ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2025»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2025»

PROCEEDINGS
of the XX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2025»

2025
Астана

УДК 001(06)
ББК 72я631
F96

«ǴYLYM JÁNE BILIM – 2025» студенттер мен жас ғалымдардың XX Халықаралық ғылыми конференциясы = XX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2025» = The XX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2025». – Астана: – 3813 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-08-5373-7

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.В сборник вошли доклады студентов, магистрантов, докторантов имолодыхученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001(06)
ББК 72я431
F96

ISBN 978-601-08-5373-7

Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2025

СЕКЦИЯ 2

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ И КОММ УНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Подсекция 2.2

Интеллектуальные информационные системы

255.	Сафонова Софья Александровна «Современные аспекты информационной безопасности в облачных вычислениях: модели, угрозы и методы защиты»	1034
256.	Смаилова Назгүл Батырбекқызы «Терең оқыту арқылы кітап ұсыныстарын әзірлеу: collaborative filtering, content-based және nlp әдістерінің комбинациясы»	1041
257.	Тажібай Аружан Айдосқызы, Кудубаева Сауле Альжановна «Көру қабілеті әлсіз адамдарға арналған аі дауыстық көмекші: нақты уақытта объектілерді анықтау және қашықтықты бағалау»	1046
258.	Тайжанов Азамат Жанкелдіұлы «Python тілінде фильмдердің интеллектуалды ұсыныс жүйесін әзірлеу»	1051
259.	Умирзахов Сундетали Кабылбекович «Сұраныстарды интеллектуалды талдау негізінде ұйымның сайты үшін чат-бот құру»	1055
260.	Шайхстан Марғұлан «IOT Сенсорлары негізінде ауа ластану деңгейін болжау»	1060

Подсекция 2.3

Современные тенденции в программной инженерии и управлении в условиях цифровой индустрии

261.	Bekenova A.B. «Development of a registration panel for users and doctors with integration into the database»	1077
262.	Bolat A.Zh. «Data analysis methods and decision making using big data and machine learning tools»	1081
263.	Алтайұлы А. «Visual studio интегралды ортасында «қойма қызметкерлеріне арналған» мәліметтер қорын жобалау»	1086
264.	Арап А.Қ. «Ақылды сурет салушы роботты әзірлеу»	1088
265.	Артыкбекқызы А. «Ақылды үйлердегі заттар интернеті(iot) мен робототехниканың өзара әрекеттесуі»	1091
266.	Ахметова А.Д. «Тоңазытқыштағы өнімдерді бақылауға және тағам әзірлеу ұсынысын беруге арналған программалық қосымша»	1096
267.	Дәрібай Д.Д. «Робототехниканы қолдану арқылы қойма логистикасындағы қолданыстағы басқару жүйелерін талдау»	1100
268.	Жамбулов С.Ж. «Білім алушыларды информатика және программалау олимпиадаларына дайындауда жасанды интеллекттің қолданысы»	1102
269.	Каиржан Р.С. «Development of system for recognition of emotional states of employees based on computer vision methods on Raspberry Pi»	1108
270.	Кайрекенова Н.Р. «Өнеркәсіптік роботты көру үшін машиналық оқытудың заманауи тәсілдері: әдістер, деректер жиынтығы және оптимизациялау»	1111

СЕКЦИЯ 3
ЕСТЕСТВЕННЫЕ НАУКИ

3. Menezes A. J., van Oorschot P. C., & Vanstone, S. A. (2021). *Handbook of applied cryptography*. CRC Press.
4. Paar C., Pelzl J. (2010). *Understanding cryptography: A textbook for students and practitioners*. Springer. https://doi.org/10.1007/978-3-642-04101-3
5. Kurose J. F., Ross K. W. (2002). *Computer networking: A top-down approach* (2nd ed.). Addison-Wesley.
6. Rivest R. L., Shamir A., Adleman L. (2022). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126.
7. Sangeetha Supriya K., Jeno Lovesum S. P. (2024). Review on lightweight cryptography techniques and steganography techniques for IoT environment. *International Journal of Advanced Intelligence Paradigms*, 17(3), 1-18. https://doi.org/10.1007/s13198-024-02476-8
8. Shamir A. (2020). How to share a secret. *Communications of the ACM*, 22(11), 612–613.
9. Tanenbaum A. S. (2005). *Computer networks* (4th ed.). Piter.
10. Zhu R. (2023). Information security and privacy protection based on intelligent encryption and cryptography. *Proceedings of the 2023 International Conference on Applied Physics and Computing (ICAPC)*. https://doi.org/10.1109/ICAPC.2023.1234567.
11. Smith J., Brown K. (2022). Exploring encryption: Symmetric and asymmetric cryptography. *Journal of Information Security Studies*, 15(3), 45–56. https://doi.org/10.1234/joiss.2022.00345
12. Schneier B. (2020). *Applied cryptography: Protocols, algorithms, and source code in C*. Wiley.
13. Goldwasser S., Micali S. (2021). Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2), 270–299.
Biham E., Shamir A. (2021). Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1), 3–72.

