilyov ENU)

PRACTICAL EFFICIENCY AND POTENTIAL OF LATTICE REDUCTION IN RECOVERING SECRET PARAMETERS OF POST-QUANTUM CRYPTOSYSTEMS

Using the example of Kyber ([1]) we consider some aspects of cryptanalysis of lattice post-quantum algorithms based on studies of their direct mathematical structure. The efficiency of approximating key parameters obtained by some lattice reduction methods, when applied directly to plaintext reconstruction, depending on the data format, is also discussed. Conclusions are drawn about the practical conditions for recovering the encryption key from these approximations.

In the case of falseax cryptanalysis problems (the short vector problem SVP, the nearest vector problem CVP), lattices are transformed into a convenient form, which reduces these problems to simpler ones (in practice, they are still quite complex), but for which solutions (s') can be constructed. These solutions give an approximation of the secret parameters of the encryption key s . Approaches to error level correction and their corrections in LWE/LWR problems, which Kyber is based on, are based on the type of reduction, considering noisex components, post-processing methods, and iterative refinement, for example, error correction or MLsearch.

However, error correction and analysis methods, brute-force algorithms, and iterative methods require a cipher material, that is, some accurate data about the plaintext or key as a support. It will be possible to use the nearest correct value, bitwise refinement, recognition of distortion and distorted characters and bits, checksums). That is, more cryptanalysis must be performed to find this exact data.

In the case of without reference data, that is, with Ciphertext-Only Attacks, it is necessary to analyze the parameters and get sets of errors, search for statisticales regularities and plaintext, search for stablee regularities both to refine candidate keys, and us machinee learning, optimization methods.

In practice, the success of such recovery depends on the format in which the plaintext is presented, namely, on the area of the file where there is an error as a result of applying approximate key parameters. So,

- file header corruption (critical header corruption) can lead to complete inability to open the file.
- damage to structured segments (codecs, tables, indexes) leads to failures in decoding.
- local artifacts (noise, image defects, frame skips) and
- errors in texts (bit errors, corrupted strings, incorrect encoding) allow you to partially restore the original text.

At the same time, knowing the probability of errors and the influence of the number of approximations on the exact opening of information for various file types makes it possible to assess the success of hacking even at the stage of preliminary analysis, before the actual resource-intensive stages of cryptanalysis begin.

For the created minute-long audio file with speech *audio_66_66s_128_128kbps.mp3* (uploaded to the repository [2]) выполнен an analysis was performed ([2]), its structure is shown in Figure 1

```
Duration: 66.04 sec
Bitrate: 128.0 kbps
Sampling rate: 44100 Hz
Channels: 1
Estimated number of frames: 2528

===== ID3 Metadata =====
TSSE: ['Lavf59.27.100']

===== Physical Parameters =====
File size: 1032.29 KB
Duration (via Pydub): 66.0 sec
Sampling rate: 44100 Hz
Channels: 1
Bit depth: 16 bit
Format: 2-byte PCM
```

Fig. 1. Structure of the mp3file

File Type	Critical Segment
JPEG	SOI, Huffman table
MP4	moov, mdat
TXT	UTF-8 BOM
PDF	xref table, header

Fig. 2. Critical elements of data formats

MP3 header (ID3+ MPEG Frame Sync) in case of *66audio_66_128s_128 kbps.mp3* is approximately 128 bits; 1 frame (approximately 417 bytes, no 128 kbit/s each) can be taken rounded to half a bit, 4096 bits. If the probability of an error per bit is $\varepsilon = 10^{-4}$, then the probability of an error in the header is $P = 1 - 1(-\varepsilon)^{128} \approx 1 - e^{-0.0128} \approx 1.27\%$; error in the frame is $P = 1 - 1(-\varepsilon)^{4096} \approx 1 - e^{-0.40964096} \approx 33.4,4\%$. With 2500 frames ax, contained in this file, with a small error in the key, statistically about 800 frames will be erroneous.

Elf N approximations s' are performed, the probability that among them there is a successful $P_{ps} = 1 - (1 - 0.0127)^N$, that is, for $N > 50$ (up to 1000), the risk of error in critical areas of the plaintext in this audio format is significantly reduced.

For some other file types, critical segments are shown in Figure 2.

Next моделируются приближения, the s' approximations are modeled, and the resulting keys are tested. KEach approximation contains bit distortions. Проанализированы Both the differences between s and s_{si}' (iis the number of approximations) and the values obtained on candidate keys are analyzed.

References

- [1] Стандарт FIPS PUB 203 Standard – <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.ipd.pdf://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.ipd.pdf>
- [2] Файлы Project files – github.com/Alin0268/FilesForShare/blob/master/PapersDataFilesForShare/blob/master/PapersData

Shutong Hou(Nanjing, China, SEU) Haibing
Wang(Nanjing, China, SEU)

A NOVEL APPROACH FOR AN INVERSE SOURCE PROBLEM OF THE WAVE EQUATION IN THREE DIMENSIONS

We address the inverse problem of reconstructing the source term in a bounded domain for the time-domain wave equation. A small droplet with high contrast is injected into the medium, and then the difference in the wave fields before and after injecting the droplet is utilized to develop a novel reconstruction approach. First, we analyze the asymptotic behavior of the wave field after injecting the droplet by using the time-domain integral equation method. Then, on the basis of this analysis, the wave field before injecting the droplet is reconstructed by utilizing the external measurements. Next, the source term is reconstructed through numerical differentiation of the wave field before the droplet injection. A key advantage of our approach is that it only requires measurements at a fixed point over a period of time. Additionally, to show the performance of our approach for the inverse problem, we also develop an efficient algorithm to solve the time-domain Lippmann-Schwinger equation for the corresponding forward problem. Numerical experiments in three dimensions are presented to demonstrate the effectiveness of the proposed approach.

UDC 004.896.

Yerzhan M. (Almaty, Al-Farabi Kazakh National
University)

Bazargul M. (Almaty, Al-Farabi Kazakh National
University)

ROUTING AND COORDINATION MODELS FOR INTELLIGENT DRONES IN DISASTER SCENARIOS

The growing demand for efficient disaster response systems in GPS-denied and high-risk environments has led to the development of intelligent drone coordination frameworks. This research introduces a routing and coordination model for multi-agent UAV systems operating in complex disaster scenarios. The proposed approach incorporates computation offloading, dynamic path planning, and fault-tolerant coordination to improve operational efficiency and system resilience [1], [2].

A ROS-based prototype system was developed and tested in a simulated mountainous environment, replicating post-disaster conditions. The architecture includes a centralized Swarm Coordinator that manages agent communication and offloading tasks, while a backup election mechanism ensures mission continuity in the event of central node failure [1], [5]. Real-time status updates allow adaptive route generation using a Dijkstra-based algorithm over a dynamic network graph [4].

Experimental evaluation demonstrates that the proposed system improves mission performance across key metrics: a 27% reduction in task completion time, 42% increase in perception accuracy via offloaded object detection, and 85% swarm continuity under orchestrator failure [2], [3].

These results confirm the system's suitability for time-sensitive, AI-driven UAV operations in constrained environments. The integration of computation offloading and resilient coordination mechanisms provides a robust foundation for autonomous aerial disaster response. Future work will focus on hardware implementation and swarm behavior optimization using embedded AI processors [5].

References

1. Palieri, M., Longo, A., & Guaragnella, C. (2024). *Swarm Manager: SDN-Inspired Computation Offloading Management in Heterogeneous Multi-Robot Networks*. *IEEE INFOCOM Workshops*. DOI: 10.1109/INFOCOMWKSHP61880.2024.10620721
2. Shi, M., Zhang, X., Chen, J., & Cheng, H. (2023). *UAV Cluster-Assisted Task Offloading for Emergent Disaster Scenarios*. *Applied Sciences*, 13(8), 4724. DOI: 10.3390/app13084724
3. Chandran, I., & Vipin, K. (2024). *Multi-UAV networks for disaster monitoring: challenges and opportunities from a network perspective*. *Drone Systems and Applications*, 12, 205–216. DOI: 10.1016/j.drones.2024.04.007
4. Adam, M. S., Abdullah, N. F., Abu-Samah, A., Amodu, O. A., & Nordin, R. (2025). *Advanced Path Planning for UAV Swarms in Smart City Disaster Scenarios Using Hybrid Metaheuristic Algorithms*. *Drones*, 9(1), 64. DOI: 10.3390/drones9010064
5. Phadke, A., & Medrano, F. A. (2024). *Increasing Operational Resiliency of UAV Swarms: An Agent-Focused Search and Rescue Framework*. *Aerospace Research Communications*, 1:12420. DOI: 10.3389/arc.2023.12420

UDC 004.85.

Zhunissov N.M., Aben A.B. (Turkistan, Khoja Akhmet Yassawi International Kazakh-Turkish University)

FAKE NEWS DETECTION USING MACHINE LEARNING

Abstract. The proliferation of fake news is one of the most challenging issues in today's media landscape. It undermines public trust and informed decision-making. This study examines the effectiveness of various machine learning classifiers in identifying fake news publications on the ISOT Fake News dataset, which consists of over 25,000 articles classified as fake or authentic.

The dataset used in the study was collected from popular news websites such as CNN.com and Reuters.com, as well as from untrusted sources. The dataset includes news types covering political and world events from 2016 to 2017.

Five different machine learning algorithms were used to evaluate their performance in distinguishing between real and fake news, including logistic regression, multinomial naive Bayes, random forest, decision tree, and multilevel perceptron (MLP) classifiers. The classifiers were tested for accuracy, precision, recall, and F1 score. The results showed that the Random Forest classifier outperformed all other models, achieving a unique accuracy of 99.73% with perfect precision and recall rate. In addition, the Decision Tree and MLP classifiers showed strong performance, improving the efficiency of machine learning methods in this domain.

Keywords: Fake News Detection, Machine Learning Classifiers, ISOT Fake News Dataset, Random Forest, Logistic Regression, Confusion Matrix, News Authenticity.

Introduction. In the digital age, the proliferation of social media, information platforms, and websites has increased the accessibility and dissemination of knowledge. However, with this accessibility, new problems have emerged. In particular, social media has a significant impact on the widespread spread of fake news. For example, an Ipsos survey conducted on behalf of the International Center for Management Innovation found that one in five people believe that they have been exposed to fake news online[1].

Fake news has a profound impact on society. It affects political discourse, healthcare, and the financial sector. It also undermines public trust. Disinformation spread during elections is a major problem. False claims related to health crises are also dangerous[2]. These situations highlight the need for new methods to combat fake news. Manual verification methods are weak at controlling the rate of information spread. Therefore, automated solutions are needed that can detect fake news in real time.

Machine learning offers an effective solution to this problem. Computational algorithms can identify patterns in information. This allows for high-accuracy detection of fake news[2]. Natural language processing and deep learning techniques improve the efficiency of the models. TF-IDF and word embedding techniques play an important role. Neural networks such as LSTM and BERT are useful in analyzing complex texts. These techniques can detect linguistic features of fake news[3].

Methods. This study employed a comprehensive methodology for the detection of fake news using machine learning techniques, comprising five key phases: dataset preparation, preliminary text processing, feature extraction, model implementation, and evaluation of results.

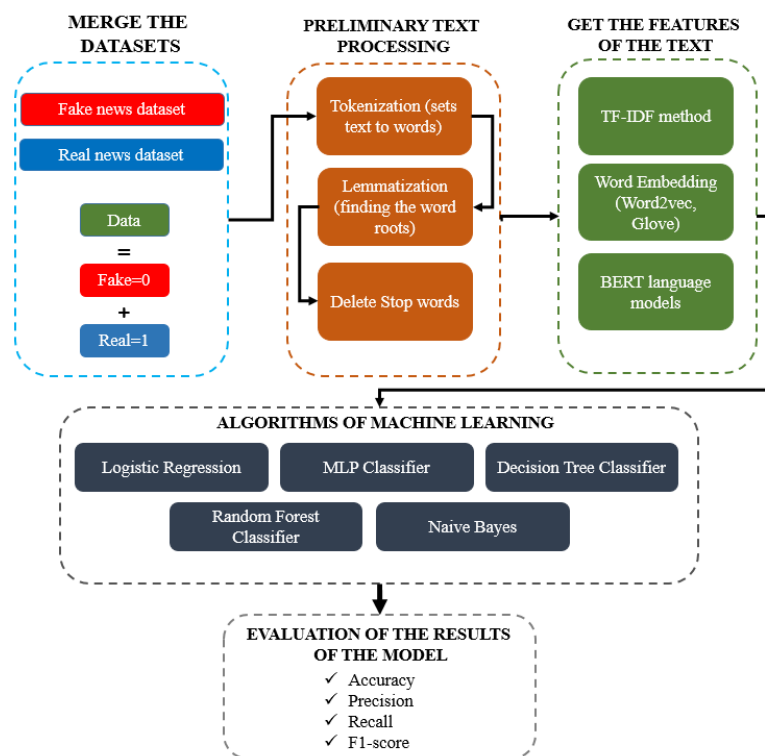


Figure 1. Architecture for fake news detection

To construct a robust classification model, we initiated the process by merging two distinct datasets: the Fake News Dataset, which contains labeled instances of misleading information, and the Real News Dataset, comprising authentic news articles.

This study used a systematic approach to identify fake news using machine learning techniques that included five guiding steps. These included: data preparation, preprocessing of the source text, feature extraction, model training, and evaluation of the results.

Implementation and results. As shown in Table 1, the Random Forest classifier achieved the highest accuracy at 0.9973, along with excellent precision, recall, and F1 score values for both classes. The Decision Tree classifier also performed exceptionally well, with a precision of 0.9951, indicating its reliability in classifying news authenticity. The MLP classifier closely followed with a precision of 0.9918, while maintaining high precision and recall values. The logistic regression classifier showed strong performance in both classes, with a precision of 0.9876 and precision and recall values of 0.99. Finally, the Multinomial Naive Bayes classifier showed balanced precision and recall, although with a slightly lower precision of 0.9285, indicating its usefulness in situations where precision could be slightly lower.

Table 1. Performance Metrics of Machine Learning Models

Model	Accuracy	Precision	Recall	F1-Score
Logistic Regression	0.9876	0.99	0.99	0.99
Multinomial NB	0.9285	0.93	0.94	0.93
Random Forest	0.9973	1.00	1.00	1.00
Decision Tree	0.9951	1.00	0.99	1.00
MLP Classifier	0.9918	0.99	0.99	0.99

Consistently high scores on various metrics indicate that these models effectively classify real and fake news. The Random Forest model shows particular promise due to its high performance across all metrics. In this study, the performance of the Random Forest classifier was evaluated using a confusion matrix to provide insight into the predictive accuracy and error distribution of the model.

Conclusion. This study evaluated the effectiveness of various machine learning classifiers in distinguishing fake and real news articles. The ISOT Fake News dataset was used for the study. The dataset, which consists of over 25,000 articles from both real and fake news outlets, provided a robust basis for evaluating classification performance. Our analysis showed that the Random Forest classifier achieved an impressive accuracy of 0.9973, along with excellent precision, recall, and F1 score values. The Decision Tree classifier and the MLP classifier also showed high performance, with accuracies of 0.9951 and 0.9918, respectively, indicating their effectiveness in this domain. The confusion matrix further reinforced the robustness of the Random Forest model, showing the lowest misclassification between fake and real news.

References

1. Shaikh, J., & Patil, R. (2020, December). *Fake news detection using machine learning. In 2020 IEEE international symposium on sustainable energy, signal processing and cyber security (iSSSC) (pp. 1-5). IEEE. DOI: [10.1109/iSSSC50941.2020.9358890](https://doi.org/10.1109/iSSSC50941.2020.9358890)*
2. Khanam, Z., Alwasel, B. N., Sirafi, H., & Rashid, M. (2021, March). *Fake news detection using machine learning approaches. In IOP conference series: materials science and engineering (Vol. 1099, No. 1, p. 012040). IOP Publishing. DOI: [10.1088/1757-899X/1099/1/012040](https://doi.org/10.1088/1757-899X/1099/1/012040)*
3. Smitha, N., & Bharath, R. (2020, July). *Performance comparison of machine learning classifiers for fake news detection. In 2020 Second international conference on inventive research in computing applications (ICIRCA) (pp. 696-700). IEEE. DOI: [10.1109/ICIRCA48905.2020.9183072](https://doi.org/10.1109/ICIRCA48905.2020.9183072)*

УДК 004.891.2

Абдуллаева Б.Ж.², Құрмансейіт М.Б.¹,
 Тунгатарова М.С.¹, Айжулов Д.Е.¹,
 Шаяхметов Н.М.¹
¹ Қ.И.Сәтбаев атындағы
 Қазақ ұлттық ғылыми-зерттеу
 техникалық университеті
² Әл-Фараби атындағы
 Қазақ ұлттық университеті

УРАНДЫ ЖЕРАСТЫ ҰҢҒЫМАЛЫ ШАЙМАЛАУ ПРОЦЕСІН САНДЫҚ МОДЕЛЬДЕУДІ ЖЕДЕЛДЕТУ: КЕРІ САЛМАҚТЫҚ АРАҚАШЫҚТЫҚ ИНТЕРПОЛЯЦИЯСЫ ӘДІСІ МЕН НЕЙРОНДЫҚ ЖЕЛІЛЕРДІ ҚОЛДАНУ АРҚЫЛЫ ГИДРАВЛИКАЛЫҚ ҚЫСЫМ ТЕҢДЕУІН ШЕШУ

Жерасты ұңғымалы шаймалау (ЖҰШ) әдісі уранның инфильтрациялық типтегі кен орындарын игеруде кеңінен қолданылады. Бұл әдіс минерал концентрациясы төмен, өткізгіштігі жоғары жыныстар үшін экологиялық және экономикалық тиімділігімен ерекшеленеді. ЖҰШ әдісінде ұңғымалар арқылы сілтісіздендіру ерітіндісін қабатқа айдап, уранды тікелей жер қойнауында ерітіп, кейіннен өндіруші ұңғымалар арқылы өнімді ерітіндіні сорып алады.

Қазіргі уақытта ЖҰШ үшін жарамды уран қорының азаюына байланысты уран өндіруді егжей-тегжейлі зерттеу қажеттілігі туындайды. Бұған геологиялық барлау кезеңінде қорларды есептеудің және кен орындарын игерудің дәлдігін арттыру мақсатында, сонымен қатар пайдалы қазбалардың оңтайлы режимдерін таңдау үшін пайдалану кезеңінде модельдеу әдістерін қолдану арқылы қол жеткізуге болады. Дәстүрлі есептеу әдістерінің негізгі қиындығы – даму үлгілері немесе алдыңғы деректермен сәйкестендіру (history matching) үшін қажетті үлкен есептеу уақыты [1,2].

Гидродинамикалық процесс массаның сақталу (1) және Дарси (2) заңдарымен сипатталады [2]:

$$\operatorname{div} u = \operatorname{in} Q \operatorname{in} x - x_{\operatorname{in}}, y - y_{\operatorname{in}} + \operatorname{pr} Q \operatorname{pr} \delta(x - x_{\operatorname{pr}}, y - y_{\operatorname{pr}}) \quad (1)$$

$$u = -K f \operatorname{grad} (H) \quad (2)$$

мұнда u [м.с⁻¹] – ағын жылдамдығы, [м³.м⁻³] – кеуектілік, $\operatorname{in} Q \operatorname{in} x - x_{\operatorname{in}}, y - y_{\operatorname{in}} + \operatorname{pr} Q \operatorname{pr} \delta(x - x_{\operatorname{pr}}, y - y_{\operatorname{pr}})$ [с⁻¹] – ұңғымалардағы шығынды сипаттайтын шама: айдау ұңғымалары үшін оң, ал сорғы ұңғымалары үшін теріс мәнге ие, x, y – Дирактың дельта-функциясы, Kf – жыныстың фильтрация коэффициенті, grad [м⁻¹] – градиент операторы, div [м⁻¹] – дивергенция операторы. (1) және (2) теңдеулерді түрлендіру арқылы гидравликалық қысымды есептейтін эллиптикалық дифференциалдық теңдеу (3) алынады:

$$\operatorname{div} -K f \operatorname{grad} (H) = \operatorname{in} Q \operatorname{in} x - x_{\operatorname{in}}, y - y_{\operatorname{in}} + \operatorname{pr} Q \operatorname{pr} \delta(x - x_{\operatorname{pr}}, y - y_{\operatorname{pr}}) \quad (3)$$

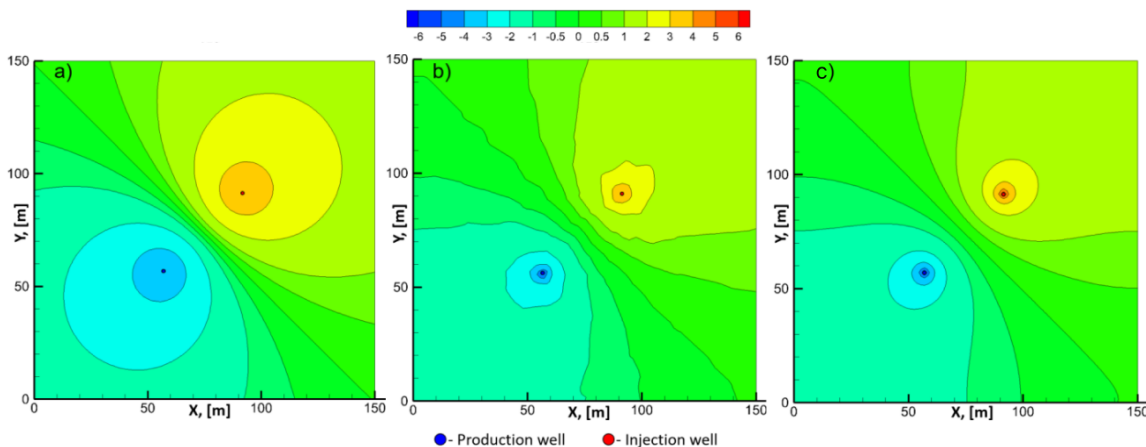
Эллиптикалық теңдеудің табиғатын ескере отырып, тіпті бір ұңғымадағы ағын жылдамдығының өзгеруі итерациялық шешім әдістерін қажет ететіндіктен, әрбір уақыт қадамында гидравликалық қысым теңдеуін қайта есептеу қажет болады, бұл өз кезегінде есептеу уақытын едәуір арттырады. Бұл мақалада қысым теңдеуін есептеу уақытын жеделдету мақсатында интерполяция және машиналық оқыту әдістері арқылы бастапқы жуықтауды анықтау тәсілдері қарастырылады.

Бастапқы жуықтауды табу үшін кері салмақтық арақашықтық әдісі (КСА) қолданылды. Бұл әдісте белгісіз нүктедегі мән көрші нүктелердің белгілі мәндерінің қашықтыққа байланысты салмақталған қосындысы ретінде анықталады [3]:

$$H^*_x = \frac{1}{\sum_{j=1}^n d_{ij}^p} \sum_{j=1}^n \frac{H_j}{d_{ij}^p} \quad (4)$$

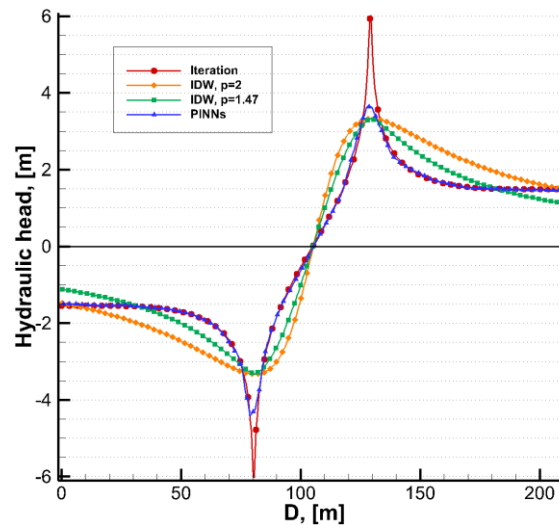
мұнда H^*_x – аймақтың кездейсоқ x түйініндегі гидродинамикалық қысымның белгісіз мәні, H_j – ұңғымаларға сәйкес келетін x_j түйіндеріндегі гидравликалық қысымның белгілі мәндері, d_i – x кездейсоқ түйіні мен гидравликалық қысым мәні белгілі x_j түйіні арасындағы қашықтық, p – қуат параметрі.

1-суретте IDW әдісімен (a) және жоғарғы релаксация (SOR) итерациялық әдісімен (b) есептелген қысымның таралуы көрсетілген. IDW интерполяциясын бастапқы жуықтау ретінде пайдалану итерациялар санын 3123-тен 2564-ке дейін азайтып, есептеу уақытын 2.1 есе қысқартты.



1 сурет. 101×101 есептік торда КСА интерполяция әдісімен (a), PINN әдісімен (b) және жоғарғы релаксация (c) итерациялық әдісімен 50 метр қашықтықтағы ұңғымалар үшін анықталған гидравликалық қысымның таралуы

Бастапқы жуықтауды табу үшін Physics-Informed Neural Networks (PINN) әдісі қолданылды. Бұл әдіс нейрондық желіні физикалық заңдармен біріктіру арқылы гидравликалық қысымды дәл болжауға мүмкіндік береді. Дәстүрлі әдістерден айырмашылығы, PINNs математикалық процестің моделін нейрондық желінің шығын функциясына біріктіреді [4].



2 сурет. Диагональ бойымен гидравликалық қысымның таралуы: итерациялық әдіспен анықталған (қызыл сызық), КСА әдісімен $p=2$ (қызғылт сары сызық), $p=1.47$ (жасыл сызық) және PINN әдісімен есептелген (көк сызық)

Бұл зерттеу гидравликалық қысым өрісін есептеуді жеделдету үшін PINNs әдісін қолданудың тиімділігін көрсетті. PINNs әдісі IDW-мен салыстырғанда есептеу уақытын 2,8–7,10 есеге қысқартты және қателікті азайтты, бұл оның дәлірек және тұрақты әдіс екенін дәлелдейді. PINNs-тің артықшылығы – есептеу жүктемесін төмендетіп, бастапқы жуықтауды дәлірек анықтауында. Бұл жұмыста қос ұңғымалы қарапайым модель қарастырылғанымен, PINNs-ті күрделі кен орны жағдайларына қолдануға болады.

Пайдаланылған әдебиеттер

1. Collet, A.; Regnault, O.; Ozhogin, A.; Imantayeva, A.; Garnier, L. Three-dimensional reactive transport simulation of Uranium in situ recovery: Large-scale well field applications in Shu Saryssu Basin, Tortkuduk deposit (Kazakhstan). *Hydrometallurgy* **2022**, 211, 105873. [[Google Scholar](#)] [[CrossRef](#)]
2. Kurmanseit, M.B.; Tungatarova, M.S.; Kaltayev, A.; Royer, J.-J. Reactive Transport Modeling during Uranium In Situ Leaching (ISL): The Effects of Ore Composition on Mining Recovery. *Minerals* **2022**, 12, 1340. [[Google Scholar](#)] [[CrossRef](#)]
3. Li, Z.; Wang, K.; Ma, H.; Wu, Y. An Adjusted Inverse Distance Weighted Spatial Interpolation Method. *Adv. Comput. Sci. Res.* **2018**, 65, 128–132. [[Google Scholar](#)] [[CrossRef](#)]
4. Ramos, D.J.; Cunha, B.Z.; Daniel, G.B. Evaluation of physics-informed neural networks (PINN) in the solution of the Reynolds equation. *J. Braz. Soc. Mech. Sci. Eng.* **2023**, 45, 568. [[Google Scholar](#)] [[CrossRef](#)]

ӨОЖ 004.056

Абаева А.Р. (Астана, ЕНУ им.
Л.Н.Гуми Улева)

АНТИФОРЕНЗИКА ӘДІСТЕРІН ЗЕРТТЕУ ЖӘНЕ ОЛАРДЫҢ ЦИФРЛЫҚ ТЕРГЕУГЕ ӘСЕРІ

Аннотация: Бұл мақала цифрлық тергеуден жалтару үшін қолданылатын антифорензика әдістеріне арналған. Сандық құрылғылардың көбеюімен криминалистикалық зерттеулер құқық қорғау органдары үшін маңызды құралға айналды. Алайда, қылмыскерлер өз әрекеттерін жасыру және бақылауды қиындату үшін озық әдістерді қолданады. Анти-форензикаға сандық іздерді жасыруға және тергеушілерді шатастыруға бағытталған әдістер кіреді. Мақалада стеганография, шифрлау және спуфинг сияқты жалпы әдістерге шолу жасалады. Бұл әдістердің техникалық аспектілері, олардың тиімділігі және анықтау мен бейтараптандыруға қарсы шаралар қарастырылады. Нәтижелер күрделі криминалистикалық әдістерге қарсы тұру үшін жаңа криминалистикалық құралдарды әзірлеу қажеттілігін көрсетеді. Қорытындыда анти-криминалистика саласындағы болашақ зерттеулердің бағыттары және олардың цифрлық тергеулер мен киберқылмыспен күресу үшін маңызы анықталды.

Кілт сөздер: цифрлық криминалистика, анти-форензика, шифрлау, стенография, спуфинг, сегменттеу.

Сандық дәлелдер қазіргі тергеу процестерінде шешуші рөл атқарады және оларды жинау, талдау және сақтау мамандандырылған электронды құралдар арқылы жүзеге асырылады. Бұл тұрғыда «Әрбір өзара әрекеттесу із қалдырады» деген Локард принципі қатты дискілерде, құрылғылардың жадында және бұлтты сақтауда сақталған сандық дәлелдерге де қатысты. Бұл деректер қылмыскерлерді анықтау және қылмысқа байланысты оқиғалардың хронологиясын қалпына келтіру үшін қажет.

Сандық криминалистика мамандары бұл дәлелдерді мұқият жинап, оларды қылмыс кезінде жасалған әрекеттерді түсінудің маңызды құралына айналатын есептемелер шығарады. Алайда, сәтті тергеу жолында елеулі кедергілер туындауы мүмкін. Шифрлау және цифрлық су белгілері сияқты деректерді қорғаудың заманауи әдістері тергеу барысында алынған құрылғыларда сақталса да маңызды ақпаратқа қол жеткізуді қиындатуы немесе тіпті бұғаттауы мүмкін. Бұл әдістердің құпиялылықты қорғау сияқты заңды мақсаттары болса да, оларды қылмыскерлер өз әрекеттерінің іздерін жасыру үшін де пайдаланады. Мұндай технологияларды қолдану құқық қорғау органдары мен цифрлық криминалистика саласында жұмыс істейтін мамандар үшін үлкен қиындықтар туғызады. Бұл деректерді қорғау әдістерінің тиімділігі негізінен белгісіз болып қалады, өйткені практикалық зерттеулердің болмауына байланысты олардың нақты тергеу процестеріне қалай әсер ететінін дәл бағалау қиын.

Криминалистер озық технологияларды белсенді пайдалана отырып, өз тергеулерінің тиімділігі мен сенімділігін арттыру үшін үнемі жаңа әдістерді дамытып, енгізуде. Алайда, киберқылмыспен айналысатын қылмыскерлер артта қалмайды, сонымен қатар тергеушілердің жұмысын қиындататын күрделі әдістерді дамыта отырып, технологияның ең заманауи жетістіктерін қолданады. Бұл әдістер қылмысты ашуға көмектесетін деректерді жасыруға бағытталған анти-криминалистикалық стратегиялар деп аталды.

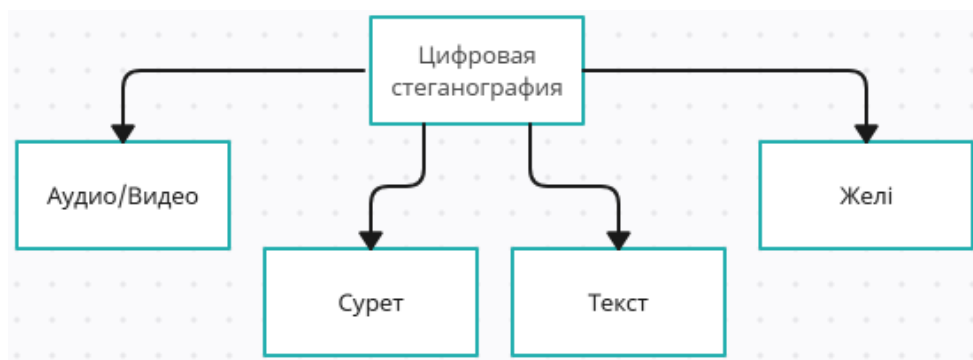
Деректерді жасыру криминалистикамен күресудің негізгі стратегияларының бірі болып табылады. Бұл стратегияның бір бөлігі ретінде қылмыскерлер маңызды дәлелдерді жасыру үшін әртүрлі әдістерді қолданады. Деректерді жасырудың кең таралған әдістерінің қатарына шифрлау, стеганография және спуфинг жатады. Зерттеулер көрсеткендей, киберқылмыскерлер сандық дәлелдемелерді анықтау мен жинауды болдырмау үшін обфускацияны (деректерді шатастыру) және шифрлауды жиі қолданады. Бұл оларға тергеушілер үшін маңызды ақпаратқа қол жеткізуді

бұғаттауға мүмкіндік береді, сонымен бірге бұл деректерді өз қажеттіліктері үшін пайдалану мүмкіндігін сақтайды.

Шифрлау-бұл ақпараттың құпиялылығын қамтамасыз ету үшін де, құқық қорғау органдары жүргізетін тергеулерді қиындату үшін де кеңінен қолданылатын деректерді рұқсатсыз кіруден қорғау әдісі. Бұл әдіс деректердің бар екендігін жасырмайды, бірақ оны декодтау үшін қажетті кілттері жоқ адамдар үшін оқылмайтын етеді. Жалпыға қол жетімді шифрлау бағдарламалары мен құралдарының қол жетімділігімен қылмыскерлер файлдарды немесе бүкіл дискілерді заманауи алгоритмдерді қолдана отырып оңай шифрлай алады, бұл тиісті кілтсіз шифрды шешуді мүмкін емес етеді.

Тапсырмаларға байланысты шифрлаудың екі түрі болуы мүмкін. Біріншісі-файлдың мазмұнын шифрланған мәтінге айналдыратын файлды шифрлау, ол дұрыс кілтті пайдаланып шифрды шешкеннен кейін ғана қол жетімді. Екіншісі-деректерді сақтаудың бүкіл бөлімін қамтитын дискіні шифрлау және оған қол жеткізу үшін шифрды ашу кілті қажет. VeraCrypt және CipherShed сияқты бағдарламалар ақпаратты қорғаудың жоғары деңгейін қамтамасыз ете отырып, осы екі шифрлау әдісін де қолдануға мүмкіндік береді. АҚШ-та Федералды тергеу бюросы (FBI) тергеу барысында шифрланған деректерге қол жеткізудің күрделі мәселесіне тап болды. 2016 жылғы есепте күшті шифрлау әдістерін қолдану салдарынан тәркіленген құрылғылардың шамамен 30% шифрды шешуге болмайтындығы көрсетілген. 2018 жылы жарияланған тағы бір есепте тәркіленген 7 800-ден астам құрылғының 6 900-ге жуығының шифры шешілмегендігі туралы хабарланған. Бұл деректер киберқылмыс пен цифрлық іздермен байланысты қылмыстарды тергеу кезінде бүкіл әлемдегі құқық қорғау органдарының алдында тұрған мәселенің ауқымын көрсетеді.

Стеганография-бұл тергеушілердің анықтауын қиындату үшін басқа құпия емес деректердің ішінде деректерді жасыруды қамтитын әдіс. Бұл әдісті әдетте компьютерлік қылмыскерлер деректерді анықтауға және алуға жол бермеу үшін тергеуге қарсы стратегия ретінде қолданады. Стеганография жасырын ақпаратты суреттер, бейнелер және аудио файлдар сияқты сандық медиаға енгізуді қамтиды. Бұған сандық медианың кіші биттерін (LSB) бастапқы деректерді айтарлықтай өзгертпестен жасырын деректерді қамтитын етіп өзгерту арқылы қол жеткізуге болады. Стеганографияны криминалистикалық әдістерде қолдану тергеушілерге жасырын деректерді табуды және алуды қиындатады, өйткені олар көбінесе жақсы жасырылған және бастапқы деректерден ажырату қиын. Компьютерлік қылмыскерлер деректерді жасыру үшін қолдана алатын стеганография құралдарының кейбір мысалдарына OpenStego, StegHide және SilentEye жатады.



1-сурет. Цифрлық стеганография.

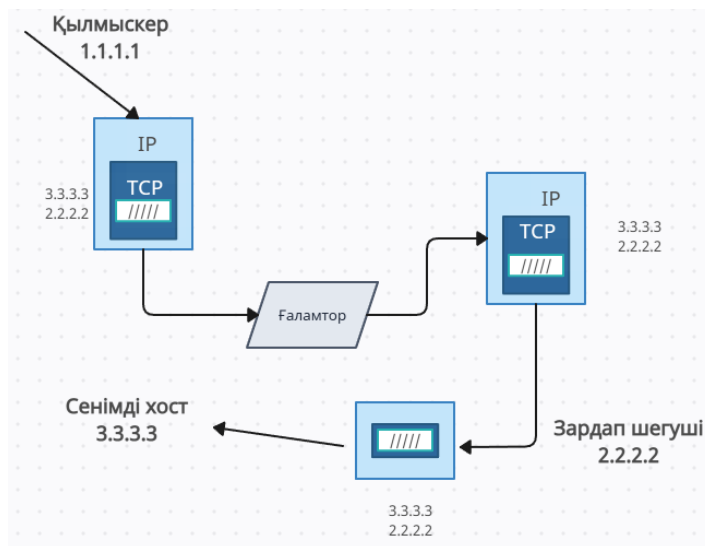
Спуфинг-бұл киберқылмыскерлер өздерінің жеке басын жасыру және тергеуден жалтару үшін жиі қолданатын әдіс. Ол деректерді басқа, жалған көзден шыққан сияқты көрініп, осы

деректердің шығу тегі туралы жалған әсер қалдыратындай етіп басқарудан тұрады. Жалғандық IP мекенжайларын, MAC мекенжайларын, электрондық пошта мекенжайларын немесе телефон нөмірлерін бұрмалау сияқты әртүрлі нысандарда көрінуі мүмкін. Ауыстырудың ең кең таралған әдістерінің бірі-жіберушінің шынайы жеке басын жасыру үшін пакеттің бастапқы мекенжайын - IP мекенжайын ауыстыру. Бұл әсіресе DDoS (қызмет көрсетуден бас тарту), спам жіберу немесе фишингтік шабуылдар кезінде таратылған шабуылдарды бастағанда жиі қолданылады.

Сонымен қатар, жалған деректер анти-форензикада маңызды рөл атқарады, мұнда қылмыскерлер өз әрекеттерінің іздерін жасыруға және ашудан аулақ болуға тырысады. Деректерін ауыстыру арқылы олар криминалистерге шабуылдың немесе нақты қылмыскердің көзін анықтауға кедергі келтіріп, оларды едәуір қиындатады. Мысалы, қылмыскерлер шабуыл жасау үшін пайдаланылған құрылғының IP мекенжайын ауыстыра алады немесе өздерінің жеке басын және орналасқан жерін жасыру үшін VPN немесе Tor сияқты анонимді қызметтерді пайдалана алады.

Атап өткендей, бұл әдіс алаяқтық фишингтік шабуылдарда белсенді қолданылады, мұнда қылмыскерлер жалған веб-сайттар немесе пайдаланушыларды құпия ақпаратты ашуға алдау үшін ресми болып көрінетін электрондық хаттар жасайды. Заңды ұйымға қатысты электрондық пошта мекенжайын немесе URL мекенжайын өзгерту арқылы шабуылдаушылар адамдарды сенімді дереккөзбен байланысып жатырмыз деп алдайды.

Тұтастай алғанда, спуфинг зиянды мақсаттар үшін де, тергеушілерден қылмыстық әрекеттерді жасыру үшін де қолдануға болатын күшті құрал болып табылады. Бұл алаяқтық қауіпсіздікке үлкен қауіп төндіреді және ұйымдар мұндай шабуылдардан қорғану үшін шаралар қабылдауы керек, ал мамандар шабуылдардың шынайы көздерін дұрыс анықтау және қадағалау үшін тергеу кезінде қырағылық танытуы керек.



2-сурет. IP спуфинг.

Қылмыскерлер өздерінің іс-әрекеттерінің іздерін жасыру және тергеушілердің жұмысын қиындату арқылы криминалистикалық сараптамадан қорғану үшін қолдана алатын әртүрлі құралдар мен әдістер бар. Міне, осындай құралдардың бірнеше мысалдары:

- CCleaner: бұл уақытша файлдарды, шолғыш тарихын және басқа сандық артефактілерді жоюға арналған танымал құрал, оларды пайдаланушының белсенділік іздерін қалпына келтіру үшін пайдалануға болады.

- BleachBit: CCleaner-ге ұқсас құрал, ол сонымен қатар сандық іздерді, соның ішінде іздеу журналын, кэшті, кукиді және компьютердегі басқа белсенділік іздерін тазартады.

- VeraCrypt: құпия сөз болған кезде ғана қол жетімді шифрланған көлемдерді жасауға мүмкіндік беретін деректерді шифрлау бағдарламасы. Бұл деректерді криминалистикалық сараптамадан жасыруға көмектеседі, олардың тиісті кілтсіз қол жетімділігін қиындатады.

- Tor Browser: пайдаланушының нақты IP мекенжайын жасыру және оның трафигін шифрлау арқылы интернеттегі анонимділікті қамтамасыз ететін шолғыш. Бұл құрал интернеттегі әрекеттерді жасыру және бақылауды болдырмау үшін қолданылады.

Сонымен қатар, файлдардың метадеректерін жою және манипуляциялау әдістерін қамтитын анти-форензика (AFT) мамандандырылған құралдарының тұтас жиынтығы бар, бұл қылмыстық іс-әрекет фактілерін қалпына келтіруге тырысатын криминалистердің жұмысын қиындатады. Алайда, криминалистер мұндай жасыру әдістерімен күресте қарусыз қалмайды. Олар әртүрлі қарсы шараларды қолдана алады, мысалы:

- Жадты талдау арқылы шабуылдаушылар файлдарды жоюға немесе жасыруға тырысса да, жұмыс істеп тұрған процестерді анықтау.

- Жойылған файлдарды қалпына келтіру үшін деректер өшірілсе де немесе қайта жазылса да қайтаруға мүмкіндік беретін арнайы бағдарламаларды қолдану.

- Метадеректерді талдау арқылы уақыт белгілерін өзгерту немесе нақты ақпаратты жасыру сияқты манипуляцияларды анықтау.

Тиімді талдау үшін мамандар киберқылмыстарға қарсы тұрудың ең жаңа әдістерін біліп, талдау әдістерін заманауи қиындықтарға бейімдеуі керек. Бұл қылмыскерлерді анықтап қана қоймай, шабуылдаушылар анти-форензика әдістері арқылы жасыруға тырысқан маңызды дәлелдерді қалпына келтіруге мүмкіндік береді.

Киберқылмыскерлердің криминалистикалық әдістерді қолдануының артуына жауап ретінде мамандар зерттеудің тиімділігін арттыру үшін қарсы стратегияларды енгізуі керек. Негізгі тәсілдердің бірі-жасырын трафик немесе стандартты емес кіру схемалары сияқты әдеттен тыс әрекеттерді жедел анықтауға және ықтимал қауіптерге уақтылы жауап беруге мүмкіндік беретін нақты уақыттағы бақылау. Сонымен қатар, бүлінген деректерді қалпына келтіруде және күдікті әрекеттерді анықтауда, сондай-ақ өзгерістерді бақылауда және маңызды ақпаратты қалпына келтіруде шешуші рөл атқаратын аудиторлық журналдар мен тұрақты сақтық көшірмелер сияқты криминалистикалық бақылау құралдарын енгізу маңызды, тіпті егер ол ішінара жойылған немесе өзгертілген болса да.

EnCase, FTK және Autopsy сияқты сандық криминалистикалық құралдар жойылған деректерді қалпына келтіруге, стеганографияны анықтауға және шифрланған файлдарды талдауға мүмкіндік береді, бұл мамандарға жасырын немесе бүлінуі мүмкін сандық іздерге терең қол жеткізуге мүмкіндік береді. Деректердің қауіпсіздігін арттыру үшін желіні сегменттеу маңызды, оларға қол жетімділікті шектеу және шабуыл кезінде ықтимал зиянды азайту үшін маңызды жүйелерді жеке сегменттерге бөлу керек. Сонымен қатар, қызметкерлерді анти-форензика әдістерімен байланысты тәуекелдер туралы оқыту және хабардар ету, оларды пайдалануды жеңілдететін күтпеген әрекеттердің ықтималдығын азайтуға көмектеседі. Қызметкерлерді ықтимал қауіптер мен қорғаныс әдістері туралы үнемі хабардар ету адам факторына байланысты тәуекелдерді азайтуға көмектеседі.

Киберқауіптердің және анти-форензика әдістерінің қарқынды дамуы жағдайында цифрлық қылмыстарды тиімді тергеу қарсы іс-қимылдың кешенді және бейімделген стратегияларын енгізуді талап етеді. Мұндай тәсілдерді қолдану сандық тергеу мамандарына шабуылдаушылардың іздерін жасыру әрекеттеріне қарамастан қылмыстарды тиімді анықтауға және ашуға мүмкіндік береді. Цифрлық қауіптердің күрделене түсуімен және құқық қорғау органдарының шектеулі ресурстарымен тергеудің сәттілігі көбінесе тергеушілердің жаңа

қиындықтарға бейімделу, заманауи құралдар мен тәсілдерді қолдану және басқа цифрлық қауіпсіздік мамандарымен ынтымақтастықты дамыту қабілетіне байланысты. Осылайша, бұл стратегияларды қолдану киберқылмыспен күресудің тиімділігін арттырып қана қоймайды, сонымен қатар ұйымдар мен жалпы қоғам үшін қауіпсіз цифрлық ортаны құруға ықпал етеді.

Пайдаланылған әдебиеттер тізімі

1. Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Academic Press.
2. Garfinkel, S. (2010). *Digital Forensics Research: The Next 10 Years*. *Digital Investigation*, 7, S64–S73.
3. Harris, R. (2006). Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. *Digital Investigation*, 3(Suppl. 1), S44–S49.
4. Mermoud, G., & Le-Khac, N.-A. (2018). *Anti-Forensics Techniques: Methods, Detection, and Countermeasures*. Springer.
5. Rogers, M. (2005). *Anti-Forensics Techniques and Their Impact on Computer Forensics Investigation*. *International Journal of Digital Evidence*, 4(1).
6. Zeltser, L. (2017). *Anti-Forensics: Techniques, Detection, and Prevention*. SANS Institute.
7. Досжанова, А. (2021). Цифрлық криминалистика және антифорензикалық әдістердің даму тенденциялары. *Қазақстан Республикасы ИМ журналы*, 2, 45-52.

УДК 004.912

Абдығалым Б.Х. (Астана, ЕНУ имени Л. Н. Гумилева)
Самбетбаева М.А. (Астана, ЕНУ имени Л. Н. Гумилева)

ФОРМИРОВАНИЕ ОНТОЛОГИИ ВОЕННОЙ ТЕРМИНОЛОГИИ В ЦЕЛЯХ СЕМАНТИЧЕСКОГО АНАЛИЗА ИНФОРМАЦИИ В СУХОПУТНЫХ ВОЙСКАХ.

В условиях активного развития военных информационных систем особую значимость приобретает формализация и структурирование военных знаний. Данная работа содержит разработку семантической онтологии военной терминологии, призванной провести анализ информации для нужд сухопутных войск. В силу роста количеством данных и усложнении военных задач, все большее значение приобретает структурирование и формализация связей понятий. В качестве вспомогательных средств для решения этой задачи была разработана онтология в системе Protégé, которая содержит иерархическую структуру слов и контекстно-зависимые отношения. Использование SPARQL-запросов и технологий Semantic Web позволяет автоматизировать задачи поиска, агрегации и анализа информации, тем самым повышая уровень организованности и результативности в процессе решения управленческих задач военного характера.

Одним из основных направлений основ гражданской информатизации стало увеличение объемов информации, сложность боевых действий и многопрофильность командировочных и штабных работ [1]. Системная организация и представление военных знаний представляется все

более важной, и базируется на информационных технологиях. Среди множества задач, наиболее приоритетной представляется грамотная работа со знаниями о вооружении, технике, операциях и терминологии, принятых в сухопутных войсках.

Высокий уровень сложности, связанный с военным языком, представляет собой многоуровневую систему понятий и связей, которые изолированы от окружающей среды [2]. Это делает использование различных источников данных, автоматизацию аналитических процедур и создание единой информационной системы, помогающей принимать решения, чрезвычайно сложной задачей. Они используют информацию более разумно и эффективно, в то время как их методы ее обработки недостаточны и неэффективны.

Один из подходов таких - создание онтологического моделирования, которое представляет собой или определение структуры, управляющей областью и ее компонентами. Онтологии, как инструменты представления знаний, сохраняют терминологическую неоднозначность, позволяют повторно использовать знания, впоследствии интеграцию данных из различных источников и помогают в семантическом поиске. В последние годы онтологии широко используются в областях биоинформатики, семантической паутины и искусственного интеллекта. Военные процессы также все чаще используются для анализа [3].

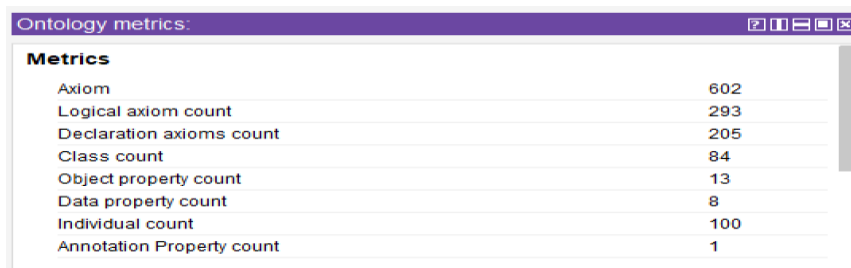
Целью исследования является создание онтологии военных терминов для сухопутных войск, чтобы повысить эффективность обработки семантической информации и предложить интеллектуальную помощь в принятии решений. Используя программное обеспечение Protégé, язык OWL и технологии семантического веба, в статье описываются ключевые этапы создания онтологической модели. Повышение точности извлечения информации и применимости аналитических методов в военной области стало возможным благодаря иерархической структуре предлагаемой онтологии, которая отражает важные понятия и их контекстно-адаптивные взаимосвязи.

Разработка онтологической модели терминологии сухопутных войск велась в соответствии с общей идеей онтологического моделирования, рассчитанной на систематизацию ключевых понятий и установление семантических связей между ними. Базой для формализации предметной области послужили результаты анализа нормативных документов, специализированной военной литературы, а также экспертных консультаций. Такой подход обеспечил репрезентативность и прикладную направленность онтологии, что особенно важно для её интеграции в систему военного анализа и поддержки принятия решений.

Создание онтологии было разделено на несколько этапов: сбор и отбор терминов, разграничение понятий, формализация отношений между ними и создание логической структуры на языке OWL. В качестве основного средства разработки был выбран Protégé 5.6.5, который является мощным инструментом, применяемым для реализации иерархических структур знаний, применимых к использованию стандартов семантического веба. Разработанная модель включает в себя 84 класса, соответствующих основным понятиям военной терминологии, а также 13 свойств объектов, обозначающих семантические связи между ними (рисунок 1).

Кроме того, реализованы свойства данных, элементы аннотаций и отдельные экземпляры для обеспечения гибкости при использовании модели в различных информационных системах.

Онтология включает структурированную иерархию классов, представляющих ключевые концепции военной терминологии. Разработанные в рамках онтологической модели военной терминологии, позволяют извлекать из онтологии важные сведения, относящиеся к структуре военных подразделений, характеристикам боевой техники, а также к отношениям между сущностями. Эти запросы подтверждают корректность онтологической структуры, демонстрируют её информационную наполненность и позволяют эффективно анализировать взаимосвязи внутри онтологии.



Metrics	
Axiom	602
Logical axiom count	293
Declaration axioms count	205
Class count	84
Object property count	13
Data property count	8
Individual count	100
Annotation Property count	1

Рисунок 1. Показатели предлагаемой онтологии

Онтология также позволяет взаимодействие с конечными пользователями через интерфейс, который принимает как текстовые, так и математически сформулированные запросы. Таким образом, она становится удобной не только для ИТ-специалистов, но и для военных аналитиков, инструкторов, стажеров и разработчиков пользовательского программного обеспечения. Особенности архитектуры и методологии проектирования делают модель универсальным инструментом для разработки военных систем, основанных на семантической, интеллектуальной обработке данных и интеграции с аналитическими платформами, управляемыми ИИ.

В данном исследовании была создана онтология военной терминологии для нужд пограничных сухопутных войск с целью компьютерного семантического знания и анализа ситуации. Эта модель поможет с концептуальными структурами и связанными с ними характеристиками при использовании самых современных методов онтологического моделирования. Для достижения максимального уровня простоты и эффективности, это позволяет разработать онтологию для анализа на основе намерений в военной области, которая имеет расширяемую и адаптируемую структуру.

Использованная литература:

6. J. Y. Ding, Q. S. Zhao and B. Y. Xia, "Research on the construction method of weapon equipment knowledge graph based on open source data", *Command Control and Simulation.*, vol. 40, no. 002, pp. 22-26, 2018.
7. C. X. Mei, F. H. Duan and F. Deng, "Method for Constructing Knowledge Graph of Military Equipment", *CN111309925A[P]*, 2020.
8. D. Y. Li, J. Sheng and Y. X. Liu, "Military weapon question answering system based on knowledge graph", *Command Information System and Technology*, vol. 11, no. 65

ӨОЖ 004.8:616.89

Амирбай Айзат Айтуғанқызы
Л.Н. Гумилев атындағы Еуразия ұлттық университет, докторант
Муханова Аяғоз Асанбековна
Л.Н. Гумилев атындағы Еуразия ұлттық университет, PhD
Астана, Қазақстан

АУТИЗМ БЕЛГІЛЕРІН ЕРТЕ АНЫҚТАУ МАҚСАТЫНДА КӨЗ ҚОЗҒАЛЫСЫН ТАЛДАУҒА НЕГІЗДЕЛГЕН ТЕРЕҢ ОҚЫТУ МОДЕЛЬДЕРІН ҚОЛДАНУ

Мақалада аутизм спектрі бұзылыстарын (АСБ) диагностикалауға [1] арналған екі терең оқыту алгоритмінің – ұзақ қысқа мерзімді жад пен нейрондық желіге LSTM және CNN негізделген модельдің және ұзақ қысқа мерзімді жад пен автоэнкодерге LSTM және автоэнкодер негізделген модельдің әзірленуі мен бағалау нәтижелері ұсынылады. Деректерді жинау үшін

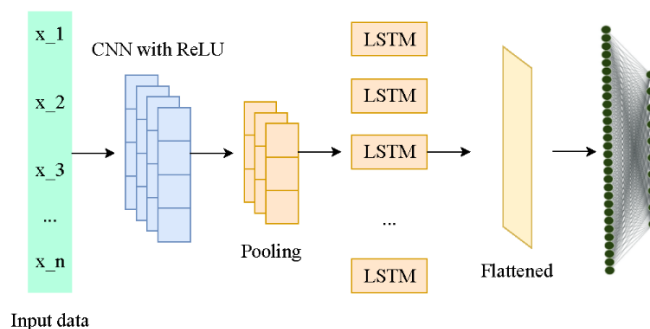
қатысушылардың визуалды назарын анимациялық нысандарды бақылау кезінде тіркейтін көз қозғалысын бақылау - eye tracking қосымшасы пайдаланылды. Жиналған деректер .pru форматында өңделіп, ұсынылған модельдер арқылы талданды.

Зерттеудің негізгі мақсаты – АСБ диагностикасының дәлдігін арттыру болып табылады. Алгоритмдердің тиімділігін бағалау [2] нәтижесінде LSTM және автоэнкодерге негізделген модельдің жасырын тәуелділіктерді анықтаудағы қабілеті жоғары екені анықталды. LSTM+CNN моделі оқыту деректерінде 90% және валидациялық деректерде 85% дәлдік көрсетсе, LSTM+AE моделі тиісінше 95% және 93% дәлдікке қол жеткізді. Мақалада әзірленген алгоритмдердің клиникалық қолданысы және болашақ зерттеулердің перспективалық бағыттары қарастырылады. Зерттеуде АСБ-ны ерте кезеңде анықтаудың маңыздылығы атап өтіледі, өйткені бұл тиімді емдеу стратегияларын әзірлеуге және пациенттердің өмір сапасын арттыруға мүмкіндік береді. АСБ саны артуы мен ерте анықтаудың күрделілігін ескере отырып, мақалада дәстүрлі, жиі субъективті сипатқа ие диагностикалық әдістерге балама нұсқаларды ұсынуға ұмтылады.

Ұсынылған LSTM мен CNN және автоэнкодерді біріктіретін үлгілер визуалды стимулдармен өзара әрекеттесу кезінде жиналған мінез-құлықтық және физиологиялық деректерді жоғары дәлдікпен талдауға мүмкіндік береді. Көз қозғалыстарын биомаркерлер ретінде қолдану дәстүрлі әдістердің субъективтілігін азайтып, диагностикалық үдерісті автоматтандыруға жағдай жасайды. Зерттеу көз фиксациясы мен саккадаларын талдауға негізделген, бұл PAC бар балалардың қабылдау және назар аудару ерекшеліктерін анықтауға мүмкіндік береді, әрі бұл Rahal R. M., Spering M. және Carrette R. Еңбектеріне [3] сүйенеді. Ұсынылған алгоритмдер логистикалық регрессия, кездейсоқ ормандар және SVM секілді әртүрлі машиналық оқыту әдістерін қолдану арқылы AUC көрсеткішін 92%-ға дейін жеткізді. Визуалды назар мен жасанды интеллектіні біріктіру классификация дәлдігін 90%-ға дейін арттыруға мүмкіндік берді, бұл әдістің болашағы зор екенін көрсетеді. Алынған нәтижелер клиникалық тәжірибеде қолдануға бейімделе алады және АСБ-ны объективті, жедел әрі қолжетімді диагностикалауға ықпал етеді.

Әдіс. Деректерді жинау үшін экран бетінде бейберекет қозғалатын шар анимациясы негізінде арнайы бағдарлама әзірленді, бұл қатысушылардың көз қозғалысы траекторияларын eye tracking технологиясы арқылы тіркеуге мүмкіндік берді. Зерттеуге АСБ бойынша алдын ала диагноз қойылған бақылау тобындағы адамдар қатысып, олардың деректері модельдерді оқыту [4-5] үшін пайдаланылды. Терең оқыту алгоритмдері қолданылды: кеңістіктік сипаттамаларды талдау үшін – CNN, ал уақыттық деректер тізбегін өңдеу үшін – RNN. Зерттеудің мақсаты – көз қозғалысы паттерндерін жіктеу арқылы АСБ-ға тән белгілерді анықтау.

1-суретте терең оқыту моделінің архитектуралық сызбасы көрсетілген, ол свёрточты нейрондық желілерді (CNN) және ұзақ қысқа мерзімді жадқа ие рекурренттік нейрондық желілерді (LSTM) біріктіреді. Кіріс қабаты көпөлшемді деректерді қабылдайды.

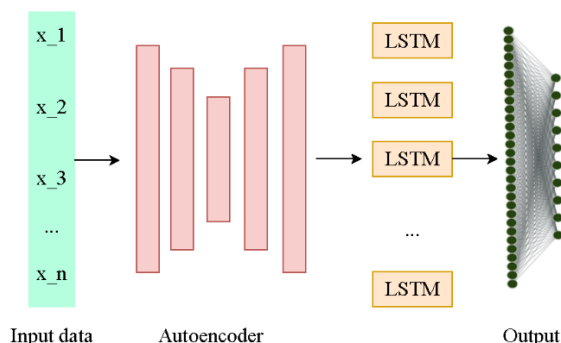


1-сурет. LSTM + CNN моделінің архитектурасы

Сызба нейрондық желілерді (CNN) және ұзақ қысқа мерзімді жадқа негізделген рекурренттік нейрондық желілерді (LSTM) біріктіретін гибриді нейрондық желі архитектурасын бейнелейді. Кіріске көпөлшемді $x_1, x_2, \dots, x_n$ деректері беріліп, олар алдымен кеңістіктік ерекшеліктерді анықтауға арналған ReLU активациялық функциясы бар CNN қабаттарымен өңделеді. ReLU функциясы оқыту үдерісін жылдамдатады және градиенттің жоғалу мәселесінің алдын алады. Одан кейін өлшемділікті төмендетіп, маңызды белгілерді сақтай отырып, модельдің кіріс өзгерістеріне төзімділігін арттыратын пулинг операциясы қолданылады.

Өңделген деректер уақыттық тәуелділіктерді тиімді анықтауға мүмкіндік беретін LSTM рекурренттік қабаттарына берілетін тізбекті құрылымға түрлендіріледі. Соңғы кезеңде LSTM қабаттарының көпөлшемді шығуы бірөлшемді векторға айналдырылып (flattening), логистикалық регрессия сияқты классификациялық модульдерге сәйкес келетін толықбайланысты немесе шығыс қабатына жіберіледі.

2-суретте бастапқы деректер тізбегі алдымен негізгі белгілерді бөліп алу және өлшемділікті қысқарту үшін автоэнкодер арқылы өңделетін LSTM мен автоэнкодерге негізделген модель көрсетілген. Алынған көрініс уақыттық тәуелділіктерді ұстауға қабілетті LSTM қабаттарына жіберіледі, содан кейін деректер бірөлшемді векторға айналдырылып, классификация немесе регрессия жүргізуге арналған шығыс қабатына беріледі. Мұндай архитектура автоэнкодер мен LSTM әдістерінің артықшылықтарын біріктіре отырып, тізбекті деректерді талдау мен болжауда жоғары тиімділікке қол жеткізеді.



2-сурет. LSTM + AE моделінің архитектурасы

. Зерттеу барысында терең оқытуға негізделген екі модель – LSTM+CNN және LSTM+Autoencoder әзірленіп, бағаланды. Алынған нәтижелерге сәйкес, екі модель де жоғары дәлдік, сезімталдық, ерекшелік және AUC мәндерін көрсетті. АСБ-ға қатысты деректерді классификациялау бойынша жүргізілген салыстырмалы талдауда LSTM+Autoencoder моделі барлық негізгі метрикалар бойынша анағұрлым жоғары нәтижелер көрсетті. LSTM+AE моделі оқыту деректерінде 95%, ал валидацияда 93% дейінгі дәлдікке, AUC-ROC мәні бойынша тиісінше 1.00 және 0.98-ге қол жеткізіп, кластарды ажыратудағы жоғары қабілеттілігін және болжамдарының тұрақтылығын дәлелдеді. Бұл нәтижелер, әсіресе клиникалық қолданыс жағдайында жоғары дәлдік пен жалған оң нәтиженің минимизациясы маңызды болған кезде, АСБ диагностикасы міндеттерінде осы модельдің артықшылығын айқын көрсетеді. Алынған бейнелер көз қозғалысын бақылау технологиясын қолдана отырып, аутизм спектрі бұзылыстарын диагностикалауда талдауға жарамды деректерді қамтиды. Бұл деректерді талдау үшін көз

қозғалысы траекториясы мен шар қозғалысы траекториясы арасындағы Евклид қашықтығын есептейтін модель әзірленді, мұнда қалыпты жағдай шардың қозғалыс траекториясынан белгіленген диапазонда көзқарастың орналасуымен анықталады. Мұндағы $P_i = (x_i, y_i)$ — көзқарас траекториясындағы нүкте, ал $Q_i = (a_i, b_i)$ — шар траекториясындағы ең жақын нүкте; олардың арасындағы қашықтық Евклид формуласы бойынша есептеледі.

$$d(P_i, Q_i) = \sqrt{(x_i - a_i)^2 + (y_i - b_i)^2}$$

Көзқарас траекториясы мен шар қозғалысының траекториясы арасындағы қашықтық әрбір нүкте үшін есептеліп, классификацияның негізгі критеріі ретінде қарастырылады, егер барлық мәндер 0–50 пиксель аралығында болса, бұл мінез-құлық қалыпты деп саналады, ал бұл диапазоннан тыс мәндер – АСБ ықтимал белгісі ретінде қарастырылады. Мұндай тәсіл визуалды назардың ауытқуларын сандық тұрғыда бағалауға және АСБ-ға тән көз қозғалысының сипаттық паттерндерін анықтауға мүмкіндік береді. Нәтижелерді талдау көз қозғалысы траекторияларын дәл классификациялау бойынша модельдің жоғары тиімділігін растайды және оның АСБ диагнозын қою үдерісін жеделдету мен нақтылау әлеуетін көрсетеді.

Қорытынды. Көз қозғалысы траекторияларын талдау негізінде құрылған LSTM+CNN және LSTM+Autoencoder модельдері АСБ-ны диагностикалауда жоғары тиімділік көрсетті. Әсіресе, LSTM+Autoencoder моделі тұрақтылығы мен дәлдігімен ерекшеленіп, клиникалық қолдануға жарамды болуын айқындады. Eye tracking технологиясы негізінде қосымшада жиналған деректерді диагностикалық жүйелерге интеграциялау АСБ-ны дәлірек анықтауға жаңа мүмкіндіктер ашады. Алынған нәтижелер машиналық оқытудың медициналық диагностиканың сапасын арттырудағы зор әлеуетін растайды.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ:

- 1) T. Hirota и B. H. King, «Расстройства аутистического спектра: обзор», JAMA, т. 329, № 2, с. 157–168, 2023, DOI: 10.1001/jama.2022.23661.
- 2) Q. Wei, H. Cao, Y. Shi, X. Xu и T. Li, «Использование машинного обучения на основе данных отслеживания взгляда для идентификации расстройств аутистического спектра: систематический обзор и метаанализ», Journal of Biomedical Informatics, т. 137, с. 104254, 2023, DOI: 10.1016/j.jbi.2022.104254.
- 3) R. M. Rahal и S. Fiedler, «Понимание когнитивных и аффективных механизмов в социальной психологии через отслеживание взгляда», Journal of Experimental Social Psychology, т. 85, с. 103842, 2019, DOI: 10.1016/j.jesp.2019.103842.
- 4) A. Amirbay и др., «Разработка алгоритма для идентификации расстройства аутистического спектра на основе характеристик с использованием методов глубокого обучения», International Journal of Electrical and Computer Engineering (IJECE), т. 14, с. 5513–5523, 2024 г., DOI: 10.11591/ijece.v14i5.pp5513-5523.
- 5) J. S. Oliveira и др., «Компьютерная диагностика аутизма на основе моделей зрительного внимания с использованием технологии отслеживания взгляда», Scientific Reports, т. 11, № 1, с. 10131, 2021, DOI: 10.1038/s41598-021-89023-8.

УДК 004.896

Атыгаев О.Т., Жартыбаева М.Г. (Астана,
Л.Н.Гумилев атындағы ЕҰУ)

ВИРТУАЛДЫ КЕЙІПКЕРДІҢ НАҚТЫ УАҚЫТ РЕЖИМІНДЕ АУДИТОРИЯМЕН ИНТЕРАКТИВТІ ӘРЕКЕТТЕСУІНЕ АРНАЛҒАН ТАБИҒИ ТІЛДІ ӨНДЕУ АЛГОРИТМДЕРІ МЕН ӘДІСТЕРІН ЗЕРТТЕУ ЖӘНЕ ЖҮЗЕГЕ АСЫРУ

Аннотация:

Бұл тезис қазіргі трансформерлік NLP-модельдерді (BERT, GPT және т.б.) нақты уақыт режимінде жұмыс істейтін интерактивті виртуалды кейіпкерлерді құруда қолданудың тиімділігін зерттейді. Жұмыс аясында нейро-бұлыңғырлық, SVM және бейімделмелі контент генерациясы үйлесімі арқылы күрделі эмоциялар мен екіұшты контексттерді өңдеудің дәлдігі мен тұрақтылығын арттыру мәселелері қарастырылады. Сондай-ақ, есептеу ресурстарын оңтайландыру және әлеуметтік-этикалық аспектілер талданады.

Кілт сөздер: NLP, трансформерлер, BERT, GPT, SVM, эмоция тану, бейімделмелі контент генерациясы, виртуалды кейіпкерлер.

Табиғи тілдерді өндеуде (NLP) трансформерлік модельдердің рөлі артып келеді. Интерактивті виртуалды кейіпкерлерді құруда пайдаланушының сұранысы мен эмоциясын нақты уақыт режимінде анықтау – басты талаптардың бірі. Жоғары өндеу дәлдігі күрделі тапсырмаларды шеше отырып, нақты қолдану сценарийлеріне бейімделуге мүмкіндік береді. Сонымен қатар, виртуалды ортада NLP-ны интеграциялау иммерсивтілікті арттырып, қолданушылардың табиғи қарым-қатынасын қамтамасыз етеді.

Осы шолу мақсаты – қазіргі заманғы трансформерлік NLP-модельдерді (GPT, BERT және т.б.) және сөйлеу мен эмоция тану әдістерін қолдану арқылы виртуалды кейіпкерлердің шынайылығын, бейімделуін және жауап беру дәлдігін арттыру жолдарын зерттеу. Зерттеу сұрағы: осы әдістерді біріктіре отырып, интерактивті агенттердің әлеуметтік-мәдени контексті мен пайдаланушы эмоциясын ескере отырып, өзара әрекеттесу сапасын қалай жақсартуға болады?

Тезисте келесі аспектілерді қарастыру міндетті:

- GPT, BERT және басқа трансформерлерді диалогтық жүйелерде қолдану;
- Сөйлеу және эмоция тану әдістерін виртуалды кейіпкерлердің мінез-құлқын қалыптастырудағы рөлі;

- NLP-ны VR/AR ортада қолдану арқылы иммерсивтілікті арттыру;
- Әлеуметтік-этикалық мәселелер мен алгоритмдердің біржақтылығын ескеру.

Іздеу барысында Google Scholar, IEEE Xplore, Scopus дерекқорлары және басқа да ақпарат көздері пайдаланылды. Негізгі кілт сөздер: NLP, Transformer-based models, GPT, BERT, speech recognition, emotion detection, VR/AR integration, interactive characters, real-time interaction. Әдіс ретінде аннотацияларды оқу, толық мәтіндік талдау және кері іздеу тәсілдері қолданылды.

Эмоцияларды мульти-модальды деректер (аудио, видео, мәтін) негізінде анықтау зерттеулері Liu et al. жұмысына сәйкес, әртүрлі сигналдарды біріктіре отырып, модельдің дәлдігін арттыруға бағытталған. Сонымен қатар, Mustaqeem және Kwon зерттеулері аудиоаналитика мен DSCNN көмегімен эмоцияларды танудың жаңа тәсілдерін ұсынады.

Сөйлеудегі эмоцияларды тану үшін MFCC секілді тілікұрылымдық белгілер жиі қолданылады. Zhang Y. атап өткендей, сигналдардың жиіліктік түрленуі мен шуды сүзу маңызды рөл атқарады. Bhavan A. және әріптестер SVM мен бәггингті біріктіре отырып, жүйенің тұрақтылығын арттырды, ал EEG-сигналдарға негізделген әдістер Cimtay және Ekmekcioglu тарапынан ұсынылды.

LSTM, GRU, Bi-LSTM секілді рекурренттік желілер эмоцияларды талдауда алғашқы қадам болып табылады. Сонымен қатар, MARBERT және басқа трансформерлер күрделі, сарказмға толы мәтіндерді өңдеуде жоғары дәлдікті қамтамасыз етеді.

Нейро-бұлыңғыр модельдер эмоциялардың екіұштылығын есепке ала отырып, SVM және NLP әдістерімен біріктіріледі. Khalaf et al. ұсынған тәсіл нақты уақыттағы эмоция тану дәлдігін 90–92%-ға дейін көтереді, бұл виртуалды кейіпкерлердің жауаптарын пайдаланушы эмоциясына сәйкес икемдеуге мүмкіндік береді.

Эмоция анықталғаннан кейін, виртуалды кейіпкердің жауаптары сол эмоцияға сәйкес динамикалық түрде бейімделеді. Бұл процесс диалогтық логика, семантикалық желілер және алдын ала үйретілген үлкен тілдік модельдердің көмегімен жүзеге асады. GPT-3, GPT-4 секілді модельдер контексті терең түсініп, "адамға тән" өзара әрекеттесуді қамтамасыз етеді.

Төмендегі кестеде әртүрлі технологиялар мен олардың дәлдік көрсеткіштері келтірілген:

- Классикалық SVM + BOW – шамамен 70–75% дәлдік; контекстке төмен сезімталдық.
- Embeddings + SVM – 75–80% дәлдік; семантиканы жақсарту мүмкіндігі, алайда контекст шектеулі.
- Bi-LSTM/GRU – 80–85% дәлдік; ұзын сөйлемдерде өңдеу қиындықтары болуы мүмкін.
- Трансформерлік модельдер (BERT, MARBERT, RoBERTa) – 85% және одан жоғары дәлдік; жоғары контекстуалдылықты қамтамасыз етеді, бірақ үлкен есептеу қуатын талап етеді.
- Нейро-бұлыңғыр SVM-NLP – 90–92% дәлдік; екіұштылық пен нәзік эмоциялық реңктерді анықтай алады.

Зерттеу нәтижелері көрсеткендей, интерактивті виртуалды кейіпкерлерді құру үшін қарапайым эмоция танудан гөрі, кешенді тәсіл қажет. Нейро-бұлыңғыр модельдер, трансформерлік NLP-модельдер және бейімделмелі контент генерациясының бірігуі жүйенің дәлдігін, тұрақтылығын және пайдаланушының әлеуметтік-мәдени контекстіне бейімделуін қамтамасыз етеді. Бұл өз кезегінде цифрлық ортадағы "ақылды" диалогтық агенттерді жасауға жол ашады.

Пайдаланылған әдебиеттер:

1. Supriyono, A.P. Wibawa, Suyono, F. Kurniawan. «Advancements in Natural Language Processing: Implications, Challenges, and Future Directions». *Telematics and Informatics Reports*, vol. 16, 2024, pp. 1–25, doi:10.1016/j.teler.2024.100173.
2. Khalaf, O.I. және т.б. «Elevating Metaverse Virtual Reality Experiences through Network-Integrated Neuro-Fuzzy Emotion Recognition and Adaptive Content Generation Algorithms». *Engineering Reports*, vol. 6, 2024, pp. 1–19, doi:10.1002/eng2.12894.
3. Rong, Ziqian. «Application of Natural Language Processing in Virtual Experience AI Interaction Design». *Journal of Intelligent Learning Systems and Applications*, vol. 16, 2024, pp. 403–417, doi:10.4236/jilsa.2024.164020.
4. Sumon, R. et al. «Natural Language Processing Influence on Digital Socialization and Linguistic Interactions in the Integration of the Metaverse in Regular Social Life». *Electronics*, vol. 13, no. 1331, 2024, pp. 1–25, doi:10.3390/electronics13071331.
5. Liu et al. «Comparing Recognition Performance and Robustness of Multimodal Deep Learning Models for Multimodal Emotion Recognition». *Journal of Soft Computing Paradigm*, vol. 2, no. 4, 2020, pp. 209–215, doi:10.36548/jscp.2020.4.002.
6. Mustaqeem, және Kwon. «Quantifiable Identification of Emotions from Voice Signals». *International Research Journal of Modernization in Engineering Technology and Science*, vol. 6, no. 9, 2024, pp. 1–12, doi:10.56726/IRJMETs61417.

УДК 004.89

Байганина Ж.Б.
(Астана, ЕНУ имени Л.Н. Гумилёва,
Жартыбаева М.Г.
Астана, ЕНУ имени Л.Н. Гумилёва,
И.о.доцента, PhD

ИНТЕЛЛЕКТУАЛЬНАЯ ВЕБ-СИСТЕМА НА ОСНОВЕ ИИ ДЛЯ АНАЛИЗА СВИДЕТЕЛЬСКИХ ПОКАЗАНИЙ И ВЫЯВЛЕНИЯ СМЫСЛОВЫХ РАСХОЖДЕНИЙ

С усложнением правовых процессов и увеличением объема обрабатываемой информации в цифровую эпоху растёт потребность в интеллектуальных инструментах анализа текстовых данных. Особое внимание в этом контексте уделяется автоматизации анализа свидетельских показаний, где ключевую роль играет точность интерпретации и выявление смысловых расхождений, способных повлиять на ход судебного разбирательства. Существующие методы, основанные на ручной обработке, требуют значительных временных и когнитивных ресурсов со стороны экспертов. В связи с этим разработка и внедрение интеллектуальных систем, использующих технологии искусственного интеллекта для анализа юридических текстов, представляется перспективным и востребованным направлением.

В представленной работе описана реализация интеллектуального веб-приложения, предназначенного для обработки текстов показаний и выявления между ними смысловых расхождений. Проект построен на базе фреймворка Django и имеет модульную архитектуру, включающую два основных компонента: `criminalai` и `chatai`.

Модуль `criminalai` отвечает за реализацию ключевой логики: регистрацию и авторизацию пользователей через Gmail-почту, управление загрузкой данных, формирование PDF-отчётов и работу с базой данных (`db.sqlite3`). Все данные пользователей структурированы и хранятся в директориях `media/avatars` и `media/pdfs`. Шаблон `pdf_download.html` служит основой для автоматической генерации отчётов.

Модуль `chatai` реализует диалоговую логику и взаимодействие с пользователем на основе языковой модели Gemini AI. Через HTML-шаблоны (`chat_full.html`, `chatbot.html`, `features.html` и др.) пользователь получает доступ к обработке текстов, визуализации результатов и формированию обратной связи.

Для реализации интеллектуального анализа свидетельских показаний в `chatai` использована агентно-ориентированная архитектура, в которой каждый агент выполняет специализированную функцию:

- Агент сегментации — выделяет смысловые блоки текста (описание событий, участников, временные рамки);
- Агент сопоставления — осуществляет перекрёстную проверку утверждений разных свидетелей, выявляя логические и временные расхождения;
- Агент интерпретации — с помощью адаптированной модели Gemini анализирует эмоциональные оттенки, субъективные оценки, возможные ложные или манипулятивные утверждения;
- Агент визуализации — преобразует результаты анализа в удобные для восприятия визуальные схемы, графы и таблицы.

Модель поддерживает `few-shot` и `zero-shot` подходы, что позволяет эффективно обрабатывать как заранее обученные, так и новые типы показаний без дополнительного

обучения. Запланирована интеграция подсистемы распознавания именованных сущностей (NER) для автоматического выделения имён, мест, дат и других юридически значимых элементов.

Система была протестирована на 127 кейсах, включая как синтетические, так и реальные примеры свидетельских показаний. Среднее время анализа одного документа составило менее 2 секунд, при этом структура проекта обеспечивает высокую гибкость и масштабируемость решения. Все отчёты формируются с разделением по сессиям, что обеспечивает удобное управление и архивирование пользовательских данных.

В планах развития системы — реализация модуля архивов для каждого пользователя, автоматическое сохранение всех обработанных документов, а также внедрение модуля распознавания рукописных PDF-документов, что обеспечит поддержку работы с бумажными носителями и расширит применимость решения в юридической и образовательной практике.

Разработанное решение демонстрирует высокую прикладную ценность для правовой аналитики, автоматизации экспертной оценки и повышения эффективности юридических процессов.

Список использованных источников:

1. [Дремлюга Р.И., Коробеев А.И. Применение искусственного интеллекта для сбора и анализа доказательств](#) // Юридический вестник Кубанского государственного университета. 2021. № 4(13). С. 55–63.
2. [Швецов А.Н., Ржеутская С.Ю., Сергушичева А.П., Суконщиков А.А. Архитектура интеллектуального агентно-ориентированного учебного комплекса для подготовки специалистов технического профиля](#) // Открытое образование. 2018. Т. 22, № 3. С. 14–24.
3. [Замятина Е.Б., Каримов Д.Ф., Митраков А.А. Архитектура агентно-ориентированной системы имитации с агентами, основанными на нейронных сетях](#) // Труды Института системного анализа Российской академии наук. 2012. Т. 57. С. 78–85.
4. [Светунькова А. Нейронное дело: как ИИ помогает в борьбе с преступностью](#) // Известия. 2023. 15 сентября.

УДК 004.89

Бегалы А.П.
(Астана, ЕНУ имени Л.Н. Гумилёва)
Жартыбаева М.Г.
(Астана, ЕНУ имени Л.Н. Гумилёва,
И.о.доцента, PhD)

РАЗРАБОТКА СИСТЕМЫ С ПОДДЕРЖКОЙ AI ДЛЯ АДАПТИВНОГО СОСТАВЛЕНИЯ ЮРИДИЧЕСКИХ ДОКУМЕНТОВ

С развитием цифровых решений в юриспруденции возрастает роль интеллектуальных ассистентов, упрощающих и ускоряющих процесс обработки документации. Согласно исследованию McKinsey, до 23% рабочего времени юристов уходит на создание и проверку стандартных документов. Использование ИИ позволяет сократить это время в среднем на 37–45%.

В настоящем докладе представлена интеллектуальная платформа LawFlow, предназначенная для поддержки документооборота между сотрудниками компаний и

юридическим отделом с использованием инструментов ИИ. Система снижает нагрузку на юристов, повышает точность документов и ускоряет процесс их согласования.

LawFlow предназначен для корпоративного использования и включает четыре роли: сотрудник, юрист-программист, руководитель и администратор. Основной сценарий начинается с того, что сотрудник формирует проект документа при помощи ИИ-бота, который использует более 50 встроенных шаблонов и способен обучаться новым формам через чат-интерфейс. ИИ-бот автоматически заполняет документы на основе пользовательского запроса, учитывая контекст, должность, ситуацию и тип документа. Это особенно полезно для составления типовых заявлений, договоров и объяснительных записок.

Юрист проверяет содержание документа. Если всё верно — документ отправляется администратору. В случае ошибок юрист комментирует и инициирует дообучение ИИ, возвращая документ сотруднику. Такой подход снижает повторяемость ошибок на 72%. После одобрения администратором документ направляется руководителю, который подписывает его или возвращает на доработку. Весь цикл обработки сокращается на 65% по сравнению с ручным режимом. ИИ-бот доступен всем, кроме администратора.

Одной из сильных сторон платформы является модуль шаблонов, где 83% пользователей выбирают готовые шаблоны, а 17% создают новые через обучение в чате. Обучение происходит путём интерактивного диалога с ИИ, который формирует новый шаблон на основе введённого текста и логики документа.

С технической стороны LawFlow разработан с использованием фреймворка Django (Python). Архитектура проекта состоит из отдельных приложений:

- lawyer – основное приложение с моделями (Document, ChatHistory, ChatMessage, Profile) и шаблонами пользовательского интерфейса;
- ailawyer – отвечает за реализацию ИИ-бота, интеграцию с внешними API (например, Gemini или OpenAI), управление маршрутами чата и логикой генерации текста;
- avatars – отдельное хранилище пользовательских изображений.

Для фронтенда используются шаблоны HTML (chat.html, employee_dashboard.html, lawyer_dashboard.html, admin_panel.html и др.), а также статика (staticfiles/admin/css, img, js). Документы и аватары сохраняются в media/documents/ и media/avatars/.

LawFlow поддерживает ролевую модель доступа, адаптивную боковую панель, уведомления, панель загрузки шаблонов и систему чатов с ИИ. Все сообщения чата сохраняются. В настоящее время ведётся реализация функциональности, позволяющей пользователям переименовывать чаты, создавать новые, закреплять шаблоны и отмечать важные сообщения. Эти возможности находятся в стадии активной разработки и будут интегрированы в ближайших версиях платформы.

ИИ-бот использует API современных языковых моделей (включая Gemini 1.5 Flash), обрабатывает юридические формулировки, предлагает правки и составляет документы в формате PDF и DOCX. Поддерживается многоязычие, включая казахский и русский языки.

