СПИСОК
научных и методических трудов
КАПАЛОВОЙ НУРСУЛУ АЛДАЖАРОВНЫ

ORCID ID: 0000-0001-9743-9981
Author ID в Scopus: 57191242124
Author ID в Web of Science: P-5631-2017
h-индекс в Scopus: 3
h-индекс в Web of Science: 3

№ п/п	Наименование научного труда	Характер	Выходные данные	Объем в п.л.	Соавторы
Публикации в базе данных Scopus, Web of Science					
1.	A block encryption algorithm based on exponentiation transform	Печ.	Cogent Engineering. – 2020. – № 7 (1788292). – P. 1-12 // https://doi.org/10.1080/23311916.2020.1788292 **Scopus (CiteScore процентиль 62, Квартиль Q2)**	0,75	Ardabek Khompysh, Müslüm Arici, Kunbolat Algazy.
2.	On a Certain Model of Cryptographic Key Management	Печ.	Eurasian Journal of Mathematical and Computer Applications. – 2020. – Volume 8, Issue 4. – P. 15-22. **Scopus (CiteScore процентиль 25, Квартиль Q3)**	0,44	Nyssanbayeva, S., Haumen A.
3.	Cryptographic Key Manage-ment System Model	Печ.	Journal of Theoretical and Applied Information Technology – 2020. – Volume 98, Issue 21. – P. 3482-3493 **Scopus (CiteScore поцентиль 36, Квартиль Q4)**	0,68	Nyssanbayeva S., Haumen A., Varennikov A.,
4.	Differential Cryptanalysis of New Qamal Encryption Algorithm	Печ.	International journal of electronics and telecommunications, No 4, 2020, P. 647-653. **(CiteScore поцентиль 27, Квартиль Q4)**	0,37	K.T. Algazy, L.K. Babenko, R.G. Biyashev, E.A. Ishchukova, S.E. Nysynbaeva, Andrzej Smolarz
5.	Development and Analysis of Symmetric Encryption Algorithm Qamal Based on a Substitution-permutation Network	Печ.	International journal of electronics and telecommunications, No 1, 2021, P. 127-132. **Scopus (CiteScore процентиль 27, Квартиль Q4)**	0,31	R.G. Biyashev, D.S. Duysenbayev, K.T. Algazy, Waldemar Wojcik, Andrzej Smolarz
6.	The model of encryption algorithm based on non-positional polynomial notations and constructed on	Печ.	Open Engineering – 2018. – Volume 8, Issue 1. – P. 140-146. **Scopus (CiteScore процентиль 40,**	0,38	Haumen A.

Ученый секретарь ИИВТ КН МОН РК _____ **Усатова О.А.**

Автор _____ **Капалова Н.А.**

	an SP-network		**Квартиль Q3)**		
7.	Development and analysis of the encryption algorithm in nonpositional polynomial notations //	Печ.	Eurasian Journal of Mathematical and Computer Applications. – 2018. - № 6(2). - P.19-33. **Scopus (CiteScore процентиль 25, Квартиль Q3)**	0,88	Biyashev, R.G., Kalimoldayev M.N., Nyssanbayeva, S.E., Dyusenbayev, D.S., Algazy K.T.,
8.	Creating an algorithm of encryption based on prime numbers in positional systems of calculating residual classes | Tworzenie algorytmu szyfrowania na bazie liczb pierwszych w pozycyjnych układach obliczania klas resztowych	Печ.	Przeglad Elektrotechniczny, - 2018, 94(2), P. 164 -169 **Scopus (CiteScore процентиль 22, Квартиль Q3)**	0,31	Wojcik, W., Kalimoldaev, M., Biyashev, R., Nugmanova S.A., Mergenbayev, Y.B.
9.	Security analysis of an encryption scheme based on nonpositional polynomial notations	Печ.	Open Engineering – 2016.- №6. – P. 250-258. **Scopus (CiteScore процентиль 40, Квартиль Q3)**	0,5	Dyusenbayev D.
В материалах конференций, индексируемых в базах Web of Science, Scopus					
10.	Algebraic cryptanalysis of block ciphers	Печ.	International Conference on Wireless Communication, Network and Multimedia Engineering. Advances in Computer Science Research. - Atlantis press, 2019. – Vol. 89. - P. 129-132. (https://doi.org/10. 2991/ wcnme-19.2019.30)	0,19	Rustem Biyashev, Dilmuhanbet Dyusenbayev, Kunbolat Algazy
11.	Investiga-tion of the different implementations for the new cipher Qamal.	Печ.	Proceedings of the 12th Inter-national Conference on Security of Information and Networks. – 2019. – P. 1-8.	0,5	Algazy K., Biyashev R., Babenko L., Ishchukova E., Nyssanbayeva S.
12.	Modified symmetric block encryption-decryption algorithm based on modular arithmetic	Печ.	Proceedings of the International Conference on Wireless Communications, Network Security and Signal Processing (WCNSSP2016). - Chiang Mai, Thailand, 2016. P. 263-265	0,13	Biyashev, R. Nyssanbayeva S., Haumen A.,
13.	Construction and analysis of models of increasing reliability for modular encryption algorithm	Печ.	Proceedings of the 10th International Conference on Computer Engineering and Applications (CEA '16). - Barcelona, Spain, February	0,25	Biyashev R., Nyssanbayeva S., Haumen A.,

