УДК 004.056:004.8
МРНТИ 20.01.45

DOI: https://doi.org/10.37788/2026-2/102-107

А.Ғ. Керім[1]*
[1]Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан
*(e-mail kerim_ag_2@enu.kz)

Криптография мен жасанды интеллект интеграциясы: ақпараттық қауіпсіздік жүйелерінің тиімділігін арттыру

Аңдатпа

Негізгі мәселе: Қазіргі цифрлық қоғам жағдайында ақпараттық жүйелердің дамуы деректер қауіпсіздігін қамтамасыз ету мәселесінің маңыздылығын арттырып отыр. Осыған байланысты криптография мен жасанды интеллект технологияларының өзара әрекеттесуін зерттеу өзекті ғылыми бағыттардың біріне айналды.

Мақсаты: Бұл мақалада криптографиялық жүйелерде жасанды интеллект технологияларын қолданудың мүмкіндіктері, қауіптері және даму перспективалары қарастырылады. Зерттеудің мақсаты – дәстүрлі криптографиялық алгоритмдер мен жасанды интеллект негізінде оңтайландырылған алгоритмдердің тиімділігін салыстырмалы түрде талдау.

Әдістері: Зерттеу барысында эксперименттік модельдеу әдісі қолданылып, әртүрлі көлемдегі деректерді шифрлау уақыты өлшенді.

*Нәтижелер және олардың маңыздылығы:*Алынған нәтижелер жасанды интеллект негізіндегі алгоритмдер дәстүрлі әдістермен салыстырғанда жоғары өнімділік көрсететінін анықтады. Сонымен қатар жасанды интеллект криптографиялық жүйелердегі осалдықтарды анықтау және қауіпсіздік жүйелерін бейімдеу мүмкіндігін арттырады. Зерттеу нәтижелері криптография мен жасанды интеллект интеграциясы ақпараттық қауіпсіздік жүйелерін жетілдірудің маңызды бағыты екенін көрсетеді.

Түйінді сөздер: криптография, жасанды интеллект, ақпараттық қауіпсіздік, шифрлау алгоритмдері, криптоанализ, машиналық оқыту, деректерді қорғау, киберқауіпсіздік.

Кіріспе

Қазіргі цифрлық қоғам жағдайында ақпараттық жүйелердің күрделенуі мен деректер көлемінің қарқынды артуы ақпараттық қауіпсіздік мәселелерінің маңыздылығын арттырып отыр. Деректердің құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз етудің негізгі құралдарының бірі – криптографиялық әдістер болып табылады. Бүгінгі таңда AES, RSA сияқты криптографиялық алгоритмдер көптеген ақпараттық жүйелерде кеңінен қолданылады.

Алайда үлкен көлемдегі деректерді өңдеу барысында дәстүрлі криптографиялық алгоритмдердің есептеу шығындары айтарлықтай өседі. Бұл мәселе әсіресе бұлттық есептеулер, үлкен деректер (Big Data) және IoT жүйелерінде өзекті болып отыр. Сондықтан криптографиялық жүйелердің өнімділігін арттыру үшін жаңа технологияларды қолдану қажеттілігі туындады.

Соңғы жылдары жасанды интеллект (Artificial Intelligence) және машиналық оқыту әдістері ақпараттық қауіпсіздік саласында кеңінен зерттелуде. AI алгоритмдері жүйелердің жұмыс параметрлерін автоматты түрде бейімдеуге, деректерді талдауға және қауіптерді алдын ала анықтауға мүмкіндік береді. Осыған байланысты криптография мен жасанды интеллект технологияларының интеграциясы ақпараттық қауіпсіздік саласындағы перспективалы ғылыми бағыттардың бірі болып саналады.

Осы зерттеудің негізгі мақсаты – дәстүрлі криптографиялық алгоритмдер мен жасанды интеллект негізінде оңтайландырылған алгоритмдердің өнімділігін салыстырмалы түрде талдау.

Зерттеу барысында келесі міндеттер қойылды:

– криптографиялық алгоритмдердің жұмыс тиімділігін бағалау;
– деректер көлеміне байланысты шифрлау уақытының өзгеруін анықтау;
– AI қолдану арқылы алгоритмдердің өнімділігін арттыру мүмкіндігін зерттеу;

– алынған нәтижелерді салыстырмалы талдау.

