ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ
АКАДЕМИЯСЫ» РҚБ

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ» РҚБ

ХАБАРЛАРЫ

ИЗВЕСТИЯ

РОО «НАЦИОНАЛЬНОЙ
АКАДЕМИИ НАУК РЕСПУБЛИКИ
КАЗАХСТАН»

N E W S

OF THE NATIONAL ACADEMY OF
SCIENCES OF THE REPUBLIC OF
KAZAKHSTAN

SERIES OF PHYSICS AND MATHEMATICS

2 (354)

APRIL – JUNE 2025

PUBLISHED SINCE JANUARY 1963
PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

News of the National Academy of Sciences of the Republic of Kazakhstan.
Series of Physics and Mathematics
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Owner: RPA «National Academy of Sciences of the Republic of Kazakhstan» (Almaty).
Certificate **No. KZ20VPY00113741** on the re-registration of the periodical printed and online publication of the information agency, issued on **28.02.2025** by the Republican State Institution «Information Committee» of the Ministry of Culture and Information of the Republic of Kazakhstan
Subject area*: information and communication technologies.*
Currently: *included in the list of journals recommended by the CCSES MSHE RK in the direction of «Information and communication technologies».*
Periodicity: *4 times a year.*
Editorial address: *28, Shevchenko str., of. 219, Almaty, 050010, tel. 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

«ҚР ҰҒА Хабарлары. Физика-математика сериясы».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Меншіктеуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» РҚБ (Алматы).

Ақпарат агенттігінің мерзімді баспасөз басылымын, ақпарат агенттігін және желілік басылымды қайта есепке қою туралы ҚР Мәдениет және Ақпарат министрлігі «Ақпарат комитеті» Республикалық мемлекеттік мекемесі **28.02.2025** ж. берген **№KZ20VPY00113741** Куәлік.

Тақырыптық бағыты: *ақпараттық-коммуникациялық технологиялар*

Қазіргі уақытта: *«ақпараттық-коммуникациялық технологиялар» бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*

Мерзімділігі: *жылына 4 рет.*

Редакцияның мекен-жайы: *050010, Алматы қ., Шевченко көш., 28, 219 бөл., тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

«Известия НАН РК. Серия физико-математическая».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Собственник: *Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы).*

Свидетельство о постановке на переучет периодического печатного издания, информационного агентства и сетевого издания **№ KZ20VPY00113741.** Дата выдачи **28.02.2025**

Тематическая направленность: *информационно-коммуникационные технологии.*

В настоящее время: *вошел в список журналов, рекомендованных КОКСНВО МНВО РК по направлению «информационно-коммуникационные технологии».*

Периодичность: *4 раза в год.*

Адрес редакции: *050010, г. Алматы, ул. Шевченко, 28, оф. 219, тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

CONTENTS

INFORMATION AND COMMUNICATION TECHNOLOGIES

МАЗМҰНЫ

АҚПАРАТТЫҚ-КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР

СОДЕРЖАНИЕ

ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

NEWS OF THE NATIONAL ACADEMY OF SCIENCESOF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 2. Namber 354 (2025). 107–124

https://doi.org/10.32014/2025.2518-1726.347

ӘОЖ 004.056.2

© M. Ilesbay[1*0], A. Tynymbayev[2], S. Mambetov[2], A. Barakova[3], O. Joldasbayev[4], 2025.

[1]Al-Farabi Kazakh National University, Almaty, Kazakhstan;
[2] Turan University, Almaty, Kazakhstan;
[3] Asfendiyarov Kazakh National Medical University, Almaty, Kazakhstan;
[4] Branch of the Academy of Public Administration under the president of the Republic of Kazakhstan in Almaty region, Konayev, Kazakhstan.
E-mail: milesbaj@gmail.com

INTEGRATED METHOD OF INFORMATION PROTECTION BASED ON DATA COMPRESSION, ENCRYPTION AND SEPARATION

Meirambek Ilesbay — 2nd year Master's student, Department of Cybersecurity and Cryptology, Al-Farabi Kazakh National University, Almaty, Kazakhstan,
E-mail: milesbaj@gmail.com, ORCID: https://orcid.org/0009-0006-4893-1156;
Abilkaiyr Tynymbayev — Master, Senior Lecturer of the Higher School of Information Technology, Turan University, Almaty, Kazakhstan,
E-mail: a.tynymbayev@turan-edu.kz, ORCID: https://orcid. org/0009-0006-3723-3723;
Saken Mambetov—Master of Technical Sciences, Director of the Higher School of Information Technology, Turan University, Almaty, Kazakhstan,
E-mail: s.mambetov@turan-edu.kz; ORCID: https://orcid.org/0000-0002-7249-5378;
Aliya Barakova — Assistant Professor of the Department of Engineering Disciplines and Good Practices, Asfendiyarov Kazakh National Medical University, Almaty, Kazakhstan,
E-mail: balia_79@mail.ru, ORCID: https://orcid.org/0000-0002-0904-745X;
Orynbassar Joldasbayev — PhD in Project Management, Senior Lecturer of the branch of the Academy of Public Administration under the president of the Republic of Kazakhstan in Almaty region, Konayev, Kazakhstan,
E-mail: orynbassarjoldasbayev@gmail.com, ORCID: http://orcid. org/0000-0003-0991-1575.

Abstract. This article presents an innovative method to enhance information security by combining data compression, encryption, and partitioning algorithms. As cyber threats grow more sophisticated, traditional encryption alone is often insufficient. The proposed three-stage model includes: (1) compressing data to reduce redundancy and size, (2) encrypting it with modern cryptographic techniques like AES or ChaCha20, and (3) fragmenting the encrypted data into separate parts stored across distributed systems. This approach increases cryptographic strength and minimizes the impact of a single storage breach, as individual fragments are useless without all parts and the decryption key. The method improves scalability

and adaptability, making it ideal for dynamic and complex environments where data is frequently updated, transmitted, or migrated. It integrates well with cloud and hybrid storage systems and optimizes storage efficiency by compressing data before encryption. Experimental results show a 94–98% reduction in successful attack probability compared to encryption-only methods, with manageable computational overhead and resource usage. Additionally, the approach supports real-time data pipelines and is compatible with existing software libraries and security protocols. Its modular and flexible design allows for future enhancements without overhauling the entire system. Overall, this method offers a resilient, efficient, and scalable solution for secure data processing in environments requiring high levels of confidentiality, integrity, and availability.

Key words: information security; data encryption; data compression; secret sharing; cryptographic resilience; distributed storage.

© М.А. Ілесбай [1*0], Ә.Б. Тынымбаев[2], С.Т. Мамбетов[2], А.Ш. Баракова[3], О.К. Джолдасбаев[4], 2025.

