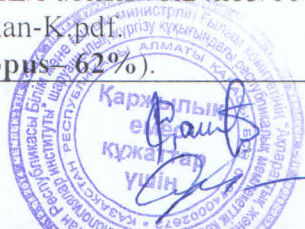





ҒЫЛЫМИ ЕҢБЕКТЕР ТІЗІМІ

p/c №	Еңбектерінің аты	Қол жазба немесе баспа	Баспа аты, журналдың аты (№, жыл), авторлық куәлік №	Баспа табак немесе бет саны,	Жұмыс серіктес авторларының фамилиясы
1	Development and analysis of the new hashing algorithm based on block cipher	Баспа	Eastern-European Journal of Enterprise Technologies. – 2022. – No. 2/9(116), pp. 60-73. Doi: 10.15587/1729-4061.2022.252060, (Scopus – 48%).	14	Nyssanbayeva S., Kapalova N., Algazy K., Khompysh A., Dyusenbayev D.
2	Design of substitution nodes (S-Boxes) of a block cipher intended for preliminary encryption of confidential information	Баспа	Cogent Engineering. – 2022. – Vol. 9, No. 1. Doi: 10.1080/23311916.2022.2080623, (Scopus – 66%, Web of Science – Q2).	14	Khompysh A., Kapalova N., Algazy K., Dyusenbayev D.
3	A new hashing algorithm – HAS01: development, cryptographic properties and inclusion in graduate studies	Баспа	Global Journal of Engineering Education. – 2022. – Vol. 24, No. 2, pp. 155-164, http://www.wiete.com.au/journals/GJEE/Publish/vol24no2/09-Sakan-K.pdf , (Scopus – 62%).	10	Kapalova N., Dyusenbayev D.
4	Differential analysis of a cryptographic hashing algorithm HBC-256	Баспа	Appl. Sci. – 2022, 12(19), 10173. Doi: 10.3390/app121910173, (Scopus – 59%, Web of Science – Q2)	15	Algazy K., Kapalova N., Nyssanbayeva S., Dyusenbayev D.
5	Development and study of an encryption algorithm	Баспа	Computation. – 2022, 10(11), 198. Doi: 10.3390/computation10110198, (Scopus – 70%, Web of Science – Q2)	16	Kapalova N., Algazy K., Dyusenbayev D.
6	Higher professional and postgraduate training of information security specialists	Баспа	Global Journal of Engineering Education. – 2022. – V. 24, No. 3, pp. 232-238, http://wiete.com.au/journals/GJEE/Publish/vol24no3/10-Sakan-K.pdf , (Scopus – 62%).	7	Kapalova N., Nyssanbayeva S., Varennikov A., Dyusenbayev D.
Ізденуші					Қ.С. Сақан
Ғалым хатшы					О.А. Усатова

7	Evaluation of the strength and performance of a new hashing algorithm based on a block cipher	Баспа	International Journal of Electrical and Computer Engineering. – 2023. –Vol. 13, No.3, pp. 3124-3130, Doi: 10.11591/ijece.v13i3.pp3124-3130, (Scopus – 66%).	7	Algazy K., Kapalova N.	
8	Разработка и исследование алгоритмов хеширования произвольной длины	Баспа	Монография. – Алматы, Guppyprint, 2022. – 95 с. ISBN 978-601-08-2549-9.	95	Бияшев Р.Г., Нысанбаева С.Е., Капалова Н.А., Дюсенбаев Д.С., Алгазы К.Т.	
9	Исследование алгоритмов шифрования «AL01» и «Qamal» на основе алгебраического криптоанализа	Баспа	Вестник КазНУТУ. – Алматы. – 2020. – № 5. – С. 620-629.	10	Дюсенбаев Д.С., Алгазы К.Т.	
10	The algorithm of block encryption «Al03» and the results of its analysis	Баспа	Bulletin of KazNPU. Series of Physics & Mathematical Sciences. – Almaty. – 2021. – No. 3(75). – pp. 108-114.	7	Kapalova N., Algazy K., Dyussenbayev D.	
11	Requirements for symmetric block encryption algorithms developed for software and hardware implementation	Баспа	Journal «KazNU Bulletin. Series Mathematics, Mechanics and Computer Science». – Almaty. – 2021. – No. 4(112). – pp. 134-147.	14	Kapalova N, Haumen A., Suleimenov O.	
12	Модификация алгоритма шифрования «Al01»	Баспа	Журнал «Вестник Алматинского университета энергетики и связи». – Алматы. – 2022. – № 1. – С. 162-70.	9	Алгазы К.Т., Капалова Н.А., Хомпыш А.	
13	CF блоқты шифрлау алгоритмі және оны биттік шашырау эффектіне зерттеу	Баспа	Вестник Евразийского национального университета имени Л.Н. Гумилева. Серия Математика. Информатика. Механика, 2022, Т. 138, № 1, С. 6-22.	15	С.Е.Нысанбаева, К.Т.Алгазы, А.Хомпыш, Д.С.Дуйсенбаев.	
14	Study of the cryptographic strength of the S-box obtained on the basis of exponentiation modulo	Баспа	Scientific Journal of Astana IT University, Vol. 12. - 2022. Doi: 10.37943/12DZLQ4553.	8	Khompysh A., Kapalova T., Algazy K.	
Ізденуші Ғалым хатшы					Қ.С. Сақан О.А. Усатова	