Ученый секретарь ИИВТ КН МОН РК **Усатова О.А.**

Автор **Капалова Н.А.**

			13-15, 2016. –P. 161-165.		
14.	Modular models of the cryptographic protection of information //	Печ.	International Conference on Computer Networks and Information Security (CNIS2015), Changsha, China. 2015. - P.393-398 (Thomson Reuters).	0,31	Biyashev R., Nyssanbayeva S., Khakimov R..
15.	Asymmetric Encryption on the Basis of Non-positional Polynomial Notations	Печ.	Proceedings of the 6th International Conference on Applied Informatics and Computing Theory (AICT '15). - Salerno, Italy, 2015.- P. 225-231 (Scopus).	0,38	R. Biyashev, S. Nyssanbayeva
16.	The Key Exchange Algorithm on Basis of Modular Arithmetic	Печ.	Proceedings of International Conference on Electrical, Control and Automation Engineering (ECAE2013), December 1-2, 2013, Hong Kong. - Lancaster, U.S.A., DEStech Publications. – P. 501-505. (index EI Compendex and ISTP).	0,25	Biyashev R., Nyssanbayeva S.,
В изданиях, включенных перечень Комитета (кроме материалов конференций)					
17.	Модифицированный алгоритм шифрования Эль-Гамаля на базе непозиционных полиномиальных систем счисления	Печ.	Известия Национальной академии наук РК. – Алматы, 2013. – № 1. – С. 22-26	5 стр	
18.	Неприводимые многочлены над полем GF(2n)	Печ.	Известия научно-технического общества «КАХАК». – Алматы, 2013. – № 1. – С. 17-28	11 стр	Нысанбаева С.Е., Хакимов Р.А.
19.	Software Implementation of the Cryptographic System Models with the Given Cryptostrength	Печ.	Совместный выпуск по матер. междунар. конф. «Вычислительные и информационные технологии в науке, технике и образовании» (CITech-2015), Вычислительные технологии, Вестник КазНУ им. Аль-Фараби, серия математика, механика, информатика, 2015. – Т. 20, № 3(86), – С.117-121.	4 стр	R. Biyashev, M. Kalimoldayev, S. Nyssanbayeva, R. Khakimov.
20.	Позициялық емес полиномдық санау жүйесіне негізделген	Печ.	Қ.И. Сәтбаев атындағы ҚазҰТУ Хабаршысы. – Техникалық ғылымдар –	4 стр	Хаумен А.