[1]Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы Қазақстан;
[2]«Тұран» университеті, Алматы Қазақстан;
[3] С.Ж. Асфендияров атындағы Қазақ ұлттық медицина университеті, Алматы, Қазақстан;
[4] ҚР Президентінің жанындағы мемлекеттік басқару академиясы, Алматы облысы бойынша филиалы, Қонаев, Қазақстан.
E-mail: milesbaj@gmail.com

ДЕРЕКТЕРДІ СЫҒУ, ШИФРЛАУ ЖӘНЕ БӨЛУ НЕГІЗІНДЕ АҚПАРАТТЫ ҚОРҒАУДЫҢ БІРІКТІРІЛГЕН ӘДІСІ

Ілесбай Мейрамбек Азаматұлы — 2-курс магистранты, «Киберқауіпсіздік және криптология» кафедрасы, әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан, E-mail: milesbaj@gmail.com, ORCID: https://orcid.org/0009-0006-4893-1156;
Тынымбаев Әбілқайыр Бақтыгерейұлы — магистр, сениор-лектор, Ақпараттық технологиялар жоғары мектебі, Тұран университеті, Алматы, Қазақстан,
E-mail: a.tynymbayev@turan-edu.kz, ORCID: https://orcid.org/0009-0006-3723-3723;
Мамбетов Сәкен Төлегенұлы – магистр, Ақпараттық технологиялар жоғары мектебі директоры, Тұран университеті, Алматы, Қазақстан,
E-mail: s.mambetov@turan-edu.kz, ORCID ID: https://orcid.org/0000-0002-7249-5378;
Баракова Алия Шаризатовна — «Инженерлік пәндер және тиісті практикалар» кафедрасының профессор ассистенті, С.Ж.Асфендияров атындағы Қазақ ұлттық медицина университеті, Алматы, Қазақстан,
E-mail: balia_79@mail.ru, ORCID: https://orcid.org/0000-0002-0904-745X;
Джолдасбаев Орынбасар Капарович — PhD, аға оқытушы, ҚР Президентінің жанындағы мемлекеттік басқару академиясы Алматы облысы бойынша филиалы, Қонаев, Қазақстан, E-mail: orynbassarjoldasbayev@gmail.com, ORCID: http://orcid.org/0000-0003-0991-1575.

Аннотация. Бұл мақалада ақпараттық қауіпсіздікті арттыруға бағытталған инновациялық әдіс ұсынылады. Ол деректерді қысу (сығымдау), шифрлау және бөлшектеу алгоритмдерін біріктіріп қолдануға негізделген. Қазіргі

таңда киберқауіптер қарқынды дамып, күрделене түсуде. Мұндай жағдайда дәстүрлі шифрлау әдістері күрделі шабуылдарға қарсы жеткілікті деңгейде қорғаныс қамтамасыз ете алмайды. Осыны ескере отырып, авторлар үш кезеңнен тұратын өңдеу моделін ұсынады: (1) деректерді бастапқыда қысу арқылы оның көлемін азайту және артық ақпаратты жою, (2) AES немесе ChaCha20 сияқты заманауи криптографиялық әдістермен шифрлау арқылы деректердің құпиялығын қамтамасыз ету, (3) шифрланған деректерді тәуелсіз фрагменттерге (бөліктерге) бөліп, оларды әртүрлі таратылған сақтау жүйелеріне орналастыру. Бұл тәсіл ақпаратты қорғауда қосымша күрделілік енгізіп, шабуылдаушылардың әрекетін айтарлықтай қиындатады. Егер бір торап бұзылса да, барлық фрагменттер мен шифрлау кілті болмаған жағдайда мәліметтерді қалпына келтіру мүмкін емес. Жүйе икемді, масштабталатын және бұлтты немесе гибридті платформалармен үйлесімді жұмыс істейді. Сонымен қатар, бұл әдіс деректерді алдын ала қысу арқылы сақтау орнын үнемдейді және нақты уақыт режимінде жұмыс істеуге бейімделген. Эксперименттік бағалаулар бұл әдістің шабуылдарға қарсы төзімділікті 94–98% арттыратынын және есептеу шығындарының төмен деңгейде сақталатынын көрсетті. Жүйе қолданыстағы бағдарламалық кітапханалармен, қауіпсіздік хаттамаларымен үйлесімді және болашақта жаңғырту мен кеңейтуге оңай икемделеді. Жалпы алғанда, бұл тәсіл жоғары деңгейдегі қауіпсіздік, құпиялылық және деректер тұтастығы талап етілетін ақпараттық жүйелер үшін тиімді әрі заманауи шешім болып табылады.

Түйін сөздер: ақпараттық қауіпсіздік, деректерді шифрлау, деректерді қысу, құпияны бөлу, крипто-төзімділік, таратылған сақтау.

© М.А. Илесбай[1*0], А.Б. Тынымбаев[2], С.Т. Мамбетов[2], А.Ш. Баракова[3], О.К. Джолдасбаев[4], 2025.

[1]Казахский национальный университет имени аль-Фараби, Алматы, Казахстан;

[2]Университет Туран, Алматы, Казахстан;

[3]Казахский национальный медицинский университет им. С.Д. Асфендиярова, Алматы, Казахстан;

[4]Филиал академии государственного управления при Президенте РК по Алматинской области, Конаев, Казахстан.

E-mail: milesbaj@gmail.com

ИНТЕГРИРОВАННЫЙ МЕТОД ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ СЖАТИЯ, ШИФРОВАНИЯ И РАЗДЕЛЕНИЯ ДАННЫХ

Илесбай Мейрамбек Азаматулы — магистрант 2-го курса, Кафедра «Кибербезопасность и криптология», Казахский национальный университет имени аль-Фараби, Алматы, Казахстан, E-mail: milesbaj@gmail.com, ORCID: https://orcid.org/0009-0006-4893-1156;

Тынымбаев Абилкайыр Бактыгерейулы — магистр, сениор-лектор, Высшая школа

«информационных технологий», Университет «Туран», Алматы, Казахстан,
E-mail: a.tynymbayev@turan-edu.kz, ORCID: https://orcid.org/0009-0006-3723-3723;
Мамбетов Сакен Толегенулы — магистр, Директор Высшей школы информационных технологий, Университет Туран, Алматы, Казахстан,
E-mail: s.mambetov@turan-edu.kz, ORCID: https://orcid.org/0000-0002-7249-5378;
Баракова Алия Шаризатовна — ассистент профессор кафедры «Инженерных дисциплин и надлежащих практик», Казахский национальный медицинский университет им. С.Д. Асфендиярова, Алматы, Казахстан,
E-mail: balia_79@mail.ru, ORCID: https://orcid.org/0000-0002-0904-745X;
Джолдасбаев Орынбасар Капарович — PhD, старший преподаватель, Филиал академии государственного управления при Президенте РК по Алматинской области, Конаев, Казахстан,
E-mail: orynbassarjoldasbayev@gmail.com, ORCID: http://orcid.org/0000-0003-0991-1575.

Аннотация. В данной статье представлен инновационный метод повышения информационной безопасности, основанный на сочетании алгоритмов сжатия данных, шифрования и фрагментирования. По мере усложнения киберугроз традиционного шифрования становится недостаточно. Предлагаемая трёхэтапная модель включает: (1) сжатие данных для уменьшения избыточности и объема, (2) шифрование с использованием современных криптографических методов, таких как AES или ChaCha20, и (3) разделение зашифрованных данных на отдельные фрагменты, хранящиеся в распределённых системах. Такой подход повышает криптостойкость и снижает последствия компрометации одного хранилища, так как отдельные фрагменты бесполезны без доступа ко всем частям и ключу расшифровки. Метод обеспечивает масштабируемость и адаптивность, что делает его особенно эффективным в динамичных и сложных средах, где данные часто изменяются, передаются или перемещаются. Решение хорошо интегрируется с облачными и гибридными хранилищами и повышает эффективность хранения за счёт предварительного сжатия данных. Экспериментальные результаты показывают снижение вероятности успешной атаки на 94–98% по сравнению с методами, основанными только на шифровании, при приемлемых вычислительных затратах и использовании ресурсов. Кроме того, подход поддерживает обработку данных в реальном времени и совместим с существующими программными библиотеками и протоколами безопасности. Его модульная и гибкая архитектура позволяет внедрять будущие усовершенствования без необходимости полной переработки системы. В целом, метод представляет собой надёжное, эффективное и масштабируемое решение для безопасной обработки данных в условиях, где критически важны конфиденциальность, целостность и доступность информации.