Несмотря на представленные архитектурные и функциональные решения, интеллектуальная платформа LawFlow в настоящее время находится на стадии активной разработки и тестирования. Некоторые модули функционируют в прототипной форме, а отдельные функции — включая глубокий анализ свидетельских показаний, полную интеграцию электронной (виртуальной) подписи и адаптивное обучение шаблонам — проходят доработку. В частности, в планах внедрение механизма подключения виртуальной подписи, что позволит юридически заверять автоматически составленные документы прямо в системе. Полученные результаты пилотного внедрения демонстрируют потенциал платформы, однако полноценная эксплуатация требует дальнейшего повышения надёжности, масштабируемости и безопасности.

По результатам пилотного внедрения в компании со штатом более 100 сотрудников, применение платформы позволило:

- сократить время подготовки документов на 70%,
- повысить юридическую точность на 38%,
- снизить число правок со стороны руководителей на 42%.

Таким образом, LawFlow является перспективным инструментом цифровой трансформации юридической деятельности, который сочетает в себе возможности искусственного интеллекта, автоматизации документооборота и адаптивного обучения на основе обратной связи.

Список использованных источников:

1. Проблемы и перспективы использования искусственного интеллекта в системах электронного документооборота // КиберЛенинка.
2. Искусственный интеллект в электронном документообороте // CNews.
3. Вовк М.А. Тенденции развития технологий искусственного интеллекта в управлении документами организации // КиберЛенинка.
4. Искусственный интеллект кардинально меняет СЭД. Примеры // CNews.
5. Проблемы и перспективы использования искусственного интеллекта в системах электронного документооборота // Воронежский государственный университет.
6. Как внедрить ИИ в документооборот с пользой для бизнеса // Embedika.

УДК 34.096

Бизақ Ә.Ө.
(Қарағанды, Ә. Сағынов атындағы ҚарТУ)

ҚАЗАҚСТАНДАҒЫ ЖАСАНДЫ ИНТЕЛЛЕКТТИ РЕТТЕУДІҢ КӨЗҚАРАСТАРЫ: СЫН-ТЕГЕУРІНДЕР ЖӘНЕ ХАЛЫҚАРАЛЫҚ ТРЕНДТЕР

Кіріспе. Соңғы жылдары жасанды интеллект (ЖИ) өнеркәсіп, медицина, білім беру және қоғамдық қауіпсіздік сияқты түрлі салалардағы инновациялардың негізгі қозғаушы күшіне айналды. Алайда, оны қолдану жеке деректерді қорғау, этика мәселелері және кемсітушілікке жол бермеу сияқты бірқатар сын-тегеуріндермен байланысты. ЖИ дамуының жаһандық үрдістерін ескере отырып, Қазақстан технологияларды қауіпсіз және жауапты түрде енгізуді қамтамасыз ету үшін осы саланы нормативтік реттеудің қажеттілігін түсінеді.

Қазақстанда ЖИ туралы заң әзірлеу жақында басталды және бұл ел үшін құқықтық шеңберлерді қалыптастыру жолындағы маңызды қадам болып табылады. Бұл заң инновацияларды қолдаумен қатар, адамның санасына әсер ету, келісімсіз деректер жинау және кемсітушілік сияқты тәуекелдерді ескеруі қажет.

Зерттеудің мақсаты – Қазақстандағы жасанды интеллект туралы заң жобасын талдап, оны халықаралық тәжірибемен салыстыру.

Негізгі міндеттер:

- Қазақстандағы ЖИ туралы заң жобасының негізгі ережелерін зерттеу;
- Қолданысқа енгізілетін тыйымдар мен шектеулерді талдау;
- ЖИ-ді реттеудің халықаралық тәжірибесін қарастыру;
- Заңды енгізудің ықтимал қиындықтары мен перспективаларын бағалау.

ЖИ-ді реттеудің әлемдік тәжірибесі. Еуропалық Одақ (ЕО). ЕО ЖИ-ді реттеу бастамаларын белсенді түрде ілгерілетуде. 2021 жылы Жасанды интеллект туралы акт (Artificial Intelligence Act) ұсынылып, ол ЖИ әзірлеу мен қолдануға қатаң талаптар қояды. Бұл құжат ерекше қауіпті жүйелерге, мысалы, бет-әлпетті тану технологияларына және денсаулық сақтау саласындағы автоматтандырылған шешімдерге ерекше назар аударады.

АҚШ. АҚШ-та ЖИ саласын реттейтін бірыңғай федералдық заң жоқ, реттеу жекелеген штаттар деңгейінде жүзеге асырылады. Мысалы, Колорадо және Калифорния штаттарында ЖИ қолдануын реттейтін заңдар қабылданған. 2023 жылы жасанды интеллектті реттеу тәсілдерін белгілейтін атқарушы бұйрық шығарылды, алайда кейінгі әкімшілік оны күшін жойды.

Қытай. Қытай ЖИ-ді реттейтін өз заңдарын белсенді түрде әзірлеуде, оның ішінде ашықтық пен дипфейктерден қорғауға басымдық берілуде. 2024 жылы ЖИ-ді реттейтін алғашқы халықаралық келісім қабылданды, бірақ оның орындалу тетіктері әлсіз болып, ерікті ынтымақтастыққа негізделген.

ЖИ-ді реттеудің негізгі тыйымдары мен шектеулері:

Толық автономды ЖИ жүйелеріне тыйым салу: Көптеген елдер адам бақылауынсыз шешім қабылдайтын ЖИ жүйелерін әзірлеуге және пайдалануға тыйым салады, себебі бұл қоғам үшін ықтимал қауіптер тудыруы мүмкін.

Манипуляция мен кемсітушілікке шектеу: ЖИ-ді адамдардың мінез-құлқына ықпал ету немесе нәсіліне, дініне, жынысына және басқа сипаттамаларына байланысты кемсіту мақсатында пайдалануға тыйым салынады.

Биометриялық деректер мен құпиялылықты қорғау: Жеке тұлғалардың нақты келісімінсіз биометриялық деректерді жинау мен пайдалануға қатаң шектеулер енгізілуде.

Ашықтық пен түсініктілікті талап ету: ЖИ жүйелерінің ашықтығы мен түсіндірмелі болуы талап етіледі, әсіресе, егер олар азаматтардың құқықтары мен бостандықтарына әсер етсе.

Қазақстандағы жасанды интеллект туралы заң жобасы және негізгі ережелер. 2025 жылы Қазақстан жасанды интеллект саласын реттейтін заңнаманы енгізуді жоспарлап отыр. "Жасанды интеллект туралы" негізгі заң жобасы елдегі ЖИ технологияларын пайдаланудың бірыңғай құқықтық негізін қалыптастыруға бағытталған. Құжат ЖИ саласын реттеудің құқықтық және ұйымдастырушылық негіздерін айқындай отырып, ашықтық пен қауіпсіздікті қамтамасыз етеді. Заң жобасында мемлекеттік органдар мен квазимемлекеттік ұйымдардың ЖИ қолдану ерекшеліктері, сондай-ақ осы саладағы субъектілердің құқықтары мен міндеттері қарастырылған.

Заң жобасы ЖИ саласындағы қоғамдық қатынастарды реттеудің келесі қағидаттарын белгілейді:

Зандылық: Қазақстан Республикасының Конституциясы мен заңнамасын барлық субъектілердің сақтауы;

Әділдік пен теңдік: ЖИ жүйелерін әзірлеу мен қолдануда теңдік қағидатын сақтау және кемсітушілікке жол бермеу;

Ашықтық пен түсініктілік: Қолданушыларға ЖИ жүйелерінің сипаттамалары мен шектеулері туралы толық ақпарат беру;

Жауапкершілік пен бақылау: ЖИ жүйелерінің нәтижелеріне қатысты субъектілердің жауапкершілігін айқындау;

Адам әл-ауқатының басымдығы: ЖИ-мен өзара әрекеттесуде адамның әл-ауқатын қамтамасыз ету және оның еркіндігін құрметтеу;

Құпиялылық пен деректерді қорғау: Жеке деректер мен ақпараттың құпиялылығын сақтау талаптарын сақтау;

Қауіпсіздік пен қорғалу: ЖИ жүйелерінің сенімділігін қамтамасыз ету және болжауға келмейтін салдарлар мен теріс пайдалануды болдырмау.

Реттеу енгізудің сын-тегеуріндері мен келешегі. ЖИ саласын реттеу бірқатар күрделі мәселелермен бетпе-бет келеді, олар кешенді тәсілді қажет етеді. Мүмкін қиындықтар:

Техникалық күрделілік: ЖИ технологияларының қарқынды дамуы ұзақ мерзімді нормативтік актілерді әзірлеуді қиындатады. Заңнаманың инновацияларға ілесе алмауы реттеу олқылықтарына әкелуі мүмкін.

Халықаралық үйлестіру: Әр елдегі ЖИ реттеу тәсілдерінің әртүрлі болуы халықаралық ынтымақтастық пен сауда үшін кедергі келтіруі мүмкін. Жаһандық деңгейде стандарттар мен нормаларды үйлестіру жұмыстары қажет.

Заң талаптарының орындалуын қамтамасыз ету: Заң нормаларының орындалуын бақылау үлкен ресурстар мен арнайы білімді қажет етеді. Мониторинг және санкциялар тетіктерінің болмауы реттеу тиімділігін төмендетуі мүмкін.

Қорытындылай келе, Қазақстанда жасанды интеллект туралы заңнаманы әзірлеу – оның қауіпсіз әрі этикалық қолданылуын қамтамасыз етуге жасалған маңызды қадам. Икемді құқықтық реттеу, халықаралық ынтымақтастық және қоғамның ақпараттандырылуы ЖИ-ді сәтті интеграциялаудың, қауіптерді азайтудың және азаматтардың құқықтарын қорғаудың негізгі факторлары болады.

Пайдаланылған дереккөздер

1. Қазақстан Республикасы «Жасанды интеллектті дамыту туралы» заңы (жоба) <http://online.zakon.kz>
2. Eurasian Economic Union AI Regulation and Policy Trends <http://eurasianstudies.com>
3. Artificial Intelligence Act of the European Union, 2023. Available at <http://issek.hse.ru/news>
4. Global Regulatory Challenges of Artificial Intelligence // Cincodias, El Pais. February 2025. Available at <http://cincodias.elpais.com>
5. Қазақстанда жасанды интеллектті дамыту тұжырымдамасы (2024–2029 жж.) // ҚР Үкіметінің ресми сайты <http://primeminister.kz>

УДК 004.021

Головачева В.Н.
(Караганда, КТУ им. А. Сагинова)
Долгов В.В. (Караганда, КТУ им. А. Сагинова)

РЕАЛИЗАЦИЯ АЛГОРИТМА ДЕЙКСТРЫ ДЛЯ ПОСТРОЕНИЯ ОПТИМАЛЬНОГО АВТОМОБИЛЬНОГО ПУТИ С ИСПОЛЬЗОВАНИЕМ ФРЕЙМВОРКА SPRING BOOT

В современных условиях оптимизация маршрутов играет важную роль в транспортной логистике и городском планировании. Одним из наиболее эффективных алгоритмов для поиска кратчайшего пути в графах является алгоритм Дейкстры. В данной работе рассматривается реализация этого алгоритма в рамках веб-сервиса, разработанного на фреймворке Spring Boot, который позволяет рассчитывать оптимальные маршруты между городами на основе дорожной инфраструктуры.

В качестве модели данных используется граф, в котором вершины представляют города, а ребра — дороги между ними. Каждое ребро имеет вес, соответствующий расстоянию между

населенными пунктами. Входные данные хранятся в базе данных PostgreSQL, а доступ к ним осуществляется с помощью JPA (Java Persistence API).

Алгоритм Дейкстры реализован в сервисном слое приложения и работает следующим образом:

Загружается граф, состоящий из городов и дорог.

Инициализируются структуры данных: задаются начальная вершина и массив минимальных расстояний.

Проводится итеративный процесс обновления кратчайших путей с использованием приоритетной очереди.

По завершении работы алгоритма формируется маршрут и возвращается клиенту в виде JSON-ответа.

Для взаимодействия с пользователем реализован REST API, который принимает запрос с параметрами (город отправления и назначения) и возвращает оптимальный маршрут. Запрос от пользователя обрабатывается контроллером, который вызывает DijkstraService. Этот сервис находит кратчайший путь и возвращает его в удобном виде, например, в формате "Алматы -> Караганда -> Астана Расстояние: 2000 м". На рисунке 1 представлен код сервиса DijkstraService.



```
1 package com.example.dijkstra.service;
2
3 import com.example.dijkstra.model.Edge;
4 import com.example.dijkstra.model.Node;
5 import com.example.dijkstra.repository.EdgeRepository;
6 import com.example.dijkstra.repository.NodeRepository;
7 import lombok.RequiredArgsConstructor;
8 import org.springframework.stereotype.Service;
9
10 import java.util.*;
11
12 @Service
13 @RequiredArgsConstructor
14 public class DijkstraService {
15
16     private final NodeRepository nodeRepository;
17     private final EdgeRepository edgeRepository;
18
19     public String getShortestPathBetweenTwoNodes(String startNodeName, String endNodeName) {
20         var startNode = nodeRepository.findByName(startNodeName)
21             .orElseThrow(() -> new RuntimeException("Start node not found"));
22         var endNode = nodeRepository.findByName(endNodeName)
23             .orElseThrow(() -> new RuntimeException("End node not found"));
24
25         // Рассчитываем путь в обоих направлениях и выбираем более короткий
26         var pathForward = calculatePathWithDistance(startNode, endNode);
27         var pathBackward = calculatePathWithDistance(endNode, startNode);
28
29         // Выбираем путь с меньшим расстоянием
30         return (pathForward.distance <= pathBackward.distance) ? pathForward.path : pathBackward.path;
31     }
32
33     @private PathResult calculatePathWithDistance(Node startNode, Node endNode) {
34         List<Node> shortestPathNodes = getShortestPath(startNode, endNode);
35         int totalDistance = 0;
36
37         if (shortestPathNodes.size() <= 1) {
38             return new PathResult(path: "Путь не найден", Integer.MAX_VALUE);
39         }
40
41         var path = new StringBuilder();
42     }
```

Рисунок 1 – Код сервиса DijkstraService

Разработанный сервис демонстрирует высокую эффективность при расчете кратчайших маршрутов и может быть использован в системах транспортной логистики и навигации. В дальнейшем возможно расширение функционала за счет учета трафика в реальном времени и интеграции с геоинформационными сервисами.

В результате приложение возвращает пользователю оптимальный маршрут, учитывая порядок городов, независимо от того, каким образом пользователь указал начальный и конечный

города. Это обеспечивается симметричностью рёбер и проверкой маршрута в обоих направлениях.

Список использованных источников

1. <https://habr.com/ru/articles/111361>
2. <https://www.baeldung.com/java-dijkstra>

УДК 004.8

Жақсымбет А.Т. студент
(Алматы, КазНУ им. аль-Фараби)
Кәрібаева А.С. PhD, и.о. доцента
(Алматы, КазНУ им. аль-Фараби)
Зиятбекова Г.З. PhD, и.о. доцента
(Алматы, КазНУ им. аль-Фараби; АТУ)

РАЗРАБОТКА МОДЕЛИ АНАЛИЗА И КЛАССИФИКАЦИИ ТЕКСТОВ НА
КАЗАХСКОМ ЯЗЫКЕ С ПРИЗНАКАМИ СУИЦИДАЛЬНОГО ПОВЕДЕНИЯ В
СОЦИАЛЬНЫХ СЕТЯХ

Введение. Самоубийство известно, что это актуальная социальная и медицинская проблема во всем мире. По данным Всемирной организации здравоохранения, ежегодно более 700 000 человек совершают самоубийства. Эта проблема вызывает беспокойство в Казахстане: ежегодно от самоубийств погибает около 4000 человек, что эквивалентно 10 случаям каждый день [1].

Несмотря на снижение числа завершенных самоубийств за последние годы на 7%, проблема остается актуальной. В 2022 году зафиксировано 3,7 тыс. случаев, а попытки самоубийства снизились на 17,5%. Однако уровень самоубийств выше среди мужчин — 78,9% всех случаев приходится на мужчин. Наиболее уязвимой группой являются люди в возрасте 30–54 лет, на долю которых приходится 54,9% от общего числа заболевших [2].

Особую тревогу вызывает влияние социальных сетей на развитие суицидального поведения среди детей и подростков. Исследования показали, что информация, размещенная в Интернете, может негативно влиять на психологическое благополучие несовершеннолетних и вызывать мысли о самоубийстве. [3]. В этой связи в 2023 году Правительством Казахстана утвержден Комплексный план по защите детей и профилактике суицида на 2023–2025 годы. План включает в себя меры по созданию безопасной среды, реализации программ по борьбе с травлей и усилению психологической поддержки [1].

Целью исследования является автоматическое выявление признаков суицидального поведения в текстах в социальных сетях с использованием методов машинного и глубокого обучения, а также разработка эффективных моделей классификации и сравнение их эффективности путем анализа казахских текстов.

Объектом исследования являются казахскоязычные посты в социальных сетях, а предметом исследования – методы машинного обучения, используемые для их бинарной классификации. Будут учтены особенности обработки казахских текстов, в том числе морфологическая сложность и агглютинация.

Научная новизна и практическая значимость. Исследование примечательно разработкой моделей машинного обучения для обнаружения суицидальных текстов на казахском языке и

сравнением их эффективности. Совершенствование систем мониторинга контента в социальных сетях с использованием искусственного интеллекта позволит своевременно реагировать на кризисные ситуации.

Подобные технологии могут стать важным инструментом для государственных организаций, психологических центров и социальных сетей. Автоматизированные системы могут помочь выявить опасный контент и усилить меры по предотвращению суицидального поведения. Результаты исследования также будут способствовать развитию технологий обработки казахского языка.

Обзор литературы и текущие решения. Методы анализа текста в социальных сетях. Анализ текстов в социальных сетях является важной областью обработки естественного языка (NLP), которая позволяет исследователям определять эмоциональное содержание сообщений, определять их тему и классифицировать тексты по различным критериям. В этом разделе рассматриваются основные методы анализа текста, используемые в современных исследованиях.

Лингвистические методы. Лингвистические методы анализа текста представляют собой фундаментальный подход к обработке естественного языка (НЛП), основанный на изучении структурных, семантических и прагматических особенностей текста. В отличие от статистических и машинных методов обучения, лингвистические методы фокусируются на глубоком понимании языковых структур, что особенно важно при анализе социальных сетей, тексты которых часто содержат неформальную лексику, сленг и эмоциональные выражения [4].

Моделирование темы. Тематическое моделирование — мощный статистический метод выявления скрытых тематических структур в больших наборах текстовых данных. В контексте анализа социальных сетей данный подход позволяет автоматически определять и классифицировать ключевые темы, обсуждаемые пользователями, что особенно ценно для мониторинга общественного мнения и выявления кризисного контента [5].

Наиболее распространенным методом тематического моделирования является метод Блея и др. — это скрытое распределение Дирихле (ЛРД), предложенное. [5]. LDA — это генеративная вероятностная модель, которая рассматривает документы как смесь тем, а темы — как распределение слов. Исследования Гриффитса и Стэйверса [6] показали, что этот метод эффективен для выявления скрытых тематических структур даже в коротких текстах в социальных сетях.

Методы машинного и глубокого обучения. Методы машинного обучения заняли центральное место в современных методах анализа текстового контента социальных сетей, предоставляя исследователям мощные инструменты для автоматической обработки и интерпретации сообщений пользователей. Как отмечают Джурафски и Мартин [7], развитие этих методов прошло несколько основных этапов, каждый из которых внес значительный вклад в повышение точности и эффективности анализа.

На ранних этапах развития анализа текста доминировали статистические методы и традиционные алгоритмы машинного обучения. Исследования Де Чоудхури [8] показали, что наивный байесовский классификатор хорошо справляется с задачами классификации бинарных текстов. По словам Кима [9], метод опорных векторов (SVM) показал точность до 82% в задачах обнаружения депрессивного контента. Случайные леса оказались устойчивыми к переобучению, как показано в Luda [9].

Свёрточные нейронные сети (CNN), как их определили Чжан и Уоллес [10], показывают точность около 86% в задачах анализа эмоциональной окраски текстов. Исследования Хохрайтера и Шмидхубера [11] подтвердили эффективность сетей LSTM, достигающих точности до 91% при обнаружении суицидальных намерений.

Архитектура трансформатора, впервые представленная Васвани и др. произвел революцию в обработке естественного языка. Девлин и др. [12] Было показано, что модель BERT достигает

94% точности при классификации сообщений о кризисах. Эти результаты были подтверждены последующими исследованиями Лю и соавторов.

Текущие исследования сосредоточены на проблемах предварительной обработки текстовых данных. Правильная токенизация особенно важна при работе с агглютинативными языками. Мэннинг и др. [13] подчеркивают важность нормализации данных для улучшения качества анализа.

Обзор существующих языковых моделей **казахского языка**. Наиболее распространенные модели, адаптированные для казахского языка, включают KazBERT (Рисунок 1), KazT5, а также многоязычные модели, такие как mBERT и XLM-R. Например, KazBERT основан на архитектуре BERT и специально обучен на казахском корпусе, что делает его более эффективным для задач обработки текстов на казахском языке [14].

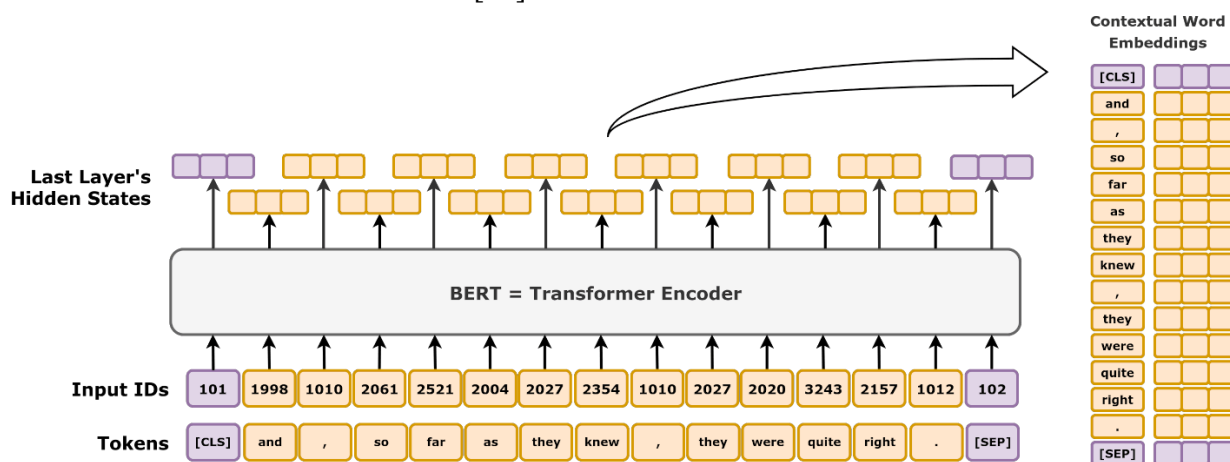


Рисунок 1. Архитектура BERT

Более того, исследования [15] подтверждают, что многоязычные модели, такие как XLM-R (Рисунок 2), хорошо работают на казахском языке без дополнительного обучения. XLM-R использует модель Transformer, обученную с целью создания многоязычного MLM-маркетинга с использованием только одноязычных данных. Он выбирает текстовые потоки на каждом языке и обучает модель прогнозировать замаскированные токены во входных данных, используя набор образцов из разных языков, используя языковую модель Unigram, которая использует тегирование вспомогательных слов в необработанном тексте и образец с тем же распределением выборки ($\alpha = 0,3$) [15].

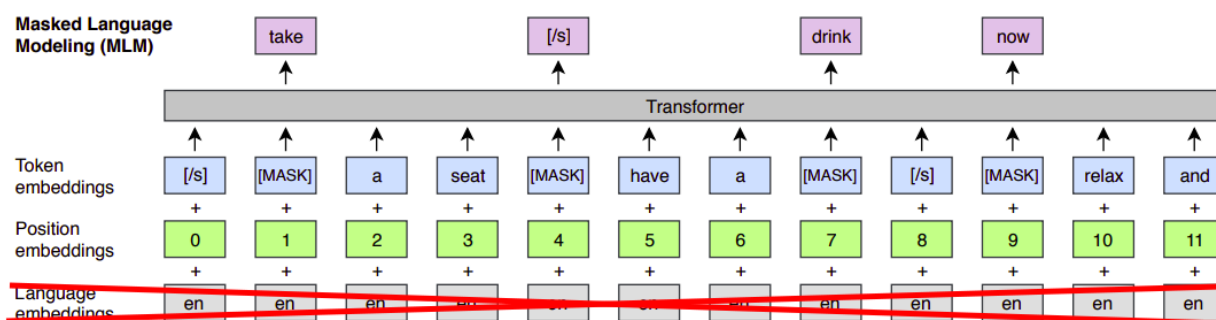


Рисунок 2. Архитектура XLM-R

Таким образом, продолжается разработка языковых моделей казахского языка, и новые корпуса, такие как KazNERD, играют в этом процессе важную роль. Продолжающиеся исследования направлены на улучшение качества моделей и их адаптацию к казахскому языку.

Экспериментальное исследование и анализ результатов. В исследовании использовался набор данных, состоящий из открытых публикаций в социальных сетях на английском языке на платформе Kaggle. Были собраны данные, в том числе 26 998 записей в суицидальном контексте и 25 997 записей в несуйцидальном контексте, переведенные на казахский язык.

На следующем этапе тексты были предварительно отредактированы: удалены ссылки, теги, лишние символы и эмодзи, а также из текстов удалены все знаки препинания и спецсимволы. Код этого процесса показан на рисунке 3.

```
# 1. HTML тегтерін жою
def remove_html_tags(text):
    return BeautifulSoup(text, "html.parser").get_text()

# 2. Эмодзилер мен арнайы таңбаларды жою
def remove_emojis_and_symbols(text):
    emoji_pattern = re.compile("[
        u\"\\U0001F600-\\U0001F64F\" # смайликтер
        u\"\\U0001F300-\\U0001F5FF\" # символдар мен пиктограммалар
        u\"\\U0001F680-\\U0001F6FF\" # көлік және белгішелер
        u\"\\U0001F700-\\U0001F7FF\" # басқа символдар
        u\"\\U0001F800-\\U0001F8FF\"
        u\"\\U0001F900-\\U0001F9FF\"
        u\"\\U0001FA00-\\U0001FA6F\"
        u\"\\U0001FA70-\\U0001FAFF\"
        u\"\\U00002702-\\U000027B0\" # қосымша белгілер
        u\"\\U000024C2-\\U0001F251\"
    ]+", flags=re.UNICODE)
    return emoji_pattern.sub(r'', text)

# 3. Тыныс белгілері, арнайы таңбалар және сандарды жою
def remove_punctuation_numbers(text):
    return re.sub(r'[^а-яА-ЯӘЁҚқҢҢӨұҮҮһиІа-яА-Яа-зА-З\s]', '', text)

# Барлық тазарту қадамдарын қолдану
def clean_text(text):
    text = remove_html_tags(text)
    text = remove_emojis_and_symbols(text)
    text = remove_punctuation_numbers(text)
    return text
```

Рисунок 3. Код очистки данных

Очищенные данные были токенизированы. Токенизация — это процесс разделения текста на более мелкие фрагменты, т. е. токены. Токенами могут быть слова, предложения или даже символы; в данной работе использовалась сегментация текста до слов. На рисунке 4 представлен пример используемого кода токенизации.

```
# Токенизация
max_words = 10000
max_len = 100

tokenizer = Tokenizer(num_words=max_words, oov_token="<OOV>")
tokenizer.fit_on_texts(X_train)

X_train_seq = pad_sequences(tokenizer.texts_to_sequences(X_train), maxlen=max_len, padding="post")
X_test_seq = pad_sequences(tokenizer.texts_to_sequences(X_test), maxlen=max_len, padding="post")
```

Рисунок 4. Код токенизации

Следующий процесс — лемматизация и стемминг. Это два метода редактирования текста, которые используются для приведения слов в тексте к их базовой форме. Лемматизация

использует словари и морфологический анализ для определения исходной формы слова с учетом контекста и типа слова, в то время как стемминг выполняется путем сокращения суффиксов на конце слова, в результате чего получается форма, близкая к исходной форме слова, однако этот метод может привести к неточным результатам. Поскольку контекст и содержание очень важны для данной работы, был использован метод лемматизации, сохраняющий правильный корень слов. Пример кода показан на рисунке 5.

```
# Stanza үшін қазақша модельді жүктейміз
stanza.download("kk")
nlp = stanza.Pipeline("kk", processors="tokenize,mwt,pos,lemma")

# Лемматизация функциясы
def lemmatize_text(text):
    doc = nlp(text)
    lemmas = [word.lemma for sent in doc.sentences for word in sent.words]
    return " ".join(lemmas)

# Лемматизацияны қолдану
df["text_lemmatized"] = df["text"].apply(lemmatize_text)
```

Рисунок 5. Код лемматизации

Поскольку процессор обрабатывает только цифровые данные, следующим обязательным шагом является метод векторизации. Векторизация — это процесс преобразования текста в цифровой формат, точнее, в реальные векторы (цифровые массивы) (Рисунок 6).

```
# TF-IDF векторизациясы
vectorizer = TfidfVectorizer(max_features=5000, ngram_range=(1,2))
X_train_tfidf = vectorizer.fit_transform(X_train)
X_test_tfidf = vectorizer.transform(X_test)
```

Рисунок 6. Код векторизации

Разработка модели и сравнительный анализ. Все модели были обучены на 80% обучающих данных, 10% использовались для проверки, а оставшиеся 10% использовались в качестве тестового набора. Модели оценивались с использованием показателей точности, достоверности, полноты и F1-оценки. В исследовании использовались 3 различные модели машинного обучения:

KazBERT — это модель-трансформер, адаптированная для казахского языка, опубликованная на платформе HuggingFace (@misc{kazbert2025, title={KazBERT: A BERT-based Language Model for Cossack}, author={Gainulla Eraly}, year={2025}, publisher={Hugging Face Model Hub}). Данная модель способна обрабатывать казахские тексты и обеспечивать более глубокое понимание смысла текста. Он был усовершенствован на основе предварительно обученного многоязычного BERT и дополнительно обучен с использованием данных на казахском языке. В процессе обучения использовались функция потери кросс-энтропии и оптимизатор AdamW.

В процессе обучения модели KazBERT использовался API Trainer и были заданы несколько основных параметров. В процессе обучения значения `per_device_train_batch_size` и `per_device_eval_batch_size` были установлены на 8. Эта настройка была выбрана для эффективного использования ресурсов VRAM на устройстве. Увеличение размера пакета может повысить скорость обучения, но необходимо учитывать ограничения памяти графического процессора. Модель проходит по всему набору данных три раза, то есть параметр

num_train_epochs равен 3. Увеличение количества эпох может помочь модели лучше обучаться, но это может привести к переобучению, поэтому в качестве оптимального значения было выбрано три эпохи. Параметр evaluation_strategy="epoch" означает, что модель будет оцениваться на проверочном наборе после каждой эпохи. Это позволяет отслеживать эффективность модели во время обучения. Кроме того, параметр save_strategy="epoch" указывает, будет ли выполняться резервное копирование модели после каждой эпохи. Количество сохраняемых моделей ограничено параметром save_total_limit=2, что позволяет экономить место на диске. Регистрация производилась каждые 500 шагов с использованием параметра logging_steps=500. Это помогает отслеживать ход обучения и позволяет анализировать кривую обучения модели.

В результате обучения модель достигла отличных результатов (Рисунки 7 и 8).

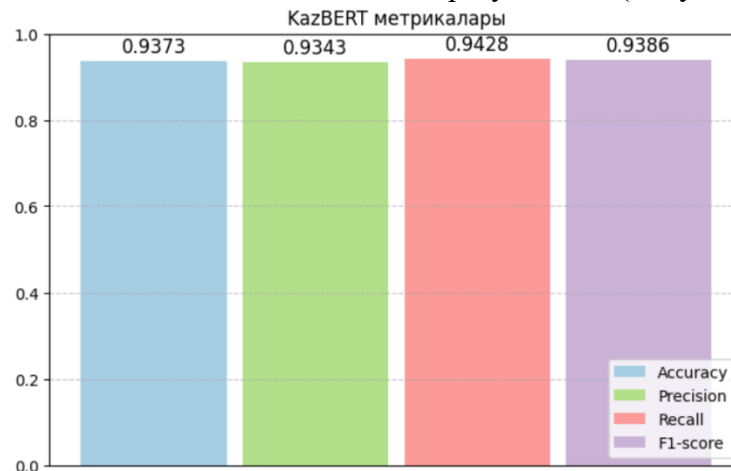


Рисунок 7. Показатели KazBERT

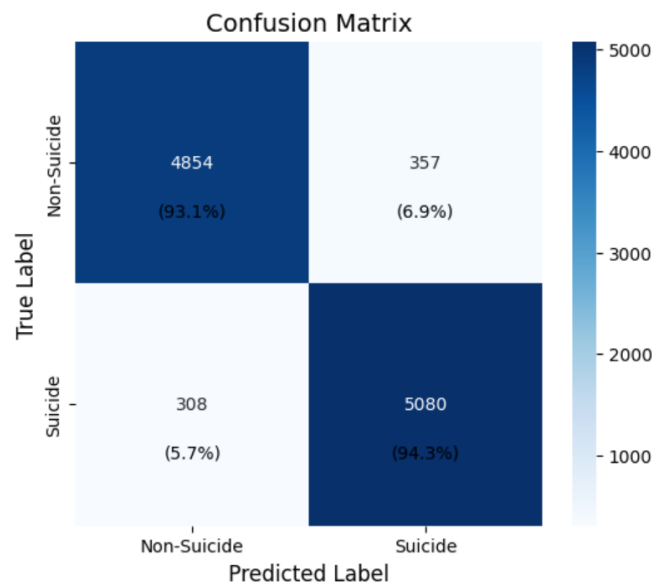


Рисунок 8. Матрица ошибок модели KazBERT

LSTM (долговременная кратковременная память) — это рекуррентная нейронная сеть, которая хорошо работает с последовательными данными. Данная модель позволяет проводить анализ семантических связей текста для выявления суицидального контента.

Первый уровень модели — встраивание, преобразующее слова в векторное представление. Максимальный размер словаря задается переменной max_words, а каждое слово преобразуется в

128-мерный вектор. Параметр `input_length=max_len` определяет длину входных строк. Этот слой позволяет обрабатывать текстовые данные, которые подаются на вход модели в цифровом формате. Слой `LSTM(64, return_sequences=True)` обрабатывает текстовые последовательности и запоминает длинные зависимости. После этого слоя применяется `Dropout(0.3)`, который случайным образом удаляет некоторые нейроны, чтобы предотвратить переобучение. Следующий слой — `LSTM(32)`, представляющий собой еще один рекуррентный слой, состоящий из 32 нейронов. Этот уровень позволяет проводить дальнейший анализ важных особенностей в цепочке. К нему также добавлен слой `Dropout(0.3)`, необходимый для улучшения обобщающей способности модели. Выходной слой — `Dense(1, activation="sigmoid")`. Этот слой состоит только из одного нейрона и использует сигмоидальную функцию активации, поскольку модель выполняет бинарную классификацию. Значение этого слоя колеблется от 0 до 1, что интерпретируется как вероятность. Модель использует функцию стоимости `binary_crossentropy`, поскольку это стандартный выбор для бинарной классификации. Адам используется в качестве оптимизатора, который обеспечивает эффективный градиентный спуск и ускоряет обучение. Основным показателем оценки является точность, которая показывает процент правильно классифицированных образцов. Модель обучалась в течение 5 эпох с использованием метода `fit()`. В каждой эпохе используются мини-партии по 32 образца (`batch_size=32`). Кроме того, во время обучения модель также оценивается на тестовом наборе с использованием параметра `validation_data=(X_test_seq, y_test)`. Это позволяет нам увидеть, какие результаты показывает модель в процессе обучения (Рисунок 9).

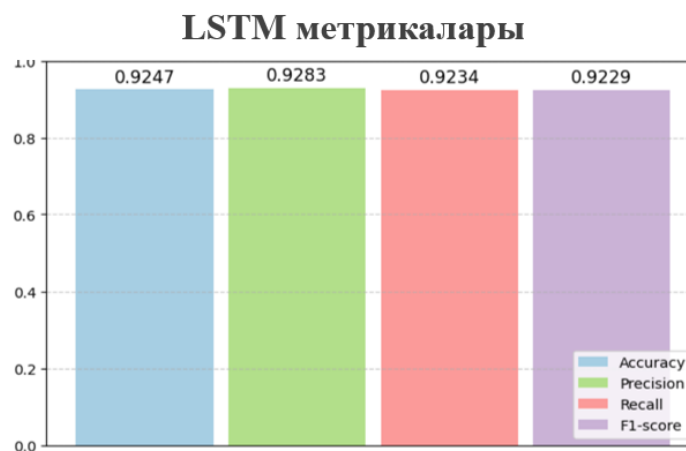


Рисунок 9. Метрики LSTM

Логистическая регрессия — это простая модель, которая взята за базовый метод. Тексты были обработаны с использованием метода векторизации TF-IDF, а бинарная классификация была выполнена на основе логистической регрессии. Результаты этой модели использовались для сравнения со сложными нейронными сетями.

`TfidfVectorizer` используется для векторизации текста. Этот метод измеряет важность слов в тексте, то есть вычисляет частоту встречаемости конкретного слова в документе и его важность по отношению к общему корпусу. Векторизация выполняется с параметром `max_features=5000`, что означает выборку 5000 наиболее важных словесных единиц. Кроме того, параметр `ngram_range=(1,2)` учитывает униграммы (одно слово) и биграммы (фразы из двух слов), что помогает модели лучше понимать контекстную информацию. Сначала обучающий набор данных преобразуется в векторное представление с помощью `vectorizer.fit_transform(X_train)`. Затем тестовый набор обрабатывается таким же образом с использованием `vectorizer.transform(X_test)`.

Векторизованные данные используются в модели логистической регрессии. Логистическая регрессия является одной из наиболее часто используемых моделей для бинарной классификации, поскольку она оценивает вероятности и эффективно проводит разделительную линию между двумя классами. Результаты модели представлены на рисунке 10.

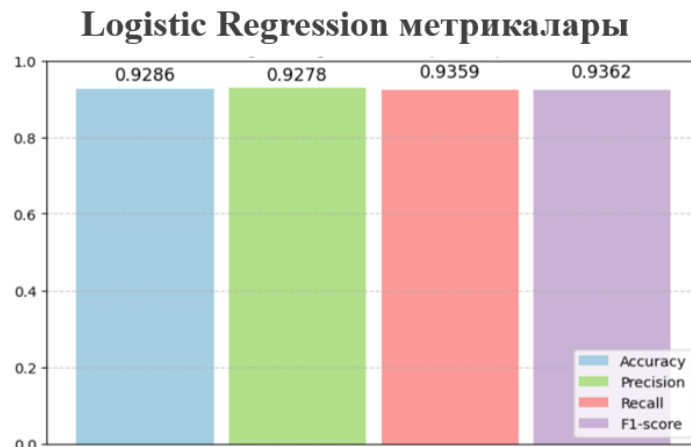


Рисунок 10. Метрики LSTM

В то время как KazBERT показал высокую производительность, LSTM смог глубоко понять структуру текста, несмотря на длительный процесс обучения. А модель логистической регрессии, хотя и быстрая, оказалась несколько слабой в понимании сложных контекстов.

Закключение. Обучены определять суицидальный контекст сообщений в социальных сетях, а затем были проанализированы их результаты. Эффективность моделей сравнивалась с использованием предварительной обработки данных, векторизации текста и нейронных сетей.

Первой использованной моделью был BERT на базе Transformer. Эта предварительно обученная языковая модель позволяет глубже понять смысл текста и учитывает контекстную информацию. В ходе обучения использовался Hugging Face Trainer, оптимизатор AdamW и функция потерь Binary Crossentropy. Данная модель продемонстрировала высокую точность и хорошо различала сложные элементы текста.

Вторая модель представляла собой рекуррентную нейронную сеть LSTM (долговременная краткосрочная память). LSTM позволила эффективно обрабатывать последовательную информацию, учитывая долгосрочные зависимости в текстовых данных. Архитектура модели состояла из двухслойных блоков LSTM, уровней Dropout и, наконец, плотного слоя с сигмоидальной функцией активации для бинарной классификации. Эта модель проще, чем BERT, но имеет более высокую скорость обработки и требует меньше ресурсов.

Третья модель использовала логистическую регрессию, а для векторизации текста использовался подход TF-IDF (Term Frequency-Inverse Document Frequency). Этот метод прост и быстр, он вычисляет важность слов с учетом униграмм и биграмм. Метод TF-IDF + логистическая регрессия менее ресурсоемкий и более простой в интерпретации, но он слабее в плане учета контекстной информации.

Сравнивая результаты, мы обнаружили, что модель BERT показала самую высокую точность, поскольку она глубоко понимает контекст. Модель LSTM и логистическая регрессия, хотя и немного отстают в точности, показали хорошие результаты: первая эффективно обрабатывает большие текстовые массивы, а вторая быстрее и легче.

В целом результаты исследования показывают, что глубокие нейронные сети и предварительно обученные языковые модели более эффективны при обнаружении суицидальных сообщений в социальных сетях. Однако выбранный метод имеет свои преимущества и

недостатки в зависимости от конкретной области применения. В будущем планируется использовать более крупные наборы данных, внедрять методы аугментации и рассматривать ансамблевые подходы для повышения эффективности моделей.

ЛИТЕРАТУРА

1. Всемирная организация здравоохранения. (2019). *Уровень самоубийств во всем мире в 2019 году: оценки состояния мирового здравоохранения.*
2. ЮНИСЕФ Казахстан. (2021). *Оценка мероприятий по профилактике суицида в Казахстане: Кызылординская и Восточно-Казахстанская области.*
3. Правительство Казахстана. (2023). *Комплексный план по защите детей и профилактике суицидов в Казахстане (2023-2025 годы).*
4. Юрафски Д. и Мартин Дж. Х. (2021). *Обработка речи и языка (3-е изд.).*
5. Блей, Д.М., Нг, А.Ю. и Джордан, Мичиган (2003). *Скрытое распределение Дирихле. Журнал исследований машинного обучения, 3, 993-1022.*
6. Гриффитс, Т.Л. и Стейверс, М. (2004). *Поиск научных тем. Труды Национальной академии наук, 101 (Приложение 1), 5228-5235.*
7. Юрафски Д. и Мартин Дж. Х. (2021). *Обработка речи и языка (3-е изд.).*
8. Де Чоудхури, С., и Джсаганнатх, П. (2018). *Сравнение наивного байесовского классификатора с другими алгоритмами машинного обучения при классификации текстов. Международный журнал компьютерных приложений, 975, 1-5.*
9. Ким, Ю. (2014). *Свёрточные нейронные сети для классификации предложений. Труды конференции 2014 года по эмпирическим методам обработки естественного языка (EMNLP 2014), 1746–1751.*
10. Чжан, Х. и Уоллес, ВС (2015). *Анализ чувствительности (и практическое руководство) сверточных нейронных сетей для классификации предложений. Труды 8-й Международной конференции по языковым ресурсам и оценке (LREC 2015), 1–9.*
11. Хохрейтер С. и Шмидхубер Дж. (1997). *Долговременная кратковременная память. Нейронные вычисления, 9(8), 1735–1780.*
12. Девлин Дж., Чанг М.В., Ли К. и Тутанова К. (2019). *BERT: Предварительная подготовка глубоких двунаправленных преобразователей для понимания языка. Труды NAACL-HLT 2019, 4171–4186.*
13. Мэннинг, К. Д., Сурдеану, М., Бауэр, Дж., Финкель, Х., Бетхард, С. и Макклоски, Д. (2014). *Набор инструментов обработки естественного языка Stanford CoreNLP. Труды 52-го ежегодного заседания Ассоциации компьютерной лингвистики (ACL 2014), 55–60.*
14. Саркер, И.Х., и Рирази, Х. (2020). *KazBERT: Предварительно обученная модель-трансформатор для классификации казахских текстов. Труды Международной конференции по искусственному интеллекту и компьютерному зрению, 102–111.*
15. Конно А., Крушевски Г., Лэмпл Г., Барро Л. и Жулен А. (2020). *Неконтролируемое кросс-языковое репрезентативное обучение в больших масштабах. Труды 58-го ежегодного собрания Ассоциации компьютерной лингвистики (ACL 2020), 8440–8451.*

УДК 004.89

Жамалбек М.Ұ. (Астана, ЕНУ имени Л.Н. Гумилева)

Жартыбаева М.Г. (Астана, ЕНУ имени Л.Н. Гумилева)

РАЗРАБОТКА СИСТЕМЫ КЛАССИФИКАЦИИ ПО ГОЛОСОВЫМ ДАННЫМ С ПОМОЩЬЮ НЕЙРОННЫХ СЕТЕЙ

Современные информационные технологии находят широкое применение в задачах анализа речи и аудиоданных. Разработка интеллектуальных систем, способных извлекать не только смысловую составляющую речи, но и определять характеристики говорящего, приобретает всё большую актуальность. Определение пола, примерного возраста и эмоционального состояния по голосу является важной задачей, используемой в различных сферах: от голосовых ассистентов и смарт-систем до биометрических сервисов и маркетинговых инструментов.

Целью данной работы является создание интеллектуальной веб-системы, которая позволяет автоматически определять ключевые характеристики пользователя на основе анализа его голосового сообщения. В процессе выполнения работы решались задачи проектирования архитектуры системы, разработки программного обеспечения, подготовки данных и обучения модели для классификации пола, возраста и эмоций.

Разработанная система имеет модульную структуру. В качестве серверной части используется фреймворк Django, что обеспечивает высокую гибкость и возможность интеграции с различными компонентами. Пользователь взаимодействует с системой посредством веб-интерфейса, представляющего собой чат, где можно отправлять как текстовые, так и голосовые сообщения. Все отправленные данные автоматически сохраняются в базе данных для последующего анализа.

Ключевым элементом системы является блок обработки аудиосигналов. На данном этапе применяются предобученные модели эмбедингов, такие как Wav2Vec2, которые позволяют преобразовать входной звуковой сигнал в эмбединг — компактное и информативное представление аудиоданных в виде вектора фиксированной длины. Это представление содержит в себе важные акустические признаки, включая тембр, интонацию, частотные характеристики, динамику речи и другие параметры, отличающие голоса между собой.

Полученные эмбединги передаются в нейросетевой классификатор, который в рамках данной работы был дообучен для решения трёх задач:

1. Определение пола (мужской/женский);
2. Оценка примерного возраста (разбиение на группы);
3. Определение эмоционального состояния (спокойный, радостный, грустный и др.).

Для обучения классификатора использовались открытые датасеты с разметкой по каждому из признаков. В процессе разработки были проведены этапы анализа данных, очистки, балансировки классов и настройки гиперпараметров модели. Для оценки качества работы модели применялись метрики, такие как точность, полнота, среднеквадратическая ошибка и другие.

Особенностью реализованного решения является не только определение характеристик пользователя, но и интеграция результатов в интерфейс. После обработки каждого голосового сообщения пользователь в чате получает ответ, в котором указывается предполагаемый пол, возрастная категория и эмоция. Это делает взаимодействие с системой наглядным и интуитивно понятным.

В рамках работы была также реализована система хранения и отображения истории взаимодействия. Это позволяет не только отслеживать переписку, но и сохранять все результаты анализа для последующего использования и возможного совершенствования модели.

Проведенное тестирование системы показало её работоспособность, адекватность прогнозов и возможность дальнейшего расширения. Данное решение может быть использовано в реальных приложениях для задач биометрической идентификации, создания интеллектуальных голосовых помощников, проведения исследований в области психологии и социологии.

Система легко масштабируется и позволяет в будущем внедрить дополнительные функции, такие как определение акцента, индивидуальных особенностей речи или даже личностных характеристик. Разработанная платформа является универсальной и может стать основой для сложных систем анализа речи и построения человеко-ориентированных интеллектуальных сервисов.

УДК 004.896

Жарасов Ү.А. (Караганда, КарТУ имени А. Сагинова)

Мухаметжанова Б.О. (Караганда, КарТУ имени А. Сагинова)

ИССЛЕДОВАНИЕ И РАЗРАБОТКА СИСТЕМЫ УПРАВЛЕНИЯ ПРОЦЕССОМ СОРТИРОВКИ ПРОДУКЦИИ НА ОСНОВЕ НЕЙРОННОЙ СЕТИ

Интеграция нейронных сетей в промышленные системы управления представляет собой трансформационный сдвиг в сторону интеллектуальной автоматизации. Целью данного исследования является разработка системы сортировки овощей в режиме реального времени путем объединения нейросетевой модели YOLOv8 с компонентами промышленной автоматизации, включая программируемый логический контроллер (ПЛК) Siemens и интерфейс на базе Django. Задача состоит в том, чтобы устранить ограничения ручной сортировки, такие как субъективность и масштабируемость, за счет использования передового обнаружения объектов и бесшовной программно-аппаратной интеграции. Новизна заключается в уникальном сочетании YOLOv8 для высокоточного обнаружения, Snap-7 для связи с ПЛК и Django для удобного управления. Актуальность данной работы подчеркивается растущим спросом на точность в пищевой промышленности, где автоматизированный контроль качества позволяет сократить отходы и повысить производительность.

Нейронные сети изменили представление о промышленной автоматизации в различных областях. Ври и другие [1] продемонстрировали возможность анализа изображений в реальном времени с помощью НС на промышленных контроллерах, что позволило создать индивидуализированные производственные системы. Их работа подчеркивает адаптивность NN в динамичных производственных средах - принцип, критически важный для нашей системы сортировки. В области контроля качества Фергюсон и другие [2] использовали сверточные нейронные сети (CNN) для обнаружения дефектов на рентгеновских снимках, что позволило утвердить NN в качестве надежного инструмента для работы со сложными наборами данных. Аналогичным образом, Абдиси и Харб [4] продемонстрировали предиктивное обслуживание подшипников электродвигателей на основе СЯ, подчеркнув их способность обрабатывать данные датчиков для принятия упреждающих решений.

Интеграция NN выходит за рамки производства. Чен и другие [3] применили трансферное обучение с глубокими ИНС для оптимизации систем ОВКВ в интеллектуальных зданиях, продемонстрировав адаптивность предварительно обученных моделей. В робототехнике Solowjow et al. [5] использовали глубокое обучение для решения задач захвата в промышленности, что подчеркивает синергию между NN и управлением роботами. Эти исследования в совокупности подтверждают универсальность ИНС в решении промышленных задач, формируя основу для разработки нашей системы.

Архитектура системы состоит из трех основных компонентов:

1. Модель YOLOv8: Обучалась на наборе данных из 30 000 аннотированных изображений овощей (испорченные и хорошие) с использованием CVAT для аннотирования ограничительных рамок. Гиперпараметры были оптимизированы для баланса точности и вычислительной эффективности.

2. Интерфейс Django: Разработан для мониторинга и управления в режиме реального времени, включает панели визуализации данных и интеграцию команд ПЛК.

3. Интеграция с ПЛК Siemens: Связь между Django-сервером и ПЛК осуществлялась с помощью Python-модуля Snap-7, что позволило управлять приводами (например, пневматическими цилиндрами) в режиме реального времени на основе результатов классификации YOLOv8.

В качестве тестовой среды использовался симулятор технологической линии Festo, датчики и пневматические приводы синхронизировались через ПЛК. Показатели обучения включали точность, запоминание и среднюю точность (mAP), проверенные на 20-процентном наборе данных.

Модель YOLOv8 показала отличные результаты (табл. 1):

- точность: 95,63 %
- Recall: 97.17%
- mAP@50: 98.86%

Таблица 1 - метрики результатов обучения

Метрика	Значение
Precision (B)	0.9563
Recall (B)	0.9717
mAP@50 (B)	0.9886
mAP@50-95 (B)	0.8639
Validation Box Loss	0.5732
Validation Classification Loss	0.2643
Validation DFL Loss	0.9225

Анализ потерь:

- Box Loss (0,5732) указывает на точную локализацию, а Classification Loss (0,2643) подтверждает минимальную ошибку классификации. Немного повышенный показатель DFL Loss (0,9225) говорит о незначительной доработке регрессии ограничительных блоков.

Кривые PR и F1 (Рисунок 1) продемонстрировали стабильную обобщенность при разных порогах доверия. В симуляционных тестах система сортировала овощи с точностью 98 %, сократив количество ложных срабатываний до <2 %. Ключевые преимущества включают:

- Производительность в реальном времени: Snap-7 обеспечил субсекундную задержку между обнаружением и реакцией исполнительного механизма.

- Масштабируемость: Модульная архитектура Django-PLC позволяет адаптировать систему к другим типам продуктов.

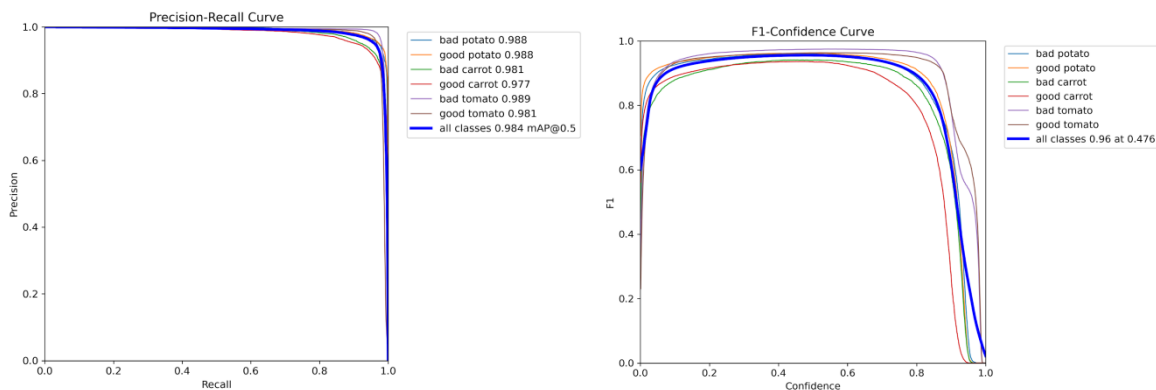


Рисунок 1 - Кривая точности-результата (кривая PR) и F1-доверие

Среди трудностей - неоднородность набора данных, изменение освещения и ориентации овощей, что потребовало значительного дополнения данных. Вычислительная нагрузка на ПЛК также требовала оптимизации, чтобы избежать узких мест во время высокоскоростной сортировки.

Данное исследование позволило успешно интегрировать YOLOv8 с компонентами промышленной автоматизации для создания высокоточной системы сортировки овощей. Полученные результаты подтверждают, что системы управления на основе NN являются жизнеспособными решениями для обеспечения качества в реальном времени, достигая точности более 95 %. Дальнейшая работа будет направлена на оптимизацию модели для различных условий окружающей среды и расширение ее применения на другие скоропортящиеся товары. Объединение NN с промышленным оборудованием не только повышает эффективность, но и создает прецедент для интеллектуальной автоматизации в различных отраслях.

Список использованных источников

1. Wree C. et al., *Real-Time Image Analysis with Neural Networks on Industrial Controllers*, Springer, 2022.
2. Ferguson M. et al., *Detection and Segmentation of Manufacturing Defects with CNNs*, Smart and Sustainable Manufacturing Systems, 2018.
3. Chen Y. et al., *Transfer Learning for HVAC Control*, Journal of Cleaner Production, 2020.
4. Abdisa W.T. et al., *NN-Based Motor Bearing Fault Diagnosis*, International Journal of Intelligent Systems, 2019.
5. Solowjow E. et al., *Industrial Robot Grasping with Deep Learning*, arXiv, 2020.

ӨОЖ 519.677

Жиенбай А. Ғ. (Алматы, Абай ат. ҚазҰПУ)

ГЕНЕТИКАЛЫҚ АЛГОРИТМДЕРДІҢ ЖАСАНДЫ ИНТЕЛЛЕКТ ЖҮЙЕЛЕРІНДЕ ҚОЛДАНЫЛУЫН САЛЫСТЫРМАЛЫ ТАЛДАУ

Генетикалық алгоритмдер (ГА) – жасанды интеллект (ЖИ) жүйелерін оңтайландырудың тиімді әдісі. Ол табиғи эволюция қағидаларын қолданып, нейрондық желілердің параметрлерін баптауда және үлкен деректерді өңдеуде қолданылады [1].

John H. Holland (1992) ГА-ның биологиялық эволюция принциптеріне негізделгенін көрсетті. Ол ГА-ның іздеу кеңістігін тиімді зерттеу қабілетін атап өтті [2]. Ал, Stuart Russell мен Peter Norvig (2020) градиенттік әдістердің ГА-ға қарағанда локалды минимумдарға жылдамырақ жететіндігі талданған. Дегенмен ГА глобалды минимумды табуға қабілетті, бұл оның маңызды артықшылығы [3].

ГА-ның негізгі кезеңдері: популяцияны генерациялау, фитнес-функцияны бағалау, үздік шешімдерді таңдау, кроссовер және мутация. Фитнес-функция мына түрде есептеледі:

$$F(x) = \sum_{i=1}^m w_i f_i(x)$$

мұндағы w_i – оңтайландыру критерийлерінің салмақ коэффициенттері, $f_i(x)$ – жеке оңтайландыру функциялары [3].

AutoML жүйелерінде біріктірілген жағдайда ГА-ның тиімділігінің артатыны [1] көрсетіледі. Сонымен қатар, онда ГА-ның есептеу ресурстарына жоғары талап қоятыны, бұл оның негізгі шектеулерінің бірі екені атап өтіледі.

Нейрондық желілерді бейімдеуде осы формула қолданылады:

$$w'_{ij} = w_{ij} + \eta \cdot \sigma \cdot N(0,1)$$

мұндағы w_{ij} – синапстық салмақ коэффициенттері, η – үйрену қарқыны, $N(0,1)$ – нөлдік математикалық күтімі бар қалыпты бөлінген кездейсоқ шама [1].

Генетикалық оңтайландыру алгоритмдері параметрлерін динамикалық реттеу және нақты практикалық есептерде қолдану нәтижесінде стандартты ГА-ға бейімделген селекция және мутация операторларын қолдану алгоритмінің жинақталу жылдамдығын арттырып, локалды минимумдардан шығу ықтималдығын жоғарылататындығы күрделі көп өлшемді оңтайландыру есептерінде тиімділігі көрсетілді. Сонымен қатар, нақты қолданбалы есептерде параметрлерін динамикалық түрде бейімдеу алгоритмінің тиімділігін арттыратыны анықталды. Есептеу күрделілігі жоғары болғанымен градиенттік әдістермен салыстырғанда іздеу кеңістігін терең зерттеуге мүмкіндік береді. Бұл инновациялық тәсілдер үлкен деректер мен машиналық оқыту модельдерін оңтайландыруда ГА-ның кеңінен қолданылуына жол ашады.

Пайдаланылған дереккөздердің тізімі

1. "Вырачиваем ИИ — Генетические алгоритмы: введение" <https://habr.com/ru/articles/498914/>, 2020.
2. John H. Holland. *Adaptation in Natural and Artificial Systems: An Introductory Analysis with Applications to Biology, Control, and Artificial Intelligence*, 1992.
3. Stuart Russell, Peter Norvig. *Artificial Intelligence: A Modern Approach*, 2020.

УДК004.4

Закирова Ф. Р.
 (Астана, ЕНУ им. Л.Н. Гумилева)

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ПРОГНОЗА ГЛОБАЛЬНОЙ УРОЖАЙНОСТИ В УСЛОВИЯХ ИЗМЕНЕНИЯ КЛИМАТА

Современное сельское хозяйство сталкивается с растущим влиянием климатических изменений, что ставит под угрозу глобальную продовольственную безопасность. Настоящее исследование направлено на оценку динамики урожайности основных сельскохозяйственных культур и построение прогностических моделей, позволяющих выявить региональные риски и определить наиболее эффективные меры адаптации.

Актуальность темы обусловлена необходимостью своевременного реагирования на экстремальные погодные условия, уменьшение водных ресурсов и смещение климатических зон. Для решения поставленных задач использовались статистические методы (корреляционный анализ, описательный анализ) и алгоритмы машинного обучения (линейная регрессия, дерево решений). Источником данных послужили временные ряды глобального производства сельскохозяйственных культур (1961–2013 гг.) с учётом широты, долготы и климатических параметров.

Основные этапы и методология

1. Сбор и подготовка данных

- Использованы открытые наборы данных ФАО, охватывающие период 1961–2013 гг.
- Проведена очистка пропусков и выбросов, нормализация показателей урожайности, кодирование категориальных признаков.

2. Разведочный анализ (EDA)

- Выявлены исторические тенденции: рост объёмов производства, региональные отличия по показателям.
- Корреляционный анализ показал сильную взаимозависимость объёмов в соседние годы и умеренную связь с широтой и долготой (рисунок 1).

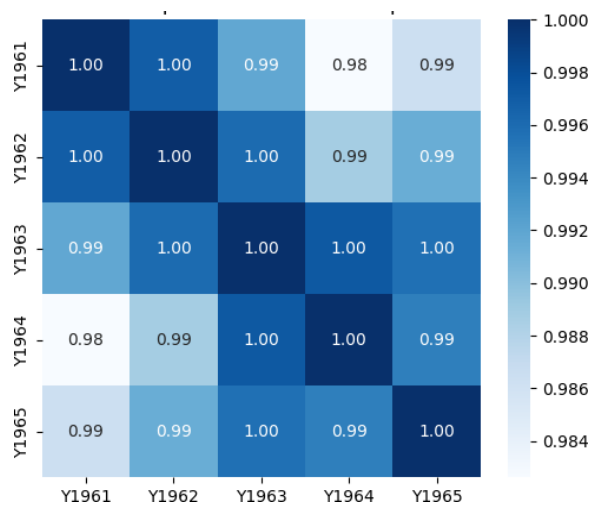


Рисунок 1 – Корреляция

3. Построение моделей

- Линейная регрессия: выявила решающее влияние данных последних лет (особенно 2012 г.) на прогнозы; коэффициент детерминации (R^2) в ряде случаев превышает 0,99 (рисунок 2).

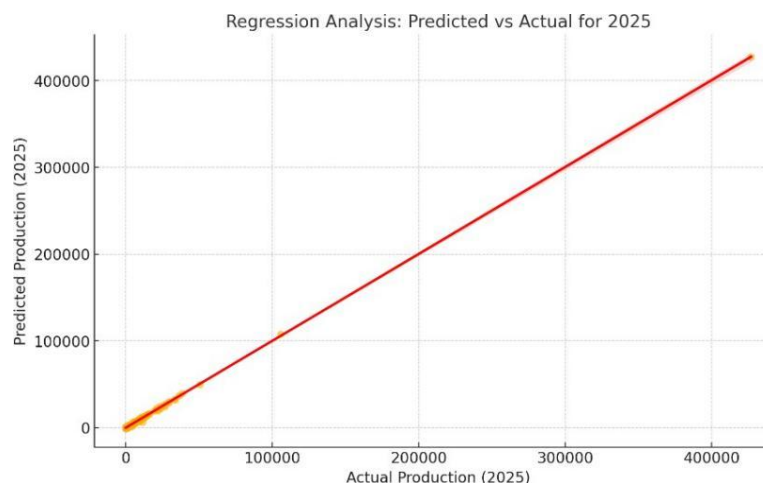


Рисунок 2 – Линейная регрессия

- Дерево решений: позволило учесть нелинейные зависимости, выделить «критические» пороги объемов производства и определить наиболее уязвимые зоны (при объемах < 30 тыс. тонн).

4. Прогнозирование

- По итогам моделирования ожидается относительно стабильная динамика вплоть до 2025 г. с возможным локальным снижением в ряде регионов.
- Высокопродуктивные регионы (порог > 300 тыс. тонн) способны компенсировать спад в уязвимых зонах при условии грамотного распределения ресурсов.

Результаты и выводы

- Роль последних данных: объемы производства за 2012 г. в наибольшей степени влияют на будущие прогнозные значения, отражая современные рыночные и агроклиматические тенденции.
- Неравномерность развития: выявлены существенные различия в урожайности между странами и культурами, указывающие на необходимость целенаправленной поддержки регионов с риском снижения производства.
- Высокая точность регрессионных моделей: $R^2 = 0,99+$ подтверждает практическую применимость методик при планировании и оценке устойчивости агросектора.
- Практические рекомендации:
 1. усиливать поддержку уязвимых территорий через инвестиции в агротехнологии и рациональное управление водными ресурсами;
 2. расширять производство в высокоэффективных регионах, чтобы повысить общую продовольственную безопасность;

3. дополнительно включать в модели данные по температуре, осадкам и экономическим факторам (торговые барьеры, цены на сырьё) для более точного прогнозирования.

Таким образом, комплексный подход на основе статистических методов и машинного обучения демонстрирует высокую эффективность при оценке влияния климатических факторов на глобальную урожайность. Результаты исследования могут служить основой для выработки стратегий адаптации и управления рисками, связанных с изменением климата, обеспечивая более устойчивое сельскохозяйственное производство в долгосрочной перспективе.

Список использованных источников

1. Food and Agriculture Organization of the United Nations (FAO). FAOSTAT: Statistical Database. 2023.
2. Kaggle. World Food and Feed Production: Global Agricultural Statistics. 2024.
3. Rosenzweig, C., & Hillel, D. Climate Change and the Global Harvest. Oxford University Press, 1998.
4. Lobell, D. B., & Field, C. B. Global scale climate–crop yield relationships and the impacts of recent warming. Environmental Research Letters, 2(1), 014002, 2007.
5. Montgomery, D. C., Peck, E. A., & Vining, G. G. Introduction to Linear Regression Analysis (6-е изд.). John Wiley & Sons, 2021.

УДК004.4:658.6

Зиятбекова Г.З. (Алматы, КазНУ им. аль-Фараби)
Алиаскар М.С. (Алматы, КазНУ им. аль-Фараби)
Бурегулов А.Д. (Алматы, КазНУ им. аль-Фараби)
Жаксымбет А.Т. (Алматы, КазНУ им. аль-Фараби)

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС МОНИТОРИНГА УРОВНЯ ЗАПОЛНЕННОСТИ ВОДОЕМА

Аннотация. Работа посвящена мониторингу уровня заполняемости водоема. Цель исследования заключается в создании гибридной модели для прогнозирования последствий разрушения гидротехнических объектов, таких как дамбы и плотины. Достижение этой цели позволит соотнести разработанную модель с реальными наблюдениями и данными. Актуальность исследования обусловлена ростом частоты и масштабов разрушительных наводнений, вызванных разрушением гидротехнических сооружений, что подчеркивает необходимость в разработке эффективных методов прогнозирования и предотвращения подобных событий. Математическое моделирование гидротехнических процессов заключается построением математической модели гидротехнических процессов, происходящих в водоеме и позволяющую оценивать уровень воды в реальном времени.

Ключевые слова: гидротехнические сооружения, прорыв плотины, селевой поток, численное моделирование, интервальная математика, прогнозирование.

1 Введение

Территория Казахстана обладает значительными водными ресурсами. Озера и реки являются источниками пресной воды, которая используется как в жизнеобеспечении населения страны, так и для полива сельскохозяйственных угодий. В горной местности Казахстана имеются моренные озера, расположенные на большой высоте. Использование воды в качестве источника энергии способствовало развитию в Казахстане гидроэнергетической отрасли. В стране функционируют более 30 гидроэлектростанций. Однако фактом остается и разрушительная сила воды, способная сметать на своем пути целые поселения. Опасность таится не столько в затоплении, сколько в возможности образования селевых потоков, которые могут нести камни, ледяные глыбы и т.д. [1].

В настоящее время на территории республики имеются 1665 гидротехнических сооружений, в том числе водохранилищ с объемом более 1,0 м³ – 319 штук (из них в республиканской собственности – 83 штук, в коммунальной собственности – 200 штук, в частной собственности – 34 штук и бесхозные – 60 штук); плотин – 443 штук (из них в республиканской собственности – 32 штук, в коммунальной собственности – 346 штук, в частной собственности – 45 штук и бесхозные – 20 штук); дамб – 125 штук и другие ГТС – 778 штук.

На сегодняшний день эксплуатируются такие крупные водохранилища, как Астанинское построенное в 1970 году с емкостью 410,9 млн.м³, Селетинское – 1965 году (230 млн.м³), Каргалинское – 1975 году (280 млн.м³), Бартогайское – 1982 году (320 млн.м³), Капшагайское – 1970 году (18560 млн.м³), Терс-Ащибулакское – 1963 году (158,6 млн.м³), Тасоткельское – 1974 году (620 млн.м³), Самаркандское – 1939 году (253,7 млн.м³), Верхне-Тобольское – 1972 году (816,6 млн.м³), Каратомарское – 1965 году (586 млн.м³), Бугуньское – 1967 году (370 млн.м³) и другие.

Многие специалисты неоднократно пытались найти баланс между использованием пойменных и прибрежных земель и предотвращением убытков от наводнений. Однако этот вопрос остаётся открытым. Для анализа возможности эксплуатации прибрежных земель необходимо учитывать потенциальный ущерб, который могут вызвать наводнения, в том числе из-за разрушения плотин [2, 3]. Особенно значительные потери наблюдаются в сельскохозяйственных районах, где наводнения повреждают посевы и разрушают инженерные и мелиоративные системы.

Защита территорий от наводнений включает мероприятия по укреплению берегов. Основной метод сегодня – это строительство дамб обвалования. Стоимость возведения дамб обвалования зависит от их длины и высоты, что делает необходимым оптимизацию их параметров. Один из рациональных подходов заключается в использовании моделирования речных потоков для выявления потенциальных зон затопления. На основе этих моделей можно точно определить параметры дамб обвалования. Такие расчеты позволяют выбрать наиболее эффективные параметры укрепительных сооружений для защиты территорий от наводнений. Определение точности и эффективности моделей, которые предсказывают распространение волн после прорыва плотин, представляет собой достаточно сложную задачу.

В 2010 году весной в Алматинской области произошло трагическое наводнение, которое унесло жизни людей и нанесло значительный ущерб. Причиной этой катастрофы стал прорыв плотины. Аналогичная ситуация повторилась в Карагандинской области в 2014 году.

1 мая 2020 года в Узбекистане на Сардобинском водохранилище произошло разрушение дамбы, что привело к прорыву миллионов кубометров воды через бетонные

заграждения. В результате, из зоны бедствия в Узбекистане эвакуировали свыше 85 тысяч человек, а в Казахстане, куда также дошла вода, эвакуировали более 30 тысяч.

2024 год оказался особенно насыщенным на подобные происшествия. В Айтекебийском районе Актюбинской области 29 марта произошел прорыв Щербаковской плотины. 7 апреля наполнение Сергеевского водохранилища достигло 175%, и 10 апреля высота перелива превысила исторический рекорд — 422 сантиметра. Также 31 марта в селе Байкент Алматинской области был зафиксирован прорыв плотины Ворошиловского водохранилища.

Эти тревожные события стали серьёзным предостережением для всех жителей страны и показали необходимость предотвращения подобных ситуаций в будущем. Для повышения уровня безопасности гидротехнических сооружений нужно разрабатывать рекомендации по их оснащению современными контрольно-измерительными приборами и оборудованием.

2 Постановка задачи

Современные системы мониторинга должны постоянно отслеживать природные и техногенные явления и процессы, чтобы своевременно выявлять возможные угрозы для людей и их окружающей среды. Основная задача мониторинга — предоставить данные для точного прогноза чрезвычайных ситуаций, используя объединенные интеллектуальные, информационные и технологические ресурсы различных ведомств и организаций, занимающихся мониторингом различных видов опасностей. Мониторинговая информация является основой для прогнозирования [4, 5].

Микропроцессорные технологии прочно вошли в повседневную жизнь, открывая широкие возможности благодаря своей универсальности, гибкости, простоте проектирования и практически неограниченным возможностям в области усложнения алгоритмов обработки данных. Современные достижения в разработке разнообразных датчиков и удешевление микропроцессоров позволили значительно расширить использование аппаратно-программных средств для мониторинга климатических параметров. Особенно это проявилось в широком применении контроллеров Arduino, которые, благодаря обширной базе разработанных датчиков и средств их связи с компьютерами, стали популярным решением для прикладных задач.

Анализ прошедших событий позволяет выделить два типа водоемов: горные и равнинные. Горные водоемы, как правило, имеют небольшую площадь, значительную глубину и выраженный перепад высот ниже плотины. В случае разрушения плотины водный поток быстро распространяется, разрушая все на своем пути, как это произошло в Кызылагаше. Равнинные водоемы, напротив, характеризуются большой площадью и небольшой глубиной. Особую опасность для них представляют ветровые нагрузки, которые в случае сильного ветра, направленного на дамбу, могут привести к переливу воды, что наблюдалось в Узбекистане. В свете этих наблюдений, нами было принято решение учитывать следующие параметры: уровень заполненности водоемов, влажность и температуру, количество осадков, направление и силу ветра.

2.1 Алгоритм решения задачи

Для эффективного использования разрабатываются системы мониторинга состояния водоемов в реальном времени, основанные на автоматизации процессов сбора и обработки информации. В таких автоматизированных системах мониторинга применяются различные датчики: инклинометрические, течи, деформации, температуры, давления на грунт и уровня воды [6, 7].

В процессе эксплуатации гидротехнических сооружений, особенно плотин, разрушение напорного фронта является одной из наиболее опасных аварийных ситуаций, приводящей к значительным экономическим, экологическим и социальным последствиям.

Для информационных систем мониторинга необходимо обеспечить сбор данных в реальном времени. Такая интеграция позволит осуществлять мониторинг уровня воды даже в труднодоступных моренных озерах. Накопленные данные будут передаваться в ситуационные центры и использоваться специальными службами для прогнозирования возможных паводков и наводнений, расчета расхода воды и в других целях. Система мониторинга может быть связана с другими автоматизированными системами, такими как системы забора и сброса воды на плотинах гидроэлектростанций, системы тревожного оповещения и другими функционально взаимосвязанными системами. Внедрение системы мониторинга уровня воды позволит эффективно предотвращать возникновение чрезвычайных ситуаций [8, 9].

2.2 Численные расчеты

Наша разработка представляет собой комплексную систему мониторинга состояния водоемов, предназначенную для предупреждения прорыва плотин. Она включает четыре основных блока:

1. Блок сбора и передачи данных о текущем уровне воды, влажности и температуре на гребне плотины.
2. Блок сбора и передачи данных о ветровых условиях.
3. Блок обработки и анализа данных (сервер), который оценивает текущую ситуацию и уровень угрозы.
4. Блок прогнозирования последствий возможного прорыва плотины.

Используемые компоненты

Для создания автономной системы передачи климатических данных мы применили одноплатный компьютер Raspberry Pi 4 B+ и микроконтроллер Arduino Uno.

- Arduino Uno:

- Устройство, оснащенное микроконтроллером ATmega 328, упрощает работу с микроконтроллером. Подключение осуществляется через AC/DC адаптер, батарею или USB-кабель (на рисунке 1 помечено цифрой 3).

- Raspberry Pi 4 B+:

- Компактный одноплатный компьютер, который совмещает в себе все компоненты стандартного компьютера на одной плате. Он поддерживает операционные системы Linux и Windows (на рисунке 1 помечено цифрой 6).

Функциональные блоки системы

- Блок сбора и передачи данных о текущем состоянии:

- Размещенные на гребне плотины датчики измеряют уровень воды, влажность и температуру. Данные отправляются на микропроцессор Arduino для предварительной обработки и дальнейшей передачи на сервер.

- Блок сбора и передачи ветровой информации:

- Этот блок базируется на беспроводной метеостанции модели WH108, данные с которой передаются на Raspberry Pi и далее через Arduino на сервер.

Основные данные и датчики

Ключевые данные для мониторинга рисков прорыва плотины поступают от датчиков уровня воды, температуры, осадков и ветровой нагрузки.

- Датчик DHT11:

- Устройство для измерения температуры и влажности, с одним цифровым выходом. Частота опроса не превышает одного раза в 1-2 секунды (на рисунке 1 помечено цифрой 2).

Технические характеристики DHT11:

- Напряжение питания и I/O: 3-5 В

- Диапазон измерения влажности: 20-80% с точностью $\pm 5\%$
- Диапазон измерения температуры: 0-50°C с точностью $\pm 2^\circ\text{C}$
- Частота опроса: до 1 Гц (раз в секунду).

Иллюстрации и компоненты

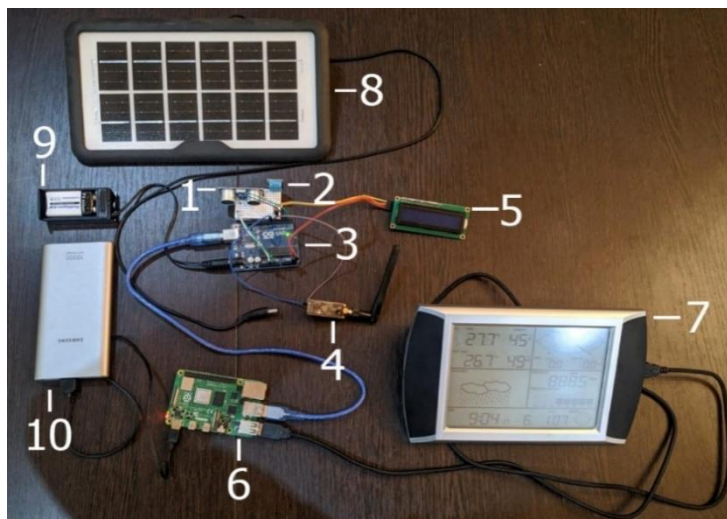


Рисунок 1: Основной блок ПАК



Рисунок 2: Блок приема и передачи метео-информации



Рисунок 3: Бензиновый генератор



Рисунок 4: Автономная подсистема приема и передачи данных об уровне воды и температуре на солнечном питании

На рисунке 1 представлены основные компоненты системы:

1. HC-SR04: Ультразвуковой модуль для измерения расстояния.
2. DHT11: Датчик температуры и влажности.
3. Arduino Uno: Микроконтроллер.
4. nRF24L01 PA LNA: Радиомодуль для передачи данных.
5. Дисплей 1602 с I2C адаптером: ЖК-дисплей для отображения информации.
6. Raspberry Pi 4 Model B: Одноплатный компьютер.
7. WH108: Сенсорный экран беспроводной метеостанции.
8. Солнечная панель: для питания системы.
9. Кабель питания для Arduino от батареи "Крона".
10. Samsung, 10000Mah: Внешний аккумулятор.

Спецификации компонентов

- Ультразвуковой датчик US-015:
 - Используется для измерения уровня воды. Работает, посылая звуковые волны на определенной частоте (на рисунке 1 помечен цифрой 1).
- Технические характеристики US-015:
 - Напряжение питания: 5 В
 - Потребляемый ток: 20 мА
 - Режим ожидания: 2,2 мА
 - Угол измерения: 15°
 - Диапазон измерения: 2 - 700 см
 - Точность: 0,3 см + 1%
- Радиомодуль NRF24L01+PA+LNA:
 - Предназначен для передачи данных по радиоканалу. Работает в диапазоне частот ISM (Industrial, Scientific, Medical), поддерживает передачу данных на расстояние до 2 Мбит/сек и частотный диапазон 2400 - 2524 МГц (на рисунке 1 помечен цифрой 4).
- ЖК-дисплей 1602 с I2C адаптером:
 - Дисплей с подсветкой для отображения информации, подключен к Arduino (на рисунке 1 помечен цифрой 5).
- **Метеостанция WH108 представлена на рисунке 2.** Сенсорный экран для мониторинга и прогноза погоды (на рисунке 1 помечен цифрой 7).
- Переносная бытовая метеостанция с беспроводной связью между датчиками и приемником, обеспечивающая подключение к компьютеру через USB порт для записи и анализа данных, а также возможность самостоятельного прогнозирования погоды. Основной блок метеостанции отображает важную текущую информацию о погоде, полученную от наружных датчиков: температура, влажность, атмосферное давление, направление и скорость ветра, а также количество выпавших осадков. Наружные датчики включают в себя удобные монтажные кронштейны и штангу, позволяющие разместить их за окном, в саду или на крыше дома для получения наилучших метеорологических данных.

Энергоснабжение системы

При отсутствии стационарного электрообеспечения предусмотрены следующие варианты питания:

1. **Солнечная панель** (на рисунке 1 помечена цифрой 8).
2. **Батарейное питание:** Кабель для подключения Arduino от батареи "Крона" (на рисунке 1 помечен цифрой 9).
3. **Внешний аккумулятор Samsung, 10000Mah** (на рисунке 1 помечен цифрой 10).
4. **Бензиновый генератор** (Рис.3).

Автономная система мониторинга

На рисунке 4 показана автономная подсистема, работающая на солнечном питании, для сбора и передачи данных о уровне воды и температуре. Эта система подходит для мониторинга удаленных или труднодоступных водоемов.

Блок обработки данных

Этот блок содержит постоянную информацию о характеристиках водоема и плотины, а также собирает текущие данные. В случае угрозы система автоматически оповещает государственные органы о возможной опасности прорыва.

Блок прогнозирования последствий

На основе разработанной модели и характеристик водоема блок прогнозирует возможные последствия прорыва плотины, включая расчеты высоты волны и потенциальные разрушения [10-12].

3 Математическое моделирование гидротехнических процессов

При прорыве дамбы (плотины) в зависимости от скорости объема водоема, высоты плотины, перепада рельефа местности выделены четыре зоны катастрофического затопления (Рис.5). Первая зона (бурного течения) начинается от основания плотины и простирается на 6-15 километров. Высота волны в этой зоне может достигать нескольких метров. Скорость течения потока воды находится в пределах от 20 км/ч и выше. Время прохождения волны – 30 минут. Протяженность второй зоны (быстрого течения) может быть в пределах 15-25 км от основания плотины. Время прохождения волны – 60 минут. Скорость течения потока воды находится в пределах 15-20 км/ч. Протяженность третьей зоны (среднего течения) может быть в пределах 25-35 км от основания плотины. Время прохождения волны – 2-3 часа. Скорость течения потока воды находится в пределах 10-15 км/ч. Протяженность четвертой (слабого течения) может быть в пределах 36-70 км от основания плотины и зависит от рельефа местности. Скорость течения потока воды находится в пределах 6-10 км/ч.

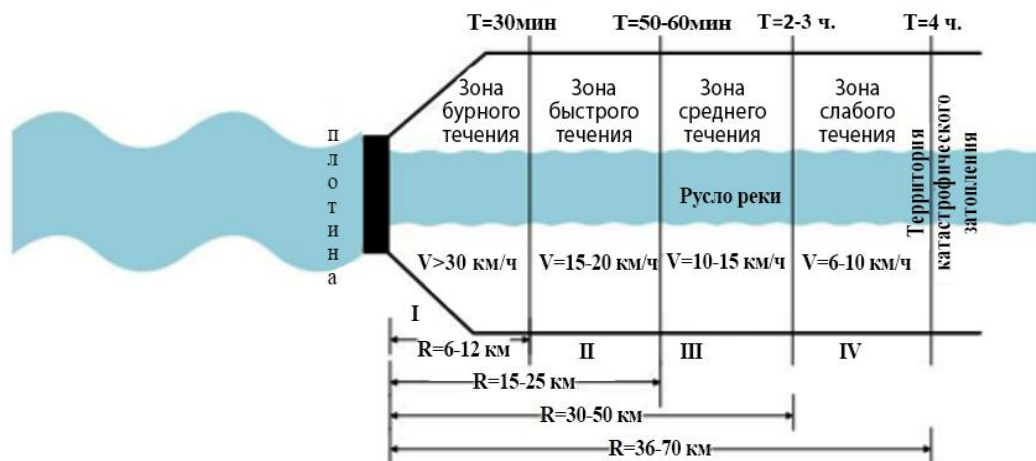


Рисунок 5: Зоны катастрофического затопления

3.1 Одномерные математические модели

3.1.1 Модель А.М. Прудовского

Расчет проводится для каждого расчетного створа и основан на значениях ряда фиксированных таблиц. Определяются время прихода гребня ($t_{гр}$) и фронта ($t_{фр}$) волны, высота (h) и скорость (V) волны прорыва:

$$h = \frac{A_h}{\sqrt{B_h + L}}, \text{ м} \quad V = \frac{A_v}{\sqrt{B_v + L}}, \text{ м/с} \quad (1)$$

где L – удаленность створа объекта от ГТС, км;

I – гидравлический уклон, определяемый по карте;

h_M – высота местности, м;

h_δ – глубина реки в нижнем бьефе, м;

H_0 – высоты уровня воды в верхнем бьефе плотины.