Ученый секретарь ИИВТ КН МОН РК _____ **Усатова О.А.**

Автор _____ **Капалова Н.А.**

Қаржылық емес құжаттар үшін

	шифрлеу алгоритмінің бір моделін зерттеу және компьютерлік жүзеге асыру		Алматы: ҚазҰТУ, 2015. - №4(110). – Б. 441-445.		
21.	«Криптографиялық кілттерді ашық тарату рәсімдерін зерттеу және дамыту»	Печ.	ҚазҰПУ Хабаршысы, №3 (55). -Алматы, 2016. - С. 165-170.	5 стр	Камбаров Ж. Н.
22.	Криптоанализ алгоритма шифрования на базе непозиционных полиномиальных систем счисления	Печ.	Вестник КазНУ. Серия математика, механика, информатика - Алматы, 2016. - №3/1(90). С. 41-51.	10 стр	Дюсенбаев Д.С.
23.	Позициялық емес полиномдық санау жүйесіне негізделген шифрлеу алгоритмінің SP-желі бойынша құрастырылған моделі	Печ.	Вестник КазНИТУ, Физико-математические науки. – Алматы, 2017. – С. 445-449.	5 стр	Хаумен А.
24.	Умножители полиномов по модулю неприводимых полиномов	Печ.	Вестник Национальной академии наук Республики Казахстан - Алматы, 2017. - №4. - С. 48-53.	5 стр	Калимолдаев М. Н., Тынымбаев С. Т.
25.	Криптоанализ генератора псевдослучайных последовательностей и ее модификация	Печ.	Вестник КазНИТУ. - 2019, №3, С. 179-185	6 стр	Бияшев Р.Г., Алғазы К.Т., Хомпыш А., Дюсенбаев Д.С.
26.	Модуль бойынша дәрежеге шығару негізінде ақпаратты криптографиялық қорғау алгоритмінің модификациясы	Печ.	Хабаршы ҚазККА. – Алматы, 2019. – № 4. – 247-253 б.	6 стр	Алгазы К.Т., Хомпыш А.
27.	«AL01» шифрлау алгоритміне криптографиялық талдау	Печ.	Хабаршы КазҰТЗУ. – Алматы, 2019. – № 5. – 92-98 б.	6 стр	Дюсенбаев Д., Сақан Қ., Алғазы К.
28.	Исследование разработанного алгоритма на основе преобразования ЕМ по критерию «лавинного эффекта»	Печ.	Вестник КазАТК. – Алматы, 2020. - №3. - С.284-292.	8 стр	Хомпыш А., Алгазы К.Т.
29.	Модель системы управления криптографическими ключами на основе НПСС	Печ.	Вестник КазНИТУ. – Алматы, 2020. – №4 (140). – С. 499-504. (ГФ АР05132568).	5 стр	Варенников А.В.
Авторские свидетельства					
30.	Программа шифрования файлов «AL01 Crypto (версия 1.0)»		А.с. 10662. опубл. 09.06.2020. – 1 с.	2 стр	Варенников А.В., Бияшев Р.Г., Нысанбаева С.Е.,

Ученый секретарь ИИВТ КН МОН РК _____ **Усатова О.А.**

Автор _____ **Капалова Н.А.**

					Дюсенбаев Д.С., Алғазы К.Т.;
31.	Система управления криптографическими ключами «CKMS Crypto 1.0» (программа для ЭВМ)		А.с. 12108. опубл. 22.09.2020.	2 стр	Нысанбаева С.Е, Варенников А.В.;
32.	Sandyq v 1.02 (программа для ЭВМ)		А. с. 4211. опубл. 25.06.2019.	2 стр	Нысанбаева С. Е., Хаумен А.
33.	Qamal v 1.0.1 (программа для ЭВМ) /		А. с. 5200. опубл. 06.09.2019.	2 стр	Бияшев Р.Г., Алгазы К.Т., Дюсенбаева Д.С., Сақан Қ.С.
34.	Программа шифрования файлов «CryptoEM v1.0.1 (программа для ЭВМ)		А. с. 5450. опубл. 24.09.2019.	2 стр	Хомпыш А.
35.	Объект авторского права под названием «Генератор псевдослучайной последовательности PSG1.1» (программа для ЭВМ)		А. с. 3619. опубл. 27.05.2019, МЮ РК	2 стр	Бияшев Р.Г., Нысанбаева С.Е, Алгазы К.Т., Дюсенбаева Д.С;
36.	Авторское свидетельство: Объект авторского права под названием «Умножитель на четыре по модулю» (произведение науки)		А. с. 009063. опубл. 26.06.2017, Бюл. № 1536. - 2 с.	2 стр	Бияшев Р. Г., Калимолдаев М. Н., Нысанбаева С. Е., Тынымбаев С. Т.,
37.	Авторское свидетельство: Объект авторского права под названием «Устройство приведения числа по модулю» (произведение науки)		А. с. 009096. опубл. 28.06.2017, Бюл. № 1572. - 2 с.	2 стр	Бияшев Р. Г., Калимолдаев М. Н., Нысанбаева С. Е., Тынымбаев С. Т.,

Ученый секретарь ИИВТ КН МОН РК _____ **Усатова О.А.**

Автор _____ **Капалова Н.А.**