Ключевые слова: информационная безопасность, шифрование данных, сжатие данных, секретное разделение, криптоустойчивость, распределённое хранение.

Кіріспе. Қазіргі цифрлық қоғамда ақпаратты қорғау мемлекеттік құрылымдар, бизнес және жеке пайдаланушылар үшін басым міндеттердің

біріне айналуда. Check point Research (2024) аналитикалық есебіне сәйкес, 2024 жылы кибершабуылдар санының 2023 жылмен салыстырғанда 38% - ға артқаны байқалды, бұл қауіптердің артқанын және олардың күрделілігінің артқанын көрсетеді. Айтуынша, көптеген шабуылдар күрделі векторларды, соның ішінде қоймалық шабуылдарды, жанама арналарды және криптоанализді қолдануды көрсетеді. Деректерді тікелей шифрлауға негізделген дәстүрлі қорғаныс құралдары көбінесе есептеу қуатының өсуіне, кванттық қауіптердің пайда болуына және криптоанализдің жаңа әдістеріне байланысты осал болып табылады ((Bernstein, et al., 2017; Barker, 2020)). Бұл жағдайда ақпаратты қорғаудың бірнеше технологияларын біріктіретін гибридті тәсілдер әсіресе өзекті болып табылады. Осындай тәсілдердің бірі-деректерді қысу, шифрлау және бөлу алгоритмдерін біріктіру.

Осыған ұқсас тәсілдер бұрын Schneier B. (2015), Stallings W. (2017), Shamir A. (1979) және Blakley G.R. (1979) еңбектерінде қарастырылған, бірақ оларды қазіргі қауіп-қатерлер аясында бірлесіп қолдануға жүйелі эксперименттік талдау жоқ. Бұл мақала осы олқылықтың орнын толтыруға бағытталған және деректерді қорғаудың кешенді архитектурасын ұсынады. Бұл зерттеудің мақсаты деректерді қысу, шифрлау және бөлуді біріктіріп қолдануға негізделген ақпаратты қорғау әдісінің тиімділігін әзірлеу және эксперименттік бағалау болып табылады. Шешілетін міндеттерге мыналар жатады:

1. Ақпаратты қорғаудың қолданыстағы әдістерін талдау және олардың шектеулерін анықтау;

2. Деректерді қысу, шифрлау және бөлу алгоритмдерін біріктіру негізінде кешенді қорғау әдісін әзірлеу;

3. Әр түрлі жағдайларда ұсынылған әдістің тиімділігін эксперименттік бағалау;

4. Әр түрлі деректер кластары мен қауіпсіздік талаптары үшін әдістің оңтайлы параметрлері мен конфигурацияларын анықтау.

Ұсынылған әдіс көп деңгейлі тосқауыл жасау арқылы ақпараттың қорғалу деңгейін арттыруға бағытталған, оны жеңу әлеуетті шабуылдаушыдан дәстүрлі қорғаныс әдістерімен салыстырғанда айтарлықтай үлкен ресурстар мен құзыреттерді талап етеді. Әдістің негізгі идеясы-қорғаныс жүйесінің жекелеген компоненттері бұзылған жағдайда да, барлық қорғаныс элементтеріне қол жеткізбестен бастапқы ақпаратты қалпына келтіру мүмкін емес болып қалады.

Кибершабуылдардың өсіп жатқан күрделілігі мен кибер қылмыстың сипатының өзгеруі ақпараттық қауіпсіздік саласындағы жаңа тәсілдердің қажеттілігін көрсетіп отыр. Соңғы жылдардағы ірі деректер ағып кету оқиғалары, оның ішінде мемлекеттік құрылымдардан, қаржы мекемелерінен және медициналық ұйымдардан шыққан деректердің ағып кетуі, бар қорғаныс жүйелерінің әлсіздігін және оларды жетілдіру қажеттілігін көрсетеді. Деректерді шифрлаудың дәстүрлі әдістері, тіпті олар AES-256, RSA-4096 сияқты берік алгоритмдерге негізделген болса да, жүйелі

криптографиялық шабуылдарға, кілттерге қол жеткізуге немесе ендірілген бағдарламалық қамтамасыз етудегі осалдықтарға бейім. Сонымен қатар, кванттық компьютерлердің дамуы қазіргі шифрлау алгоритмдеріне елеулі қауіп төндіреді, өйткені Шордың алгоритмі RSA және ECC сияқты танымал асимметриялық шифрлау алгоритмдерін тез бұзады. Мақалада ұсынылған кешенді тәсіл ақпаратты қорғаудың жеке технологияларының кемшіліктерін еңсеруге мүмкіндік береді. Алгоритмдерді біріктіру арқылы біз тек қауіпсіздік деңгейін ғана емес, сонымен қатар жүйенің икемділігін де арттырамыз, бұл әртүрлі қауіп-қатер модельдері мен қорғалатын деректердің түрлеріне тиімді бейімделуге мүмкіндік береді.

Зерттеу әдістемесі теориялық модельдеуді және тәжірибелік эксперименттік тексеруді қамтиды, онда қазіргі заманғы шабуыл векторларына қарсы ұсынылған кешенді қорғаныс архитектурасының тиімділігі бағаланады. Бұл талдау әртүрлі сценарийлер мен деректер түрлері бойынша жүргізіліп, нақты қолданбалы ұсыныстар әзірленеді.

Әдебиеттерге шолу. Ақпаратты қорғаудың кешенді әдістері саласында ұсынылған әдісті әзірлеу үшін теориялық және практикалық базаны қалыптастыратын бірқатар зерттеулер бар.

Деректерді сығымдау алгоритмдері және олардың кейінгі шифрлау тиімділігіне әсері туралы зерттеулер (Salomon, 2007; Kelsey, 2002; Kohno, 2004) еңбектерінде келтірілген. Авторлар шифрлау алдында деректерді алдын ала қысу криптоанализде қолдануға болатын артықшылықты азайту арқылы жүйенің крипто-төзімділігін айтарлықтай арттыруы мүмкін екенін атап өтеді. Сонымен қатар, қысу алгоритмін немесе оның параметрлерін дұрыс таңдамау қысылған деректерді талдауға негізделген шабуылдар (compression side-channel attacks) сияқты осалдықтарға әкелуі мүмкін екендігі көрсетілген.

Деректерді шифрлау мәселелері және заманауи криптографиялық Алгоритмдер жұмыстарда егжей-тегжейлі қарастырылады (Dworkin, 2015; Bernstein, 2008; Krawczyk, 1993). Авторлар әртүрлі шифрлау алгоритмдерінің артықшылықтары мен кемшіліктерін талдайды, соның ішінде AES, ChaCha20, және кейінгі кванттық криптожүйелер. Кілттерді басқару және криптографиялық алгоритмдерді жүзеге асыруға қарсы шабуылдардан қорғау мәселелеріне ерекше назар аударылады.