Зерттеу әдістері

Зерттеу барысында криптографиялық алгоритмдердің өнімділігін бағалау үшін салыстырмалы талдау және эксперименттік модельдеу әдістері қолданылды. Бұл тәсілдер криптографиялық жүйелердің тиімділігін зерттеуде кеңінен қолданылатын ғылыми әдістердің қатарына жатады.

Зерттеу әдістемесі қолданбалы криптография және жасанды интеллект саласындағы ғылыми еңбектерге негізделді. Атап айтқанда, криптографиялық алгоритмдердің теориялық негіздері В. Столлингс [1], Дж. Кац және Й. Линделл [2], сондай-ақ Б. Шнайер [3] еңбектерінде сипатталған криптографиялық жүйелерді талдау қағидаттарына сүйене отырып қарастырылды. AES және RSA алгоритмдерінің құрылымы мен жұмыс істеу ерекшеліктері Р. Ривест, А. Шамир, Л. Адлеман [10] және Й. Даэмен мен В. Реймен [11] еңбектеріндегі классикалық модельдер негізінде таңдалды.

Жасанды интеллект және машиналық оқыту әдістерін қолдану тәсілдері И. Гудфеллоу, Й. Бенджио және А. Курвилльдің Deep Learning еңбегіндегі нейрондық желілер мен алгоритмдерді оңтайландыру принциптеріне, сондай-ақ С. Рассел мен П. Норвигтің жасанды интеллект жүйелерін талдау әдістеріне негізделді [4;5]. Сонымен қатар киберқауіпсіздік саласында жасанды интеллект қолдану мәселелері Y. Chen және әріптестерінің зерттеулерінде қарастырылған тәсілдерге сүйенді [13].

Эксперименттік зерттеу криптографиялық алгоритмдердің өнімділігін модельдеу арқылы жүргізілді. Мұндай тәсіл алгоритмдердің есептеу тиімділігін нақты жүйені толық іске қоспай-ақ бағалауға мүмкіндік береді. Эксперимент барысында әртүрлі көлемдегі тесттік деректер жиынтығы қолданылды: 100 МБ, 200 МБ, 400 МБ, 600 МБ, 800 МБ және 1000 МБ. Бұл деректер көлемдері ақпараттық жүйелердегі типтік жүктемені модельдеу мақсатында таңдалды.

Зерттеу барысында екі түрлі алгоритмдік тәсіл қарастырылды:

– дәстүрлі криптографиялық алгоритмдер (AES, RSA);

– жасанды интеллект негізінде оңтайландырылған алгоритмдер.

AI негізіндегі тәсілде машиналық оқыту алгоритмдері жүйенің есептеу жүктемесін және деректер көлемін талдау арқылы шифрлау алгоритмдерінің параметрлерін динамикалық түрде бейімдеу үшін қолданылды.

Алгоритмдердің тиімділігін бағалау үшін негізгі көрсеткіш ретінде шифрлау операциясының орындалу уақыты (секунд) алынды. Алынған нәтижелер кейіннен кестелер мен графиктер арқылы салыстырмалы түрде талданды.

Зерттеу логикасын көрсету мақсатында криптографиялық алгоритмдерді AI негізінде оңтайландырудың авторлық эксперименттік схемасы ұсынылды (Сурет 1). Бұл схема криптография және жасанды интеллект саласындағы ғылыми зерттеулерді талдау негізінде әзірленген тұжырымдамалық модель болып табылады.

Зерттеу нәтижелері

Эксперимент криптографиялық алгоритмдердің өнімділігін бағалау мақсатында жүргізілді. Зерттеу барысында деректер көлемінің өзгеруі шифрлау алгоритмдерінің жұмыс уақытына қалай әсер ететіні талданды. Эксперименттік зерттеу Python бағдарламалау ортасында жүзеге асырылды. Криптографиялық операцияларды іске асыру үшін PyCryptodome кітапханасы қолданылды, ал деректерді өңдеу және нәтижелерді визуализациялау үшін NumPy, Pandas және Matplotlib кітапханалары пайдаланылды.