УДК 004.056.5

VISUALVM КӨМЕГІМЕН CAST-128 ЖӘНЕ KUZNYECHIK БЛОКТЫҚ ШИФРЛАРЫНЫҢ КІЛТ ГЕНЕРАЦИЯСЫН САЛЫСТЫРУ ЖӘНЕ СТАНДАРТТАРҒА ШОЛУ.

Айдарова Айдана Айдарқызы
aidarovaaidana02@gmail.com
Л.Н.Гумилев атындағы ЕҰУ «Ақпараттық технологиялар» факультетінің 2-курс магистранты, Астана, Қазақстан
Ғылыми жетекшісі – Ж.Сауханова

Криптография саласында блоктық шифрлар деректердің құпиялылығы мен тұтастығын қамтамасыз етуде шешуші рөл атқарады. Бұл мақалада екі маңызды блоктық Шифр қарастырылған: ISO/IEC 18033-3 стандартында көрсетілген CAST-128 және ГОСТ Р 34.12-2015 стандартына кіретін Kuznechik. Сонымен қатар, ол осы криптографиялық алгоритмдердің кілт генерациясын Java-да іске асырылуын талдау үшін VisualVM - құралын қолдануды талқылайды. Мақаланың мақсаты-осы блоктық шифрлардың техникалық аспектілерін, олардың ұқсастықтары мен айырмашылықтарын және VisualVM олардың Java тілінде жазылған кодтарының өнімділігін оңтайландыруға қалай көмектесетінін зерттеу.

CAST-128 техникалық сипаттамасы (ISO/IEC 18033-3)

CAST - 128-1996 жылы Карлайл Адамс пен Стаффорд Таварес жасаған симметриялы блок шифры. Бұл ISO/IEC 18033-3 блоктық шифрлау алгоритмдері стандартының бөлігі. Негізгі функциялар: бекітілген 64 биттік блок өлшемі, айнымалы 40-128 биттік кілт өлшемі, шифрлау кезеңдері – 80 битке дейінгі кілттер үшін 12, одан ұзын кілттер үшін 16 кезең. CAST-128 блоктық шифр Фейстель желісін пайдаланады, онда шифрлау процесі ашық мәтінді екіге бөлуді және round функцияны қайталап қолдануды қамтиды. CAST-128-дегі әр раундтың жалпы формуласы келесідей:

Шифрлау процесі:

1. Ашық мәтін екі 32 биттік бөлікке бөлінеді: $P = L_0 \,||\, R_0$

2. Әрбір i раунд үшін (мұндағы i=1,2,...,R және R=12 немесе 16):

Li=Ri−1; $R_i = L_{i-1} \oplus f(R_{i-1}, Km_i, Kr_i)$

3. Шифрлық мәтін соңғы блоктарды ауыстыру арқылы жасалады: $C = R_{16} \,||\, L_{16}$

Раунд функциясы: CAST-128 раунд нөміріне байланысты үш түрлі раунд функциясын қолданады:

- 1 түрі (раунд 1, 4, 7, 10, 13, 16):

$I = ((Km_i + D) <<< Kr_i)$;

$f = ((S1[Ia] \oplus S2[Ib]) - S3[Ic]) + S4[Id]$

- 2 түрі (раунд 2, 5, 8, 11, 14):

$I = ((Km_i \oplus D) <<< Kr_i)$;

$f = ((S1[Ia] - S2[Ib]) + S3[Ic]) \oplus S4[Id]$

- 3 түрі (раунд 3, 6, 9, 12, 15):

$I = ((Km_i - D) <<< Kr_i)$;