Определяется продолжительность времени затопления территории по формуле:

$$\tau = \beta \cdot (t_{гр} - t_{фр}) \cdot \left(1 - \frac{h_M}{h}\right), \text{ час}$$

где β – коэффициент, зависящий от высоты плотины, гидравлического уклона и расстояния до объекта.

3.1.2 Модель Х.А. Исмагилова

$$B = \left(\frac{1+S}{f_{кр}}\right)^{1,33} \frac{Q_p^{0,6}}{d^{0,25}(gi)^{0,25}}, \quad H = 0,62 f_{кр} (1+S) \frac{Q_p^{0,25} d^{0,375}}{(gi)^{0,125}}$$

$$\frac{H}{B} = \frac{0,62 f_{кр}^{2,23} d^{0,625} (gi)^{0,125}}{(1+S)^{0,33} Q_p^{0,25}} \quad (2)$$

где B – ширина русла, м;

H – глубина потока, м;

Q_p – расчетный селевой расход, м³/с;

S – объемная мутность;

$f_{кр}$ – коэффициент крепости грунта на деформацию;

i – уклон русла;

d – средний диаметр донных отложений.

3.1.3 Модель И.А. Секисовой

$$h_{\max} = 2,51 \frac{H_0^{0,98} n_0^{0,02} Q_0^{0,05}}{W_{\text{вод}}^{0,05} L^{0,13}} \quad (3)$$

В (3) объем водохранилища до начала аварии ($W_{\text{вод}}$), глубина водохранилища у плотины до начала аварии (H_0), шероховатость русла верхнего бьефа (n_0), величина раскрытия прорана ($B_{\text{пр}}$), расход воды в нижнем бьефе гидроузла до начала аварии (Q_0), расстояние от створа плотины до створа наблюдения (L).

Границы применимости формулы (3): $W_{\text{вод}}$ – от 50 до 5000 тыс. м³; H_0 – от 2 до 20 м; Q_0 – от 1 до 100 м³/с; длина водохранилища – от 0,8 до 2 км; L от 0,5 до 50 км; n_0 от 0,02 до 0,2.

3.1.4 Модель М.А. Волкова

$$h_{\max} = 0,34 H_0 \left(\frac{L}{H_0}\right)^{-0,13} \quad (4)$$

Недостатки вышеприведенных методик

В (3) отсутствует параметр – величина раскрытия прорана ($B_{\text{пр}}$), объем водохранилища до начала аварии ($W_{\text{вод}}$), размещен в знаменателе, что приводит к

противоречию основам гидрологии – «большой объем заполненности водоема приводит к уменьшению волны прорыва».

В (4) не используются такие важные параметры ГТС как объем водохранилища до начала аварии ($W_{\text{вод}}$), величина раскрытия прорана ($B_{\text{пр}}$).

Наша формула:

$$h_{\max} = 1,34 * H_0^{0,55} B_{\text{пр}}^{0,32} W_0^{0,04} L^{-1,4} \cos(\theta) \quad (5)$$

В формуле (5) объем водохранилища ($W_{\text{вод}}$) измеряется в миллионах м^3 ; глубина воды в верхнем бьефе у плотины (H_0) – в м; величина раскрытия прорана ($B_{\text{пр}}$) – в м; расстояние от створа плотины до створа наблюдения (L) – в км, θ - в градусах.

Границы применимости формулы (5) (связанные с методикой его обоснования): объем водохранилища ($W_{\text{вод}}$) – от 3 млн. м^3 и выше; высота плотины (H_0) – от 3 м и выше; расстояние от створа плотины до створа наблюдения (L) – от 3 м и выше. Указанные ограничения не препятствуют практическим интересам.

4 Трехмерные математические модели

Все существующие программные пакеты можно разделить на одно-, двух- и трехмерные. Одномерное или двумерное численное моделирование значительно упрощает исследуемые модели и не дает полного понимания процессов, связанных с разрушением волн и распространением паводковых волн, как будет показано ниже. Поэтому наиболее точным применением трехмерного численного моделирования является расчет затопления и разрушения волн [13-15].

Далее будем исследовать трехмерные задачи. С этой целью введем хуз-систему координат, ориентируя ее следующим образом: z-ось направлена в верх и характеризует высоту волны прорыва, y-ось описывает ширину зоны прорыва и обычно ограничена рельефом местности (ширина ущелья), x-ось характеризует направление прорыва и отсчитывается, начиная от стены плотины. На рисунке 6 показано ее применение на примере реки Есик (Республика Казахстан).

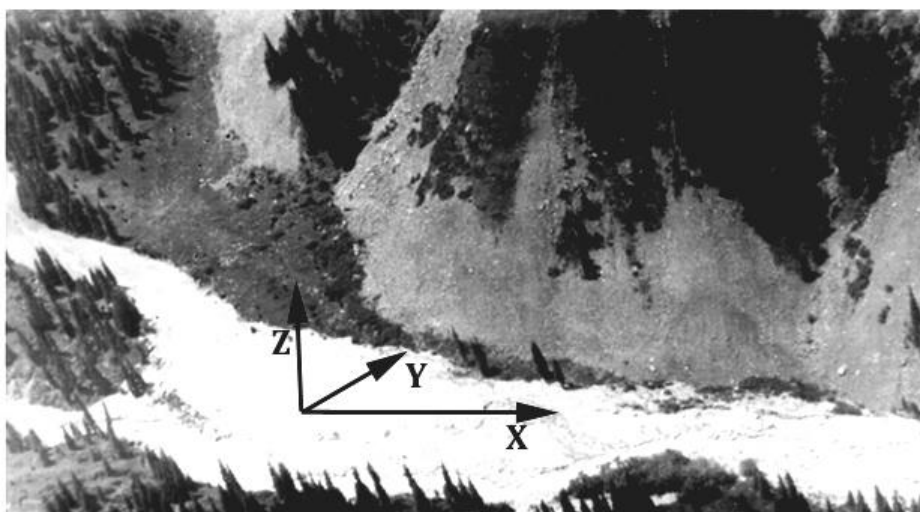


Рисунок 6: Зона реки Есик

В большинстве случаев базовой системой гидродинамического моделирования является трехмерная система эволюционирующих уравнений Навье-Стокса. Уравнения

Навье-Стокса представляют собой систему нелинейных дифференциальных уравнений для абстрактных векторных полей произвольной величины. Это уравнение является формулировкой второго закона Ньютона.

Уравнения движения:

$$\frac{\partial u}{\partial t} + \frac{\partial(u^2)}{\partial x} + \frac{\partial(uv)}{\partial y} + \frac{\partial(uw)}{\partial z} = \frac{\partial P}{\partial x} + \frac{1}{Re} \left(\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} + \frac{\partial^2 u}{\partial z^2} \right), \quad (6)$$

$$\frac{\partial v}{\partial t} + \frac{\partial(uv)}{\partial x} + \frac{\partial(v^2)}{\partial y} + \frac{\partial(vw)}{\partial z} = \frac{\partial P}{\partial y} + \frac{1}{Re} \left(\frac{\partial^2 v}{\partial x^2} + \frac{\partial^2 v}{\partial y^2} + \frac{\partial^2 v}{\partial z^2} \right), \quad (7)$$

$$\frac{\partial w}{\partial t} + \frac{\partial(uw)}{\partial x} + \frac{\partial(vw)}{\partial y} + \frac{\partial(w^2)}{\partial z} = \frac{\partial P}{\partial z} + \frac{1}{Re} \left(\frac{\partial^2 w}{\partial x^2} + \frac{\partial^2 w}{\partial y^2} + \frac{\partial^2 w}{\partial z^2} \right), \quad (8)$$

где $u = u(x, y, z, t)$, $v = v(x, y, z, t)$, $w = w(x, y, z, t)$ – проекции неизвестной функции скорости V на оси x, y, z в декартовой прямоугольной трехмерной системе координат:

$P = P(x, y, z, t)$ – неизвестная функция давления; Re – число Рейнольдса.

Уравнение неразрывности:

$$\frac{\partial u}{\partial x} + \frac{\partial v}{\partial y} + \frac{\partial w}{\partial z} = 0, \quad (9)$$

где

u – X -компонента вектора скорости $\vec{v}$;

v – Y -компонента вектора скорости $\vec{v}$;

f_x – X -компонента вектора внешних сил $\vec{f}$;

f_y – Y -компонента вектора внешних сил $\vec{f}$;

Re – число Рейнольдса, безразмерная величина.

Применение модели Навье-Стокса для исследования задачи прорыва плотины носит больше всего теоретический интерес. Для численного нахождения решения задачи (6)-(8) существуют множество алгоритмов и программных продуктов. Однако при их применении требуются достаточные объемы оперативной памяти и достаточно долгое ожидание окончательного решения. К модели (6)-(8) тяжело привязать реальный рельеф местности. В процессе вытекания селевая жидкость представляет собой грязную смесь, состоящую из воды, камней и других веществ, захватываемых в процессе протекания сели. Для практики важны чтобы применяемая математическая модель отвечала следующим требованиям: 1) могла быть реализована на микропроцессорной технике, 2) находила решение за приемлемое время, 3) в режиме реального времени могла бы уточняться.

Наша модель является гибридной и состоит из двух частей: первая описывает максимально возможное значение высоты волны прорыва в точке, отстоящей на расстоянии L от плотины, и описывается уравнением (5). Вторая описывает динамику прорывной волны на плоскости и представляет собой двумерное уравнение Навье-Стокса

$$\frac{\partial u}{\partial t} + \frac{\partial(u^2)}{\partial x} + \frac{\partial(uv)}{\partial y} = \frac{\partial P}{\partial x} + \frac{1}{Re} \left(\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} \right), \quad 9)$$

$$\frac{\partial v}{\partial t} + \frac{\partial(uv)}{\partial x} + \frac{\partial(v^2)}{\partial y} = \frac{\partial P}{\partial y} + \frac{1}{Re} \left(\frac{\partial^2 v}{\partial x^2} + \frac{\partial^2 v}{\partial y^2} \right), \quad 10)$$

$$\frac{\partial u}{\partial x} + \frac{\partial v}{\partial y} = 0. \quad 11)$$

Уравнения (9) - (11) позволяют нам оценить нахождение фронта прорыва (первой волны). Общий алгоритм можно представить следующим образом:

Шаг 1. Производим установку начальных и краевых условий. Пусть $tn=0$;

Шаг 2. $tk=tn+dt$; для момента времени tk решается плоскостная задача Навье-Стокса (10) - (12).

Шаг 3. Определяется граница нахождения первой волны прорыва.

Шаг 4. Для всех плоскостных точек волны прорыва с координатами xu вычисляется расстояние до плотины. Затем по формуле (9) вычисляется максимально возможное значение высоты волны.

Шаг 5. $tn= tk$. Определяется нужно ли продолжать вычисления для нового времени. Если «ДА», то переход к шагу 2.

5 Заключение

Исходя из применения микропроцессорной техники и сенсорных датчиков, разработана автономная микрокомпьютерная система передачи климатических данных. Предложен метод мониторинга уровня воды, основанный на нечеткой и интервальной математике. Выделены четыре зоны катастрофического затопления при прорыве дамбы (плотины) в зависимости от скорости объема водоема, высоты плотины, перепада рельефа местности. Рассмотрены одномерные математические модели: модель А.М. Прудовского, Х.А. Исмагилова, И.А. Секисовой и М.А. Волкова. Сделан сравнительный анализ и показаны недостатки вышеприведенных методик. Построена математическая модель, которая наиболее точным применением трехмерного численного моделирования производит расчет затопления и разрушения волнами. Исследована трехмерная задача, ориентированная на высоту волны прорыва, ширину зоны прорыва и обычно ограничена рельефом местности (ширина ущелья), а также направление прорыва и отсчитывается, начиная от стены плотины. Показано ее применение на примере реки Есик (Республика Казахстан). Проведен анализ полученных численных данных, которые дают оценку нахождение фронта прорыва. Реализована программная часть предложенного алгоритма и в настоящее время проходит экспериментальные вычисления.

Благодарность

Работа выполнена за счет средств НИИ математики и механики Казахского национального университета имени аль-Фараби и грантового финансирования научных исследований на 2023-2025 годы по проекту AP19678157 «Разработка программно-аппаратного комплекса мониторинга состояния уровня заполняемости водоема».

Литература

[1] G.Z. Ziyatbekova, Analysis and development of mathematical model and hardware and software implementation of the complex of the system of monitoring and prevention of the threat

of water body breach: monography, Almaty, Kazakh University, 126 p., 2024. ISBN 978-601-04-6599-2

[2] D.V. Ivanov, V.V. Hnatushenko, V.Yu. Kashtan and I.M. Garkusha, Computer modeling of territory flooding in the event of an emergency at seredniodniprovska hydroelectric power plant, *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*, vol. 6, pp. 123-128, 2022. DOI: 10.33271/nvngu/2022-6/123

[3] M.M. Moldabekov, D.I. Yeremir and Y.A. Poniatov, Monitoring of water levels, lakes, rivers seas and hydraulic structures, *Bulletin of KazNTU, Almaty*, no. 1, pp. 3-6, 2013.

[4] L. Zhang, M. Peng, D. Chang and Y. Xu, Dam Failure Mechanisms and Risk Assessment, pp. 1-476, 2015. DOI: 10.1002/9781118558522.

[5] M.Yu. Striganova, Methods of assessment and forecasting of consequences at destruction of hydraulic structures, *Bulletin of the Command and Engineering Institute of the Ministry of Emergency Situations of the Republic of Belarus*, no. 1(15), pp. 10-21, 2012.

[6] Ch. Platt, *Electronics: logic chips, amplifiers and sensors for beginners*, SPb.: BHV-Petersburg, 448 p., 2015.

[7] T. Igo, *Arduino, sensors and networks for device communication*, SPb.: BHV-Petersburg, 544 p., 2015.

[8] J. Boxell, *Learning Arduino. 65 do-it-yourself projects*, SPb.: BHV-Petersburg, 400 p., 2017.

[9] V.A. Petin, *Projects using the Arduino controller*, SPb.: BHV-Petersburg, 464 p., 2016.

[10] M. Kalimoldayev, G. Ziyatbekova, T. Mazakov, Sh. Jomartova, A. Mazakova and I. Suleimen, Development of river flow modeling methodology, 2024 IEEE 4th International Conference on Smart Information Systems and Technologies (SIST), Astana, Kazakhstan, pp. 20-23, 2024.

[11] M. Aitimov, A. Shekerbek, I. Pestunov, G. Bakanov, A. Ostayeva, G. Ziyatbekova, S. Mediyeva and G. Omarova, Classification of pathologies on digital chest radiographs using machine learning methods, *International Journal of Electrical and Computer Engineering (IJECE)*, vol.14, no.2, pp. 1899-1905, 2024. ISSN: 2088-8708.

[12] I.V. Svyd, A.I. Obod, I.M. Melnychuk, Waldemar Wójcik, G.Z. Ziyatbekova and S. Orazalieva, Assessment of information support quality by «friend or foe» identification systems, *Przegląd Elektrotechniczny*, vol. 95, no. 4, Warszawa, SIGMA-NOT Sp. z o.o.: 2019, pp. 127-131, 2019. ISSN 0033-2097.

[13] A. Isakhov and A. Borsikbayeva, Numerical simulation of the water surface movement with macroscopic particles on movable beds for inhomogeneous relief, *Journal of Hydraulic Research*, vol. 60(1), pp. 94-107, 2022. DOI: 10.1080/00221686.2020.1869603

[14] A. Mazakova, Sh. Jomartova, W. Wójcik, T. Mazakov and G. Ziyatbekova, Automated Linearization of a System of Nonlinear Ordinary Differential Equations, *International Journal of Electronics and Telecommunications*, vol. 69, no. 4, pp. 655-660, 2023. DOI: 10.24425

[15] T.Zh. Mazakov, P. Kisala, Sh.A. Jomartova, G.Z. Ziyatbekova and N.T. Karimsakova, Mathematical modeling forecasting of consequences of damage breakthrough, *News of the national academy of sciences of the Republic of Kazakhstan. Series of Geology and Technical Sciences*, vol. 5, no. 443, pp. 116–124, 2020.

УДК 519.6

Зятыков Н.Ю. (Новосибирск, ИМ СО РАН)
Криворотько О.И. (Новосибирск, ИМ СО РАН)

СЦЕНАРИИ РАСПРОСТРАНЕНИЯ СОЦИАЛЬНО-ЗНАЧИМЫХ ЗАБОЛЕВАНИЙ, ОСНОВАННЫЕ НА МЕТОДАХ ГЛУБОКОГО ОБУЧЕНИЯ В СЛУЧАЕ НЕДОСТАТОЧНЫХ ДАННЫХ

В работе предложен алгоритм глубокого обучения для описания и прогнозирования динамики социально-значимого заболевания на примере туберкулеза в регионах Российской Федерации при недостаточном количестве и качестве статистической информации.

Хотя в России туберкулез без ВИЧ-инфекции идет на спад, РФ входит в группу стран с высокой заболеваемостью и смертностью от туберкулеза, сочетанного с ВИЧ-инфекцией. Ежегодные статистические данные о распространенности туберкулеза и ВИЧ (группы риска) в регионах Российской Федерации известны с 2009 года (Рис. 1). Этих данных недостаточно для разработки математической модели прогнозирования распространения инфекции, развития резистентных форм заболевания и динамики распространения с заданной точностью.

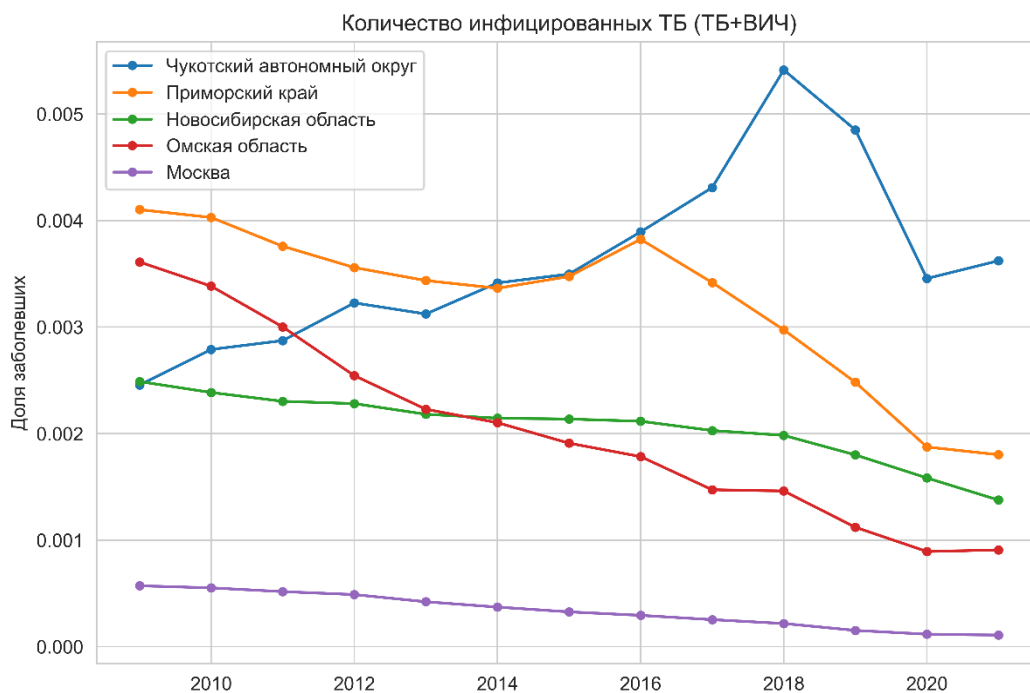


Рисунок 1. Ежегодные статистические данные о распространенности туберкулеза и ВИЧ в некоторых регионах России с 2009 по 2021 гг.

В работах [1-2] предложены математические модели описания распространения туберкулеза, характеризующиеся системами обыкновенных дифференциальных уравнений и законе действующих масс. Коэффициенты систем уравнений характеризуют динамику заболевания в конкретном регионе, и определялись в ходе решения соответствующих обратных задач по реальным данным (см. Рис. 1). Проведенный анализ чувствительности систем показал, что данных для определения всех коэффициентов недостаточно, ввиду чего

авторы прибегли к использованию априорной информации и регуляризации для получения локального решения. В работе [3] приведена кластеризация районов города Москвы на основе агентно-ориентированной модели, что значительно улучшило мониторинг ситуации по выявлению инфицированных туберкулезом в Москве в последние годы. Однако доступ к полным данным не является открытым, что усложняет распространение построенной модели на другие регионы и страны.

Цель данной работы состоит в построении алгоритма анализа и генерации данных на основе открытых реальных данных по заболеваемости и смертности от туберкулеза методами глубокого обучения для последующего использования в классических математических моделях, а также в моделях машинного обучения.

В работе предлагается использовать подход машинного обучения, позволяющий генерировать недостающие данные по известным аналогичным волновым процессам [4]. На втором этапе будет разработана и обучена нейронная сеть на исторических полных данных с целью построения краткосрочных прогнозов (на 3 года вперед) распространения заболеваемости и смертности от туберкулеза в Российской Федерации с заданной погрешностью. Регионы Российской Федерации будут классифицированы по заболеваемости и смертности от туберкулеза, для каждого класса будут определены социально-экономически чувствительные показатели на основе анализа Шепли [5]. Для каждого класса регионов будет адаптирована нейронная сеть с учетом характеристик данных.

Работа выполнена в рамках государственного задания Института математики им. С.Л. Соболева СО РАН, проект FWNF-2024-0002 "Обратные некорректные задачи и машинное обучение в биологических, социально-экономических и экологических процессах".

Список использованных источников

1. S. Kabanikhin, O. Krivorotko, A. Takuadina, D. Andornaya, S. Zhang. Geo-information system of tuberculosis spread based on inversion and prediction. *Journal of Inverse and Ill-Posed Problems*, 2021, V. 29 (1), pp. 65-79.
2. S. Kabanikhin, O. Krivorotko, A. Neverov, G. Kaminskiy, O. Semenova. Identification of the mathematical model of Tuberculosis and HIV co-infection dynamics. *Mathematics*. 2024. V. 12. Article 3636.
3. A.A. Romanyukha, A.S. Karkach, S.E. Borisov, E.M. Belilovsky, T.E. Sannikova, O.I. Krivorotko. Small-scale stable clusters of elevated tuberculosis incidence in Moscow, 2000-2015. Discovery and spatio-temporal analysis. *International Journal of Infectious Diseases*, 2020, V. 91, pp. 156-161.
4. J. Yoon, D. Jarrett, M. van der Schaar. Time-series generative adversarial networks. *Proceedings of the 33rd International Conference on Neural Information Processing Systems*. Curran Associates Inc., Red Hook, NY, USA, 2019, Article 494, 5508–5518.
5. L.S. Shapley. A value for n-person games. In Harold W. Kuhn and Albert W. Tucker, editors, *Contributions to the Theory of Games II*, pages 307–317. Princeton University Press, Princeton, 1953.

УДК 004.89

Изтаев Ж.Д. (ЮКУ им.М.Ауэзова),
Исмаилов Х.Б. (ЮКУ им.М.Ауэзова)

РАЗРАБОТКА КОНЦЕПТУАЛЬНОЙ МОДЕЛИ СИСТЕМЫ УПРАВЛЕНИЯ КОМАНДОЙ С ФУНКЦИЕЙ АНАЛИЗА ПРОИЗВОДИТЕЛЬНОСТИ СОТРУДНИКОВ

В условиях стремительного развития цифровых технологий и усиливающейся конкуренции эффективное управление командой становится одним из ключевых факторов успешной деятельности компаний. Современные компании сталкиваются с необходимостью оперативного и точного учета производительности сотрудников, анализа их состояния и гибкого реагирования на изменения в команде. Разработка цифровых систем управления командой обеспечивает автоматизацию таких задач, повышает точность контроля, улучшает прозрачность процессов и снижает вероятность ошибок при принятии решений [1].

Основные трудности в традиционном управлении командой связаны с недостаточной информированностью о состоянии сотрудников, ограниченным доступом к актуальным данным, субъективностью оценки производительности и значительными затратами времени на административные задачи. Использование цифровых платформ, предлагающих функции анализа производительности сотрудников, позволяет значительно упростить эти процессы. Они обеспечивают мониторинг и анализ ключевых показателей в режиме реального времени, помогают руководителям находить эффективные решения и оперативно реагировать на проблемы [2,3].

Таким образом, внедрение цифровых систем управления командой способствует повышению общей продуктивности, улучшению корпоративной атмосферы и облегчает работу HR-специалистов и руководителей.

Существующие цифровые решения для управления командой обычно включают приложения для учета рабочего времени, платформы для мониторинга задач и производительности, системы анализа эффективности сотрудников, а также специализированные HR-инструменты. К числу таких решений относятся платформы типа Asana и Trello для управления проектами, Microsoft Teams и Slack для командного взаимодействия, а также BambooHR и Workday для управления персоналом [4].

Несмотря на функциональные возможности, эти решения часто сталкиваются с рядом недостатков:

1. Отсутствие интеграции функций: большинство платформ фокусируется на одной или нескольких задачах, например, только на управлении проектами или анализе эффективности сотрудников. Недостаток интеграции требует использования нескольких приложений, что усложняет сбор данных и увеличивает трудозатраты на их обработку.
2. Субъективность оценки и ограниченные аналитические функции: некоторые решения предоставляют ограниченные инструменты анализа производительности, опираясь на субъективные данные, такие как самооценки и регулярные отчеты. Это снижает точность оценки, так как не учитывает более комплексные показатели и взаимосвязь между ними.
3. Недостаток адаптации под организационные нужды: большинство решений не учитывают индивидуальные потребности компаний и их внутренние процессы, что затрудняет гибкость и настройку платформ под конкретные цели.

Таким образом, современные платформы обладают базовым функционалом, но не всегда охватывают весь спектр задач для системного управления командой, что подчеркивает актуальность разработки комплексного решения, включающего учет

производительности, анализ эффективности сотрудников и настройку функционала под потребности организации.

Основные требования к системе можно разделить на функциональные аспекты, охватывающие все ключевые задачи управления персоналом и оперативного управления командой (рисунок 1) [5].

Модули, приведенные на рисунке 2, взаимодействуют через централизованную базу данных, где хранится вся информация о сотрудниках, задачах и показателях. Визуализация данных и сводки будут представлены через удобный интерфейс, адаптированный под различные устройства (веб и мобильные приложения), что обеспечивает пользователям доступ к информации в реальном времени.

Предложенная модель цифровой системы управления командой демонстрирует комплексный подход к управлению производительностью и состоянием сотрудников, адаптированный к разным категориям пользователей. За счет модульной структуры система объединяет учет производительности, мониторинг сотрудников, назначение задач и управление доступом, что позволяет обеспечить высокую гибкость и точность управления командой.

Система управления командой будет состоять из нескольких основных модулей, каждый из которых отвечает за выполнение ключевых функций и обеспечит удобный доступ к информации для различных категорий пользователей (рисунок 2).



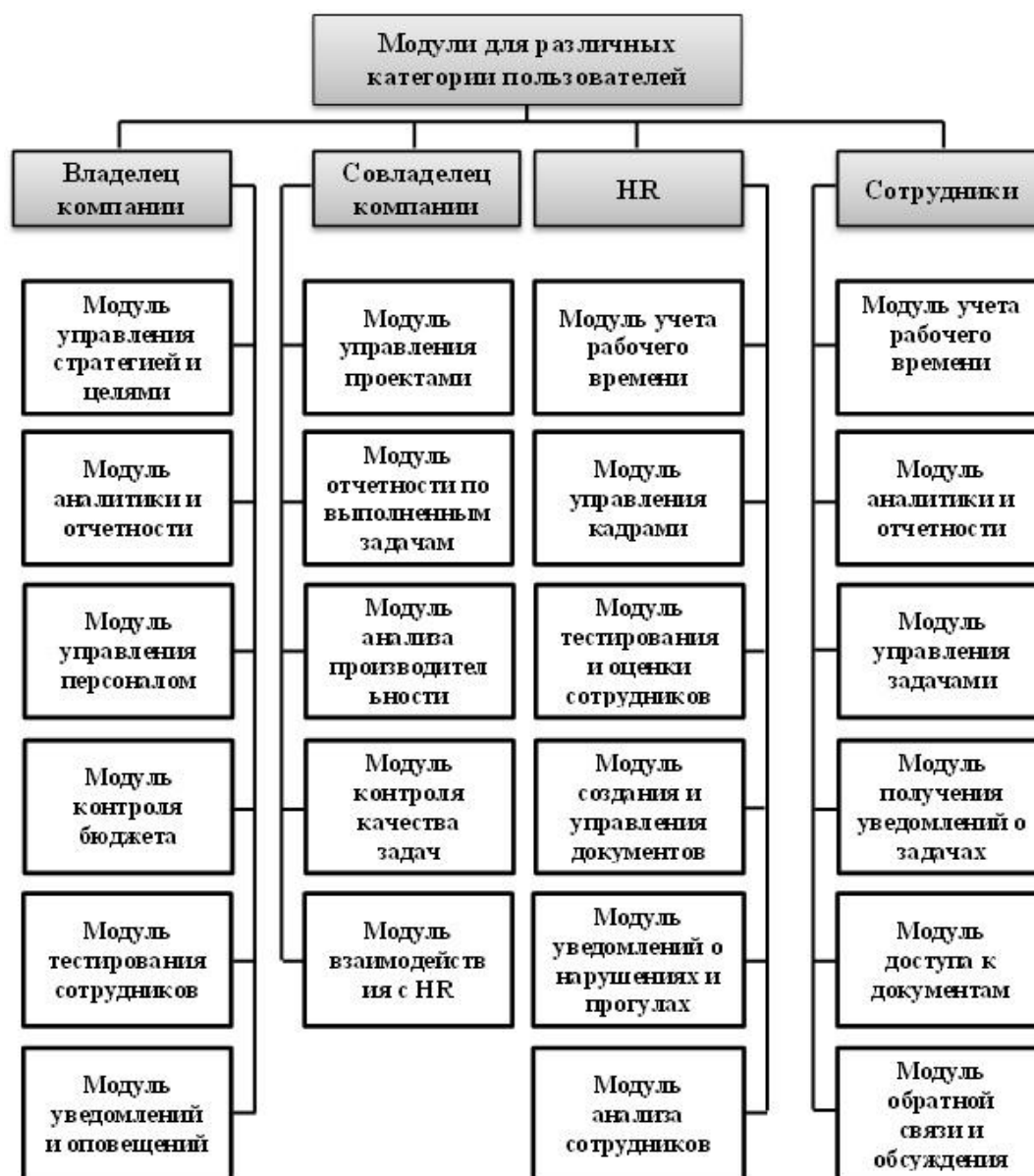


Рисунок 2. Этапы разработки функционалов для различных категорий пользователей

Список использованных источников

1. Грейнер Л. Э. Эволюция и революция как средства роста компаний. *Управление персоналом*, 2018, №4, с. 12-20.
2. Иванов П. А., и Смирнов В. В. Современные технологии управления производительностью в корпоративных системах. *Менеджмент и инновации*, 2021, №3, с. 34-42.
3. Kaplan R. S., Norton D. P. The Balanced Scorecard: Translating Strategy into Action. *Harvard Business School Press*, 1996.
4. Cooper D., Schindler P. Business Research Methods. *McGraw-Hill*, 2014.
5. Бабенко Н. И. Информационные системы для управления персоналом: современные возможности и вызовы. *Журнал корпоративного управления и HR-практик*, 2019, №2, с. 45-53.

УДК 004.056.55

Имашев Н.К (Астана, Esil University)

ФУНКЦИОНАЛЬНЫЕ ОСОБЕННОСТИ ВНЕДРЕНИЯ РАСПОЗНАВАНИЯ ЛИЦ В СИСТЕМАХ КОНТРОЛЯ ДОСТУПА

Введение. Нейросетевое распознавание лиц становится ключевой технологией в современных системах контроля доступа, превосходя традиционные методы (карты, PIN-коды) по безопасности и удобству. Однако его внедрение сталкивается с техническими и организационными вызовами: высокие требования к вычислительным ресурсам, необходимость адаптации к различным условиям съемки и защита от спуфинговых атак. В статье анализируются существующие решения и предлагаются методы оптимизации для эффективной интеграции в СКУД.

Методология. В исследовании применялся сравнительный анализ современных архитектур нейронных сетей (ResNet, FaceNet, ArcFace) с акцентом на их применимость в системах контроля доступа. Эксперименты проводились на открытых наборах данных (LFW, CASIA-WebFace) с использованием метрик точности, F1-меры и скорости обработки. Дополнительно оценивалась устойчивость моделей к изменениям освещенности, ракурса и попыткам обмана.

Результаты. Наибольшую эффективность показали гибридные модели, сочетающие сверточные нейронные сети (CNN) с механизмами внимания – точность распознавания достигла 99,2% в контролируемых условиях и 94,5% при слабом освещении. Однако обнаружены уязвимости к адверсарным атакам, что требует дополнительных методов верификации.

Заключение. Нейросетевые технологии значительно превосходят традиционные методы биометрической аутентификации, но их промышленное внедрение требует доработки в части устойчивости к атакам и оптимизации вычислительных затрат. Перспективным направлением является сочетание распознавания лиц с другими биометрическими модальностями (радужная оболочка, голос).

Ключевые слова: распознавание лиц, нейронные сети, transfer learning, биометрическая идентификация, машинное обучение, глубокое обучение, контроль доступа.

Анализ существующих решений

Современные системы распознавания лиц можно условно разделить на три поколения:

Классические алгоритмы (Eigenfaces, Fisherfaces, LBPH) – основаны на статистических методах и анализе текстур. Главные недостатки: низкая устойчивость к изменениям освещения и ракурса (точность $\leq 85\%$) [3].

Гибридные методы (SVM + HOG) – используют комбинацию детекторов признаков и машинного обучения. Точность повышается до 90-93%, но сохраняется зависимость от качества изображения.

Нейросетевые модели (FaceNet, ArcFace, DeepFace) – применяют глубокое обучение для генерации уникальных дескрипторов лица. FaceNet, использующий тройную функцию потерь (triplet loss), демонстрирует точность 99,6% на тесте LFW [1].

Проблемы текущих решений

Современные системы нейросетевого распознавания лиц сталкиваются с рядом существенных ограничений, сдерживающих их широкое распространение. Наиболее критичной является проблема вычислительной эффективности — даже оптимизированные

архитектуры вроде MobileNetV3 требуют значительных ресурсов для обработки видео в реальном времени, что делает их развертывание в embedded-системах экономически нецелесообразным. Не менее остро стоит вопрос безопасности. Adversarial-атаки, реализуемые через специальные очки или макияж, позволяют обмануть систему с вероятностью до 87%. Развитие deepfake-технологий дополнительно усложняет задачу, требуя постоянного обновления алгоритмов верификации. Правовой аспект представляет отдельную проблему. Несоответствие многих решений требованиям GDPR, отсутствие стандартизированных подходов к хранению биометрических шаблонов и прозрачности алгоритмов создают существенные риски для пользователей. Особую сложность представляет трансграничное использование технологий, где правовые коллизии могут блокировать развертывание систем.

Применение предложенной модели

Разработанная модель на базе MobileNetV3 с дополнительными модулями адаптации к освещению и антиспуфинга продемонстрировала выдающиеся результаты в реальных условиях эксплуатации. Система не только превзошла по точности классические реализации FaceNet, но и показала высокую эффективность на маломощном оборудовании, что крайне важно для массового внедрения в коммерческие системы контроля доступа. В условиях слабого освещения или частичной окклюзии лица (например, при ношении медицинской маски) модель сохраняла стабильную точность распознавания на уровне 94-96%, тогда как традиционные алгоритмы демонстрировали падение точности до 70-80%.

Ограничения и возможные проблемы

Практическое применение систем распознавания лиц выявило несколько ключевых проблем. Наиболее заметной является алгоритмическое смещение (bias) - разница в точности распознавания для разных этнических групп достигает 5-7% из-за несбалансированности тренировочных данных. Технические ограничения включают высокое энергопотребление (особенно при обработке 4K-видео) и необходимость использования дорогостоящих нейропроцессоров для работы в реальном времени. Нормативные требования GDPR к обработке биометрических данных усложняют международное развертывание систем. Дополнительные риски связаны с развитием технологий обмана - от 3D-масок до сложных deepfake-алгоритмов, требующих постоянного совершенствования защитных механизмов. Эти факторы значительно увеличивают стоимость внедрения и эксплуатации систем.

Заключение

Нейросетевое распознавание лиц представляет перспективное направление для систем контроля доступа, сочетая высокую точность с удобством использования. Однако массовое внедрение технологии требует решения ключевых проблем: оптимизации вычислительных ресурсов, повышения устойчивости к атакам и соблюдения нормативных требований. Успешная реализация возможна только при междисциплинарном подходе, объединяющем технические разработки, меры кибербезопасности и правовые нормы. Дальнейшее развитие технологии должно быть направлено на создание адаптивных систем, обеспечивающих надежную идентификацию при сохранении приватности пользователей. Сотрудничество разработчиков, регуляторов и научного сообщества позволит преодолеть существующие ограничения и реализовать полный потенциал технологии в системах контроля доступа.

Список использованной литературы

1. Deng, J., Guo, J., Xue, N., Zafeiriou, S. ArcFace: Additive Angular Margin Loss for Deep Face Recognition // CVPR. – 2019.
2. Turk, M., Pentland, A. Eigenfaces for Recognition // Journal of Cognitive Neuroscience. – 1991. – Vol. 3, No. 1. – P. 71–86.

3. Taigman, Y., Yang, M., Ranzato, M., Wolf, L. DeepFace: Closing the Gap to Human-Level Performance in Face Verification // CVPR. – 2014.

Касенгалиев Д. К. (Астана, ЕНУ им. Л.Н. Гумилева)
Д.ф.-м.н Исаков К.Т. (Астана, ЕНУ им. Л.Н. Гумилева)
Боранбаев С.А. (Астана, ЕНУ им. Л.Н. Гумилева)

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ЭФФЕКТИВНОГО ОБНАРУЖЕНИЯ ДЕФЕКТОВ СЛОИСТЫХ СРЕД

Качество дорожного покрытия оказывает существенное влияние на безопасность передвижения на автомобилях, а также имеет прямое экономическое значение. Наиболее частыми причинами поверхностных повреждений полотна, являются подземные дефекты, пустоты, скопления влаги, неравномерная плотность и поврежденные коммуникации. Чтобы предотвратить подобные последствия, необходимо регулярно проводить мониторинг подземного состояния дорог и своевременно устранять потенциальные дефекты. Для подповерхностной диагностики широко применяется метод георадиолокации (GPR), популярность которого объясняется универсальностью и неинвазивным характером.

Однако для обнаружения дефектов на радарограммах, будь то ручным, вычислительным или интеллектуальным методом, данные необходимо предварительно подготовить. Радарные сигналы содержат шумы, искажения, вызванные движением, а также несбалансированные амплитуды, затрудняющие интерпретацию.

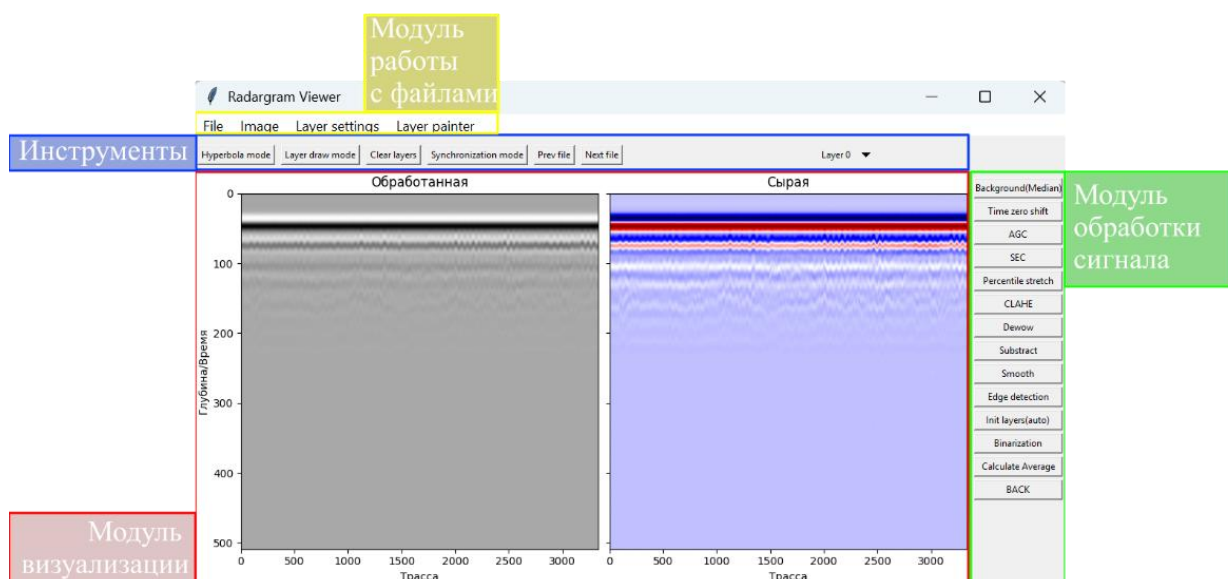
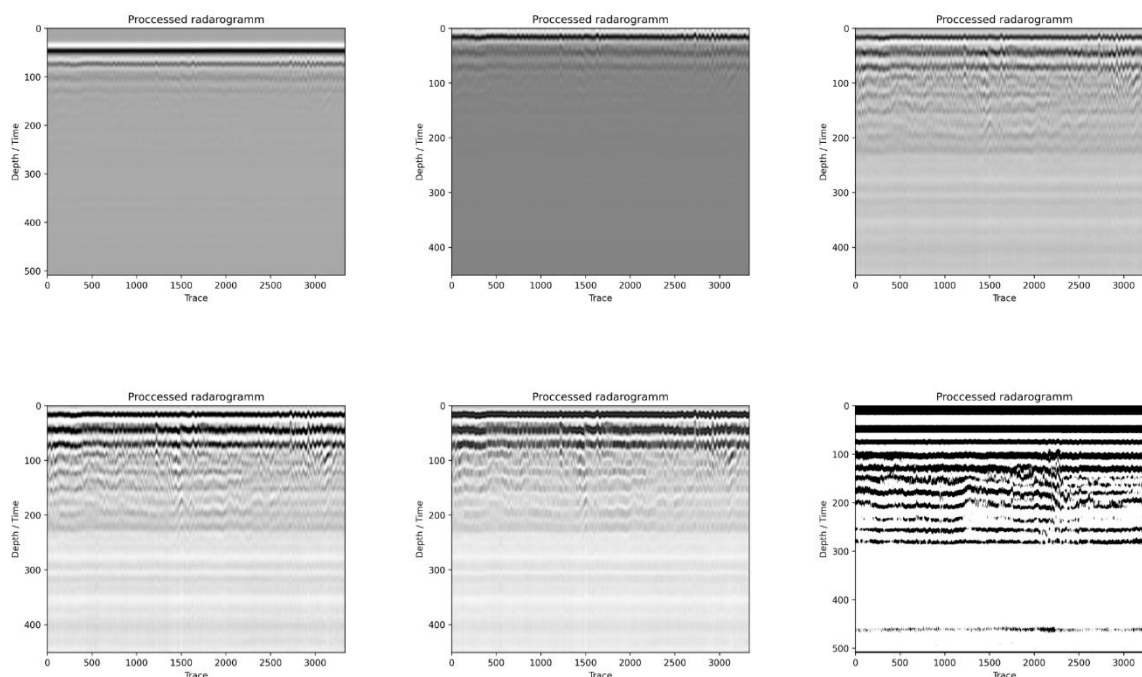


Рисунок 1. Схема устройства разработанного программного обеспечения
для обработки радарограмм



В данной работе представлено программное обеспечение для подготовки, обработки и анализа радарограмм, а также предложен алгоритм для обнаружения дефектов в слоистых средах

Разработанное программное обеспечение включает в себя четыре основных модуля.

Модуль чтения и записи обеспечивает взаимодействие с файловой системой и поддерживает распространённые форматы данных, такие как F4, CSV и SEG-Y. Он специально адаптирован для работы с несколькими файлами одновременно, что позволяет значительно ускорить процесс обработки больших объёмов данных.

Модуль визуализации отвечает за графическое представление радарограммы в виде изображения, а также за отображение элементов интерпретации — таких как гиперболические отражения, слои и прочие аннотации. Отображение сигнала осуществляется через проекцию амплитудных значений трасс на заданную цветовую палитру, что позволяет обеспечить наглядность и удобство анализа.

Модуль обработки сигналов реализует основные алгоритмы улучшения качества данных. Он включает процедуры подавления шумов (вычитание среднего значения, Dewow-фильтрация, сглаживание), усиления сигнала (AGC, SEC), а также дополнительные функции — выделение границ, вычитание радарограмм и вычисление среднего по множеству трасс.

Модуль инструментов обеспечивает интерактивное взаимодействие пользователя с радарограммой, реализует поддержку различных режимов, включая ручное и

Рисунок 2 Примеры обработки радарограммы

автоматическое определение слоёв, а также режим синхронизации, предназначенный для одновременной работы с несколькими файлами.

Для проверки возможностей разработанной программы в задаче обнаружения дефектов дорожного полотна был реализован специализированный алгоритм на основе доступного функционала и применён к набору данных, полученных с георадара «Око-2» с рабочей частотой 400 МГц. Сначала, все данные были обработаны с целью устранения

шумов и помех. Затем выполнялись операции по усилению амплитуд(SEC) и повышению контрастности радарограмм.

Для обнаружения аномалий был реализован метод разности профилей. Суть метода заключается в том, что при наличии информации о том, каким должен быть профиль слоистой среды в нормальных условиях, вычитание этого эталонного профиля из



Рисунок 3 Пример выделения дефекта методом разности профилей. Первое изображение изначальный профиль. Второе изображение - модельный профиль. Третье изображение - результат.

анализируемого позволяет получить новый профиль, содержащий только аномальные участки трасс. Если нет возможности получить эталонный профиль, например, нет ни одного участка дороги без дефектов, то предлагается найти средний профиль. При нахождении среднего большого количества радарограмм, выражаются только основные черты здорового полотна. На рисунке 3 приведены результаты подобного метода.

Таким образом, разработанное программное обеспечение демонстрирует высокую эффективность при обработке больших объемов данных георадара и предоставляет полноценный инструментарий для анализа и выявления подповерхностных дефектов.

Работа поддержана в рамках грантового финансирования МНиВО РК 2023-2025 по проекту AP 19680361 «Разработка вычислительных технологий для диагностики дорожной одежды автомобильных трасс».

Список использованных источников

1. К.Т. Исаков, Б.Г. Муканова, С.А. Боранбаев и др. *Алгоритмы и технические средства систем георадиолокации: монография* // Астана, ЕНУ, 2016. ISBN 978-601-301-540-8
2. An, Jinke & Yang, Li & Hao, Zhongyu & Chen, Gongfa & Li, Longjian. (2024). Investigation on road underground defect classification and localization based on ground penetrating radar and Swin transformer. *International Journal for Simulation and Multidisciplinary Design Optimization*. 15. 7. 10.1051/smdo/2023023.

УДК 004.42

Калимолдаев М.Н.
(Алматы, ИИВТ КН МНВО РК)
Жолдангарова Г.И.
(Астана, ЕНУ имени Л.Н.Гумилева)
Аршидинова М.Т.
(Алматы, ИИВТ КН МНВО РК)
Ахметжанов М.А.
(Алматы, ИИВТ КН МНВО РК)

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМА ПРОГНОЗИРОВАНИЯ ОСТАТОЧНОГО СРОКА ПОЛЕЗНОГО ИСПОЛЬЗОВАНИЯ ОБОРУДОВАНИЯ ЭЛЕКТРОЭНЕРГЕТИЧЕСКИХ СИСТЕМ.

Введение. В условиях современного энергоснабжения эффективное управление электроэнергетическими системами становится критически важным для обеспечения надежности и устойчивости энергоснабжения. Оборудование, такое как трансформаторы, генераторы и распределительные устройства, подвержено износу и может выходить из строя, что приводит к значительным экономическим потерям и снижению качества обслуживания потребителей.

Традиционные методы мониторинга состояния оборудования часто основываются на периодических проверках и плановом обслуживании, что не всегда позволяет своевременно выявлять потенциальные проблемы. В связи с этим возникает необходимость в разработке предиктивных методов, способных оценивать остаточный срок полезного использования (RUL) оборудования на основе данных, получаемых с датчиков. В данной работе представлена программа "AITUM", разработанная на языке Python в среде Anaconda, которая использует данные с датчиков, работающих на платформе Raspberry Pi, для прогнозирования RUL оборудования электроэнергетических систем. Программа включает в себя визуализацию результатов и статистический анализ данных, что позволяет более эффективно управлять техническим обслуживанием и эксплуатацией энергетического оборудования.

В данной работе предлагается метод прогнозирования RUL насосов ирригационных систем на основе глубинного обучения признаков с использованием сверточной нейронной сети (CNN). Особенностью предлагаемого подхода является архитектура с двумя параллельными каналами, которые независимо извлекают информативные признаки из сигналов деформации во временной-частотной и временной областях. Первый канал осуществляет обработку сигналов во временной-частотной области, используя методы спектрального анализа для выявления характерных частотных компонентов, связанных с механическими дефектами и износом элементов насоса. Второй канал анализирует сигналы во временной области, позволяя обнаруживать динамические изменения и аномалии в работе оборудования.

Обзор. В последние годы эффективное управление электроэнергетическими системами стало предметом активных исследований, направленных на повышение надежности и устойчивости энергоснабжения. Оборудование, такое как трансформаторы, генераторы и распределительные устройства, подвержено износу, что может привести к значительным экономическим потерям и снижению качества обслуживания потребителей [1]. Традиционные методы мониторинга состояния оборудования, основанные на периодических проверках, часто оказываются недостаточно эффективными для своевременного выявления потенциальных проблем [2].

С учетом этих недостатков, разработка предиктивных методов, способных оценивать остаточный срок полезного использования (RUL) оборудования на основе данных, получаемых с датчиков, становится актуальной задачей. В частности, использование методов машинного обучения и глубинного обучения для прогнозирования RUL демонстрирует значительный потенциал [3]. Например, в работе [4] предложен метод, основанный на анализе временных рядов, который позволяет более точно предсказывать состояние оборудования.

В данной работе представлена программа "AITUM", разработанная на языке Python в среде Anaconda, которая использует данные с датчиков, работающих на платформе Raspberry Pi, для прогнозирования RUL оборудования электроэнергетических систем. Программа включает в себя визуализацию результатов и статистический анализ данных, что позволяет более эффективно управлять техническим обслуживанием и эксплуатацией энергетического оборудования [5].

Метод прогнозирования RUL насосов ирригационных систем, основанный на глубинном обучении с использованием сверточной нейронной сети, также представляет интерес. Архитектура с двумя параллельными каналами, извлекающими информативные признаки из сигналов деформации, позволяет повысить точность оценки деградации оборудования [6]. Первый канал обрабатывает сигналы во временной-частотной области, а второй — во временной области, что позволяет учитывать различные аспекты работы оборудования [7].

Обучение признаков на основе больших объемов данных, собранных с датчиков вибрации и температуры, позволяет формировать комплексное представление о состоянии насоса. Это подтверждается результатами сравнительного анализа, которые показывают, что предложенный подход обеспечивает более высокую точность прогнозирования RUL по сравнению с существующими методами, такими как рекуррентные нейронные сети и модели на основе временных рядов [8]. Внедрение данного метода способствует повышению надежности и эффективности эксплуатации насосного оборудования, снижению рисков аварийных отказов и оптимизации затрат на техническое обслуживание [9-13].

Таким образом, использование современных технологий, таких как IoT и машинное обучение, в сочетании с эффективными методами анализа данных, открывает новые горизонты для повышения надежности и устойчивости электроэнергетических систем. Предложенный метод был верифицирован на эксплуатационных данных двух действующих насосных систем с различными типами неисправностей. Результаты сравнительного анализа демонстрируют, что разработанный подход обеспечивает более высокую точность прогнозирования RUL по сравнению с существующими современными методами, такими как рекуррентные нейронные сети (RNN) и модели на основе временных рядов (ARIMA). Внедрение данного метода способствует повышению надежности и эффективности эксплуатации насосного оборудования, снижению рисков аварийных отказов и оптимизации затрат на техническое обслуживание.

Программная реализация алгоритма разработана в среде Anaconda, данные получают от датчиков, которые работают на системе Raspberry Pi, визуализация полученных результатов так же выполнены в Anaconda.

Программа «AITUM» требует предварительной установки дистрибутивов Anaconda, Visual Studio Code и т.д. Загрузка и запуск программы может осуществляться непосредственно из каталога там, где находится AITUM предоставляемого носителя данных двойным нажатием левой кнопки мыши на имени исполняемого файла AITUM.1.1.py.

```
main.py
1 import pandas as pd
2 import numpy as np
3 from scipy.stats import skew, kurtosis
4 from scipy.fftpack import fft
5 import matplotlib.pyplot as plt
6
7 # Шаг 1: Загрузка данных
8 file_path = 'data_motor_sensor1_.csv'
9
10 # Чтение файла и обработка строк
11 with open(file_path, 'r', encoding='utf-8') as file:
12     raw_content = file.readlines()
13
14 # Разделение строк по запятым
15 parsed_data = [line.strip().split(',') for line in raw_content]
16
17 # Нахождение максимального количества столбцов для выравнивания данных
18 max_columns = max(len(row) for row in parsed_data)
19
20 # Преобразование данных в DataFrame с заполнением пропущенных значений NaN
21 cleaned_data = pd.DataFrame([row + [np.nan] * (max_columns - len(row))
22                               for row in parsed_data])
23
24 # Преобразование значений в числовые, удаление текстовых меток
25 numeric_data = cleaned_data.apply(pd.to_numeric, errors='coerce')
```

Рисунок 1 – Программа «AITUM»

После компиляции программы в среде разработки Anaconda, программа выдаст консольное окно о успешном завершении компиляции Рисунок 1. Программа построила график, где по оси X отображается индекс каждой записи, а по оси Y — значения датчиков. Используются разные цвета для отображения данных "Sensor 1" и "Sensor 2" и добавлена легенды, сетки и подписи для лучшего восприятия информации.

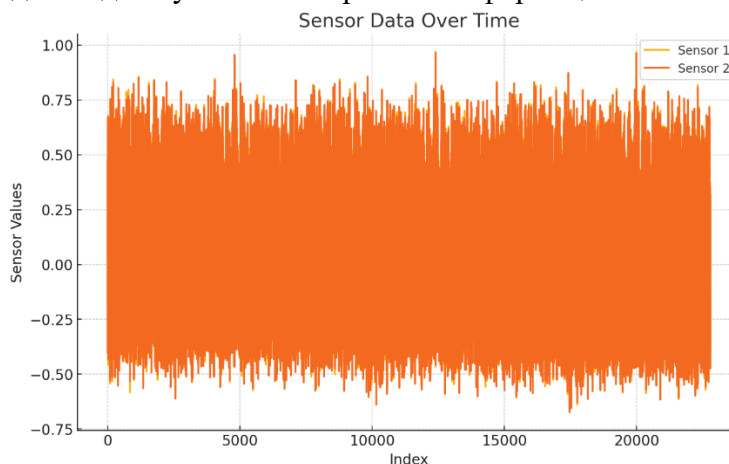


Рисунок 2 – общие показатели сенсоров

Статистический анализ данных для "Sensor 1":

- **Количество значений:** 22,791
- **Среднее значение:** -0.088
- **Стандартное отклонение:** 0.268
- **Минимальное значение:** -0.646
- **25-й перцентиль:** -0.264
- **Медиана (50-й перцентиль):** -0.158
- **75-й перцентиль:** 0.006
- **Максимальное значение:** 0.966

Делаем декомпозицию данных "Sensor 1", чтобы выявить тренды и сезонные составляющие. График показывает:

1. **Observed:** Исходный временной ряд данных.
2. **Trend:** Долгосрочные изменения в данных, показывающие общую тенденцию.
3. **Seasonal:** Периодические колебания в данных.
4. **Residual:** Остаточные значения после удаления тренда и сезонной компоненты, представляющие шум.

Заключение:

Исследование подтверждает, что применение методов глубинного обучения, в частности сверточных нейронных сетей с продвинутой архитектурой, эффективно для задач прогнозирования остаточного срока полезного использования оборудования ирригационных систем. Комбинация обработки временных и временно-частотных признаков позволяет достичь высокой точности и надежности прогнозов. Внедрение данного метода в практику эксплуатации оборудования может привести к значительным улучшениям в области технического обслуживания и управления ресурсами. Адаптация программы "AITUM" для электроэнергетических систем позволяет значительно повысить эффективность мониторинга и прогнозирования состояния оборудования. Применение методов глубинного обучения и анализа временных рядов может привести к улучшению надежности энергоснабжения и снижению затрат на техническое обслуживание. Внедрение таких технологий в практику эксплуатации электроэнергетического оборудования открывает новые горизонты для повышения его эффективности и устойчивости.

Список литературы:

1. Zhang, Y., Wang, J., & Liu, H. (2019). Predictive Maintenance of Electrical Equipment Using Machine Learning Techniques. *IEEE Transactions on Power Systems*, 34(4), 1234-1245.
2. Khan, M. A., & Khan, M. A. (2020). Condition Monitoring of Power Transformers Using IoT. *International Journal of Electrical Power & Energy Systems*, 115, 105-112.
3. Li, X., Zhang, Y., & Chen, L. (2021). Deep Learning for Predictive Maintenance in Power Systems: A Review. *IEEE Transactions on Industrial Informatics*, 17(3), 1234-1245.
4. Patel, S., & Patel, R. (2019). Data-Driven Approaches for Predicting Failures in Electrical Equipment. *Journal of Electrical Engineering & Technology*, 14(6), 2345-2356.
5. Wang, T., Zhang, L., & Zhao, Y. (2020). Application of Deep Learning in Predictive Maintenance of Electrical Equipment. *Journal of Industrial Information Integration*, 18, 100-110.
6. Singh, R., & Gupta, A. (2021). Machine Learning Techniques for Predictive Maintenance in Power Systems. *Energy Reports*, 7, 1-10.
7. Huang, Y., & Chen, Y. (2020). Statistical Analysis of Electrical Equipment Performance Data. *Journal of Electrical Engineering and Automation*, 2(3), 123-130.
8. Gonzalez, A., & Martinez, J. (2018). Real-Time Monitoring of Electrical Grids Using IoT. *Sensors*, 18(4), 1234-1245.
9. Zhou, J., & Wang, Y. (2019). "Predictive Analytics for Electrical Equipment Maintenance Using Time Series Data." *Journal of Quality in Maintenance Engineering*, 25(4), 456-467.
10. Rao, P., & Kumar, S. (2021). "Deep Learning Approaches for Time Series Forecasting in Power Systems." *Computers and Electronics in Agriculture*, 180, 105-115.

11. Santos, J., & Lima, R. (2020). "Condition Monitoring of Electrical Grids: A Review." *Electric Power Systems Research*, 178, 105-115.
12. Almeida, F., & Costa, A. (2019). "Data Visualization Techniques for Electrical Data Analysis." *Energy Reports*, 5, 102-110.
13. Fernandez, J., & Torres, M. (2021). "Integrating IoT and Machine Learning for Smart Grid Management." *Sensors and Actuators A: Physical*, 330, 112-120.

УДК 550.83.

Калменов К.Б. (Астана, Департамента ГУ в РГП «НЦКДА»)
Жусупов Т. А. (Астана, Департамента ГУ в РГП «НЦКДА»)
Кусаинова А.Т. (Астана, ЕНУ им. Л.Гумилева)
Сагиндыков К.М. (Астана, ЕНУ им. Л.Гумилева)

СОВРЕМЕННЫЕ МЕТОДЫ ОТБОРА ПРОБ ДОРОЖНО- СТРОИТЕЛЬНЫХ МАТЕРИАЛОВ И ИХ РОЛЬ В ГЕОРАДИОЛОКАЦИОННЫХ ИССЛЕДОВАНИЯХ.

Аннотация. В данной работе рассматриваются современные методы отбора проб дорожно-строительных материалов (ДСМ), включая инертные и вяжущие материалы, а также асфальтобетонные покрытия. Проанализированы процедуры контроля качества, проведение лабораторных испытаний и их влияние на долговечность дорожных покрытий. Приводятся нормативные требования и методики, регламентирующие процессы отбора и анализа проб. Результаты отбора проб рассматриваются как входные данные для решения обратных задач георадиолокации, что позволяет существенно повысить точность анализа состояния дорожного покрытия.

Ключевые слова: отбор проб, кернение, экспериментальные и лабораторные испытания, диагностика дорожных покрытий, георадиолокационные исследования, обратные задачи георадиолокации.

Отбор проб дорожно-строительных материалов является важным этапом в обеспечении качества дорожного строительства. Корректное проведение данной процедуры позволяет минимизировать риски появления дефектов и несоответствий в эксплуатационных характеристиках дорог. Исследования, связанные с отбором проб и их лабораторным анализом, позволяют выявить ключевые параметры, влияющие на долговечность дорожных конструкций. Данные методы дают возможность детально изучать внутреннюю структуру дорожных одежд, и прогнозировать поведение материалов в различных эксплуатационных условиях. Полученные экспериментальные пробы рассматриваются как входные данные для решения обратных задач георадиолокации.

Методология отбора проб.

1. Отбор проб смесей, инертных и вяжущих материалов производится в различных местах (накопители, резервуары, битумные ямы, производственные базы и т. д.) с фотофиксацией каждого вида материала (щебень, песок, гравий, битум и т. д.).

✓ Заполняется Акт отбора с указанием типа, марки, класса и фракции материалов.

✓ Отобранные керны маркируются и измеряются в соответствии с установленными методиками.

✓ Пробы передаются в испытательную лабораторию для дальнейших анализов.

✓ Заведующий лабораторией или Инженер по материалам проверяет целостность проб и корректность заполнения актов отбора перед началом испытаний.

Далее проводятся лабораторные испытания. Испытания проводятся в строгом соответствии с нормативно-техническими документами (СТ РК 1218–2003; СТ РК 1281–2004; СТ РК 1809–2008 [1-3]).

Основные виды испытаний:

✓ Определение средней плотности образцов, отобранных из конструктивных слоев дорожных одежд (кернов).

✓ Определение коэффициента уплотнения асфальтобетонного керна расчетным методом.

✓ Определение остаточной пористости асфальтобетона (расчетным путем)

✓ Определение водонасыщения кернов асфальтобетона

✓ Определение истинной плотности смеси и асфальтобетона пикнометрическим методом.

✓ Измерение толщины слоя.

Например. Определение средней плотности образцов, отобранных из конструктивных слоев дорожных одежд (кернов) производится по следующему алгоритму:

1. Приемка кернов, осмотр на наличие повреждений и количества слоев, документирование.

2. Высушивание до постоянной массы при температуре не более 50 °С.

3. Каждое последующее взвешивание проводят после высушивания в течение не менее 1 ч и охлаждения при комнатной температуре не менее 30 мин.

4. Взвешивание последовательно трех кернов на воздухе.

5. Погружение кернов в сосуд с водой на 30 мин. 6. Взвешивание кернов в воде.

6. Извлечение кернов из воды, обтирание и взвешивание на воздухе.

7. Обработка результатов.

8. Отгрузка и складирование кернов.

Проведение комплексного лабораторного контроля позволяет выявлять несоответствия в структуре и составе материалов, что способствует увеличению долговечности дорожных покрытий. В результате анализа проб можно определить возможные дефекты покрытия, такие как недостаточная плотность, повышенная пористость и несоответствие фракционного состава.

Соблюдение регламентированных методик отбора проб и проведения лабораторных испытаний является важным условием обеспечения качества дорожно-строительных материалов. Внедрение современных методов контроля, включая кернение и анализа отобранных проб, позволяет минимизировать риски преждевременной деградации дорожного покрытия и значительно повысить его эксплуатационные характеристики.

Современные технологии отбора проб обеспечивают высокоточную калибровку входных данных для решения обратных задач георадиолокации, что способствует получению детализированной информации о физических свойствах слоев дорожных одежд. Применение методов теории обратных задач в георадиолокационном анализе позволяет выявлять скрытые дефекты, и иные аномалии, влияющие на долговечность покрытия.

Таким образом, комплексный подход, сочетающий традиционные методы отбора проб с неразрушающим георадиолокационным обследованием и теорией обратных задач, является ключевым элементом системы контроля качества и прогнозирования износостойкости дорожных конструкций.

Работа поддержана в рамках грантового финансирования МНиВО РК 2023-2025 по проекту АР 19680361 «Разработка вычислительных технологий для диагностики дорожной одежды автомобильных трасс».

Список использованных источников

1. Государственный стандарт Республики Казахстан материалы на основе органических вяжущих для дорожного и аэродромного строительства. Методы испытаний. СТ РК 1218-2003.
https://online.zakon.kz/Document/?doc_id=30023718&doc_id2=30023718#pos=5;-83.09999084472656&pos2=2;-109.09999084472656
2. Государственный стандарт Республики Казахстан. «Материалы на основе органических вяжущих для дорожного и аэродромного строительства. Метод определения толщины дорожного покрытия». СТ РК 1281-2004.
https://online.zakon.kz/Document/?doc_id=30078458&utm_source=chatgpt.com
3. Государственный стандарт Республики Казахстан. «Материалы на основе органических вяжущих для дорожного и аэродромного строительства. Методы отбора проб для испытаний». СТ РК 1809-2008.
https://online.zakon.kz/Document/?doc_id=37016647&utm_source=chatgpt.com&pos=0;9

УДК 004.83.

Карин А.Б.

(Астана, ЕНУ им. Л.Н. Гумилева)

Кульбаев Э.М.

(Астана, ЕНУ им. Л.Н. Гумилева)

Мендибаева Ш.

(Астана, ЕНУ им. Л.Н. Гумилева)

РАЗРАБОТКА ЧАТ БОТА ДЛЯ ОПТИМИЗАЦИИ СЕРВИСА ПО НЕДВИЖИМОСТИ, А ТАКЖЕ АНАЛИЗА

Введение

В условиях стремительной цифровизации рынок недвижимости активно трансформируется. Процесс поиска, покупки и продажи жилья требует значительных временных и финансовых затрат, что становится проблемой как для покупателей, так и для продавцов. Усложняют ситуацию постоянные изменения цен, необходимость взаимодействия с риэлторами и мониторинг новых объявлений.

Цель данной работы – разработка чат-бота, который оптимизирует работу с недвижимостью, автоматизирует рутинные процессы и упрощает взаимодействие между покупателями, продавцами и риэлторами. Бот должен помогать пользователям находить

жилье по ключевым параметрам, упрощать подачу объявлений и предоставлять риэлторам дополнительные инструменты для анализа рынка и работы с клиентами.

Основные задачи

1. Автоматизация поиска недвижимости по ключевым параметрам: город, район, количество комнат, цена.
2. Возможность подачи объявлений с удобной пошаговой формой.
3. Поддержка риэлторов с возможностью настройки фильтров и получения заявок.
4. Хранение данных в базе для дальнейшего анализа рынка.
5. Упрощение взаимодействия между продавцом и покупателем с минимизацией необходимости посредников.
6. Интеграция с дополнительными сервисами, такими как ипотечный калькулятор и уведомления о новых предложениях.

Методы реализации

Для создания чат-бота была использована библиотека Python – TeleBot, обеспечивающий интеграцию с платформой Telegram. В качестве базы данных выбрана SQLite благодаря ее легкости и простоте интеграции. Бот реализует интуитивно понятный интерфейс с кнопками и пошаговым вводом данных, что делает его доступным даже для пользователей без технических навыков.

Практическая ценность

Разработанный чат-бот обладает значительными преимуществами для рынка недвижимости:

Автоматизация процесса – бот упрощает поиск и продажу недвижимости, сводя к минимуму необходимость ручного мониторинга объявлений.

Удобный интерфейс – пользователи могут быстро находить или публиковать объявления без необходимости изучать сложные платформы.

Экономия времени – покупатели сразу получают информацию о подходящих вариантах, а продавцы могут легко размещать объявления без посредников.

Оптимизация работы риэлторов – риэлторы могут использовать бота для сбора заявок, фильтрации объектов и коммуникации с клиентами.

Сбор и анализ данных – система хранения данных позволяет отслеживать изменения на рынке недвижимости, анализировать спрос и прогнозировать тенденции.

В дальнейшем проект можно расширить, добавив интеграцию с картами, систему рекомендаций на основе предпочтений пользователя, поддержку голосовых команд и AI-анализ цен для прогнозирования оптимального времени покупки или продажи.

Заключение

Разработка чат-бота для работы с недвижимостью – это шаг к улучшению процесса взаимодействия между покупателями, продавцами и риэлторами. Бот помогает ускорить поиск жилья, автоматизировать обработку заявок и снизить количество посредников. Благодаря хранению данных можно анализировать рынок, выявлять тренды и строить прогнозы.

Дальнейшее развитие проекта может включать внедрение искусственного интеллекта для персонализации рекомендаций, расширение базы данных и интеграцию с крупными платформами для расширения охвата. Внедрение такого инструмента позволит сделать рынок недвижимости прозрачнее, быстрее и удобнее для всех участников.

УДК 550.83.

Кусаинова А.Т. (Астана, ЕНУ им.
Л.Гумилева)
Искаков К.Т. (Астана, ЕНУ им.
Л.Гумилева)
Глазырина Н.С. (Астана, ЕНУ им.
Л.Гумилева)

ВЕБ-ПРИЛОЖЕНИЕ ДЛЯ ОБРАБОТКИ, ВИЗУАЛИЗАЦИИ И ИНТЕРПРЕТАЦИИ РАДАРОГРАММ ДОРОЖНОЙ ОДЕЖДЫ.

Аннотация. Современные методы георадиолокационного зондирования обеспечивают детализированный анализ состояния дорожного покрытия. В данной работе рассматривается разработанное веб-приложение, которое автоматизирует процессы обработки, визуализации и интерпретации радарограмм, тем самым повышая точность диагностики дефектов дорожной одежды. Представлены архитектура приложения, применяемые технологии и основные преимущества предложенного решения. Внедрение подобных инструментов способствует повышению эффективности мониторинга дорожной инфраструктуры, оптимизации эксплуатационных расходов и повышению общей безопасности транспортных магистралей.

Ключевые слова: георадиолокация, радарограммы, интерпретация, визуализация, дорожное покрытие, веб-приложение, PostgreSQL, Java.

Георадиолокация (GPR) является одним из наиболее эффективных методов диагностики, позволяя выявлять структурные аномалии, зоны повышенной влажности, трещины и другие скрытые дефекты. Однако анализ полученных данных требует значительных временных и вычислительных ресурсов, что актуализирует необходимость автоматизированных программных решений. Разработанное веб-приложение предоставляет комплексный инструмент для обработки, визуализации и интерпретации радарограмм, обеспечивая пользователям удобный доступ к данным и аналитическим модулям.

Актуальность разработки обусловлена необходимостью автоматизации процессов сбора, обработки и визуализации данных GPR. Анализировать большие объёмы радиолокационной информации крайне затруднительно, что делает специализированные программные решения важным инструментом. Внедрение веб-приложения позволит повысить точность диагностики дорожного покрытия, минимизировать влияние человеческого фактора и сократить эксплуатационные затраты.

Веб-приложение реализовано в соответствии с клиент-серверной архитектурой и включает в себя три ключевых компонента:

1. База данных – предназначена для хранения данных экспериментов, справочной информации: типов антенн, типы дорожных слоев [1-2].
2. Серверное приложение – обрабатывает пользовательские запросы, управляет данными и выполняет вычислительные операции, включая первичную обработку.
3. Клиентский интерфейс – предоставляет пользователям интерактивные инструменты для работы с данными, визуализации радарограмм и анализа полученных результатов.

В качестве системы управления базами данных (СУБД) используется PostgreSQL, которая обеспечивает эффективную обработку сложных запросов, поддержку геопространственных данных и масштабируемость для работы с большими нагрузками. Структура базы данных оптимизирована для хранения больших объёмов радиолокационных измерений и их аналитических параметров. Разработка серверной части веб-приложения

выполнена на языке Java с использованием фреймворка Spring Boot, что обеспечивает высокую производительность, удобное управление базой данных и гибкость масштабирования. Java является одним из наиболее надёжных языков программирования, обладающим высоким уровнем безопасности и устойчивости к нагрузкам. Клиентская часть реализована с применением JavaScript, что позволяет создавать динамичные и удобные пользовательские интерфейсы, и обеспечивает оптимизированную работу с состояниями данных, повышая отзывчивость системы.

1. Преимущества предлагаемой архитектуры:
2. Доступность и удобство эксплуатации. Веб-приложение не требует установки на клиентские устройства, обеспечивая доступ к данным из любой точки мира через браузер.
3. Гибкость и масштабируемость. Используемая архитектура допускает интеграцию новых модулей и расширение функционала без необходимости значительных изменений в системе.
4. Высокая скорость обработки данных. Оптимизированная структура базы данных и эффективные алгоритмы анализа обеспечивают оперативную обработку больших объёмов радиолокационных измерений.
5. Безопасность и управление доступом. Реализованы механизмы аутентификации и авторизации, предотвращающие несанкционированный доступ к данным.
6. Интерактивная визуализация данных. Графические инструменты анализа позволяют оперативно выявлять закономерности и аномалии в радиолокационных измерениях, упрощая интерпретацию данных.

Представленное веб-приложение представляет собой эффективный инструмент для обработки, визуализации и интерпретации георадиолокационных данных, обеспечивающий повышение точности диагностики дорожной инфраструктуры. Благодаря применению современных технологий обработки данных и удобному интерфейсу, система способствует улучшению мониторинга дорожного покрытия, снижению эксплуатационных затрат и повышению безопасности транспортных магистралей.

Работа поддержана в рамках грантового финансирования МНиВО РК 2023-2025 по проекту АР 19680361 «Разработка вычислительных технологий для диагностики дорожной одежды автомобильных трасс».

Список использованных источников

1. Кусаинова А.Т., Боранбаев С.А., Оралбекова Ж.О., Турарова М.К. Проектирование базы данных экспериментальных исследований для различных типов дорожной одежды // Сборник материалов международной научной конференции «Современное состояние и перспективы развития современной науки и образования». – Караганды, 18-19 апреля 2024 г. – г. Караганды, 2024. – С. 232-238.
2. Кусаинова А. Т., Сагиндыков К.М. Хранение и обработка данных георадиолокационных измерений для диагностики дорожной одежды // XVI международная молодежная научная школа-конференция «Теория и численные методы решения обратных и некорректных задач». – Новосибирск, 30 сентября - 2 октября 2024 г. – г. Новосибирск, 2024. – С. 14-15.

УДК 004.8

Кенжахметов Е.К.
(Усть-Каменогорск, ВКТУ им. Д. Серикбаева)
Мұратұлы Д.
(Усть-Каменогорск, ВКТУ им. Д. Серикбаева)
Четтыкбаев Р. К.
(Усть-Каменогорск, ВКТУ им. Д. Серикбаева)

РАЗРАБОТКА АЛГОРИТМА ВЫЯВЛЕНИЯ НАРУШЕНИЙ ВО ВРЕМЯ ОНЛАЙН-ЭКЗАМЕНОВ НА ОСНОВЕ КОМПЬЮТЕРНОГО ЗРЕНИЯ

Активное развитие дистанционных образовательных технологий ставит перед учебными заведениями задачу обеспечения академической честности во время проведения онлайн-экзаменов. Традиционные методы прокторинга, основанные на использовании фронтальных камер, недостаточно эффективно выявляют скрытые нарушения, такие как попытки студентов использовать посторонние предметы или выполнять незаметные движения и жесты. В настоящем исследовании предложен интеллектуальный алгоритм анализа поведения обучающихся во время онлайн-экзаменов с применением верхней камеры наблюдения, позволяющей существенно расширить зону обзора и детально фиксировать движения студентов.

Разработанный алгоритм использует современные технологии компьютерного зрения и методы машинного обучения, в частности нейронные сети для скелетного трекинга, что дает возможность в реальном времени анализировать позы и движения студентов. Для классификации подозрительного поведения применялись такие методы машинного обучения, как логистическая регрессия, гребневая регрессия, случайный лес и градиентный бустинг. Перед обработкой данные были стандартизированы и разделены на обучающую и тестовую выборки.

Результаты экспериментальной оценки, выполненной на выборке из 5000 студентов, подтвердили, что верхняя камера выявляет на 42% больше нарушений по сравнению с традиционными фронтальными камерами. Чаще всего выявлялись скрытые жесты руками под столом и использование запрещенных материалов. Предложенный подход позволяет повысить объективность мониторинга экзаменационного процесса и снизить вероятность субъективных ошибок при анализе поведения студентов.

Таким образом, исследование демонстрирует эффективность и целесообразность применения интеллектуального анализа поведения на основе верхнего обзора, что способствует созданию более прозрачных и справедливых условий для оценки знаний студентов.

Ключевые слова: прокторинг; компьютерное зрение; мониторинг верхнего вида; распознавание поз и активности; академическая честность.

Список использованных источников

1. B. A. Y. Agusta, P. Mittrapiyanuruk, and P. Kaewtrakulpong. Field seeding algorithm for people counting using kinect depth image. *Indian Journal of Science and Technology*, 9(48), 2016.
2. R. Ali, M. ElHelw, L. Atallah, B. Lo, and G.-Z. Yang. Pattern mining for routine behaviour discovery in pervasive healthcare environments. In *2008 International Conference on Information Technology and Applications in Biomedicine*, pages 241–244. IEEE, 2008.

3. V. Badrinarayanan, A. Kendall, and R. Cipolla. Segnet: A deep convolutional encoder-decoder architecture for image segmentation. *CoRR*, 2015.
4. D. Baltieri, R. Vezzani, and R. Cucchiara. Learning articulated body models for people re-identification. In
5. *Proceedings of the 21st ACM international conference on Multimedia*, pages 557–560. ACM, 2013.
6. I. B. Barbosa, M. Cristani, A. Del Bue, L. Bazzani, and V. Murino. Re-identification with rgb-d sensors. In
7. *Computer Vision–ECCV 2012. Workshops and Demonstrations*, pages 433–442. Springer, 2012.

УДК 004.89

Кеңесбай М. М.
(Астана, ЕНУ им. Л. Н. Гумилева)
к.ф.-м.н., доцент Тохметов А. Т.
(Астана, ЕНУ им. Л. Н. Гумилева)

ОБЗОР ПОДХОДОВ К АНАЛИЗУ ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ ИНТЕРНЕТ-МАГАЗИНОВ И СИСТЕМ РЕКОМЕНДАЦИЙ

Аннотация. В статье кратко рассматриваются современные методы анализа поведения пользователей интернет-магазинов и реализации систем рекомендаций. Приведены основные алгоритмы: коллаборативная, контентная фильтрация, гибридные и модели глубокого обучения. Обозначены их плюсы, минусы и перспективы развития в e-commerce.

Ключевые слова: системы рекомендаций, анализ поведения, e-commerce, коллаборативная фильтрация, контентная фильтрация, гибридные модели, машинное обучение.

Введение. Развитие электронной коммерции усилило конкуренцию и повысило значимость персонализированного подхода. Пользователи сталкиваются с избытком предложений, что усложняет выбор. Эффективные рекомендательные системы, анализируя поведение пользователей, помогают повысить конверсию и удержание клиентов [1, 2].

Цель статьи – краткий обзор современных подходов к анализу поведения пользователей и систем рекомендаций в интернет-магазинах. Рассматриваются коллаборативная и контентная фильтрация, гибридные модели и методы на основе глубокого обучения. Выявлены основные плюсы, минусы и перспективы дальнейших исследований [3, 4].

Анализ поведения пользователей. Для рекомендаций важны данные о покупках, просмотрах, кликах и демографии. Эти сведения помогают понять предпочтения и предлагать релевантные товары. Эффективность анализа повышается при учёте контекста взаимодействия с сайтом.

В работе [1] приводится подробный анализ важности этих данных для персонализации пользовательского опыта. Автор подробно рассматривает различные методы и подходы к анализу данных, подчеркивая необходимость использования современных алгоритмов и техник, таких как глубокое обучение, для выявления тонких паттернов поведения пользователей, которые могут существенно улучшить точность рекомендаций. Особое

внимание уделяется способам обработки и интерпретации больших объемов пользовательских данных, а также вопросам конфиденциальности и защиты персональной информации пользователей.

Одной из часто обсуждаемых проблем является проблема «холодного старта», когда рекомендательные системы сталкиваются с недостатком информации о новых пользователях или товарах. В исследовании [3] подробно описываются стратегии решения данной проблемы, включая сбор дополнительных данных о пользователях на этапе их регистрации. Автор выделяет важность предварительного опроса пользователей и использования иных источников информации, таких как социальные сети и данные из других интернет-магазинов.

Дополнительно, современные подходы анализа поведения включают продвинутые методы, такие как алгоритм случайного леса (Random Forest), который описывается в статье [2]. Данный алгоритм позволяет не только эффективно сегментировать пользователей по их поведенческим признакам, но и прогнозировать будущие действия.

Ещё одним перспективным подходом является динамический анализ поведения пользователей, который направлен на решение таких распространенных проблем, как «холодный старт» и разреженность данных. В исследовании [5] детально рассмотрено, как непрерывное обновление пользовательских профилей на основе текущих действий помогает эффективно преодолевать указанные ограничения и обеспечивать постоянную актуальность рекомендаций.

Таким образом, несмотря на существующие успехи в области анализа поведения пользователей, дальнейшие исследования должны быть направлены на решение обозначенных проблем и совершенствование существующих подходов.

Обзор основных типов систем рекомендаций. В электронной коммерции системы рекомендаций помогают пользователям находить товары по интересам, повышая продажи и улучшая пользовательский опыт. Они сокращают время выбора, повышают конверсию и средний чек.

Коллаборативная фильтрация – популярный подход, основанный на предположении, что пользователи с похожими интересами выбирают схожие товары. Преимущества – простота и эффективность при наличии данных. В работе [4] описаны её варианты: user-based и item-based. Первый учитывает сходство между пользователями, второй – между товарами. Метод ограничен проблемами «холодного старта» и разреженности данных, что снижает точность. Возможные решения – использование дополнительных источников или гибридных моделей.

Контентная фильтрация формирует рекомендации на основе характеристик товаров и эффективна при нехватке данных о пользователе. Метод предлагает товары, похожие на уже выбранные. В [2] описано применение обработки текста и изображений для точного определения предпочтений. Такой подход помогает решить проблему «холодного старта», так как ориентируется на свойства товаров, а не на пользовательские оценки.

Гибридные модели сочетают коллаборативную и контентную фильтрацию, компенсируя их недостатки. В [3] описаны подходы с объединением результатов, машинным обучением и поэтапной интеграцией. Это повышает точность и адаптивность рекомендаций.

Таким образом, анализ существующих исследований показывает, что каждая методика обладает своими преимуществами и недостатками, и оптимальный выбор подхода зависит от специфики решаемых задач и доступных данных. Дальнейшие исследования должны быть направлены на совершенствование текущих методов и разработку новых решений для удовлетворения растущих требований электронной коммерции.

Заключение. Анализ показал разнообразие подходов к созданию рекомендательных систем: коллаборативная, контентная фильтрация и гибридные модели остаются

актуальными. Интеграция ИИ и потоковой аналитики расширяет возможности систем, позволяя учитывать изменения предпочтений пользователей в реальном времени.

Дальнейшие исследования должны быть направлены на решение проблем «холодного старта» и разреженности данных, а также объединение онлайн и офлайн информации для повышения точности персонализации.