Есептеу эксперименттері келесі аппараттық конфигурацияда орындалды:

Intel Core i7 процессоры, 16 ГБ жедел жады (RAM), Windows 10 операциялық жүйесі.

Эксперимент бірнеше кезеңнен тұрды:

– Әртүрлі көлемдегі тесттік деректер жиынтығын генерациялау (100 МБ, 200 МБ, 400 МБ, 600 МБ, 800 МБ және 1000 МБ).

– Әрбір деректер көлемі үшін AES және RSA алгоритмдері арқылы шифрлау операциясын орындау.

– Сол деректер жиынтығы үшін AI негізінде оңтайландырылған алгоритмді қолдану.

– Әрбір шифрлау операциясының орындалу уақытын секундпен өлшеу.

– Әрбір тәжірибені бірнеше рет қайталап, нәтижелердің орташа мәнін есептеу.

Алынған нәтижелер негізінде алгоритмдердің өнімділігін сипаттайтын сандық деректер қалыптастырылды. Бұл мәліметтер 1-кестеде көрсетілген.

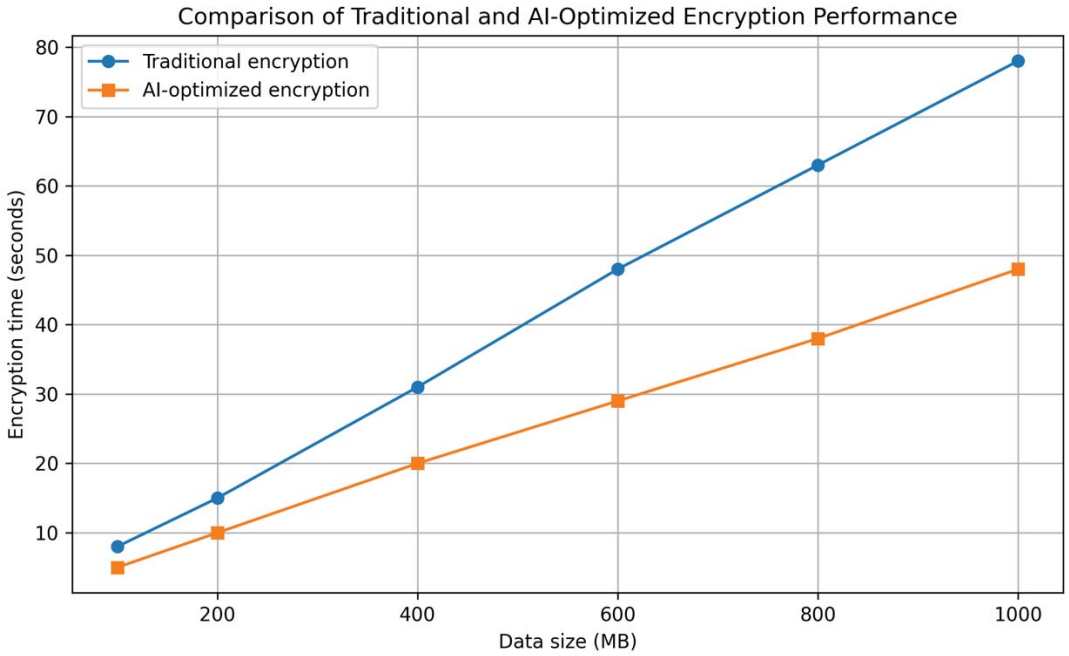
Кесте 1. – Деректер көлеміне байланысты шифрлау алгоритмдерінің өнімділігі

Деректер көлемі (МБ)	Дәстүрлі алгоритмдер (сек)	AI алгоритмдері (сек)
100	8	5
200	15	10
400	31	20
600	48	29
800	63	38
1000	78	48

Кестеден көріп отырғанымыздай, деректер көлемі артқан сайын дәстүрлі криптографиялық алгоритмдердің шифрлау уақыты айтарлықтай өседі. Мысалы, 100 МБ деректерді өңдеу кезінде шифрлау уақыты шамамен 8 секунд болса, 1000 МБ көлемінде бұл көрсеткіш 78 секундқа дейін артады.