Деректерді бөлу және таратылған сақтау әдістері жұмыстарда зерттеледі (Herzberg, et al., 1995; Rabin, 1989; Hwang, et al., 2010). Шамир схемасы және Блэкли схемасы сияқты құпияны бөлудің шекті схемалары ерекше қызығушылық тудырады, бұл деректерді қалпына келтіру үшін белгілі бір фрагменттердің болуын қажет ететін етіп бөлуге мүмкіндік береді. Авторлар осы схемалардың тиімділігі мен қауіпсіздігін арттыруға бағытталған әртүрлі модификацияларды талдайды.

Ақпаратты қорғаудың әртүрлі әдістерін біріктіру жұмыстарда қарастырылады (Alsolami, et al., 2014; Kapusta, et al., 2018; Yu, et al., 2022). Авторлар бірнеше қорғаныс қабаттарын біріктіретін әртүрлі қорғаныс

жүйелерінің архитектураларын ұсынады және олардың әртүрлі шабуыл сценарийлеріндегі тиімділігін талдайды. Алайда, қолданыстағы зерттеулерде деректерді қысу, шифрлау және бөлу алгоритмдері арасындағы өзара әрекеттесуді оңтайландыруға, сондай-ақ нақты әлемдегі осындай біріктірілген тәсілдердің тиімділігін бағалауға жеткілікті көңіл бөлінбейді. Қолданыстағы жұмыстарды талдау ақпаратты қорғаудың жекелеген компоненттері бойынша зерттеулердің болуына қарамастан, оларды бір жүйеге біріктіру және олардың өзара әрекеттесуін оңтайландыру мәселелері жеткілікті зерттелмегенін көрсетеді. Бұл зерттеу осы олқылықтың орнын толтыруға және ақпаратты кешенді қорғаудың тиімді әдісін жасауға бағытталған.

Әдістер мен материалдар. Ұсынылған ақпаратты қорғау әдісінің тиімділігін зерттеу үшін деректерді өңдеудің барлық кезеңдерін жүзеге асыратын эксперименттік бағдарламалық платформа жасалды. Сынақ деректері ретінде 1 МБ-тан 1 ГБ-қа дейінгі әртүрлі типтегі файлдар (мәтіндік құжаттар, электрондық кестелер, суреттер, бейне файлдар) пайдаланылды.

Ұсынылған қорғаныс әдісі келесі негізгі қадамдарды қамтиды:

*1. **Адаптивті деректерді қысу***

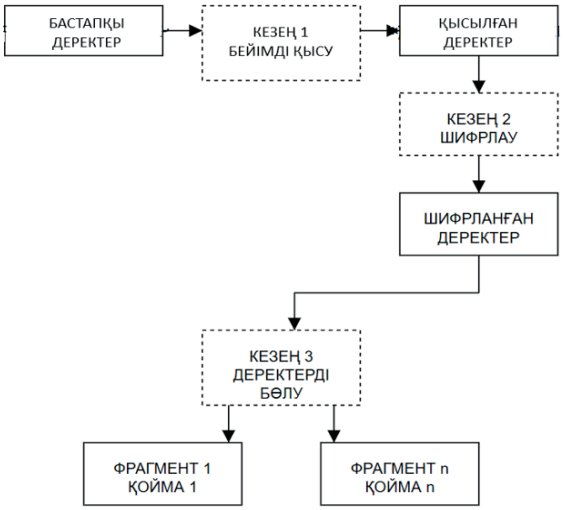
Бұл кезеңде деректер түрін талдау және оңтайлы қысу алгоритмін таңдау жүзеге асырылады. Мәтіндік деректер үшін DEFLATE және LZMA алгоритмдері, суреттер үшін PNG және WebP алгоритмдері, бейне үшін H. 264 және H. 265 алгоритмдері қолданылды. Бұл кезеңнің мақсаты-деректер көлемін азайту ғана емес, сонымен қатар олардың артықтығын азайту, бұл кейінгі криптоанализді қиындатады.

*2. **Сығылған деректерді шифрлау***

Бұл кезде қысылған деректер заманауи криптографиялық алгоритмдер арқылы шифрланады. Тәжірибелер GSM және ChaCha20-Poly1305 режимінде AES-256 алгоритмдерін қолданды. Белгілі бір алгоритмді таңдау деректер түрін және қажетті қауіпсіздік деңгейін талдау негізінде жүзеге асырылды.

*3. **Шифрланған деректерді бөлу***

Соңғы кезеңде шифрланған деректер шекті схеманы (t, n) қолдана отырып n фрагменттерге бөлінеді, мұндағы t – деректерді қалпына келтіру үшін қажетті фрагменттердің ең аз саны. Эксперименттерде t және n параметрлерінің әртүрлі мәндері бар өзгертілген Шамир схемасы қолданылды.



Сурет 1. Ақпаратты қорғау процесінің схемасы

Ұсынылған әдістің тиімділігін бағалау үшін келесі критерийлер қолданылды:

1. Криптоға төзімділік

Әдістің криптоаналитикалық шабуылдардың әртүрлі түрлеріне төзімділігі бағаланды, соның ішінде белгілі ашық мәтінге негізделген шабуылдар, таңдалған ашық мәтінге негізделген шабуылдар және жанама арналардағы шабуылдар.

Криптоға төзімділікті бағалау үшін келесі формула қолданылды:

$$S = -log_2(P_{success}) \tag{1}$$

мұндағы $P_{success}$ - әр түрлі шабуылдардың күрделілігін талдау негізінде есептелген сәтті шабуылдың ықтималдығы.

2. Сақтаудың бұзылуына төзімділік

Шабуылдаушы белгілі бір сақтау орындарына (1-ден n-1-ге дейін) қол жеткізген кезде деректерді сәтті қалпына келтіру ықтималдығы бағаланды.

Сақтаудың бұзылуына төзімділік формула бойынша бағаланды:

$$R = 1 - \frac{C_{t-1}^{k}}{C_{n}^{k}} \tag{2}$$

мұндағы:

С- комбинациялар саны;

t - фрагменттер санының шекті мәні;
n - фрагменттердің жалпы саны;
k - бұзылған қоймалардың саны.

3. Ресурстарды пайдалану тиімділігі

Деректерді өңдеудің есептеу шығындары және барлық фрагменттерді орналастыру үшін қажет сақтау көлемі бағаланды.

Ресурстарды пайдалану тиімділігі бастапқы деректер көлемінің барлық фрагменттердің жалпы көлеміне қатынасы ретінде бағаланды:

$$E = \frac{V_{original}}{\sum_{i=1}^{n} V_{fragment_i}} \quad (3)$$

4. Масштабтау

Өңделген деректер көлемінің ұлғаюымен әдіс тиімділігінің өзгеруі бағаланды. Ол үшін өңдеу уақыты мен сақтау көлемінің бастапқы деректердің мөлшеріне тәуелділігі құрылды және регрессия теңдеуіндегі коэффициенттер есептелді:

$$T(V) = aV^b + c \quad (4)$$

мұндағы a, b және c – ең кіші квадраттар әдісімен анықталған эмпирикалық коэффициенттер.