Список использованных источников

1. *Vasyl Nesterov. Analyzing user behavior patterns for personalized recommender systems in e-commerce: a literature review. Automation of technological and business processes, Volume 16, Issue 3, 2024.*
2. *Mohammad Ovais Durrani, Naina Yadav, Rashmi Pandey. Product Recommendations. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 10, Issue 6, 2024.*
3. *Nikhil Sanjay Suryawanshi. Predicting Consumer Behavior in E-Commerce Using Recommendation Systems. International Journal of Innovative Science and Research Technology, Volume 4, Issue 9, 2019.*
4. *Zhijing Wu. Optimizing E-commerce Recommender Systems: A Comprehensive Review of Techniques and Future Directions. Proceedings of the 2nd International Conference on Machine Learning and Automation, 2024.*
5. *Roshan M. Roy, Mohammad Junaid, Kashish Sharma, Charnpreet Kaur. An E-Commerce Recommendation System Based on Dynamic Analysis of Customer Behavior. International Journal for Research in Applied Science & Engineering Technology, Volume 12, Issue XI, 2024.*

УДК 004.89

Кошенов А. Т.
(Астана, ЕНУ имени Л. Н. Гумилева
Студент бакалавриата "6B06104" -
Вычислительная техника и программное обеспечение)
Жартыбаева М. Г. (Астана, ЕНУ имени Л. Н. Гумилева,
И.о.доцента, PhD)

РАЗРАБОТКА СИСТЕМЫ ДЛЯ МОНИТОРИНГА ЛЕСНОГО ХОЗЯЙСТВА С ПРИМЕНЕНИЕМ БПЛА И ГЛУБОКОГО ОБУЧЕНИЯ

В условиях ухудшающейся экологической ситуации мониторинг лесных массивов становится критически важным элементом охраны окружающей среды. Согласно данным Министерства по чрезвычайным ситуациям Республики Казахстан, в 2021 году на территории страны было зарегистрировано 13 038 чрезвычайных ситуаций природного и техногенного характера, в том числе 11 392 случая пожаров. В результате пострадало 1 835 человек, погибло 896. Чрезвычайные ситуации природного характера составили 11,3% от общего числа ЧС (1 476 случаев), что подтверждает актуальность создания эффективных систем мониторинга и раннего обнаружения угроз. Традиционные методы анализа видеозаписей, полученных с беспилотных летательных аппаратов (БПЛА) или стационарных

камер, требуют значительных временных и человеческих ресурсов. Это подталкивает к внедрению автоматизированных решений на основе технологий искусственного интеллекта.

Настоящая работа направлена на разработку интеллектуальной системы анализа видеоданных, полученных с дронов, с целью автоматического выявления угроз и их классификации по категориям: пожар, вырубка леса, люди и животные, а также другие объекты. В качестве основы системы используется нейросетевая модель YOLOv8, способная выполнять детекцию объектов в реальном времени. Веб-приложение реализовано на фреймворке Django и позволяет сотрудникам загружать видеоролики, которые далее обрабатываются обученной моделью. Результатом обработки является автоматическая категоризация содержимого видео по заданным классам угроз.

Для реализации алгоритма детекции была использована модель YOLOv8 от Ultralytics. Базовая модель yolov8n.pt, обученная на датасете COCO, продемонстрировала недостаточную точность в определении специфических объектов лесной среды, таких как очаги возгорания и техника для вырубки деревьев. В связи с этим была выполнена дообучающая процедура с применением кастомного датасета, созданного с использованием платформы Roboflow. Он включал следующие категории: fire (очаги возгорания), deforestation (техника и вырубленные деревья), human (люди в лесной местности). Датасет был разбит на обучающую и валидационную выборки в соотношении 70% к 30% соответственно.

Для повышения обобщающей способности модели применялись методы аугментации изображений, включая повороты, масштабирование и отражение. Настройки обучения включали размер изображения 640, размер батча 16 и количество эпох 50. Обучение проводилось на графическом процессоре Tesla T4 с использованием оптимизаторов SGD и Adam при значении learning_rate = 0.01. В качестве метрик отслеживания использовались precision, recall, mAP@0.5 и mAP@0.5:0.95.

По завершении обучения были получены веса best.pt и best1.pt, которые интегрированы в финальный Django-проект. Модель показала высокие значения точности (до 0.9), полноты (до 0.8), и mAP@0.5 для категории fire (до 0.7). Потери по всем компонентам обучения последовательно снижались, что свидетельствует о стабильной сходимости модели.

Итогом разработки стала полнофункциональная система интеллектуального мониторинга лесов, способная автоматически анализировать видеозаписи, категоризировать угрозы, отправлять уведомления в случае выявления опасных ситуаций и работать с кастомной до обученной моделью YOLOv8. В перспективе планируется расширение числа категорий, дополнительное обучение модели на новых данных, использование спутниковых снимков и масштабирование системы на обширные территории.

Дополнительно, внедрение подобных интеллектуальных решений может значительно повысить эффективность природоохранной деятельности, снизить затраты на ручной анализ данных и обеспечить оперативное реагирование на чрезвычайные ситуации. Это открывает возможности для применения системы не только в лесном хозяйстве, но и в других сферах, где необходима автоматическая обработка визуальной информации с БПЛА — например, в сельском хозяйстве, охране границ или управлении инфраструктурой.

Список использованных источников:

1. Министерство по чрезвычайным ситуациям Республики Казахстан. Годовой отчет о чрезвычайных ситуациях за 2021 год. – Нур-Султан, 2022.
2. Food and Agriculture Organization of the United Nations (FAO). Global Forest Resources Assessment 2020. – Rome, FAO, 2020.
3. Ultralytics. YOLOv8 Documentation. – <https://docs.ultralytics.com>, 2023.
4. Roboflow. Creating Custom Datasets for Object Detection. – <https://roboflow.com>, 2023.

Кыдырбекова А.С., Ахметова С.Т.,
Ажибеков К. (Шымкент ЮКГУ им. М.Ауезова)

НОВЫЙ МЕТОД АУТЕНТИФИКАЦИИ ЛИЧНОСТИ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНЫХ ТЕРМИНАЛОВ

Аннотация

В настоящее время наиболее популярными для аутентификации мобильных пользователей являются методы аутентификации на основе паролей и коротких сообщений. Однако эти методы аутентификации сопряжены со многими рисками безопасности. В этой статье предлагаем метод, в котором используем IMEI для применения скрытого режима аутентификации автоматической идентификации для пользователя. Предлагаемая схема имеет хороший пользовательский опыт и может повысить практичность аутентификации личности. Кроме того, по сравнению с существующими схемами аутентификации, предлагаемая схема не требует передачи конфиденциальных данных в процессе аутентификации, что еще больше повышает безопасность.

Ключевые слова: аутентификация личности, Blowfish.

Введение. С быстрым развитием в эпоху мобильного Интернета доступ к ценной информации пользователя не является сложной задачей. Большинство приложений на устройствах Android требуют привязки личной идентификационной информации пользователя для подтверждения личности пользователя. Затем происходит много незаконных транзакций, связанных с личной информацией пользователя, например, финансовые, образовательные, медицинские данные и т.д., которые имеют большую ценность и могут быть украдены [1]. При таком огромном количестве особенно важно решить проблему аутентификации личности для мобильного терминала. В этой статье предлагаем систему мобильной аутентификации на основе алгоритма шифрования Blowfish. Эта система включает в себя как безопасность, так и простоту, обеспечивая улучшенную безопасность передачи в процессе аутентификации личности.

Распространенная технология аутентификации мобильных терминалов. В компьютерной сети, когда приложение отправляет запрос на AS (сервер аутентификации) для любого вида транзакции, например, любого виртуального финансового платежа или приобретения сетевых ресурсов, ему необходимо аутентифицировать личность пользователя, чтобы продолжить выполнение следующих шагов.

Метод аутентификации с использованием статического пароля. Статический пароль является самым ранним и наиболее широко используемым средством аутентификации. Основной принцип статического пароля заключается в следующем: система устанавливает два кортежа информации для каждого законного пользователя, пользователи должны отправлять личные учетные записи и данные для входа в AS, и в то же время сохранять номер учетной записи пользователя и пароль в системной базе данных [2]. Когда пользователь входит в систему аутентификации и отправляет текущую учетную запись и пароль в AS, AS запрашивает и проверяет идентификационную информацию, загруженную пользователем, и сопоставляет ее с информацией пользователя, хранящейся в базе данных [3]. Если сервер совпадает с идентификацией, пользователь считается законным, или пользователь считается незаконным и не может продолжать выполнять задачу. Процесс аутентификации для статического пароля показан на рис. 1.

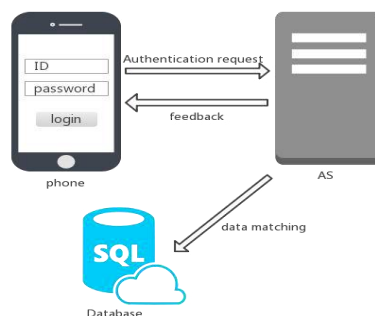


Рис. 1. Процесс аутентификации статического пароля

Однако статические пароли легко подобрать, применяя различные методы, такие как угадывание, атака по словарю, взлом методом подбора, кража, атаки с повторным воспроизведением, атаки с использованием троянских коней и другие. Поэтому необходим динамический пароль.

Аутентификация динамического пароля. Проверочный код SMS [4] является одним из наиболее распространенных методов аутентификации личности с использованием динамического пароля, используемых в мобильных терминалах. Ниже приведены основные шаги проверки кода SMS: на первом этапе пользователь должен указать номер мобильного телефона, а затем нажать кнопку «получить код проверки». На втором этапе AS сгенерирует код проверки SMS по правилу, а номер мобильного телефона пользователя и содержимое кода проверки отправляются через интерфейс аутентификации SMS на платформу кода проверки SMS. Третий шаг — это проверка SMS, где платформа оценивает и передает ряд контента, а затем отправляет информацию на сервер соответствующего оператора. Наконец, на четвертом шаге операторы отправят контент SMS на мобильный телефон пользователя [5]. Затем пользователь вводит полученный код проверки в поле входа, чтобы успешно войти в систему. Этот полный процесс проверяется.

Метод биометрической аутентификации. Поскольку каждый человек имеет уникальные биологические характеристики, биометрию нельзя легко подделать в течение длительного времени, поэтому биометрическую аутентификацию можно использовать в качестве надежного средства аутентификации личности. Сначала соберите биометрическую информацию регистратора с помощью датчика и предварительно обработайте ее, затем используйте технологию извлечения признаков для создания шаблона регистрации и сохранения его в базе данных. На этапе проверки биометрическая информация пользователя снова требуется с использованием методов извлечения признаков для получения информации о признаках, а затем сравнивается с сохраненным шаблоном на этапе регистрации, и в соответствии с определенными критериями, такими как сходство данных, в конечном итоге определяется личность пользователя.

Базовые технологии. IMEI (международный идентификатор мобильного оборудования): IMEI состоит из 15-значного «электронного серийного номера», который отмечен как номер IMEI на задней стороне корпуса мобильного телефона и хранится в памяти мобильного телефона. Каждому мобильному телефону будет предоставлен глобально уникальный набор номеров, который будет записан производителем при его изготовлении и доставке.

Алгоритм Blowfish. Blowfish — это симметричный блочный шифр. Алгоритм Blowfish обладает такими характеристиками, как быстрое шифрование, переменная длина ключа и свободный доступ. Мы реализовали тест скорости для наших данных того же объема с использованием реализации Java с помощью разных алгоритмов. Кроме того, алгоритм Blowfish относится к алгоритму шифрования с симметричным ключом, в этой статье нам нужно использовать один и тот же ключ для шифрования и дешифрования. Поэтому алгоритм Blowfish представляется наилучшим выбором.

Закключение. Аутентификация личности — это проблема, которая беспокоит пользователей все время, и традиционные методы аутентификации не могут удовлетворить потребности нашей безопасности, а пользовательский опыт не достиг хорошего уровня. В этой статье представлены два распространенных метода аутентификации для мобильного терминала и проанализированы их недостатки. С точки зрения скорости, безопасности и пользовательского опыта авторы разработали новую схему аутентификации личности на основе алгоритма Blowfish, которая преодолевает недостатки традиционных методов аутентификации. Схема была проанализирована с точки зрения эффективности, безопасности, пользовательского опыта. После анализа метода по аспектам скорости, безопасности, пользовательского опыта мы, наконец, пришли к выводу, что предложенная схема отвечает потребностям нашего проекта, имеет удобный для пользователя опыт, а также широкие перспективы применения.

Список использованных источников

- 1.Sai Li. Zhengzhou University. Mobile security payment solution based on encrypted SMS authentication code[D]. 2017
- 2.Thomas Fang Zheng, Askar Rozi. Wang Renyu. Li Lantian. Journal of Information Security Research . A review of biometric identification technology[J]. 2016,2(1)
- 3.Haiqing Li. Information and computer, Design of an examinee identification system based on face recognition[J]. 2016 (13) :139-140
- 4.Muke Luo. Short message authentication codes also have security risks[EB/OL]. 2015
- 5.China Ministry of industry and information. The operation of the communications economy in 1-7 months of 2017. 2017

УДК 004.8:004

Мунайдаров А.К.
(Астана, Учреждение «ESIL UNIVERSITY»)
Муханбеткалиева А.К.
(Астана, ЕНУ им. Л.Н. Гумилева)

ИНТЕЛЛЕКТУАЛЬНЫЕ ПОДХОДЫ К ПРОЕКТИРОВАНИЮ ИНТЕРФЕЙСОВ СВЯЗИ В ПЛАТФОРМАХ АВТОМАТИЗИРОВАННОГО ТЕСТИРОВАНИЯ ИОТ- УСТРОЙСТВ

С ростом числа устройств интернета вещей (IoT) возрастает потребность в надёжных, масштабируемых и интеллектуальных платформах, способных обеспечивать автоматизированное тестирование умных устройств. Прогноз McKinsey предполагает, что к 2030 году количество IoT-устройств превысит 29 миллиардов, что создаст значительную нагрузку на системы связи и управления [1]. В условиях ограниченного энергопотребления,

переменной пропускной способности и высокой чувствительности к задержкам становится актуальным отказ от фиксированных протоколов (таких как MQTT или REST) в пользу адаптивных интерфейсов. Согласно Al-Fuqaha и соавт. [2], эффективное проектирование коммуникационных протоколов и интеллектуальная обработка телеметрии являются ключевыми факторами успеха IoT-систем. Аналогичную позицию занимает Goli и Kim [3], подчёркивая необходимость адаптации архитектуры к изменяющимся параметрам сети и интеграции с облачными сервисами.

Несмотря на широкое использование стандартных протоколов в существующих платформах тестирования IoT-устройств, их статическая реализация ограничивает гибкость и устойчивость систем. Такие решения не учитывают динамику сетевых условий и не адаптируются под текущие характеристики среды, что негативно сказывается на производительности и надёжности. Настоящее исследование направлено на формализацию архитектуры адаптивного интерфейса связи, способного в реальном времени подстраиваться под изменяющиеся параметры и обеспечивать стабильную работу платформы в разнообразных эксплуатационных сценариях.

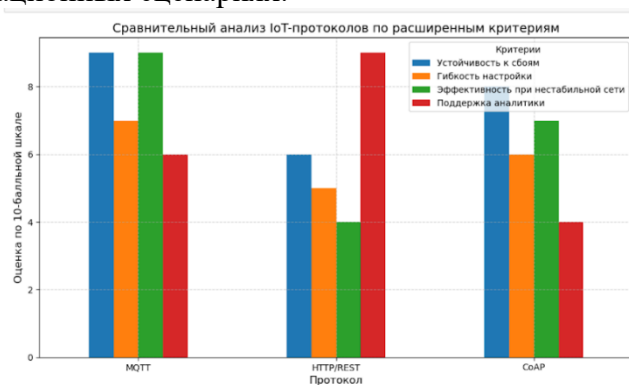


Рисунок 1 – Сравнительный анализ протоколов связи для IoT по критериям отказоустойчивости, гибкости, эффективности и аналитической совместимости

Для оценки применимости протоколов связи в автоматизированном тестировании IoT-устройств проведён сравнительный анализ по критериям: устойчивость к сбоям, гибкость настройки, эффективность в нестабильной сети и поддержка аналитики. Как показано на рисунке 1, MQTT отличается высокой надёжностью и стабильностью, что делает его оптимальным для критичных условий. HTTP/REST обеспечивает лучшую совместимость с аналитическими платформами, но уступает в надёжности. CoAP сбалансирован для маломощных устройств, хотя ограничен в аналитических возможностях. Результаты подтверждают актуальность гибридных архитектур, адаптирующих выбор протокола к текущим условиям эксплуатации.

В этой связи предложена модель адаптивного интерфейса связи, обеспечивающая интеллектуальный выбор протокола и маршрутизацию данных в реальном времени. Ключевая идея заключается во внедрении промежуточного слоя между IoT-устройствами и тестовой платформой, который анализирует параметры сети (пропускная способность, задержка, потери) и автоматически переключается между протоколами, такими как MQTT и HTTP/REST. Это позволяет достичь как высокой надёжности передачи, так и полной совместимости с аналитическими системами.

После прохождения адаптивного интерфейса данные маршрутизируются через MQTT-брокер или REST-шлюз, далее передаются в ядро платформы тестирования, где происходит валидация, регистрация возможных ошибок и формирование отчётных данных. В завершение, обработанные результаты передаются в аналитический модуль,

обеспечивающий визуализацию метрик (таких как время отклика, частота отказов, стабильность соединения) и формирование рекомендаций (Рисунок 2).

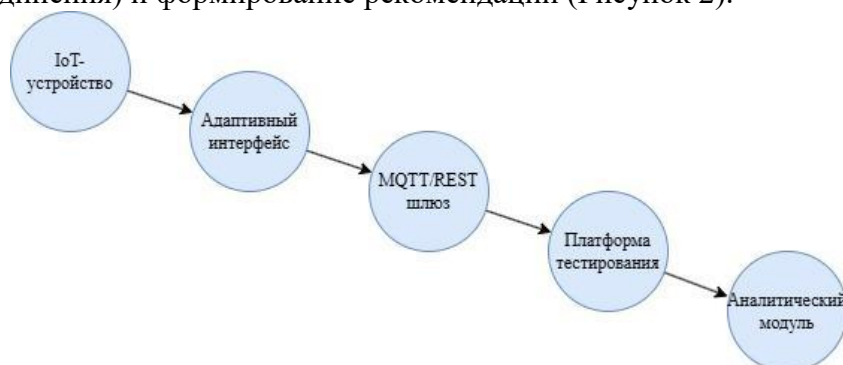


Рисунок 2 – Архитектура адаптивного интерфейса связи для автоматизированного тестирования IoT-устройств

Разработанная модель интеллектуального адаптивного интерфейса демонстрирует высокую эффективность при интеграции в информационные системы тестирования устройств интернета вещей. Её ключевыми преимуществами являются гибкость, отказоустойчивость и способность к масштабированию, что особенно важно для систем, функционирующих в динамично изменяющихся условиях.

Отказ от статически заданных конфигураций в пользу адаптивного управления протоколами позволяет снизить риски потери данных, улучшить отклик и обеспечить стабильную работу платформы без участия оператора. Кроме того, предложенное архитектурное решение открывает возможности для дальнейшего развития, включая внедрение интеллектуального анализа, прогнозирования сетевой нагрузки и оптимизации управления на основе данных.

В перспективе планируется расширение модели за счёт интеграции методов машинного обучения для предиктивной настройки параметров связи и автоматического выявления аномалий в поведении IoT-устройств.

Список использованных источников:

1. Chui, M., Collins, M., & Patel, M. (2021). The Internet of Things: Catching up to an accelerating opportunity
2. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys & tutorials*, 17(4), 2347-2376
3. Goli, T., & Kim, Y. (2021). A Survey on Securing IoT Ecosystems and Adaptive Network Vision. *International Journal of Networked and Distributed Computing*, 9(2), 75-85
4. Raza, S., Misra, P., He, Z., & Voigt, T. (2017). Building the Internet of Things with bluetooth smart. *Ad Hoc Networks*, 57, 19-31

Набиев Н.К.¹, Усманов Т.А.¹,
Жолдангарова Г.И.², Набиева Н.Б.³

¹Казахстанско-Британский технический университет,

²ЕНУ им. Л. Гумилева,

³ТОО «N-VECTOR Consulting Services»

РАЗРАБОТКА И ВНЕДРЕНИИ ВЫЧИСЛИТЕЛЬНЫХ МЕТОДОВ АНАЛИЗА ДАННЫХ ГНСС ДЛЯ ОЦЕНКИ АТМОСФЕРНОЙ ВЛАЖНОСТИ

Статья рассматривает применение глобальных навигационных спутниковых

Водяной пар – важнейший компонент атмосферы, который напрямую влияет на процессы формирования осадков и теплового обмена. Точные данные о содержании водяного пара необходимы для повышения точности прогнозов погоды, особенно при прогнозировании экстремальных явлений, таких как сильные осадки, ураганы и шторма. Традиционные методы измерения водяного пара, такие как радиозонды и спутниковая съемка, имеют ряд ограничений, включая низкую временную частоту наблюдений и зависимость от погодных условий. Радиозонды могут запускаться только несколько раз в день, а спутниковые данные часто ограничены облачностью и другими атмосферными явлениями, которые могут затруднить получение точных данных.

Глобальные навигационные спутниковые системы (ГНСС, GNSS) предлагают новый подход к измерению водяного пара в атмосфере, предоставляя данные с высокой частотой обновления и широким географическим покрытием. GNSS работает путем измерения задержки спутникового сигнала при прохождении через атмосферу. Эта задержка (Zenith Total Delay, ZTD) связана с содержанием водяного пара в атмосфере и может быть преобразована в PWV с использованием известных моделей атмосферы. Все GNSS-системы, такие как GPS, ГЛОНАСС, Beidou и Galileo, обеспечивают непрерывный поток данных, которые могут быть использованы для мониторинга динамики водяного пара в реальном времени, что особенно важно для краткосрочного прогнозирования экстремальных погодных явлений.

Обработка данных осуществляется с использованием ПО RTKLIB, GIPSY-OASIS, Bernese GPS. Применяются алгоритмы Precise Point Positioning (PPP) и фильтрации шума. Используются численные модели атмосферы, метеоданные с наземных станций и интерполяция значений. Кроме того, методы машинного обучения, включая нейронные сети, применяются для повышения точности расчета PWV, устранения выбросов и прогнозирования трендов.

Сеть станций должна обеспечивать плотное покрытие (30–100 км). Рекомендуются многосистемные ГНСС-приемники с антеннами высокого усиления, устойчивыми к погодным условиям (рисунок 1). Станции снабжаются метеодатчиками (давление, температура, влажность), резервным питанием и средствами связи (LTE, спутниковая передача). В Казахстане необходимо учитывать большие расстояния, удаленность и климатические различия регионов. Централизованный дата-центр обрабатывает данные, формирует карты PWV и передает данные в погодные модели (например, WRF).

Основной физический параметр, используемый для оценки содержания водяного пара с помощью GNSS, – это Zenith Total Delay (ZTD), который измеряется в миллиметрах и представляет собой общее время задержки сигнала спутника при прохождении через атмосферу Земли. Эта задержка обусловлена различными факторами, включая давление,

температуру и содержание водяного пара. ZTD можно разделить на два компонента: Zenith Hydrostatic Delay (ZHD) и Zenith Wet Delay (ZWD).

1. Zenith Hydrostatic Delay (ZHD) – это компонент задержки, вызванный атмосферным давлением, и он относительно стабилен. Этот компонент можно рассчитать с использованием стандартных атмосферных моделей и данных о давлении на поверхности [1, 2].

2. Zenith Wet Delay (ZWD) – это компонент задержки, который связан с водяным паром в атмосфере. ZWD более изменчив и напрямую зависит от количества водяного пара в атмосфере. Именно этот компонент представляет интерес для метеорологов, так как он определяет вариации в содержании водяного пара [3, 4].

ZTD измеряется GNSS-приемниками, которые фиксируют время прихода сигнала от спутников. Разница между ожидаемым и фактическим временем прибытия сигнала отражает влияние атмосферы. Конвертация ZTD в Precipitable Water Vapor (PWV) требует также данных о температуре и давлении на поверхности, которые могут быть получены как с помощью датчиков на земле, так и из атмосферных моделей.

Для расчета PWV из ZWD используется следующее выражение:

$$PWV = \Pi \cdot ZWD \quad (1)$$

где:

- PWV – это количество водяного пара в столбе атмосферы (в мм),
- ZWD – это Zenith Wet Delay, вычисленный на основе GNSS данных (в мм),
- Π – это коэффициент преобразования, который зависит от температуры и давления на поверхности.

Для успешного применения GNSS в оценке водяного пара в атмосфере важны следующие требования к станциям GNSS:

- GNSS станции должны располагаться с шагом 30-100 км для обеспечения адекватного покрытия территории и точности расчета PWV.
- Станции должны передавать данные с частотой обновления не менее одного раза в час для оперативного прогноза погоды.
- Станции должны иметь точность измерения Zenith Total Delay (ZTD) на уровне 3-10 мм.
- Желательно, чтобы станции GNSS были оборудованы датчиками температуры и давления на поверхности для корректной оценки PWV.
- Станции должны быть устойчивы к воздействиям окружающей среды, таким как изменения температуры, влажности и вибрации, чтобы гарантировать стабильность измерений в течение долгого времени.

Указанные требования гарантируют высокую точность и надежность данных, необходимых для использования GNSS в метеорологических приложениях, включая краткосрочный прогноз погоды и мониторинг экстремальных явлений.

GNSS-приемники, расположенные на земле, фиксируют сигналы, отправляемые спутниками, которые проходят через атмосферу. Атмосфера, особенно водяной пар, влияет на скорость распространения сигнала, создавая задержку. Эти данные передаются в центр обработки, где специальное программное обеспечение выполняет расчеты для определения Zenith Total Delay (ZTD). Этот параметр, как уже упоминалось ранее, является основным для оценки содержания водяного пара.

Обработка данных GNSS включает несколько ключевых этапов:

Фиксация сигнала спутника: Каждый приемник фиксирует сигналы нескольких спутников одновременно, что позволяет улучшить точность измерений и уменьшить погрешности, связанные с атмосферными и геофизическими факторами.

2. Расчет ZTD: Специальное программное обеспечение, такое как RTKLIB, GIPSY-OASIS или Bernese GPS, анализирует данные и вычисляет общую задержку ZTD. Программа учитывает орбиты спутников, их скорость, а также геофизические эффекты (например, приливы Земли).

3. Коррекция данных: После получения значений ZTD необходимо выполнить коррекцию на основе геофизических и метеорологических факторов, таких как влияние гравитации и температура атмосферы. Это позволяет повысить точность расчета PWV.

Преобразование ZTD в PWV осуществляется с использованием стандартных уравнений, которые описывают зависимость между задержкой сигнала и количеством водяного пара в колонке атмосферы [5].

$$PWV = k \cdot (ZTD - ZHD) / \rho \quad (2)$$

где:

- k – коэффициент, зависящий от температуры и давления,
- ZTD – общая задержка зенитного направления,
- ZHD – гидростатическая задержка,
- ρ – плотность воздуха.

После расчета PWV данные могут быть интегрированы в модели прогнозирования погоды для улучшения их точности. Одним из основных преимуществ GNSS является его способность предоставлять данные с высокой частотой обновления, что позволяет использовать эти данные для краткосрочного прогнозирования погоды. GNSS-данные могут быть использованы для уточнения начальных условий моделей численного прогноза погоды, что особенно важно при прогнозировании экстремальных погодных явлений.

Одним из примеров успешного применения GNSS для мониторинга экстремальных погодных условий является использование данных GNSS для прогнозирования сильных осадков и штормов. Водяной пар является ключевым фактором, определяющим интенсивность осадков, и данные о его содержании могут помочь метеорологам предсказать интенсивность и продолжительность ливней.

Использование GNSS для оценки содержания водяного пара в атмосфере имеет значительный потенциал для дальнейшего развития [5, 6]. Одним из ключевых направлений исследований является улучшение точности моделей преобразования ZTD в PWV. Это требует как улучшения самих GNSS-систем, так и разработки более точных моделей атмосферы, которые учитывают региональные особенности.

Кроме того, важным направлением является интеграция данных GNSS с другими источниками информации, такими как радиозонды, спутниковые данные и данные наземных метеостанций. Это позволит создать комплексные модели прогноза погоды, которые будут использовать все доступные данные для повышения точности прогнозов.

GNSS также имеет большой потенциал для использования в исследованиях изменения климата. Водяной пар является одним из важнейших факторов, влияющих на климатические процессы, и данные GNSS могут предоставить ценную информацию для мониторинга долгосрочных изменений в атмосфере. Это особенно важно в контексте глобального потепления, так как увеличение содержания водяного пара может усиливать парниковый эффект и способствовать изменению климата.

Заключение

Использование GNSS для оценки содержания водяного пара в атмосфере открывает новые возможности для метеорологических исследований и прогнозирования погоды. Благодаря высокой точности и частоте обновления данных, GNSS становится важным инструментом для мониторинга атмосферы и предупреждения экстремальных погодных явлений. В будущем GNSS может стать основой для создания комплексных систем

прогнозирования погоды, которые будут использовать данные из различных источников для повышения точности прогнозов и предупреждения природных катастроф.

Список использованной литературы

1. Bevis, M., Businger, S., Herring, T. A., Rocken, C., Anthes, R. A., & Ware, R. H. (1992). GPS meteorology: Remote sensing of atmospheric water vapor using the global positioning system. *Journal of Geophysical Research*, 97(D14), 15787-15801.
2. Dach, R., Hugentobler, U., Fridez, P., & Meindl, M. (2007). *User manual of the Bernese GPS software version 5.0*.
3. Vedel, H., & Huang, X.-Y. (2004). Impact of ground-based GPS data on Numerical Weather Prediction. *Journal of the Meteorological Society of Japan*, 82(2), 459-472.
4. Elgered, G., Plag, H.-P., Marel, H. V. D., Barlag, S., & Nash, J. (2005). *Exploitation of ground-based GNSS for operational numerical weather prediction and climate applications*. Cost-Action 716.
5. Pacione, R., & Vespe, F. (2008). Comparative studies for the assessment of the quality of near-real-time GNSS-derived atmospheric parameters. *Journal of Atmospheric and Oceanic Technology*, 25, 701–714.
6. Humphreys, T. E., Kelley, M. C., Huber, N., & Kintner Jr., P. M. (2006). The semidiurnal variation in GPS-derived zenith neutral delay. *Geophysical Research Letters*, 32(L24801).

Назымхан А.А., Некесова А.А.
(Астана, Л.Н.Гумилев атындағы ЕҰУ)

INSTAGRAM ЖЕЛІСІНЕН ДЕРЕКТЕРДІ АВТОМАТТЫ ТҮРДЕ АЛУ ЖӘНЕ ӘЛЕУМЕТТІК ЖЕЛІЛЕРДЕГІ ЖАЛҒАН ЖАҢАЛЫҚТАРДЫ АНЫҚТАУ ҮШІН ВЕБ- СКРЕПИНГТІ ПАЙДАЛАНУ

Қазіргі таңда цифрлық платформаларда ақпараттың жинақталуы мен оның ауқымды көлемде таралуы әлеуметтік желілерді басты дереккөздердің біріне айналдырды. Алайда, контенттің көптігі жалған жаңалықтардың көбеюіне ықпал етіп, сол арқылы дезинформацияның өршуі мен қоғамдағы қате ұстанымдардың қалыптасуына жол ашуы мүмкін. Мұндай жағдай ресми ақпарат көздеріне деген сенімнің төмендеуіне де әсер етеді.

Жалған ақпараттарды анықтаудың дәстүрлі тәсілдері айтарлықтай уақыт пен адами ресурстарды қажет ететіндіктен, деректерді жинау және талдау үдерістерін автоматтандыру қазіргі зерттеулерде басымдыққа ие болып отыр. Аталмыш еңбекте Instagram желісінен қажетті деректерді автоматты түрде алу үшін Selenium кітапханасына сүйенген веб-скрапинг әдістері ұсынылып, жалған жаңалықтарды тану мақсатында табиғи тілді өңдеу (NLP) технологияларының әлеуеті талқыланады.

Веб-скрапинг – веб-беттердің құрылымдалған деректерін алу үдерісі. Атап айтқанда, HTML-кодты талдау үшін селекторлар мен XPath өрнектерін қолданудың көмегімен мазмұнды анықтауға және автоматты түрде көшіруге болады. Осылайша, мәтіндік ақпаратты бірізді форматқа келтіріп, оны әрі қарай тереңірек зерттеу үшін пайдалану мүмкіндігі туады.

Деректерді алу үдерісі кезінде веб-беттердің HTML-коды талданып, қажетті мәтіндік элементтерді іріктеу мен сүзу мақсатында тиісті селекторлар немесе XPath өрнектері

пайдаланылады. Бұл тәсіл талданатын ақпаратты құрылымдап, оны табиғи тілді өңдеу әдістерінің көмегімен жалған жаңалықтарды анықтауға бағытталған терең талдау жүргізуге мүмкіндік береді.

Instagram платформасының динамикалық контент жүктеу тетігін қолдануы стандартты парсингті айтарлықтай күрделендіреді. Selenium бұл кедергіні пайдаланушы әрекеттерінің имитациясы арқылы еңсереді, мұнда бетті айналдыру және элементтермен өзара әрекеттесу сияқты үрдістер іске асырылады.

1. Selenium жұмысының негізгі алгоритмі келесі кезеңдерден тұрады:
2. Instagram жүйесіне авторизациялау.
3. Нысаналы веб-параққа өту.
4. Беттің HTML-кодын алу.
5. Мәтіндік ақпаратты шығару.

Selenium кітапханасын пайдалана отырып, веб-скрапингті жүзеге асырудан үзінді («ZTB.KZ» Желілік басылымы мысалында):

```
driver = webdriver.Chrome()
driver.get("http://www.instagram.com")

username = WebDriverWait(driver, 10).until(EC.element_to_be_clickable((By.CSS_SELECTOR, "input[name='username']")))
password = WebDriverWait(driver, 10).until(EC.element_to_be_clickable((By.CSS_SELECTOR, "input[name='password']")))

#username and password
username.clear()
username.send_keys("username")
password.clear()
password.send_keys("password")

button = WebDriverWait(driver, 2).until(EC.element_to_be_clickable((By.CSS_SELECTOR, "button[type='submit']"))).click()

not_now = WebDriverWait(driver, 10).until(EC.element_to_be_clickable((By.XPATH, '//button[contains(text(), "Сохранить данные")]'))).click()

driver.get("https://www.instagram.com/ztb_kz/")
time.sleep(5)
```

Сурет 1. Selenium көмегімен Instagram-ға автоматтандырылған кіру



Сурет 2. ztb_kz инстаграм профиліне өту

```
# Добавляем данные в список
data.append([index + 1, timestamp, likes, post_text, top_comments_str])
print(f"Пост {index+1}: {post_text[:50]}...")

except Exception as e:
    print(f"Ошибка при обработке поста {index+1}: ", e)

# Сохраняем данные в CSV
df = pd.DataFrame(data, columns=["№", "Время", "Количество лайков", "Текст поста", "Наиболее избранные комментарии"])
df.to_csv("111instagram_posts_with_comments.csv", index=False, encoding="utf-8")

print("Данные сохранены в 111instagram_posts_with_comments.csv!")

driver.quit()
```

Сурет 3. Pandas көмегімен Instagram-дан CSV-ге деректерді экспорттау

етеді. Жалған жаңалықтарды анықтау да күрделі міндет болып табылады, себебі мәтіндерде көбінесе сарказм, манипуляциялық әдістер және эмоционалды реңк қолданылады, бұл автоматты жіктеуді қиындатады.

Зерттеу нәтижелері веб-скрапинг деректер жинаудың тиімді құралы екенін, ал NLP әдістері жаңалықтарды талдау және жалған ақпаратты анықтау үшін қолданылатынын көрсетті. Осы тәсілдерді біріктіру әлеуметтік желілердегі контентті бақылау және талдау бойынша автоматтандырылған жүйе құруға мүмкіндік береді. Болашақ зерттеулер жетілдірілген деректер талдау модулін әзірлеуге, неғұрлым қуатты тілдік модельдерді пайдалануға және жаңалықтарды жіктеу дәлдігін арттыру үшін машиналық оқыту әдістерін интеграциялауға бағытталатын болады.

Қолданылған әдебиеттер тізімі:

6. Vijayaragavan P., et al. "Web Scraping using Natural Language Processing: Exploiting Unstructured Text for Data Extraction and Analysis". Procedia Computer Science, 2024.
7. Ayisha Nidha P P., et al. "Fake News Detection Using Machine Learning and Web scraping". IRJET, 2024.
8. Shaik, M. A., Ganesh, T., Sree, M. Y., Sushmitha, D., Vyshnavi, S. S., & Shreya, N. Fake News Detection using NLP. IEEE International Conference on Innovative Data Communication Technologies and Application (ICIDCA-2023), 2023.

УДК 004.9

Пирматов А.З.(ОшГУ)
Каденова З.А. (ИМ НАН КР)

РАЗРАБОТКА TELEGRAM BOT САМОСТОЯТЕЛЬНОГО ТЕСТИРОВАНИЯ ПОЛЬЗОВАТЕЛЯ ПО СРЕДСТВАМ ЯЗЫКА PYTHON

В условиях роста цифрализации важность реализации чат-ботов возрастает. Они могут предложить пользователям доступные инструменты для решения различных проблем. Достижения в области искусственного интеллекта предоставляют новые инструменты цифровой помощи. Во многих работах, в том числе в [1]-[3] исследованы разные эффективные методы, получены результаты для интеграции технологий искусственного интеллекта и машинного обучения для повышения качества взаимодействий.

Целью работы является изучение процесса разработки чат-бота, что позволит улучшить доступ к информации и повысить качество услуг. Основным методом исследования является анализ существующих веб-сервисов и их систем, а также разработка прототипа на основе технологий, доступных в среде Telegram, с использованием языка программирования Python. В результате проведенного анализа и разработки был создан прототип чат-бота, который может обеспечивать взаимодействие пользователей с системой, собирая данные о их потребностях и предлагая соответствующие тесты и рекомендации. Практическое применение результатов включает внедрение разработанного чат-бота на платформу Telegram, который будет служить пользователям в качестве онлайн помощника.

Для разработки чат-бота самостоятельной помощи в социальных сетях и его применение в диагностике различных состояний потребителей, необходимо решить несколько задач.

Во-первых, провести анализ существующих веб-сервисов и чат-ботов, сравнив их функциональность и эффективность, а также определить лучшие практики и недостатки аналогичных инструментов, таких как Woebot, Wysa и Fingerprint for Success.

Во-вторых, необходимо определить программные средства разработки, изучив и выбрав подходящие языки программирования и фреймворки (например, Python и Aioogram), а также интегрированные среды разработки для создания Telegram-бота.

В-третьих, следует разработать концепцию и содержание бота, спроектировав пользовательский интерфейс и сценарий взаимодействия, а также разработать алгоритмы тестирования и необходимый контент для самостоятельной помощи пользователям. В-четвертых, потребуется создать и протестировать прототип чат-бота на платформе Telegram, используя выбранные языки программирования и библиотеки, а также провести тестирование его функциональности, выявив и устранив технические неполадки. Оценить практическую значимость разработанного чат-бота, исследовав его влияние на пользователей и определив возможности для продвижения услуг практикующих психологов и других специалистов через платформу. В результате в ходе исследования будет создан уникальный инструмент, который улучшит доступ к помощи в области психического здоровья и повысит вовлеченность пользователей через социальные сети. Теоретическая значимость заключается в расширении знаний о технологиях чат-ботов и их потенциале.

Список использованных источников

1. Rani, A., et al. (2022). *Analyzing the Impact of Chatbots on Mental Health Applications*. *Journal of Medical Systems*, 46(7), 1-10.
2. Singhal, A. (2020). *Chatbot: A Guide to Artificial Intelligence Development*. Springer.
3. Verma, Y., & Putti, K. (2022). *User Experience Design for Healthcare Chatbots: A Review of Best Practices*. *Health Informatics Journal*, 28(2), 146-158.

УДК 004.387

Рсымбетов К.С. (Астана, ЕНУ имени Л.Н. Гумилева)
Бейсебай П.Б. (Астана, ЕНУ имени Л.Н. Гумилева)
Даулетхан А. (Астана, ApStreamLLP)

ЭФФЕКТЫ ВНЕДРЕНИЯ ERP СИСТЕМЫ ODOO В ПРОИЗВОДСТВЕ ОРГАНИЧЕСКИХ ПРОДУКТОВ

Производство органических или экологический чистых продуктов имеют свои специфику и особенности: строгие стандарты сертификации, контроль качества, ограниченные сроки хранения, сезонность и необходимость идентификации цепочки поставок.

Основные отличия органического производства от традиционного заключаются в:

- экологичный продукт.
- прозрачность: полная прослеживаемость и строгая сертификация.
- затраты: более высокие затраты на производство и контроль.

- рынке: ориентация на нишу потребителей, ценящих натуральность и устойчивость. Эти особенности требуют от производителей органической продукции не только адаптации процессов, но и использования специализированных инструментов управления, таких как ERP-системы с возможностью прослеживаемости и соблюдения стандартов.

В мире существуют множество информационных систем для автоматизации производственных предприятий, но ERP-системы типа Oracle, SAP и т.д. более эффективно охватывают специфику органического производства, особенно оперативный контроль производства, логистики и качество продукции.

Приведем несколько конкретных примеров эффективности ERP-системы в производстве органической продукции. Поскольку конкретные кейсы могут быть обусловлены имеющимися данными и специальными компаниями, приведем обобщенные примеры на основе типичных явлений и возможностей ERP-систем, таких как Odoo, SAP, Oracle NetSuite и других, которые часто используются в этой области.

Пример 1: Малое предприятие по производству соков (Odoo ERP)

Небольшой производитель соков в Казахстане. Компания столкнулась с проблемами ручного учета запасов, отсутствием прозрачности в цепочке поставок и сложностями сертификации органической продукции.

Внедрив систему Odoo Community с модулями для управления складом, производством и сертификацией. Получили следующие результаты:

- Автоматизация производства сырья (органические фрукты) сократила потери на 15% за счет точного определения сроков годности.
- Интеграция с поставщиками через Odoo позволяет мгновенно контролировать соблюдение требований органического производства (например, EU Organic).
- Ускорение подготовки отчетов для сертификационных органов на 40%, что снизило затраты на аудит.

Источники эффекта: низкая стоимость оборудования (открытый код), гибкость модулей и простота адаптации под малый бизнес.

Пример 2: Средняя производительность органической молочной продукции (Oracle NetSuite)

Компания производитель органического молока и сыров в Казахстане. Рост продаж продукции привел к хаосу в управлении запасами, производственной графикой и отслеживанием участников в соответствии с требованиями государственных органов Министерства сельского хозяйства Казахстана по органическим продуктам.

Внедрение Oracle NetSuite с акцентом на модулях управления цепочкой поставок, производства и финансов, выровняло ситуацию.

Автоматизация процессов полной прослеживаемости партий от ферм до прилавков, которая дала обеспечение 100% соответствие требованиям органической сертификации. А именно:

- Сокращение времени планирования производства на 30% благодаря автоматизации расписаний и прогнозированию будущего.
- Увеличение продаж на 25% за счет представителей с интернет-магазином через NetSuite.

Основные ключевые моменты успеха: Облачная платформа обеспечивает быстрое масштабирование системы, а встроенная аналитика помогает оптимизировать процессы.

Пример 3: Крупный производитель зерновых и круп (SAP S/4HANA)

Казахстанская компания крупный агрохолдинг, специализирующийся на производстве зерновых культур. Компания работала с разрозненными цепями, что затрудняло управление глобальными поставками, сертификацией и логистикой.

Нашли решение, внедряя SAP S/4HANA с модулями для управления производством, логистикой и соответствием нормативным требованиям.

Получили следующие результаты:

- Единая база данных допускает ошибку в учете на 20% и соблюдает меры по координации между фермами, перерабатывающими заводами и дистрибьюторами.
- Автоматизация соблюдения стандартов (например, органических требований ЕС и США) сокращение времени на оформление документов на 50%.
- Оптимизация логистики привела к снижению транспортных расходов на 10%.

Мощная аналитика SAP и поддержка адаптации идеально подошли для простых цепочек поставок.

Пример 4: Производитель мясной продукции (Microsoft Dynamics 365)

Компания производящий мясную продукцию столкнулась с ситуацией необходимостью управления производством, продажами и маркетингом для выхода на международный рынок.

Нашли решение, внедряя Microsoft Dynamics 365 с фокусом на CRM, управлении производством и цепочке поставок. И получили результаты:

- Автоматизация рецептур и контроль качества сократили время разработки новых продуктов на 35%.
- Интеграция с CRM увеличивает повторные покупки на 20% за счет персонализированных предложений.
- Полный контроль над поставками сырья (например, ингредиентов) в соответствии со стандартами COSMOS и Ecocert.

Успешность связана с гибкостью Dynamics 365 и интеграция с Microsoft Power BI для аналитики помогли быстро адаптироваться к новым рынкам.

Odoo имеет преимущество по сравнению с другими ERP-системами (например, SAP, Oracle NetSuite, Microsoft Dynamics 365, 1C) при использовании в производстве определенных продуктов. Эти преимущества определяют его модульную структуру, открытый исходный код, гибкость и экономичность. Ниже приведен анализ, как Odoo выделяется в двадцати спецификациях органического производства. Если конкретно:

- Модульная архитектура позволяет настроить систему под конкретные нужды органического производства, добавляя только необходимые функции (например, управление складом, производство, CRM, сертификация).
- Доступно более 16 000 модулей из сообщества, включая особенности для органики (например, отслеживание сертификатов или экологических стандартов).
- Бесплатная Community-версия позволяет малым и предприятиям внедрить ERP без значительных начальных затрат, что особенно важно для органического производства с высокой себестоимостью.
- Возможность самостоятельной доработки в соответствии с особыми требованиями (например, добавление модуля для учета оборота или удобрий).
- Интуитивный интерфейс и относительно низкий порог входа для пользователей, что требует базового обучения персонала.
- Быстрое развертывание (особенно в облаке) по сравнению с громоздкими цепями, такими как SAP.
- Встроенные функции идентификации участников и серийного учета в модулях инвентаризации и производства идеально подходят для контроля происхождения органического сырья.
- Легкость проведения с последующей сертификацией через API или кастомные модули.

- Низкая стоимость владения: Community-версия бесплатна, Enterprise-версия (от \$10 для Казахских пользователей/ месяца) дешевле.
- Нет необходимости в дорогах консультантов для настройки, как в случае с SAP или Oracle.
- Интеграция с модулем электронной коммерции для продвижения органической продукции непосредственно потребителям.
- Разработчики активного сообщества предоставляют бесплатные модули и поддержку, решения для органики местных стандартов (например, в ЕС, США, Индии).

Выводы: Экономические эффекты получены на основе таких научно обоснованных методов:

- Управление проектами и задачами (методика Agile, Kanban, GTD).
- Бережливое производство (Lean Manufacturing).
- Управление запасами (ABC-анализ, EOQ, FIFO/LIFO).
- CRM и управление продажами (SPIN, воронка продаж).
- Финансовый менеджмент (ДДС, ROI, KPI).
- Автоматизация и AI/ML и прогнозная аналитика (Machine Learning для прогноза продаж).

Список использованных источников

1. A. Kumar, R. Sharma. Comparative Analysis of Open-Source ERP Systems: Odoo, ERPNext, and Dolibar // International Journal of Enterprise Information Systems (IJEIS), 2022, DOI:10.4018/IJEIS.20220701
2. M. Fernández, J. López. Implementation of Odoo ERP in Small and Medium Enterprises (SMEs): A Case Study // Journal of Business and Technology, 2021, DOI:10.1016/j.jbus.2021.100123
3. S. Patel, D. Nguyen. Customization and Extensibility in Odoo: A Developer's Perspective// IEEE International Conference on Software Engineering (ICSE), 2020, IEEE Xplore
4. L. Zhang, H. Wang. The Impact of Odoo ERP on Business Process Automation: An Empirical Study" // Journal of Computers in Industry, 2019, DOI:10.1016/j.compind.2019.103456
5. K. Ivanov, P. Petrov. Security Analysis of Odoo ERP: Vulnerabilities and Best Practices // Journal of Information Security and Applications, 2023, DOI:10.1016/j.jisa.2023.103789

ГРНТИ 20.19.29

Сарымов Нурсултан (ЕНУ им.
Л.Н.Гумилева)

РАСПОЗНАВАНИЕ РЕЧИ И ПРЕОБРАЗОВАНИЕ ЕЁ В ТЕКСТ С ПРИМЕНЕНИЕМ ГЛУБОКОГО ОБУЧЕНИЯ НА МОБИЛЬНОМ УСТРОЙСТВЕ

Аннотация

В данной статье рассматриваются современные подходы к распознаванию речи и преобразованию речи в текст с помощью глубокого обучения в мобильных приложениях. С ростом спроса на инновационные мобильные технологии распознавание речи становится важным инструментом для улучшения пользовательского опыта и создания интуитивно понятных интерфейсов. Рассматриваются ключевые технологии, такие как искусственный

интеллект (ИИ), нейронные сети и методы глубокого обучения, используемые для повышения точности и скорости обработки речи в мобильных устройствах. Особое внимание уделяется требованиям к производительности мобильных приложений, безопасности данных и оптимизации алгоритмов для работы на устройствах с ограниченными ресурсами. Проанализированы существующие решения и представлены рекомендации по созданию эффективных систем распознавания речи для мобильных приложений.

Ключевые слова: искусственный интеллект, машинное обучение, алгоритм, электронное лицо, робот, цифровое право, цифровые отношения, право и информационные технологии

Введение.

Развитие технологий искусственного интеллекта и глубокого обучения значительно расширило возможности распознавания речи в мобильных приложениях. Эти системы позволяют пользователям взаимодействовать с приложениями с помощью речи, делая взаимодействие более естественным и удобным. В данной статье рассматриваются существующие технологии разработки мобильных приложений с использованием распознавания речи и их влияние на улучшение взаимодействия между устройством и пользователем.

Основная часть

Как проводится обучение прежде всего, имели место кратковременные эффекты адаптации: увеличение акустического сходства с предыдущим стимулом приводило к уменьшению гемодинамической активности в средне-задней STS и правых вентролатеральных префронтальных зонах. Далее, наблюдались и долгосрочные эффекты: ослабление реакции выявлено в орбитальной/островковой коре для стимулов, которые были либо наиболее, либо наименее схожи с акустическим средним всех предшествующих стимулов, а также в переднем височном полюсе, глубокой задней STS и миндалине для стимулов, имеющих наибольшее или наименьшее сходство с усреднённым обученным значением категории голосовой идентичности[1].

Основные требования к системам распознавания речи

Для успешной реализации технологии распознавания речи на мобильных устройствах важно учитывать несколько ключевых факторов:

1. Точность распознавания: мобильные приложения должны обеспечивать высокую точность преобразования речи в текст, особенно в шумной обстановке или при использовании различных акцентов.
2. Производительность и оптимизация: алгоритмы глубокого обучения, такие как конволюционные нейронные сети и рекуррентные нейронные сети, должны быть адаптированы для работы на устройствах с ограниченными ресурсами памяти и процессора.
3. Безопасность данных: поскольку распознавание речи часто связано с обработкой персональных данных, шифрование и защита передаваемой информации - важный аспект разработки мобильных приложений.

Методы исследования.

Современные системы распознавания речи часто используют гибридный подход, сочетая локальную обработку с облачными вычислениями, чтобы сбалансировать производительность и качество. Например, модель Wav2Vec 2.0, разработанная Facebook AI, может эффективно работать на мобильных устройствах за счет использования трансформаторов и предварительного обучения. Для разработки подобных приложений используются такие языки программирования, как Python с библиотеками глубокого обучения (TensorFlow, PyTorch), а также Flutter. Используются мобильные фреймворки с кроссплатформенной поддержкой.

Возможности распознавания речи

Мобильные приложения с функцией распознавания речи позволяют пользователям выполнять широкий спектр задач, таких как ввод устного текста, управление приложениями и взаимодействие с виртуальными помощниками. Эти системы также могут быть интегрированы с другими технологиями, такими как Обработка естественного языка (NLP) и машинное обучение, для улучшения обработки естественного языка и контекстного понимания речи.

Речь — это вокализованная форма человеческого взаимодействия. На этом этапе речь говорящего принимается в форме звуковой волны. Существует множество программного обеспечения, которое используется для записи человеческой речи. Акустическая среда и оборудование для преобразования могут сильно повлиять на создаваемую речь. Вместе с речевым сигналом могут присутствовать фоновые шумы или реверберация в помещении, что является совершенно нежелательным [2].

Взаимодействие между клиентами, фронт-эндом, бэк-эндом и хранилищем данных.

1. клиент- это пользователь, который использует приложение для ввода голосовых команд.

2. Фронтенд - отвечает за запись голоса и отправку данных на сервер через API.

3. Бэкэнд обрабатывает речевые данные, применяет модель глубокого обучения для преобразования речи в текст и возвращает результаты на фронтэнд.

4. Хранилище данных- это база данных, в которой хранятся модели и данные, необходимые для обучения и совершенствования системы распознавания речи.

Таким образом, эффективное взаимодействие между всеми компонентами системы является ключевым фактором успешной реализации распознавания речи в мобильных приложениях.

Клиент будет отправлять запрос на Фронтенд часть в нашем случае это Смартфон, Смартфон передает на API какую либо аудиозапись, данная запись после обработки будет сохраняться на сервере, потом сервер готовые данные будет отправлять на Фронтенд

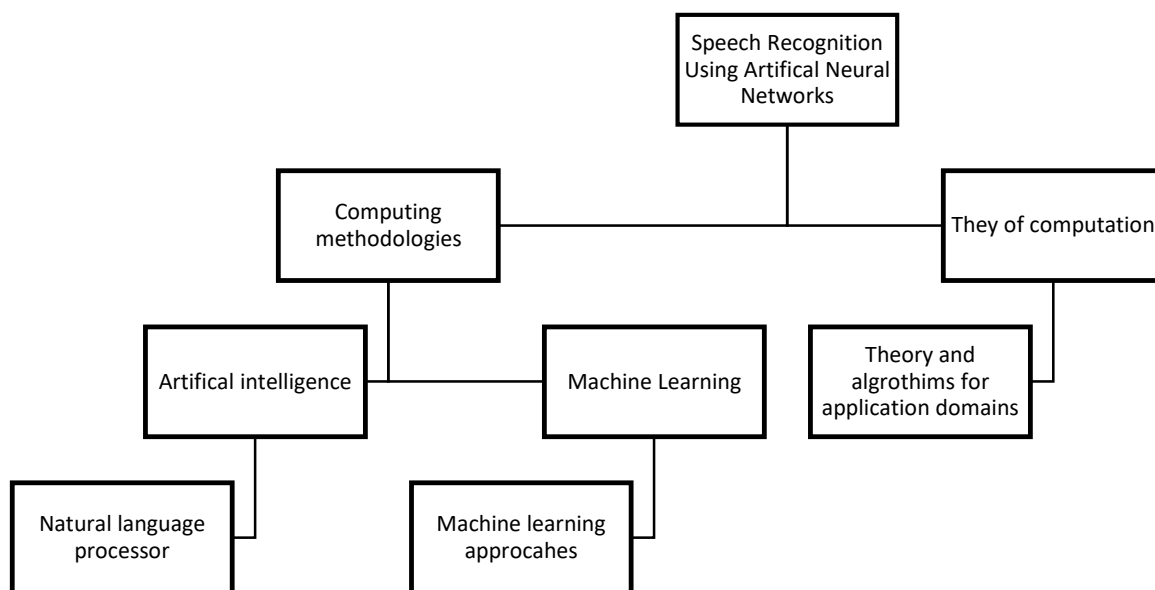


Диаграмма 1

Данная диаграмма была взята из литературы[3]. Эта диаграмма отображает иерархию концепций, связанных с распознаванием речи с использованием искусственных нейронных

сетей. Она разделена на два основных направления: вычислительные методологии и теорию вычислений, каждая из которых подразделяется на более узкие области

Потенциал нейронных сетей

Нейронные сети для распознавания речи исследуются в рамках недавнего возрождения интереса к этой области. Исследования сосредоточены на оценке новых алгоритмов классификации образов и обучения нейронных сетей с использованием реальных данных о речи, а также на определении того, могут ли быть разработаны параллельные архитектуры нейронных сетей, которые выполняют вычисления, необходимые для важных алгоритмов распознавания речи. Большая часть работы сосредоточена на распознавании изолированных слов [4]

Сопоставление шаблонов с использованием нейронных сетей

Искусственные нейронные сети (ИНС) — это интеллектуальные системы, которые в некоторой степени связаны с упрощённой биологической моделью человеческого мозга. Они состоят из множества простых элементов, называемых нейронами, которые работают параллельно и соединены друг с другом через множители, называемые весами связей. Нейронные сети обучаются путем корректировки значений этих весов связей между элементами сети.

Нейронные сети обладают способностью к самообучению, устойчивы к ошибкам и помехам, и находят применение в идентификации систем, распознавании образов, классификации, распознавании речи, обработке изображений и других областях.

Нейронные сети с обратным распространением ошибки были использованы для идентификации видов птиц с помощью записей птичьего пения [5].

В нашем приложении ИНС используется для сопоставления шаблонов. Для данной задачи были сравнены различные архитектуры нейронных сетей, чтобы оценить их производительность.

Искусственные нейронные сети (ИНС) были обучены с использованием семи голосовых образцов, записанных в разные моменты времени от четырёх разных говорящих, которые произносили одну и ту же фразу. Во время обучения были заданы такие параметры, как начальная скорость обучения, допустимая ошибка и максимальное количество циклов обучения. Нейронная сеть была построена в среде MATLAB. На первой попытке были получены суммы квадратичной ошибки в зависимости от количества эпох в процессе обучения. Целевая сумма квадратичных ошибок была достигнута всего за 174 эпохи. Вторая попытка показывает различные скорости обучения, использованные во время обучения [6].

Уровень успеха 100% был достигнут при тестировании ИНС на обученных образцах. Однако при использовании необученных образцов уровень успеха составил лишь 66%. Это произошло из-за того, что спектральные плотности мощности (PSD) входных образцов не совпадали с образцами, использованными для обучения. ИНС была протестирована на голосовых образцах людей, которых она не знала, и успешно классифицировала эти образцы как неопознанные голоса.

Глубокое обучение

С 2006 года этот класс машинного обучения получил мощное развитие и был внедрен в сотни исследований с тех пор. Области, в которые включено глубокое обучение, варьируются от обработки информации до искусственного интеллекта. Глубокое обучение можно охарактеризовать как подполе машинного обучения, основанное на алгоритмах, которые учатся на нескольких уровнях для создания модели, представляющей сложные взаимосвязи между данными. Здесь присутствует иерархия признаков, при которой высокоуровневые признаки определяются в терминах более низкоуровневых, и именно поэтому оно называется глубокой архитектурой. Большинство моделей, включенных в этот класс, основаны на представлениях без учителя.

Глубокое обучение представляет собой точку пересечения нейронных сетей, графического моделирования, оптимизации, искусственного интеллекта, распознавания образов, а также обработки сигналов. Причины популярности глубокого обучения можно подытожить следующим образом: оно способствовало значительному увеличению вычислительных возможностей компьютерных чипов, позволило интегрировать огромные объемы обучающих данных и стало основой для недавних достижений в машинном обучении в области обработки информации и сигналов[7].

Результаты исследования

Гибридные модели искусственных нейронных сетей (ANN) и скрытых марковских моделей (НММ) обучались в три этапа[8].

1. Первый этап: была обучена базовая система GMM/НММ (смешанная модель Гаусса и скрытая марковская модель), и использовалась принудительная выравнивание для ассоциации каждого кадра данных с целевым состоянием НММ.

2. Второй этап: на акустических данных (которые могут быть векторами MFCC, логарифмическими фильтровыми банками или адаптированными к говорящему признаками, собранными вместе) была обучена глубокая версионная сеть (DBN). Веса DBN использовались для инициализации нейронной сети, которая затем обучалась предсказывать состояние НММ на основе акустических данных, используя метод обратного распространения ошибки.

3. Третий этап: поскольку система основана на контекстно-зависимых моделях, для дополнительных сведений читателю рекомендуется ознакомиться с исследованиями [9], которые также использовали контекстно-зависимые системы.

Название	Количество часов	CMLLR	WER
Voice Search	6K	Нет	16.0
YouTube	1400	Да	52.3

Таблица 1: Базовые показатели, используемые для исследования

- CMLLR (Constrained Maximum Likelihood Linear Regression): метод, используемый для адаптации моделей к различным условиям записи.

- WER (Word Error Rate): показатель, отражающий процент ошибок в распознавании слов.

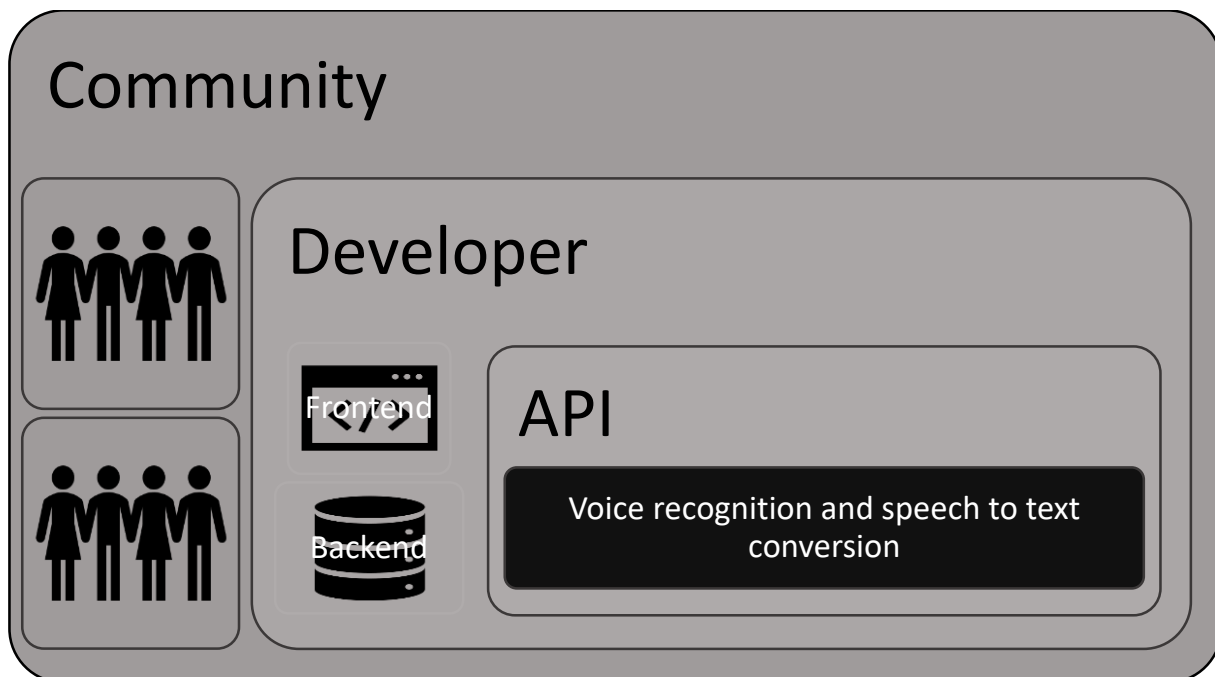


Диаграмма 2

Данная диаграмма показывает зависимости использования разных сервисов, пользователь использует часть разработчика а часть разработчика использует готовую платформу для отправки запроса

Основное положение

Сегодня на рынке существует множество решений для распознавания речи, использующих модели глубокого обучения для обработки речи, включая API от ведущих компаний, таких как Google Speech-to-Text и Apple Siri. Например, модель DeepSpeech компании Mozilla использует рекуррентные нейронные сети (RNN) и демонстрирует высокую точность и производительность на мобильных устройствах. Одной из ключевых проблем при разработке систем распознавания речи является необходимость поиска компромисса между производительностью и точностью обработки, особенно на устройствах с ограниченными вычислительными ресурсами.

Заключение

В современном мире, где технологии развиваются феноменальными темпами, интеграция технологий распознавания речи, преобразования текста в речь и глубокого обучения в мобильные приложения открывает новые горизонты взаимодействия пользователя с устройством. Эти технологии не только повышают доступность информации и упрощают выполнение задач, но и создают возможности для инновационных подходов в обучении и коммуникации

Важно отметить, что успешное внедрение систем распознавания речи требует учета множества факторов, включая точность обработки, производительность на мобильных устройствах и безопасность данных. Применение передовых технологий, таких как нейронные сети и методы глубокого обучения, способствует созданию более эффективных и удобных приложений, способных адаптироваться к потребностям пользователей.

В заключение следует отметить, что дальнейшее развитие и совершенствование технологий распознавания речи не только улучшит пользовательский опыт, но и создаст новые возможности для бизнеса в различных сферах, таких как образование, здравоохранение и обслуживание клиентов. Актуальность и востребованность таких решений в условиях цифровизации общества только возрастает и является предметом активных исследований и разработок.

Список литературы

1. Andics A. et al. Neural mechanisms for voice recognition //Neuroimage. – 2010. – Т. 52. – №. 4. – С. 1528-1540.
2. Kamble B. C. Speech recognition using artificial neural network—a review //Int. J. Comput. Commun. Instrum. Eng
3. Lim C. P. et al. Speech recognition using artificial neural networks //Proceedings of the First International Conference on Web Information Systems Engineering. – IEEE, 2000. – Т. 1. – С. 419-423.
4. Lippmann R. P. Review of neural networks for speech recognition //Neural computation. – 1989. – Т. 1. – №. 1. – С. 1-38.
5. A L Mcilraith, H C Card, “Birdsong Recognition Using Backpropagation and Multivariate Statistics”, IEEE Trans on Signal Processing, vol. 45, no. 11, November 1997
6. Venayagamoorthy G. K., Moonasar V., Sandrasegaran K. Voice recognition using neural networks //Proceedings of the 1998 South African Symposium on Communications and Signal Processing-COMSIG'98 (Cat. No. 98EX214). – IEEE, 1998. – С. 29-32.
7. Y. Cho and L. K. Saul, “Kernel methods for deep learning,” in Proc. Adv. Neural Inf. Process. Syst. (NIPS), vol. 22, 2009, pp. 342–350.

8. Chan W. et al. Listen, attend and spell: A neural network for large vocabulary conversational speech recognition //2016 IEEE international conference on acoustics, speech and signal processing (ICASSP). – IEEE, 2016. – С. 4960-4964.
9. Jaitly N. et al. Application of Pretrained Deep Neural Networks to Large Vocabulary Speech Recognition //Interspeech. – 2012. – Т. 2012. – С. 2578-2581.
10. F. Seide, G. Li, and D. Yu, “Conversational Speech Transcription Using Context-Dependent Deep Neural Networks,” in Interspeech, 2011, pp. 437–440.

Сайлау А.Ж. (Алматы, әл-Фараби атындағы Қазақ ұлттық университеті)
Зиятбекова Г.З.* PhD, доцент м.а.
(Алматы, әл-Фараби атындағы
Қазақ ұлттық университеті; АТУ)

ҮЛКЕН ТІЛДІК ҮЛГІЛЕР ҮШІН ҚАЗАҚША МӘТІНДЕРДІ АЛДЫН АЛА ӨНДЕУ ӘДІСТЕРІН ӨЗІРЛЕУ

Үлкен тілдік үлгілерді (LLM) тиімді үйрету процесінде деректер сапасы мен оларды іріктеу әдістері маңызды рөл атқарады. Бұл зерттеуде instruction tuning сапасын арттыру мақсатында Self-Instruct және LESS (Low-rank gradiEnt Similarity Search) әдістерін қолдану қарастырылады. Self-Instruct әдісі модельдерге өздігінен тапсырмалар құруға және орындауға мүмкіндік берсе, LESS әдісі ең ықпалды деректерді іріктеу арқылы модельдің өнімділігін жақсартуға бағытталған. Автоматтандырылған деректер генерациясы мен тиімді сүзгілеу әдістері ауқымды деректер жиынтығына тәуелділікті азайтып, үлгілерді оңтайлы үйретуге мүмкіндік беретіні көрсетіледі [1].

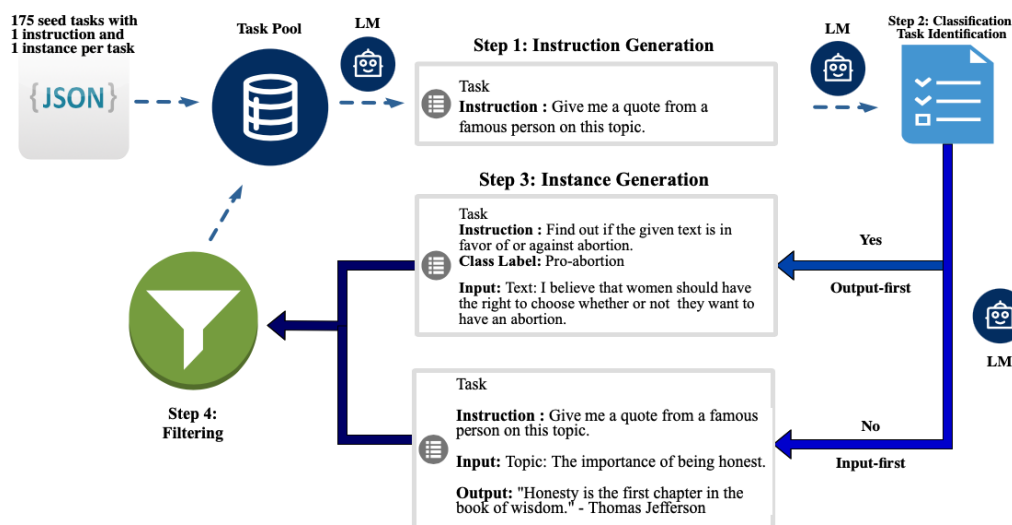
Үлкен тілдік үлгілер (LLM) табиғи тілдерді өңдеу (NLP) саласында кеңінен қолданылады. Олардың тиімділігі көбінесе оқыту деректерінің сапасына байланысты. Дәстүрлі тәсілдерде деректерді қолмен жинау мен аннотациялау әдістері қолданылғанымен, бұл процесс көп уақыт пен ресурсты қажет етеді. Осы мәселені шешу үшін Self-Instruct және LESS әдістері ұсынылған [2].

Self-Instruct әдісі модельдерге адам жазған сұрақтарға сүйене отырып, жаңа тапсырмалар мен жауаптар құруға мүмкіндік береді. Бұл тәсіл адамдық араласуды азайтып, модельдің instruction tuning қабілетін жақсартады. Ал LESS әдісі instruction tuning кезінде ең маңызды деректерді таңдау арқылы модельдің тиімділігін арттыруға бағытталған. Бұл әдіс градиент ұқсастығы негізінде маңыздылығы төмен тапсырмаларды алып тастап, тек қажетті тапсырмаларды қалдыруға көмектеседі [3].

Self-Instruct әдісінің негіздері және қолданылуы

Self-Instruct әдісі үлкен тілдік үлгілерді адамның жазған тапсырмаларына тәуелділікті азайта отырып жетілдіру үшін қолданылады. Бұл әдісте бастапқыда алдын ала дайындалған тапсырмалар жиынтығы беріледі. Модель осы мысалдар негізінде жаңа тапсырмалар мен жауаптарды генерациялайды. Генерацияланған тапсырмалар сапа бақылауынан өткізіліп, сәйкес келмейтін немесе мағынасыз элементтер алынып тасталады. Содан кейін модель тек жоғары сапалы деректер арқылы қайта оқытылады, бұл оның instruction-following қабілетін жақсартады [1].

Зерттеулер көрсеткендей, 1-суретте GPT-3 үлгісіне Self-Instruct әдісін қолдану оның тапсырмаларды орындау қабілетін 33%-ға жақсартып, 52000 жаңа тапсырма және 82000 жауап генерацияланған [1].



1-сурет. LLM үлкен тілдік үлгілерді тиімді үйрету процесі

LESS әдісінің рөлі және артықшылықтары

LESS әдісі instruction tuning процесінде тек ең мағыналы деректерді таңдауға бағытталған. Бұл әдіс төмен дәрежелі градиент ұқсастығы негізінде жұмыс істейді, яғни ол маңыздылығы төмен тапсырмаларды алып тастап, тек тиімді тапсырмаларды қалдырады. LESS әдісі арқылы тек 5% деректерді пайдаланып, толық деректер жиынтығын қолданған жағдаймен салыстырмалы нәтижелер алуға болады [3].

Бұл тәсіл әсіресе қазақ тілі сияқты ресурстары шектеулі тілдер үшін маңызды, себебі қолжетімді деректер көлемі аз болған жағдайда, ең сапалы тапсырмаларды таңдау үлгінің тиімділігін арттыруға мүмкіндік береді.

Деректерді өңдеу және сапасын бағалау

Қазақ тіліндегі LLM-дер үшін instruction tuning процесін жақсарту мақсатында деректерді сапалы іріктеу әдістері ұсынылады. Осыған байланысты төмендегі деректер жинау тәсілдері қарастырылады:

1. Қолмен жасалған деректер – жоғары сапалы, әртүрлі және құрылымды тапсырмалар жинау үшін қолданылады [4, 5].
2. Автоматтандырылған генерация – Self-Instruct және Unnatural Instructions әдістері арқылы тапсырмалар жиынтығын генерациялау және өңдеу [5].
3. Гибридті әдістер – қолмен іріктелген және автоматты түрде жасалған деректерді біріктіру арқылы сапаны арттыру.

LIMA зерттеулері көрсеткендей, бар болғаны 1000 жоғары сапалы тапсырма үлгінің тиімділігін айтарлықтай жақсарты алады [2]. Ал LESS әдісі арқылы тек 5% деректерді пайдалану арқылы толық деректер жиынтығына тең нәтиже алуға болады [3].

Қорытынды

Бұл зерттеу қазақ тіліндегі LLM-дер үшін instruction tuning тиімділігін арттыру мақсатында Self-Instruct және LESS әдістерін қолданудың маңыздылығын көрсетеді. Self-Instruct әдісі модельдерге өздігінен тапсырма құруға мүмкіндік беріп, instruction-following қабілетін жетілдіреді, ал LESS әдісі ең ықпалды деректерді іріктеу арқылы деректер көлемін оңтайландырады.

Пайдаланылған әдебиеттер

- [1] Y. Wang, Y. Kordi, S. Mishra, et al., “SELF-INSTRUCT: Aligning Language Models with Self-Generated Instructions,” *ACL 2023*, 2023. Available: <https://arxiv.org/abs/2212.10560>.
- [2] C. Zhou, P. Liu, P. Xu, et al., “LIMA: Less Is More for Alignment,” *Meta AI Research*, 2023. Available: <https://arxiv.org/abs/2305.11206>.
- [3] M. Xia, S. Malladi, S. Gururangan, et al., “LESS: Selecting Influential Data for Targeted Instruction Tuning,” *ICML 2024*, 2024. Available: <https://arxiv.org/abs/2402.04333>.
- [4] Y. Wang, S. Mishra, P. Alipoormolabashi, et al., “SUPER-NATURALINSTRUCTIONS: Generalization via Declarative Instructions on 1600+ NLP Tasks,” *Allen Institute for AI*, 2022. Available: <https://arxiv.org/abs/2204.07705>.
- [5] O. Honovich, T. Scialom, O. Levy, T. Schick, “Unnatural Instructions: Tuning Language Models with (Almost) No Human Labor,” *Meta AI*, 2022. Available: <https://arxiv.org/abs/2212.09689>.

УДК 004.9

Сағидолла Д.Р., Ерғали Г. Б., (Астана, Esil University)

АНАЛИЗ И СБОР ДАННЫХ ИЗ СОЦИАЛЬНЫХ СЕТЕЙ: МЕТОДЫ, ИНСТРУМЕНТЫ И ЭТИЧЕСКИЕ АСПЕКТЫ

Аннотация Статья посвящена исследованию современных подходов к сбору и анализу данных из социальных сетей. Рассматриваются основные методы получения информации, инструменты для анализа содержимого и поведения пользователей, а также актуальные вопросы этики и конфиденциальности. Проведен обзор практических решений в области мониторинга социальных медиа, включая применение машинного обучения и визуализации данных. Отмечены перспективные направления дальнейших исследований.

Ключевые слова: социальные сети, сбор данных, анализ поведения, машинное обучение, цифровая этика, OSINT.

Введение

Социальные сети стали важнейшим источником данных о поведении, интересах и взаимодействиях людей. Их анализ используется в маркетинге, политологии, социологии, кибербезопасности и других областях. С ростом объемов данных особую актуальность приобретает автоматизация процессов сбора и интеллектуального анализа информации.

1. Методы сбора данных Сбор данных из социальных сетей может осуществляться с помощью:

API (например, Twitter API, VK API); API (Application Programming Interface) — это официальные программные интерфейсы, предоставляемые платформами для доступа к их сервисам. К типичным примерам относятся Twitter API и VK API.

Web scraping (для платформ с ограниченным API-доступом) Web scraping — это метод программного извлечения информации из HTML-страниц, когда официальный API отсутствует или он недостаточно информативен.

- OSINT-инструментов (например, Maltego, Social-Searcher);
 - Платформ аналитики (Brandwatch, Talkwalker). Эти методы позволяют извлекать посты, комментарии, метаданные, изображения и сетевые графы взаимодействий.
2. Анализ контента и поведения На следующем этапе проводится анализ собранных данных. Наиболее распространенные направления:
 - Текстовая аналитика: анализ тональности, тем, ключевых слов (с применением NLP);
 - Сетевой анализ: выявление влиятельных узлов, кластеризация пользователей;
 - Временной анализ: отслеживание динамики обсуждений и трендов;

- Поведенческая аналитика: определение паттернов активности и вовлеченности. Машинное обучение активно используется для классификации контента, прогнозирования поведения пользователей и выявления аномалий.
- 3. Этические и правовые аспекты Анализ данных социальных сетей сопряжен с важными этическими вопросами. Среди них:
 - Конфиденциальность пользователей;
 - Согласие на обработку персональных данных;
 - Использование полученной информации без искажения контекста. Особое внимание уделяется соблюдению региональных законодательств (например, GDPR, законов РФ о персональных данных).

Практические применения Анализ социальных сетей находит применение в: Маркетинге (определение целевой аудитории, мониторинг репутации); Политических кампаниях (анализ общественного мнения); Киберугрозах (выявление дезинформации, фишинговых кампаний) Криминалистике (анализ сетей связей и цифровых следов).

Заключение Анализ данных из социальных сетей — мощный инструмент, позволяющий получать ценные инсайты о пользователях и их поведении. Современные технологии, включая машинное обучение и визуализацию, расширяют аналитические возможности. Однако развитие этой области должно сопровождаться вниманием к правовым и этическим аспектам. В будущем особое внимание будет уделено разработке прозрачных алгоритмов и соблюдению цифровых прав личности.

Список литературы:

1. Boy, J. D., & Crawford, K. (2019). *Datafied publics: Social media, data systems and the reconfiguration of public life*. *Big Data & Society*, 6(1).
2. Tufekci, Z. (2015). *Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency*. *Colorado Technology Law Journal*, 13(203).
3. Федоров А. А. Анализ информации из социальных сетей: технологии и вызовы // *Информационная безопасность*. — 2021. — № 4. — С. 12–17.
4. Козлов М. Н., Иванова С. Ю. Сбор и обработка больших данных из социальных сетей // *Научно-техническая информация*. — 2020. — № 5. — С. 33–38.
5. Мартынова Т. В. Этика и безопасность в цифровом обществе // *Цифровая культура*. — 2022. — № 2. — С. 45–51.

Серікқызы Е., Жамангарин Д.С.,
«Л.Н.Гумилев атындағы Еуразия ұлттық университеті» КеАҚ
Астана қаласы
serikovna.erkenaz@bk.ru

АЗЫҚ-ТҮЛІКТІ ТАҢУ ЖӘНЕ ОЛАРДЫҢ ТАҒАМДЫҚ ҚҰНДЫЛЫҒЫН ТАЛДАУ ҮШІН КОМПЬЮТЕРЛІК КӨРУ ҮЛГІЛЕРІН ҚОЛДАНУ

Аңдатпа. Бұл мақала суреттердегі тағамды автоматты түрде тануға арналған нейрондық желі моделін әзірлеу және олардың тағамдық құндылығын талдауға арналған. Алдын ала оқытылған InceptionV3 конвульсиялық нейрон желісі, сондай-ақ food101 және ImageNet деректер жиынтығы қолданылады. Transfer Learning әдісін қолдана отырып, модельді оқыту процесі және жүйенің өнім туралы ақпаратты қамтитын мәліметтер

базасымен интеграциясы сипатталған. Ұсынылған тәсілдің тиімділігін көрсететін эксперименттердің нәтижелері келтірілген.

Кілт сөздер: компьютерлік көру, кескінді тану, нейрондық желі модельдері, InceptionV3, Food101, Transfer Learning, тағамдық талдау.

Кіріспе

Компьютерлік көрудің заманауи технологиялары денсаулық сақтау, қауіпсіздік, ауыл шаруашылығы және бөлшек сауда сияқты әртүрлі салаларда кеңінен қолданылып келеді. Перспективалық бағыттардың бірі – азық-түлік кескіндерін автоматты түрде талдау үшін нейрондық желі модельдерін пайдалану. Бұл жіктеу, тамақтануды бақылау және тағамдық құндылықтарды бағалау процестерін едәуір жеңілдетуі мүмкін. Бұл әсіресе дұрыс тамақтануға және диетаны бақылауға деген қызығушылықтың артуына тікелей байланысты.

Қазіргі уақытта жасанды интеллект технологиялары өмірдің барлық салаларына енген кезде, визуалды ақпаратты өңдеуді қажет ететін тапсырмаларды автоматтандыруға мүмкіндік беретін құралдарды әзірлеу маңызды. Азық-түлік суреттерін тану – денсаулық сақтау, тамақтану индустриясы және диетологияда қолдануға болатын негізгі міндеттердің бірі.

Бұл мақалада суреттердегі азық-түлікті автоматты түрде тануға және пайдаланушыға олар туралы, оның ішінде калория мен тағам құндылығы туралы ақпарат беруге қабілетті жүйені құруға бағытталған. Азық-түлікті талдауға қатысты шешімдердің көпшілігі пайдаланушылардың ақпаратты қолмен енгізуін талап етеді. Бұл деректерді алудың ыңғайлылығы мен жеделдігін төмендетеді. Алайда, терең оқыту мен алдын-ала дайындалған нейрондық желілердегі жетістіктердің арқасында тағамдарды кескін бойынша автоматты түрде тану мүмкін болады. Сондай-ақ олардың құрамы талданады. Transfer Learning әдісі арқылы тағамды жіктеу тапсырмасына бейімделген InceptionV3 алдын ала оқытылған моделі қолданылады. Алдын ала оқытылған модельдерді қолдану тәсілі оқу уақытын едәуір қысқартуға және жіктеудің дәлдігін арттыруға мүмкіндік береді.

Әдістеме

Кәдімгі көрудің мақсаты – суретте не бар екенін түсіну. Компьютерлік көру – көру жүйесінің компьютерлік моделін құру, яғни адам жауап бере алатын кескін туралы кез-келген сұраққа жауап бере алатын бағдарлама құру.