Ал AI негізіндегі алгоритмдерді қолдану кезінде шифрлау уақыты салыстырмалы түрде төмен болады. Мысалы, 1000 МБ деректерді өңдеу кезінде AI алгоритмдерінің шифрлау уақыты шамамен 48 секундты құрады.

Кестеде көрсетілген сандық нәтижелер негізінде алгоритмдердің өнімділігін визуалды түрде көрсету үшін график құрастырылды.



Сурет 1. – Дәстүрлі және AI негізіндегі шифрлау алгоритмдерінің өнімділігін салыстыру

1-ші суретте көлденең осьте деректер көлемі (МБ), ал тік осьте шифрлау операциясының орындалу уақыты (секунд) көрсетілген. График екі түрлі алгоритмдік тәсілді салыстыруға мүмкіндік береді: дәстүрлі криптографиялық алгоритмдер және AI негізіндегі оңтайландырылған алгоритмдер.

График нәтижелері деректер көлемі артқан сайын дәстүрлі алгоритмдердің есептеу уақыты тез өсетінін көрсетеді. Ал AI негізіндегі алгоритмдерде уақыттың өсу қарқыны біршама төмен болады. Бұл жасанды интеллект алгоритмдерінің жүйе параметрлерін динамикалық түрде бейімдеу арқылы криптографиялық процестердің тиімділігін арттыра алатынын көрсетеді.

Осылайша, жүргізілген эксперимент нәтижелері AI технологияларын криптографиялық жүйелерде қолдану деректерді өңдеу жылдамдығын арттыруға және үлкен көлемдегі ақпаратпен жұмыс істеу тиімділігін жақсартуға мүмкіндік беретінін көрсетті.

Нәтижелерді талқылау

Жүргізілген эксперимент нәтижелері жасанды интеллект технологиялары криптографиялық жүйелердің тиімділігін арттыруда маңызды рөл атқара алатынын көрсетті. Машиналық оқыту әдістері шифрлау алгоритмдерінің параметрлерін динамикалық түрде өзгерту арқылы жүйенің жұмысын оңтайландыра алады.

AI қолданудың негізгі артықшылықтарына мыналар жатады:

– криптографиялық алгоритмдердің жұмыс жылдамдығын арттыру;
– қауіпсіздік жүйелеріндегі осалдықтарды автоматты түрде анықтау;
– қауіптерге бейімделетін адаптивті жүйелер құру мүмкіндігі.

Сонымен қатар AI қолданудың белгілі бір шектеулері де бар. Машиналық оқыту модельдерін әзірлеу және оқыту үшін үлкен есептеу ресурстары қажет. Сонымен қатар қауіпсіздік жүйелерінде AI қолдану деректердің құпиялылығы мен құқықтық реттеу мәселелерін туындатуы мүмкін.

Болашақта криптография мен жасанды интеллекттің интеграциясы келесі бағыттар бойынша дамуы мүмкін:

– кванттық есептеулерге төзімді криптографиялық алгоритмдерді әзірлеу;
– адаптивті қауіпсіздік жүйелерін дамыту;
– AI негізіндегі криптоанализ әдістерін жетілдіру.

Жалпы алғанда, жүргізілген зерттеу жасанды интеллект технологиялары криптографиялық жүйелердің тиімділігін арттырудың перспективалы құралы екенін көрсетеді.

Қорытынды

Жүргізілген зерттеу криптография мен жасанды интеллект технологияларының өзара әрекеттесуі ақпараттық қауіпсіздік жүйелерін дамытуда маңызды рөл атқаратынын көрсетті. Эксперименттік талдау нәтижелері дәстүрлі криптографиялық алгоритмдер мен жасанды интеллект негізінде оңтайландырылған алгоритмдердің өнімділігі арасында айырмашылық бар екенін анықтады. Алынған нәтижелер жасанды интеллект технологияларын қолдану шифрлау процесінің тиімділігін арттыруға және деректерді өңдеу уақытын қысқартуға мүмкіндік беретінін дәлелдейді.