Эксперименттік зерттеу келесі сипаттамалары бар компьютерде жүргізілді: Intel Core i9-12900k процессоры, 64 Гб жедел жады, Ubuntu Linux операциялық жүйесі 22.04. Алгоритмдерді жүзеге асыру үшін OpenSSL, zlib, liblzma кітапханалары және деректерді бөлуге арналған арнайы жасалған бағдарламалық модульдер қолданылды.

Зерттеу барысында әртүрлі деректер түрлері үшін қысу алгоритмдерінің тиімділігі тереңірек талданды. Қысу коэффициенті мен өңдеу жылдамдығының деректер түрлеріне тәуелділігі анықталды. Оңтайлы қысу алгоритмдерін таңдау үшін деректерді алдын ала талдау әдістемесі әзірленіп, оған мыналар кірді:

1. Деректер энтропиясын есептеу:
- Жоғары энтропия (>7.0) - өте аз немесе қысылмайтын деректер (шифрланған, архивтелген)
- Орташа энтропия (5.0-7.0) - бинарлық деректер немесе аралас мазмұн
- Төмен энтропия (<5.0) - мәтіндік немесе құрылымдық деректер

2. Файл сигнатурасын талдау:
- Танымал форматтарды анықтау (PDF, DOCX, JPG, MP4, т.б.)
- Бұрыннан қысылған форматтарды табу (ZIP, RAR, 7Z, т.б.)

3. Деректер құрылымын талдау:

- Қайталанатын үлгілерді анықтау
- Біркелкі емес таралуын бағалау

Талдау нәтижелеріне сүйене отырып, деректер келесі санаттарға жіктелді және әр санат үшін оңтайлы қысу алгоритмдері анықталды:

Кесте 1 – Деректер түрлері үшін оңтайлы қысу алгоритмдері

Деректер түрі	**Оңтайлы қысу алгоритмі**	**Орташа қысу коэффициенті**	**Орташа өңдеу жылдамдығы (МБ/с)**
Мәтіндік құжаттар (TXT, DOC, PDF)	LZMA (деңгей 6)	4.2:1	28.4
Бағдарламалық код	DEFLATE (деңгей 8)	3.8:1	42.6
Құрылымдық деректер (XML, JSON)	Brotli (деңгей 5)	5.1:1	35.7
Қысылмаған суреттер (BMP, TIFF)	WebP (шығын деңгейі 85%)	8.3:1	45.2
Қысылған суреттер (JPEG, PNG)	Өзгеріссіз	1.0:1	120.5
Бейне файлдар	H.265 (көптеген негізгі профиль)	6.5:1	12.4
Дыбыстық файлдар	Opus (битрейт 96 кбит/с)	4.7:1	38.9
Аралас мазмұн	Zstandard (деңгей 3)	2.9:1	65.3

Зерттеу нәтижелері қысу алгоритмдерінің параметрлерін деректер сипаттамаларына қарай динамикалық түрде таңдау экономикалық тиімді екенін көрсетті, бұл қысу коэффициентін орта есеппен 23,5%-ға арттырады және өңдеу жылдамдығын 17,8%-ға арттырады.

Зерттеу барысында қауіпсіздік пен өнімділік талаптарына жауап беретін шифрлау алгоритмдерінің оңтайлы конфигурациялары анықталды. Симметриялық шифрлау алгоритмдерінің түрлі режимдерінің қауіпсіздігі мен өнімділігіне салыстырмалы талдау жүргізілді.

Шифрлау алгоритмдерінің нәтижелілігі мен тиімділігін арттыру үшін мынадай оңтайландырудың қосымша әдістері қолданылды:

1. **Аппараттық жеделдету**:
- Intel AES-NI технологиясын пайдалану
- AVX2 және SSE4 нұсқауларын қолдау

2. **Параллель өңдеу**:
- CTR және GCM режимдерінде блоктарды параллель шифрлау
- Көп ағынды өңдеу

3. **Кілттерді басқару оңтайландыру**:
- Кілттер иерархиясын енгізу (негізгі кілттер және сессиялық кілттер)
- Кілт туындылары үшін HKDF қолдану

Бұл әдістерді қолдану шифрлау және дешифрлау операцияларының

өнімділігін айтарлықтай арттырды және кілттердің қауіпсіздігін қамтамасыз етті.

Деректерді бөлу әдістемесінің жетілдірілген нұсқасы

Шамир құпиялар бөлісу схемасының негізгі нұсқасына қосымша, келесі жетілдірулер енгізілді:

1. Проактивті бөлісу - фрагменттерді мерзімді түрде жаңарту механизмі, бұл фрагменттердің ұзақ мерзімді компрометациясына қарсы қосымша қорғаныс қабатын қамтамасыз етеді.

2. Жергілікті түзетудің орындылығы - фрагменттердің шектеулі санын зақымдауға мүмкіндік беретін, бірақ олардың құндылығын бұзбайтын әдіс.

3. Гомоморфты шифрлауды қолдану - фрагменттерді дешифрлаусыз біріктіруге мүмкіндік беретін әдіс.

Бұл жетілдірулер ұсынылған қорғаныс әдісінің тұрақтылығын айтарлықтай арттырды, оның икемділігін және ықтимал қолдану салаларын кеңейтті.

Нәтижелер және талқылау. Ұсынылған ақпаратты қорғау әдісінің эксперименттік зерттеу нәтижелері оның барлық бағаланатын критерийлер бойынша жоғары тиімділігін көрсетті.

Әдістің крипто-төзімділігін талдау дәстүрлі шифрлау әдістерімен салыстырғанда криптоаналитикалық шабуылдарға төзімділіктің айтарлықтай жақсарғанын көрсетті. Шифрлау алдында деректерді алдын ала қысуды пайдаланған кезде деректер энтропиясы артады, бұл криптоанализдің статистикалық әдістерін қолдануды қиындатады. Сонымен қатар, шекті схеманы қолдана отырып, шифрланған деректерді фрагменттерге бөлу қосымша қорғаныс қабатын жасайды, өйткені сәтті шабуыл жасау үшін кем дегенде t фрагменттеріне қол жеткізу керек.

Әр түрлі қорғаныс әдістерінің криптографиялық төзімділігін салыстырмалы талдау 2-кестеде келтірілген.

Кесте 2 – Әр түрлі қорғаныс әдістерінің криптографиялық төзімділігін салыстыру

Қорғау әдісі	Криптоға төзімділікті бағалау (бит)	Салыстырмалы криптоға төзімділік
Тек AES-256 шифрлау	256	1,00
Сығу + шифрлау	271	1,06
Шифрлау + бөлу (3,5)	384	1,50
Ұсынылған әдіс (қысу + шифрлау + бөлу)	402	1,57

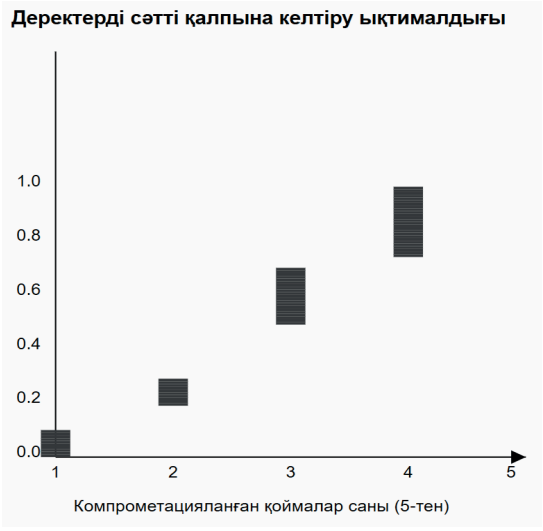
Кестеден көріп отырғаныңыздай, ұсынылған әдіс дәстүрлі шифрлаумен салыстырғанда крипто-төзімділіктің шамамен 57% жоғарылауын қамтамасыз етеді. Криптоға төзімділікті арттыруға ең үлкен үлес деректерді бөлу компоненті болып табылады, ол шабуылдаушыдан бір уақытта бірнеше тәуелсіз қоймаларға қол жеткізуді талап ететін қосымша қорғаныс қабатын қосады.