$f = ((S1[Ia] + S2[Ib]) \oplus S3[Ic]) - S4[Id]$

Кілттер кестесі. CAST-128 әр раунд үшін бірнеше кіші бөлімді пайдаланады:

- Km_i - 32 биттік "жасыру" ("masking") кілті ретінде қолданылады
- 5 биттік Kri "айналмалы" ("rotation") кілт ретінде қолданылады

Кілттерді құру схемасы S5, S6, S7 және S8 S -блоктарын, күрделі операциялар тізбегін қолдана отырып, 128 биттік негізгі кілттен 32 ішкі кілттерді (K_1 -ден K_{32} -ге дейін) жасайды. Алғашқы 16 ішкі кілттер (K_1-ден K_{16}) маскировка ретінде қолданылатын кілттер (Km_1 -ден Km_{16}), ал келесі 16 ішкі кілттер (K_{17}-ден K_{32}) айналу кілттері ретінде қолданылады (Kr_1 -ден Kr_{16}).

Шифрды дешифрлау процесінде шифрлау қадамдары кері тәртіпте бірдей round функциясын қолдану арқылы кері тәртіпте орындалады.

ГОСТ Р 34.12-2015 блоктық шифр: Kuznechik-ке шолу

Kuznechik-2015 жылы ГОСТ Р 34.12-2015 Ресей Федералдық стандарты аясында ұсынылған заманауи симметриялы блоктық шифр. Оны "ИнфоТеКС" АҚ қатысуымен Ресей Федерациясының Федералды қауіпсіздік қызметінің ақпаратты қорғау және арнайы байланыс орталығы әзірледі.

Kuznechik - орнына қою-ауыстыру (Substitution-Permutation Network (SPN)) желілік шифры. Әр раунд үш негізгі кезеңнен тұрады: кілт қосу, сызықтық емес алмастыру және сызықтық түрлендіру. Kuznechik он алты 8 биттік байт ретінде ұсынылған 128 биттік күйді пайдаланады. Шифрлау процесі мыналардан тұрады:

1. Бастапқы кілтті немесе бірінші раунд кілтін ашық мәтінмен XOR операциясынан өткізу.
2. Түрлендірудің 9 раунды: әр раундта үш операция қолданылады:

• S: S блоктарын қолдана отырып, сызықтық емес алмастыру. Ауыстыру деңгейі күйдің әрбір байтына бекітілген биективті S-тәрізді π блогын қолданады:

$S(a) = S(a_{15}||...||a_0) = \pi(a_{15})||...||\pi(a_0)$

• L: сызықтық түрлендіру. L сызықтық түрлендіру R функциясының 16 дәйекті қолданылуынан тұрады: $L(a) = R^{16}(a)$

R функциясы келесідей анықталады: $R(a_{15}||...||a_0) = \ell(a_{15},...,a_0)||a_{15}||...||a_1$

L сызықтық функциясы нақты коэффициенттері бар $GF(2^8)$ Галуа өрісінде көбейтуді орындайды: $\ell(a_{15},..,a_0) = 148 \bullet a_{15} + 32 \bullet a_{14} + 133 \bullet a_{13} + ... + 148 \bullet a_1 + 1 \bullet a_0$

• Кілтті қосу: раунд кілттін пайдаланып XOR. Кілт кестесі фейстель тәрізді құрылымды қолдана отырып, 256 биттік k негізгі кілтінен он 128 биттік раунд кілттерді (K_1-дан K_{10}-ға дейін) жасайды:

1. Алғашқы екі раунд кілттері тікелей негізгі кілттен алынған:

$K_1 = k_{255}||...||k_{128}$ $K_2 = k_{127}||...||k_0$

2. Кейінгі кілттер Итерация тұрақтылары бар Фейстель желісінің көмегімен жасалады: $(K_{2i+1}, K_{2i+2}) = F[C_{8i}]...F[C_{8i-7}](K_{2i-1}, K_{2i})$

мұндағы i = 1,2,3,4 және C1,...,C32-ретінде анықталған итерация тұрақтылары:

$C_i = L(Vec_{128}(i))$

3. Кілтті соңғы қосу: онынші раунд кілттін пайдаланып XOR

Шифрлау процесі:

$E\_K_1,...,K_{10}(a) = X[K_{10}]LSX[K_9]...LSX[K_2]LSX[K_1](a)$

Декодтау процесінде кері операциялар кері тәртіпте қолданылады:

$D\_K_1,...,K_{10}(a) = X[K_1]S^{-1}L^{-1}X[K_2]...S^{-1}L^{-1}X[K_9]S^{-1}L^{-1}X[K_{10}](a)$

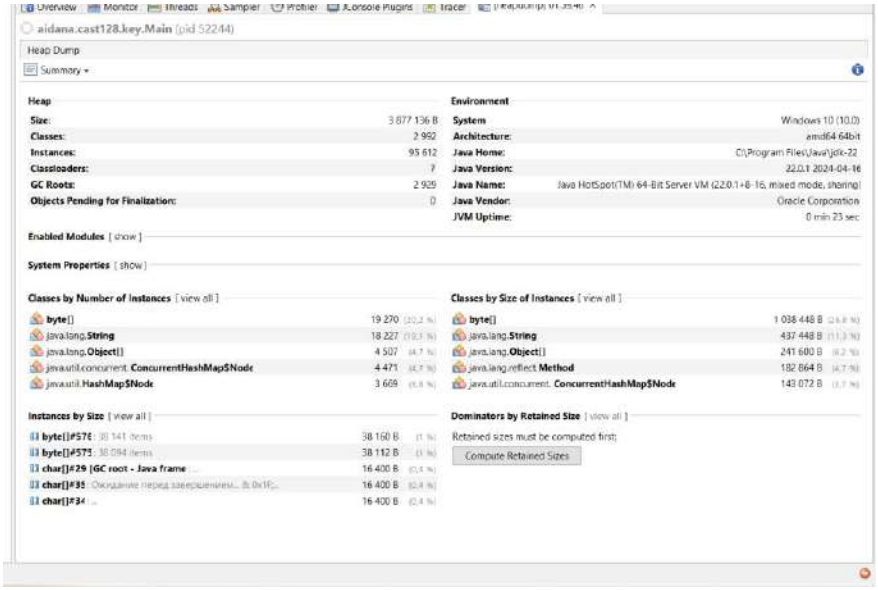
Екі блоктық шифрлардың алгоритімдеріне шолу жүргізу арқылы келесі ерекшеліктер алынды:

Ерекшеліктер	**CAST-128**	**Kuznyechik**
Блок өлшемі	64 бит	128 бит
Кілттің өлшемі	өзгереді (40-128 бит)	бекітілген (256 бит)
Шифрлау раундтарының саны	раундтар саны - 12-16	раундтар саны - 10
Құрылымы	Фейстель желісінің	Substitution-Permutation Network (SPN)
S-box дизайны	бірнеше раундқа тәуелді S-блоктары	қауіпсіздікті қамтамасыз ету үшін оңтайландырылған бір бекітілген S-блоктары

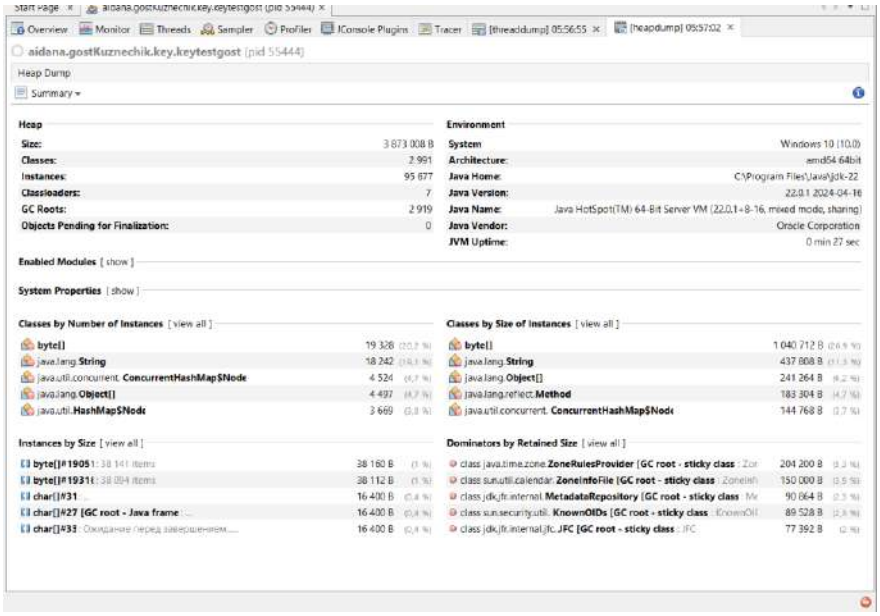
Кесте 1. CAST-128 және Kuznyechik блоктық шифрларының блок өлшемі, кілттің өлшемі, шифрлау раундтарының саны, құрылымы, S-box дизайны бойынша салыстырмалы сипаттамасы.