Сонымен қатар зерттеу барысында жасанды интеллект криптографиялық жүйелердегі осалдықтарды анықтау процесін автоматтандыруға, қауіпсіздік жүйелерінің адаптивтілігін арттыруға және ықтимал қауіптерді алдын ала анықтауға мүмкіндік беретіні анықталды. Бұл факторлар ақпараттық жүйелердің сенімділігі мен тұрақтылығын арттыруға ықпал етеді.

Сонымен бірге жасанды интеллектті криптография саласында қолдану белгілі бір қиындықтар мен шектеулерді де қамтиды. Оларға есептеу ресурстарының жоғары талаптары, машиналық оқыту модельдерін оқыту үшін үлкен деректер көлемінің қажеттілігі және қауіпсіздік жүйелерінде AI қолдануға байланысты құқықтық және этикалық мәселелер жатады.

Жалпы алғанда, криптография мен жасанды интеллекттің интеграциясы ақпараттық қауіпсіздік жүйелерінің тиімділігін арттырудың перспективалы бағыты болып табылады. Болашақ зерттеулер кванттық есептеулерге төзімді криптографиялық алгоритмдерді әзірлеуге, адаптивті қауіпсіздік жүйелерін жетілдіруге және AI негізіндегі криптографиялық әдістердің қауіпсіздігін тереңірек зерттеуге бағытталуы тиіс.

ӘДЕБИЕТТЕР ТІЗІМІ

1 Stallings W. Cryptography and Network Security: Principles and Practice. – 7th ed. – Boston: Pearson Education, 2017. – 768 p.
2 Katz J., Lindell Y. Introduction to Modern Cryptography. – 2nd ed. – Boca Raton: CRC Press, 2015. – 640 p.
3 Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C. – New York: John Wiley & Sons, 2015. — 816 p.
4 Goodfellow I., Bengio Y., Courville A. Deep Learning. – Cambridge: MIT Press, 2016. – 652 p.
5 Russell S., Norvig P. Artificial Intelligence: A Modern Approach. – 4th ed. – Boston: Pearson, 2021. – 1408 p.
6 Абдикеев Н.М., Тютюнник И.Г. Искусственный интеллект в экономике и управлении. – Москва: ИНФРА-М, 2019. – 336 с.
7 Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. – Москва: Горячая линия–Телеком, 2020. – 312 с.

8 Хорошко В.А., Азаров А.А. Основы информационной безопасности. – Москва: Либроком, 2018. – 256 с.
9 Баранов А.А. Правовые аспекты обеспечения информационной безопасности в условиях цифровизации // Информационное право. – 2020. – № 3. – С. 15–21.
10 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. – P. 120–126.
11 Daemen J., Rijmen V. The Design of Rijndael: AES – The Advanced Encryption Standard. – Berlin: Springer, 2002. – 238 p.
12 Dwork C., Roth A. The Algorithmic Foundations of Differential Privacy. – Boston: Now Publishers Inc., 2014. – 407 p.
13 Chen Y., Yu F.R., Song M., Zhang Z. Artificial Intelligence in Cyber Security: Research Advances and Challenges // IEEE Access. – 2018. – Vol. 6. – P. 35330–35341.
14 Boneh D., Shoup V. A Graduate Course in Applied Cryptography. – Stanford University, 2020. – 824 p.