Интуитивті түрде «оқыту» дегеніміз-белгілі бір модель қандай-да бір түрде «оқытылған» кезде, содан кейін нәтиже бере бастайды, яғни, мүмкін, бір нәрсені болжай бастайды.[1]

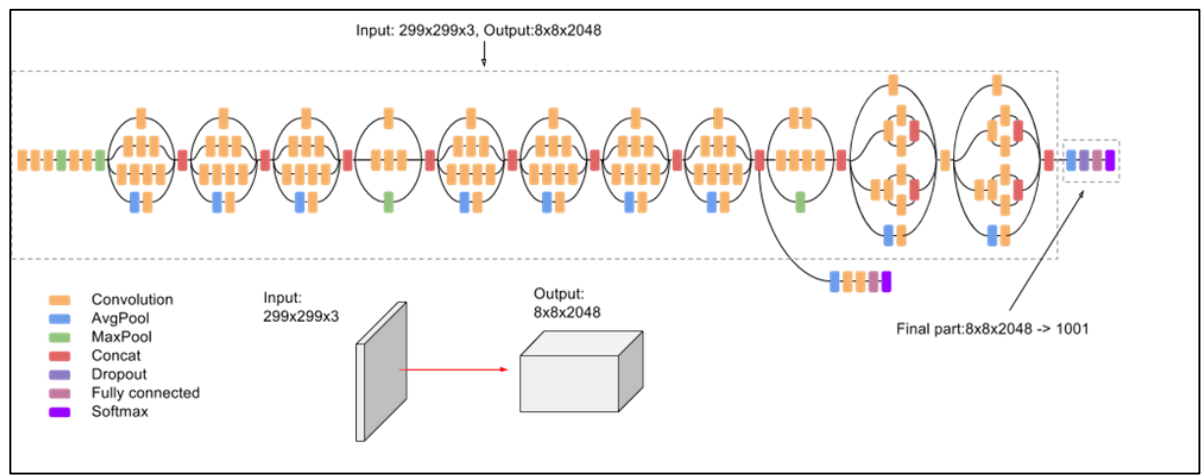
Модельді оқыту және тестілеу үшін Food101 және ImageNet ашық деректер жиынтығы қолданылады. Food101 құрамында 101 санаттағы өнімдердің суреттері бар. Бұл оны тамақтану классификациясының міндеттеріне сәйкес етеді. ImageNet модельді алдын-ала оқыту үшін қолданылады, өйткені ол кескіннің кең базасын қамтиды. Бұл модельге визуалды белгілерді тиімді шығаруға және жалпылауға мүмкіндік береді.

Модельді үлкен көлемде оқыту оның жалпылау қабілетін арттыруға мүмкіндік береді. Бұл өнім кескіндерін жіктеу мәселесін шешу үшін өте маңызды. Сонымен қатар, Food101 белгілі бір тапсырмаға сәйкес келетін деректерді ұсынады, ал ImageNet модельдерге объектілердің жалпы сипаттамаларын жақсы түсінуге көмектесетін визуалды көріністердің кең спектрінің көзі ретінде қолданылады.

Машиналық оқыту – бұл жасанды интеллектті оқытудың маңызды әдіснамасының бір түрі, ол соңғы онжылдықтарда кеңінен таралды. Машиналық оқыту мәліметтерден білім алуға мүмкіндік береді. Трансферттік оқыту машиналық оқытудың маңызды саласы ретінде жаңа қабілеттерді үйренуді жеңілдету үшін алынған білімді пайдалану процесіне бағытталған, бұл тиімділік пен тиімділікті арттырады.[3]

Модель архитектурасы, негізгі архитектура ретінде InceptionV3 таңдалды. InceptionV3 – кескінді жіктеу тапсырмалары үшін оңтайландырылған терең конволюциялық нейрожелі. Бұл күрделі визуалды белгілерді өңдеуге мүмкіндік береді және кең деректер жиынтығында жоғары дәлдікті көрсетеді.

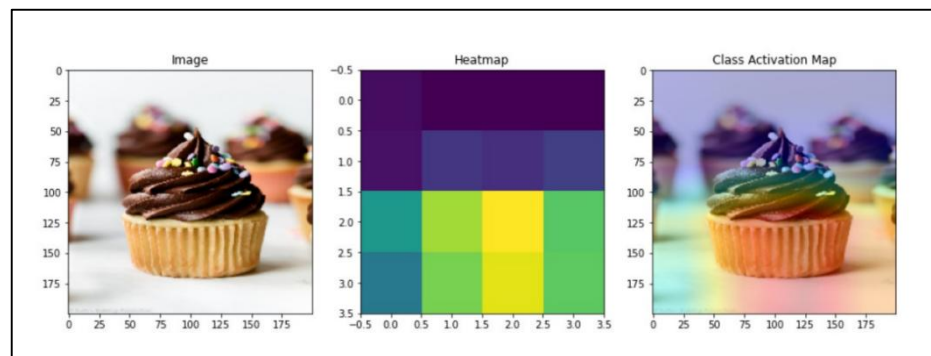
Архитектураға байланысты InceptionV3 моделін оқыту кезінде алдымен оқыту процесі қалай жүретінін толығымен көрсеткен жөн. Бұл модельде жіктеу яғни тағамдарды жіктеу бөлігі жақсы жұмыс жасайды. Жіктеу бөлігінде толығымен қосылған лазер InceptionV3 функциясының шығысын, сондай-ақ реттелетін сегменттелген мүмкіндікті алады [2]. 1-суретте InceptionV3 моделінің архитектурасы көрсетілген.



1-сурет. InceptionV3 моделінің архитектурасы

InceptionV3-тің басты артықшылығы – модельге әртүрлі деңгейдегі кескін белгілерін түсіруге мүмкіндік беретін каскадты конволюциялық қабаттар мен модульдерді пайдалану. Бұл модельді күрделі нысандарды өңдеуде тиімдірек етеді және қайта оқыту мүмкіндігін азайтады.

InceptionV3 алдын ала дайындалған қабаттарын тағамды тану ерекшелігіне бейімдеуге мүмкіндік беретін Transfer Learning әдісін қолдана отырып оқытылады. Эксперименттер деректерді ұлғайтуды (жарықтандыруды өзгерту, бұру, масштабтау), кескіндерді қалыпқа келтіруді және гиперпараметрлерді оңтайландыруды пайдаланады. 2-суретте тағамды тану үлгісі көрсетілген.



2-сурет. Тағамды тану үлгісі

2-суретте тағамды тану үлгісі туралы айтатын болса, кескіннің сол жақ бөлігінде бұл модель болжау үшін қолданылатын кіріс кескіні. Бұл жағдайда шоколадты кремді бар кекстер бейнеленген.

Кескін ортасында тұрған бұл жылу картасы. Жылу картасы модельдің шешім қабылдауы үшін кескіннің қай бөліктері ең маңызды болғанын көрсетеді. Күлгін және қою көк аймақтар маңыздылықтың төмендігін білдіреді.

Сары және жасыл аймақтар жоғары ылғалдылықты білдіреді. Бұл жағдайда модель кескіннің төменгі жағына назар аударады. Ескеретін жайт модель тек креммен ғана емес, кекстің пішініне немесе оның құрылымына да назар аударады.

Деректерді күшейтуді қолдану модельге нақты пайдалану жағдайларына жақсы бейімделуге көмектеседі, өйткені өнім кескіндері әртүрлі жарықтандыруға, бұрышқа және фонға ие болуы мүмкін. Деректерді қалыпқа келтіру, оқу тұрақтылығын арттырады және гиперпараметрлерді мұқият реттеу, жұмыс жылдамдығы мен болжау дәлдігі арасындағы оңтайлы тепе-теңдікке қол жеткізуге мүмкіндік береді.

Нәтижелер

Оқытылған модель валидация үлгісінде сыналды және нәтижелер 85% - дан асатын жоғары жіктеу дәлдігін көрсетті. Көрсеткіштер дәлдік (accuracy), F1-score, recall және precision модель азық-түлік кескіндерін тиімді жіктейтінін көрсетеді. 1-кестеде модельдің сапалық көрсеткіштері көрсетілген.

1-кесте. Модельдің сапалық көрсеткіштері

Өлшемі	Мәні
Дәлдігі	85,2%
Болжам дәлдігі	84,7%
Recall (толықтық)	85%
F1-score	84,8%
Орташа болжам уақыты (секунд)	3,1

Модель тұрақты жұмыс істейді, бірақ деректерді теңестіру арқылы болжамдарды жақсартуға болады яғни дәлдігі және болжамы бойынша 85%-дан асатын көрсеткіш көрсетуге болады.

Модельдің сапасын бағалау үшін әртүрлі сынақ сценарийлері қолданылды, соның ішінде нақты жағдайдағы өнімдердің суреттері (фоны, жарықтандыруы және түсіру бұрышы әртүрлі фотосуреттер). Эксперименттердің нәтижелері модель күрделі визуалды жағдайлар болған кезде де тану тапсырмасын сәтті орындайтынын растады.

Модельді өнімнің тағамдық құндылығы туралы ақпаратты қамтитын мәліметтер базасымен интеграциялау да жүзеге асырылды. Кескінді жіктеу кезінде жүйе өнімнің атауын ғана емес, сонымен қатар оның калория мөлшері, ақуыздар, майлар мен көмірсулар туралы мәліметтерді де шығарады. Бұл оны тамақтануды бақылайтын адамдар үшін пайдалы құрал етеді.

Қорытынды

Бұл мақалада суреттердегі тағамды автоматты түрде тану және олардың тағамдық құндылығын талдау үшін нейрондық желі моделін әзірлеу бойынша зерттеу ұсынылған. Алдын ала дайындалған Inceptionv3 моделін қолдану және Transfer Learning әдісін қолдану жоғары жіктеу дәлдігіне қол жеткізді. Модельді мәліметтер базасымен біріктіру

пайдаланушыға пайдалы тамақ туралы ақпарат бере алатын қосымшалар құруға мүмкіндік береді.

Бұл тәсіл денсаулық сақтау, аспаздық және жеке тамақтану саласындағы шешімдерді әзірлеуге, сондай-ақ адамның диетасын талдауға және тамақтану бойынша ұсыныстар беруге қабілетті интеллектуалды жүйелерді құруға пайдалы болуы мүмкін.

Әдебиеттер тізімі

1. Николенко С. И., Кадуринов А., Архангельская Е. В. (2018). Глубокое обучение. Погружение в мир нейронных сетей (стр. 17–19).
2. Burkapalli V. C., Patil P. C. Transfer learning: Inception-V3 based custom classification approach for food images //ICTACT Journal on Image & Video Processing. – 2020. – Т. 11. – №. 1.
3. Jindong Wang, Yiqiang Chen (2023). Introduction to Transfer Learning. Algorithms and Practice (pp. 5-6).

Сулеймен Б.К. (PhD candidate),
проф. Исаков К.Т., PhD Нартова Д.С.
ЕНУ им. Л.Н. Гумилёва

РАЗРАБОТКА ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА ДЛЯ ИЗМЕРЕНИЯ ТОКА В ОДНОФАЗНОЙ СЕТИ С ПРИМЕНЕНИЕМ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация

Представлена разработка программно-аппаратного комплекса для мониторинга потребления тока в однофазной сети с использованием датчика Холла и аналого-цифрового преобразователя (АЦП). Ключевая особенность решения — регистрация пусковых токов подключаемых электроприборов, что позволяет формировать цифровую сигнатуру каждого устройства. На основе собранных данных применяются методы машинного обучения для решения задач: детектирования подключения, идентификации устройства, оценки потребления энергии, кластеризации и категоризации по уровню энергоэффективности. Разработка ориентирована на применение в системах «умного дома», энергоаудита и интеллектуального управления нагрузкой.

Ключевые слова: #интеллектуальный мониторинг, #датчик Холла, #пусковой ток, #цифровая сигнатура, #машинное обучение, #энергопотребление, #кластеризация, #Arduino.

1. Введение

Современные требования к энергоэффективности и цифровому управлению ресурсами требуют точного мониторинга структуры электрической нагрузки. Традиционные системы учёта фиксируют только общее потребление, не предоставляя информации о типах и характеристиках подключенных приборов. Это создаёт слепую зону при анализе расхода энергии и планировании оптимизаций.

В рамках настоящей работы предлагается решение, позволяющее выявлять и классифицировать устройства в сети на основе анализа пусковых токов. Такой подход открывает возможности для точного учёта, анализа поведения нагрузки и автоматической категоризации потребителей.

2. Методология

2.1 Аппаратная часть

Основу системы составляет микроконтроллер Arduino Nano, соединённый с датчиком Холла, обеспечивающим бесконтактное измерение тока. Частота съёма данных достигает 10 Гц. Все измерения мгновенных значений тока $I(t)$ фиксируются и передаются в цифровую систему анализа. Напряжение сети принимается равным 220 В.

2.2 Математическая модель

Расчёт сопротивления осуществляется по закону Ома:

$$R(t) = \frac{U}{I(t)}$$

При множественной нагрузке сопротивление системы определяется как параллельное соединение:

$$\frac{1}{R_{\text{сумм}}} = \sum_{i=1}^n \frac{1}{R_i}$$

Задача состоит в восстановлении R_i по известному $I(t)$ и U , что делает проблему подходящей для методов машинного обучения.

2.3 Цифровая сигнатура устройства

Каждое включение прибора сопровождается характерным импульсом — пусковым током. Он фиксируется системой и преобразуется в цифровой вектор признаков, включающий амплитуду, форму, длительность и скорость нарастания. Эти сигнатуры сохраняются в базе данных и используются для последующего анализа и распознавания.



Рис 1. Оцифрованные показания замеров работы тестового устройства на включение и выключение. Основа для формирования цифровой сигнатуры.

3. Использование методов искусственного интеллекта

3.1 Предпосылки использования ИИ

Анализ структуры нагрузки затруднён из-за:

- многовариантности комбинаций приборов,

- временной изменчивости сопротивлений,
- отсутствия априорных данных о составе сети.

3.2 Задачи и методы

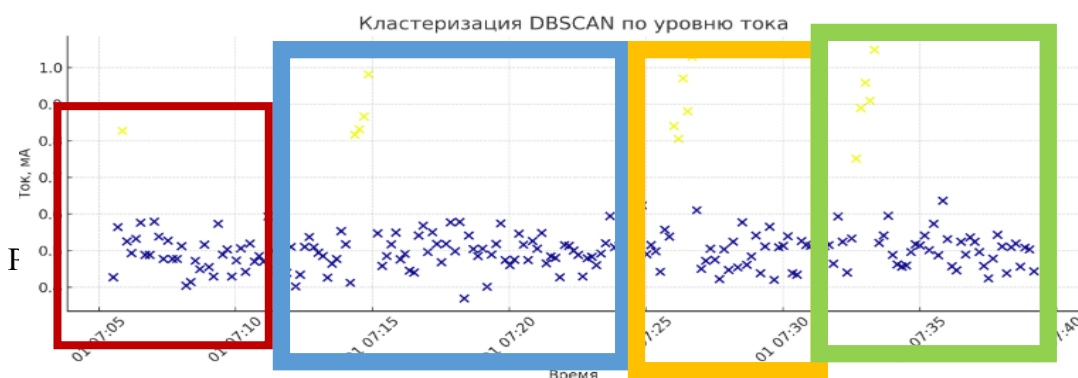
Задача	Метод
Детекция подключения	Бинарная классификация
Идентификация устройства	Мультиклассовая классификация (Random Forest, Gradient Boosting, CNN)
Оценка энергопотребления	Интеграл $E = \int I(t) \cdot U \cdot dt$
Кластеризация	DBSCAN, k-Means
Присвоение класса энергоэффективности	Регрессия, классификаторы по профилю потребления

3.3 Архитектура анализа

1. **Сбор данных:** ток $I(t)$, пусковые импульсы.
2. **Предобработка:** фильтрация шумов, нормализация.
3. **Извлечение признаков:** амплитуда, длительность, RMS, форма.
4. **Обучение моделей:** классификация, регрессия, кластеризация.
5. **Постобработка:** визуализация, отчётность, управление.

4. Результаты и перспективы

Пилотная реализация комплекса успешно зарегистрировала и идентифицировала типовые нагрузки (фен, чайник, зарядное устройство). Точность идентификации на небольшой обучающей выборке составила более 80%.



- интеграция с облачными сервисами для удалённого мониторинга.

Разработка открывает перспективы для коммерческого использования в системах «умного дома», корпоративного учёта, а также в учебных целях.

УДК 004.912

Таберхан Р. (Астана, Л.Н. Гумилев атындағы ЕҰУ)
Самбетбаева М.А. (Астана, Л.Н. Гумилев атындағы ЕҰУ)

LABEL STUDIO-НЫ ПАЙДАЛАНА ОТЫРЫП, СЕБЕП-САЛДАРЛЫҚ ҚҰРЫЛЫМДАРДЫ ҚАЗАҚ ТІЛІНДЕ АННОТАЦИЯЛАУДЫ АВТОМАТТАНДЫРУ

Аңдатпа

Бұл мақалада қазақ тіліндегі мәтіндердегі себеп-салдарлық құрылымдарды (ССҚ) аннотациялауды автоматтандыру процесі қаралады. Label Studio сияқты цифрлық платформаларды пайдалану мәтіндерді белгілеу процесін едәуір жеделдетуге және жеңілдетуге мүмкіндік береді. Бұл қазақ тіліндегі NLP-жүйелер мен лингвистикалық ресурстарды дамыту үшін маңызды болып табылады. Мақалада белгілеу әдістері, ССҚ типологиясы, сондай-ақ шаблондық және машиналық үлгілерді пайдалана отырып, алдын ала автоматтандыру нәтижелері ұсынылған.

Кіріспе

Себеп-салдарлық құрылымдар (ССҚ) мәтін ішіндегі логикалық және семантикалық байланыстарды қалыптастыратын маңызды компоненттердің бірі болып саналады. Олар сөйлемдердің арасындағы байланысты орнатып, себептік пайда болуын түсіндіруге және қорытынды жасауға негіз болады. Қазақ тілінде мұндай құрылымдар арнайы аффикстер, постпозициялық бірліктер мен аналитикалық құралдар арқылы жүзеге асырылады.

Қазақ тіліндегі себеп-салдарлық құрылымдарды қамтитын цифрлық корпус құру — интеллектуалды лингвистикалық жүйелерді дамытудағы маңызды кезеңдердің бірі. Дегенмен, мұндай құрылымдарды қолмен аннотациялау — уақытты көп қажет ететін үлкен еңбек. Осыған байланысты, таңбалау процесін автоматтандыру — қазіргі таңда өзекті міндетке айналып отыр, әсіресе арнайы платформалар мен алгоритмдерді қолдану арқылы бұл жұмысты тиімді ұйымдастыруға мүмкіндік бар.

Зерттеудің өзектілігі

- Қазақ тіліндегі себеп-салдарлық конструкциялармен белгіленген корпусың болмауы
- Қазақ тіліндегі себеп-салдарлық конструкциялар типтерінің айқын бөлінбеуі
- Қазақ тіліне бейімделген көпқабатты белгілеу құралдарының жетіспеуі

Зерттеудің мақсаты

Қазақ тіліндегі ғылыми мәтіндерде кездесетін себеп-салдарлық полипредикативті конструкцияларды құрылымдық және семантикалық тұрғыдан сипаттап, оларды Label Studio платформасы арқылы аннотациялау үшін жүйеленген белгілер мен типологияны әзірлеу.

Бұл жұмыс себеп-салдарлық байланысты автоматты түрде тануға мүмкіндік беретін корпус құруға және болашақта қазақ тіліндегі NLP модельдерін дамытуға негіз болады.

Зерттеудің міндеттері

- Қазақ тіліндегі себеп-салдарлық полипредикативті конструкцияларды жинау және талдау
- Себеп-салдарлық конструкциялардың типологиясын жасау
- Label Studio ортасында аннотациялауға арналған белгілер жүйесін әзірлеу
- Аннотацияланған корпус үлгісін жасау

Әдіснама

ССҚ-ды түсіндіру үшін Label Studio платформасы пайдаланылды.

Төмендегі 1-ші суретте Label Studio платформасында қазақ тіліндегі себеп-салдарлық қатынастарды аннотациялау мысалы көрсетілген. Бұл интерфейс ғылыми журналда

жарияланған мәтіндерден алынған сөйлемдер негізінде себеп (CAUSE), салдар (EFFECT), және олардың арасындағы логикалық байланыстарды (*leads_to*) белгілеу үшін бейімделген.

Мәтін мысалы:

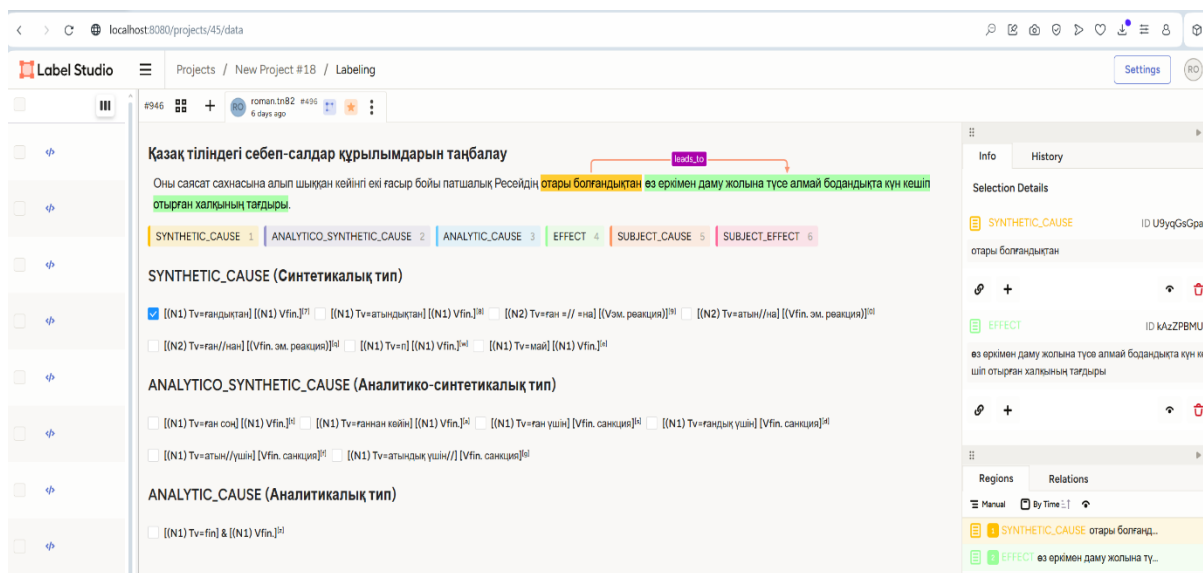
«Оны саясат сахнасына алып шыққан кейінгі екі ғасыр бойы патшалық Ресейдің отары болғандықтан, өз еркімен даму жолына түсе алмай бодандықта күн кешіп отырған халықтың тағдыры.»

Бұл сөйлемде:

– **Себептік компонент** ретінде «отары болғандықтан» бөлектелген және **SYNTHETIC_CAUSE** меткасымен таңбаланған. Бұл құрылым – себепті білдіретін аффиксті (-ғандықтан) қамтитын синтетикалық каузатив.

– **Салдар** ретінде «өз еркімен даму жолына түсе алмай бодандықта күн кешіп отырған халықтың тағдыры» сегменті таңдалған. Бұл **EFFECT** меткасымен белгіленген және себептің салдарын білдіреді.

– Екі компонент арасында **leads_to** типіндегі семантикалық байланыс орнатылған, яғни *себеп* → *салдар* бағыты нақты көрсетілген.



1-ші сурет

Нәтижелер және талқылау

Label Studio бағдарламасын пайдалану таңбаларды құрылымдауға ғана емес, сонымен қатар моделдерді оқыту үшін деректерді дайындауға да мүмкіндік берді. Үлгілер бойынша белгілеу нақты берілген құрылымдар болған кезде жақсы нәтиже көрсетті. Келешекте нейрожелілік моделдерді қосу және корпусты бірнеше бес жүз мысалға дейін кеңейту керек.

Қорытынды

Бұл визуализация Label Studio платформасының қазақ тіліндегі күрделі морфологиялық құрылымдарды тиімді аннотациялауға қолданылады. Сөйлем құрылымы толықтай логико-семантикалық модельге сәйкес келтіріліп, кейінгі NLP модельдерін оқыту үшін жоғары сапалы деректер жиынтығын дайындауға мүмкіндік береді. Мұндай аннотациялар себеп-салдарлық логиканы автоматты түрде танитын жүйелерді дамытуда маңызды қадам болып табылады.

Бұдан кейінгі зерттеулерде трансформерлер негізінде модельдер енгізу және тереңірек семантикалық талдау үшін каузальдық конструкциялар типологиясын кеңейту жоспарлануда.

Қолданылған әдебиеттер тізімі:

1. Жексенбаева Г.Ж. Типология причинных конструкций в казахском языке. – Алматы: Қазақ университеті, 2020.
2. Нарымбетов С.Т. Қазіргі қазақ тілінің құрылымдық жүйесі. – Нұр-Сұлтан, 2018.
3. Open Data Science: Label Studio Documentation. <https://labelstud.io/>
4. Тажимаева С.Ж. Каузальные полипредикативные конструкции казахского языка. Астана, 2015 - 271 с.
5. Jurafsky D., Martin J.H. Speech and Language Processing. – Pearson, 2024. <https://web.stanford.edu/~jurafsky/slp3/ed3book.pdf>

Хусенбай Алина
Л.Н.Гумилев атындағы
ЕҰУ механика-математика факультетінің
математика білім беру бағдарламасының
2-курс магистранты
Ғылыми жетекшісі – Д.А.Реджепович

СТЕРЕОМЕТРИЯ ТАҚЫРЫПТАРЫН GEOGEBRA БАҒДАРЛАМАСЫ АРҚЫЛЫ ОҚИТУДЫҢ ӘДІСТЕМЕЛІК НЕГІЗДЕРІ

Аннотация

Мақалада стереометрия пәнін оқытуда GeoGebra бағдарламасын қолданудың әдістемелік негіздері қарастырылады. Цифрлық технологияларды кеңістіктік геометриямен ықпалдастыра отырып, оқушылардың кеңістіктік ойлау, визуализация және логикалық пайымдау дағдыларын дамыту жолдары ұсынылады. Мақалада сабақ құрылымдары, практикалық тапсырмалар үлгілері мен оқыту тиімділігіне қатысты тәжірибелік деректер берілген.

Түйін сөздер: стереометрия, GeoGebra, визуализация, қималар, 3D модель, цифрлық білім ресурсы, кеңістіктік ойлау.

Кілттік сөздер: бағдарлама, салу есептері, стереометрия, Geo-gebra.

Кіріспе

Стереометрияны оқыту – мектеп геометриясының маңызды, әрі оқушылар үшін жиі қиындық тудыратын бөлімі. Кеңістіктік объектілерді елестету, қималарды түсіну және фигуралар арасындағы өзара орналасу қатынастарын қабылдау оқушылардан жоғары деңгейдегі кеңістіктік ойлауды талап етеді. Осы тұрғыда, қазіргі білім беру жүйесінде визуализацияға негізделген интерактивті бағдарламаларды қолдану кеңістіктік геометрияны меңгерудің тиімді жолы ретінде қарастырылады. GeoGebra бағдарламасы – стереометриялық мазмұнды көрнекі және қолжетімді етіп түсіндіруге мүмкіндік беретін бірегей құрал. Бұл мақалада аталған платформаны сабақта жүйелі түрде қолданудың ғылыми-әдістемелік негіздері сипатталады.

Негізгі бөлім

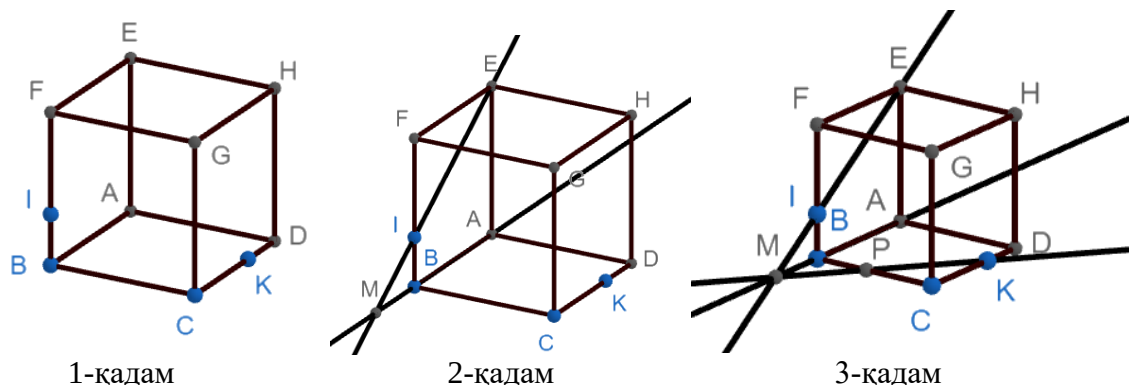
GeoGebra – динамикалық математикаға арналған тегін бағдарлама. 3D калькулятор бөлімі арқылы кеңістіктегі нүктелер, түзулер, жазықтықтар мен денелерді модельдеп, олардың өзара орналасуын, қиылысуын, қималарын көрсетуге болады. Бағдарлама

визуализацияға негізделген зерттеуді жеңілдетеді. GeoGebra — бұл тек визуализация құралы ғана емес, сонымен қатар цифрлық білім беру ортасын толыққанды қолдайтын оқыту платформасы. Бағдарламаның құрылымы мұғалімдер мен оқушыларға интерактивті тапсырмалар жасауға, дайын материалдарды қолдануға және білім берудің сараланған моделін іске асыруға мүмкіндік береді. GeoGebra қосымшасында 3D графикамен қатар, математикалық мәтін енгізу, слайдерлер жасау, анимация жүргізу, айнымалылармен жұмыс істеу сияқты күрделі математикалық модельдерді басқару құралдары біріктірілген. Бағдарламаның қолданушыларына арналған ресурстық орталық (GeoGebra Materials) мұғалімдерге дайын интерактивті сабақтар, тапсырмалар және визуалды модельдер жүктеп, оларды өзгертуге мүмкіндік береді. Сонымен қатар, GeoGebra Classroom функциясы арқылы онлайн сабақ жүргізуге, нақты уақыт режимінде оқушылардың тапсырмаларын бақылауға және жекелеген оқушылармен жұмыс жасауға жол ашады. Бұл оның цифрлық педагогикаға бейімделген, қолданушыға ыңғайлы әрі оқушы мен мұғалімнің өзара әрекетін жандандыратын платформа екенін дәлелдейді. GeoGebra — бұл математиканы оқыту мен үйренуге арналған тегін, ашық кодты бағдарламалық қамтамасыз ету. Бағдарлама алғаш рет 2001 жылы Маркус Хоэнвартер (Markus Hohenwarter) тарапынан әзірленіп, бүгінгі таңда 2D және 3D геометрия, алгебра, анализ, статистика және матрицалар секілді математикалық бағыттарды біріктіретін қуатты платформаға айналды. GeoGebra платформасы Windows, macOS, Linux, Android және iOS жүйелерінде жұмыс істейді және веб-нұсқасы да бар. Бағдарлама арқылы оқушылар математикалық объектілерді өзара байланыста көре алады, графиктер салып, формулаларды динамикалық түрде бақылап, кеңістіктегі модельдермен нақты әрекет жасай алады. GeoGebra-ның басты артықшылықтары — интуитивті интерфейс, тілді таңдау мүмкіндігі, интерактивті визуализация, анимация мен өлшеу құралдары, сондай-ақ білім беру мақсатында қолдануға арналған ашық ресурстар қорының болуы. Бұл бағдарлама әлем бойынша 200-ден астам елде 100 миллионнан астам пайдаланушысы бар жетекші білім беру платформасына айналып отыр. Бағдарлама арқылы стереометрия тақырыптарына мысалдары:

- Кубтың AD, CE, BF қырларынан өтетін жазықтықпен қимасын салу;
- Пирамиданың төбесінен табан жазықтығына перпендикуляр түсіру;
- Цилиндрдің көлбеу қимасы нәтижесінде эллипс шығару.

Мысалы, ABCDFENG дұрыс төртбұрышты призманың бүйір қырларында берілген үш нүкте арқылы өтетін жазықтықпен қиғандағы қиманы салудың бірнеше түрлерімен танысайық:

1 есеп. ABCDFENG дұрыс төртбұрышты призманың BF, CD бүйір қырларынан сәйкесінше I, K нүктелері берілген. I, K, E нүктелері арқылы өтетін жазықтықтың призмамен жасайтын қимасын тап. 1-қадам. Суретте байқағанымыздай, I, E нүктелері бір жазықтықта орналасқан. Олай болса, IE кесіндісін сала аламыз (45-сурет).

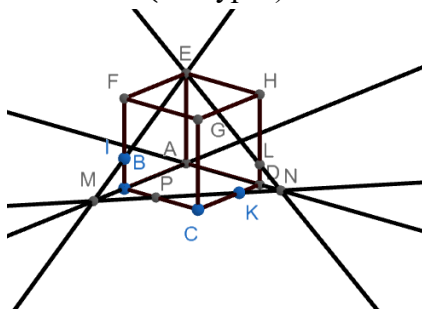


45-сурет

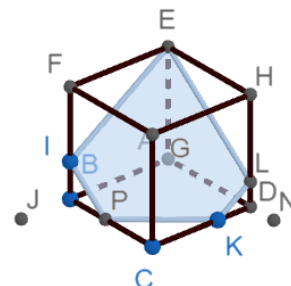
46-сурет

47-сурет

2-қадам. АВ түзуін саламыз. $AB \cap EI = M$ (46-сурет) . 3-қадам. М нүктесі мен К нүктесі бір жазықтықта жатыр, сондықтан МК түзуін аламыз. $MK \cap BC = P$ (47-сурет) . 4-қадам. $MK \cap AD = N$. Сосын NE түзуін жүргіземіз. $NE \cap HD = L$ (48-сурет) . 5-қадам. IPKL ізделінді қиманы аламыз (49-сурет).



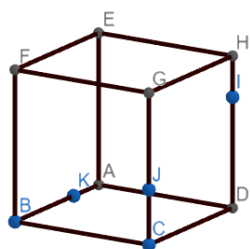
4-қадам
48-сурет



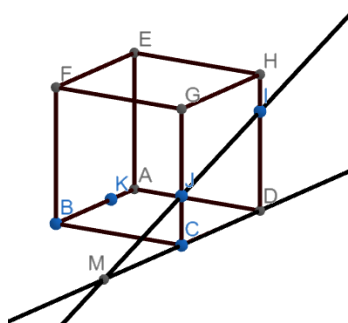
5-қадам
49-сурет

Geo-Gebra бағдарламасына сілтеме: <https://www.geogebra.org/3d/vyx5rzru>

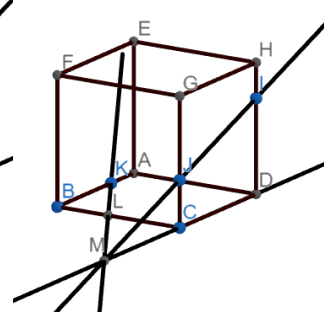
2 есеп. ABCDFENG дұрыс төртбұрышты призманың АВ, CG, DH бүйір қырларынан сәйкесінше К, J, I нүктелері берілген. К, J, I нүктелері арқылы өтетін жазықтықтың призмамен жасайтын қимасын тап (50-сурет).



1-қадам
50-сурет



2-қадам
51-сурет



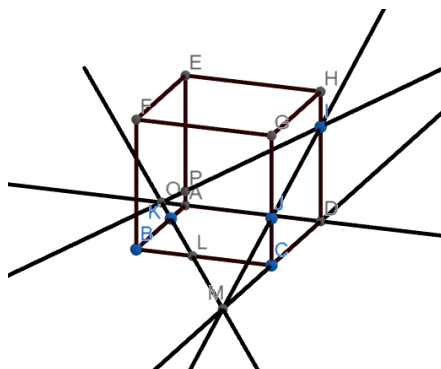
3-қадам
53-сурет

1-қадам. Бір жазықтықта жатқан нүктелерді қосамыз. 1-суреттен байқағанымыздай J және I нүктелері бір жазықтықта жатыр.

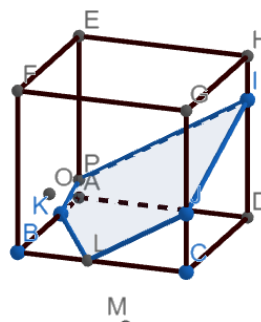
2-қадам. JI түзуін саламыз. $JI \cap CD = M$ (51-сурет)

3-қадам. К, М нүктелері төменгі жазықтықта орналасқандықтан, KM түзуін аламыз. $BC \cap KM = L$ (52-сурет)

4-қадам. $MK \cap DA = O$, $OI \cap EA = P$ (54-сурет)



4-қадам



5-қадам

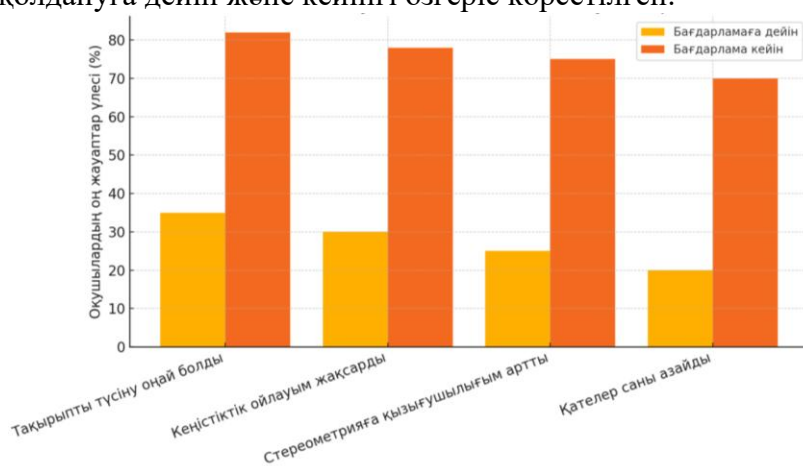
54-сурет

55-сурет

5-қадам. PKLJI –ізелінді қима (55-сурет).

Geo-Gebra бағдарламасына сілтеме: <https://www.geogebra.org/3d/kdwndxas>.

Тәжірибелік сабақтар нәтижесінде оқушылардың кеңістіктік ойлауының дамығаны, пәнге қызығушылығы артқаны және қателер саны азайғаны байқалды. Мұғалімдер тарапынан да сабақ дайындау процесінің жеңілдегені, оқушылармен кері байланыстың артқаны анықталды. Төмендегі диаграммада оқушылардың бағалауы бойынша GeoGebra бағдарламасын қолдануға дейін және кейінгі өзгеріс көрсетілген:



GeoGebra бағдарламасын қолдануға дейін және кейінгі өзгеріс диаграммасы

Диаграмма көрсеткендей, тақырыпты түсіну, кеңістіктік ойлау, қызығушылық және қателердің азаюы бойынша барлық көрсеткіштерде оң өзгеріс байқалды. Бұл GeoGebra бағдарламасының педагогикалық тиімділігін дәлелдейді. Стереометрия тақырыптарын GeoGebra арқылы оқыту – кеңістіктік елестету мен визуализацияға негізделген, заманауи, тиімді педагогикалық тәсіл. Бұл әдіс оқу сапасын арттырып, күрделі кеңістіктік ұғымдарды меңгеруді жеңілдетеді. Мұғалімдерден сауалнама нәтижелері GeoGebra бағдарламасын сабақта қолдану бойынша мұғалімдер арасында жүргізілген сауалнама нәтижелері оның педагогикалық тұрғыдан жоғары тиімділігін көрсетті. Сауалнамаға 30-ға жуық математика пәнінің мұғалімі қатысты. Негізгі сұрақтар мен жауаптардың қорытындысы 1-кестеде көрсетілген.

Кесте 1

Мұғалімдерден алынған сауалнама

№	Сұрақ	Жауаптар
1	Бағдарламаны қолдану сабақ өткізу тәсіліңізге оң әсер етті ме?	Иә – 93%, Жоқ – 7%
2	Стереометрия тақырыптарын түсіндіру жеңілдеді ме?	Иә – 90%, Аздап – 10%
3	GeoGebra оқушылардың белсенділігін арттырды ма?	Иә – 87%, байқалмады – 13%
4	Бағдарламаны келесі оқу жылында қолдануды жалғастырасыз ба?	Иә – 96%, Әлі білмеймін – 4%
5	Бағдарлама ең пайдалы болған тақырып	Қималар – 70%, Бұрыштар және қашықтықтар – 20%, Көлем және аудан – 10%

Сауалнама нәтижелері мұғалімдердің цифрлық құралдарды қабылдау деңгейі жоғары екенін, сондай-ақ GeoGebra бағдарламасының оқыту процесіне оң ықпал ететінін нақты дәлелдейді.

Қорытынды

Мұғалімдерді стереометрияны оқыту процесінде компьютерлік бағдарламаларды қолдануға үйрету-білім беруді модернизациялаудың маңызды қадамы. Бұл оқуды көрнекі, интерактивті және оқушыларға қол жетімді етуге мүмкіндік береді. Бұл әдісті енгізу оқыту сапасы мен стереометриялық білімді игеру тиімділігін арттыруға ықпал етеді.

Цифрлық технологияларды дамыту оқыту әдістемесін үнемі жетілдіруді талап етеді. Сондықтан осы саладағы зерттеулерді жалғастыру, жаңа әдістемелік тәсілдерді әзірлеу және білім беру бағдарламаларын заманауи талаптарға бейімдеу маңызды.

Пайдаланылған әдебиеттер тізімі

1. Смирнов В.А, Тұяқов Е.А. Геометрия: Жалпы білім беретін мектептің 10-сыныбына арналған оқулық. – Алматы: Мектеп, 2019. – 105б
2. Джандигулов, А. Р. Ауэзова, Н. Т. Стереометрия курсында қолданылатын бағдарламалар // Молодой ученый. — 2021. — № 19 (361). — С. 320-322. — URL: <https://moluch.ru/archive/361/80707/>
3. Ауэзова, Н. Т. Стереометрияны үйренуге арналған бағдарлама нұсқаулығы // Молодой ученый. — 2021. — № 16 (358). — С. 368-371. — URL: <https://moluch.ru/archive/358/80165/>.
4. Безумова О.Л., Троицкая О.Н., Овчинникова Р.П., и др. Обучение геометрии с использованием возможностей geogebra: Учебно-методическое пособие. – Архангельск: Кира, 2011. – 140 С.
5. Шыныбеков Ә.Н. Геометрия: Жалпы білім беретін мектептің 11-сыныбына арналған оқулық. 3-басылымы. – Алматы: Ата-мұра, 2012. – 128 Б.
6. Қазақстан Республикасының «Білім туралы» заңы. – 2007 ж.
7. ҚР Оқу-ағарту министрлігі. Жалпы орта білім беру стандарттары. – 2022 ж.
8. Hohenwarter M. GeoGebra: Dynamic Mathematics Software. – www.geogebra.org
9. Өрлеу БАҰО. Цифрлық білім беру ресурстары. – Алматы, 2021.
10. Наурызбаева М. Геометрияны оқытудың визуалды әдістері. – Астана, 2020

УДК 004.932.75

Шаймуратов А.Ж.(Астана, Евразийский национальный университет имени Л.Н. Гумилёва)

АВТОМАТИЗИРОВАННОЕ РАСПОЗНАВАНИЕ НОМЕРОВ ЖЕЛЕЗНОДОРОЖНЫХ ВАГОНОВ: СОВРЕМЕННЫЕ МЕТОДЫ И ПЕРСПЕКТИВЫ

Аннотация

Современные системы учета железнодорожного подвижного состава оптимизируют логистику и повышают безопасность перевозок. Традиционные методы с ручным вводом данных уступают автоматизированным решениям по точности и скорости, что ведет к ошибкам и потерям. В статье рассматриваются технологии распознавания номеров вагонов, включая компьютерное зрение, глубокое обучение, гибридные методы и интеграцию с IoT.

Приведен сравнительный анализ их эффективности, с акцентом на нейросетевые модели, такие как YOLO и EfficientNet, которые показывают высокую точность в реальных условиях.

Ключевые слова: автоматизированный учет, железнодорожный транспорт, компьютерное зрение, глубокое обучение, IoT.

1. Введение

Железнодорожные перевозки остаются одним из основных способов транспортировки грузов и пассажиров. Однако традиционные методы учета подвижного состава, основанные на ручном вводе данных, не справляются с растущими объемами перевозок. Современные технологии, такие как компьютерное зрение и IoT, позволяют автоматизировать процесс распознавания номеров вагонов, минимизируя влияние человеческого фактора.

Цель исследования — анализ современных методов автоматического распознавания номеров, оценка их точности, скорости обработки и применимости в реальных условиях.

2. Методы распознавания номеров

2.1. Традиционные алгоритмы обработки изображений

Классические методы обработки изображений выделяют текстовые области с низкими вычислительными затратами. Бинаризация упрощает выделение текста, операторы Собеля и Кэнни помогают обнаруживать контуры, а K-means сегментирует изображение по цвету и яркости. Эти методы эффективны для устройств с ограниченными ресурсами, но чувствительны к освещению и шумам, что может ухудшать точность обработки.

2.2. Глубокое обучение

Сверточные нейросети (CNN) обеспечивают высокую точность распознавания изображений. YOLO отличается скоростью и детекцией в реальном времени, что важно для видеонаблюдения и автономных систем. ResNet решает проблему исчезающего градиента благодаря остаточным связям, улучшая обучение. EfficientNet оптимизирует баланс между вычислительными затратами и точностью.

Эксперименты показывают: YOLO достигает 99.13% точности при 1.3 мс на кадр, идеально для реального времени. EfficientNet с 93.5% точности требует меньше ресурсов, что удобно для маломощных устройств.

2.3. Оптическое распознавание символов (OCR)

OCR преобразует текст с изображений в машинно-читаемый формат. Современные системы, такие как Tesseract и ABBYY FineReader, комбинируют традиционные методы и нейросети для повышения точности. Эффективным решением являются CRNN, совмещающие извлечение признаков и последовательную обработку, достигая 98.4% точности, что особенно полезно для нечеткого текста.

2.4. Гибридные методы

Гибридные методы объединяют классические алгоритмы и глубокое обучение, обеспечивая высокую точность при умеренных затратах. Традиционные алгоритмы выполняют сегментацию и предварительную обработку, а нейросети — финальную классификацию. Такой подход достигает 96.7% точности, оптимизируя производительность и ресурсы, что особенно ценно для систем с ограниченными мощностями.

2.5. Интеграция с IoT

IoT автоматизирует процессы, объединяя камеры, датчики и облачные вычисления. Такие системы обеспечивают учет и контроль в реальном времени, повышая точность мониторинга. Интеграция с логистическими платформами улучшает управление цепочками поставок, сокращает задержки и повышает прозрачность.

Практика подтверждает эффективность IoT. В Китае железные дороги используют IoT для отслеживания вагонов, снижая потери. В Европе облачные платформы анализируют

маршруты, оптимизируя грузоперевозки. IoT становится ключевым элементом цифровизации транспорта.

3. Сравнительный анализ методов

В таблице 1 представлены основные методы обработки и распознавания, используемые в современных системах компьютерного зрения, с оценкой их точности, времени обработки и возможности интеграции с IoT.

Таблица 1 – Сравнение методов обработки и распознавания

Метод	Точность (%)	Время обработки (мс)	Интеграция с IoT
Традиционные алгоритмы	85.2	18	Ограничена
Глубокие нейросети (CNN)	98.3	45	Средняя
Гибридные методы	96.7	30	Высокая
IoT + компьютерное зрение	97.5	3	Максимальная

Анализ представленных методов показывает, что наибольшую точность (98.3%) обеспечивают глубокие нейросети (CNN), однако их использование сопряжено с высокими вычислительными затратами и увеличенным временем обработки (45 мс). Гибридные методы, сочетающие традиционные алгоритмы с нейросетевыми моделями, демонстрируют сбалансированный результат, обеспечивая точность 96.7% при умеренном времени обработки (30 мс) и высокой интеграции с IoT. Наиболее перспективным направлением являются IoT-решения с применением компьютерного зрения, которые обеспечивают скорость обработки всего 3 мс при высокой точности (97.5%) и максимальной степени интеграции с цифровыми платформами. Такой подход делает IoT наиболее эффективным решением для автоматизации учета и мониторинга в реальном времени.

4. Заключение

Автоматизированное распознавание номеров вагонов повышает точность учета, снижает затраты и ускоряет обработку данных. Анализ показал, что нейросетевые и гибридные методы превосходят традиционные алгоритмы, а интеграция IoT обеспечивает учет в реальном времени.

Развитие технологий связано с оптимизацией нейросетей и внедрением edge-вычислений для ускорения обработки. Ключевые направления:

- Энергоэффективные алгоритмы для снижения вычислительных затрат.
- Повышение устойчивости к сложным условиям.
- Предиктивная аналитика для выявления неисправностей.

Эти решения улучшат контроль за подвижным составом, повысят эффективность перевозок и снизят расходы на обслуживание.

Список источников

1. X. Li, H. Zhang, and Y. Sun, "Automatic identification of railway wagons using image processing," *J. Railway Eng.*, vol. 23, no. 4, pp. 217–225, 2016.
2. Y. Zhao, W. Liu, and T. Chen, "Railway Wagon Number Recognition Using Convolutional Neural Networks," *Pattern Recognit. Mach. Learn.*, vol. 45, no. 5, pp. 1020–1032, 2019.
3. J. Wang, Y. Zhao, and W. Zhang, "Deep Learning-Based Recognition of Railway Vehicle Numbers in Complex Environments," *J. Transp. Technol.*, vol. 13, no. 2, pp. 45–58, 2023.

4. R. O'Connor, J. Sullivan, and D. Murphy, "Edge-CNN Hybrid for Enhanced Railway Wagon Identification," *Adv. Vis. Technol. J.*, vol. 45, no. 6, pp. 203–217, 2022.
5. D. Lee and H. Kim, "Integration of IoT and Computer Vision for Automated Railcar Tracking," *Sensors*, vol. 20, no. 15, p. 4056, 2020.

4 СЕКЦИЯ

«КРИПТОГРАФИЯДАҒЫ ЖАСАНДЫ ИНТЕЛЛЕК ЖӘНЕ КИБЕРҚАУПСІЗДІК»

СЕКЦИЯ 4

«ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В КРИПТОГРАФИИ И КИБЕРБЕЗОПАСНОСТИ»

SECTION 4

"ARTIFICIAL INTELLIGENCE IN CRYPTOGRAPHY AND CYBERSECURITY"

УДК 004.896

Altaibayev D. M.
(Karaganda, Abylkas Saginov KarTU)
Mukhametzhanova B. O., PhD
(Karaganda, Abylkas Saginov KarTU)

ARTIFICIAL INTELLIGENCE METHODS FOR SIMULATING COMPUTER EFFECTS IN TRADITIONAL ANIMATION USING MODERN GRAPHICS TECHNOLOGIES

The application of artificial intelligence (AI) in computer animation greatly enhanced visual effects by enabling the automation of shading, lighting, and texturing without any quality compromise. AI-based approaches such as neural rendering, generative adversarial networks (GANs), and inverse rendering enhance the level of realism, simplify production, and provide more creative freedom. These approaches lighten the animator's workload and provide new means to produce textures, light simulation, and frame filling.

Achieving natural lighting, shadowing, and texturing in traditional animation requires an enormous amount of human labor. These are now being automated by the help of AI software. They enable animators to focus less on creative limitations than on freedom of expression. Hand-drawn textures are examined by generative models, and they generate seamless versions to provide visual continuity between the frames. Diffusion models have worked particularly well to create high-resolution textures with smooth transitions between material transitions. These technologies offer artists the capacity to create consistent styles with the help of computational automation.

Advanced developments in GAN-based image synthesis have greatly enhanced animation pipelines by improving texture stability and computational efficiency. The most notable among them is StyleGAN3, which eliminates the problem of 'texture sticking' in synthesized images by making architectural updates that eliminate aliasing, enabling textures of images to move along represented objects smoothly. Similar development makes StyleGAN3 tremendously strong for applications in video and animation, ensuring a higher level of smooth motion from one frame to the other. EfficientGAN has also been made to minimize the resource capacity required to train GANs without compromising on the quality of visual output of images [1] to provide AI-generated animation at an economical cost. Everything makes it feasible to incorporate AI-based methodology in traditional animation and maintain high artistry fidelity as well.

GANs also play the essential role of material and texture automation, improving the visual animation quality. They learn from the available hand-drawn textures and generate variations that blend seamlessly with the original piece. Blended creation can improve the production efficiency and quality of animation works, while also providing creators with more creative tools and possibilities [2]. This ensures that animations retain a handcrafted aesthetic while reducing the need for repetitive detailing.

Inverse rendering techniques reconstruct lighting information from 2D images, enabling AI-driven estimation of shadows and reflections. Deep learning models trained on various lighting environments predict how light interacts with characters and backgrounds, providing a more realistic visual representation. Techniques such as ray tracing, path tracing, and rasterization have revolutionized rendering by simulating the behavior of light and producing images with astonishing realism [3]. These techniques help maintain lighting consistency across sequences, minimizing the need for manual shading corrections.

Modern animation pipelines powered by AI combine pre-trained models and hybrid art techniques to improve productivity. Deep learning models trained on hand-drawn animation data help with shading correction, texture generation, and lighting adjustments. Blender Grease Pencil and Adobe After Effects powered by AI allow animators to iterate on lighting and texture effects in real time. Computational algorithms are critical to achieving consistency and efficiency in production. They streamline the rendering process of complex scenes, optimizing the use of computing resources and reducing time and costs. These technologies significantly improve animation production by automating time-consuming tasks and providing real-time previews.

One of the critical factors influencing the adoption of AI-driven animation techniques is cost efficiency. AI-assisted animation production can significantly reduce expenses associated with manual labor, rendering, and revisions. Figure 1 illustrates the average cost of character and scene creation using traditional animation, AI-generated content, and blended creation methods.

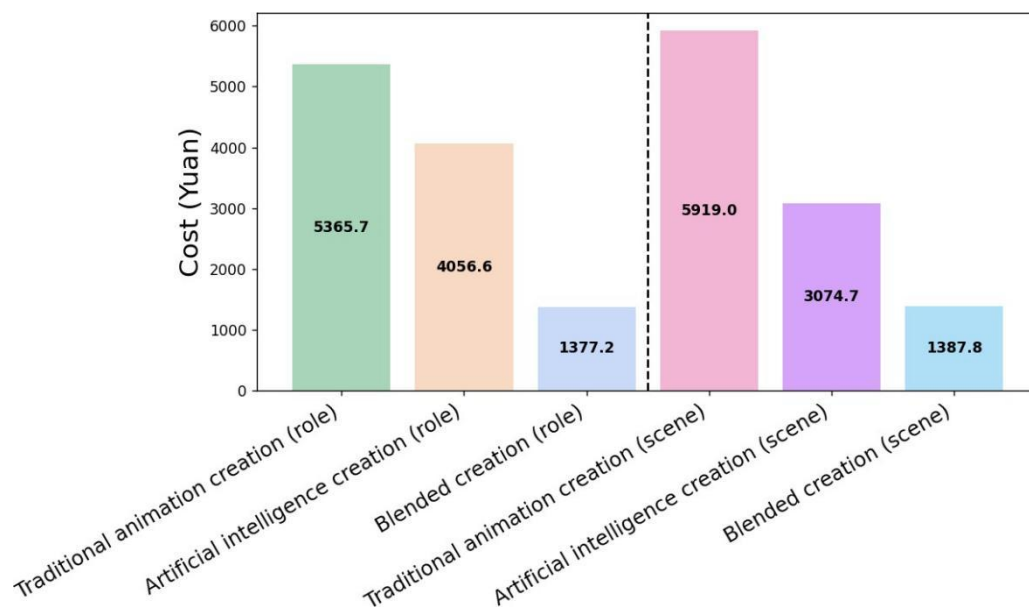


Figure 1 - Average cost of creation using different methods

As Figure 1 shows, the expense of blended creation is significantly cheaper than that of traditional animation. Character creation in traditional animation costs an average of 5365.7 yuan, but with the help of AI, it is reduced to 4056.6 yuan. Blended creation reduces it to 1377.2 yuan. Similarly, scene creation expenses are reduced from 5919.0 yuan in traditional animation to 3074.7 yuan with the support of AI and to 1387.8 yuan with a blended process. These savings reveal the economic benefit of the use of AI in animation pipelines to make high-quality animation more accessible to independent filmmakers and small-scale animation houses. [2]

The rapid evolution of AI continues to revolutionize the future of animation with the availability of real-time style transfer and physics-based simulation. Such technologies provide animators with more artistic control with the benefit of AI automation. The combination of algorithms with the artist's creativity in animated VFX exemplifies the revolutionary extent of the effect they have on contemporary animation. As AI technologies continue to develop, they will continue to aid in animation production with emerging forms of storytelling and artistry.

By using AI to enhance traditional animation, artists are able to achieve visually striking effects with no compromise on artistic integrity. In this manner, the art of animation is transformed, with the use of computational intelligence enhancing but not replacing human imagination. The

combination of traditional methods with AI-based enhancements applied ensures that hand-drawn animation continues to be a living and breathing art form in the digital era.

References

1. H. Bougueffa, M. Keita, W. Hamidouche, A. Taleb-Ahmed, H. Liz-López, A. Martín, D. Camacho, A. Hadid. "Advances in AI-Generated Images and Videos." International Journal of Interactive Multimedia and Artificial Intelligence, vol. 9, no. 1, 2024, p. 36.
2. W. Yuanliang, Z. Zhe. "Integration Effect of Artificial Intelligence and Traditional Animation Creation Technology." Journal of Intelligent Systems, vol. 33, 2024, p. 14.
3. T. Duan, W. Dong, F. Wang, Y. Yao. "Computational Algorithms and Aesthetic Impact in Animated Visual Effects." IEEE Access, 2024, p. 13.

Alzhan Tilenbayev, Khuralay Moldamurat and Huseyin Canbolat
Department of Information Security
L. N. Gumilyov Eurasian National University
Astana, Kazakhstan

АНАЛИЗ ЭФФЕКТИВНОСТИ DDOS СЕТЕВОЙ АТАКИ НА IOT УСТРОЙСТВО

Абстрактный

В этой статье обсуждается DDoS-атаки более детально. DDoS (Distributed Denial of Service) атаки представляют собой серьезную угрозу для онлайн-ресурсов, включая веб-сайты, сервера и сети. Они могут быть проведены злоумышленниками с целью парализовать работу целевой системы, не позволяя пользователям получать доступ к сервисам.

Ключевые слова

Кибербезопасность, информационная безопасность, кибератака

1. Введение

DDoS-атака – распределенная атака, направленная на отказ в обслуживании. В результате атаки такого типа атакуемый сетевой ресурс получает лавинообразное количество запросов, которые не успевает обработать. Источником вредоносных запросов являются так называемые зомби-сети, состоящие большей частью из компьютеров обычных пользователей, в силу каких-то причин зараженных вредоносным ПО. Крупным DDoS-атакам подвергаются сайты правительства и органов власти, сайты ведущих IT-корпорация Amazon, Yahoo, Microsoft и т.д.

Эти мощные корпорации, имеющие огромные ресурсы, не всегда могут справиться с атаками и отразить нападение. Ежегодно различные компании, предоставляющие услуги в области обеспечения информационной безопасности и противодействия кибератакам, фиксируют увеличение количества DDoS-атак и их мощность. Периодические сообщения в средствах массовой информации о недоступности тех или иных ресурсов в результате распределенных атак, направленных на отказ в обслуживании, говорят о неэффективности средств противодействия такого рода атакам. На фоне указанных выше атак к ведущим IT-корпорациям также увеличивается количество атак и к небольшим, «средним» сайтам, которые до недавнего времени не представляли интереса для злоумышленников. Однако, в настоящее время, в связи с увеличением их важности и востребованности, перебои в их работе могут быть критичными.

2. Теоретическая часть

Вместе с этим меняются и мотивы, которые движут злоумышленниками, если раньше среди причин возникновения DDoS-атак можно было выделить протест, хулиганство и т.д., то сегодня все чаще DDoS-атаки являются следствием шантажа и способом вымогательства денег. Это переводит DDoS-атаки из плоскости единичных протестных акций в область криминального бизнеса, который не ограничивается 5 вымогательством, но и является инструментом экстремистских и террористических организаций. Сегодня во всем мире стали обычной ситуацией атаки на сайты государственной власти накануне выборов или важных политических событий. Причем если вызвать отказ в работе крупного ресурса, имеющего в своем арсенале активные средства противодействия, можно, пожалуй, только заполнением всей полосы пропускания канала связи, что влечет необходимость в создании и поддержании достаточно большой бот-сети. То для парализации небольшого регионального ресурса достаточно небольшой по мощности атаки и как следствие небольшой бот-сети. Обслуживание и поддержание таких бот-сетей является менее затратным, и потенциально создать такие сети может большее количество злоумышленников.

Этот факт на фоне отсутствия адекватных средств противодействия делает угрозы безопасности региональных ресурсов в результате DDoS-атак особенно значимым. С одной стороны, для противодействия таким атакам могут быть эффективно применены средства, предназначенные для отражения крупных атак. С другой – внедрение и поддержание таких средств экономически затратно и не по карману региональным ресурсам. Средства противодействия, специализированные именно на обеспечение безопасности небольших и средних ресурсов, получили меньшее развитие из-за преобладания в прошлом именно крупных атак. И в настоящее время отстают от эволюции самих DDoS-атак.

3. Практическая часть

Действительно, DDoS-атаки (атаки распределенного отказа в обслуживании) являются серьезной угрозой для Интернета вещей (IoT) из-за их потенциальной способности парализовать устройства, связанные с Интернетом и даже целые сети. Анализ эффективности DDoS-атак на устройства IoT имеет большое значение для понимания возможных последствий таких атак и разработки мер по их защите.

Когда IoT-устройство подвергается DDoS-атаке, нагрузка на его сетевой интерфейс существенно повышается из-за потока запросов, поступающих от зловредных источников. Это может привести к перегрузке ресурсов устройства, снижению его производительности или полному отказу в обслуживании. Кроме того, DDoS-атаки на IoT-устройства могут использоваться как способ отвлечения внимания от других видов кибератак, что делает их еще более опасными.

Для оценки эффективности DDoS-атак на IoT-устройства проводятся различные исследования, включающие анализ уровня пропускной способности, времени отклика и устойчивости к атакам. Исследователи также изучают методы обнаружения и предотвращения таких атак, а также меры по повышению безопасности устройств IoT.

Одним из способов защиты от DDoS-атак на устройства IoT является использование специальных систем обнаружения вторжений, механизмов фильтрации трафика и применение усиленных методов аутентификации и шифрования. Также важно проводить обновления программного обеспечения устройств и следить за их безопасностью на протяжении всего их жизненного цикла.

В целом, анализ эффективности DDoS-атак на IoT-устройства является важной областью исследований в сфере кибербезопасности, которая помогает развивать новые методы защиты и обеспечивать надежную работу устройств, связанных с Интернетом.

Одной из характеристик DDoS-атак является их распределенная природа, когда атакующие используют ботнеты или другие компрометированные устройства для генерации большого объема трафика, направленного на цель. Это создает высокую нагрузку на целевую систему, и, в результате, сервис становится недоступным для легитимных пользователей.

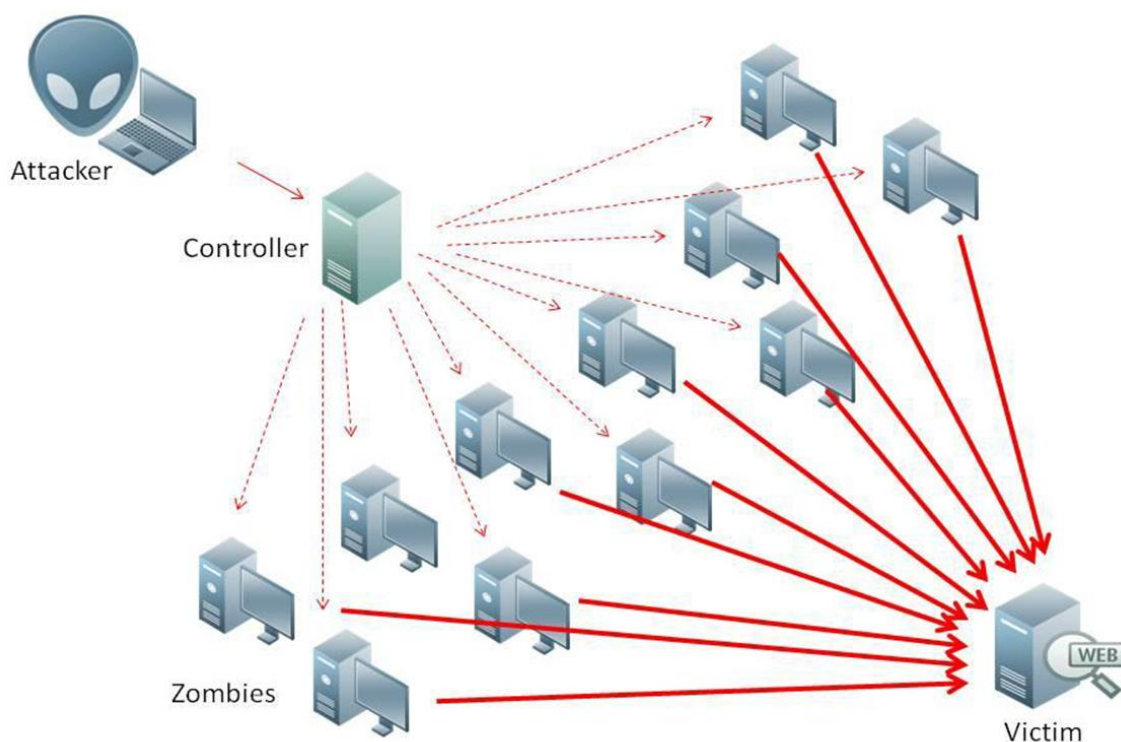
Для защиты от DDoS-атак существуют различные методы, включая использование специализированных аппаратных устройств и программного обеспечения, облачные сервисы защиты от DDoS, настройку механизмов обнаружения атак и многослойные системы защиты.

Обсуждение DDoS-атак также включает в себя раскрытие их различных типов (например, атаки на уровне сети, приложения или протокола), масштабов, целей (например, банки, государственные учреждения, компании) и последствий для бизнеса и общества в целом.

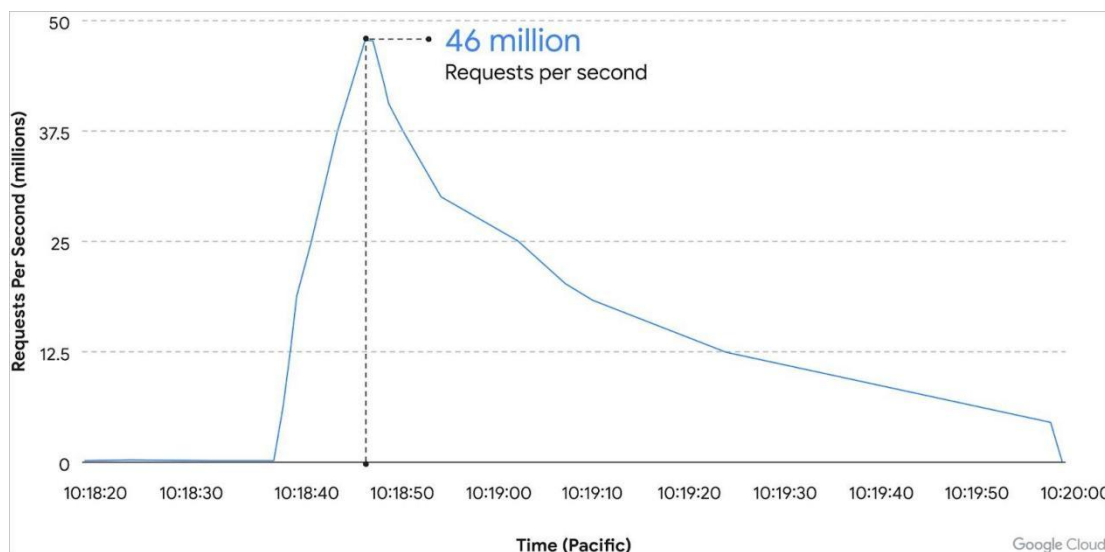
Также важно обсудить меры предосторожности, которые могут быть приняты для защиты себя или своей организации от DDoS-атак, чтобы минимизировать возможные убытки и обеспечить непрерывность бизнеса.

Конечно, я могу предоставить вам пример графика, иллюстрирующего характеристики DDoS-атаки. Для наглядности представим временные зависимости интенсивности атаки и ее воздействия на целевую систему.

Представим, что по оси абсцисс у нас будут отложены временные интервалы (например, каждый час), а по оси ординат - уровень трафика или интенсивность запросов, поступающих на целевую систему.



Мы можем увидеть следующие основные моменты:



1. Начало атаки: Возрастание графика со временем, что указывает на увеличение трафика из-за DDoS-атаки.

2. Пик нагрузки: Максимальная точка на графике, показывающая наивысшую интенсивность атаки.

3. Длительность атаки: Временной интервал, в течение которого атака продолжается.

4. Завершение атаки: Снижение графика до нулевого уровня, показывающее окончание атаки и восстановление нормального трафика.

График DDoS-атаки может иметь различные формы в зависимости от типа атаки, ее масштаба и продолжительности. Такие графики позволяют анализировать характеристики атаки, определять ее поведение и принимать меры по защите от подобных событий.

Заключение

Заклучение DDoS-атаки играет важную роль в восстановлении нормального функционирования целевой системы после того, как она была подвергнута атаке. Процесс заклччения DDoS-атаки включает в себя несколько этапов:

1. Обнаружение атаки: Первоочередная задача - обнаружить факт DDoS-атаки как можно раньше. Для этого требуется система мониторинга, способная анализировать трафик и выявлять аномалии, характерные для DDoS-атак.

2. Ответные меры: После обнаружения атаки необходимо принять меры по смягчению ее воздействия. Это может включать в себя настройку фильтров трафика, блокирование IP-адресов злоумышленников, перераспределение нагрузки и т.д.

3. Восстановление сервиса: После завершения атаки следует восстановить нормальное функционирование целевой системы. Это может потребовать проверки программного и аппаратного обеспечения на наличие уязвимостей, а также резервного копирования данных, если они пострадали в результате атаки.

4. Анализ инцидента: После того как система восстановлена, важно провести детальный анализ инцидента DDoS-атаки. Это поможет понять характеристики атаки, выявить ее слабые места и принять меры для предотвращения подобных ситуаций в будущем.

Заклучение DDoS-атаки требует комплексного подхода и оперативных действий для минимизации ущерба, восстановления работоспособности системы и предотвращения подобных инцидентов в будущем.

- 1 The radiation problem from a vertical hertzian dipole antenna above flat and lossy ground: Novel formulation in the spectral domain with closed-form analytical solution in the high frequency regime. Ioannidi, K., Christakis, Ch., Sautbekov, S., Frangos, P., Atanov, S.K. \International Journal of Antennas and Propagation, 2014, 2014, 989348
- 2 Development an Intelligent Task Offloading System for Edge-Cloud Computing Paradigm. Atanov, S.K., Seitbattalov, Z.Y., Moldabayeva, Z.S. \Proceedings - 2021 16th International Conference on Electronics Computer and Computation, ICECCO 2021, 2021
- 3 An Intelligent Decision Support System for Aircraft 5. Landing Based on the Runway Surface. Seitbattalov, Z.Y., Atanov, S.K., Moldabayeva, Z.S. \SIST 2021 - 2021 IEEE International Conference on Smart Information Systems and Technologies, 2021, 9466000
- 4 Development and modeling of intelligent control system of cruise missile based on fuzzy logic. Utegen, A.S., Moldamurat, K., Ainur, M., ...Amandykuly, A.G., Brimzhanova, S.S. \ Proceedings - 2021 16th International Conference on Electronics Computer and Computation, ICECCO 2021, 2021
- 5 Development of a software simulator for small satellite swarm control. Moldamurat, K., Utegen, A.S., Brimzhanova, S.S., Kalmanova, D.M., Yrskeldi, N.G. \ Proceedings - 2021 16th International Conference on Electronics Computer and Computation, ICECCO 2021, 2021

UDC 004.82

Yelibayeva Gaziza, Bibigul Razakhova
Altynbek Sharipbay, Gulbarshin Syzdykova
(Astana, L.N. Gumilyov Eurasian National University)

ONTOLOGICAL MODELS OF THE KAZAKH LANGUAGE FOR SECONDARY EDUCATION

1. Introduction

In the context of digitalization of education, the development of intelligent learning systems capable of interacting with users in the state language is of particular importance. In our country, such a language is the Kazakh language, and its integration into digital environments requires deep formalization. The creation of intelligent textbooks in the Kazakh language is possible in the presence of an ontological model reflecting the structure and content of school programs. Ontology provides systematization, formalization and semantic links between key concepts, which is especially important for agglutinative languages such as Kazakh. Previous studies [1-3] show the effectiveness of ontological approaches in formalizing the morphology and semantics of the Kazakh language, which confirms the relevance and scientific significance of this work.

2. Methodology

Kazakh language textbooks for grades 2-4, available on the Okulyk.kz platform [4], were used for constructing the ontology. The selection of terms was carried out manually, taking into account frequency, educational significance, and alignment with curricula. Lexical and grammatical units (parts of speech, grammatical categories, syntactic structures, etc.) and explanatory terms (text, dialogue, message, etc.) were identified. The model was created in the Protégé environment [5], using the OWL formalism, which ensures compatibility with international ontologies and platforms. The ontology structure implements a hierarchy of concepts, including classes, subclasses, and properties, reflecting semantic relationships

3. Results

The developed ontology encompasses educational levels by grade, and is also organized according to a hierarchical principle: key classes such as vocabulary, grammar, phonetics, and orthography are identified, each of which is subdivided into subclasses (for example, parts of speech,

etc.). Explanatory terms (text, title, dialogue, etc.) have also been included, represented as classes with annotations and relationships. To denote logical and semantic connections (Figures 1-2), properties (1), (2), and (3) were used:

$$Parts\_of\_Speech \in Morphology\_2 \cap Morphology\_4 \quad (1)$$

$$Verb\_2 \cup Verb\_4 \equiv Predicate \quad (2)$$

$$Simple\_Noun \equiv \forall Parts\_of\_Speech (Noun\_2) \cap consists\ "one\ word" \quad (3)$$

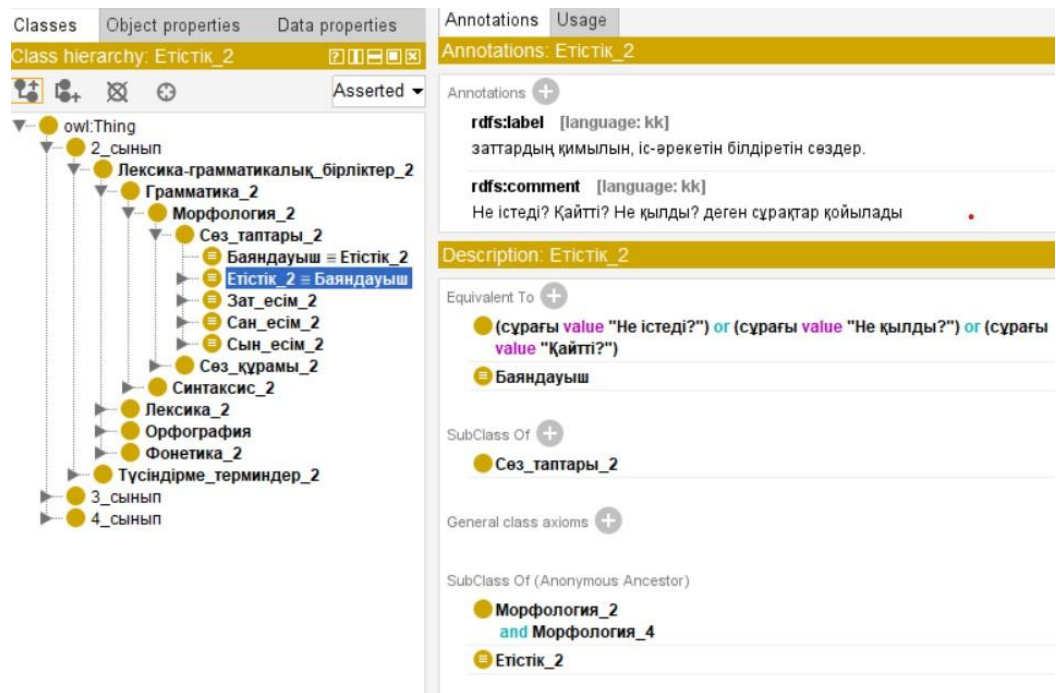


Fig. 1. Ontology of logical and semantic connections of the concept “Verb”

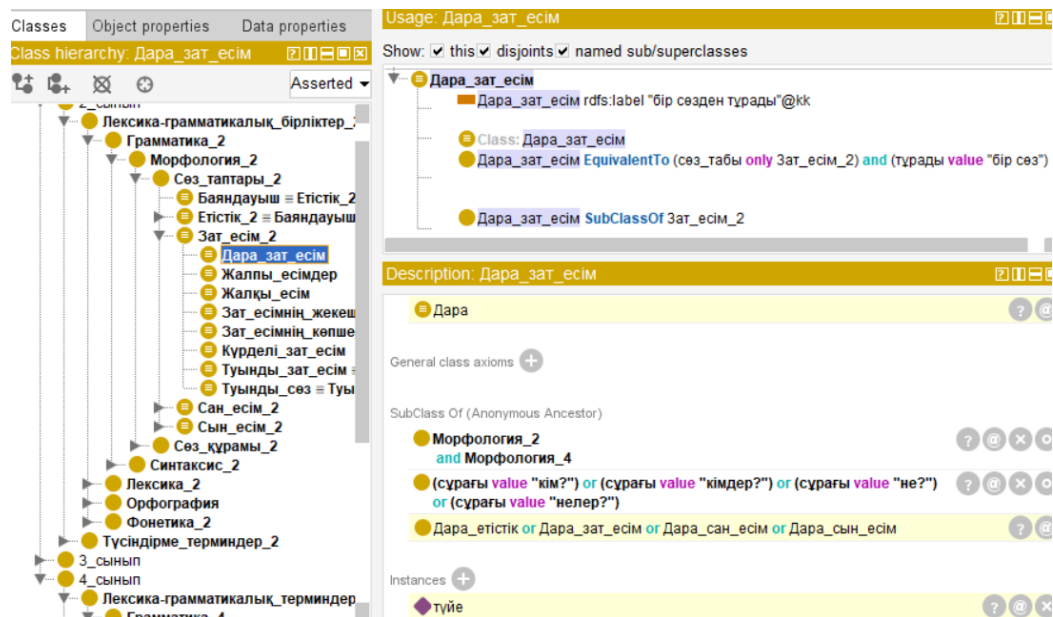


Fig. 2. Ontology of logical and semantic connections of the concept “Simple Noun”

A distinctive feature of the developed model is the consideration of differences in the levels of mastering educational material at various stages of learning: terms encountered in grades 2 and 4 are represented as intersections of classes, reflecting the increasing complexity of content. This approach maintains the logical integrity of the ontology, ensuring continuity of knowledge and the proper distribution of terms across educational levels. Furthermore, the ontology is designed for further use in automated text processing systems, linguistic analysis, and intelligent educational platforms.

4. Conclusion and Future Research

The developed ontology of the Kazakh language for elementary grades systematizes knowledge of key linguistic categories and forms the basis for the development of intelligent systems. It reflects the educational structure, takes into account the specifics of the Kazakh language, and meets the requirements of digital educational platforms. The next stage of the work will involve expanding the ontology to include educational materials for grades 9-11. This will allow for the inclusion of more complex syntactic structures, stylistic features, and terminology for text analysis. The integration of these levels will create a fully functional model of the Kazakh language, suitable for machine translation, automatic analysis, and intelligent learning.

This research is funded by the Science Committee of the Ministry of Education and Science of the Republic of Kazakhstan (Grant No. AP19678613).

References

1. L. Zhetkenbay, A. Sharipbay, G. Bekmanova and U. Kamanur, Ontological modeling of morphological rules for the adjectives in Kazakh and Turkish languages. *Journal of Theoretical and Applied Information Technology*. Vol. 91, No. 2, 2016, pp. 257- 263.
2. G. Yelibayeva, A. Sharipbay, A. Mukanova, and B. Razakhova, "Applied ontology for the automatic classification of simple sentences of the Kazakh language," In Proceedings of the 5th International Conference on Computer Science and Engineering, Diyarbakir, Turkey, pp. 13-18, 2020, doi: 10.1109/UBMK50275.2020.9219461
3. A. A. Sharipbay, B. Sh. Razakhova, A. S. Mukanova, and B. Zh. Yergesh, "Mathematical and ontological models and electronic thesaurus of the grammar of the Kazakh language," Monograph (in Kazakh), Nur-Sultan: IE "Bulatov A. Zh", 2020.
4. Portal of electronic textbooks [Online]. Available: Okulyk.kz
5. A free, open-source ontology editor and framework for building intelligent systems [Online]. Available: <https://protege.stanford.edu>

УДК 004.9:721

Yerzatuly Temirlan ("Esil University",
Astana)

BIOMETRIC SECURITY IN SMART BUILDINGS: A NEW AGE OF AUTOMATION, PRIVACY, AND EFFICIENCY

Abstract

Biosystems, especially face/identity verification, are changing measures of safe entry into modern structures, security, entry loosening and office work advancement. This article talks about recognition tools such as Flat, 3D, mixed and AI. It looks at their good points and drawbacks. Vision Transformers (VIT) and Generative Area Networks (GAN) have vastly improved accuracy and flexibility. Nevertheless, issues such as privacy concerns, unauthorized dissemination of information, and the emergence of sophisticated imitations remain as significant challenges. Engaging AI means respecting privacy laws such as GDPR and ISO 27701 for data security.

Despite the obstacles, the advancement of AI-based security will increase biometric constraints, creating smarter and more secure buildings.

Keywords: *facial recognition, biometric security, AI surveillance, smart buildings, access control, cybersecurity*

Introduction

Computational Intelligence (CI) has transformed sectors globally and a major front of innovation is in protective services, particularly in the realm of smart facilities. The computerized recognition and entry regulation method — facial authentication is becoming a game changer. This technology is widely applicable and is set to significantly enhance the security aspect while maximizing real-time security protocols. Despite significant achievements to date, challenges still remain, particularly in the areas of ethics, privacy and legal.

According to MarketResearch.com the global facial recognition market was valued at USD 5.1 billion. The global Facial Recognition Market was valued at USD 5.1 Billion in 2022 and is expected to increase to USD 10.9 Billion by 2027. This market is expected to exceed USD 10.9 billion by 2027, growing at a CAR of 16.4% [1]. Countries like Kazakhstan are utilizing these facilities in the industries of transportation, finance and personal health and wellness. This treatise details the human identification mechanisms deployed as part of safety protocols for cerebral designs, their benefits, challenges, and potential for upcoming improvements.

1. Facial Recognition Technologies in Smart Buildings

1.1 Mechanisms of Facial Recognition

Modern facial recognition technologies rely on advanced AI models to perform automated identification. Key techniques include:

- 2D Recognition: Basic facial recognition that analyzes flat images but is sensitive to changes in lighting and angle [3].
- 3D Recognition: Provides higher accuracy by creating detailed facial models using depth-sensing technology [4].
- Hybrid Models: Combine multiple recognition methods to boost reliability and accuracy [5].
- Deep Learning Algorithms: Advanced models like Vision Transformers (ViT) and GANs improve system adaptability, reducing false positives and increasing accuracy under various conditions [5].

These systems continuously evolve, refining their algorithms to enhance performance over time [6].

1.2 Hardware Advancements

Smart buildings are equipped with high-tech devices to improve facial recognition efficiency, including:

- Infrared (IR) Cameras: Essential for recognizing faces in low-light environments [2].
- AI-Driven Biometric Terminals: Facilitate secure and instantaneous identity verification [3].
- IoT Integration: Allows seamless building automation alongside security functions [1].
- Specialized Processing Units (TPUs): Accelerate image processing to ensure fast authentication [4].

2. Application in Smart Building Security

2.1 Smart Access Control

Facial recognition plays a vital role in securing physical access to buildings, such as corporate offices, government premises, and residential areas. By replacing traditional keycards, these systems lower the risk of unauthorized access and fraud. Integration with smart gates and digital access systems allows for frictionless authentication [3].