VisualVM көмегімен блоктық шифрлауды жүзеге асыруды талдау

VisualVM-Java программаларын бақылауға, ақаулықтарды жоюға және оңтайландыруға арналған қуатты, жан-жақты құрал. Бірнеше JDK пәрмен жолы құралдарын бір графикалық интерфейске біріктіру арқылы VisualVM әзірлеушілерге программа өнімділігін талдаудың, қиындықтарды анықтаудың және жұмыс уақытында ақауларды жоюдың интуитивті түсінікті құралы болып келеді.



Сурет 1. CAST-128 кілт генерациясының VisualVM программасындағы көрінісі.



Сурет 2. Kuznechik кілт генерациясының VisualVM программасындағы көрінісі.

VisualVM көмегімен CAST-128 және Kuznechik Кілттерін генерациялау алгоритмдерін салыстыру нәтижесі алынды. Екі алгоритмде де кілттерді генерациялау функциялары қолданылады, бірақ олардың дизайн философиясы, ресурстарды пайдалану және криптографиялық күшті жақтары айтарлықтай ерекшеленеді. Төменде VisualVM көмегімен жүргізілген талдаулар негізінде егжей-тегжейлі салыстыру берілген.

Аспектілері	CAST-128 кілт генерациясы	Kuznechik кілт генерациясы
Алгоритм түрі	Фейстель құрылымы бар жеңіл блоктық шифр.	SPN құрылымы бар заманауи блок шифры.

Аспектілері	CAST-128 кілт генерациясы	Kuznechik кілт генерациясы
Жадты пайдалану	Тиімді үйін көлемі ~12 МБ, онда byte[] және String нысандары басым	byte [] нысандары басым және жадтың жүктемесі сәл жоғары (~13 МБ үйін).
CPU қолданылуы	Процессордың жүктелуі минималды (~0,0%), бұл операциялардың жеңілдетілгенін көрсетеді (1-сурет).	Процессордың төмен жүктемесі (~40%), бұл операциялардағы үлкен есептеу жүктемесін көрсетеді (2-сурет).
Ағын белсенділігі	13 белсенді ағын мен тұрақты ағын әрекеті; ағынның минималды уақыты (~43 мс).	Тұрақты жұмыс уақыты бар тұрақты ағын әрекеті (~50 мс).
Қоқыс жинау	кілттерді жоспарлау кезінде жадының тиімді басқарылуын, қоқыс жинаудың минималды белсенділігінен көреміз.	үздіксіз орындалудың қамтамасыз етілгенін, деректерді жинау белсенділігінің аздығынан көрінеді.
Кілт генирациясының күрделілігі	Модульдік арифметика мен биттік амалдарды қолданатын салыстырмалы түрдегі қарапайым кілт генирациясы.	Бірнеше S-блоктарын, сызықтық түрлендірулерді және модульдік математиканы қамтитын күрделі кілт генирациясы.
Криптотөзімділік	Ескірген жүйелер үшін жеткілікті, бірақ блоктың кішірек өлшеміне байланысты қазіргі стандарттар бойынша төмен (64 бит).	Блоктың үлкендігі(128 бит) және заманауи дизайн принциптері болғандықтан қауіпсіздігі жоғары

Кесте 2. CAST-128 және Kuznechik кілт генерациясын VisualVM программасы арқылы келесі аспектілерді салыстыру кестесі: алгоритм түрі, жадты пайдалану, CPU қолданылуы, ағын белсенділігі, қоқыс жинау, кілт генирациясының күрделілігі, криптотөзімділік.