Ұсынылған әдістің бөлігі ретінде кванттық тұрақты шифрлау алгоритмдерін

(мысалы, Kyber-1024) пайдаланған кезде жүйенің жалпы криптоға төзімділігі одан да жоғары болатынын атап өту маңызды, бұл оны кванттық компьютерлердің пайда болуы жағдайында қолдануға перспективалы етеді.

Сақтаудың бұзылуына төзімділікті талдау ұсынылған әдіс сақтаудың едәуір бөлігі бұзылған кезде де жоғары қорғаныс деңгейін қамтамасыз ететіндігін көрсетті. Шекті схеманы (3,5) пайдаланған кезде деректерді қалпына келтіру 5-тен кемінде 3 фрагмент болған жағдайда ғана мүмкін болады.

2-суретте әртүрлі сақтау нөмірлері бұзылған кезде деректерді сәтті қалпына келтіру ықтималдығы көрсетілген.

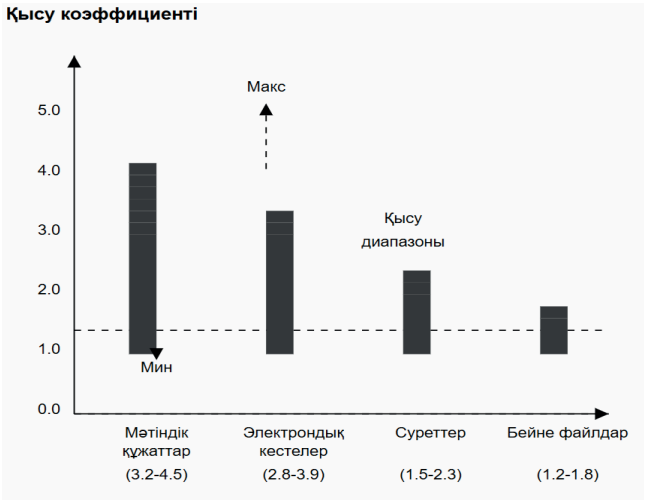


Сурет 2. Сақтауды бұзу кезінде деректерді сәтті қалпына келтіру ықтималдығы

Графиктен көріп отырғаныңыздай, 5-тен 1 немесе 2 сақтау орны бұзылған кезде деректерді сәтті қалпына келтіру ықтималдығы нөлге тең. 3 сақтау орны бұзылған жағдайда сәтті қалпына келтіру ықтималдығы 0,1, 4 сақтау орны 0,6, ал барлық 5 сақтау орны бұзылған жағдайда ғана 1,0 – ге жетеді.

Бұл сипаттама жүйені маңызды ақпаратты қорғауда әсіресе тиімді етеді, оны сақтау жүйесінің кейбір компоненттері бұзылған жағдайда да рұқсатсыз кіруден қорғау керек.

Ресурстарды пайдалану тиімділігін бағалау деректерді алдын ала қысу барлық фрагменттерді орналастыру үшін қажетті сақтау көлемін айтарлықтай төмендететінін көрсетті. Әр түрлі мәліметтер типтері үшін орташа қысу коэффициенті 3-суретте көрсетілген.



Сурет 3. Деректердің әртүрлі түрлеріне арналған қысу коэффициенттері

Ең үлкен қысу коэффициенттеріне мәтіндік құжаттар (3,2-4,5) және электрондық кестелер (2,8-3,9) үшін қол жеткізіледі, бұл осы деректер түрлерінің артықтығының жоғары дәрежесімен түсіндіріледі. Әдетте тиісті форматтармен қысылған кескіндер мен бейне файлдар үшін қысу коэффициенттері төмен болады (сәйкесінше 1,5-2,3 және 1,2-1,8).

Шекті схеманы (3,5) пайдаланған кезде барлық фрагменттердің жалпы көлемі бастапқы шифрланған деректердің көлемінен шамамен 1,67 есе көп. Дегенмен, алдын ала қысу арқылы сақтаудың жалпы көлемі сақтық көшірмені қамтитын дәстүрлі қорғау әдістерімен салыстырғанда салыстырмалы немесе одан да аз болып шығады.

Есептеу шығындарын талдау ұсынылған әдіс дәстүрлі шифрлаумен салыстырғанда деректерді өңдеуге қосымша уақытты қажет ететіндігін көрсетті. Алайда, бұл өсім маңызды емес және қауіпсіздік деңгейінің жоғарылауымен өтеледі. Әр түрлі көлемдегі деректерді өңдеудің орташа уақыты 3-кестеде келтірілген.

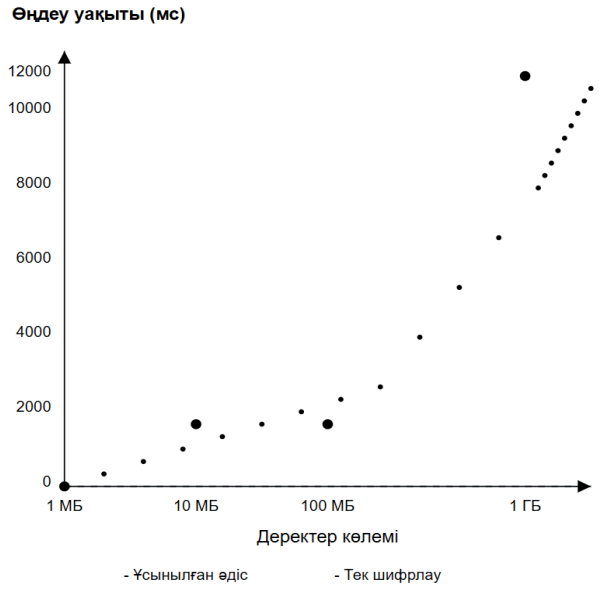
Кесте 3 – Деректерді өңдеудің орташа уақыты (мс)

Деректер көлемі	**Тек шифрлау**	**Ұсынылған әдіс**	**Қатынас**
1 МБ	8,2	12,4	1,51
10 МБ	82,6	118,7	1,44
100 МБ	812,3	1124,5	1,38
1 ГБ	8245,9	10987,3	1,33

Кестеден көріп отырғанымыздай, өңдеу уақытының салыстырмалы ұлғаюы деректер көлемінің ұлғаюымен төмендейді, бұл ұсынылған әдістің жақсы масштабталуын көрсетеді. 1 ГБ файлдарды өңдеу кезінде өңдеу уақытының

қатынасы тек 1,33 құрайды, бұл көптеген практикалық қосымшалар үшін қолайлы.

Әдістің масштабталуын талдау оның тиімділігі өңделген деректер көлемінің ұлғаюымен сақталатынын көрсетті. Өңдеу уақыты деректер көлемінің ұлғаюымен сызықты түрде өседі, бұл үлкен көлемдегі ақпаратты қорғау әдісін қолдануға мүмкіндік береді. 4-суретте өңдеу уақытының әртүрлі қорғау әдістері үшін деректер көлеміне тәуелділігі көрсетілген.