REFERENCES

1 Stallings W. (2017). Cryptography and Network Security: Principles and Practice. 7th ed. – Boston: Pearson Education. – 768 p.
2 Katz J., Lindell Y. (2015). Introduction to Modern Cryptography. 2nd ed. – Boca Raton: CRC Press. – 640 p.
3 Schneier B. (2015) Applied Cryptography: Protocols, Algorithms and Source Code in C. – New York: John Wiley & Sons. – 816 p.
4 Goodfellow I., Bengio Y., Courville A. (2016). Deep Learning. – Cambridge: MIT Press. – 652 p.
5 Russell S., Norvig P. (2021). Artificial Intelligence: A Modern Approach. 4th ed. – Boston: Pearson. – 1408 p.
6 Abdikeev N.M., Tyutyunnik I.G. (2019). Iskusstvennyj intellekt v ekonomike i upravlenii. [Artificial intelligence in economics and management]. – Moscow: INFRA-M. – 336 p.
7 Malyuk A.A. (2020). Informatsionnaya bezopasnost′: kontseptual′nye i metodologicheskie osnovy zashchity informatsii. [Information Security: Conceptual and Methodological Foundations of Information Protection]. Moscow: Goryachaya Liniya-Telecom. – 312 p.
8 Khoroshko V.A., Azarov A.A. (2018). Osnovy informatsionnoj bezopasnosti. [Fundamentals of Information Security]. – Moscow: Librokom. – 256 p.
9 Baranov A.A. (2020). Pravovye aspekty obespecheniya informatsionnoj bezopasnosti v usloviyakh tsifrovizatsii. [Legal aspects of ensuring information security in the context of digitalization]. Informatsionnoe pravo – Information law. – No. 3. – P. 15-21.
10 Rivest R.L., Shamir A., Adleman L. (1978) A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM. – Vol. 21. – No. 2. – P. 120–126.
11 Daemen J., Rijmen V. (2002). The Design of Rijndael: AES – The Advanced Encryption Standard. – Berlin: Springer. – 238 p.
12 Dwork C., Roth A. (2014). The Algorithmic Foundations of Differential Privacy. – Boston: Now Publishers Inc. – 407 p.
13 Chen Y., Yu F.R., Song M., Zhang Z. (2018). Artificial Intelligence in Cyber Security: Research Advances and Challenges. IEEE Access– Vol. 6. – P. 35330–35341.
14 Boneh D., Shoup V. (2020). A Graduate Course in Applied Cryptography. – Stanford University. – 824 p.

А.Ғ. Керім[1]
[1]Евразийский национальный университет им. Л.Н. Гумилева, Казахстан

Интеграция криптографии и искусственного интеллекта: повышение эффективности систем информационной безопасности

В условиях стремительного развития цифровых технологий вопросы обеспечения безопасности данных приобретают особую актуальность. В этой связи исследование взаимодействия криптографии и технологий искусственного интеллекта становится одним из перспективных научных направлений. В данной статье рассматриваются возможности, риски и перспективы применения искусственного интеллекта в криптографических системах. Целью исследования является сравнительный анализ эффективности традиционных криптографических алгоритмов и алгоритмов, оптимизированных с использованием методов искусственного интеллекта. В ходе исследования применялось экспериментальное моделирование, в рамках которого измерялось время шифрования данных различного объема. Полученные результаты показали, что алгоритмы, оптимизированные с использованием искусственного интеллекта, демонстрируют более высокую производительность по сравнению с традиционными методами. Кроме того, использование искусственного интеллекта позволяет автоматизировать процесс обнаружения уязвимостей и повышает адаптивность систем информационной безопасности. Результаты исследования свидетельствуют о значительном потенциале интеграции криптографии и искусственного интеллекта для повышения эффективности систем защиты информации.

Ключевые слова: криптография, искусственный интеллект, информационная безопасность, алгоритмы шифрования, криптоанализ, машинное обучение, защита данных.

A.G. Kerim[1]
[1]L.N. Gumilyov Eurasian National University, Kazakhstan

Integration of cryptography and artificial intelligence: enhancing the efficiency of information security systems

The rapid development of digital technologies has significantly increased the importance of ensuring data security. In this context, the study of the interaction between cryptography and artificial intelligence has become one of the most relevant research areas. This article examines the opportunities, risks, and future prospects of applying artificial intelligence technologies in cryptographic systems. The main objective of the study is to perform a comparative analysis of the efficiency of traditional cryptographic algorithms and algorithms optimized using artificial intelligence techniques. The research is based on experimental modeling, during which the encryption time for different data volumes was measured. The obtained results demonstrate that AI-optimized algorithms provide higher performance compared to traditional methods. In addition, artificial intelligence can automate the process of identifying vulnerabilities in cryptographic systems and improve the adaptability of security mechanisms. The findings indicate that the integration of cryptography and artificial intelligence has significant potential for enhancing modern information security systems.

Key words: cryptography, artificial intelligence, information security, encryption algorithms, cryptoanalysis, machine learning, data protection, cybersecurity.

Қолжазбаның редакцияға келіп түскен күні: 31.03.2026 ж.