15	Жаңа 4 биттік S-блок алу әдісі және алынған S-блоқты катал лавиндік критерийі бойынша зерттеу	Баспа	Университет еңбектері ҚарТУ – Қарағанды, 2022. – № 4(89). – 411-417 б.	7	Хомпыш А., Капалова Н.А., Дюсенбаев Д.С., Алғазы К.Т.	
16	Криптографиялық хеш алгоритмдер жасаудың әртүрлі жолдарын қарастыру	Баспа	Материалы V международной научно- практической конференции «Информатика и прикладная математика», 29 сентября – 01 октября 2020. – Алматы. – С. 374- 378.	5	Алғазы К.Т.	
17	Принципы построения блочных шифров и требования к ним //	Баспа	Материалы V международной научно- практической конференции «Информатика и прикладная математика», 29 сентября – 01 октября 2020. – Алматы. – С. 378- 384.	7	Алғазы К.Т.	
18	Cryptographic attack to encryption algorithm “AL01” by the boomerang method	Баспа	Advanced technologies and computer science. – Almaty. – 2020. – No 2. – Pp. 21-25.	5	К.Т.Алғазы	
19	Симметриялы шифрларда қолданылатын сызықты емес түйіндерді зерттеу	Баспа	Материалы международной научно- практической конференции «Актуальные проблемы информационной безопасности в Казахстане». – Алматы. 11 июня 2021 г., – С. 34-38.	5	Д.С.Дюсенбаев, К.Т.Алғазы.	
20	Хештеу алгоритмдерін жасаудағы блокты шифрлау алгоритмдерін қолдану ерекшеліктері	Баспа	Материалы VI международной научно- практической конференции «Информатика и прикладная математика», 29 сентября – 02 октября 2021. – Алматы. – С. 406- 410.	5	С.Нысанбаева	
Ізденуші Ғалым хатшы					Қ.С. Сақан О.А. Усатова	

21	НАS03 хеш алгоритмін құру және зерттеу	Баспа	Материалы международной научной конференции в области информационных технологий, посвященной 75-летию профессора У.А. Тукеева. – Алматы. 08 октября 2021 г., – С. 55-61.	7	К.Алгазы, Н.Капалова, Д.Дюсенбаев.
22	Разработка и анализ алгоритма хеширования «НАS01»	Баспа	Сборник статей IV международной научно-технической конференции «Минские научные чтения-2021». – Минск. 09 декабря 2021 г. – Т. 3. – С. 181-187.	7	Д.С. Дюсенбаев, К.Т. Алгазы, О.А. Лизунов, А. Хомпыш
23	Investigation of the stastical security of a pseudo-random sequence generator //	Баспа	International Conference “Computer Data Analysis and Modeling: Stochastics & data Science” (CDAM-2022). – Minsk. September 06-10, 2022, Pp. 137-144.	8	S.E. Nysanbayeva, N.A. Kapalova, D.S. Dyusenbayev, K.T. Algazy.
24	Исследование свойств хеширования «НВС-256»	Баспа	Материалы VII международной научно-практической конференции «Информатика и прикладная математика», 20 октября – 21 октября 2022. – Алматы. – С. 362–373.	12	Ищукова Е.А., Маро Е.А., Бабенко Л.К., Алгазы К.Т.
25	«НВС-256» хештеу алгоритміндегі S-блоктардың дифференциалды криптоталдаудағы критикалық нүктелерін зерттеу	Баспа	Advanced technologies and computer science. – Almaty. – 2022. – No. 4. – Pp. 15-24.	10	С. Нысанбаева
26	Ақпаратты хештеу бағдарламасы «ISL_HASH 1.0»		Авторлық куәлік № 20661. жариял. 2021 жылғы 05 қазан. – 1 б.		Варенников А.В., Нысанбаева С.Е., Капалова Н.А., Дюсенбаев Д.С., Лизунов О.А.
27	Ақпаратты хештеу бағдарламасы «CSP_HASH 1.0»		Авторлық куәлік № 23886. жариял. 2022 жылғы 24 ақпан. – 1 б.		Лизунов О.А., Нысанбаева С.Е., Капалова Н.А., Дюсенбаев Д.С., Варенников А.В.
Изденуші Ғалым хатшы					 Қ.С. Сакан О.А. Усатова

28	ЭВМ-ге арналған бағдарлама «Криптопровайдер ISL_CSP 1.0»		Авторлық куәлік № 29379. жариял. 2022 жылғы 12 қазан. – 1 б.		Варенников А.В., Капалова Н.А., Алғазы К.Т., Дюсенбаев Д.С., Лизунов О.А.
29	Ақпаратты хештеу алгоритмі «НВС-256»		Авторлық куәлік № 20318. жариял. 2021 жылғы 20 қыркүйек. – 1 б.		Нысанбаева С.Е.
Изденуші Ғалым хатшы					Қ.С. Сақан О.А. Усатова