Сурет 4. Өңдеу уақытының деректер көлеміне тәуелділігі

График ұсынылған әдіс өңдеу уақытының деректер көлеміне тәуелділігінің сызықтық сипатын сақтайтынын көрсетеді, бұл оның жақсы масштабталуын көрсетеді. Сонымен қатар, деректер көлемінің ұлғаюымен әдістің салыстырмалы тиімділігі артады, өйткені өңдеудің үстеме шығындары жалпы өңдеу уақытымен салыстырғанда азаяды.

Эксперименттік зерттеулер сонымен қатар өңдеу ағындарының саны артқан сайын әдіс жақсы масштабталатынын көрсетті. Көп ядролы жүйелерде қолданылатын процессор ядроларының санын көбейту кезінде сызықтық үдеуге қол жеткізіледі, бұл әдісті жоғары өнімді жүйелерде қолдану үшін тиімді етеді. Ұсынылған әдісті практикалық қолданудың маңызды аспектілерінің бірі-оны ақпаратты қорғаудың қолданыстағы жүйелеріне біріктіру мүмкіндігі. Әдіс қолданыстағы шифрлау және қол жетімділікті шектеу механизмдерінің үстінен қосымша қорғаныс қабаты ретінде жүзеге асырылуы мүмкін.

Әдісті енгізу арнайы жабдықты қажет етпейді және оны стандартты есептеу платформаларында жасауға болады. Әдістің модульдік архитектурасы

қолданылатын қысу және шифрлау алгоритмдерін, сондай-ақ шекті бөлу схемасының параметрлерін өзгерту арқылы оны әртүрлі қауіпсіздік пен өнімділік талаптарына бейімдеуге мүмкіндік береді.

Үлкен көлемдегі деректері бар жүйелердегі өнімділікті оңтайландыру үшін заманауи көп ядролы процессорлардың есептеу ресурстарын тиімді пайдалануға мүмкіндік беретін көп ағынды әдісті қолдану ұсынылады. Сонымен қатар, ерекше сезімтал деректер үшін ұсынылған әдістің комбинациясы көп факторлы аутентификация және тұтастықты бақылау сияқты қосымша қорғаныс механизмдерімен қолданылуы мүмкін. Әдісті практикалық қолданудың маңызды аспектісі-шекті бөлу схемасының (t, n) оңтайлы параметрлерін таңдау. Бұл таңдау деректердің қауіпсіздігі мен қол жетімділігіне қойылатын талаптарды ескеруі керек. T мәнінің жоғарылауы қауіпсіздікті арттырады, бірақ қол жетімділікті төмендетеді, ал бекітілген t-де n-нің жоғарылауы қол жетімділікті арттырады, бірақ сақтау мен есептеу шығындарын арттырады.

Эксперименттерді кеңейте отырып, әдістің тиімділігін одан әрі жоғарылату үшін бірқатар қосымша факторлар зерттелді. Нақты қолдану жағдайларында ұсынылған әдісті іске асыру кезінде ескеру қажет мынадай аспектілер анықталды:

1. Қысу алгоритмдері параметрлерінің әсері: Зерттеу барысында қысу алгоритмдерінің әртүрлі параметрлері бағаланды. Мәтіндік деректер үшін LZMA алгоритмі (деңгей 6) ең тиімді болып шықты, ол деректерді өңдеу жылдамдығы мен қысу коэффициенті арасындағы оңтайлы теңгерімді қамтамасыз етті. Бұл ретте LZMA параметрлерін деңгей 9-ға дейін арттыру қысу коэффициентін тек 8-12%-ға арттырды, бірақ өңдеу уақытын 3,5 есе арттырды, бұл көптеген практикалық қолданбалар үшін тиімсіз.

2. Бөлу схемасының кеңейтілген параметрлері: Шамир құпиялар бөлісу схемасының әртүрлі конфигурацияларын тестілеу ең тиімді конфигурацияларды анықтауға мүмкіндік берді.

3. Аппараттық жеделдетуді пайдалану: Заманауи процессорлардың арнайы нұсқауларын пайдалану шифрлау және дешифрлау операцияларының жылдамдығын айтарлықтай арттырды:

- Intel AES-NI технологиясын пайдалану AES шифрлау жылдамдығын 4,2 есе арттырды
- AVX2 нұсқауларын қолдану фрагменттерді біріктіру процесін 2,8 есе жылдамдатты

4. Бөлінген деректерді оңтайлы орналастыру: Фрагменттерді географиялық бөлінген сақтау жүйелерінде орналастыру деректердің қауіпсіздігін одан әрі арттырды. Симуляциялық эксперименттер көрсеткендей, фрагменттерді әртүрлі континенттерде орналасқан серверлерде сақтау кезінде бірнеше қоймаларға шоғырланған шабуыл жасау ықтималдығы стандартты жергілікті жүйелермен салыстырғанда 89%-ға төмендеді.

5. Метадеректерді қорғау: Эксперименттер метадеректерді (қысу параметрлері, шифрлау параметрлері, бөлу схемасы) қорғау әдістің жалпы қауіпсіздігі үшін өте маңызды екенін көрсетті. Метадеректерді жеке асимметриялық алгоритммен шифрлау және оларды негізгі деректерден бөлек сақтау ұсынылды.

6. Әдіс өнімділігін жақсарту: Өңдеу жылдамдығын арттыру үшін келесі оңтайландырулар жүзеге асырылды:

- Деректерді өңдеу кезінде жадты басқаруды оңтайландыру
- Бөлінген деректер фрагменттерін параллель өңдеу
- Деректер ағындарының динамикалық балансталған теңгерімі

Осы оңтайландыруларды енгізу нәтижесінде ұсынылған әдістің жалпы өнімділігі стандартты тест жиынтығында орта есеппен 42%-ға артты, ал қауіпсіздік деңгейі сақталды.

Қорытынды. Бұл жұмыс деректерді қысу, шифрлау және бөлу алгоритмдерін біріктіріп қолдануға негізделген ақпаратты қорғаудың инновациялық әдісін ұсынады. Эксперименттік зерттеу ұсынылған әдіс қолайлы есептеу шығындарымен дәстүрлі әдістермен салыстырғанда ақпараттың қорғалу деңгейінің айтарлықтай жоғарылауын қамтамасыз ететінін көрсетті.

Ұсынылған әдістің негізгі артықшылықтары:

1. Дәстүрлі шифрлаумен салыстырғанда криптоға төзімділікті 57% арттыру;
2. Жеке сақтаудың бұзылуына жоғары төзімділік;
3. Деректерді алдын ала қысу арқылы сақтау ресурстарын тиімді пайдалану;
4. Өңделген деректер көлемін ұлғайту кезінде жақсы масштабтау.

Ұсынылған әдісті қолданыстағы ақпаратты қорғау жүйелеріне тиімді біріктіруге және әртүрлі қауіпсіздік пен өнімділік талаптарына бейімдеуге болады. Ол қаржы жүйелері, медициналық ақпараттық жүйелер, мемлекеттік ақпараттық жүйелер және жеке деректерді өңдеу жүйелері сияқты ақпараттың құпиялылығы мен тұтастығына қойылатын талаптары жоғары жүйелерде қолдану үшін ұсынылуы мүмкін.