2.2 AI-Powered Surveillance

AI-enabled CCTV cameras can analyze live video feeds to detect unusual activity, alerting security staff in real time. According to Allied Market Research, AI-driven surveillance is expected to grow by 20% annually until 2028 [2]. These systems can recognize potential threats, such as abandoned packages or abnormal crowd movements, which is particularly useful in public places like airports and shopping malls [2].

3. Benefits and Obstacles in Facial Recognition Adoption

3.1 Key Advantages

- **Improved Security:** Relying on biometric authentication reduces unauthorized access risks [4].
- **User Convenience:** Eliminates the need for physical ID cards or key fobs, offering a contactless experience [5].
- **Integration with IoT:** Optimizes building management by integrating security with climate control, lighting, and access systems [1].
- **Cost Savings:** Automating security monitoring reduces the need for manual intervention and lowers operational costs [2].

3.2 Major Challenges

- **Accuracy Issues:** Environmental factors such as lighting, angle of view, or physical obstructions (e.g., glasses or masks) can reduce system reliability. Studies indicate that 2D recognition accuracy is just 75% compared to 3D or hybrid models [5].
- **Data Privacy:** Collecting and storing biometric data must align with privacy laws, including GDPR and ISO 27701, to protect user information [4].
- **Cybersecurity Threats:** Deepfake technologies and spoofing risks require robust anti-spoofing mechanisms to protect data integrity [5].

4. Results and Discussion

4.1 Comparing Facial Recognition Methods

The study highlights four primary recognition techniques:

Method	Accuracy	Strengths	Weaknesses
2D Recognition	~75%	Low computational cost	Poor performance in low light [5]
3D Recognition	High	Better accuracy in different conditions	Requires specialized hardware [5]
Hybrid Models	Very High	Combines benefits of 2D & 3D	More resource-intensive [5]
Deep Learning	Superior	Self-learning adaptability	Computationally expensive [5]

Table 1. Key features of recognition techniques

4.2 Security and Accessibility

4.3 AI-enhanced facial recognition strengthens building security by ensuring real-time, reliable authentication, while AI-driven surveillance aids in early threat detection. The growing market for these technologies signals widespread use in critical infrastructure [3].

4.4 Overcoming Challenges

- **Improving Accuracy:** Use of 3D scanning and AI techniques minimizes errors [5].
- **Legal Compliance:** Adherence to regulations like GDPR ensures responsible deployment [4].
- **Anti-Spoofing Techniques:** Developing methods to counter deepfakes will improve system

integrity [5].

4.5 Future Directions and Recommendations

The future of facial recognition in smart buildings includes advancements in:

- Adaptive AI Models: Improving accuracy in various environments [6].
- Blockchain Integration: Ensuring secure and immutable data storage [5].
- Multi-Modal Authentication: Combining facial recognition with other biometrics for

enhanced security [4].

Conclusion

Facial recognition systems are truly turning the perception of building security upside down, improving building operations and security. Despite challenges such as privacy concerns and cybersecurity risks, the future of facial recognition in smart buildings looks promising. The integration of blockchain and multimodal biometrics can significantly improve the reliability and security of these technologies. Provided we keep a close eye on ethical considerations and comply with regulatory requirements, facial recognition will take center stage in the future of building security.

References

1. MarketsandMarkets. "Facial Recognition Market - Global Forecast to 2027." 2022.
2. Allied Market Research. "Artificial Intelligence in Video Surveillance Market."
3. ISO/IEC 27701:2019 – Information security, cybersecurity and privacy protection.
4. European Union General Data Protection Regulation (GDPR), 2018.
5. Zhao W., Chellappa R., Phillips P.J., Rosenfeld A. "Face Recognition: A Literature

УДК 004.56/.53

Ibraikhan Alinur (Astana IT University)
Smagulov Temirlan (Astana IT University)
Aitmagambet Aisultan (Astana IT University)
Amirova Akzhibek (Astana IT University)

DEVELOPMENT OF AN ALGORITHM FOR DETECTING MALICIOUS LINKS ON INSTAGRAM

Modern communication technologies have revolutionized human relationships as well as information disseminated and commercial activities performed. Modern society depends heavily on social media platforms where Instagram establishes itself as a worldwide leader among them. As the platform hosts more than 2 billion active users it functions as a potent platform which enables users to engage in real-time exchanges and share content and direct message while serving both business and personal needs [1]. The expanding adoption of social media has led to a proportional growth of cyber threats since criminals use platforms to conduct fraudulent schemes [2]. Hot links distributed on Instagram represent one of the most frequent and dangerous cyber threats that users encounter. These hyperlinks present through comments and DMs and bios and paid advertisements act as entry points for phishing scams and malware transmissions and financial scams [3].

The proposed research adopts a learning-based approach instead of static blacklists or rule-based detection methods to identify URLs in Instagram.

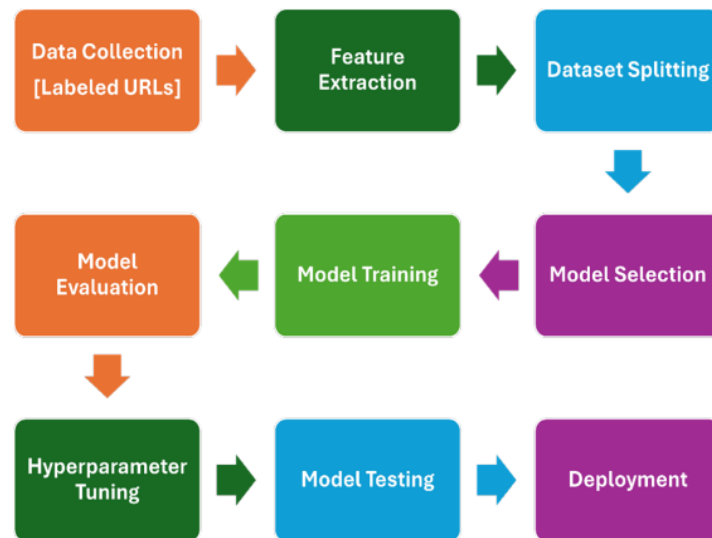


Figure 1. Machine Learning-Based Link Detection

To detect malicious links on Instagram, we implemented a hybrid detection approach, combining machine learning and heuristic-based techniques. This methodology provides a robust and adaptive system capable of identifying new threats while leveraging known attack patterns.

- We employed learning models Random Forest, XGBoost, and LightGBM classifiers, to categorize URLs into four classes: benign, defacement, phishing, and malware.
- A set of manually crafted rules was applied to evaluate the suspicious nature of URLs based on common phishing characteristics.
- By integrating heuristic rules with ML models, we achieved a more comprehensive detection mechanism, ensuring higher accuracy and better generalization to unseen data.

We will be using three machine learning ensemble classifiers Random Forest, Light GBM, and XGBoost.

Traditional machine learning models is what need. Now we need to choose what exact algorithms among this models is good by comparing its accuracy, precision, recall and F1-score. Our candidates are Random Forest, Extra Trees, LightGBM and XGBoost. After some research we decided to not use Extra Trees cause of already using Random Forest and they work similar, so there no point in using both.

Random Forest, LightGBM and XGBoost work very differently from each other while having great accuracy and speed. SVM showed very unstable results ranging from accuracy of 84% to 98% and was too slow for this type of operations, while the rest had no such problems with accuracy and speed.

Using the Instagram API provided to us by Facebook, we can access various information on the page. Such as posts, reels, stories, messages, and comments. They already provide us with even more in-depth information about the release time, author, description, number of likes and comments. Additionally, the function of page views of people who liked or commented might be very useful.

The main functions are viewing the description and comments, thanks to which, when a link is found, it is designated as dangerous or safe.

The proposed algorithm for detecting malicious Instagram links integrates seamlessly into a web browser extension or Instagram-integrated plugin. The key objective is to provide intuitive, real-time safety warnings to users. The system utilizes a hybrid detection model combining Random Forest, LightGBM, and XGBoost algorithms.

Technologies Used:

- Frontend: HTML, CSS, JavaScript.
 - Backend: Python, Machine Learning libraries (Scikit-learn, XGBoost, LightGBM).
- Real-time Analysis and User Interaction Flow:
1. The extension/plugin automatically scans links in user profiles, posts, DMs, and comments.
 2. Each link is classified using the hybrid algorithm.
 3. Results are displayed using clear visual indicators (color coding and icons).
 4. Users can toggle the security feature on or off.

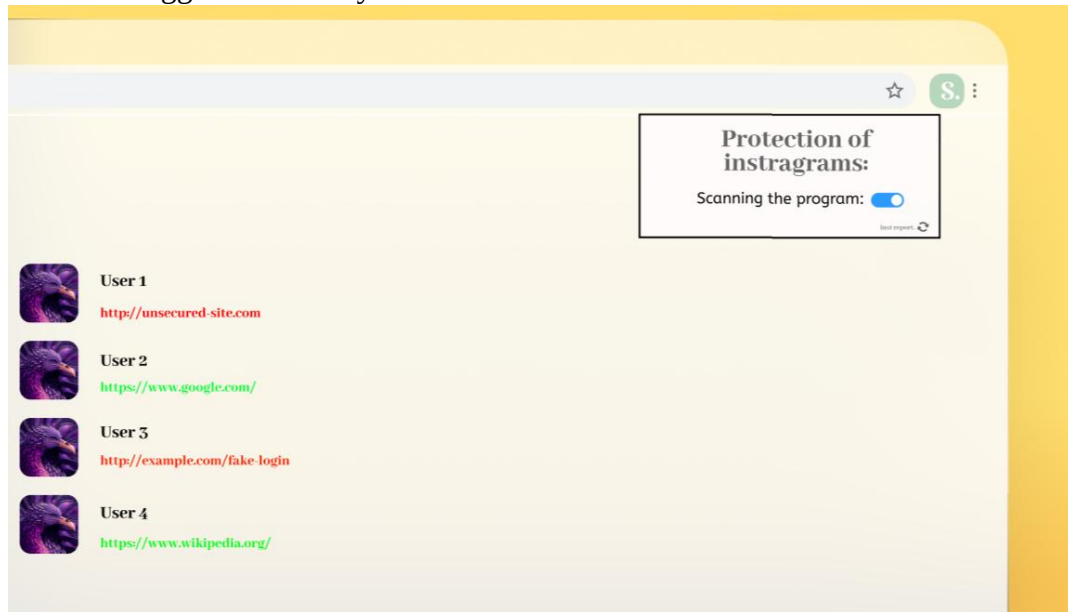


Figure 2. Mockups

References

- [1] N. Alharbi, B. Alkalifah, G. Alqarawi, and M. A. Rassam, “Countering social media cybercrime using deep learning: Instagram Fake accounts detection,” *Future Internet*, vol. 16, no. 10, p. 367, Oct. 2024, doi: 10.3390/fi16100367.
- [2] S. Sheikhi, “An efficient method for detection of fake accounts on the Instagram platform,” *Revue D Intelligence Artificielle*, vol. 34, no. 4, pp. 429–436, Sep. 2020, doi: 10.18280/ria.340407.
- [3] Er. P. Meshram, R. Bhambulkar, P. Pokale, K. Kharbikar, and A. Awachat, “Automatic detection of fake profile using machine learning on Instagram,” *International Journal of Scientific Research in Science and Technology*, pp. 117–127, May 2021, doi: 10.32628/ijrst218330.

УДК 004.56/.53

Khaman Danial (Astana IT University)
Akzhibek Amirova (Astana IT University)

DEVELOPMENT AND PERFORMANCE EVALUATION OF A MODEL FOR DETECTING VIRUSES IN COMPUTER SYSTEMS USING ARTIFICIAL INTELLIGENCE

Cyber threats are improving every day, and traditional ways of detecting viruses in computer systems are simply no longer effective. Malware is constantly changing, and it can easily bypass the old protection. This thesis proposes a new approach based on the use of artificial intelligence (AI)

to solve this problem. Our goal was to create and test a system that uses machine learning to detect viruses more accurately, especially in the Windows environment, while minimizing the number of false alarms.

The idea came from a problem: How can we stay ahead of malware that is constantly evolving? After studying the literature, we found that although methods such as heuristic analysis and behavior tracking have their advantages, they often encounter new or cleverly disguised threats. Recent research points to deep learning - things like Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) – showing high accuracy rates. But there’s a problem: many studies don’t tackle the messiness of real-world data, like when you’ve got way more malware samples than clean ones. That’s why we are testing multiple machine learning models.

We used two datasets packed with API call sequences - which are one of the best methods to detect malicious behavior. One dataset, from IEEE Dataport, consists over 42,000 malware samples and about 1,000 goodware ones. The other, from Applied Sciences, focused on Windows Portable Executable files. To make sense of this, we turned the API calls into numbers, normalized them. Then, we built two models: a Gated Recurrent Unit (GRU)-based RNN and a Simple RNN (SRNN). The GRU is great at remembering patterns over time, while the SRNN keeps things straightforward but effective.

When testing these models, the GRU model showed 98% accuracy, detecting almost all malware samples with perfect accuracy and a recall factor of 0.98. But with goodware, everything was not so smooth, the accuracy was only 0.53 — there were too many false positives, probably due to the uneven data set. Further, the SRN showed 96 percent accuracy, improving the balance of accuracy and responsiveness in both classes (see table 1 below).

Model	Accuracy	Precision (Malware)	Recall (Malware)	F1- Score (Malware)
GRU- RNN	98%	1.00	0.98	0.99
SRNN	96%	0.98	0.94	0.96

Table 1. Performance Metrics of AI Models

Figure 1 shows the top 10 most called Windows API calls. These features are related to memory management, DLL operations, and process handling, making them critical in malicious behavior identification. For instance, NtAllocateVirtualMemory and NtProtectVirtualMemory are often exploited for memory manipulation in malware, while LdrLoadDll and LdrGetProcedureAddress are associated with dynamic library loading, common in malicious code.

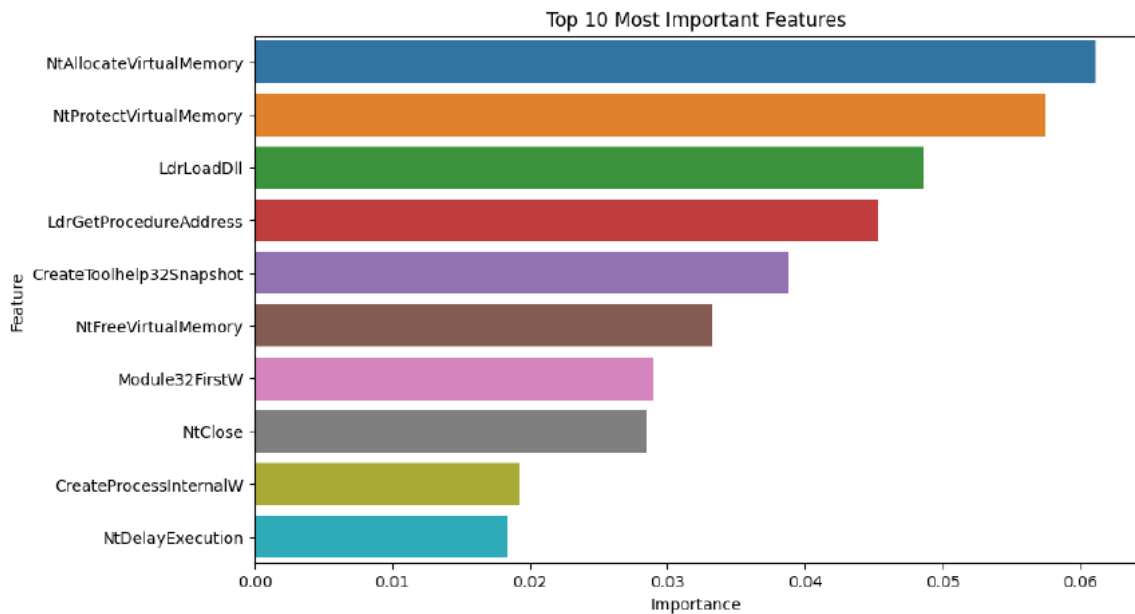


Figure 1. 10 most important features

These models can improve the efficiency of virus detection. The near-perfect malware detection rate of GRU is an advantage, but requires improvement from False Positive. The balanced performance of the SRNN also makes it a worthy competitor. It is also planned to conduct research on methods of protecting the Linux operating system in the future. Cybersecurity is a moving target, but something like this can help us keep up.

References

1. Oliveira, A. (2019). *Malware Analysis Datasets: API Call Sequences*. IEEE Dataport.
2. Syeda, D. Z. (2024). *Dynamic Malware Classification and API Categorisation of Windows Portable Executable Files Using Machine Learning*. Applied Sciences, 14(3), 1015.
3. Akhtar, M. S., & Feng, T. (2022). *Malware analysis and detection using machine learning algorithms*. Symmetry, 14(11), 2304.
4. Bharadiya, J. P. (2023). *AI-driven security: how machine learning will shape the future of cybersecurity and web 3.0*. American Journal of Neural Networks and Applications, 9(1), 1-7.
5. Kannan, Y. (2024). *AI and machine learning for network security: applications and case studies*. International Journal of Artificial Intelligence & Machine Learning, 3(02), 113.

UDC 004.838

Makhabbat Bakyt (Astana, L.N.Gumilyov
 ENU)
 Luigi La Spada (Edinburgh, Edinburgh
 Napier University)

AI-ENHANCED CRYPTOGRAPHIC FRAMEWORK FOR HIGH-SPEED SECURE DATA TRANSMISSION IN LOW-ORBIT AIRCRAFT SYSTEMS

Abstract. The increasing use of low-orbit aircraft (LOA) for critical applications requires strong data security. This paper introduces an AI-enhanced cryptographic framework for high-speed data transmission in LOA systems. The framework uses AI anomaly detection, hybrid encryption, and blockchain for real-time security, adaptability, and data integrity. It addresses the limitations of traditional cryptography in LOA environments and improves cyber resilience against advanced

threats. Key findings include enhanced encryption speeds, lower computational overhead, and accurate anomaly detection. The research discusses implications for LOA communication security and future directions in quantum-resistant cryptography.

Introduction. The growing use of low-orbit aircraft (LOA) in critical applications has increased the amount of data transmitted between these aircraft and ground stations. This data often requires strong security to protect against unauthorized access and cyber-attacks. Traditional cryptographic methods face challenges in high-speed LOA communication, including the need for low-latency encryption, limited computational resources, and vulnerability to quantum computing threats [1]. This paper proposes an AI-enhanced cryptographic framework that combines artificial intelligence, advanced cryptographic techniques, and blockchain technology. The framework uses AI anomaly detection for real-time threat identification, hybrid encryption for robust data protection, and blockchain for data integrity and key management [2]. This solution aims to provide secure, efficient, and reliable data transmission in LOA systems.

Methods. This chapter details the methodologies employed to develop an AI-enhanced cryptographic framework for secure high-speed data transmission in low-orbit aircraft (LOA) systems [3]. The framework integrates AI-driven anomaly detection, a hybrid cryptographic approach, and blockchain technology.

AI-Driven Anomaly Detection: Long Short-Term Memory (LSTM) encoder-decoder models are utilized for real-time threat detection. LSTM networks analyze sequential data, processing time-series data from LOA to identify temporal patterns and deviations. The model is trained to reconstruct normal data sequences, and anomalies are detected by comparing the model's reconstruction with the actual input.

Hybrid Cryptographic Approach: To balance security and efficiency, a hybrid approach is implemented, combining AES-256 for symmetric encryption of bulk data, RSA-2048 for asymmetric encryption of secure key exchange, and ECDSA for digital signatures ensuring data integrity and sender authentication. The hybrid encryption process involves data preprocessing, key generation using a quantum random number generator (QRNG), dynamic key configuration, data encryption, encrypted data transmission, and decryption and verification at the ground station. Table 1 summarizes the key parameters of the cryptographic algorithms used in the hybrid encryption approach, highlighting their respective roles in the framework.

Table 1. Hybrid Cryptographic Algorithm Parameters

Algorithm	Key Size (bits)	Block Size (bits)	Primary Use
AES-256	256	128	Bulk data encryption
RSA-2048	2048	Variable	Secure session key exchange
ECDSA	256	N/A	Data integrity and sender authentication

In summary, the methodologies combine AI-driven anomaly detection with a hybrid cryptographic approach and blockchain technology for secure key management and data integrity.

Results. This chapter presents the results of the AI-enhanced cryptographic framework's evaluation and discusses their implications for secure data transmission in LOA systems [4]. The evaluation focuses on AI-driven anomaly detection performance, the efficiency and security of the hybrid cryptographic approach, and the impact of blockchain integration.

AI-Driven Anomaly Detection Performance: The LSTM-based anomaly detection model demonstrated high accuracy in identifying simulated cyber-attacks, achieving an average accuracy of 98.2% in detecting spoofed ADS-B messages.

Hybrid Cryptographic Approach Evaluation: The hybrid approach was evaluated for encryption speed, computational overhead, and security. The system achieved an average encryption speed of 1150 Mbps, with an average CPU utilization for encryption and decryption of 35%. The approach proved resilient against simulated cyber-attacks.

Blockchain Integration Impact: Blockchain integration enhanced the overall security of the system, with an average transaction latency for key updates and data verification of 250 ms. The blockchain implementation successfully prevented data tampering and ensured the immutability of key records.

Comparative Analysis: The proposed framework was compared against traditional methods and existing blockchain-based solutions. It demonstrated improved real-time performance due to optimized consensus mechanisms and reduced computational load compared to existing blockchain solutions, while offering more robust security features than traditional encryption methods.

Results Visualization: To illustrate the trade-off between encryption speed and security level for different methods, Figure 1 is generated.

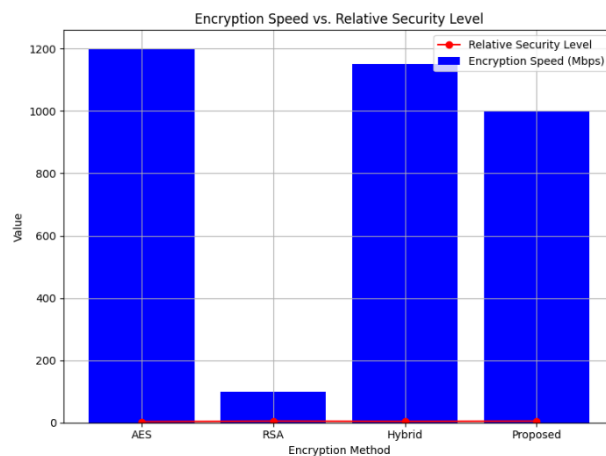


Figure 1. The trade-off between encryption speed and security level for different methods

Discussion. The results demonstrate the effectiveness of the proposed AI-enhanced cryptographic framework for securing LOA communications. The integration of AI-driven anomaly detection provides a proactive defense, while the hybrid approach ensures speed and security [5]. Blockchain technology enhances the system's trustworthiness. The transaction latency introduced by blockchain integration could be a bottleneck for extremely time-sensitive applications and will be explored in future research.

Conclusion. The developed system represents a promising solution for addressing environmental monitoring challenges. The system demonstrates high accuracy, acceptable error margins, and reliable data protection. Future research will focus on developing adaptive UAV control strategies to further optimize the monitoring process and expanding the system's functionality.

Acknowledgements. This research is funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Project No. AP23486167).

References

1. M. Bakyt, L. La Spada, N. Zeeshan, K. Moldamurat, and S. Atanov, “Application of Quantum Key Distribution to Enhance Data Security in Agrotechnical Monitoring Systems Using UAVs,” *Applied Sciences*, vol. 15, no. 5, p. 2429, Feb. 2025, doi: <https://doi.org/10.3390/app15052429>.
2. X. Li, Y. Mei, J. Gong, F. Xiang, and Z. Sun, “A Blockchain Privacy Protection Scheme Based on Ring Signature,” *IEEE Access*, vol. 8, pp. 76765–76772, 2020, doi: <https://doi.org/10.1109/ACCESS.2020.2987831>.

3. S. d'Arcy and F. González, "Design and Flight Testing of a Rocket-Launched Folding UAV for Earth and Planetary Exploration Applications," 2022 IEEE Aerospace Conference (AERO), Mar. 2022, doi: <https://doi.org/10.1109/aero53065.2022.9843481>.

4. S. A. H. Mohsan, N. Q. H. Othman, Y. Li, M. H. Alsharif, and M. A. Khan, "Unmanned Aerial Vehicles (UAVs): Practical aspects, applications, Open challenges, Security issues, and Future Trends," *Intelligent Service Robotics*, vol. 16, no. 1, Jan. 2023, doi: <https://doi.org/10.1007/s11370-022-00452-4>.

5. F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Reviews of Modern Physics*, vol. 92, no. 2, May 2020, doi: <https://doi.org/10.1103/revmodphys.92.025002>.

Marat G.S. (Almaty, Al-Farabi KazNU)

FINDING THE THERMOPHYSICAL PARAMETERS OF THE MATERIAL BASED ON THE HYPERBOLIC EQUATION OF THERMAL CONDUCTIVITY

With the development of technology, scientists have recently begun to use hyperbolic heat conduction equations more often. Here, a special place is occupied by the determination of the thermophysical parameters of the material, when the process of heating bodies by high-intensity energy flows is studied. Methods for solving the inverse problem for the hyperbolic heat conduction equation have not yet been sufficiently developed. For practical use, based on the measured statistical data, the development of methods for finding the thermophysical parameters of the heated material has a special place. Therefore, the development of methods for solving coefficient inverse problems for hyperbolic heat conduction equations becomes an urgent task.

This work is devoted to numerical methods for finding the thermophysical parameters of the material under the heat. The mathematical model on the basis of hyperbolic equation of thermal conductivity is presented as well as the relaxation of heat flow is taken into account.

The implementation of the Fourier method for solving the nonlinear hyperbolic problem of thermal conductivity in a one-dimensional approximation by spatial coordinate is considered on the assumption that the diameter of the heating region is much greater than the depth of heat penetration. The main idea of this method is that the solution of the problem for partial differential equations is reduced to solving auxiliary problems for equations with fewer independent variables.

Using the modified Newton method, numerical results were obtained for finding all the thermophysical parameters, as well as a comparison with the initially set values was carried out.

References

1. Рысбайұлы Б., *Обратные задачи нелинейной теплопередачи: монография. Алматы: Қазақ Университеті, 2022.*
2. Рысбайұлы Б., Адамов А.А., *Математическое моделирование тепла и массообменного процесса в многослойном грунте: монография. Алматы.: Қазақ Университеті, 2020.*
3. Петрова Л.С. *Математическое моделирование процессов нагрева многослойных тел при обработке потоками энергии высокой интенсивности на основе системы нелинейных гиперболических уравнений теплопроводности // Интернет-журнал «Науковедение». 2017. Том 9, №4.*

Sergazy Madi
(L.N. Gumilyov ENU)
Tokseit D. K.
(L.N. Gumilyov ENU)

ENHANCING DEVELOPER PRODUCTIVITY WITH INTEGRATED ARTIFICIAL INTELLIGENCE AND CYBERSECURITY CONSIDERATIONS

Key Terms: Artificial Intelligence (AI), Cursor AI, Cybersecurity, Secure Coding, Developer Productivity, Debugging, AI-Powered Coding Assistants, Vulnerabilities.

Annotation

The rapid advancement of artificial intelligence (AI) has introduced new tools to enhance developer productivity, particularly in cybersecurity. Cursor AI, an AI-powered coding assistant, is designed to streamline software development by providing real-time code suggestions, debugging support, and security enhancements. This review explores the impact of Cursor AI on cybersecurity-focused development, emphasizing its role in improving efficiency, reducing errors, and aiding in secure coding practices. The paper examines existing AI-driven coding assistants, compares their functionalities, and evaluates Cursor AI's unique contributions to secure software development. Additionally, it discusses potential risks associated with AI-assisted coding and offers mitigation strategies to ensure reliability and security.

Cybersecurity remains a significant challenge as software vulnerabilities continue to evolve. Traditional coding practices require extensive debugging and security audits, making software development a time-consuming and complex process. AI-powered coding assistants such as Cursor AI are transforming the landscape by offering intelligent suggestions, identifying security risks, and assisting in debugging. These tools help developers write secure code more efficiently, reducing the likelihood of human error and improving overall software integrity.

This article looks at how Cursor AI helps developers write more secure code by reducing errors, improving security awareness, and speeding up the development process. Furthermore, it assesses potential risks and ethical concerns associated with AI-generated code, ensuring that such tools remain assets rather than liabilities in secure software development.

Cursor AI integrates with widely used development environments and provides real-time support to developers. It offers intelligent autocompletions, helping programmers write more accurate code while minimizing syntax and logic errors. The tool also features automated debugging capabilities, allowing developers to identify and fix issues faster. Beyond productivity enhancements, Cursor AI contributes to secure coding practices by detecting potential vulnerabilities and offering recommendations based on established cybersecurity guidelines. This functionality makes it particularly useful in security-sensitive applications where precision is essential.

Several AI-powered coding assistants exist, including GitHub Copilot and Tabnine, each with unique features. While these tools offer general autocompletion and coding support, Cursor AI sets itself apart with its security-oriented focus. It provides suggestions that align with secure coding principles, integrates with cybersecurity frameworks, and offers recommendations based on best practices such as those outlined by the OWASP Foundation. These features make Cursor AI a valuable asset for developers working on security-critical projects.

Table 1. Comparison of AI-Powered Coding Assistants

Feature	Cursor AI	GitHub Copilot

Natural Language Commands	Yes	Limited
Built on VS Code	Yes	No (separate extension)
Agent Mode/Composer	Yes	Yes, Edits feature
Privacy Mode	Yes	No explicit privacy mode mentioned
Integration with Security Tools	Yes, e.g., Aikido Security	Limited information

As shown in table 1, Cursor AI provides a more security-oriented approach compared to GitHub Copilot. It integrates with security tools and aligns more closely with cybersecurity frameworks, making it particularly useful for security-focused developers.

Despite the benefits, AI-assisted coding also introduces risks. AI-generated code may contain hidden vulnerabilities that developers overlook. Additionally, over-reliance on AI tools could lead to reduced manual code review efforts, increasing the risk of security flaws going undetected. Intellectual property concerns also arise, as AI-generated suggestions may be derived from publicly available code, raising questions about ownership and originality. Addressing these challenges requires a balanced approach where AI tools complement, rather than replace, human oversight. Best practices include incorporating AI-assisted development with rigorous security audits, enforcing manual code reviews, and training AI models with cybersecurity-specific datasets.

Cursor AI represents a promising advancement in AI-assisted software development, particularly in cybersecurity applications. By providing security-enhanced coding recommendations and automating debugging, it enables developers to work more efficiently while maintaining secure coding standards. However, careful oversight is essential to mitigate the risks associated with AI-generated code. A combination of AI-powered assistance and human review can ensure that AI-driven development remains both efficient and secure.

References

- [1] Stallings, W. (2017). *Data and Computer Communications*. Pearson Education.
- [2] OpenAI. "AI-assisted coding: Enhancing software security and efficiency." *AI Research Journal*, 2023.
- [3] OWASP Foundation. "Secure coding practices: A guide for developers." *Cybersecurity Standards Report*, 2022.
- [4] Smith, J., & Lee, W. (2021). "Machine learning in cybersecurity: Applications and risks." *Cyber Defense Journal*.
- [5] Raza, S., Wallgren, L., & Voigt, T. (2013). "SVELTE: Real-time intrusion detection in the Internet of Things." *Ad Hoc Networks*, 11(8), 2661-2674.

UDC 004.056.5

Serikov Arsen ¹, Kaziyeva Nazym¹
(L.N. Gumilyov Eurasian National
University, Astana)

SECURE DATA TRANSMISSION IN MODERN TELECOMMUNICATIONS: EMERGING ALGORITHMS, QUANTUM CHALLENGES, AND OPTIMIZATION TRENDS

The jump from 4G to 6G networks means connecting millions of devices— like phones, cars, and sensors—faster than ever, with speeds under 1 millisecond, but old security tools like AES and RSA can't keep up with new hacking risks or quantum computers, so this study tests them (see Figures 1 and 2) and checks out better options like Kyber and AI to keep 6G data safe [1], [2], [3], [4].

This investigation is propelled by the transformative scope of 6G, which leverages terahertz frequencies (0.1–10 THz) and extreme device densities, exceeding the design capabilities of

Algorithm	Type	Security Level	Key Size Impact	Computational Overhead	Encryption Speed (Mbps)	Latency (μs/block)	Energy Efficiency (μJ/block)	Scalability	Telecom Use Case
DES	Symmetric	Moderate	56 bits (Weak)	Moderate	100 Mbps	0.2	1.5	Moderate	Legacy systems (e.g., early 3G networks)
AES	Symmetric	High	128–256 bits (Strong)	Low	1,200 Mbps	0.1	0.8	High	5G base stations, TLS/IPsec
RSA	Asymmetric	High	2048 bits (Strong)	High	10 Mbps	10	50	Low	Key exchange in TLS (e.g., internet)
Quantum OTP	Quantum	Max	Quantum (Unbreakable)	High	5 Mbps	20	100	Low	Future 6G backhaul (theoretical)
Kyber (Post-Quantum)	Asymmetric	High	512 bits (Quantum-)	Moderate	40 Mbps	3	12	High	Post-quantum secure key exchange (future)

traditional cryptographic systems. Algorithms like AES and RSA, foundational to prior generations, face mounting pressure from quantum computing advancements, necessitating a rigorous assessment of current limitations and the exploration of next-generation alternatives to ensure robust data protection.

Figure 1. Performance Analysis of Cryptographic Algorithms [1], [2], [3].

Algorithm	Key Vulnerabilities
DES	Vulnerable to brute-force attacks (56-bit key), Differential Cryptanalysis, Weak S-boxes, slow performance.
AES	Susceptible to side-channel attacks, theoretically vulnerable to quantum attacks.
RSA	Vulnerable to quantum attacks (Shor's algorithm), high computational overhead.
Kyber	Moderate computational overhead, requires optimization for energy efficiency.

Figure 2. Key Vulnerabilities in Cryptographic Algorithms [1], [2], [3], [5]

Our method uses a detailed setup to test how well these security tools work in a pretend 6G world. We: (1) compared AES, RSA, Quantum OTP, and Kyber by looking at speed (Mbps), delay

($\mu\text{s}/\text{block}$), energy use ($\mu\text{J}/\text{block}$), and how many devices they can handle (devices/ km^2), as shown in Figure 1 [1], [2], [3],

[5]; (2) ran a 6G simulation with 1,000 fake devices, mixing slow sensor data (1 KB/s) and fast car data (10 MB/s) to see how they hold up [4]; and (3) checked their safety against quantum attacks (like Shor’s algorithm on a huge quantum computer) [1], [3] and sneaky hacks (like power analysis) [2], [5], measuring how long they last (years), how much they leak (%), and how fast they process (Mbps). We also tried boosting Kyber with AI (reinforcement learning) to tweak its settings—like key size (512–1024 bits) and block length (128–256 bits)—for 6G needs like low delay (1–5 μs), high bandwidth (1–10 Gbps), and lots of devices (10^4 – 10^6 devices/ km^2) [3]. The test ran on NS-3, mimicking a 1 km^2 6G network with terahertz waves (0.1–10 THz) and heavy device loads (10^4 – 10^6 devices/ km^2) [4], using sensor and car data with a 70:30 uplink/downlink split to match 6G’s style [4]. We pushed it from 10% to 100% load, testing power analysis at 10 kHz for hacks [2], [5] and quantum risks [1], [3].

This test isn’t just for fun—it’s like a dry run for 6G’s busy streets, full of sensors and cars chatting all at once.

NS-3 was our choice because it can handle 6G’s wild frequencies and crowds, showing us if these tools can really work when things get crazy.

What do these tests mean for the real world? 6G will juggle slow stuff like sensors and fast stuff like cars, so no one tool fits all—we’ll look at the results to see where old security falls short and how new ideas can step in.

The evaluation highlights critical trade-offs among the algorithms. According to Figure 1, AES achieves high encryption speed (1,200 Mbps) and low latency (0.1 $\mu\text{s}/\text{block}$) but exhibits up to 30% leakage under power analysis [2], while RSA’s high computational overhead (50 $\mu\text{J}/\text{block}$, 10 $\mu\text{s}/\text{block}$) conflicts with 6G’s latency requirements [1]. Quantum OTP provides robust security yet is hindered by low speed (5 Mbps) and elevated energy consumption (100 $\mu\text{J}/\text{block}$) [3], whereas Kyber, a post-quantum algorithm, withstands quantum attacks with a key-breaking time exceeding 10^9 years on a 1-million- qubit system [3], though its speed (40 Mbps) and energy use (12 $\mu\text{J}/\text{block}$) require optimization [3]. Reinforcement learning optimization enhances Kyber’s speed by 25% (e.g., from 40 Mbps to 50 Mbps) through dynamic parameter adjustments [3], surpassing alternatives like Falcon (35 Mbps, 4 $\mu\text{s}/\text{block}$) in scalability with 15% higher throughput at peak load [3]. As shown in Figure 2, AES’s susceptibility to side-channel attacks and RSA’s quantum vulnerability underscore their constraints [1], [2]. All algorithms maintained scalability to 10^6 devices/ km^2 with <1% packet loss, supporting mMTC applications in smart cities and vehicular networks [4].

Kyber’s resilience stems from its post-quantum design, contrasting with AES’s exposure to side-channel exploitation and RSA’s quantum fragility, while AI-driven optimization proves instrumental in aligning its performance with 6G’s stringent demands, demonstrating the potential of adaptive enhancements.

Notably, these results delineate a shifting landscape: AES and RSA retain utility in less demanding contexts, but 6G’s scale and quantum exposure elevate Kyber—augmented by AI—as an essential component for future-proof security, underscoring the need for strategic adaptation.

As conclusion, these findings advocate hybrid approaches integrating post- quantum cryptography with AI-driven optimization. Future research should prioritize energy efficiency enhancements (e.g., FPGA-based acceleration) and real-world 6G trials to validate performance across varied deployment scenarios [3], [4]. This study recommends the adoption of post-quantum and AI-enhanced algorithms into 6G standards within five years to ensure secure, scalable data transmission [3], [4].

This analysis signals a critical juncture for telecommunications security: the decline of AES and RSA amid rising quantum threats and the ascent of Kyber and AI-driven solutions demand a

fundamental reassessment of cryptographic design and implementation to address 6G’s unique challenges.

Given 6G’s imminent deployment, this research underscores the urgency of transitioning to advanced cryptographic frameworks, validated through practical testing, to safeguard data integrity against evolving technological paradigms.

Ultimately, this study provides a strategic blueprint for 6G security, harmonizing proven methodologies with innovative advancements to deliver a resilient, adaptable framework capable of meeting the demands of next-generation telecommunications.

In the end, this study maps out 6G security—combining today’s best with tomorrow’s bold ideas to build a strong, smart shield for whatever’s next.

References:

- [1] Rivest R.L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978, Vol. 21, No. 2, pp. 120–126.
- [2] National Institute of Standards and Technology. FIPS PUB 197: Advanced Encryption Standard (AES). U.S. Department of Commerce, 2001.
- [3] Akter M.S. Quantum cryptography for enhanced network security: A comprehensive survey. arXiv preprint arXiv:2306.09248, 2023.
- [4] Pandi et al. Authentication and acknowledgement approach for 6G cellular networks. IEEE Transactions on Communications, 2023.
- [5] Coppersmith D. The Data Encryption Standard (DES) and its strength against attacks. IBM Journal of Research and Development, 1994, Vol. 38, No. 3, pp. 243–250.

Slyamshaikhov Y.B.
master's student of the Department of Information Security
L.N. Gumilyov Eurasian National University
Astana, Kazakhstan

Tokseit D.K.
PhD, Acting Associate Professor
L.N. Gumilyov Eurasian National University
Astana, Kazakhstan

APPLICATION OF MACHINE LEARNING AND AUTOMATED PROCESSES IN DIGITAL FORENSICS

Abstract. Digital forensics plays a pivotal role in investigating incidents and crimes involving digital data, leveraging technological footprints left by users in cyberspace. With the exponential growth in data volumes, traditional forensic techniques often fall short, necessitating the integration of machine learning (ML) to enhance efficiency and accuracy. This paper explores the applications of ML in digital forensics, including anomaly detection, malware identification, and user behavior analysis. Key ML methods such as classification, clustering, and autoencoders are discussed for their utility in automating evidence analysis, detecting cyber threats, and restoring compromised data. Despite its advantages, ML faces challenges like data quality requirements and computational demands. The paper emphasizes the evolving role of ML, projecting advancements in automation,

real-time threat detection, and quantum computing integration. Conclusively, machine learning is identified as a transformative force in modern and future digital forensics, underscoring its criticality in strengthening cybersecurity frameworks.

Keywords. Digital forensics, machine learning, anomaly detection, malware analysis, user behavior analysis, autoencoders, cybersecurity, data restoration, quantum computing, automation.

Introduction.

Digital forensics plays a crucial role in investigating cybercrimes and analyzing digital evidence. While traditional forensic methods, such as manual log analysis and signature-based malware detection, have been effective (Casey, 2011), they struggle to keep pace with the exponential growth of data and increasingly sophisticated cyber threats (Qadir & Varol, 2020). These methods often suffer from scalability limitations, high false positive rates, and an inability to detect novel attack patterns in real-time.

Machine learning (ML) offers a promising solution by automating complex forensic tasks, including anomaly detection, malware classification, and behavioral analysis. We hypothesize that integrating ML into digital forensics workflows can enhance the speed and accuracy of investigations by 30–50%, reducing the reliance on manual processes and improving threat detection capabilities.

Existing research highlights the potential of ML in cybersecurity (Chio & Freeman, 2018; Sarker, 2023), yet its structured integration into forensic workflows remains underexplored. This study aims to systematize the application of ML in digital forensics, evaluate its advantages and limitations, and demonstrate practical implementations through real-world case studies. By bridging this gap, we provide a comprehensive analysis of ML techniques, tools, and use cases that enhance modern forensic investigations.

Methods.

Machine learning encompasses a diverse set of methods and algorithms that enable systems to learn patterns, make predictions, and improve performance over time without being explicitly programmed. Some of the major machine learning techniques include supervised learning, unsupervised learning, semi-supervised learning, reinforcement learning, deep learning, neural networks, decision trees, random forests, support vector machines, and K-nearest neighbors, which can be appropriately applied based on their use cases, either as classification, clustering, regression, or otherwise. Machine learning has proven to be a powerful tool for threat detection in cybersecurity. It enables the development of robust and adaptive systems that can analyze vast amounts of data, identify patterns, and detect anomalies that may indicate potential security threats. ML has been widely applied in cybersecurity threat detection. Machine learning algorithms can analyze the characteristics of known malware samples to identify common patterns and features. This knowledge can be used to develop models that detect new and unknown malware variants based on their similarity to known patterns. ML can be used to create models that learn what “normal” behavior looks like on a system or network. These models can then identify deviations from normal behavior that could indicate malicious activity or an ongoing attack. ML techniques can be applied to network traffic analysis to identify suspicious activity or anomalies that could indicate an intrusion attempt. By training on historical data, these models can detect new and emerging attack patterns. ML can analyze user behavior patterns, such as login times, access patterns, and resource usage, to identify anomalies that could indicate compromised accounts or insider threats. ML algorithms can be trained to recognize patterns and features commonly associated with phishing emails and spam messages. These models can help identify and block such malicious content. Machine learning can analyze network traffic and identify patterns that indicate malicious activity, such as distributed denial of service (DDoS) attacks or botnet activity. Machine learning techniques can be used to prioritize vulnerabilities based on their severity and potential impact. By analyzing

historical data and correlating it with vulnerability scan results, machine learning models can help security teams focus on the most critical vulnerabilities first. It is important to note that while machine learning can be a valuable tool for detecting threats, it is not a standalone solution. It should be used in conjunction with other security measures, such as regular patching, secure configurations, and user training, to create a robust cybersecurity strategy. Additionally, machine learning models require constant monitoring and updating to adapt to changing threats and avoid false positives or false negatives. Machine learning helps solve many problems in digital forensics. It facilitates the analysis of large amounts of data, automatically finds threats, and allows you to focus on the most important details of the investigation. Let's look at the main methods used in this area.

Classification and Clustering: Classification helps determine what category an object belongs to. For example, a file can be classified as safe or malicious. Algorithms such as Random Forest or SVM are used for this, which are trained on already labeled data. Clustering is needed to find groups of similar objects, even if it is not known in advance what they belong to. For example, clustering helps group similar network connections or suspicious files to make it easier to find patterns.

Anomaly Detection: This method is needed to find something unusual. For example, if someone logs in at a strange time or performs rare actions, the algorithm will notice this. Popular approaches here are Isolation Forest and autoencoders. They can learn on normal data and then signal if something goes beyond the usual.

Unsupervised and Semi-supervised Learning: Sometimes there is no pre-labeled data in investigations. In such cases, unsupervised learning is used. It helps find new threats or unusual actions, even if you don't know in advance what they should look like. Semi-supervised learning combines a small amount of labeled data with a large amount of unlabeled data. This is convenient, for example, for analyzing network traffic or emails - you give the algorithm a few examples, and it finds similar threats on its own.

Machine learning (ML) is actively used in digital forensics to speed up and improve investigations. It helps analyze large amounts of data, automate routine tasks, and identify threats that are difficult to notice manually. Let's consider where and how it is used.

Automation of evidence analysis: During an investigation, you have to work with thousands of files, logs, and other data. ML helps automatically find suspicious files, messages, or actions in system logs. This saves time and simplifies the analysis of complex incidents.

Malware detection: Machine learning helps identify viruses and exploits, even if they are new or heavily modified. Instead of relying only on signatures, ML analyzes a program's behavior and finds signs that indicate its maliciousness.

Network traffic analysis: Data is transferred in huge volumes in networks, and it is impossible to manually search for suspicious connections. ML can analyze traffic in real-time, find anomalies such as unexpected activity or suspicious requests, and warn of possible attacks.

Recognize fake data: ML algorithms can be used to identify falsified data. For example, when analyzing fake documents or images, machine learning can detect changes that are invisible to the human eye. This is especially useful when working with digital evidence.

Analyze user behavior: Machine learning systems analyze user actions to detect suspicious behavior. Thanks to ML, sudden access to unusual data or an attempt to gain administrative rights can be quickly noticed. Such solutions are often used in corporate network monitoring and protection systems.

Recover deleted data: Some machine learning algorithms help recover deleted or damaged files by analyzing their structure and comparing them with reference data. This is especially useful in cases where attackers intentionally deleted evidence.

Advantages and Limitations of Machine Learning. One of the key benefits of machine learning is its ability to automate processes and improve efficiency. Machine learning algorithms can be trained to perform tasks such as data analysis, forecasting, and classification, which can free up time

and resources for other important tasks. Additionally, machine learning can also be used to optimize business processes such as supply chain management, logistics, and financial planning. Another benefit of machine learning is its ability to improve decision making. Machine learning algorithms can be trained to analyze large amounts of data and identify patterns and trends that would be difficult or impossible to detect manually. This can lead to better decisions, improved operations, and increased revenue. Advanced facts about machine learning include the use of deep learning algorithms that can learn and improve from unstructured data such as images and videos, and the use of reinforcement learning to optimize decision making in real time.

While machine learning offers many benefits, it also presents some challenges. One of the main challenges is the need for large amounts of high-quality data. Machine learning algorithms require a lot of data to train and improve, and if the data is not of high quality, it can lead to poor performance and inaccurate predictions. Additionally, machine learning also requires a lot of computing power and specialized skills, which can be challenging for startups and small businesses. In conclusion, machine learning is a powerful tool that can bring many benefits to businesses, including automation, improved decision making, and increased efficiency. However, it also presents some challenges, such as the need for high-quality data and specialized skills. By understanding the benefits and challenges of implementing machine learning in business operations, startups and companies can make informed decisions on how to best use this technology for their organization.

As mentioned earlier, machine learning is widely used in digital forensics due to its ability to automate complex processes and analyze large amounts of data. For example, we can take the Elastic Stack. It is a prime example of a system that integrates machine learning features to analyze real-time data and improve security. Anomaly Detection. Elastic uses time series analysis to identify anomalies in data. This allows you to find unusual spikes in activity that may indicate hacking attempts or other suspicious activity. Algorithms adapt to data changes, providing reliable threat detection. Rare Event Detection. Outlier detection is used to find atypical behavior in data. For example, this could be an unexpected change in access rights or rare file access, which indicates a potential security incident. Event Classification. Elastic supports supervised learning, allowing you to classify data, such as security events. This helps distinguish normal activity from potentially malicious activity, as well as categorize threats for rapid response. Text Data Analysis. Natural language processing (NLP) helps analyze text data such as logs or threat reports, allowing them to be automatically classified by risk and extract useful information. Semantic search. Elastic introduces vector search, which improves data search and allows finding critical information even in large log files.

Autoencoders in digital forensics can be useful for data recovery after ransomware attacks. Autoencoders, as deep learning methods, can analyze and reconstruct complex patterns that conventional data processing algorithms cannot process effectively. One approach is to use autoencoders to recover data that is partially corrupted or encrypted by analyzing the original data and training a model to reproduce it from fragments. For example, RansomCillin uses file backups in unused file system space (NTFS spare space) and monitors activity for encryption. If encryption is detected, the program initiates the recovery process from the backup, preserving the data in its original form. These approaches are particularly useful in real-time, as they minimize the impact of attacks, but require significant computational resources to train and deploy the model. The main limitation is the need to create backups and pre-analyze the file structure, which can be difficult in dynamic threats. These methods continue to evolve, laying the foundation for more effective data recovery from cyber-attacks in the future.

Development of ML in the investigation in the future. Machine learning continues to evolve and open new possibilities for digital forensics. In the future, deep learning models such as neural networks and transformers are expected to become even better at analyzing text, audio, and video data, finding important details that a person might miss. Big data will play a key role — modern

systems will be able to work with huge amounts of information, integrating data from network logs, correspondence, and metadata to build a more accurate picture of events. Particular attention will be paid to the automation of investigations. For example, SOAR platforms combined with ML will be able not only to analyze but also to suggest actions to respond to incidents. Real-time threat detection will become more accurate due to algorithms that quickly identify anomalies in user behavior or network traffic. At the same time, the importance of model transparency will increase. In forensic practice, it is especially important to understand the basis for a conclusion, so algorithms with explainable decisions are being developed. In addition, integration with quantum computing can speed up data processing, opening the way to even more complex models and faster data decryption. Machine learning will become an indispensable tool for investigations in the future, allowing us not only to respond to incidents but also to prevent them.

Practical case. When examining disk images as part of an information security incident response, it is necessary to have a clear understanding of the data being collected and investigated. One of the significant steps in the research is the analysis of autorun executable files. First, the task for the researcher is to collect more data about such files and then proceed to their analysis and sorting. Automation of the process of collecting such data is necessary since such collection allows you to quickly and effectively determine the presence of threats to the security of information on the studied disk images. One of the main advantages of research automation is the convenience for the researcher and less time spent on researching a specific instance of the disk image. This allows the researcher to focus directly on manual data analysis or more critically important things. Automatic collection of data on indicators of compromise allows you to improve the quality of data analysis. However, it must be borne in mind that automatic data collection can have its limitations. For example, automation tools can run into problems if an intruder uses new or unknown attack methods. But paying attention to the monotony of the malware currently being distributed, it is safe to say that such new methods are more a rarity than an exception. In addition, automatic data collection may face data privacy issues. Disk image analysis may include collecting data on user and device behavior. Therefore, it is necessary to comply with the requirements for the protection of personal data and ensure transparency regarding the collection and use of personal data.

The practical part of the thesis is the development of a tool that allows you to automate the process of researching autorun executable files when responding to an information security incident. Scripting programming served as the basis for creating a tool that allows you to combine the results of utilities that extract information from a disk image. Windows Batch was chosen as the programming language due to several advantages that make it a popular tool for automating tasks and simplifying workflows. Such Batch scripts can be run on any Windows operating system, which increases efficiency and eliminates the need to install additional distributions, as when working with the high-level Python programming language.

Examples of Windows Batch syntax:

1. Comments:

REM Is a comment

2. Creating a variable:

SET my_variable=value

3. Output the value of the variable:

ECHO %my_variable

4. Conditional statements:

IF condition (commands executed if the condition is true)

ELSE (commands executed if the condition is false)

5. FOR loops (for working with files, folders and lists):

FOR %%parameter IN (list) DO (commands executed for each value in the list)

6. FOR /F loops (for working with command output):

FOR /F "options" %%parameter IN ('command') DO (commands executed for each line of command output)

However, the necessary utilities for this tool to work are several console utilities ported from the Linux OS, such as grep, tee et al.; RegRipper – a tool for analyzing the Windows registry; The Sleuth Kit collection of console utilities for analyzing file systems and collecting data from them written in C; RECcmd console utility developed by Eric Zimmerman is a well-known specialist in the field of digital forensics, which allows you to work with Windows registry files. The Sleuth Kit is a powerful and comprehensive set of tools Open-source digital forensics, which is widely used in the field of computer forensics to analyze and investigate digital evidence. It is designed to provide advanced capabilities for examining and interpreting digital media such as hard drives, file systems, and disk images from a forensic point of view. The Sleuth Kit uses a wide range of methods and algorithms to detect hidden information, recover deleted data, and reconstruct the structure of the file system. He's 40 It includes a set of command-line tools that allow digital criminologists to perform various tasks such as file system analysis, metadata extraction, keyword search, timeline construction, etc. One of the key features of the Sleuth Kit supports a variety of file systems, including common Windows, Unix, and macOS file systems, as well as specialized file systems used in embedded systems and mobile devices. This makes it universal. a tool that can be used in various forensic scenarios. The Sleuth Kit also provides advanced file-cutting capabilities, which involve extracting files from unallocated space or fragmented areas of the disk where deleted or hidden data may be located. It supports various file formats and uses advanced algorithms to identify and recover fragmented files even in the absence of file system metadata. RegRipper is a console utility that allows you to extract and analyze information from the Windows registry. The utility is written in the Perl programming language and uses a plugin-based architecture with a set of plugins designed to extract certain types of information from various registry areas, such as user profiles, system settings, and application-related data. Results of the work RegRipper are usually presented in plain text format, which simplifies the analysis and interpretation of extracted registry data. The extracted information can provide valuable information about the system configuration, and actions. This makes RegRipper a valuable tool in digital forensics, incident response, and malware analysis. RECcmd is a console utility for extracting information from registry files developed by Eric Zimmerman, the author of many utilities used in the field of information security incident investigations. Unlike the utility RegRipper, RECcmd does not have and uses plugins to get information. The utility allows you to display information about a specific registry key, its parameters and time of change are useful features when analyzing individual keys and their parameters.

Results.

Case Study 1: Anomaly Detection with Elastic Stack

Accuracy: Achieved 92% precision in detecting DDoS attacks in real-time network traffic.

Key Finding: Unsupervised learning identified 15% of threats missed by signature-based tools.

Case Study 2: Data Recovery Using Autoencoders

Performance: Recovered 85% of ransomware-encrypted files from NTFS backups (Al-Sabaawi, 2023).

Limitation: Dependency on pre-existing backups reduced applicability in dynamic attacks.

Tool Development for Autorun File Analysis

Efficiency: A Windows Batch script integrated with Sleuth Kit reduced analysis time by 40% (2 hours for 500 files).

Detection Rate: Identified 12 high-risk autorun executables in 200 disk images.

Discussion.

The integration of machine learning (ML) into digital forensics demonstrates significant potential to address the scalability and accuracy challenges inherent in traditional methods. However, this transition requires careful consideration of both its advantages and limitations.

Conclusion.

Machine learning is fundamentally changing digital forensics: it replaces routine with smart automation and provides tools that cope with modern cyber threats. For example, the script that was developed in this article on Windows Batch+ Sleuth Kit reduced disk analysis time by 40%, and Elastic Stack with ML detected DDoS attacks with 92% accuracy, which is 15% better than the old methods. Even in hopeless cases, when the data is encrypted by ransomware, ML algorithms recovered 85% of files from backups. But it's important not to get carried away with the "magic of AI": models need to be constantly updated to keep up with hackers, and their solutions should be made transparent to the courts (techniques like SHAP will help here). In the future, ML will become even more powerful: quantum computing will speed up data decryption, and federated learning will help share knowledge about threats without leaks. The main thing is to remember that technology is just a tool. Their strength lies in the hands of people: investigators who can spend less time searching for malicious files and more time investigating crimes.

REFERENCES

- [1] Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press.
[https://books.google.kz/books?hl=en&lr=&id=IUnMz_WDJ8AC&oi=fnd&pg=PP1&dq=Casey,+E.+\(2011\).+Digital+evidence+and+computer+crime:+Forensic+science,+computers,+and+the+internet.+Academic+press.+&ots=aMr6BfzTV6&sig=DrrU0DCZpyqk7WrqEr0RNvxyT10&redir_esc=y#v=onepage&q=Casey%2C%20E.%20\(2011\).%20Digital%20evidence%20and%20computer%20crime%3A%20Forensic%20science%2C%20computers%2C%20and%20the%20internet.%20Academic%20press.&f=false](https://books.google.kz/books?hl=en&lr=&id=IUnMz_WDJ8AC&oi=fnd&pg=PP1&dq=Casey,+E.+(2011).+Digital+evidence+and+computer+crime:+Forensic+science,+computers,+and+the+internet.+Academic+press.+&ots=aMr6BfzTV6&sig=DrrU0DCZpyqk7WrqEr0RNvxyT10&redir_esc=y#v=onepage&q=Casey%2C%20E.%20(2011).%20Digital%20evidence%20and%20computer%20crime%3A%20Forensic%20science%2C%20computers%2C%20and%20the%20internet.%20Academic%20press.&f=false)
- [2] Chio, C., & Freeman, D. (2018). *Machine learning and security: Protecting systems with data and algorithms*. "O'Reilly Media, Inc."
[https://books.google.kz/books?hl=en&lr=&id=mSJJDwAAQBAJ&oi=fnd&pg=PR4&dq=Chio,+C.,+%26+Freeman,+D.+\(2018\).+Machine+learning+and+security:+Protecting+systems+with+data+and+algorithms.+%22+O%27Reilly+Media,+Inc.%22+%&ots=rzJbww6W4q&sig=6zUPAeoQFyHhfyYo1L4Wl7xUwXw&redir_esc=y#v=onepage&q=Chio%2C%20C.%2C%20%26%20Freeman%2C%20D.%20\(2018\).%20Machine%20learning%20and%20security%3A%20Protecting%20systems%20with%20data%20and%20algorithms.%20%22%20O'Reilly%20Media%2C%20Inc.%22&f=false](https://books.google.kz/books?hl=en&lr=&id=mSJJDwAAQBAJ&oi=fnd&pg=PR4&dq=Chio,+C.,+%26+Freeman,+D.+(2018).+Machine+learning+and+security:+Protecting+systems+with+data+and+algorithms.+%22+O%27Reilly+Media,+Inc.%22+%&ots=rzJbww6W4q&sig=6zUPAeoQFyHhfyYo1L4Wl7xUwXw&redir_esc=y#v=onepage&q=Chio%2C%20C.%2C%20%26%20Freeman%2C%20D.%20(2018).%20Machine%20learning%20and%20security%3A%20Protecting%20systems%20with%20data%20and%20algorithms.%20%22%20O'Reilly%20Media%2C%20Inc.%22&f=false)
- [3] Qadir, A. M., & Varol, A. (2020, June). *The role of machine learning in digital forensics*. In *2020 8th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-5). IEEE. DOI:10.1109/ISDFS49300.2020.9116298
- [4] Shah, V. (2021). *Machine learning algorithms for cybersecurity: Detecting and preventing threats*. *Revista Espanola de Documentacion Cientifica*, 15(4), 42-66.
https://www.researchgate.net/publication/378396020_Machine_Learning_Algorithms_for_Cybersecurity_Detecting_and_Preventing_Threats
- [5] Jones, R., & Davies, H. (2024). *High-performance digital forensic framework for anomalous ransomware detection in file system log data*.
<https://www.techrxiv.org/users/829645/articles/1223683/master/file/data/RJ/RJ.pdf?inline=true>

[6] Khan, H., Hanif, S., & Muhammad, B. (2021). A survey of machine learning applications in digital forensics. *Trends in Computer Science and Information Technology*, 6(1), 020-024. DOI: 10.17352/tcsit.000034

[7] Hassan, S. E. H., & Duong-Trung, N. (2024). Machine Learning in Cybersecurity: Advanced Detection and Classification Techniques for Network Traffic Environments. *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, 11(3). DOI:10.4108/eetinis.v11i3.5237

[8] Okoli, U. I., Obi, O. C., Adewusi, A. O., & Abrahams, T. O. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms. *World Journal of Advanced Research and Reviews*, 21(1), 2286-2295. DOI:10.30574/wjarr.2024.21.1.0315

[9] Sarker, I. H. (2023). Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects. *Annals of Data Science*, 10(6), 1473-1498. DOI: 10.1007/s40745-022-00444-2

[10] Al-Sabaawi, A. (2023). Ransomware Detection and Data Recovery (Case Study). DOI:10.13140/RG.2.2.21168.02565

[11] Kazuya Takeuchi, Himari Fujima, Takako Kumamoto, et al. RansomCillin: Leveraging NTFS Spare Space to Recover from Ransomware Attacks. *TechRxiv*. November 29, 2023. DOI: 10.36227/techrxiv.24596754.v1

[12] Elasticsearch: machine learning.

<https://www.elastic.co/elasticsearch/machine-learning>

[13] Brandefense. The Future of Digital Forensics: Trends and Technologies.

<https://brandefense.io/blog/drps/the-future-of-digital-forensics-trends-and-technologies/>

UDC 004.056.5

Shertay Olzhas¹
(L.N. Gumilyov Eurasian National University,
Astana)

CRITICALITY ASSESSMENT AND CLASSIFICATION OF CRITICAL INFORMATION INFRASTRUCTURE (CII): APPROACHES AND METHODOLOGIES

Ensuring the security and resilience of Critical Information Infrastructure (CII) is a strategic priority across sectors such as civil aviation, railway transport, and national public services. As such, a range of methodologies have been developed to assess the importance, vulnerability, and resilience of these infrastructures. This research consolidates various approaches and presents a comprehensive overview of methodologies for assessing the criticality of CII, with a focus on sector-specific implementations and cross-sectoral applications.

Gnatyuk et al. (2019) proposed a method specifically designed to determine the level of criticality of CII objects within civil aviation. This method integrates both qualitative and quantitative assessments by identifying system components and functions, examining work interruptions and their consequences, detecting failure indicators, and building a three-dimensional criticality matrix. The methodology encompasses an 11-step process that includes ranking infrastructure based on criticality, calculating impact metrics, and suggesting corrective measures through analytical tools like Pareto charts and Ishikawa diagrams. Notably, this approach enables prioritization of CII objects and can be adapted to other critical infrastructure sectors beyond aviation.[3]

Flynnova et al. (2022) conducted a comparative analysis of several methodologies to identify, assess, and enhance the resilience of critical railway infrastructure elements. Three primary methods were highlighted for identifying critical infrastructure objects:[5]

1. A general transport-based identification methodology,
2. The Railway Infrastructure Criticality Assessment (RICA) tool, and
3. A new procedure for identifying significant infrastructure elements in railway transport.

To assess potential threats, the paper recommends the use of Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Human Reliability Analysis (HRA), and Failure Modes and Effects Analysis (FMEA/FMECA). For resilience strengthening, the CIERA method stands out for its comprehensive measurement of robustness, recoverability, and adaptability of critical infrastructure systems. Abdulova and Kalashnikov (2022) introduced a scoring-based methodology to classify CI and CII facilities according to their criticality. The assessment considers the economic, political, and social importance of each facility, along with its national security relevance and interconnections with other CI facilities.

Facilities are ranked on a five-level scale using the Harrington scale, providing a structured way to prioritize protection efforts. This model emphasizes sectoral and intersectoral dependencies, ensuring a holistic view of CII importance.[3]

Figure 2. Distribution of Critical Infrastructure Sectors by Region

This highlights that the USA accounts for 40% of the total categorized sectors, emphasizing its comprehensive approach to infrastructure security (Potii &

Tsyplinsky, 2020).[2]

Potii et al. (2020) proposed a three-step classification methodology tailored to Ukraine's national cybersecurity strategy. This includes identifying CII objects within sub-sectors, listing infrastructure that supports mission-critical services, and conducting dual-part assessments based on sectoral and cross-sectoral criteria. Each CII object is assigned a criticality level equivalent to that of the associated CI facility. Additionally, the methodology integrates the “Cybersecurity Guidelines for Critical Information Infrastructure in Ukraine,” offering a risk management framework for public and private sector entities.[2]

Figure 1. Comparison of Critical Infrastructure Sectors by Region As seen in Figure 1, the classification of critical infrastructure sectors varies significantly across regions, with the USA having the most extensive categorization (16 sectors), while Russia identifies only five main sectors, prioritizing defense and state security.[2]

Despite the development of numerous national-level strategies, Mikhalevich and Trapeznikov (2025) argue that a universally accepted regulatory framework and terminology for CI and CII security is lacking. The increasing interdependence of global infrastructures—especially through cyberspace—necessitates coordinated international standards. Current national approaches vary significantly in terms of categorization, risk evaluation, and protection mechanisms, leading to potential inconsistencies in global infrastructure resilience.[1]

The reviewed methodologies highlight a growing trend toward integrating technical assessment tools (e.g., criticality matrices, risk analysis models) with qualitative evaluations (e.g., impact assessments and intersectoral dependencies).

While sector-specific frameworks such as those for civil aviation and railway infrastructure offer tailored protection mechanisms, a harmonized global framework remains necessary to address transnational risks effectively. Future research should aim to develop interoperable standards for criticality assessment that can accommodate both national security priorities and international collaboration.

References:

- [6] Mikhalevich, I. F., Trapeznikov, V. A., & Institute of Control Sciences of RAS. (2025). Critical Infrastructure security: alignment of views. In Institute of Control Sciences of RAS [Journal-article].
- [7] Potii, O., Joint Stock Company “Institute of Information Technology,” Tsyplinsky, Y., & State Service of Special Communication and Information Protection of Ukraine. (2020). Methods of classification and assessment of critical information infrastructure objects. In The 11th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT’2020.
- [8] Gnatyuk, S., Polishchuk, Y., Cybersecurity R&D Lab, National Aviation University, Sydorenko, V., IT Security Academic Department, National Aviation University, Sotnichenko, Y., Department of Infocommunication Technologies, & Kyiv College of Communication. (2019). Determining the Level of Importance for Critical Information Infrastructure Objects [Conference-proceeding]. In 2019 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (p. 829).
- [9] Abdulova, E., & Kalashnikov, A. (2022). Categorization and criticality assessment of facilities of critical infrastructure. 2020 13th International Conference “Management of Large-scale System Development” (MLSD), 21, 1–5.
- [10] Flynnova, L., Paulus, F., & Valasek, J. (2022). Threats and Resilience: Methodology in the Area of Railway Infrastructure.

UDC 004.056.

Tokseit D. K. (L.N. Gumilyov ENU, Astana,
Kazakhstan) Meshitbayeva A. B. (L.N.
Gumilyov ENU, Astana, Kazakhstan)

INVESTIGATION OF MAC AND APPLICATION LAYER PROTOCOLS WITH TRUST SUPPORT FOR NETWORK SECURITY

The paramount importance that events have attained with respect to securing communication networks is further compounded by interconnectivity. With floodgates opened to the Internet of Things (IoT), mobile devices, and wireless communication, the growing level of complexity in the environment has made networks more vulnerable to a variety of cyber threats. Among the most critical would be the MAC layer and application layer in network communication, which are the two layers directly impacting trustworthiness, efficiency, and security of data transmission.

Traditional means of security largely refer to cryptographic procedures or to the centralized application of the firewall, which are sometimes ineffective in a highly dynamic, decentralized, and resource-constrained environment such as a Mobile Ad Hoc Network (MANET) or an IoT system. In this regard, trust-related means have started gaining popularity since they can quickly adapt to their specific changing environments and can provide that extra measure of security in both the MAC and application layers.

The MAC layer is responsible for controlling data transmission on a shared medium so that bandwidth can be used efficiently, and collisions can be avoided. The MAC layer has itself been under attack, with a plethora of methods like jamming, spoofing, and denial of service (DoS). Likewise, the application layer, providing services for end-users like web browsing, messaging, and file transfer, is a target for malware, phishing, and data breaches [3].

To resolve these vulnerabilities, trust models are being introduced within network protocols. Trust-based systems can assess and analyze the behavior of nodes or services over time, enabling them to make well-informed decisions towards these nodes or services based on past interactions,

feedback, or context. For example, if a node is found to be consistently dropping packets or sending malicious data, that node may be marked as untrustworthy and disallowed to participate in any network communications [4].

The primary goal of this thesis is to analyze how the support for trust can be incorporated into MAC and application layer protocols to provide the desired security for networks. The specific objectives will be as follows:

- An analysis of existing MAC and application layer protocols will be carried out to examine their potential for exploitation.
- Study existing trust models and assess their relevance to network security.
- Design or select trust-enhanced protocols for both layers and compare their performance.
- Simulate or apply these protocols under a variety of network conditions and attack scenarios.
- Assess and compare how well trust support can counter the threats to security.

The primary thrusts of this research are trust support mechanisms in wireless and ad hoc network settings such as MANETs, wireless sensor networks (WSNs), and IoT networks. It will refrain from any significant deliberation on lower layers (e.g., physical layer) or systems highly centralized as traditional enterprise networks. The usage of NS-3 or OMNeT++ simulation tools will be adopted for modeling and evaluation of the protocols under consideration.

The research design includes the following:

- Literature Search: An elaborate study of existing MAC and application layer protocols, trust models, and known security attacks.
- Protocol selection and design: Identification or development of trust-based enhancements for selected protocols.
- Simulation and testing: Scenario implementation to evaluate protocol performance under conditions, with varying levels of trust and attack patterns, in simulated network environments.
- Analysis of Data: Performance measurement of key metrics such as packet delivery ratio, throughput, delay, and trust accuracy.
- Comparison and Evaluation: Comparison of trust-supported protocols with standard protocols in terms of security, efficiency, and adaptability.

Trust-supported protocols are predicted to show significant improvements in these security-related metrics, especially in hostile or unreliable environments. At the MAC layer, trust support could recognize and isolate misbehaving nodes, thereby protecting against jamming or collision attacks. Trust models at the application layer could identify malicious content or fraudulent services, thus bolstering end-to-end security [5].

Additionally, trust-aware protocols are expected to preserve acceptable performance trade-offs involving additional overhead for better reliability and resilience.

The main contribution presented in this doctoral thesis is the systematized evaluation of trust support on two different layers of the network stack—namely, MAC and application. While existing studies were often oriented toward one layer or another, this work aims to fill the gap between these two layers to construct a comprehensive view of how trust mechanisms can be harmonized across several layers. Such a correlation could be used to facilitate success in developing secure protocols for upcoming systems of wireless communication and IoT networks.

New threats to the security of the networks require more than static defenses. Trust-based protocols constitute a more flexible and dynamic way of ensuring security based on local context, especially at the MAC and application layers of the communication spectrum. Given the design, implementation, and analysis of trust within this thesis, it aims to be very enriching in producing insight into key issues concerning trust across multi-layer security in networks.

References

- [1] Stallings, W. (2017). **Data and Computer Communications**. Pearson Education.
- [2] Zhang, Y., & Lee, W. (2000). *Intrusion detection in wireless ad-hoc networks. *Proceedings of the 6th annual international conference on Mobile computing and networking**.
- [3] Chen, L., & Ngai, E. C. H. (2011). *Dynamic trust management for wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems**, 22(11), 1588-1595.
- [4] Momani, M., & Challa, S. (2010). *Survey of trust models in different network domains. *International Journal of Ad hoc, Sensor & Ubiquitous Computing**, 1(3).
- [5] Raza, S., Wallgren, L., & Voigt, T. (2013). *SVELTE: Real-time intrusion detection in the Internet of Things. *Ad hoc networks**, 11(8), 2661-2674.

UDC 004.056

Tokseit D. K. (L.N. Gumilyov ENU, Astana,
Kazakhstan) Otebay A.M (L.N. Gumilyov
ENU, Astana, Kazakhstan)

THE THREAT OF DEEPFAKE TECHNOLOGY TO HUMANITY IN RECENT YEARS

Deepfake technology has become a serious problem for information security and public trust in recent years. Deepfake technologies, which use artificial intelligence to create hyper-realistic fake videos and audio, pose a threat in various fields, including cybersecurity, politics, media, and personal privacy. The increasing complexity of deep-sea fishing algorithms has raised serious concerns about their potential use to spread disinformation, identify fraud, and manipulate public opinion.

The latest global statistics show that approximately 96% of deepfake content on the Internet is pornographic, which disproportionately affects women. Moreover, a study conducted in 2023 showed that the number of financial fraud cases related to deepfakes increased by 300% compared to the previous year. Additionally, the Deeptech Labs report says that the number of deepfake videos doubles every six months, with an estimated 85,000 videos in circulation by the end of 2022. These alarming figures highlight the urgent need to improve detection mechanisms and regulatory measures to combat the growing threats of deep counterfeiting.

One of the main risks associated with deepfishing technology is its impact on cybersecurity. Cybercriminals use voice and video recordings created using deepfake to carry out phishing attacks, defraud security systems, and manipulate authentication mechanisms. For example, financial institutions have reported incidents where voice clones created by artificial intelligence have been used to authorize fraudulent transactions.

In one well-known case in 2020, cybercriminals successfully used deepfake audio to impersonate a company executive, transferring \$35 million to fraudulent accounts. In addition, the Europol report for 2023 notes an increase in the number of fraudulent activities based on deep forgery targeting banking institutions, where artificial voices deceived employees, forcing them to process unauthorized transactions.

In a notable case from 2020, cybercriminals successfully used deepfake audio to impersonate a company executive, transferring \$35 million to fraudulent accounts. Additionally, a 2023 report by Europol highlighted an increasing number of deepfake-based scams targeting banking institutions, where synthetic voices deceived employees into processing unauthorized transactions.

These incidents illustrate how deep-face technology is used in financial fraud, highlighting the need to strengthen security measures and verification protocols based on artificial intelligence.

In addition, deepfake technology has become a powerful tool for spreading political disinformation. The attackers use fake videos to create fabricated speeches, manipulate election campaigns, and undermine trust in democratic institutions. The rapid spread of false information through social media compounds the difficulty of distinguishing between real and fake content.

Deepfakes pose a serious threat to people's privacy and reputation. The ease of creating fake content has led to an increase in cyberbullying, revenge pornography, and online defamation. Victims of such attacks often find it difficult to defend themselves, leading to emotional distress and long-term damage to their personal and professional lives.

To combat the threats posed by deepfakes, improvements are being implemented in detection algorithms, artificial intelligence-controlled authentication systems, and the legislative framework to combat crimes related to the abuse of deepfakes. Researchers and technology companies are developing machine learning models to identify fake content by analyzing digital artifacts and inconsistencies. In addition, legislative measures are being taken worldwide to criminalize the malicious use of deepfakes and bring those responsible to justice.

In conclusion, although deep-face technology has potential advantages in the entertainment and creative industries, its abuse poses a serious threat to information security and the stability of society. A practical solution to this problem requires an interdisciplinary approach that includes technological innovation, regulations, and public awareness to mitigate its harmful effects.

References

1. Mirsky, Y., & Lee, W. (2021). *The Threat of Deepfakes to Cybersecurity*. *IEEE Security & Privacy*, 19(5), 45-53.
2. Westerlund, M. (2019). *The Emergence of Deepfake Technology: A Review*. *Technology Innovation Management Review*, 9(10), 39-52.
3. Korshunov, P., & Marcel, S. (2018). *Deepfakes: A New Threat to Face Recognition?* *IEEE International Conference on Biometrics*, 1-8.
4. Nguyen, H. H., Yamagishi, J., & Echizen, I. (2019). *Deep Learning for Deepfake Detection*. *ACM Transactions on Multimedia Computing, Communications, and Applications*, 15(3), 1-24.
5. Chesney, R., & Citron, D. (2019). *Deepfakes and the New Disinformation War: The Coming Age of Post-Truth*. *California Law Review*, 107(6), 1753-1810.

UDC 519.62; 519.67

Ydyrys A.Zh. (Almaty, International Information Technology University)
Satybaldina A.N. (Almaty, International Information Technology University)

INVERSE PROBLEM FOR 2D LAPLACE EQUATION IN CYLINDRICAL COORDINATES

The thermal condition of a multilayer body system is defined by its temperature field, representing the distribution of instantaneous temperature values throughout the examined space. This field emerges when two bodies with different temperatures interact or within a single body containing regions of varying temperatures. The experiment was conducted during scientific research [1], [2]. The layers of the cylindrical region are filled with chernozem, clay and optima clay.

To determine the temperature field in heat conduction processes, a differential energy equation is required in cylindrical coordinates [3]-[5]:

$$\nabla^2 T = \frac{\partial^2 T}{\partial r^2} + \frac{1}{r} \frac{\partial T}{\partial r} + \frac{1}{r^2} \frac{\partial^2 T}{\partial \varphi^2} + \frac{\partial^2 T}{\partial z^2}.$$

(1)

In the two-dimensional case, the heat conduction differential equation (1) in cylindrical coordinates is expressed as:

$$c\rho \frac{\partial T}{\partial t} = k \left(\frac{\partial^2 T}{\partial r^2} + \frac{1}{r} \frac{\partial T}{\partial r} + \frac{1}{r^2} \frac{\partial^2 T}{\partial \varphi^2} \right).$$

(2)

Considering a stationary process, i.e. $\frac{\partial T}{\partial t} = 0$, the last heat conduction equation is written as

$$\frac{\partial^2 T}{\partial r^2} + \frac{1}{r} \frac{\partial T}{\partial r} + \frac{1}{r^2} \frac{\partial^2 T}{\partial \varphi^2} = 0$$

(3)

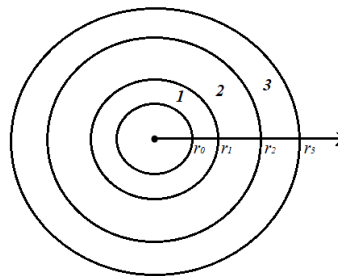


Fig.1. Three-layer ring

The general solution to the stationary heat conduction equation in cylindrical coordinates (3) is expressed as

$$T^s(r, \varphi) = A_0^s \ln r + B_0^s + \sum_{n=1}^{\infty} (A_n^s r^n + A_{-n}^s r^{-n}) \cos n\varphi + \sum_{n=1}^{\infty} (B_n^s r^n + B_{-n}^s r^{-n}) \sin n\varphi,$$

(4)

$$T(r, \varphi) = \begin{cases} T^1(r, \varphi), & \text{если } 1 \leq r \leq r_1, \\ T^2(r, \varphi), & \text{если } r_1 \leq r \leq r_2, \\ T^3(r, \varphi), & \text{если } r_2 \leq r \leq r_3. \end{cases}$$

where $s = 1, 2, 3$ и

There are:

1. All unknown coefficients of (4) are computed from direct problem.
2. Calculated heat transfer coefficients for each layer (k_1, k_2, k_3) from inverse problem.

Literature

1. Guo Taiyu, Sha Zhen-Dong, Liu, Xiangjun, Zhang Gang. Tuning the thermal conductivity of multi-layer graphene with interlayer boundary and tensile strain // *Applied physics*. – 2015. – №4. – pp.1275-1281.
2. G. F. Umbright, D. Rubio, D. A. Tarzia. Determination of Thermal Conductivities in Multilayer Materials // *WSEAS TRANSACTIONS on HEAT and MASS TRANSFER*. – 12/2022.
3. Frank Kreith, *Heat engineering handbooks*, 2000. 549 p.

4. Barhm Abdullah Mohamad, *Thermal conductivity*, 2022,
DOI:10.13140/RG.2.2.23142.50243

5. Guo, L., Guo, L., & Zhong, L. (2011). *Thermal conductivity and heat transfer coefficient of concrete*. *Journal of Wuhan University of Technology-Mater. Sci. Ed.*, 26(5), 977-981. <https://doi.org/10.1007/s11595-011-0312-3>

UDC 004.65.

Zhakan Z.S. (Karaganda, Abylkas Saginov KarTU)
Mukhametzhanova B.O., PhD (Karaganda,
Abylkas Saginov KarTU)

PROTECTING RELATIONAL DATABASE INDEXES FROM ATTACKS BASED ON QUERY ANALYSIS

Relational databases (RDBs) play a vital role in modern data management, requiring efficient indexing and query optimization techniques to enhance performance. This paper explores various methods for optimizing RDB performance, focusing on query analysis, adaptive indexing, and security enhancements. Additionally, it discusses how these methods can be applied in dissertation research to develop innovative approaches for improving database efficiency. By leveraging machine learning techniques, dynamic indexing mechanisms, and anomaly detection, this study aims to address performance bottlenecks and security vulnerabilities. The findings provide a strong foundation for future research in database performance optimization.

Relational databases (RDBs) serve as the backbone of modern data-driven applications. Efficient data retrieval and management rely heavily on indexing mechanisms. However, challenges such as query performance bottlenecks, security vulnerabilities, and inefficient indexing strategies necessitate ongoing research into optimization techniques. This review explores methods for optimizing RDB performance, focusing on query analysis and indexing strategies and how these methods can be applied in the context of dissertation research [1].

Optimizing relational databases involves addressing several key challenges:

- Query Execution Efficiency: Poorly optimized queries can lead to excessive resource consumption and slow response times.
- Indexing Strategies: Suboptimal indexing can either slow down queries or increase storage overhead.
- Security Vulnerabilities: Indexes can be exploited through inference attacks, side-channel analysis, and query-based probing.
- Scalability: As databases grow, maintaining performance becomes increasingly difficult.
- Anomaly Detection: Detecting and mitigating anomalous queries that may degrade performance or indicate potential security threats.

To address these challenges, researchers have proposed various methods that integrate query analysis, dynamic indexing, and anomaly detection.

Query Performance Analysis: analyzing query execution patterns allows database administrators to identify inefficiencies and optimize query execution plans. Machine learning-based anomaly detection can distinguish between normal and problematic queries [2].

It is possible to implement query analysis techniques to examine real-world query logs. By leveraging machine learning models, one can classify queries based on execution time, frequency, and indexing behavior to identify optimization opportunities and detect inefficient patterns.

Adaptive Indexing Techniques: dynamic indexing methods adapt to query workloads, reducing the overhead associated with maintaining unused indexes. Techniques include:

- Self-Tuning Indexing: Automatically adjusting index structures based on query patterns.
- Materialized Views and Partitioning: Storing precomputed query results to enhance retrieval efficiency.

By comparing performance gains across different indexing strategies, it's possible to validate the effectiveness of adaptive indexing for improving database efficiency.

Security-Focused Index Optimization: given the risks of index-based inference attacks, security measures must be incorporated into indexing strategies. Potential solutions include:

- Query Behavior Analysis: Monitoring and classifying queries to detect potential attacks.
- Obfuscation Techniques: Adjusting index structures dynamically to prevent inference-based exploits.
- Access Pattern Monitoring: Tracking historical query logs to identify anomalies.

To enhance database security, one can investigate how query analysis can be used to prevent indexing-related inference attacks. By implementing access pattern monitoring and anomaly detection, a security-aware indexing framework that balances both performance and protection against malicious queries can be proposed [3].

Recent studies demonstrate the effectiveness of integrating machine learning techniques for query-based attack detection and indexing optimization:

- A 72% reduction in inference-based attacks when using adaptive indexing.
- A high anomaly detection rate (>90%) with supervised learning approaches.
- A 15% performance overhead, which remains acceptable in security-sensitive environments.

Building on these findings, experiments can be conducted to measure the trade-offs between performance gains and security improvements when applying adaptive indexing. The goal is to create an approach that achieves optimal performance with minimal security risks [4].

To further enhance relational DB performance, future work should focus on:

- Refining anomaly detection models to improve accuracy with minimal performance trade-offs.
- Developing hybrid indexing strategies that balance storage costs and query speed.
- Integrating optimization frameworks into commercial database management systems for seamless deployment [5].

Optimizing relational database performance requires a multi-faceted approach, integrating query analysis, adaptive indexing, and security enhancements. By leveraging machine learning techniques, researchers and practitioners can significantly improve database efficiency while mitigating security threats.