Қорытынды

Бұл зерттеу криптографиялық дизайнның өнімділік пен қауіпсіздікке қалай әсер ететінін көрсетеді. Feistel құрылымы бар CAST-128 процессорды (~0%) және жадты (~12 МБ үйінді) аз пайдаланудың арқасында ескірген жүйелер үшін тиімді, бірақ оның 64 биттік блок өлшемі мен айнымалы кілт ұзындығы заманауи шабуылдарға төзімділікті шектейді. Kuznechik (ГОСТ Р 34.12-2015), оның SPN құрылымы, 128 биттік блоктары және 256 биттік кілттері бар, қауіпсіздіктің жоғары деңгейін қамтамасыз етеді, бірақ есептеу шығындарын (процессор ресурстарының~40%) және жадты көбірек пайдалануды (~13 МБ үйінді) қажет етеді. Visualvm профилі cast-128-дің төмен қауіпті тапсырмаларға жарамдылығын және kuznechik-тің жоғары

қауіпсіздік қосымшаларына сенімділігін көрсете отырып, осыиссаларды растайды. Болашақта kuznechik өнімділігін оңтайландыру үшін гибридті іске асыруды немесе аппараттық жеделдетуді зерттеуге болады.

Қолданылған әдебиеттер тізімі

1. RFC 2144: The CAST-128 Encryption Algorithm // Internet Engineering Task Force (IETF). – 1997. – URL: https://www.rfc-editor.org/rfc/rfc2144.txt.
2. RFC 7801: GOST R 34.12-2015 Block Cipher "Kuznyechik" // Internet Engineering Task Force (IETF). – 2016. – URL: https://www.rfc-editor.org/rfc/rfc7801.html.
3. ISO/IEC 18033-3 Standard: Information Technology – Security Techniques – Encryption Algorithms – Part 3: Block Ciphers // International Organization for Standardization (ISO). – Geneva, 2005.
4. Comparative Study of AES, Blowfish, CAST-128 and DES Encryption Algorithm // IOSR Journal of Engineering, Vol.6 Issue6, June 2016. – URL: https://www.iosrjen.org/Papers/vol6_issue6%20(part-1)/A066010107.pdf (дата обращения: 30.03.2025).
5. Profiling JVM Applications Remotely Using VisualVM // ITNEXT, June 2024. – URL: https://itnext.io/profiling-jvm-applications-remotely-using-visualvm-c0df9816aabf (дата обращения: 30.03.2025).

ӘӨЖ 004.056.5

ЖЕРГІЛІКТІ ЖЕЛІНІҢ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТЕТІН НЕГІЗГІ ПАРАМЕТРЛЕР

Акимбекова Дильназ Маратовна, Каиржанова Дильназ Жалғасқызы
akimbekovadilnaz@mail.ru, *dikairzhanova@gmail.com*
Л. Н. Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультеті Ақпараттық қауіпсіздік жүйесі кафедрасының 3 курс студенттері, Астана, Қазақстан
Ғылыми жетекші – Казиева Назым Магидулловна

Қазіргі заманғы желілер кибершабуылдарға жиі ұшырайды, олардың ішінде рұқсатсыз қол жеткізу, «қызмет көрсетуден бас тарту» (DoS/DDoS) шабуылдары және деректерді ұстап қалу сияқты қауіптер бар. Желілік құрылғылардың қауіпсіздігін қамтамасыз ету ақпаратты қорғаудың және ықтимал шабуылдардың алдын алудың негізгі шараларының бірі болып табылады.

Үйлердегі немесе үй желілеріндегі жергілікті желілерге (LAN) ерекше назар аударған жөн. Үй желілері – бұл жергілікті желілердің бір түрі; олар интернетке қосылған құрылғылардың кең және алуан түрін қамтуы мүмкін және оларды басқару оңай, сенімді және қауіпсіз болуы керек, әсіресе олардың иелері көбінесе техникалық дағдылары жоқ пайдаланушылар болғандықтан [1].

Көптеген жылдар бұрын үй желісі сымсыз желіге қосылған бірнеше ноутбуктан тұрған. Бүгінгі таңда оған смартфондар, сымсыз принтерлер, термостаттар, дыбыс датчиктері, түтін датчиктері, шамдар, камералар, теледидарлар, аудио жүйелері, ақылды динамиктер, тоңазытқыштар және тағы басқалар кіруі мүмкін. "Заттар интернеті" (IoT, Internet of Things) деп аталатын интернетке үйлесімді құрылғылардың көбеюі кез-келген электрониканы, соның ішінде әртүрлі сенсорларды желіге қосуға мүмкіндік береді. Қосылған құрылғылардың бұл