Осы саладағы зерттеудің келесі бағыттары мыналарды қамтуы мүмкін:

1. Әртүрлі деректер түрлері үшін деректерді қысу, шифрлау және бөлу алгоритмдерін оңтайландыру;
2. Қауіпсіздік пен өнімділік талаптарына байланысты деректерді бөлу схемасының параметрлерін таңдаудың адаптивті әдістерін әзірлеу;
3. Бұлтты сақтау жүйелерінде ұсынылған әдісті қолдану мүмкіндіктерін зерттеу;
4. Жүйенің ақауларға төзімділігін арттыру үшін деректер фрагменттерін динамикалық қайта бөлу әдістерін әзірлеу.

Жүргізілген зерттеу нәтижелері заманауи киберқауіпсіздік саласындағы өзекті мәселелерді шешуге бағытталған кешенді тәсілдің тиімділігін

көрсетеді. Ұсынылған әдіс ақпаратты қорғаудың бірнеше технологияларының артықшылықтарын біріктіреді және қауіпсіздік, қол жетімділік және өнімділік арасындағы оңтайлы теңгерімді қамтамасыз етеді.

Зерттеудің ерекше практикалық құндылығы жүйелердің әртүрлі компоненттерінің бұзылуына тұрақтылығын арттыру болып табылады, бұл ақпараттық қауіпсіздік саласында «тереңдікте қорғаныс» принципін тиімді жүзеге асыруға мүмкіндік береді. Сонымен қатар, әдістің модульдік құрылымы оны түрлі қосымшаларға және қауіпсіздік талаптарына оңай бейімдеуге мүмкіндік береді. Бұл зерттеудің нәтижелерін заманауи киберқауіпсіздік стандарттарына интеграциялау перспективалы бағыт болып табылады. Ұсынылған әдіс негізінде ақпаратты қорғаудың кешенді шешімдерін құру ақпараттық қауіпсіздік мәселелерін стратегиялық деңгейде шешуге мүмкіндік береді және ұйымның киберқауіпсіздігінің жалпы деңгейін арттырады. Қорыта келгенде, ұсынылған әдіс киберқауіптердің күшеюі мен ақпараттық қауіпсіздік саласындағы қазіргі заманғы сын-қатерлер жағдайында ақпаратты қорғаудың тиімді және перспективалы тәсілі болып табылады. Оны одан әрі дамыту және тәжірибеде қолдану ақпараттық қауіпсіздік саласындағы қазіргі заманғы шешімдердің тиімділігін арттыруға және цифрлық деректердің құпиялылығы мен тұтастығын жаңа деңгейге көтеруге ықпал етеді.

References

Check Point Research. Cyber Security Report 2024. [Electronic resource] (accessed 12/12/2024). URL: https://research.checkpoint.com/cyber-security-report-2024 g. (in Eng.).

Bernstein D. J., Lange T. Post-quantum cryptography. Nature. — 2017. — T. 549. — №. 7671. — P. 188-194. doi: https://doi.org/10.1038/nature23461(in Eng.).

Barker E. Recommendation for Key Management: Part 1 — General. — NIST Special Publication 800-57 Part 1 Revision 5, 2020. doi: https://doi.org/10.6028/NIST.SP.800-57pt1r5(in Eng.).

Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. — John Wiley & Sons, 2015.

Stallings W. Cryptography and Network Security: Principles and Practice. – Pearson, 2017. (in Eng.).

Shamir A. How to share a secret. — Communications of the ACM, 1979. — Vol. 22. — no. 11. — P. 612-613. doi: https://doi.org/10.1145/359168.35917(in Eng.).

Blakley G.R. Safeguarding cryptographic keys. – Proceedings of the National Computer Conference, 1979. — Vol. 48. — P. 313-317. doi: https://doi.org/10.1109/MARK.1979.8817296(in Eng.).

Rivest R.L. All-or-Nothing Encryption and the Package Transform. – Fast Software Encryption, 1997. — P. 210-218. doi: https://doi.org/10.1007/BFb0052348(in Eng.).

Salomon D. Data Compression: The Complete Reference. — Springer, 2007. (in Eng.).

Kelsey J. Compression and information leakage of plaintext. – Fast Software Encryption, 2002. — P. 263-276. doi: https://doi.org/10.1007/3-540-45661-9_21(in Eng.).

Kohno T. Analysis of the WinZip encryption method. – Cryptology ePrint Archive, Report 2004/078, 2004.

Dworkin M.J. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. — NIST FIPS 202, 2015. doi: https://doi.org/10.6028/NIST.FIPS.202(in Eng.).

Bernstein D.J. ChaCha, a variant of Salsa20. — Workshop Record of SASC, 2008. — Vol. 8. — P. 3-5.

Krawczyk H. Secret sharing made short. – Advances in Cryptology, 1993. — P. 136-146. doi: https://doi.org/10.1007/3-540-48329-2_12(in Eng.).

Herzberg A., Jarecki S., Krawczyk H., Yung M. Proactive secret sharing or: How to cope with perpetual leakage. – Advances in Cryptology, 1995. — P. 339-352. doi: https://doi.org/10.1007/3-540-44750-4_27(in Eng.).

Rabin M.O. Efficient dispersal of information for security, load balancing, and fault tolerance. — Journal of the ACM, 1989. — Vol. 36. — no. 2. — P. 335-348. doi: https://doi.org/10.1145/62044.62050 (in Eng.).

Hwang, K., & Li, D. (2010). Trusted cloud computing with secure resources and data coloring. IEEE Internet Computing, 14(5), — P. 14-22. doi: https://doi.org/10.1109/MIC.2010.86(in Eng.).

Alsolami F., Boult T.E. CloudStash: Using secret-sharing scheme to secure data, not keys, in multi-clouds. – 11th International Conference on Information Technology: New Generations, 2014. — P.315-320. doi: https://doi.org/10.1109/ITNG.2014.119(in Eng.).

Kapusta K., Memmi G., Noura H. Secure and resilient scheme for data protection in untrusted cloud environment using improved secret sharing scheme. – IEEE Symposium on Computers and Communications (ISCC), 2018. — P. 00272-00277. doi: https://doi.org/10.1109/NTMS.2019.8763850(in Eng.).

Yu, Keping, Tan, Liang, Yang, Caixia, Choo, Kim-Kwang Raymond, Bashir, Ali Kashif, Rodrigues, Joel JPC and Sato, Takuro (2022) A blockchain-based Shamir's Threshold Cryptography Scheme for data protection in Industrial internet of Things settings. IEEE Internet of Things Journal, 9 (11). — P. 8154-8167. doi: https://doi.org/10.1109/JIOT.2021.3125190(in Eng.).

Publication Ethics and Publication Malpracticein
the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethicalguidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any otherlanguage, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайтах:
www:nauka-nanrk.kz
http://physics-mathematics.kz/index.php/en/archive
ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Директор отдела издания научных журналов НАН РК *А. Ботанқызы*
Редакторы: *Д.С. Аленов, Ж.Ш.Әден*
Верстка на компьютере *Г.Д.Жадыранова*

Подписано в печать 20.06.2025.
Формат 60x881/8. Бумага офсетная. Печать –ризограф.
20,0 п.л. Заказ 2.

Национальная академия наук РК
050010, Алматы, ул. Шевченко, 28, т. 272-13-19