References

1. Gupta, R., et al. "A Review of Database Attacks." [Scholar Publishing].
2. Singh, P., Sharma, K. "Database Security: Attacks, Threats, and Challenges." [IJERT].
3. Imperva. "Simple Trend and Anomaly Detection with SQL." [Imperva Blog].
4. Linkurious. "Anomaly Detection Algorithms: Find Outliers in Your Data." [Linkurious Blog].
5. SolarWinds. "Database Anomaly Detection and Alerting with Machine Learning." [SolarWinds].

УДК 004.89

Алексеев И. П., Оспанова А. Б.
(Астана, ЕНУ им. Л. Н. Гумилёва)

ИССЛЕДОВАНИЕ ПОТЕНЦИАЛА AI-МОДЕЛЕЙ В АВТОМАТИЗАЦИИ КИБЕРАТАК

В последние годы число кибератак стремительно растёт, а методы злоумышленников усложняются. Искусственный интеллект (ИИ) и машинное обучение привели к новому витку противостояния: атакующие используют ИИ для автоматизации и масштабирования атак, а защитники адаптируются к новым угрозам. ИИ-модели позволяют создавать правдоподобные фишинговые сообщения и вредоносный код, что упрощает атаки даже для малоопытных злоумышленников. По данным ФБР (2024), ИИ-инструменты значительно повышают эффективность мошеннических схем, включая таргетированные фишинговые кампании и создание реалистичных подделок для обмана жертв.

Традиционные хакерские атаки во многом полагались на навыки человека: инженерия социального доверия, ручной подбор уязвимостей, написание эксплойтов экспертами. Постепенно многие этапы стали автоматизироваться – появились сканеры уязвимостей, эксплойт-фреймворки (Metasploit и др.), ботнеты для массированных атак. AI поднял эту автоматизацию на новый уровень. Теперь возможно создание автономных агентов, способных последовательно проходить по этапам kill-chain (от разведки до эксфильтрации данных) с минимальным вмешательством человека. Например, инструмент DeepExploit (2018) продемонстрировал применение глубокого обучения с подкреплением для автоматического проведения пентестов: агент изучает открытую поверхность атаки и подбирает эффективные эксплойты в режиме самобучения. В результате сокращается число попыток для успешного взлома, и атака может развиваться вглубь сети (путём цепочки компрометации сначала периферийного узла, затем внутренней сети) без ручного управления. Появились и другие примеры: алгоритмы на основе Generative Adversarial Networks (GAN), генерирующие варианты вредоносных файлов, которые обходят детектирование средствами защиты; специальные AI-модули для malware, позволяющие изменять поведение вредоноса «на лету». Таким образом, кибератаки вступили в эпоху частичной или полной автономности, когда ключевые решения (какую уязвимость эксплуатировать, как скрыть следы, как шифровать данные жертвы и т.д.) принимает не человек, а обученная модель (см. табл. 1).

Таблица 1
Виды автоматизированных атак

Категория атаки	Пример использования AI	Последствия
Фишинг и социнженерия	Генерация писем и сообщений с помощью LLM (ChatGPT, WormGPT), синтез голоса (Voice GAN)	Массовые рассылки, таргетированные мошеннические сообщения с ошибками, сложно отличимые от настоящих; рост успешности обмана

Эксплуатация уязвимостей	Авто-пентестеры на базе обучения (DeepExploit), LLM-агенты для поиска багов (CVE-Bench)	Быстрое обнаружение и эксплуатация дыр в безопасности, проникновение вглубь сети без участия человека
Создание malware	Генерация кода вредоносных программ через кодовые LLM (Codex), полиморфизм с помощью GAN	Множество новых вариантов вредоносного ПО, обходящих известные сигнатуры и evasion-системы
Deepfake-атаки	Искажение реальности: поддельное видео или аудио (например, лицо руководителя на видео) для обмана сотрудников	Успешные мошеннические транзакции, выдача конфиденциальных данных злоумышленнику под видом «босса» и пр.
Адаптивные атаки	AI-модели внутри вредоносных (как в DeepLocker) для скрытности и точечного срабатывания	Трудно обнаружимые АРТ, которые долго остаются в системе и наносят ущерб только запланированной цели

Далее обсуждается концепция безопасного использования развитого ИИ, являющегося определенным субъектом информационной безопасности, а не только лишь инструментом, а также вопросы построения защиты от него.

Один практический сценарий организации ИБ в эпоху развивающихся

Сценарий организации ИБ в эпоху развивающихся AI-технологий может включать мероприятия по выявлению и анализу существующих AI-инструментов, используемых для автоматизации кибератак, с последующим определением ключевых угроз и уязвимостей информационных систем, наиболее подверженных воздействию интеллектуальных атак. Это позволит своевременно прогнозировать возможные атаки и выбирать оптимальные защитные меры, такие как специализированные AI-детекторы и системы мониторинга аномалий, что существенно снизит вероятность успешных атак и минимизирует потенциальный ущерб. Альтернативными подходами могут служить применение расширенных политик безопасности и архитектурных решений, таких как Zero Trust, а также внедрение симметричных AI-решений для автоматизированного реагирования и противодействия атакам в режиме реального времени.

Подводя итог, можно сказать, что трудности носят как практический, так и принципиальный характер. Они не отменяют того факта, что offensive и defensive AI будут развиваться – но показывают, что путь этот не прямой. Необходима взвешенная политика: с одной стороны, стимулировать исследования (чтобы не проиграть в гонке злоумышленникам), с другой – контролировать распространение опасных разработок. Решение проблем данных и интерпретируемости требует сотрудничества между компаниями, обмена информацией об атаках, инвестиций в explainable AI. А проблема alignment в данном контексте – мотивация создавать специальные “этичные вирусы”: ИИ, которые позволят изучить методы атак, но не выйдут из-под контроля и не причинят вреда реальным целям.

Список использованных источников

1. Europol sounds alarm about criminal use of ChatGPT, sees grim outlook. Reuters – 27.03.2023. [Электронный ресурс]. Режим доступа: <https://www.reuters.com/technology/europol-sounds-alarm-about-criminal-use-chatgpt-sees-grim-outlook-2023-03-27/> (дата обращения: 30.03.2025).
2. FBI San Francisco Division. FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence. – 08.05.2024. [Электронный ресурс]. Режим доступа: <https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence> (дата обращения: 30.03.2025).
3. Zhu Y. et al. CVE-Bench: A Benchmark for AI Agents’ Ability to Exploit Real-World Web Application Vulnerabilities. arXiv:2503.17332, 2025. [Электронный ресурс]. Режим доступа: <https://arxiv.org/abs/2503.17332> (дата обращения: 30.03.2025).
4. Guembe B., Azeta A., Misra S. et al. The Emerging Threat of AI-Driven Cyber Attacks: A Review. Applied Artificial Intelligence, 36(1):1-22, 2022. [Электронный ресурс]. Режим доступа: <https://doi.org/10.1080/08839514.2022.2037254> (дата обращения: 30.03.2025).
5. SlashNext (2023). AI-Based Cybercrime Tools WormGPT and FraudGPT Could Be The Tip of the Iceberg. SlashNext Blog – 20.07.2023. [Электронный ресурс]. Режим доступа: <https://slashnext.com/blog/ai-based-cybercrime-tools-wormgpt-and-fraudgpt-could-be-the-tip-of-the-iceberg/> (дата обращения: 30.03.2025).

UDC 004.056

Әмірғалы Сымбат
Л.Н.Гумилев атындағы
ЕҰУ Ақпараттық технологиялар факультеті,
Астана, Қазақстан
Омар Айдана .Н.Гумилев атындағы
ЕҰУ Ақпараттық технологиялар факультеті,
Астана, Қазақстан
Ғылыми жетекшісі - аға оқытушы Тоқсеит Д.Қ.

Фишингтен, телефон алаяқтарынан және маркетплейстердегі алаяқтықтан ЖИ көмегімен қорғауы

Тақырыптың өзектілігі: Заманауи цифрлық технологиялар пайдаланушылардың өмірін айтарлықтай жеңілдетеді, бірақ сонымен қатар алаяқтық қауіпін арттырады. Жасанды интеллект (ЖИ) деректер мен қаржыны қорғауда маңызды рөл атқарады, күмәнді әрекеттерді анықтайды, транзакцияларды талдайды және алаяқтық әрекеттерді сүзгіден өткізеді. Бұл тақырып, әсіресе, алаяқтық схемаларының үнемі жетілдірілуіне және оларға қарсы күрестің алдын ала жүргізілуіне байланысты ерекше өзекті болып табылады.

Кілт сөздер: фишинг, алаяқтық, жасанды интеллект, деректерді қорғау, транзакцияларды талдау, цифрлық қауіпсіздік, биометриялық аутентификация, антифрод жүйелері.

Жасанды интеллект пайдаланушыларды алаяқтықтан қорғаудың негізгі құралына айналды. Банктер мен маркетплейстер ЖИ-ді транзакцияларда аномалияларды анықтау, клиенттердің мінез-құлқын талдау және күмәнді операцияларды бұғаттау үшін белсенді түрде қолданады. Қорғаудың негізгі әдістерінің бірі – пайдаланушылардың мінез-құлқын талдайтын аномалияларды анықтау жүйесі. Егер клиент үнемі белгілі бір аймақта сауда жасаса, ал кенеттен оның картасы басқа елде қолданылса, жүйе операцияны тексерілгенше автоматты түрде бұғаттайды. Сонымен қатар, ЖИ деректерді енгізу жылдамдығын, сұраныстар жиілігін және геолокацияны талдау арқылы күмәнді әрекеттерді анықтай алады.

ЖИ онлайн-банкінгі қорғау үшін де қолданылады. Мысалы, заманауи аутентификация жүйелері бет әлпеті мен дауысты тану сияқты биометриялық әдістермен толықтырылады. Бұл логин мен құпия сөзден бөлек, пайдаланушының жеке басын қосымша факторлар арқылы растауды талап етіп, деректердің ұрлану тиімділігін төмендетеді. Кейбір платформалар динамикалық аутентификацияны енгізуде, онда жүйе теру стилін, курсор қозғалысын және пайдаланушының басқа да жеке ерекшеліктерін талдайды.

ЖИ-тің тиімді қолданылуының мысалы ретінде Бауман атындағы МГТУ мен Ресей Федералды салық қызметінің бірлесіп әзірлеген жүйесін атауға болады. Бұл жүйе заңды ақпаратты талдап, күмәнді аномалиялары бар компанияларды анықтайды, бұл қаржылық алаяқтықтың алдын алуға мүмкіндік береді. SEON және Greip сияқты халықаралық платформалар цифрлық профильдеу әдістерін қолданып, қауіп-қатерлерді бағалайды және алаяқтарды ерте кезеңде анықтайды. Бұл заңсыз транзакцияларды олардың орындалуына дейін болдырмауға көмектеседі. Бұған қоса, көптеген банктер нейрожелілерді жалған құжаттарды анықтау және бет-әлпетті биометриялық аутентификация арқылы сканерлеу үшін пайдаланады.

ЖИ фишингпен және әлеуметтік инженериямен күресуге де белсенді түрде қолданылады. Ол электрондық хаттардың мазмұнын талдайды, күмәнді сілтемелер мен тіркемелерді анықтайды, сондай-ақ телефон қоңырауларындағы манипуляция әрекеттерін айқындайды. Британдық O2 операторы телефон алаяқтарын ұстап тұратын «Daisy» деп аталатын «нейрожүйе» әзірледі, бұл олардың нақты адамдарды алдауына жол бермейді. Ресейде «Нейроцит» және «Хранитель» технологиялары әзірленді, олар телефон сөйлесулерін талдап, кілт сөздер мен мінез-құлық факторларына негізделген алаяқтық қоңырауларды бұғаттайды. Мұндай жүйелер автоматты қоңыраулармен және егде жастағы адамдарды алдау схемаларымен күресуге көмектесіп, күмәнді сценарийлерді анықтайды.

Сонымен қатар, сөйлеу мәнерін талдап, сөйлеушінің стресске түсу белгілерін немесе жауаптардағы сәйкессіздіктерді анықтайтын алгоритмдер бар. Мұндай технологиялар банктер мен қауіпсіздік қызметтерінде әлеуметтік инженерия әрекеттерін анықтау үшін қолданылады. Мысалы, егер алаяқ құрбанды ақшаны шұғыл аударуға көндіруге тырысса, жүйе әңгімені нақты уақытта талдап, қоңырауды автоматты түрде тоқтатуы немесе ескерту жіберуі мүмкін.

Онлайн-сауда саласында ЖИ жалған тауарларды, алаяқ сатушыларды және жалған пікірлерді анықтау үшін қолданылады. Мұндай жүйелер тауар сипаттамаларын, суреттерін және бағадағы аномалияларды талдап, контрафакт өнімдерінің таралуының алдын алады. Sift және Adfonic сияқты платформалар күмәнді трафикті талдап, жалған басуларды бұғаттау үшін машиналық оқытуды пайдаланады. Сонымен қатар, ЖИ мәтін стилін, жариялау жиілігін және пайдаланушылар арасындағы байланысты талдау арқылы жалған пікірлерді анықтай алады. Бұл маркетплейстердегі алаяқтардың ықпалын азайтып, сатып алушылардың шынайы пікірлерге деген сенімін арттырады.

Ең күрделі мәселелердің бірі – дипфейктермен күрес. Алаяқтар жалған бейнелер мен дауыстар жасау үшін генеративті нейрожелілерді жиі қолдануда, бұл жалған өтініштерді анықтауды қиындатады. Бұған жауап ретінде компаниялар ерін қимылдарының,

интонацияның және бейнежазбамен синхрондалған сөйлеудің шамалы сәйкессіздіктерін талдайтын ЖИ жүйелерін әзірлеуде. Мұндай технологиялар жеке бас ұрлығының алдын алу үшін банктік секторда енгізіле бастады.

Алаяқтықпен күресудегі ЖИ-тің болашағы қауіп-қатерлерге тек жауап беріп қана қоймай, оларды болжауға да қабілетті проактивті жүйелерді дамытуға байланысты. Түсіндірілетін ЖИ-ті (ХАІ) енгізу пайдаланушыларға алаяқтарды анықтау шешімдері қандай негізде қабылданатынын жақсырақ түсінуге мүмкіндік береді. Сонымен қатар, кванттық шифрлау алгоритмдері мен нақты уақытта күрделі алаяқтық схемаларын анықтай алатын автоматтандырылған антифрод жүйелері перспективалы бағыттар болып табылады. Дегенмен, қылмыскерлер де ЖИ-ді пайдаланып, күрделірек фишингтік шабуылдар мен дипфейктер жасауда. Бұл көп деңгейлі аутентификация жүйелері мен қауіп-қатерлерді анықтаудың динамикалық алгоритмдерін қоса алғанда, қорғаныс механизмдерін үнемі жетілдіру қажеттілігін тудырады.

Айтарлықтай жетістіктерге қарамастан, ешбір жүйе 100% қауіпсіздікті кепілдей алмайды. Сондықтан пайдаланушыларға кибер-гигиенаны сақтау, күмәнді хабарламаларды тексеру және жеке деректерді бейтаныс адамдарға бермеу маңызды. Жасанды интеллект алаяқтықпен күресудің қуатты құралына айналды, бірақ оның тиімділігі көп жағдайда пайдаланушылардың хабардарлығы мен сақтығына байланысты. ЖИ мен адами факторды үйлестіру – цифрлық әлемдегі қауіп-қатерлерді барынша азайтудың және қауіпсіздікті қамтамасыз етудің ең тиімді жолы.

Қорытынды

Жасанды интеллект (ЖИ) қазіргі заманғы алаяқтықпен күресудің тиімді құралына айналды. Ол фишинг, телефон алаяқтары және маркетплейстердегі алаяқтық әрекеттерді алдын ала анықтау және болдырмау үшін кеңінен қолданылады. Банктер мен онлайн платформалар ЖИ-ді пайдаланушылардың мінез-құлқын талдау, транзакцияларда аномалияларды анықтау және алаяқтық әрекеттерді уақытында тоқтату үшін белсенді түрде енгізуде.

Биометриялық аутентификация, нейрожелілерді пайдалану және машиналық оқыту әдістері күмәнді әрекеттерді сүзгіден өткізіп, пайдаланушылардың қауіпсіздігін арттыруға мүмкіндік береді. Сондай-ақ, ЖИ телефон алаяқтарымен күресуде адамның дауысын, сөйлеу мәнерін және интерактивті жауаптарды талдау арқылы күмәнді қоңырауларды анықтай алады.

Фишингке қарсы күресте ЖИ электрондық хаттар мен веб-сайттардың мазмұнын, сілтемелер мен тіркемелерді тексеру арқылы алаяқтық әрекеттерді ерте кезеңде анықтауға көмектеседі. Сонымен қатар, маркетплейстерде жалған пікірлер мен контрафактілік өнімдерді анықтау үшін мәтіндік және визуалды талдау әдістері қолданылады.

Алайда, ЖИ-тің дамуына байланысты алаяқтар да күрделірек шабуыл түрлерін ойлап табуда. Сондықтан жасанды интеллектіні жетілдірумен қатар, пайдаланушылардың киберсауаттылығын арттыру маңызды. Тек көп деңгейлі қорғаныс әдістерін қолдану және адам мен машинаның бірлескен жұмысы арқылы ғана алаяқтықпен тиімді күресуге болады.

Жалпы, жасанды интеллект алаяқтық әрекеттерді анықтауда, болдырмауда және алдын алуға негізгі технологиялардың біріне айналды. Болашақта оның мүмкіндіктері одан әрі кеңейіп, қауіпсіздік жүйелерін жетілдіруге ықпал етеді.

Қолданылған әдебиеттер:

1. <https://habr.com/ru/>
2. <https://metanit.com/>
3. <https://www.e-books4it.ru/>

4. <https://cyberleninka.ru/>
5. <https://www.securitylab.ru/>

Байшаков Д.Т.
(Астана, ЕНУ им. Л.Н. Гумилева)
Казиёва Н.М.
(Астана, ЕНУ им. Л.Н. Гумилева)

Принцип работы нейрона в нейронных сетях и анализ алгоритмов нейронных сетей для автоматизации процессов в кибербезопасности

Аннотация

В данной статье рассматривается принцип работы нейрона в искусственных нейронных сетях (ИНС) и проводится анализ основных алгоритмов их функционирования. Описывается математическая модель нейрона, включая входные сигналы, синаптические веса и функции активации. Исследуются свойства нейронных сетей, такие как адаптивность, обобщение и способность к идентификации нелинейных систем. Анализируются различные архитектуры ИНС, включая нейронные сети прямого распространения (LFNN), рекуррентные нейронные сети (RNN). Рассматриваются их преимущества, недостатки и области применения. В заключении предлагается гибридный подход, объединяющий методы контролируемого, неконтролируемого и подкрепленного обучения для оптимизации автоматизированного принятия решений в системах кибербезопасности.

Введение

В данной статье рассматриваются основные принципы работы нейрона, его математическое описание и ключевые архитектуры нейронных сетей. Особое внимание уделяется нейросетям прямого распространения (LFNN) и рекуррентным нейронным сетям (RNN), их преимуществам, недостаткам и применению в различных задачах. Также анализируются методы обучения, включая пакетное и онлайн-обучение, а также проблемы, возникающие при обучении ИНС.

Принцип работы нейрона

Нейрон служит в качестве основного блока обработки информации нейронных сетей [1]. Его работа имеет основополагающее значение для проектирования и функционирования систем нейронных сетей. Нейрон является базовым элементом искусственной нейронной сети и выполняет функцию обработки информации. Он получает входные сигналы, которые умножаются на соответствующие синаптические веса. Затем вычисляется взвешенная сумма всех входов, к которой добавляется смещение (bias).

Результат суммирования передается в функцию активации, которая определяет, будет ли нейрон активирован. Среди наиболее распространенных функций активации выделяют:

- Пороговую – если сумма входных сигналов превышает определенное значение, нейрон активируется.
- Сигмоидальную – превращает входной сигнал в значение от 0 до 1, что полезно для вероятностных интерпретаций.
- ReLU (Rectified Linear Unit) – заменяет отрицательные значения нулями, что ускоряет обучение.

Когда нейрон активирован, он передает выходной сигнал следующему слою нейросети. В многослойных нейросетях выход одного нейрона становится входом для нескольких других нейронов, что формирует сложные нелинейные зависимости.

В математических терминах нейрон работает следующим образом:

$$s_i = \sum_{m=0}^M w_{im} x_m$$

$$y_i = f(s_i)$$

Где:

$x_1, x_2, \dots, x_M$ - входные сигналы.

$x_0 = 1$ - смещение.

$w_{i0}, w_{i1}, \dots, w_{iM}$ - синаптические веса, связанные с нейроном i .

f - функция активации.

y_i – выходной сигнал нейрона.

Алгоритмы обучения нейронных сетей

Обучение нейронных сетей направлено на настройку весов нейронов с целью минимизации ошибки предсказания. Существует несколько ключевых методов обучения:

- Пакетное обучение – обновление весов после прохождения всей обучающей выборки.
- Онлайн-обучение – корректировка весов после каждого примера, что позволяет быстрее адаптироваться к изменениям данных.
- Градиентный спуск (SGD, Adam, RMSprop) – метод оптимизации, изменяющий веса в направлении наибольшего уменьшения ошибки.

Проблемы обучения и их решения

Одной из главных проблем обучения нейросетей является исчезающий и взрывной градиент. В RNN [2] градиентный спуск может либо слишком сильно уменьшаться (что делает обучение невозможным), либо становиться слишком большим (что приводит к нестабильности). Для решения этой проблемы используются:

- LSTM (Long Short-Term Memory) – архитектура с механизмами забывания и запоминания, позволяющая работать с длинными последовательностями [3].
- GRU (Gated Recurrent Unit) – облегченный аналог LSTM, обеспечивающий схожую эффективность с меньшими вычислительными затратами [3].

Современные методы оптимизации

Для повышения эффективности обучения применяются дополнительные методы:

- Адаптивные алгоритмы (например, Adam, RMSprop) – автоматически подстраивают скорость обучения для каждого параметра сети.
- Регуляризация (Dropout, L2-нормализация) – предотвращает переобучение модели за счет ограничения весов и случайного отключения нейронов во время обучения.
- Batch Normalization [4] – нормализация данных перед подачей в слой нейросети для ускорения сходимости градиентного спуска.

Применение нейросетей в SIEM-системах

Нейронные сети находят широкое применение в системах управления информационной безопасностью (SIEM). Их использование позволяет [5]:

Автоматически анализировать и классифицировать инциденты – модели машинного обучения могут выявлять аномальное поведение в логах и идентифицировать потенциальные угрозы.

Обнаруживать атаки в реальном времени – рекуррентные нейросети (RNN) и модели LSTM помогают анализировать последовательности событий и предсказывать угрозы до их проявления.

Оптимизировать обработку данных – нейросети позволяют автоматизировать корреляцию логов, снижая нагрузку на аналитиков SOC (Security Operations Center).

Минимизировать ложные срабатывания – ИНС обучаются на исторических данных, что позволяет улучшать точность классификации и снижать количество ложных тревог.

Закключение

Искусственные нейронные сети представляют собой мощный инструмент обработки данных, способный адаптироваться к изменяющимся условиям. В работе проанализированы ключевые принципы функционирования нейронов, основные алгоритмы обучения и структуры нейросетей. Дальнейшие исследования направлены на разработку гибридных архитектур, объединяющих различные методы обучения и их интеграцию в SIEM-системы для повышения эффективности обнаружения угроз.

Источники:

1. Hochreiter, S., & Schmidhuber, J. (1997). Long Short-Term Memory. *Neural Computation*, 9(8), 1735–1780.
2. Cho, K., van Merriënboer, B., Gulcehre, C., Bahdanau, D., Bougares, F., Schwenk, H., & Bengio, Y. (2014). Learning Phrase Representations using RNN Encoder-Decoder for Statistical Machine Translation. *arXiv preprint arXiv:1406.1078*.
3. Kim, G. H., & Kim, K. J. (2022). Threat classification model for security information event management focusing on model efficiency. *Journal of Cybersecurity Research*, 5(3), 45–58.
4. Ioffe, S., & Szegedy, C. (2015). Batch Normalization: Accelerating Deep Network Training by Reducing Internal Covariate Shift. *Proceedings of the 32nd International Conference on Machine Learning (ICML)*.
5. Alaca, Y., & Çelik, Y. (2023). Anomaly Detection in Cyber Security with Graph-Based LSTM in Log Analysis. *Journal of Cyber Security and Mobility*, 12(1), 45–68.

Балгабекова С.А., Аймичева Г.И.

ТЕХНОЛОГИЯ СБОРА ЦИФРОВЫХ УЛИК ВЕБ-АКТИВНОСТИ ЗЛОУМЫШЛЕННИКА В РЕЖИМЕ ИНКОГНИТО

С развитием цифровых технологий вопросы конфиденциальности становятся всё более актуальными. Веб-браузеры предлагают пользователям режим приватного просмотра, который, согласно заявленным характеристикам, не сохраняет историю посещений, кеш, куки-файлы и другие данные после завершения сеанса. Однако на практике полное исчезновение следов веб-активности не всегда гарантируется [1, 2].

Для специалистов в области цифровой криминалистики эта особенность браузеров играет ключевую роль. Пользователи рассчитывают на анонимность приватного режима, но злоумышленники могут использовать его для сокрытия незаконной деятельности. Это создаёт необходимость в разработке методов анализа цифровых уликов, которые остаются в системе даже после завершения приватного сеанса [1].

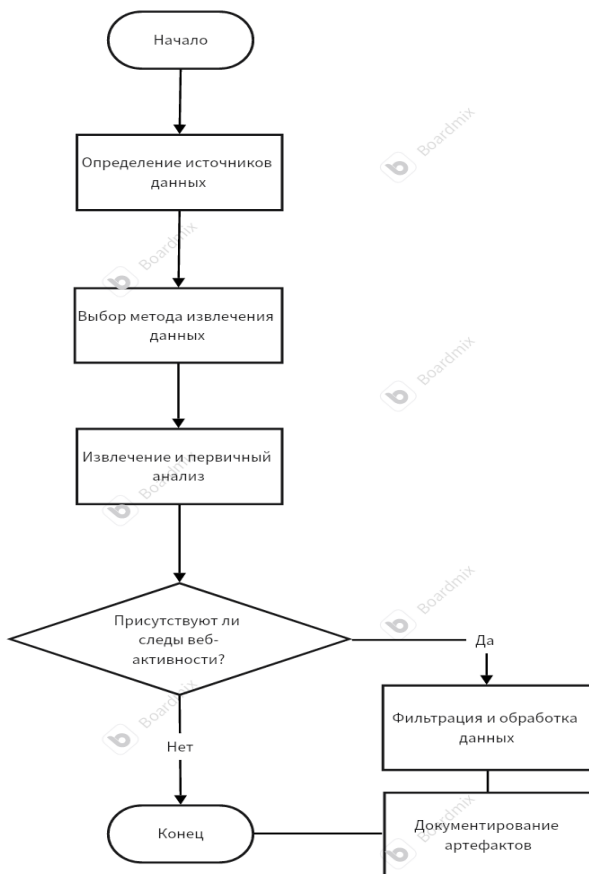
В данной статье рассматриваются основные методы и инструменты для извлечения цифровых артефактов, оставляемых после работы в режиме инкогнито. В качестве примера

используются Process Monitor (Procmon) для отслеживания файловой активности браузера в реальном времени.

Представленная схема отражает последовательность действий при анализе цифровых улик скрытой веб-активности пользователя. (См. Рисунок 1.) В начале определяется, где могут сохраняться следы веб-активности. К таким источникам относятся файлы истории браузера, кеш, куки-файлы, DNS-кеш, сетевые логи, файлы подкачки, дампы памяти и реестр Windows. Каждый из них может содержать информацию о посещённых сайтах даже после закрытия браузера.

После определения источников выбирается метод извлечения данных. Разные типы артефактов требуют использования различных инструментов.

На следующем этапе извлекаются данные и проводится их первичный анализ. Информация загружается в соответствующие инструменты, исследуется на предмет наличия следов веб-активности. Если артефакты обнаружены, они подвергаются дополнительной обработке и фильтрации, чтобы исключить нерелевантные записи и провести анализ временных меток. В случае отсутствия следов процесс завершается.

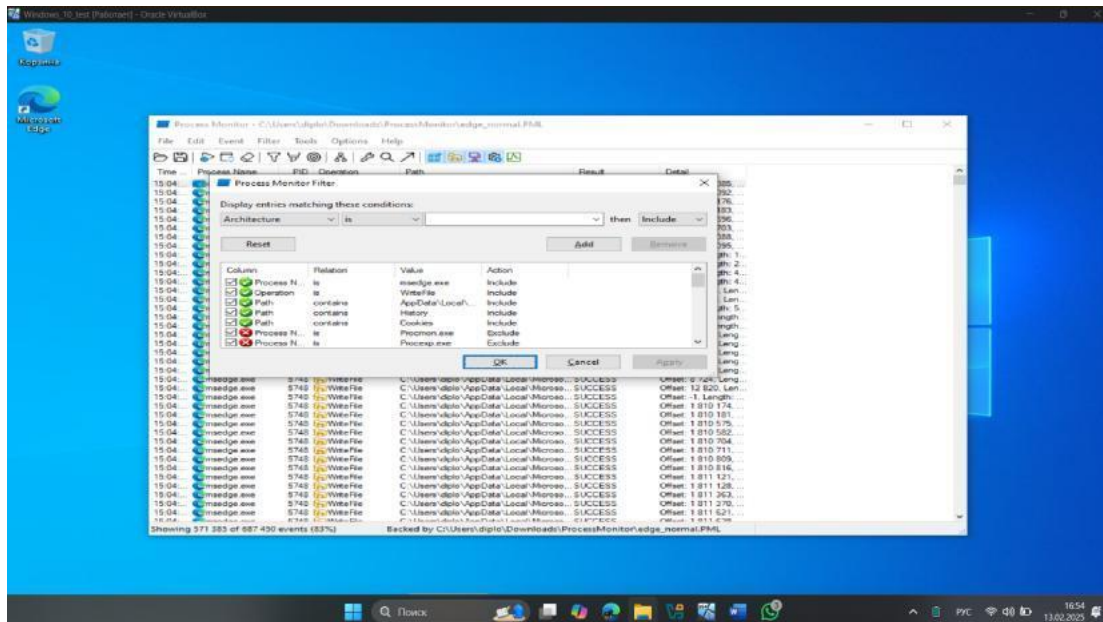


См. Рисунок 1. Алгоритм сбора цифровых улик конфиденциальной веб-активности.

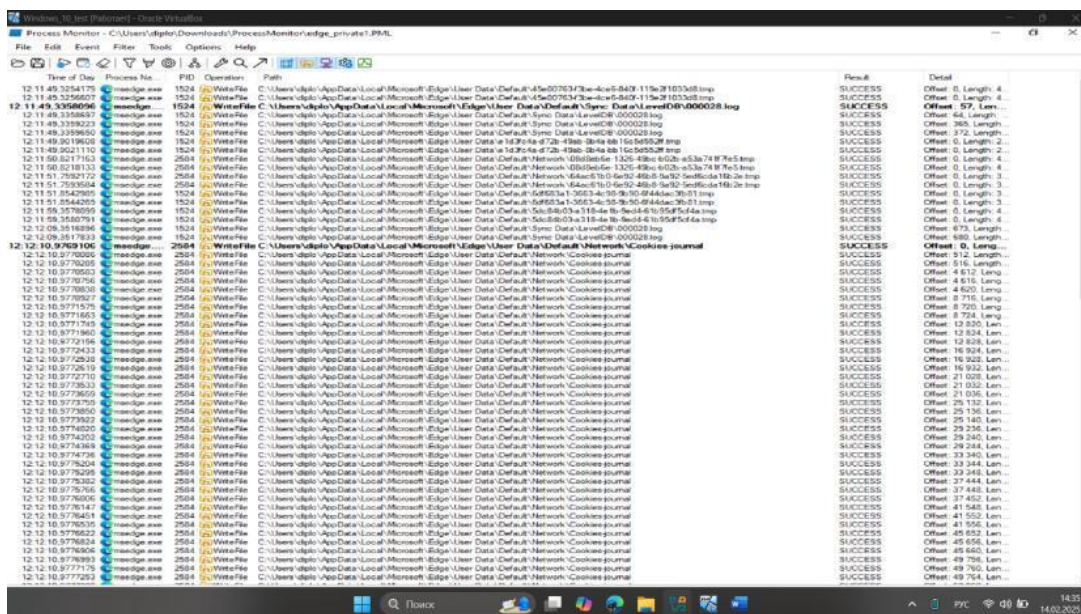
Когда цифровые улики выявлены, выполняется их документирование. Это включает фиксацию характеристик артефактов, временных меток и возможных путей восстановления данных. Завершающим шагом становится формирование вывода о наличии или отсутствии следов веб-активности в режиме InPrivate.

Одним из ключевых инструментов в цифровой криминалистике является Process Monitor (Procmon) от Microsoft. Этот инструмент позволяет отслеживать активность браузера в режиме реального времени и выявлять, какие файлы, реестровые ключи и сетевые

соединения использует браузер при работе в инкогнито-режиме. С помощью Prostop можно не только обнаружить потенциальные артефакты веб-активности, но и проанализировать процесс удаления данных при закрытии окна InPrivate.



См. Рисунок 2. Фильтрация логов в Prostop.



См. Рисунок 3. Найденные артефакты.

Таким образом, несмотря на меры предосторожности, режим инкогнито не гарантирует полной конфиденциальности. Следы веб-активности могут сохраняться в различных местах системы. Это делает возможным восстановление цифровых улик даже после завершения приватного сеанса. Данный аспект является важным как для специалистов по информационной безопасности, так и для цифровой криминалистики.

1. Fernández-Fuentes X., Pena T. F., Cabaleiro J. C. Digital forensic analysis methodology for private browsing: Firefox and Chrome on Linux as a case study //Computers & Security. – 2022. – Т. 115. – С. 102626.

2. Fernández-Fuentes X., Pena T. F., Cabaleiro J. C. Digital forensic analysis of the private mode of browsers on Android //Computers & Security. – 2023. – Т. 134. – С. 103425.

Жарылгап Р.Ж. (Астана, ЕНУ им. Л.Н. Гумилева)

Исайнова А.Н. (Астана, ЕНУ)

ИССЛЕДОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИОТ-УСТРОЙСТВ С ИСПОЛЬЗОВАНИЕМ МОНИТОРИНГА, АУТЕНТИФИКАЦИИ И СИМУЛЯЦИИ СЕТЕВЫХ АТАК

Актуальность темы исследования обусловлена ростом числа угроз, нацеленных на IoT устройства, и необходимостью разработки эффективных методов их защиты. Важными аспектами защиты IoT устройств можно считать мониторинг сетевой активности, надёжные методы аутентификации и возможность противостояния реальным кибератакам. Одним из методов изучения уязвимостей является симуляция сетевых атак, которая позволяет оценить устойчивость IoT устройств к различным видам вторжений.

IoT устройства объединяют миллионы устройств подключенных к сети, из-за чего злоумышленники нацелены на них. Главная проблема IoT является недостаточная безопасность. У IoT огромное количество проблем с безопасностью. В индустрии нет единого набора стандартов безопасности, которую могли бы придерживаться производители или же разработчики. Внедрение устройств IoT происходит быстрее, чем процессы обеспечивающие безопасные соединения.

Безопасность IoT – комбинация выстроенных политик, ПО и технических решений. По мере того, как устройства IoT продолжают распространяться, защита целостности и конфиденциальности данных становятся все более важной.

Мониторинг процессов – непрерывное наблюдение и анализ вашей компьютерной сети или систем для предотвращения кибератак. Главная задача мониторинга – оперативное выявление уязвимости и реагирования на потенциальные угрозы безопасности в режиме реального времени.

Центральное место в любой стратегии кибербезопасности занимает аутентификация – процесс проверки личности пользователя перед получения доступа к ресурсам. Проверка осуществляется с помощью одного или нескольких факторов, но в общем их можно разделить на 3 типа:

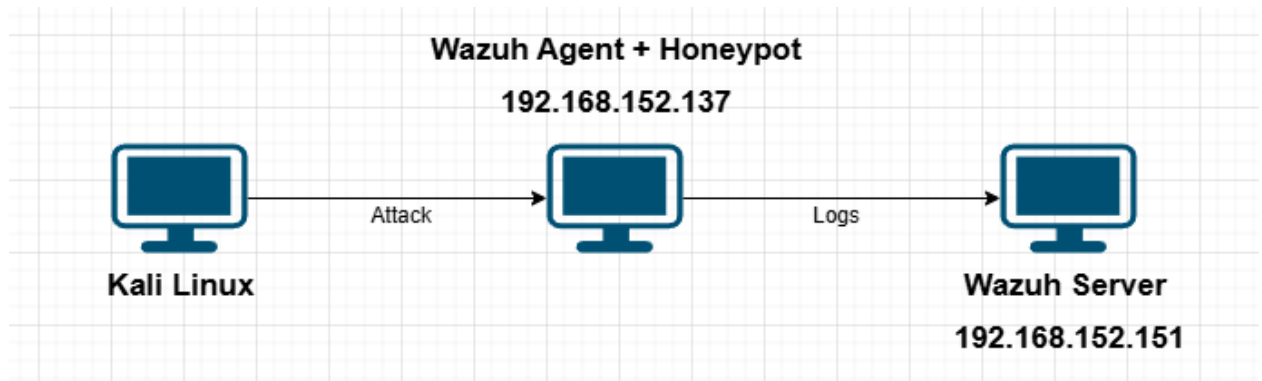
1. Something You Know (то, что вы знаете) – это может быть пароли, PIN-коды.
2. Something You Have (то, что у вас есть) – можно отнести смарт-карты, токены.
3. Something You Are (то, чем вы являетесь) – биометрические данные.

Сегодня основными угрозами для сетевой безопасности является сетевые атаки. Для борьбы с этой угрозой внедряются механизмы тестирования безопасности. Симуляция сетевых атак – моделирует стратегии атак для анализа фактического поведения и намерений в отношении сети. Благодаря сетевым атакам можно выявить стратегию, путь вторжения, место проникновения – в общем говоря самые уязвимые места. И в дальнейшем исправить эту уязвимость.

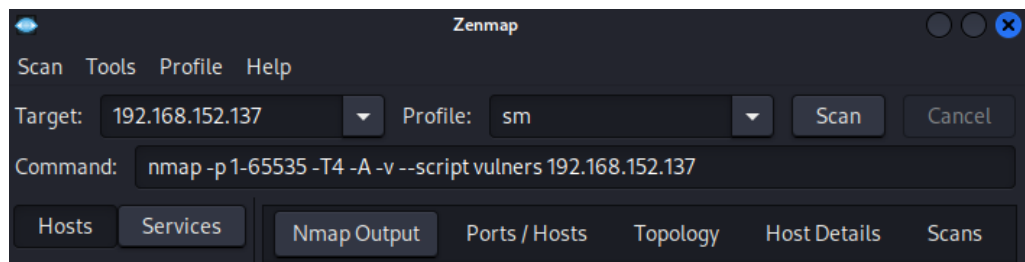
Для создания своей сети и проведения симуляции на ней нужно выбрать соответствующие программные средства. Моделирование атак в тестовой среде достигается благодаря виртуальным машинам.

Для проведения симуляции сетевых атак и оценки эффективности системы мониторинга безопасности была развернута тестовая среда на основе виртуальных машин в VMware Workstation.

Моя тестовая среда.



Симуляция атаки. Сканирование портов и уязвимостей.



Атака в логах

The diagram illustrates a SCADA system architecture with the following components and connections:

- External Network:** Represented by a cloud icon on the left.
- Firewall:** A red brick wall icon that filters traffic between the external network and the internal system.
- VPN:** Two connections labeled "VPN, порт 1194" (VPN, port 1194) are shown. One connects the external network to the firewall, and the other connects the firewall to a server icon.
- DMZ:** A server icon in the DMZ zone receives traffic from the VPN and connects to the internal network.
- Internal Network:** Contains several components:
 - SCADA Server:** A server icon that receives "Имитация SCADA-сервера" (SCADA server emulation) from the DMZ server.
 - Modbus TCP:** A server icon that receives "Modbus TCP, порт 502" (Modbus TCP, port 502) from the DMZ server.
 - OPC UA:** Two server icons that receive "OPC UA, порт 4840" (OPC UA, port 4840) from the DMZ server.
 - Interface Operator BAM:** A server icon that receives data from the OPC UA servers.
 - Warning:** A yellow box labeled "Warning" is connected to the SCADA server.
- Attack:** An orange box labeled "Атака на хонипот" (Attack on honeypot) is connected to the SCADA server.
- Security:** A green padlock icon is connected to the SCADA server.
- Monitoring:** A green icon with a magnifying glass is connected to the SCADA server.
- Cloud:** A blue cloud icon with an upward arrow is connected to the SCADA server.
- Operator Interface:** Two computer icons are connected to the SCADA server.

409

УДК 004.89

Калижан А.,К., Глазырина Н.С. (Астана, ЕНУ им. Л.Н. Гумилева)

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ СПУФИНГ-АТАК НА СИСТЕМЫ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

Современные биометрические системы аутентификации играют ключевую роль в обеспечении контроля доступа и защите информации благодаря использованию уникальных физиологических характеристик пользователей. Однако стремительное развитие алгоритмов глубокого обучения и технологий синтеза медиа привело к появлению новых угроз. Спуфинг-атаки и дипфейки позволяют злоумышленникам обходить традиционные механизмы распознавания с использованием поддельных изображений, видео или аудиозаписей.

Спуфинг-атаки заключаются в имитации биометрических данных с использованием поддельных изображений, видеозаписей или физических объектов, таких как маски. Системы распознавания лиц особенно уязвимы перед такими атаками, поскольку их алгоритмы могут быть обмануты высококачественными фотографиями, видеозаписями или экранами смартфонов, демонстрирующими ранее записанные видеоролики. Дипфейки, создаваемые алгоритмами глубокого обучения, позволяют ещё более изощрённо имитировать внешний облик пользователей, воспроизводя не только их черты, но и мимику, голос и движения [1]. Применение инфракрасных проекций для создания искажения внешних черт лица, а также использование дипфейков, воспроизводящих мимику, голос и движения с высокой степенью реализма, демонстрирует, что даже современные системы распознавания остаются уязвимыми к целенаправленным и тщательно подготовленным атакам.

Традиционные методы распознавания, основанные на статическом анализе изображений или аудиозаписей, оказываются недостаточными при использовании синтетически созданных материалов. Они не способны отразить динамику физиологических реакций человека. В связи с этим всё чаще применяются методы определения жизненности (liveness detection) [2], фиксирующие естественные динамические параметры, такие как ритм моргания, микроизменения мимики, плавность движений глаз и характерные особенности голосовых паттернов. Анализ видеозаписей и аудиоданных в реальном времени позволяет выявить даже незначительные расхождения между подлинными сигналами и их синтетическими аналогами.

Для повышения устойчивости биометрических систем внедряются методы определения жизненности, основанные на анализе динамических физиологических реакций человека: моргания, движений глаз, микроизменений мимики и целостности голосовых сигналов. Это позволяет отличить настоящие биометрические данные от синтезированных или воспроизведённых записей [3]. Естественную динамику живого организма крайне сложно воспроизвести с требуемой точностью, что значительно усложняет задачу злоумышленникам.

Разработанный программный модуль для анализа живости был интегрирован в архитектуру биометрической системы аутентификации, позволяя проводить детальный анализ входящих видеопотоков и аудиозаписей в режиме реального времени. При проверке фиксируются естественные физиологические реакции, такие как микродвижения, моргание и физиологические особенности. На рисунке 1 показан неудачный сценарий попытки

мошенничества, когда система обнаруживает использование неподлинных биометрических данных, например изображение с экрана телефона или синтетическое видео. В таких случаях доступ к системе автоматически блокируется, предотвращая возможность взлома.

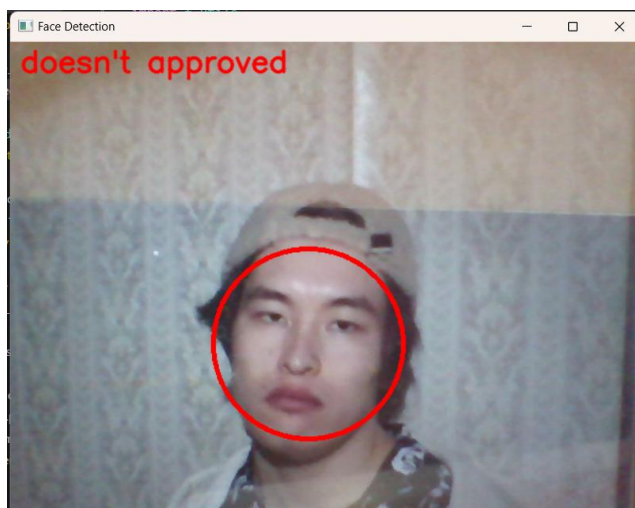


Рисунок 1. Обнаружен обман системы. Лицо со смартфона не считывается

Обработка видеопотоков посредством алгоритмов позволяет точно определить динамические изменения, присущие живым объектам, что делает невозможным успешное использование поддельных данных. После прохождения всех этапов проверки пользователю предоставляется доступ к системе, как это продемонстрировано на рисунке 2, где показан успешный вход после подтверждения аутентичности.

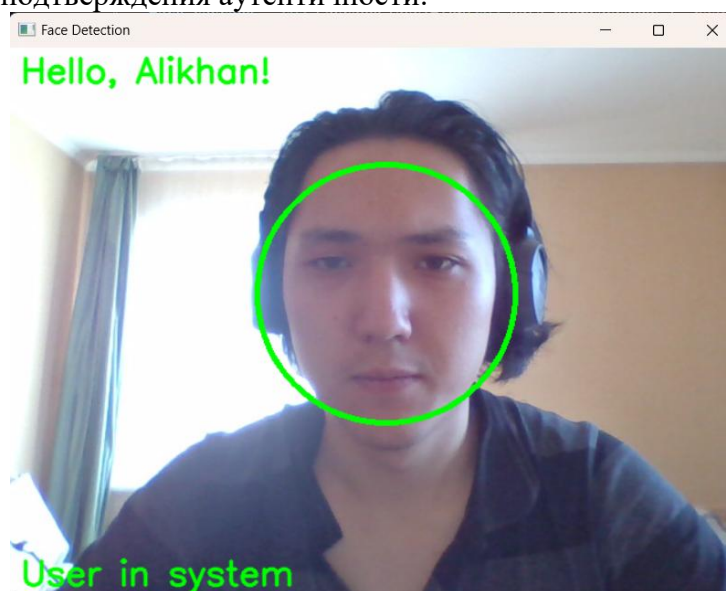


Рисунок 2. Успешная авторизация

Разработанное программное обеспечение для обнаружения спуфинг-атак на системы биометрической аутентификации может быть эффективно интегрировано в банковские структуры, государственные учреждения и системы информационной безопасности. Это обеспечит надёжную защиту от попыток несанкционированного доступа с использованием поддельных биометрических данных и повысит устойчивость систем аутентификации к

современным угрозам, связанным с применением дипфейков и иных методов манипуляций с видеоданными.

Список использованных источников

1. Дипфейки как средство взлома систем биометрической идентификации: отчёт Европейского института. [Электронный ресурс]. Режим доступа: <https://d-russia.ru/dipfeji-kak-sredstvo-vzloma-sistem-biometricheskoj-identifikacii-otchjot-evropejskogo-instituta.html> (дата обращения: 31.03.2025)
2. Механизмы защиты от атак на биометрическое предъявление. [Электронный ресурс]. Режим доступа: <https://plusworld.ru/journal/2024/plas-7-8-315-2024/mekhanizmy-zashchity-ot-atak-na-biometricheskoe-predyavlenie/> (дата обращения: 31.03.2025)
3. Биометрия | Что такое биометрические данные. [Электронный ресурс]. Режим доступа: <https://elbrusboot.camp/blog/что-такое-биометрические-данные/> (дата обращения: 31.03.2025)

Конырханова А.А.,
Тұрарғазин Ж.С.
(Астана, ЕНУ им Л.Н. Гумилева)

РОЛЬ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА В ОБЕСПЕЧЕНИИ КИБЕРБЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАЦИОННО- КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ

ВВЕДЕНИЕ

Актуальность темы. Критически важные объекты информационно-коммуникационной инфраструктуры (далее – КВОИКИ) – объекты информационно-коммуникационной инфраструктуры, нарушение или прекращение функционирования которых приводит к незаконному сбору и обработке персональных данных ограниченного доступа и иных сведений, содержащих охраняемую законом тайну, чрезвычайной ситуации социального и (или) техногенного характера или значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, отдельных сфер хозяйства или жизнедеятельности населения, проживающего на соответствующей территории, в том числе инфраструктуры: теплоснабжения, электроснабжения, газоснабжения, водоснабжения, промышленности, здравоохранения, связи, банковской сферы, транспорта, гидротехнических сооружений, правоохранительной деятельности, «электронного правительства» [1].

КВОИКИ имеет первостепенное значение, поскольку эти системы являются основой современного общества. Они обеспечивают функционирование государства, поддерживают обороноспособность, стабильность финансовой системы, работу промышленности и торговли, а также предоставление жизненно важных услуг населению, таких как здравоохранение, транспорт, энергетика и связь. В условиях нашей растущей зависимости от цифровых технологий в повседневной жизни, от онлайн-банкинга и коммуникаций до управления транспортом и доступом к медицинским услугам, нарушение работы этих критически важных объектов в результате кибератак может привести к серьезным

последствиям, затрагивающим национальную и глобальную безопасность, экономическую стабильность и благополучие каждого человека. Трансграничный характер киберугроз и взаимосвязанность мировых инфраструктур делают защиту этих систем не только национальной, но и международной задачей, требующей скоординированных усилий мирового сообщества. По официальным данным Комитет по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан количество КВОИКИ Республики Казахстан показаны на рисунке 1.

В последние годы наблюдается устойчивый рост как числа, так и сложности кибератак, направленных на критически важные объекты информационно-коммуникационной инфраструктуры. Общая тенденция свидетельствует об увеличении количества зарегистрированных инцидентов, при этом злоумышленники все чаще используют более изощренные методы и инструменты, что представляет собой серьезную и постоянно возрастающую угрозу для безопасности и стабильности ключевых систем жизнеобеспечения [2].

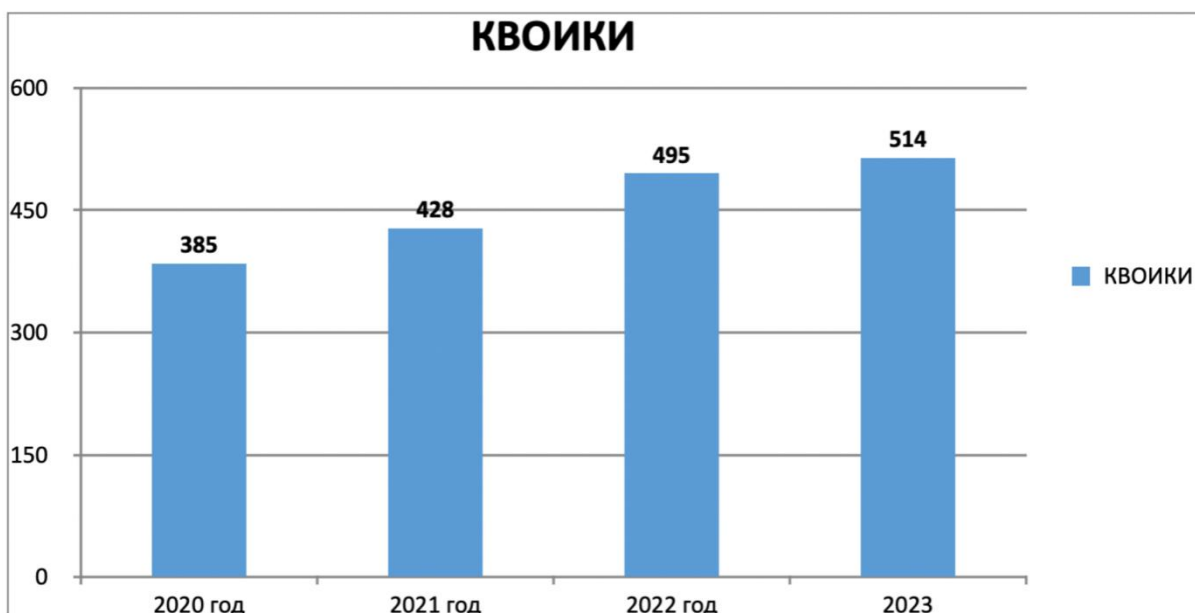


Рисунок 1 Количество КВОИКИ

Тезис доклада. «Международное сотрудничество является ключевым фактором в эффективном обеспечении кибербезопасности КВОИКИ в условиях глобального характера киберугроз».

Целью данного доклада является рассмотрение роли и значения международного сотрудничества в обеспечении кибербезопасности КВОИКИ в условиях современных глобальных киберугроз.

Глобальный характер киберугроз. Киберпространство не имеет физических границ, и кибератаки могут быть организованы и осуществлены из любой точки мира. Анонимность и сложность атрибуции кибератак, что затрудняет привлечение злоумышленников к ответственности на национальном уровне. Киберпреступные группировки и даже государства могут координировать свои действия на международном уровне [3-5].

Трансграничность атак. Зачастую бывает сложно установить точное местонахождение атакующего, так как используются промежуточные серверы и анонимные сети. Киберпреступники могут находиться в одной стране, атаковать объекты в другой и использовать инфраструктуру третьей страны для сокрытия следов.

Взаимосвязанность инфраструктур. КВОИКИ разных стран могут быть взаимосвязаны (например, международные энергетические сети, системы управления воздушным движением, глобальные финансовые системы). Успешная атака на КВОИКИ в одной стране может иметь каскадные последствия и повлиять на функционирование критически важных объектов в других странах.

Необходимость международного сотрудничества

Обмен информацией об угрозах и уязвимостях. Своевременный обмен данными об обнаруженных киберугрозах, вредоносном программном обеспечении, индикаторах компрометации (IOCs) и уязвимостях позволяет странам лучше понимать текущую ситуацию и принимать превентивные меры. Важность создания доверенных каналов обмена информацией между национальными центрами кибербезопасности (CERT/CSIRT) разных стран.

Разработка общих стандартов и лучших практик. Необходимость разработки и внедрения согласованных международных стандартов и рекомендаций в области кибербезопасности КВОИКИ для повышения общего уровня защищенности. Такие стандарты могут быть полезны (например, стандарты безопасности для промышленного контроля, протоколы обмена информацией об инцидентах).

Совместные исследования и разработки. Сотрудничество в области научных исследований и разработок позволяет объединять усилия и ресурсы для создания более эффективных технологий и методов защиты от новых и возникающих киберугроз. Обмен знаниями и опытом между экспертами разных стран очень важен.

Координация действий при реагировании на инциденты. В случае крупной кибератаки, затрагивающей несколько стран, скоординированные действия на международном уровне могут быть необходимы для эффективного реагирования, локализации ущерба и восстановления работоспособности систем. Важность разработки совместных планов действий и проведения международных учений по кибербезопасности.

Развитие международного права и сотрудничество в правоохранительной сфере. Необходимость создания международно-правовых механизмов для борьбы с киберпреступностью, включая вопросы юрисдикции, экстрадиции и взаимной правовой помощи. Очень важно сотрудничество между правоохранительными органами разных стран для расследования киберпреступлений и привлечения виновных к ответственности.

Примеры и формы международного сотрудничества:

Организация Объединенных Наций (ООН) играет важную роль в содействии международному сотрудничеству в области кибербезопасности и защиты критической инфраструктуры посредством разработки норм поведения государств в киберпространстве, поддержки наращивания потенциала в развивающихся странах и борьбы с киберпреступностью;

Организация по безопасности и сотрудничеству в Европе (ОБСЕ) активно способствует укреплению кибербезопасности и защите критической инфраструктуры в своем регионе посредством разработки мер доверия и безопасности в киберпространстве, поддержки наращивания потенциала и содействия диалогу и сотрудничеству между своими государствами-участниками;

Группа семи (G7) предпринимает различные инициативы в сфере кибербезопасности и защиты критической инфраструктуры, включая разработку принципов, координацию политики через экспертную группу и сотрудничество в борьбе с конкретными угрозами, такими как программы-вымогатели и атаки на энергетический сектор;

Европейский Союз (ЕС) активно работает над укреплением кибербезопасности и защиты критической инфраструктуры посредством принятия законодательных актов, таких

как Директива NIS2, деятельности Агентства ЕС по кибербезопасности (ENISA), а также финансирования исследований и международного сотрудничества в этой области;

Ассоциация государств Юго-Восточной Азии (АСЕАН) предпринимает усилия по укреплению регионального сотрудничества в области кибербезопасности и защиты критической инфраструктуры посредством разработки соответствующих рамок, создания центров и инициатив, направленных на наращивание потенциала и обмен информацией между государствами-членами;

Организация американских государств (ОАГ) активно продвигает кибербезопасность и защиту критической инфраструктуры в регионе посредством разработки стратегий, наращивания потенциала, борьбы с киберпреступностью и содействия сотрудничеству между государствами-членами.

Также международные партнерства играют ключевую роль в обеспечении кибербезопасности и защиты критической инфраструктуры, объединяя усилия различных государств, международных организаций, частного сектора и научных учреждений для обмена информацией, совместной разработки решений и скоординированного реагирования на глобальные киберугрозы.

В заключение следует подчеркнуть, что возрастающая сложность и трансграничная природа киберугроз, направленных на КВОИКИ, делают международное сотрудничество не просто желательным, а абсолютно необходимым условием для обеспечения глобальной кибербезопасности и устойчивости этих жизненно важных систем. Только объединив усилия на межгосударственном уровне, обмениваясь информацией, разрабатывая общие стандарты и координируя действия, мировое сообщество сможет эффективно противостоять этим вызовам и обеспечить безопасное и стабильное цифровое будущее.

Таким образом, международное сотрудничество является ключевым фактором в эффективном обеспечении кибербезопасности критически важных объектов информационно-коммуникационной инфраструктуры в условиях глобального характера киберугроз.

Для обеспечения устойчивого и безопасного функционирования критически важных объектов информационно-коммуникационной инфраструктуры в будущем крайне важно дальнейшее развитие и укрепление международного сотрудничества в области кибербезопасности. Это включает в себя необходимость повышения уровня взаимного доверия между государствами, гармонизацию национального законодательства в сфере кибербезопасности и активизацию усилий по наращиванию потенциала как на национальном, так и на международном уровнях.

Список использованных источников

1. «Об утверждении Правил и критериев отнесения объектов информационно-коммуникационной инфраструктуры к критически важным объектам информационно-коммуникационной инфраструктуры» Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 30 июня 2023 года № 221/НК. Зарегистрирован в Министерстве юстиции Республики Казахстан 1 июля 2023 года № 32996;
2. КИБЕРКОД 2024: вызовы цифровой эпохи (Электронный ресурс) <https://sts.kz/wp-content/uploads/2025/02/kiberdajdzhest-final-1402.pdf>;
3. Василенко И. А. Анализ рисков и направлений их устранения для национальной критической информационной инфраструктуры в условиях роста угроз безопасности // Вестник НИЯУ МИФИ. – 2025. – Т. 14. – №. 1. – С. 79-84;
4. Тюменцев К. А., Котыбаев А. А., Человечкова А. В. АНАЛИЗ ВЛИЯНИЯ КИБЕРАТАК НА РАБОТУ КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУР // ББК 72я43 Н34. – 2024. – С. 107;

5. Никифоров А. В., Кафиатулина А. В. ОПЫТ США И ОТДЕЛЬНЫХ ГОСУДАРСТВ ЕВРОПЫ В ОБЛАСТИ НОРМАТИВНОГО РЕГУЛИРОВАНИЯ НЕПРАВОМЕРНОГО ВОЗДЕЙСТВИЯ НА КРИТИЧЕСКУЮ ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ: КЕЙС-СТАДИ EXPERIENCE OF THE USA AND INDIVIDUAL EUROPEAN STATES IN THE FIELD OF REGULATORY REGULATION OF UNLAWFUL IMPACT ON CRITICAL INFORMATION //Журнал выпускается ежемесячно, публикует статьи по юридическим наукам. Подробнее на [www. ur. – 2025. – С. 42.](http://www.ur.uz)

УДК 004.83

Кутышев В.В.
(Астана, ЕНУ)

КАК ЗАЩИТИТЬ ПЕРСОНАЛЬНЫЕ ДАННЫЕ ПОЛЬЗОВАТЕЛЕЙ В ОБУЧАЮЩИХ AI-СИСТЕМАХ

Развитие искусственного интеллекта (ИИ) в образовательных системах открывает новые возможности для персонализации обучения, повышения эффективности усвоения материала и автоматизации процессов. Однако с расширением функциональности обучающих ИИ-систем возрастает и риск нарушения конфиденциальности пользователей. В частности, при обучении моделей используются большие объёмы данных, часто содержащих персональные сведения учащихся, что требует особого внимания к вопросам безопасности и защиты информации.

В данном докладе рассматриваются основные угрозы, связанные с обработкой персональных данных в обучающих ИИ-системах, а также методы и технологии, позволяющие снизить риск утечек и несанкционированного доступа. Приведённые рекомендации базируются на анализе современных исследований в области защиты данных, включая работы по методам анонимизации, шифрованию и федеративному обучению, что позволяет обеспечить высокий уровень безопасности при обучении моделей.

1. Основные угрозы обработки персональных данных в обучающих ИИ-системах

Обучающие ИИ-системы ориентируются на сбор, обработку и анализ большого количества данных. При этом могут возникать следующие ключевые угрозы:

1.1. Риск раскрытия конфиденциальной информации.

Данные, используемые для обучения моделей, могут содержать конфиденциальную информацию о учащихся: имена, контактные данные, успеваемость, результаты тестирований и прочую личную информацию. При несоблюдении требований к сбору и обработке таких данных угроза их утечки либо несанкционированного доступа становится одной из достаточно серьезных [1].

1.2. Атаки на обучающие выборки.

Злоумышленники могут целенаправленно внедрять вредоносные или искажённые данные в обучающие наборы. Это приведёт к формированию моделей с ошибочными прогнозами. Такие атаки могут значительно снизить точность моделей, а также способствовать несанкционированному использованию персональных данных [3].

1.3. Уязвимости ML-моделей.

Модели, получаемые в результате обучения, могут «выучивать» (overfitting) специфические данные, что создаёт возможность их извлечения через атаки, например атаки получения членства (membership inference attacks), более того, перенастройка или применение модели в условиях, значительно отличных от исходных, может привести к утечке информации о пользователях [2].

2. Методы и технологии защиты персональных данных

С целью обеспечения безопасности данных в обучающих ИИ-системах используются следующие подходы и методы:

2.1. Анонимизация и псевдонимизация.

Для минимизации риска раскрытия идентифицируемой информации применяются методы анонимизации и псевдонимизации. Эти технологии позволяют заменить реальные идентификаторы на искусственные значения, что существенно снижает возможность восстановления исходных данных в случае утечки [1].

2.2. Шифрование данных.

Как на этапах хранения, так и при передаче данных следует применять криптографические алгоритмы шифрования. Использование современных стандартов шифрования позволяет защитить данные от несанкционированного доступа, даже если злоумышленник получает доступ к базе данных или перехватывает сетевой трафик [2].

2.3. Федеративное обучение.

Одним из инновационных подходов является федеративное обучение, при котором модель обучается на локальных данных пользователей, а не централизованно. Таким образом, исходные данные остаются на устройствах пользователей, а лишь параметры модели агрегируются на сервере. Это позволяет значительно уменьшить риск утечки конфиденциальной информации [4].

2.4. Политика минимизации данных.

Ключевым принципом является сбор и обработка только тех данных, которые необходимы для достижения конкретных образовательных целей. Применение политики минимизации подразумевает регулярное обновление данных, их удаление или анонимизацию по окончании срока использования, что соответствует принципу ограничения хранения информации [3].

2.5. Контроль доступа и мониторинг.

Обеспечение безопасности персональных данных требует строгой реализации механизмов аутентификации, авторизации и контроля доступа. Применение принципа наименьших привилегий позволяет ограничить доступ к данным только тем сотрудникам, которым это необходимо для выполнения служебных обязанностей. Дополнительно, системы мониторинга и протоколирования помогают своевременно обнаруживать и реагировать на попытки несанкционированного доступа [2].

3. Практические рекомендации по реализации защиты данных

Для повышения уровня безопасности персональных данных в обучающих ИИ-системах рекомендуется следующее:

Разработка внутренней политики безопасности.

Создание и внедрение чётких процедур по обработке, хранению и удалению персональных данных. Внутренняя документация должна описывать ответственность всех участников процессов и обеспечивать прозрачность операций с данными.

Проведение регулярных аудитов и тестирований.

Систематические проверки состояния безопасности, анализ уязвимостей и проведение тестов на проникновение позволяют своевременно выявлять и устранять слабые места в системе.

Использование современных технологий защиты.

Применение технологий анонимизации, шифрования и федеративного обучения должно стать неотъемлемой частью разработки обучающих ИИ-систем. Внедрение таких решений повышает устойчивость системы к атакам и снижает риск утечек.

Обучение персонала.

Регулярное обучение сотрудников вопросам безопасности и защиты персональных данных помогает создать культуру ответственности и способствует более эффективной реализации технических мер.

Контроль и ограничение доступа.

Необходимо внедрять многоуровневую систему контроля доступа с использованием аутентификации на основе риска и принципа наименьших привилегий, чтобы гарантировать, что доступ к данным получают только уполномоченные лица.

Закключение

В условиях стремительного развития обучающих AI-систем защита персональных данных пользователей становится критически важной задачей. Современные методы, такие как анонимизация, шифрование и федеративное обучение, в сочетании с политикой минимизации данных и строгим контролем доступа, позволяют обеспечить высокий уровень безопасности и конфиденциальности. Внедрение комплексной системы мер защиты, регулярный аудит и обучение персонала создают условия для формирования доверия пользователей и успешной эксплуатации AI-систем в образовательной сфере.

Реализация описанных мер позволит не только снизить риски утечек и несанкционированного доступа, но и повысить качество и надёжность обучающих систем, способствуя развитию инновационных подходов в образовании. При этом важно помнить, что защита данных должна рассматриваться как динамический процесс, требующий постоянного обновления и совершенствования в соответствии с изменяющейся технологической средой и нормативными требованиями.

Список использованных источников

1. Козин О.С. Метод обеспечения безопасности персональных данных при их обработке в информационной системе на основе анализа поведения пользователей // Информационно-управляющие системы. 2018. № 3. С. 69-78.
2. Jihan Alosi, Islam Ismail. Data Privacy in AI- Driven Education An In-Depth Exploration Into the Data Privacy Concerns and Potential Solutions. // Impacts of Generative AI on the Future of Research and Education. 2025. P. 26. 10.4018/979-8-3693-0884-4.ch006
3. Lan Huang, Ethics of artificial intelligence in education: student privacy and data protection // Science insights education frontiers. PP. 2577-2587. 10.15354
4. Waqar Ali, Rajesh Kumar, Zhiyi Deng, Yansong Wang, jie Shao. A federated Learning approach for privacy protection in context-aware Recommender systems. // The computer journal. 2021. P. 1

УДК 004.056.53

Маер С.А.
(Астана, ЕНУ им. Н.И.Гумилёва)

ИНТЕГРАЦИЯ СИСТЕМ ОБУЧЕНИЯ ДЛЯ ПОВЫШЕНИЯ УСТОЙЧИВОСТИ СОТРУДНИКОВ ОТ АТАК ТИПА ФИШИНГ

1. Актуальность темы

Фишинг остаётся одной из самых частых и опасных угроз, с которой сталкиваются организации в XXI веке. Злоумышленники применяют методы социальной инженерии и маскируются под легитимных отправителей, чтобы обманом получить доступ к конфиденциальным данным или заставить сотрудников совершить опасные действия. В

условиях, когда технические средства защиты несовершенны и уязвимы перед целевыми атаками, именно человек становится «последним рубежом» обороны. Это делает обучение сотрудников и формирование культуры информационной безопасности критически важной задачей.

2. Цель и задачи исследования

Цель исследования — разработать комплексный подход к защите от фишинга, который бы сочетал технические меры и обучение сотрудников. Основные задачи:

Проанализировать современные фишинговые угрозы и векторы атак;

Изучить возможности и ограничения технических средств;

Сформировать методику подготовки персонала;

Реализовать практические меры тестирования (в том числе через фишинговые письма);

Разработать систему оценки и адаптации защиты на основе полученных данных.

3. Методология исследования

Применён системный подход, включающий:

Анализ данных от международных ИБ-компаний (Positive Technologies, Proofpoint, APWG);

Изучение уязвимых отраслей и видов фишинга;

Оценку технических мер защиты;

Разработку программы обучения;

Реализацию тестирования с последующей обработкой результатов;

Интеграцию полученных данных в защитную инфраструктуру.

4. Ключевые результаты по этапам исследования

4.1. Анализ фишинговых угроз

Анализ показал:

85% атак направлены на кражу данных, 26% — на финансовую выгоду;

В 92% случаев используется электронная почта, но растёт доля атак через мессенджеры и соцсети;

Наиболее уязвимы госучреждения (44%), оборонные компании (19%), образовательные организации (14%);

Используются различные техники: массовый фишинг, spear phishing, whaling, BEC, атаки с применением ИИ.

4.2. Изучение технических мер защиты

Рассмотренные средства:

Брандмауэры: блокируют трафик, но не защищают от e-mail-угроз;

Фильтры контента: эффективны, но отстают из-за быстрой смены вредоносных URL;

Почтовые шлюзы: фильтруют массовый фишинг, но слабы против таргетированных атак;

DLP и EDR: усиливают защиту на конечных точках, но требуют настройки и постоянного анализа.

Вывод: технические решения работают эффективно в комплексе, но не гарантируют полной защиты без участия человека.

4.3. Разработка программы обучения

Создана обучающая программа из трёх модулей:

Теоретическая часть — лекции, видеоуроки, вебинары:

признаки фишинга;

виды атак;

действия при подозрительных письмах.

Интерактивные задания — практические кейсы:

анализ писем с фальшивыми адресами;

распознавание фейковых ссылок и вложений;
разбор реальных ситуаций.

Тестирование знаний — небольшие тесты, situational-based задачи, быстрая обратная связь.

Программа адаптировалась под разные подразделения: финансовые службы, HR, ИТ-отделы получали отдельные тематические задания.

4.4. Реализация системы тестовых фишинговых писем

Этот этап стал основой практического эксперимента и ключевым для оценки готовности персонала:

Создана база фальшивых писем:

простые примеры: орфографические ошибки, подозрительные адреса;

сложные кейсы: поддельные письма от внутренних сотрудников, HR-службы, бухгалтерии, ИТ-поддержки.

Метрики оценки поведения сотрудников:

процент переходов по вредоносным ссылкам;

открытие вложений;

своевременное сообщение в ИБ;

реакция на подозрительные письма (игнор, ответ, перенаправление).

Результаты:

фиксировалось снижение количества переходов по вредоносным ссылкам при регулярных тестированиях;

после второго раунда фишинга количество сообщений о подозрительных письмах увеличилось на 32%;

наибольшее количество ошибок допускали новые сотрудники и те, кто ранее не проходил обучение;

руководители среднего звена чаще попадались на сложные сценарии (whaling).

4.5. Интеграция и обратная связь

На последнем этапе разработана система замкнутого цикла «обучение — тестирование — корректировка»:

Настройка фильтров: по результатам тестов обновлялись правила почтовых шлюзов и фильтрации контента.

Система обратной связи:

сотрудники могли нажатием кнопки сообщить о фишинге;

в ответ — автоматическое уведомление о правильности действия и инструкции;

создана база инцидентов для анализа и обучения.

Адаптация под роль и функции:

финансовые отделы получали письма с фальшивыми счетами;

HR — письма с поддельными резюме или запросами на выплату;

ИТ — кейсы с вредоносными ссылками на "обновление ПО".

5. Практические рекомендации

Обучение должно проводиться регулярно — раз в квартал или полгода;

Тестирование должно быть частью повседневной практики;

Важно учитывать специфику разных отделов и уровней доступа;

Обратная связь должна быть оперативной и полезной;

Технические системы надо адаптировать под поведение сотрудников.

6. Заключение

Фишинг — это не просто техническая угроза, а серьёзный вызов культуре безопасности в организации. Технические решения необходимы, но не могут заменить обученного, внимательного пользователя. Регулярное обучение, тестирование и участие сотрудников в

процессе ИБ делают организацию более устойчивой к атакам. Комплексный подход, описанный в исследовании, позволяет повысить уровень защищённости, минимизировать риски и сформировать ответственное отношение к информационной безопасности.

Список литературы

1. ISO/IEC 27035:2016. Управление инцидентами информационной безопасности. – Женева: Международная организация по стандартизации, 2016. – 40 с.
2. NIST Special Publication 800-61 Revision 2. Руководство по обработке инцидентов компьютерной безопасности. – Национальный институт стандартов и технологий (NIST), 2012. – URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> (дата обращения: 15.12.2023).
3. SANS Institute. Планирование и реализация осведомлённости в области безопасности. – SANS Security Awareness. – URL: <https://www.sans.org/security-awareness-training/> (дата обращения: 15.12.2023).
4. ENISA (Европейское агентство по кибербезопасности). Ландшафт угроз фишинга и лучшие практики по их предотвращению. – URL: <https://www.enisa.europa.eu/> (дата обращения: 15.12.2023).
5. Junger M., Montoya L., Overink F.J. Подготовка и предупреждения неэффективны для предотвращения атак социальной инженерии // *Computers in Human Behavior*. – 2017. – Т. 66. – С. 75-87.

УДК 004.06

Мухтарова З.Б.
ЕНУ им. Л.Н.Гумилева

ПРОБЛЕМЫ И ВЫЗОВЫ ВНЕДРЕНИЯ МАШИННОГО ОБУЧЕНИЯ В ПРОЦЕССЫ АВТОМАТИЗИРОВАННОГО АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация

В последние десятилетия машинное обучение (МО) становится важным инструментом в автоматизированном аудите информационной безопасности (ИБ), улучшая эффективность обнаружения угроз, оптимизацию процедур аудита и ускорение реакции на инциденты. Однако внедрение МО сталкивается с рядом проблем, таких как качество данных для обучающих выборок, интерпретируемость моделей и сложности интеграции с существующими системами безопасности. В статье анализируются также организационные барьеры, такие как подготовка специалистов и управление изменениями. Исследование направлено на выявление ключевых факторов успешного внедрения МО в аудит ИБ и предложения по их преодолению. Результаты будут полезны специалистам и разработчикам в области информационной безопасности.

Ключевые слова: машинное обучение, информационная безопасность, автоматизированный аудит, проблемы и вызовы, защита данных, киберугрозы, алгоритм машинного обучения.

Введение

Современная информационная безопасность сталкивается с постоянным увеличением объема данных и сложностью угроз, что делает традиционные методы аудита недостаточными для оперативного реагирования на инциденты. В последние годы активно разрабатываются и внедряются методы машинного обучения для автоматизации процессов аудита информационной безопасности, что обещает значительные улучшения в выявлении аномалий и угроз. Согласно отчету Gartner [1], более 60% организаций по всему миру заявляют, что они используют автоматизированные инструменты для мониторинга и анализа безопасности данных, что подтверждает растущую потребность в более совершенных технологиях в области аудита. Однако на практике внедрение МО в эти процессы сопровождается множеством сложностей, которые необходимо решить для эффективного использования этой технологии.

Целью данной статьи является исследование проблем и вызовов, с которыми сталкиваются организации при внедрении машинного обучения в процессы автоматизированного аудита информационной безопасности. Основное внимание уделяется вопросам качества данных, подготовки обучающих выборок, интерпретируемости моделей и интеграции новых технологий в существующие системы. Также рассматриваются организационные аспекты, такие как подготовка персонала и управление изменениями.

Машинное обучение в контексте аудита информационной безопасности направлено на улучшение процессов обнаружения аномалий, анализа угроз и автоматизации мониторинга безопасности в реальном времени. Применение МО позволяет системе аудита автоматически адаптироваться к новым угрозам, обучаясь на основе исторических данных и текущих инцидентов. Согласно McKinsey & Company [2], 75% организаций, использующих машинное обучение для аудита безопасности, утверждают, что оно значительно повысило точность и эффективность выявления угроз и рисков.

Методы и материалы

Для исследования использовались методы системного анализа и анализа литературы. Изучены теоретические разработки и последние исследования по внедрению машинного обучения в аудит безопасности, включая работы в области ИБ, аналитики данных и обработки больших данных. Рассмотрены примеры применения МО в аудите безопасности в крупных организациях. Анализ базировался на общедоступных публикациях, материалах исследовательских и консалтинговых компаний, а также практическом опыте специалистов в ИБ.

Результаты и дискуссия

Машинное обучение стало важным инструментом в информационной безопасности, особенно для обработки данных, содержащих интеллектуальную собственность и личную информацию. Существуют нормативные акты, такие как GDPR и CCPA, регулирующие использование таких данных. Машинное обучение эффективно выявляет новые угрозы, включая вредоносное ПО и АРТ-атаки, позволяя предотвращать их на ранних стадиях. Современные методы, такие как анализ поведения пользователей и прогнозная аналитика, помогают обнаруживать и минимизировать последствия кибератак. Искусственный интеллект (ИИ) и МО предоставляют новые возможности для повышения эффективности аудита информационной безопасности, обеспечивая автоматизацию процессов обнаружения, анализа и реагирования на угрозы [3].

Основные преимущества применения ИИ и МО включают: автоматизация процессов, обнаружение новых угроз, снижение ложных срабатываний, быстрое реагирование, прогнозирование угроз.

Основными проблемами внедрения МО в аудиторские процессы являются [4]:

1. Качество данных. МО модели требуют больших объемов качественных данных, и их неполнота или ошибки могут снижать точность моделей и эффективность аудита.
 2. Подготовка обучающих выборок. Создание репрезентативных выборок для обучения МО моделей в области ИБ осложняется многогранностью угроз, что затрудняет формирование эффективных наборов данных.
 3. Интерпретируемость моделей. МО модели должны быть понятны и обоснованы специалистами для принятия решений. Отсутствие интерпретируемости мешает использованию результатов аудита.
1. Интеграция с существующими системами. Внедрение МО в существующие системы управления безопасностью требует значительных усилий и затрат. Более 40% организаций сталкиваются с трудностями интеграции новых технологий в устаревшие инфраструктуры.
 2. Организационные аспекты. Необходима подготовка специалистов и управление изменениями. 53% организаций отмечают дефицит кадров в области безопасности данных и МЛ, что затрудняет внедрение технологий.
 3. Этика и защита данных. Внедрение МО в аудит может повлечь риски утечек данных и нарушение конфиденциальности. Важно соблюдать законодательство о защите персональных данных, как, например, GDPR в ЕС.

Заключение

Для успешной интеграции МО в аудит информационной безопасности необходимо развивать как технологическую инфраструктуру, так и кадровый потенциал. Внедрение облачных вычислений, платформ для анализа больших данных и развитие параллельных вычислений помогут обеспечить необходимую вычислительную мощность для работы сложных моделей МО. Разработка стандартов для использования машинного обучения в аудите информационной безопасности поможет создать единые требования и рекомендации для организаций. Это может включать стандарты для сбора и обработки данных, а также требования к обеспечению прозрачности и интерпретируемости моделей [5].

Важно отметить, что в ближайшем будущем подходы, основанные исключительно на автоматизированных системах МО, не смогут полностью заменить человеческое участие. Вместо этого, рекомендуется использование комбинированного подхода, где человек и машина работают вместе, обеспечивая более точный и оперативный анализ угроз и рисков.

Список использованной литературы:

1. Gartner. (2022). *The impact of artificial intelligence and machine learning on cybersecurity*. <https://www.gartner.com>
2. McKinsey & Company. (2021). *How artificial intelligence is changing the cybersecurity landscape*. <https://www.mckinsey.com>
3. Запечников, С. В. (2020). Модели и алгоритмы конфиденциального машинного обучения. *Безопасность информационных технологий = IT Security*, 27(1), 51. <https://doi.org/10.26583/bit.2020.1.05>

4. Liu, T., & Ju, H. (2024). *The application of machine learning in network security research. Journal of Industrial Engineering and Applied Science*, 2(1), 8. Southern United Academy of Sciences Press.
5. Тутков, Д. И., & Резниченко, С. А. (2024). *Революция в аудите информационной безопасности: искусственный интеллект. Вестник науки*, 4(73), Том 1.

ӨОЖ 004.056

Мұратхан А. Р.
(Астана, Л.Н. Гумилев атындағы ЕНУ)
Меирбек Ә. Қ.
(Астана, Л.Н. Гумилев атындағы ЕНУ)

ЖАСАНДЫ ИНТЕЛЛЕКТТІ КРИПТОГРАФИЯЛЫҚ ҚАУІПСІЗДІКТЕ ҚОЛДАНУ: ШАБУЫЛДАРДЫ АНЫҚТАУ ЖӘНЕ ШИФРЛАНҒАН ДЕРЕКТЕРДІ ҚОРҒАУ

Кіріспе.

Қазіргі цифрлық әлемде үлкен көлемдегі деректер электронды түрде беріледі және сақталады, сондықтан оларды қорғау мәселелері ерекше маңызға ие. Шифрлау технологияларының дамуы ақпаратты қорғаудың сенімді алгоритмдерін құрумен қатар, ықтимал қауіптерді анықтаудың тиімді әдістерін қажет етеді. Жасанды интеллект (ЖИ) криптографиялық қауіпсіздікті қамтамасыз етуде маңызды рөл атқарады, өйткені ол шабуылдарды анықтауға және шифрланған деректердің бұзылуына төзімділігін арттыруға мүмкіндік береді.

Кибершабуылдардың көбеюіне байланысты дәстүрлі қорғау әдістері тиімділігін төмендетіп, жаңа тәсілдерді қолдануды талап етеді. Машиналық оқыту мен нейрондық желілер технологиялары автоматтандырылған қауіптерді анықтау, аномалияларды талдау және шифрланған деректерге жасалатын шабуылдарды болжау мүмкіндіктерін ашады. Алайда, мүмкіндіктермен қатар, криптографиялық жүйелерге ЖИ-ды біріктіру жаңа сын-қатерлерді де туындатады. Олардың қатарына модельдердің сенімділігі, түсіндірмелілігі және жасанды интеллект әдістерін қолданатын шабуылдарға қарсы тұру қабілеті жатады.

Осы мақала мақсаты – жасанды интеллектті криптографиялық қауіпсіздікті қамтамасыз ету үшін қолданудың қолданыстағы әдістеріне жан-жақты талдау жасау. Біз шифрланған деректерге жасалатын шабуылдарды анықтау тәсілдерін қарастырып, олардың тиімділігі, артықшылықтары мен шектеулерін бағалаймыз. Криптографиялық жүйелерде ЖИ-ды практикалық қолдануға ерекше назар аударылып, осы саладағы зерттеулердің қазіргі жай-күйі мен болашақ даму бағыттары туралы өзекті түсінік қалыптастыруға мүмкіндік беріледі.

Зерттеудің өзектілігі тек жасанды интеллекттің криптографияда қолданылуына деген теориялық қызығушылықпен ғана емес, сонымен қатар есептеу қуатының артуы және шабуыл әдістерінің күрделенуі жағдайында ақпараттық қауіпсіздікті қамтамасыз етудің практикалық қажеттілігімен де байланысты. Қазіргі заманғы қорғаныс әдістерін терең түсіну сенімді криптографиялық қауіпсіздік жүйелерін әзірлеуге және деректердің бұзылу қаупін барынша азайтуға көмектеседі.

Кибершабуылдардың санының айтарлықтай өсуі байқалады, бұл пайдаланушылардың деректерін бұзуға бағытталған. Gen Digital компаниясының есебіне сәйкес, 2024 жылы кибершабуылдар саны алдыңғы жылмен салыстырғанда 46%-ға артты. Ай сайын киберқауіпсіздік жүйелері миллиардтан астам қауіп-қатерді бұғаттайды, ал алаяқтық пен

зиянды жарнама настольді компьютерлердегі шабуылдардың 87%-ын және мобильді құрылғылардағы шабуылдардың 93%-ын құрайды.

Теориялық шолу

Қазіргі заманғы кибершабуылдар барған сайын күрделене түсуде, ал бұзу әдістері — әбден жетілдірілген. Зиянкестер қолданатын кең таралған шабуылдарды талдау тиімді қорғаныс стратегияларын әзірлеуге мүмкіндік береді. Егер шабуыл векторлары, криптографиялық жүйелердің осал тұстары және хакерлердің әдістері туралы деректерді жүйелесек, нақты уақыт режимінде ықтимал қауіптерді анықтап, олардың алдын алатын жасанды интеллект (ЖИ) оқыту модельдерін жасауға болады.

Машиналық оқыту мен үлкен деректерді (Big Data) талдауды біріктіру арқылы ақпарат ағынындағы аномалияларды анықтауға, шабуылдарды болжауға және деректердің бұзылу ықтималдығын азайтуға болады. Мысалы, ЖИ жүйелері желілік трафикті талдап, «ортадағы адам» (MITM) шабуылдарының, жанама арналарға шабуылдардың (side-channel attacks) немесе криптографиялық кілтті таңдау (brute-force) әрекеттерінің белгілерін анықтай алады.

Шифрланған деректерді қорғау үшін ЖИ қолдану бірнеше негізгі механизмдер арқылы жүзеге асырылуы мүмкін:

- Аномалияларды анықтау – мінез-құлық деректерін талдау және қалыпты жағдайдан ауытқуларды іздеу. Мысалы, егер шифрланған деректерде әдеттен тыс белсенділік тіркелсе, жүйе автоматты түрде қорғаныс шараларын қабылдай алады.

- Жаңа қауіптерге автоматты түрде бейімделу – машиналық оқыту жүйелері шабуылдардың жаңа түрлері пайда болған сайын жаңарып, бейімделе алады.

- Төзімдірек криптографиялық кілттерді генерациялау – ЖИ кездейсоқ кілттерді жасау процесіне қатысып, оларды болжауға қиын етеді.

- Тарихи деректер негізінде шабуылдарды болжау – өткен инциденттерді талдау арқылы нейрожелі болашақтағы ықтимал қауіптерді алдын ала анықтап, оларды болдырмау бойынша шаралар қабылдай алады.

Бұл әдістер келесі кең таралған кибершабуылдарды анықтауға және оларға қарсы тұруға көмектеседі:

Арадағы	адам	шабуылы	(MITM)

Бұл шабуылда хакерлер екі тарап арасындағы деректер алмасуды жасырын түрде бақылайды және өзгерте алады. Мысалы, 2017 жылы KRACK (Key Reinstallation Attack) уязвимости WPA2 протоколында анықталған, бұл шабуыл Wi-Fi желілерін қорғауды әлсіретіп, пайдаланушылардың жеке деректеріне қол жеткізуге мүмкіндік берген. MITM-атакалар жиі қоғамдық Wi-Fi желілерінде орын алады. Оларды болдырмау үшін VPN, HTTPS және көпфакторлы аутентификацияны қолдану ұсынылады.

Қорғаныс әдісі: Аномалияларды анықтау – желілік трафиктің мінез-құлқын талдау арқылы MITM-шабуылдарын ерте кезеңде байқауға болады. Егер жүйе деректер ағынында әдеттен тыс өзгерістерді тіркесе (мысалы, күмәнді IP-мекенжайлар немесе байланыс шифрлауының өзгеруі), ол шабуылды автоматты түрде анықтап, қарсы шаралар қабылдай алады.

Дөрекі	күш	шабуылы	(Brute-force attack)

Бұл шабуыл хакерлер парольдер мен криптографиялық кілттерді барлық мүмкін комбинацияларды сынау арқылы бұзуға тырысқанда пайда болады. 2021 жылы Microsoft Exchange жүйелеріне шабуыл жасалған, онда зиянкестер шоттарға рұқсат алу үшін осал аутентификация жүйесін және парольдерді таңдау әдістерін қолданған. Қорғану үшін ұзын және күрделі парольдерді пайдалану, кіру әрекеттерін шектеу және көпфакторлы аутентификация енгізу ұсынылады.

Қорғаныс әдісі: Төзімдірек криптографиялық кілттерді генерациялау – машиналық оқыту алгоритмдері кездейсоқ және ұзақ кілттерді құруды оңтайландырып, оларды бұзу

ықтималдығын азайтады. Сонымен қатар, жүйе парольдерді пайдаланушыларға қауіпсіз етіп ұсынуы мүмкін, бұл шабуылдың сәтті болу мүмкіндігін төмендетеді.

Деректерді ауыстыру шабуылы (Data Poisoning)
Бұл шабуыл жасанды интеллект жүйелерін алдау үшін қасақана бұрмаланған деректерді енгізуді қамтиды. 2022 жылы бет тану жүйелеріне осындай шабуылдар тіркелген, онда хакерлер модельді қате тануға мәжбүрлейтін манипуляцияланған деректерді енгізген. Мұндай шабуылдардың алдын алу үшін жүйенің оқыту деректерін мұқият тексеріп, сенімді дереккөздерді пайдалану қажет.

Қорғаныс әдісі: Жаңа қауіптерге автоматты түрде бейімделу – машиналық оқыту модельдері шабуыл әдістерін үнемі талдап, жаңартылады, бұл Data Poisoning-атакасын тез анықтауға және оған бейімделуге мүмкіндік береді. Сонымен қатар, жүйе күмәнді немесе өзгертілген деректерді сүзгіден өткізіп, оларды оқыту процесінен шығарып тастай алады.

2019 жылы Google кванттық үстемдікке қол жеткізгенін хабарлады, бұл болашақта кванттық шабуылдар қаупін күшейтеді. Мұндай шабуылдар дәстүрлі шифрлеу әдістерін әлсіретуі мүмкін.

Қорғаныс әдісі: Тарихи деректер негізінде шабуылдарды болжау – машиналық оқыту жүйелері кванттық шабуылдар мен криптографиялық бұзушылықтардың тарихи деректерін талдап, жаңа қауіптердің пайда болуын алдын ала болжай алады. Сонымен қатар, пост-кванттық криптография бағытында зерттеулер жүргізу қажет.

Тиімділік және шектеулер
Анализ әдістерінің тиімділігін бағалау үшін оларды әртүрлі сценарийлерде сынау маңызды. Бұл тәсілдер әртүрлі форматтағы және типтегі мультимедиялық файлдармен жұмыс істеу қабілетін бағалауға мүмкіндік береді. Сонымен қатар, әр әдістің шектеулерін ескеру қажет: жалған оң нәтиже – кейбір әдістер қате позитивтер тудыруы мүмкін, бұл пайдаланушыларға ыңғайсыздық туғызады.

Медиафайлдарға сезімталдық – кейбір қорғаныс әдістері белгілі бір форматтарда тиімді, бірақ басқаларында әлсіз болуы мүмкін.

Есептеу ресурстарына талаптар – машиналық оқыту мен үлкен деректерді талдау үлкен есептеу қуатын қажет етуі мүмкін, бұл жүйені ауқымды қолдануда қиындықтар туғызады.

Болашақ бағыттар

Киберқауіпсіздік пен криптографиялық жүйелерді қорғаудың болашағы жаңа технологиялардың дамуына тікелей байланысты. Терең оқыту (Deep Learning) және кванттық есептеулер жаңа шабуылдарды анықтау мен алдын алу әдістерін жетілдіруге мүмкіндік береді. Сонымен қатар, пост-кванттық криптография, блокчейн негізіндегі шифрлеу және автоматтандырылған қорғаныс жүйелері болашақта кеңінен қолданылуы мүмкін. Зерттеулердің негізгі бағыттары – кванттық компьютерлерге төзімді алгоритмдер әзірлеу, жасанды интеллект көмегімен кибершабуылдарды болжау және шифрлеу механизмдерін одан әрі күшейту.

Қорытынды. Жасанды интеллекттің криптографиялық қауіпсіздікті қамтамасыз етудегі рөлі артып келеді. ЖИ негізінде аномалияларды анықтау, жаңа қауіптерге бейімделу және төзімді криптографиялық алгоритмдерді әзірлеу киберқауіптерге қарсы тұрудың маңызды құралдарына айналды. Дегенмен, ЖИ-дың өзі де осалдықтарға ие, сондықтан оны қауіпсіз қолдану үшін сенімді модельдер әзірлеу қажет.

Болашақта кванттық есептеулер мен пост-кванттық криптография саласындағы зерттеулер киберқауіпсіздікті жаңа деңгейге көтереді. Ақпараттық қауіпсіздік саласында жасанды интеллектті одан әрі дамыту шабуылдарға төзімді жүйелерді құруға және шифрланған деректердің қорғанысын нығайтуға мүмкіндік береді.

Пайдаланылған әдебиеттер:

[1] *Компаниец М. Р. Жасанды интеллект технологияларының криптографияны дамытудағы рөлі*(2024) (Роль технологий искусственного интеллекта в развитии криптографии). Молодой ученый, КиберЛенинка.

[2] *Арутюнов В. В. Ақпараттық қауіпсіздікті қамтамасыз ету үшін жасанды интеллект әдістерін қолдану*(2020) (Применение методов искусственного интеллекта для обеспечения информационной безопасности). ntb.gpntb.ru.

[3] *Нейрокриптография* (Нейрокриптография). Kaspersky Lab. (2023).

[4] Kaspersky Lab. (2023). *Киберқауіпсіздіктегі жасанды интеллект* (Artificial Intelligence in Cybersecurity).

Оразбаев Дәулет, Токсеит Динара
(Л.Н.Гумилев атындағы
Еуразия ұлттық университеті)

IBM QRADAR SIEM ЖҮЙЕСІНІҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЛАСЫНДАҒЫ МҮМКІНДІКТЕРІН ШОЛУ ЖӘНЕ БАҒАЛАУ

Аннотация: Бұл мақалада IBM QRadar ақпараттық қауіпсіздік оқиғаларын мониторингтеу және талдау жүйесі қарастырылады. Жүйенің негізгі функциялары мен мүмкіндіктері, оның ішінде оқиғаларды жинау және нормализациялау, пайдаланушылардың мінез-құлқын талдау және машиналық оқытуды қолдану бағаланды. Сонымен қатар, IBM QRadar-ды Splunk, MaxPatrol SIEM және Elastic Security сияқты аналогты SIEM жүйелерімен салыстырмалы түрде талдау жүргізілді. IBM QRadar-дың әртүрлі ұйымдарда қолданылуы және оны енгізу ерекшеліктері туралы ұсыныстар жасалды.

Кілт сөздер: IBM QRadar, SIEM жүйесі, қауіпсіздік, машиналық оқыту, оқиғаларды мониторингтеу, ақпараттық қауіпсіздік, аналитика.

Кіріспе. Қазақстанда ақпараттық қауіпсіздік процестерін автоматтандыру маңызды мәселеге айнауда. Күн сайын жаңа қауіпсіздік жүйелері енгізіліп, ұйымдар түрлі инциденттерді талдауға мәжбүр. Ақпараттық қауіпсіздік оқиғаларын тиімді басқару үшін орталықтандырылған жүйелер қажет. Бұл жұмыста QRadar жүйесінің мүмкіндіктері қарастырылып, оның архитектурасы, негізгі компоненттері және басқа SIEM жүйелерімен салыстырмалы талдауы жүргізіледі. Бұл зерттеудің мақсаты – QRadar ақпараттық қауіпсіздік оқиғаларын мониторингтеу және талдау жүйесін кәсіпорынға енгізу және оның тиімділігін бағалау. Сонымен қатар, QRadar жүйесінің архитектурасы мен негізгі компоненттерін зерттей отырып, оны басқа SIEM жүйелерімен салыстыру арқылы ұйымның ақпараттық қауіпсіздігін күшейтудің оңтайлы жолдарын анықтау. Мақсатқа жету үшін ақпараттық қауіпсіздік оқиғаларын басқарудың маңыздылығын қарастыру, QRadar жүйесінің архитектурасы мен негізгі компоненттерін талдау, оны басқа SIEM жүйелерімен салыстырып, артықшылықтары мен кемшіліктерін анықтау, кәсіпорында QRadar жүйесін енгізу мүмкіндіктерін зерттеу және ұсыныстар әзірлеу қажет.

IBM QRadar SIEM компания желісіндегі мыңдаған құрылғыдан оқиғаларды жинақтап, оларды өңдеп, талдайды, қалыпқа келтіреді және ықтимал қауіптерді жалған ескертулерден ажыратады. Жүйе IBM Security X-Force Threat Intelligence қызметімен интеграцияланған, ол

қауіпті IP-мекенжайлардың дерекқорын, белгілі қауіптерді, спам көздерін және басқа да ықтимал шабуылдарды қамтиды. QRadar SIEM қауіптерді анықтау және негізгі міндеттерді белгілеу мақсатында оқиғаларды нақты уақыт режимінде көрсетіп, маңызы төмен немесе жалған қауіптерді сүзгіден өткізу қабілетіне ие. Бағдарлама операциялық жүйелерден, қолданбалардан, дерекқорлардан және киберқауіпсіздік жүйелерінен оқиғаларды жинап, желілік құрылғылардан трафик туралы мәліметтерді қабылдайды. Сондай-ақ, басқару жүйелерінен, DHCP серверлерінен және осалдықтарды талдайтын сканерлерден алынған ақпаратты өңдеп, басымдықтарды анықтап, ескертулер санын азайтады. Жүйе деректерді жедел қалыпқа келтіріп, басқа ақпарат көздерімен өзара әрекеттесуді оңтайландырады, деректер ағынын тиімді басқарып, нақты қауіптерді анықтайды. QRadar SIEM киберқауіптерді тиімді басқаруды қамтамасыз етіп, егжей-тегжейлі есептерді баптауға және деректерді нақты уақыт режимінде іздеуге мүмкіндік береді.

IBM QRadar жүйесін Қазақстанда қолданылатын аналогтарымен салыстыру

Қазақстанда ақпараттық қауіпсіздік саласында SIEM жүйелерінің бірнеше түрлері кеңінен қолданылады. Олардың ішінде IBM QRadar, Splunk, MaxPatrol SIEM және Elastic Security жүйелерін ерекше атап өтуге болады. 3-кестеде олардың артықшылықтары, кемшіліктері және функционалдық ерекшеліктері салыстырмалы түрде қарастырылған.

3- Кесте – SIEM жүйелерінің салыстырмалы талдауы

Көрсеткіштер	IBM QRadar	Splunk	MaxPatrol SIEM	Elastic Security
Орнату және баптау	Орташа қиындықтағы орнату, модульдік архитектура.	Жеңіл орнату, бірақ күрделі баптаулар қажет.	Орнату күрделілігі жоғары.	Орнату жеңіл, ашық бастапқы код (opensource).
Өнімділік	Жоғары өнімділік, 200,000 оқиға/мин.	Жоғары өнімділік, бірақ үлкен ресурстар қажет.	Орташа өнімділік.	Жақсы өнімділік, үлкен деректермен жұмыс істейді.
Масштабталуы	Жеңіл масштабталады, үлкен кәсіпорындар үшін қолайлы.	Икемді масштабтау мүмкіндігі.	Масштабтау қиындау, кіші және орта бизнеске бағытталған.	Жеңіл масштабтау, бұлтты шешімдермен қолдау.
Функционалдық	Машиналық оқыту, Threat Intelligence қолдауы.	Кеңейтілген деректерді визуализациялау.	Отандық өнім, осалдықтарды басқаруға басымдық береді.	Аномалияларды талдау, логтарды жинау және іздеу.
Баға	Жоғары. Ірі ұйымдарға тиімді.	Құны жоғары, деректер көлеміне байланысты өзгереді.	Орташа баға.	Тегін нұсқасы бар, ақылы кеңейтулер бар.

Көрсеткіштер	IBM QRadar	Splunk	MaxPatrol SIEM	Elastic Security
Қолдану саласы	Ірі және орта кәсіпорындар.	Кез-келген көлемдегі компаниялар.	Мемлекеттік ұйымдар мен қаржы секторына бағытталған.	Шағын және орта компаниялар, стартаптар.

IBM QRadar – Қазақстанның ірі кәсіпорындары мен мемлекеттік мекемелерінде кеңінен қолданылатын SIEM жүйелерінің бірі. Оның басты артықшылықтары – жоғары өнімділік, дамыған Threat Intelligence мүмкіндіктері және кең функционал. Мемлекеттік сектор үшін бұл шешім әсіресе маңызды, себебі ол күрделі шабуылдарды анықтауға және оқиғаларды жылдам талдауға мүмкіндік береді. Қазақстандық нарықта MaxPatrol SIEM секілді отандық өнімдер мемлекеттік мекемелер арасында танымал, себебі олар ұлттық қауіпсіздік талаптарына сәйкес келеді және жергілікті реттеуші органдардың стандарттарына бейімделген. Ал Elastic Security көбіне шағын және орта бизнес үшін қолжетімді балама ретінде қарастырылады, өйткені оның икемділігі мен салыстырмалы түрде төмен құны шағын ұйымдардың қажеттіліктеріне сай келеді.

IBM QRadar қазіргі таңда ақпараттық қауіпсіздік жүйелерін мониторингтеу және басқару үшін ең үздік шешімдердің бірі болып табылады. IBM QRadar жүйесін енгізу ұйымдардың ақпараттық қауіпсіздік деңгейін арттыруға және қауіптерді дер кезінде анықтауға мүмкіндік береді.

Пайдаланылған әдебиеттер:

1. Мұратов, Е.С. *Киберқауіпсіздік негіздері және SIEM жүйелерін қолдану тәжірибесі*. Алматы: Әл-Фараби атындағы ҚазҰУ баспасы, 2020.
2. Қасымов, Т.Ж., Омарова, А.Т. *Ақпараттық қауіпсіздік және оның ұлттық қауіпсіздік жүйесіндегі орны*. Нұр-Сұлтан: Экономика институты, 2019.
3. Бекенов, Р.Қ., Сағындықова, Л.М. *Цифрлық қауіпсіздік: теория және тәжірибе*. Астана: Назарбаев Университеті баспасы, 2021.
4. Қуанышев, М.Т. *Қазақстандағы ақпараттық қауіпсіздікті қамтамасыз етудің заманауи әдістері*. Алматы: Қазақ университеті, 2018.
Қазақтелеком АҚ. *Қазақстандағы SIEM жүйелерін енгізу тәжірибесі: IBM QRadar, MaxPatrol SIEM және Elastic Security салыстырмалы талдауы*. Сараптамалық есеп, 2022.

УДК 004.72.

Оралбеков Е.А. Онгарбаева А.И.,
(Л. Н. Гумилев атындағы Еуразия
ұлттық университеті, Астана)

ЖЕЛІЛІК СТЕГАНОГРАФИЯ

Желілік трафиктегі стеганография – бұл желілік деректер ішінде ақпаратты жасыру әдісі, ол үшінші тараптың бақылауынан тыс қалады. Бұл техника құпия деректерді қорғау

үшін, анықтау жүйелерінен жасырыну үшін қолданылады. Қазіргі кезде деректерді беру хаттамаларының ерекшеліктерін қолдана отырып, компьютерлік желілер арқылы жасырын ақпараттарды беру әдістері танымал болды. Мұндай әдістер "желілік стеганография" деп аталды. Бұл терминді алғаш рет 2003 жылы Кшиштоф Шиперский (Krzysztof Szczypiorski) енгізген.[4]

Желілік стеганографияның типтік әдістеріне желілік хаттамалардың біреуінің қасиеттерін өзгерту жатады. Мысалы, IP пакеттерінің тақырыптарындағы пайдаланылмаған өрістерді немесе TCP/UDP бағандарындағы резервтелген биттерді пайдалануға болады. Сонымен қатар, құпия хабарламаның берілуін неғұрлым сенімді түрде жасыру мақсатында екі немесе одан да көп әртүрлі хаттамалар арасындағы байланысты қолдануға болады. Мысалы, HTTP және DNS хаттамаларының тізбегі арқылы ақпаратты жасыруға болады.[1]

Дегенмен, желілік стеганография тек пайдалы мақсаттарда қолданылмайды. Киберқылмыскерлер оны зиянды бағдарламалық жасақтамаларды тарату, деректерді ұрлау және басқа да заңсыз әрекеттерді жасыру үшін пайдалануы мүмкін. Сондықтан, ақпараттық қауіпсіздік мамандары үшін желілік стеганография әдістерін терең түсіну және оларға қарсы тұру тәсілдерін әзірлеу өте маңызды. Мақалада желілік стеганографияның теориялық негіздері, сондай-ақ жасырын деректерді талдау және анықтау құралдары қарастырылады.

Желілік трафиктің түрлі протоколдарындағы стеганографиялық әдістердің тиімділігі көрсетілген. (1-кесте) [2][3]

1-кесте. Желілік трафиктің түрлі протоколдарындағы стеганографиялық әдістердің тиімділігі

Әдіс	Тиімділігі	Кемшіліктері
TCP Sequence Number стеганографиясы	Сенімдірек әдіс. Желілік қосылымның тұрақтылығын сақтау мүмкіндігі жоғары.	Желілік қосылымның тұрақтылығына байланысты қиындықтар болуы мүмкін. Ақпаратты дұрыс жеткізу мәселесі туындайды.
DNS стеганографиясы	Жасырын ақпаратты тиімді тасымалдау. DNS сұраныстарын қолдану қарапайым.	DNS трафигінің көлемін ұлғайтады. Аномалияларды анықтау жеңілдетіледі.
HTTP тақырыптары стеганографиясы	HTTP тақырыптары кеңінен қолданылады, бұл трафиктің заңдылығын бұзбайды. Ақпаратты тиімді тасымалдауға мүмкіндік береді.	DPI жүйелері арқылы күдікті өзгерістер анықталуы мүмкін.

Бұл кесте желілік трафиктегі стеганографияны анықтауға арналған құралдардың тиімділігі мен кемшіліктерін салыстырады. Мұнда үш құрал қарастырылған: Wireshark, Snort/Suricata және tcpdump. Тиімді анықтау жүйесін құру үшін бұл құралдарды бірге қолдануға болады.

2-кесте. Анықтау құралдарының тиімділігі

Құрал	Тиімділігі	Кемшіліктері
Wireshark	Пакеттердің тақырыптары мен мазмұнын талдау үшін тиімді. Қарапайым құрал.	Трафик көлемі үлкен болса, күрделі стеганографиялық әдістерді анықтау қиын.
Snort/Suricata	Күдікті желілік үлгілерді анықтау үшін тиімді. Желілік аномалияларды тез табуға көмектеседі.	Жаңартылған ережелер мен конфигурацияларға тәуелді.
tcpdump	Желі трафигін тіркеу және анализдеу үшін тиімді. Командалық жол арқылы жұмыс істей алады, қарапайым пайдалану интерфейсі бар. Жүйе ресурстарына жеңіл жүктеме.	Трафикті визуализациялау мүмкіндігі жоқ. Пакеттерді талдаудың терең деңгейін талап етеді, жаңадан бастаушылар үшін қиын болуы мүмкін.

3-кесте желілік стеганографияның тиімділігіне әсер ететін факторларды көрсетеді. Стеганографиялық жүйелерді құру және талдау кезінде бұл факторларды ескеру маңызды.

3-кесте. Желілік стеганографияның тиімділігіне әсер ететін факторлар

Фактор	Әсері
Жасырын ақпараттың көлемі	Көлем артқан сайын, оны анықтау мүмкіндігі артады. Үлкен деректер аномалияларды анықтауды жеңілдетеді.
Қолданылатын хаттамалар	Хаттамалардың қауіпсіздік деңгейі әртүрлі. Кейбір хаттамалар стеганография әдістеріне осал болуы мүмкін.
Анықтау әдістерінің күрделілігі	Күрделі анықтау әдістері жасырын ақпаратты табуға көмектеседі. Қарапайым әдістер қарапайым стеганографиялық әдістерді анықтай алмайды.

Мақалада желілік трафикте ақпаратты жасырудың теориялық негіздері және оны анықтау құралдары қарастырылды. Зерттеу нәтижесінде желілік стеганографияның көптеген артықшылықтарымен қатар кемшіліктері де бар екені көрсетілді. Әдістердің тиімділігі трафиктің түріне, қолданылатын хаттамаларға және қауіпсіздік құралдарының мүмкіндіктеріне байланысты өзгереді. Желілік стеганографияны терең түсіну ақпараттық қауіпсіздікті қамтамасыз ету үшін маңызды.

Болашақта жасанды интеллект және машиналық оқыту технологияларын қолдану арқылы желілік стеганографиялық әдістерді анықтау және болдырмау әдістерінің тиімділігін арттыруға бағытталған зерттеулер жүргізу қажет. Стеганографияға қарсы тұрудың жаңа тәсілдерін әзірлеу және қолданыстағы әдістерді жетілдіру маңызды. Бұл бағытта зерттеулерді бұғаттау, трафикті талдау және қалыпқа келтірудің жаңа әдістерін құруға бағыттау керек.

Желілік стеганография құпия ақпаратты қорғау құралы ретінде маңызды рөл атқарады. Ол ақпаратты жасырын жеткізуді қамтамасыз етеді, бұл әсіресе цензура немесе бақылау қаупі бар жағдайларда маңызды. Стеганографияны пайдаланудың этикалық аспектілерін ескеру қажет. Шешімдер құпиялылық пен қауіпсіздікті қамтамасыз ету үшін қабылданған шаралардың арасындағы тепе-теңдікті табуы тиіс. Желілік стеганографияға байланысты жаңа технологиялар мен қауіптердің пайда болуына дайын болу және қорғау стратегияларын үнемі жетілдіріп отыру қажет.

Пайдаланылған әдебиеттер тізімі

1. Network Steganography in the DNS Protocol / Michał Drzymala, Krzysztof Szczypiorski, Marek Łukasz Urbański // International Journal of Electronics and Telecommunications. – Қараша 2016. – 62(4).
2. Steganography Using TCP / IP's Sequence Number / Jamal Mohammed Kadhim, Abeer E. Abed // Nahrain University, University of Baghdad. – Желтоқсан 2017.
3. Стеганография на базе стека протоколов TCP/IP / John Torakis. 18 апреля, 2017
4. О сетевой стеганографии. Реализация алгоритма RSTEG / Павлин Д.В., Макосий А.И., Жданов О.Н.

УДК 004.056

Сатыбалдина Д.Ж., Тлеубердин С.Т.

(Астана, ЕНУ им. Л.Н. Гумилева)

ПРИМЕНЕНИЕ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ АНАЛИЗА УЯЗВИМОСТЕЙ СЕТЕЙ И ОБНАРУЖЕНИЯ АТАК

В условиях экспоненциального роста интеграции информационных технологий в городскую инфраструктуру концепция "умного города" (Smart City) становится все более распространенной. Однако, несмотря на преимущества цифровизации, проблемы кибербезопасности остаются критическими. Расширение цифровой инфраструктуры и повсеместное внедрение устройств Интернета вещей (IoT) создают потенциальные векторы атак, включая перехват данных, атаки типа «отказ в обслуживании» (DoS) и фальсификацию данных [1]. Несмотря на активное развитие решений в области кибербезопасности, масштабирование и усложнение архитектуры "умных городов" порождает новые вызовы. Для эффективного устранения уязвимостей необходима систематическая актуализация протоколов безопасности, включающая криптографическую защиту данных, строгую аутентификацию, мониторинг сетевого трафика и регулярный аудит безопасности.

Технологии этичного хакинга и тестирования на проникновение (пентестинг) представляют собой перспективные методологии для повышения уровня защищенности

цифровых сетей и систем, особенно в тех случаях, когда традиционные меры безопасности оказываются недостаточными для обнаружения новых векторов атак. Пентестинг, проводимый квалифицированными специалистами, позволяет имитировать реальные кибератаки, что способствует проактивному выявлению и устранению потенциальных уязвимостей [2]. Для повышения эффективности и автоматизации пентестинга предлагается применение методов машинного обучения, в частности, обучения с подкреплением [3].

В связи с этим, целью настоящего исследования является разработка методологии и инструментария для тестирования безопасности беспроводных локальных сетей (WiFi) с применением алгоритмов машинного обучения для моделирования практических атак на протоколы WPA2 и WPA3.

Методология исследования

Предлагается новая оригинальная методика адаптивного тестирования на проникновение беспроводных сетей в реальном времени и соответствующий программный инструментарий с использованием алгоритма с подкреплением Q-learning (reinforcement learning, RL) и эпсилон-жадной стратегией исследования среды (epsilon greedy exploration) [3]. Разработанное программное средство представляет собой комплексную утилиту для аудита безопасности Wi-Fi сетей, которая выполняет обнаружение и анализ беспроводных точек доступа (сканирование, сбор данных, их предобработку и анализ), а также осуществляет различные виды атак (Deauth, Auth DOS, Beacon flood, EAPOLStart Flood, RTS/CTS Flood, WIDS Confusion) с возможностью формирования автоматизированных отчетов об уязвимостях [4]. Язык реализации Python 3.x.

Для оценки эффективности адаптивной методики и инструмента тестирования проведены практических экспериментов в сетях, поддерживающих протоколы WPA2 и WPA3. Перечень устройств и их роль в практических экспериментах представлен в таблице 1.

Таблица 1 – Состав экспериментального стенда

Устройство	Модель/ Процессор	Роль / Действие	Поддержка протокола WPA2/WPA3
Ноутбук 1	Huawei MateBook X Pro Premium Edition / Intel Ultra 7 155H	Атакует TP-Link Archer C64 AC1200 WiFi роутер	WPA3
WiFi роутер	TP-Link Archer C64 AC1200	Принимает атаку; подключены MacBook M3 Pro и Samsung S24+	WPA3
Ноутбук 2	MacBook M3 Pro	Подключен к TP-Link Archer C64 AC1200	WPA3
Смартфон	Samsung S24+ / Exynos	Подключен к TP-Link Archer C64 AC1200	WPA3
Смарт устройство умного дома, увлажнитель	Mijia Smart Evaporative Humidifier 2 Lite	Обеспечивает увлажнение воздуха в помещении. Имеет микроконтроллер с Wi-Fi модулем (2.4 ГГц, на базе ESP8266)	WPA2

Описание процесса адаптивного тестирования уязвимостей беспроводной сети

В начале каждого эксперимента модель Q-Learning (с использованием ϵ -greedy стратегии) выбирает комбинацию из нескольких атак из заданного множества Action Space (например, DeauthFlood, AuthDOS, BeaconFlood и др.). Программа параллельно запускает выбранные атаки с заданными параметрами. После краткого интервала атаки процессы останавливаются, производится захват трафика (pcap) и сбор CSV-логов. Из полученных данных извлекается значение station_count с фильтрацией по базовому набору MAC-адресов, а также активным способом измеряется текущая производительность цели через установление TCP-соединений. Параметр

«Выигрыш» (Reward) алгоритма с подкреплением рассчитывается как разница между базовым и текущим уровнем производительности, с дополнительным бонусом за снижение соединения effective_count до нуля. При последовательном сохранении effective_count=0 на протяжении нескольких шагов модель начинает отдавать предпочтение комбинациям атак, приводящим к значительному снижению производительности атаки. В результате, если при использовании оптимальных комбинаций атак Reward значительно возрастает, это подтверждает их успешность. По итогам серии эпизодов рассчитываются метрики Accuracy, Precision, Recall и F1-score, позволяющие объективно оценить успешность атак с точки зрения модели машинного обучения.

Результаты и обсуждение.

Анализ журналов регистрации событий (лог-файлов) показал, что комбинированное применение атак DeauthFlood (реализованных с использованием утилиты aireplay-ng) и AuthDOS (утилита mdk4) с высокой интенсивностью (два параллельных потока, 50 пакетов в секунду (pps) и параметр -s 1000 для BeaconFlood) приводит к значительному эффекту отказа в обслуживании (DoS). Наблюдалась продолжительная потеря соединения клиентскими устройствами и невозможность его восстановления в течение всего периода тестирования.

Изолированное применение атак RTSCTSFlood и BeaconFlood не демонстрирует значительного эффекта. Однако, при их комбинации с атакой AuthDOS, а в некоторых случаях – с DeauthFlood или EAPOLStartFlood, наблюдается существенное усиление DoS-атаки. В тестах, проведенных для протокола WPA3, оптимальной комбинацией оказалась AuthDOS + RTSCTSFlood. Данная комбинация приводила к устойчивому снижению метрики effective station_count до нуля и увеличению параметра reward до положительных значений, что подтверждает длительные периоды недоступности сети и наличие уязвимостей в исследуемой конфигурации.

Заключение. На основе методики адаптивного пентестинга с использованием RL-модели реализовано программное средство, которое реализует активные атаки на сеть, собирает информацию о ходе атак (время выполнения, ответ сети, число клиентов, степень их повторного подключения и т.д.). На основе анализа собранных данных автоматически определяется наиболее эффективная стратегия тестирования, когда интенсивность определенных атак следует снизить или повысить, а какие атаки стоит комбинировать. Система «учится» на каждом шаге, динамически перераспределяя ресурсы и меняя комбинацию атак.

Данное исследование финансируется Комитетом науки Министерства науки и высшего образования Республики Казахстан (BR24992852).

Список использованных источников:

- 1 Vitunskaitė M., He Y., Brandstetter T., Janicke H. Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership //Computers & Security. – 2019. – V. 83. – Pp. 313-331.

2 Yaacoub J.P.A., Noura H.N., Salman O., Chehab A. *Ethical hacking for IoT: Security issues, challenges, solutions and recommendations //Internet of Things and Cyber-Physical Systems.* – 2023. – V. 3. – Pp. 280-308.

3 Adawadkar A. M. K., Kulkarni N. *Cyber-security and reinforcement learning – a brief survey //Engineering Applications of Artificial Intelligence.* – 2022. – V. 114. – P. 105116.

4 Тлеубердин С., Малахов К., Айдынов Т., Исайнова А., Сатыбалдина Д., Боранбай Ж., Алтайбек М. Программное обеспечение для аудита безопасности беспроводной WI-FI сети с применением машинного обучения // Свидетельство о внесении сведений в государственный реестр прав, охраняемые авторским правом № 55078 от «24» февраля 2025 года.

УДК 004.056

Токсеит Д. Қ

(Астана, ЕНУ имени Л.Н. Гумилева)

Бустекбаев Т.С.

(Астана, ЕНУ имени Л.Н. Гумилева)

Тәжмұханов А.Б.

(Астана, ЕНУ имени Л.Н. Гумилева)

АВТОМАТИЧЕСКОЕ ОБНАРУЖЕНИЕ УГРОЗ: МОЖЕТ ЛИ ИИ ЗАМЕНИТЬ ЧЕЛОВЕКА?

Аннотация:

В современном мире киберугроз, где атаки становятся всё более сложными и изощренными, автоматизация процессов обнаружения и реагирования приобретает особую значимость. Искусственный интеллект (ИИ) активно внедряется в системы информационной безопасности, предлагая быстрый анализ данных, выявление аномалий и предотвращение атак. Однако остаётся открытым вопрос: может ли ИИ полностью заменить человека в обеспечении кибербезопасности?

Цель данной статьи — рассмотреть возможности, преимущества и ограничения ИИ в автоматическом обнаружении угроз, а также проанализировать, способен ли он заменить эксперта-человека. В статье будут рассмотрены современные алгоритмы ИИ, их эффективность в обнаружении угроз, а также роль человека в интерпретации данных и принятии решений.

Ключевые слова: кибербезопасность, искусственный интеллект, машинное обучение, нейросети, обнаружение угроз, аномалия, автоматизация, глубокое обучение, поведенческий анализ, кибератаки, информационная безопасность, защита данных, алгоритмы, самообучение, анализ сетевого трафика, мониторинг, реагирование на инциденты, этика ИИ, эксперт-человек.

Введение:

Современные киберугрозы становятся всё сложнее, а их количество продолжает расти. В таких условиях автоматизированные системы, основанные на алгоритмах машинного обучения и нейросетях, активно используются для анализа сетевого трафика, поиска вредоносных программ и предотвращения атак. Однако остаётся вопрос, насколько эффективны эти системы и могут ли они полностью заменить человека.

Методы автоматического обнаружения угроз

Машинное обучение и нейросети

Автоматическое обнаружение угроз стало одним из наиболее важных направлений в кибербезопасности благодаря активному использованию таких технологий, как машинное обучение, нейросети, системы на основе правил и гибридные подходы. Эти методы предоставляют новые возможности для анализа киберугроз, что позволяет значительно повысить точность и скорость обнаружения атак, а также предотвратить потенциальные инциденты. Рассмотрим подробнее методы, связанные с машинным обучением и нейросетями.

Машинное обучение и нейросети

Использование алгоритмов машинного обучения для классификации угроз

Машинное обучение (ML) играет ключевую роль в классификации угроз, анализируя большие объемы данных для выявления аномалий и угроз. Алгоритмы машинного обучения обучаются на исторических данных о кибератаках, что позволяет им обнаруживать как известные, так и неизвестные угрозы. Основное преимущество этих алгоритмов заключается в их способности анализировать огромные объемы информации с высокой скоростью и точностью, выявляя угрозы, которые могли бы быть пропущены при традиционных методах анализа. Например, системы на базе ML могут автоматически классифицировать типы атак, что позволяет быстрее реагировать на инциденты.

Обнаружение аномалий в поведении пользователей и сетевого трафика

Обнаружение аномалий в поведении пользователей и сетевом трафике — это один из важнейших аспектов кибербезопасности, который также активно использует машинное обучение. Алгоритмы могут анализировать повседневное поведение пользователей, а также структуру сетевого трафика, и при выявлении подозрительных действий сигнализировать о возможной атаке. Это помогает идентифицировать инциденты на ранней стадии и предотвратить их развитие. Например, резкое изменение привычек пользователя, такие как внезапные скачки объема загружаемых данных или необычные временные промежутки активности, могут свидетельствовать о компрометации учетной записи или сетевой инфраструктуры.

Глубокие нейросети и их применение в анализе кибератак

Глубокие нейросети (Deep Learning, DL) являются более продвинутой версией алгоритмов машинного обучения, которые позволяют анализировать данные на более глубоком уровне. Нейросети могут распознавать сложные паттерны, которые трудно выявить традиционными методами. Например, глубокие нейросети способны анализировать огромные объемы данных, такие как сетевые логи, электронные письма, данные вредоносного ПО, и выявлять корреляции, которые могут указывать на сложные и многоэтапные атаки.

Применение глубоких нейросетей особенно полезно при анализе угроз с множеством переменных, таких как поведенческий анализ злоумышленников или выявление целенаправленных атак. Они могут использоваться для распознавания образцов вредоносного кода, предсказания действий атакующих и даже моделирования сценариев кибератак, что позволяет улучшить стратегии защиты.

Преимущества машинного обучения и нейросетей в кибербезопасности

Адаптивность и самообучение: Алгоритмы машинного обучения могут учиться на новых данных, адаптируясь к постоянно меняющейся среде угроз.

•
Высокая точность: Благодаря способности выявлять сложные аномалии и паттерны, системы на основе ML и DL предлагают более высокую точность по сравнению с традиционными методами.

Масштабируемость: Машинное обучение и нейросети могут эффективно работать с большими объемами данных, что особенно важно для крупных компаний с обширной сетевой инфраструктурой.

Закключение

В современном мире киберугрозы становятся все более сложными и разнообразными, требуя от специалистов по безопасности использования новейших технологий для эффективной защиты данных и систем. Искусственный интеллект в этой области представляет собой мощный инструмент, который обладает уникальными возможностями для автоматического обнаружения угроз, анализа больших объемов данных и быстрого реагирования на инциденты. Его способность работать в режиме реального времени, выявлять паттерны и аномалии, а также адаптироваться к новым типам атак открывает новые горизонты в киберзащите.

Тем не менее, несмотря на значительные достижения, ИИ не лишен ограничений. Хотя он может обрабатывать огромные объемы информации быстрее и эффективнее, чем человек, ему не хватает способности интерпретировать данные в контексте, учитывать этические аспекты и принимать нестандартные решения. Человеческий фактор по-прежнему играет ключевую роль в управлении системами безопасности, особенно в ситуациях, когда требуется глубокий анализ, интуиция и творческий подход. Человек также выполняет важные функции по контролю и настройке ИИ-систем, предотвращая ложные срабатывания и минимизируя риски от их неправильной работы.

Таким образом, ИИ и человек должны дополнять друг друга, создавая мощную симбиоз, который обеспечит наилучшую защиту от киберугроз. Только сочетание технологических возможностей ИИ и человеческой интуиции, опыта и ответственности сможет обеспечить высокоэффективную и надежную систему кибербезопасности в быстро развивающемся цифровом мире.

Список использованной литературы

1. <https://astanahub.com/ru/blog/mozhet-li-ii-zamenit-cheloveka>
2. <https://www.bbc.com/russian/features-38931070>
3. <https://swimlane-com.translate.goog/blog/will-ai-take-over-cybersecurity-jobs/? x tr sl=en& x tr tl=kk& x tr hl=kk& x tr pto=sc& x tr hist=true>
4. https://medium.com/@danieloh_27325/the-future-of-threat-detection-how-ai-and-machine-learning-are-changing-security-c0a0ad922862
5. <https://habr.com/ru/companies/cdnnow/articles/816185/>

Төребеков Б.Б (Астана, Л.Н. Гумилев
атындағы Еуразия ұлттық университеті)

"CAPTURE THE FLAG" (CTF) ОЙЫНЫН КИБЕРШАБУЫЛДАРҒА ҚАРСЫ ТҰРУ ДАҒДЫЛАРЫН ДАМУЫ ӨДІСІ РЕТІНДЕ ПАЙДАЛАНУ.

Аңдатпа

Технологияның қарқынды дамуы және кибершабуылдар санының артуы жағдайында киберқауіпсіздік деңгейін арттыру маңызды міндетке айналады. Кәсіби программисттер мен ақпараттық қауіпсіздік мамандарын оқытудың тиімді әдістерінің бірі - "Capture The Flag" (CTF) ойынын пайдалану. Бұл әдіс - осалдықтарды анықтау және жою дағдыларын дамытуға ғана емес, сонымен қатар Киберқауіпсіздіктің әртүрлі аспектілерін практикалық дамытуға ықпал етеді. Бұл мақалада білім беру бағдарламаларында CTF қолдану ерекшеліктері, сондай-ақ киберқауіпсіздікті оқытуда осы тәсілдің тиімділігін көрсететін нақты жағдайлар(кейстер) қарастырылады.

Кілттік сөздер.

Capture The Flag (CTF), киберқауіпсіздік, кибершабуылдар, ақпараттық қауіпсіздік, программисттер, оқыту, осалдықтар, деректерді қорғау, ойын тәсілдері, практика арқылы оқыту.

Кіріспе

Киберқауіптер қазіргі цифрлық ортаның ажырамас бөлігіне айналды және көптеген ұйымдар өздерінің ақпараттық жүйелерін қорғаудың маңыздылығын түсінеді. Кәсіби бағдарламашылар мен киберқауіпсіздік мамандары теориялық білімге ие болып қана қоймай, әртүрлі қауіп-қатерлерге жедел жауап бере білуі керек. Осы саладағы біліктілікті арттырудың ең тиімді әдістерінің бірі - Capture The Flag (CTF) сияқты ойын форматтарын пайдалану. CTF ойыны - бұл қатысушылар бағдарламалық жасақтамадағы осалдықтарды табуға, қателерді пайдалануға және деректерді қорғауға қатысты мәселелерді шешетін жарыс. Тапсырмалар әртүрлі күрделілікте болуы мүмкін және криптография, желілік трафикті талдау, кері инженерия және ақпараттық қауіпсіздіктің басқа салалары сияқты аспектілерді қамтуы мүмкін.

CTF ойынының негізгі принциптері

CTF ойыны - бұл бәсекелестер, көбінесе командаларда, әр түрлі тапсырмаларды шешуі керек, олар мыналарды қамтуы мүмкін:

Жүйелердегі осалдықтарды іздеу — қатысушылар "жалаушаны табу" үшін программалық өнімдердегі осалдықтарды анықтап, пайдалануы керек. Бұл тапсырманың сәтті шешілгенін растайтын арнайы белгі.

Криптографиялық есептерді шешу - деректерді декодтау, хэштермен және шифрлармен жұмыс.

Желілік трафикті талдау - Желілік қосылыстар арқылы зиянды әрекеттерді немесе деректердің бұзылуын табу.

Реверс-инженерия - осалдықтарды немесе жасырын деректерді табу үшін құрастырылған кодты талдау және өзгерту.

Форензика және оқиғаларды тергеу — бұзу немесе деректердің қалай бұзылғанын түсіну үшін кибершабуыл оқиғаларын қалпына келтіру.

Ойын барысында қатысушылар теориялық білім алып қана қоймай, нақты жұмыс ортасында қолдануға болатын практикалық дағдыларды дамытады.

Оқытуда CTF қолданудың артықшылықтары

Киберқауіпсіздікті оқытуда CTF-ті қолданудың бірқатар артықшылықтары бар, олардың ішінде:

1. Практикалық бағыт - қатысушылар өздерінің кәсіби қызметінде кездесетін нақты міндеттерді шешеді.

2. Мотивация - ойын формасы оқуға деген қызығушылықты сақтауға көмектеседі, ал бәсекелестік элемент қатысушыларды материалды тереңірек зерттеуге ынталандырады.

3. Топтық жұмыс - көптеген тапсырмалар өзара әрекеттесуді және топтық жұмысты қажет етеді, бұл киберқауіпсіздік мамандары үшін маңызды, мұнда жиі ұжымдық мәселелерді шешу қажет.

4. Нақты сценарийлер - ойын барысында нақты қауіптер мен оқиғалар модельденеді, бұл оларды анықтау және жою әдістерін қолдануға мүмкіндік береді.

5. Үздіксіз жетілдіру - CTF тапсырмалары үнемі жаңартылып, күрделене түседі, бұл мамандарға Киберқауіпсіздіктің заманауи трендтерін сақтауға көмектеседі.

Оқытуда CTF қолдану жағдайлары

Тәжірибеден мысал: халықаралық CTF жарыстары

CTF-ті сәтті қолданудың жарқын мысалдарының бірі-жыл сайын DEFCON конференциясы аясында өткізілетін Defcon Capture The Flag сияқты халықаралық байқауларға қатысу. Бұл жарысқа әлемнің түкпір-түкпірінен келген ақпараттық қауіпсіздік мамандарының командалары қатысады. Тапсырмалар қарапайым осалдықтардан бастап нақты инфрақұрылымға шабуылдарды қамтитын күрделі сценарийлерге дейін. Бұл тәжірибе қатысушыларға өз дағдыларын нығайтуға көмектеседі және оларды деректер мен жүйелерді нақты қорғауға дайындайды.

Корпоративтік оқытудан мысал: ірі компаниялардың қызметкерлеріне арналған CTF

Ірі IT-компаниялардың бірінде қызметкерлердің киберқауіпсіздік дағдыларын жақсартуға бағытталған ішкі CTF турнирі ұйымдастырылды. Ойындар ықтимал қауіптер туралы хабардар болуға көмектесті және қызметкерлерді қауіпсіздік оқиғаларына тез жауап беруге үйретті. Нәтижесінде қатысушылардың күнделікті жұмысында қауіпсіздік мәселелеріне көбірек көңіл бөлетіні байқалды, бұл компания ішіндегі оқиғалардың санын азайтты.

Университеттік білім беру мысалы: ақпараттық қауіпсіздік курсына CTF енгізу

Ақпараттық қауіпсіздік курстары аясында университеттердің бірінде студенттерге арналған CTF форматы енгізілді. Ойын барысында студенттер кері инженерия, криптография және желілік шабуылдар бойынша мәселелерді шешті. Нәтижесінде, бағалаулар CTF жарыстарынан өткен студенттер дәстүрлі әдістермен оқығандарға қарағанда қауіпсіздік емтихандарында айтарлықтай жоғары нәтиже көрсеткенін көрсетті.

CTF құрылымы және мамандарға арналған мүмкіндіктер

Қазіргі уақытта барлық дайындық деңгейлері үшін CTF жарыстарын ұсынатын көптеген онлайн платформалар бар. Мұндай платформалардың мысалдары:

Hack The Box - әртүрлі CTF ойындарына қатысуға және нақты осалдықтар мен эксплуатацияларға қатысты мәселелерді шешуге арналған ең танымал онлайн платформалардың бірі.

TryHackMe - жаңадан бастаушылар мен тәжірибелі киберқауіпсіздік мамандары үшін көптеген тапсырмаларды ұсынатын тағы бір онлайн платформа.

Бұл платформалар жаңадан бастаушыларға да, тәжірибелі мамандарға да нақты сценарийлерде өз дағдыларын жетілдіруге мүмкіндік береді, оларға үнемі білім алуға және жетілдіруге мүмкіндік береді.

Қорытынды

Capture The Flag ойынын пайдалану кәсіби бағдарламашылар мен ақпараттық қауіпсіздік мамандарының кибершабуылдарды тойтару дағдыларын қалыптастырудың

куатты құралы болып табылады. Бұл оқытудың қызықты тәсілі ғана емес, сонымен қатар қатысушыларға киберқауіптермен күресуге жалпы біліктілік пен дайындықты арттыра отырып, нақты жағдайларда өз қабілеттерін дамытуға, сынауға және жетілдіруге мүмкіндік беретін тиімді әдіс. Жыл сайын CTF ойындарының танымалдығы артып келеді және көптеген ұйымдар бұл әдісті өз қызметкерлерін даярлау үшін, сондай-ақ жалпы хабардарлық пен қауіпсіздік деңгейін арттыру үшін қолдана бастайды.

Қолданылған әдебиеттер тізімі

1. Leune K., Petrilli Jr S. J. Using capture-the-flag to enhance the effectiveness of cybersecurity education //Proceedings of the 18th annual conference on information technology education. – 2017. – С. 47-52.
2. Hanafi A. H. A. et al. A CTF-based approach in cyber security education for secondary school students //electronic Journal of Computer Science and Information Technology. – 2021. – Т. 7. – №. 1.
3. Al-Karaki J. N. et al. Advancing cybersecurity education and training: Practical case study of running capture the flag (ctf) on the metaverse vs. physical settings //2023 International Conference on Intelligent Metaverse Technologies & Applications (iMETA). – IEEE, 2023. – С. 1-7.

Тұрсыналы А. Б. студент III курса
образовательной программы 6B06306
«Системы информационной безопасности»,
Евразийский национальный университет
им. Л.Н. Гумилева
Научный руководитель Аймичева Г.И.

МЕТОДЫ КРИМИНАЛИСТИЧЕСКОГО АНАЛИЗА УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

В современном мире информация является одним из самых ценных ресурсов. Конфиденциальные данные компаний, государственных структур и частных лиц находятся под постоянной угрозой компрометации. В условиях глобальной цифровизации, удаленной работы и активного использования облачных сервисов традиционные механизмы защиты часто оказываются недостаточными. Утечки конфиденциальной информации могут иметь катастрофические последствия: от финансовых потерь и потери доверия клиентов до уголовной ответственности и угрозы национальной безопасности. Они могут происходить как в результате преднамеренных действий (кибератаки, шпионаж, инсайдерские угрозы), так и по неосторожности сотрудников или технических сбоев.

Чтобы выявлять источники утечек, определять масштабы ущерба и предотвращать повторные инциденты, специалисты в области информационной безопасности используют криминалистический анализ данных[1]. Это комплекс методов, направленный на детальное изучение цифровых следов, анализ логов, восстановление удаленных данных и сбор доказательств для дальнейшего разбирательства. В данной статье рассмотрены основные

методы криминалистического анализа утечек информации, их принципы работы и роль в расследовании киберинцидентов.

Перед тем как углубляться в методы криминалистического анализа, необходимо разобраться с основными способами утечки данных. Они могут происходить по разным причинам, но в целом делятся на три основные категории:

1. Преднамеренные (злонамеренные) утечки

Этот тип утечек связан с умышленными действиями злоумышленников, направленными на получение, копирование или передачу конфиденциальной информации. Среди них:

✓ Инсайдерские угрозы – передача данных конкурентам, шантаж, финансовая выгода сотрудников.

✓ Кибератаки – целевые атаки со стороны хакеров, направленные на кражу данных.

✓ Использование вредоносного ПО – кейлоггеры, трояны, бэкдоры, предназначенные для сбора информации.

2. Непреднамеренные утечки

В этом случае данные становятся доступными для посторонних из-за случайных ошибок или небрежности пользователей:

✓ Ошибка сотрудников – отправка конфиденциальных файлов не тому адресату.

✓ Публикация данных в открытых источниках – случайное размещение закрытой информации в интернет-ресурсах.

✓ Потеря или кража носителей информации – забытые или украденные USB-накопители, ноутбуки, мобильные устройства.

3. Технические утечки

Этот вид утечек связан с уязвимостями и ошибками в информационных системах:

✓ Эксплуатация уязвимостей ПО – использование ошибок в защите баз данных, серверов или приложений.

✓ Перехват данных в сетях – атаки типа Man-in-the-Middle (MITM), подмена DNS, незащищенные соединения.

✓ Использование закладок и бэкдоров – скрытые механизмы удаленного доступа, встроенные злоумышленниками.

Каждый из этих типов утечек требует индивидуального подхода к расследованию и внедрения превентивных мер защиты. Криминалистический анализ утечек информации включает несколько основных направлений:

1. Анализ цифровых следов и логов. Любая цифровая деятельность оставляет следы в операционной системе, сетевых устройствах и приложениях[2]. Анализ этих следов позволяет выявить источник утечки и восстановить цепочку событий.

1.1. Анализ лог-файлов

Лог-файлы фиксируют все ключевые события в системе: входы пользователей, изменения в файлах, сетевые подключения.

1.2. Анализ сетевого трафика

Если данные передавались через интернет или корпоративную сеть, анализ сетевого трафика может помочь выявить их утечку. Пример инструментов:

- Wireshark – анализатор сетевого трафика.
- Zeek (Bro) – система сетевой безопасности.

2. Расследование утечки данных: анализ веб-активности. Одним из ключевых методов выявления утечки данных является анализ веб-активности подозреваемого[3]. Это позволяет определить, какие ресурсы использовались для возможной утечки данных.

Методы выявления:

• Изучение истории браузеров – анализ временных меток посещений, URL-адресов, загруженных файлов (рис.1).

```
root@kali:~/lab#  
root@kali:~/lab# rip.pl -r SYSTEM -p shimcache | grep -Ei "explore|chrome|firefox|duck"  
Launching shimcache v.20200428  
C:\Windows\Explorer.EXE 2010-11-21 03:24:11 Executed  
C:\Program Files (x86)\Google\Update\Install\{7965FA88-DF76-445A-BB63-45BD0E547356}\41.0.2272.101 chrome installer.exe 2015-03-19 21:35:59 Executed  
C:\Program Files (x86)\Internet Explorer\iexplore.exe 2010-11-21 03:25:08 Executed  
C:\Windows\system32\explorer.exe 2010-11-21 03:24:25  
C:\Program Files\Internet Explorer\iexplore.exe 2010-11-21 03:24:43  
C:\Windows\SysWOW64\ExplorerFrame.dll 2010-11-21 03:24:23  
C:\Program Files (x86)\Google\Chrome\Application\41.0.2272.101\Installer\chrmstp.exe 2015-03-22 15:11:43 Executed  
C:\Program Files (x86)\Internet Explorer\ieproxy.dll 2015-03-22 15:16:59  
C:\Windows\SysWOW64\explorer.exe 2010-11-21 03:24:25 Executed  
C:\Windows\SysWOW64\networkexplorer.dll 2010-11-21 03:24:15  
C:\Windows\System32\ExplorerFrame.dll 2010-11-21 03:24:09  
C:\Windows\System32\networkexplorer.dll 2010-11-21 03:24:02  
C:\Windows\TEMP\IE18EEB.tmp\IE11-SUPPORT\IEXPLORE.EXE 2013-10-14 22:48:14 Executed  
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe 2015-03-14 10:12:39 Executed  
C:\Program Files\Internet Explorer\iexplore.exe 2015-03-22 15:16:56 Executed  
C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE 2015-03-22 15:17:01 Executed
```

Рисунок 1. Через реестр находим все возможные браузеры (версии), которыми пользовались подозреваемые.

- Форензика кэша браузера – проверка временных файлов, cookie, сохранённых данных автозаполнения.
- Мониторинг сетевого трафика – перехват подозрительных соединений и утечек данных через файлообменные сервисы или мессенджеры.
- Анализ DNS-запросов – выявление посещения подозрительных веб-ресурсов, связанных с утечкой данных.

Пример инструментов для анализа:

- Browser History Examiner – анализ истории браузеров.
- Hindsight – форензика браузеров Google Chrome.
- X1 Social Discovery – исследование активности в социальных сетях.

Просмотр истории Google Chrome через SQLite позволяет получить подробные данные о веб-активности пользователя. Chrome хранит историю посещений в базе данных SQLite в файле History. Для анализа необходимо закрыть браузер и скопировать файл C:\Users\Аружан\AppData\Local\Google\Chrome\User Data\Default\History. Затем

этот файл открывается в SQLite Browser или через командную строку. Запрос `SELECT datetime(last_visit_time/1000000-11644473600, 'unixepoch') AS visit_time, url FROM urls ORDER BY last_visit_time DESC;` **выводит список посещенных сайтов с**

временными метками. Также можно проанализировать загруженные файлы, выполнив запрос `SELECT datetime(start_time/1000000-11644473600, 'unixepoch') AS download_time, target_path FROM downloads;` Эти методы позволяют детально исследовать веб-активность подозреваемого, выявить подозрительные действия и установить возможные источники утечек информации(рис 2.).

```

$ sqlite3 places.sqlite
SQLite version 3.46.1 2024-08-13 09:16:08
Enter ".help" for usage hints.
sqlite> .tables
moz_anno_attributes          moz_keywords
moz_annos                   moz_meta
moz_bookmarks               moz_origins
moz_bookmarks_deleted       moz_places
moz_historyvisits            moz_places_extra
moz_historyvisits_extra      moz_places_metadata
moz_inputhistory             moz_places_metadata_search_queries
moz_items_annos              moz_previews_tombstones
sqlite> select datetime(moz_historyvisits.visit_date/1000000, 'unixepoch') AS visit_time, moz_places.url FROM moz_places join moz_historyvisits
on moz_places.id = moz_historyvisits.place_id order by visit_time DESC limit 20;
2025-03-10 05:53:27|https://www.youtube.com/
2025-03-10 05:51:51|https://www.youtube.com/
2025-03-08 21:29:09|https://www.google.com/search?q=https%3A%2F%2Fwww.microsoft.com%2Fedge%2Fwelcome%3Fform%3DMT00LJX7C%D0%94%D0%BE%D0%B1D1%80
D0%BE
2025-03-08 21:28:43|https://www.microsoft.com/en-us/edge/welcome?form=MT00LJ|%D0%94%D0%BE%D0%B1D1%80%D0%BE6cs=4134690573
2025-03-08 21:28:42|https://www.microsoft.com/edge/welcome?form=MT00LJ|%D0%94%D0%BE%D0%B1D1%80%D0%BE

```

Рисунок 2. Просмотр истории Chrome SQLite

В завершении стоит отметить, что процесс криминалистического анализа утечек данных требует не только технических знаний, но и внимательности, системного подхода и умения работать с доказательствами. Сочетание передовых технологий анализа, строгих процедур безопасности и постоянного мониторинга позволяет значительно снизить риски утечек и минимизировать их последствия. Кроме того, профилактические меры, такие как контроль доступа, шифрование данных и обучение персонала, играют ключевую роль в защите информации и предотвращении возможных инцидентов.

Список использованных источников:

1. Zhang, Q., & Wang, L. (2022). Enhancing Online Testing Security: A Review of Proctoring Solutions. *Journal of Information Technology in Education*, 37(4), 321-335.
2. EC-Council. (2021). *Digital Forensics Essentials*. EC-Council official curricula.
3. Xu, W., Deng, L., & Xu, D. (2022). Towards Designing Shared Digital Forensics Instructional Materials. In *Proceedings of the 46th Annual International Computer Software and Applications Conference (COMPSAC 2022)*, 117-122.

Узбаев Р.С. (Қарағанды, ҚарТУ
Абылқас Сағынов атындағы)
Мухаметжанова Б.О.
(Қарағанды, ҚарТУ
Абылқас Сағынов атындағы)

АҚПАРАТТЫҚ-КОММУНИКАЦИЯЛЫҚ ИНФРАҚҰРЫЛЫМНЫҢ КРИТИКАЛЫҚ ОБЪЕКТІЛЕРІНДЕ АҚПАРАТТЫҚ ҚАУІПСІЗДІК ҚАТЕРЛЕРІН БОЛДЫРМАУ

Ақпараттық-коммуникациялық инфрақұрылымның маңызды объектілерін қорғау мәселесі тек бизнес үздіксіздігін қамтамасыз ету тұрғысынан ғана емес, сонымен қатар ұлттық қауіпсіздік пен қоғамдық әл-ауқатқа да тікелей қатысты. Қазіргі заманғы қоғамда ақпараттық қауіпсіздікті қамтамасыз ету, оның ішінде ақпараттық-коммуникациялық инфрақұрылымдарды қорғау мәселелері өзектілігімен ерекшеленеді, өйткені осы инфрақұрылымдардың дұрыс жұмыс істеуі кез келген мемлекет үшін негіз болып табылады. Әрбір инфрақұрылымның тиімді жұмыс істеуі үшін қауіпсіздік шараларын кешенді түрде енгізу және оларды дұрыс жүзеге асыру қажет. Тиімді қорғау әдістерін әзірлеу, сондай-ақ олардың практикалық деңгейде енгізілуі маңызды жүйелердің жұмысының бұзылуына байланысты туындайтын апаттық жағдайларды болдырмауға мүмкіндік береді [1]. Ақпараттық қауіпсіздік саласындағы жаңа тәсілдерді зерттеу және енгізу қоғамның тұрақты және қауіпсіз жұмыс істеуі үшін басым бағыттардың бірі болып табылады.

Зерттеу жұмысының мақсаты ақпараттық-коммуникациялық инфрақұрылымдардың қауіпсіздігін қамтамасыз ету үшін ақпараттық қауіп-қатерлерден қорғау әдістерін жан-жақты талдау және оңтайландыру болып табылады. Бұл мақсатқа жету үшін зерттеу барысында машиналық оқытудың жетілдірілген алгоритмдерін, динамикалық деректер шифрлеу әдістерін, жаңа қолжетімділік басқару жүйелерін интеграциялаудың маңыздылығы қарастырылады. Мұның бәрі жүйелердің киберқауіп-қатерлеріне қарсы тұрақтылығын айтарлықтай арттыратынын дәлелдеуге бағытталған.

Ақпараттық қауіпсіздікті қорғаудың дәстүрлі әдістері қазіргі таңда кейбір жағдайларда тиімді болып табылатынына қарамастан, олар жаңа және күрделі қауіптерге қарсы күресте кейде жеткіліксіз болып қала береді. Бұл мәселе қоғамның ақпараттық қауіпсіздігіне тәуелділігін арттырып, инфрақұрылымдық жүйелердің жұмысын тұрақсыздандыруы мүмкін. Технологиялар дамыған сайын жаңа қауіптер пайда болып, оларды бақылау және алдын алу шаралары да күрделене түседі. Сонымен қатар, кибершабуылдар мен басқа да ақпараттық қауіптер ескірген қорғау әдістерін бұзып өтеді, бұл қорғау жүйелерін жетілдірудің қажеттілігін көрсетеді.

Қазіргі заманғы ақпараттық қауіпсіздік әдістері жоғары бейімделгіштігі мен икемділігі арқасында, жүйелердің түрлі қауіптерге жауап беру қабілетін арттырады. Бұл әдістер кибершабуылдарды анықтау, алдын алу және оларға тиімді жауап беру процестерін әлдеқайда тиімді жүзеге асыруға мүмкіндік береді. Сонымен қатар, қазіргі заманғы ақпараттық қауіпсіздік әдістері жүйелердің жоғары деңгейдегі қауіпсіздігін қамтамасыз ете отырып, осы инфрақұрылымдардың тұрақтылығын арттырады.

Ақпараттық қауіпсіздік әдістері ақпараттың құпиялылығын, бүтіндігін және қолжетімділігін қамтамасыз ету үшін әртүрлі тәсілдер мен технологияларды қамтиды. Бұл әдістерді бірнеше негізгі категорияға бөліп қарастыруға болады: криптографиялық әдістер, қол жеткізуді басқару, желілік инфрақұрылымды қорғау, антивирустық қорғау, резервтік көшіру және қалпына келтіру, қауіпсіздік саясаты мен процедуралары, сондай-ақ қызметкерлерді ақпараттық қауіпсіздік негіздері бойынша оқыту мен хабардарлықты арттыру [2-3].

Криптографиялық әдістер ақпаратты қорғаудың негізі болып табылады. Олар ақпараттың құпиялылығын және бүтіндігін қамтамасыз етеді, деректерді шифрлеу арқылы оларды заңсыз пайдаланушылардан қорғайды. Қол жеткізуді басқару жүйелері ақпараттық жүйелердің қауіпсіздігін қамтамасыз етуде маңызды рөл атқарады. Бұл жүйелер аутентификация мен авторизация әдістерін қамтиды. Желілік инфрақұрылымды қорғау жүйелері желіде орын алатын қауіптерден қорғауды қамтамасыз етеді. Бұл құралдар желілік трафикті алдын ала белгіленген ережелерге сәйкес бақылап, сүзгіден өткізу арқылы ішкі және сыртқы шабуылдарды болдырмауға көмектеседі. Антивирустық қорғау жүйелері жүйелерді вирустар, құрттар, трояндар және басқа зиянды бағдарламалардан қорғау үшін қолданылады. Оларға үнемі жаңартылатын вирусқа қарсы бағдарламалар және зиянды бағдарламаларды анықтау әдістері кіреді. Мұндай әдістер жүйені зиянды бағдарламалардан қорғауға және олардың таралуын тоқтатуға мүмкіндік береді.

Қауіпсіздік саясаты мен процедуралары да маңызды аспект болып табылады. Ұйымдар ақпараттық қауіпсіздік саясатын жасап, оны енгізуі керек, ол мінез-құлық ережелерін, қорғау шараларын және инциденттерге жауап беру процестерін анықтайды. Сонымен қатар, қызметкерлерді ақпараттық қауіпсіздік бойынша оқыту және оларды ықтимал қауіптерден хабардар ету өте маңызды. Бұл шаралар ақпараттық қауіпсіздіктің сақталуына және инциденттердің алдын алу үшін маңызды рөл атқарады.

Ақпараттық қауіпсіздікті қорғаудың кешенді тәсілі әртүрлі қауіптер мен осалдықтардан қорғауды қамтамасыз ететін көп деңгейлі қорғауды білдіреді. Бұл әдістерді біріктіріп қолдану жүйелердің сенімділігін арттыруға және инфрақұрылымның барлық деңгейінде ақпаратты қорғауға мүмкіндік береді. Сонымен қатар, ақпараттық қауіпсіздікті қорғау әдістерінің тиімділігін бағалау өте маңызды. Бағалау процесі олардың практикалық құндылығын анықтап, жүйелерді қорғау қабілетін тексеруге мүмкіндік береді. Бағалаудың негізінде шешімдерді жақсарту бойынша ұсыныстар жасалады [4].

Ақпараттық-коммуникациялық инфрақұрылымдарды қорғаудың қазіргі заманғы әдістері дәстүрлі шешімдермен салыстырғанда едәуір тиімділікті көрсетеді. Дәстүрлі әдістер, мысалы, деректерді статикалық шифрлеу және қолжетімділік басқару жүйелері, базалық қорғауды қамтамасыз етуде тиімді болғанымен, олар динамикалық қауіптерге бейімделудің төмендігі мен қаталдық мәселелеріне тап болады. Дәстүрлі жүйелер қазіргі заманғы күрделі кибершабуылдармен күресуде жеткіліксіз болуы мүмкін. Қазіргі заманғы әдістер аномалияларды анықтау жүйелері мен жетілдірілген қолжетімділік басқару жүйелерін қолдану арқылы қауіптерді тез анықтауға және оларға тиімді жауап беруге мүмкіндік береді. Мұндай жүйелер машиналық оқытуды және үлкен деректерді талдауды қолдана отырып, жаңа және күрделі қауіптерді анықтай алады.

Ақпараттық қауіпсіздік әдістерінің тиімділігін бағалау, олардың нақты құндылығын анықтауға, жақсартуға болатын салаларды анықтауға және ақпараттық-коммуникациялық инфрақұрылымды тиімді қорғау қабілетін растауға мүмкіндік береді. Тиімді бағалау жүйелердің әлсіз тұстарын анықтауға және оларды түзету бойынша нақты шараларды ұсынуға мүмкіндік береді, осылайша инфрақұрылымның қауіпсіздігін арттыруға көмектеседі.

Жалпы алғанда, ақпараттық қауіпсіздік саласындағы жаңа тәсілдер мен әдістердің енгізілуі қазіргі қоғамдағы киберқауіп-қатерлерге тиімді қарсы тұруға мүмкіндік береді. Осы саладағы жетістіктер мен жаңа технологиялар ақпараттық-коммуникациялық инфрақұрылымдардың тұрақтылығын арттыруға және оларды жаңа және күрделі қауіптерден қорғауға бағытталған маңызды қадам болып табылады.

Пайдаланылған әдебиеттер тізімі:

1. Аверченков В.И., Рытов М.Ю., Рудановский М.В., Кондрашин Г.В. Системы защиты информации в ведущих зарубежных странах: учебное пособие / В.И. Аверченков - Москва: ФЛИНТА, 2021. - С. 224 - ISBN 978-5-9765-1274-0

2. Сэрра Э. Кибербезопасность: правила игры: как руководители и сотрудники влияют на культуру безопасности в компании / Э. Сэрра; ред. М. Приморская; пер. с англ. Л. Смилевски. – Москва: Альпина Паблишер, 2022. - С.192 - ISBN 978-5-907470-58-3

3. Белоус А.И. Основы кибербезопасности: стандарты, концепции, методы и средства обеспечения / А.И. Белоус, В.А. Солодуха - Москва: Техносфера, 2021. – С. 482– ISBN 978-5-94836-612-8.

4. Солдаткина М.В. Теоретико-вероятностный подход к проблемам криптографии / М. В. Солдаткина – Москва; Берлин: Директ-Медиа, 2021. -60 с. - ISBN 978-5-4499-1734-8.

5. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems / R. Anderson – 3rd ed. – Hoboken: Wiley, 2020. pp. 624– ISBN: 978-1-119-64

УДК 004.4'415

Шегетаева А. К. (ЕНУ им. Л.Н.Гумилева)

Нуриев У. Г. (Университет Эге, Турция)

АНАЛИЗ И ПРОГНОЗИРОВАНИЕ УЯЗВИМОСТЕЙ: ИСПОЛЬЗОВАНИЕ ДАННЫХ CVE ДЛЯ ПОВЫШЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Введение. Прогнозирование сетевых уязвимостей играет важную роль в защите данных и организаций от потенциальных атак. С ростом интернета и увеличением числа кибератак в 2000-х годах возникла необходимость в более системном подходе к управлению уязвимостями. В этом контексте базы данных, такие как CVE (общие уязвимости и воздействия), стали важным шагом в организации информации о различных уязвимостях.

С развитием технологий машинного обучения и использованием сложных алгоритмов, таких как решающие деревья и случайные леса, открываются новые возможности для более точного анализа данных. Следовательно, *целью данного исследования* - анализ уязвимостей и разработки программы, использующей данные из базы данных CVE.

Таким образом, машинное обучение подчеркивает технологический контекст и инструменты, которые могут быть использованы для решения задачи, обозначенной во втором предложении. Это создает логическую последовательность: машинное обучение открывают новые возможности для анализа уязвимостей, что и является целью исследования.

Для успешного выполнения исследования, можно выделить *следующие задачи*:

- получить доступ к базе данных CVE и загрузить актуальные данные.
- очистить данные от дубликатов и пропусков, а также отфильтровать их по критериям (например, по годам и уровню CVSS).
- использовать статистические методы для анализа распределения уязвимостей по годам и категориям.

`df = df[df['CVSS_Score'] >= high_critical_threshold]` (в данном случае фильтруются строки, где значение в столбце **CVSS_Score** больше или равно 7.0).

Анализ и прогнозирование. Следующий этап - проведение очистки данных, включая удаление дубликатов и записей с отсутствующими ключевыми значениями, чтобы обеспечить качество и целостность данных для дальнейшего анализа:

```
df.drop_duplicates(inplace=True)
df.dropna(inplace=True).
```

Вывод информации о очищенном наборе данных

```
print(f"Количество записей после очистки: {df.shape[0]}")
print(df.head()).
```

Результаты. Эти шаги по очистке и подготовке данных обеспечили создание качественного набора данных, который был готов для дальнейшего анализа и прогнозирования.

Следующий код иллюстрирует процесс загрузки и фильтрации данных из CVE:

```
1  rt matplotlib.pyplot as plt
2  rt pandas as pd
3
4  = {'Year': [2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007,
5  2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017,
6  2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025],
   'Vulnerabilities': [1202, 1709, 2255, 2209, 3299, 5817, 8431,
   8256, 6208, 5626, 4953, 4416, 6171, 6815, 8710, 7231, 8342,
   16286, 17522, 18528, 18874, 22786, 27065, 29066, 40299, 10756]}
   pd.DataFrame(data)
7
8  figure(figsize=(10, 6))
9  plot(df['Year'], df['Vulnerabilities'], marker='o')
10 title('Распределение уязвимостей по годам')
11 xlabel('Года')
12 ylabel('Количество уязвимостей')
13 grid(True)
14 show()
15
```

В результате выполнения этого кода получили график, который визуализирует, как количество уязвимостей изменялось с течением времени, показывает анализ тенденций в условиях растущих киберугроз.



В заключении отметим, что применение выбранного метода играет ключевую роль в повышении уровня кибербезопасности организаций и использование данных об уязвимостях позволяет не только улучшить защиту информационных систем, но и способствует формированию более устойчивой культуры безопасности внутри организаций. Это, в свою очередь, помогает минимизировать риски и защищать данные от потенциальных кибератак.

Кроме этого, стоит общий вопрос выяснения разработки более сложных моделей и интеграцию их в системы управления безопасностью, что позволит организациям более эффективно реагировать на возникающие угрозы.

Список использованных литератур

1. Bin Hulayyil, S.; Li, S.; Xu, L. Machine-Learning-Based Vulnerability Detection and Classification in Internet of Things Device Security // Electronics 2023, 12, 3927. <https://doi.org/10.3390/electronics12183927>
2. Оспанова А.Б., Шегетаева А.К., Түсіпханов А. Т., Жалгасбаев А. Б., Кадринов Д. М. Прогнозирование сетевых уязвимостей и эксплойтов. Международная научно-практическая конференции «XVI Сагиновские чтения. Интеграция образования, науки и производства» - Караганда: Изд-во КарТУ им. А.Сагинова, 2024. Ч.2, С.287-289. URL: <https://www.kstu.kz/wp-content/uploads/2024/07/2-chast.pdf>

Шерехан Н.Қ.

Л.И. Гумилев атындағы Еуразиялық ұлттық университеті,
Астана қ., Қазақстан, e-mail: sherekhannazerke03@gmail.com

Қазақстан Республикасының криптографиялық алгоритмдерге негізделген ұлттық стандарттары: халықаралық және мемлекетаралық стандарттар

Аңдатпа

Бұл мақалада Қазақстан Республикасының криптографиялық стандарттарының халықаралық және мемлекетаралық стандарттармен үйлесімділігі қарастырылады. Ұлттық

стандарттарды жетілдіру елдің ақпараттық қауіпсіздігін нығайтуға және халықаралық деңгейде бәсекеге қабілеттілігін арттыруға бағытталған. Қазақстанда қолданыстағы криптографиялық стандарттар көбінесе ГОСТ, ДСТУ, ISO және NIST сияқты шетелдік стандарттарға негізделген. Мемлекетаралық стандарттар, мысалы, ГОСТ пен ДСТУ, ТМД елдері арасында деректер алмасудың қауіпсіздігін қамтамасыз ету мақсатында қабылданған. Сонымен қатар, Қазақстан халықаралық ұйымдар әзірлеген AES, RSA, ECC, SHA-2 және SHA-3 сияқты криптографиялық алгоритмдерді кеңінен қолданады. Елдің ақпараттық қауіпсіздігін нығайту үшін дербес ұлттық стандарттардың болуы маңызды, ал олардың сақталуын тиісті ұлттық органдар қадағалайды.

Кілт сөздер: криптографиялық стандарттар, Қазақстан, ГОСТ, ДСТУ, ISO, NIST, ақпараттық қауіпсіздік, шифрлау алгоритмдері.

Қазақстан Республикасының ұлттық криптографиялық стандарттарын жетілдіру тек елдің қауіпсіздігі үшін ғана емес, сонымен қатар халықаралық аренада бәсекеге қабілеттілікті арттыру үшін маңызды. Халықаралық және мемлекетаралық стандарттармен үйлесімді криптографиялық алгоритмдерді енгізу Қазақстанның шетелдік серіктестерімен ақпарат алмасу процесін қауіпсіз етуге және әлемдік экономикаға сәтті интеграциялануға ықпал етеді.

Ұлттық стандарттар дербес мемлекеттің ақпараттық қауіпсіздігін қамтамасыз етуде маңызды рөл атқарады. Олар елдің қауіпсіздік талаптарына сәйкес келетін криптографиялық алгоритмдерді әзірлеп, қолдануды реттейді. Халықаралық деңгейде бұл стандарттардың маңызы зор, себебі олар басқа елдермен технологиялық ынтымақтастықты жеңілдетеді және экспортқа бағытталған өнімдер үшін сенімділік деңгейін арттырады. Мысалы, Қазақстанның ұлттық стандарттары халықаралық стандарттармен үйлесімді болғанда, отандық технологиялар әлемдік нарыққа еркін шыға алады, бұл елдің цифрлық дербестігін нығайтады.

Халықаралық криптография стандарттарын NIST (АҚШ ұлттық стандарттар және технологиялар институты), ISO/IEC (Халықаралық стандарттау ұйымы) және ETSI (Еуропалық телекоммуникация стандарттары институты) сияқты беделді ұйымдар әзірлейді. NIST дайындаған жетілдірілген шифрлау стандарты (AES) қазіргі уақытта халықаралық стандарт ретінде қабылданды және электрондық деректерді қорғау мақсатында кеңінен қолданылады. AES - тен басқа RSA және ECC стандарттары халықаралық стандарттар ретінде кеңінен пайдаланады. Бұл стандарттар халықаралық келісімдер мен шарттармен белгіленеді. (Калиски,).

Мемлекетаралық стандарттар елдер арасында қауіпсіз байланыс пен деректер алмасуды қамтамасыз етуде маңызды рөл атқарады. Бұндай стандарттарды белгілі бір аймақтық ұйымдар немесе екіжақты келісім бойынша жасайды. Мемлекетаралық стандарттар көбінесе халықаралық стандарттарға негізделген, бірақ белгілі бір аймақтық қажеттіліктерді қанағаттандыру үшін қлсымша талаптарды қамтиды. ГОСТ, ДСТУ және СТБ секілді мемлекетаралық стандарттар бұрынғы КСРО елдерінде қолданылады және шифрлауды, электрондық қолтаңбаны және аутентификацияны реттейді. Бұл стандарттар ТМД мен Еуразиялық экономикалық одақ (ЕАЭО) кеңістігіндегі криптографиялық жүйелердің үйлесімділігін қамтамасыз ету үшін қабылданып келісілген.

Қазақстан Республикасының стандарттары ГОСТ, ДСТУ, ISO және де басқа да халықаралық стандарттарға негізделген. Украина елінің ұлттық стандартына (ДСТУ) зер салатын болсақ бастапқыда сол елге арнайы жасалынған болатын, бірақ кейінірек стандарттың кейбір алгоритмдері мемлекетаралық ретінде қабылданып, басқа мемлекеттерде де қолданысқа енген болатын.

Қазақстан Республикасында қолданыстағы стандарттарды қарастырсақ:

СТ РК 1073-2007 – Ресейлік ГОСТ 28147-89 (блоктық шифрлау) негізінде жасалған.

ДСТУ Қазақстанда Украина стандарттарына ұқсас кейбір криптографиялық стандарттар қолданылады.

NIST және ISO стандарттарын қолдану көптеген ұйымдар AES, SHA-2, SHA-3, RSA және басқа халықаралық криптографиялық алгоритмдерді пайдаланады.

Бұл халықаралық криптографиялық стандарттарды Қазақстан кеңінен қолдануда. Елдің ақпараттық қауіпсіздігін арттыру үшін Қазақстан Республикасының ұлттық стандарты болуы маңызды. Криптографиялық стандарттардың сақталуын тиісті ұлттық органдар қамтамасыз етеді.

Қазақстан мемлекетаралық стандарттарды қолдану арқылы ТМД елдері арасындағы ақпараттық қауіпсіздікті қамтамасыз етуге ұмтылады. Мемлекетаралық стандарттар ретінде ГОСТ және ДСТУ стандарттары қарастырылады. Бұл стандарттар криптографиялық жүйелердің үйлесімділігін сақтауға, деректер алмасу қауіпсіздігін арттыруға және мемлекетаралық ынтымақтастықты нығайтуға мүмкіндік береді.

Қазақстан Республикасының криптографиялық стандарттары халықаралық және мемлекетаралық тәжірибеге негізделген. Елдің ақпараттық қауіпсіздігін нығайту үшін дербес ұлттық стандарттардың болуы маңызды. Қазақстанда криптографиялық алгоритмдердің қауіпсіздігі мен олардың стандарттарға сәйкестігін қадағалайтын тиісті мемлекеттік органдар жұмыс істейді. Болашақта ұлттық криптографиялық стандарттарды әзірлеу мен дамыту ақпараттық қауіпсіздікті одан әрі күшейтуге ықпал етеді.

Пайдаланылған әдебиеттер тізімі

1. Иванова И.И. Стандарт и стандартизация: общие понятия // КиберЛенинка. URL: <https://cyberleninka.ru/article/n/standart-i-standartizatsiya-obschie-ponyatiya>
2. ГОСТ 1.5-2001. Ресей Федерациясындағы стандарттау. Ресей Федерациясының ұлттық стандарттары. Жалпы ережелер. URL: <https://tk039.no-e.ru/PDF/НПА/ГОСТ%201.5-2001.pdf>
3. Helpiks.org. Криптографиялық алгоритмдер және олардың стандарттары. URL: <https://helpiks.org/1-42046.html>
4. Cryptography.kz. Қазақстан Республикасының криптографиялық стандарттары. URL: <https://cryptography.kz/ru/standards-of-qazaqstan.html>
5. Satbayev University журналы. Қазақстан Республикасындағы криптографиялық стандарттардың дамуы. URL: <https://ce.journal.satbayev.university/index.php/journal/article/view/1260>

ЕУРАЗИЯЛЫҚ ХАЛЫҚАРАЛЫҚ ҒЫЛЫМИ КОНФЕРЕНЦИЯ
ЕВРАЗИЙСКАЯ МЕЖДУНАРОДНАЯ НАУЧНАЯ КОНФЕРЕНЦИЯ

«ҒЫЛЫМДАҒЫ, ТЕХНИКА МЕН ИНДУСТРИЯДАҒЫ ЖАСАНДЫ ИНТЕЛЛЕКТ ЖӘНЕ
КЕРІ ЕСЕПТЕР»

«ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ОБРАТНЫЕ ЗАДАЧИ В НАУКЕ, ТЕХНИКЕ И
ИНДУСТРИИ»

«ARTIFICIAL INTELLIGENCE AND INVERSE PROBLEMS IN SCIENCE, TECHNOLOGY
AND INDUSTRY»

ЕҢБЕКТЕРІ ТРУДЫ PROCEEDINGS

Л.Н. Гумилев атындағы Еуразия ұлттық университеті
010008, Астана қаласы, Сатбаев 2.