УДК 004.056.5:004.93
DOI https://doi.org/10.32782/2521-6643-2026-2-72.29

Свинаренко М. С., кандидат технічних наук, професор, завідувач кафедри Фотомистецтво та візуальні практики Харківської державної академії дизайну і мистецтв
ORCID: 0000-0001-9134-2759

Бондаренко Ю. В., старший викладач кафедри Аудіовізуального мистецтва
Харківської державної академії дизайну і мистецтв
ORCID: 0000-0002-3693-8282

Литвиненко Є. М., інженер ТОВ «Тереком»
ORCID: 0000-0003-3127-2255

МАТЕМАТИЧНА МОДЕЛЬ ТА ПРОГРАМНИЙ КАЛЬКУЛЯТОР ДЛЯ ОЦІНКИ ПАРАМЕТРІВ ШИФРУВАННЯ МЕДІАКОНТЕНТУ

В умовах стрімкого розвитку цифрових технологій та зростаючого обсягу мультимедійного контенту, що передається відкритими телекомунікаційними каналами, фундаментальні питання захисту інформації набувають критичного значення. Мультимедійні дані регулярно стають об'єктами кібератак та несанкціонованого доступу. Практичне застосування шифрування вимагає врахування численних технічних чинників, оскільки медіаконтент принципово відрізняється від транзакційних даних специфічними характеристиками ентропії та різним потенціалом до стиснення. Незважаючи на наявність теоретичних досліджень, наразі спостерігається дефіцит комплексних математичних моделей, здатних органічно поєднувати оцінку продуктивності, зміну розміру даних та рівень безпеки в єдину предиктивну систему, що адаптується до типу контенту. У статті представлено математичну модель та програмний калькулятор для комплексної оцінки параметрів шифрування мультимедійних даних. Розроблена предиктивна модель охоплює чотири типи медіаданих (відео, аудіо, зображення, документи) та п'ять популярних алгоритмів симетричного шифрування (AES-128, AES-256, ChaCha20, Blowfish, Twofish). Симетричне шифрування розглядається як безальтернативний вибір для масової обробки об'ємних мультимедійних файлів завдяки його високій швидкодії. Запропонований математичний апарат дозволяє точно прогнозувати розмір зашифрованого файлу, час шифрування, рівень безпеки та вимоги до обчислювальних ресурсів із середньою похибкою менш ніж 5 %. Для врахування стохастичної природи процесу обробки у модель було введено відповідну складову, що дозволило сформувати реалістичні довірчі інтервали. Крім того, у дослідженні сформульовано та розв'язано задачу багатокритеріальної оптимізації вибору алгоритму. Із застосуванням методу Парето-оптимальності та нормалізованих зважених сум забезпечено можливість гнучко балансувати між криптографічною безпекою та апаратною швидкодією. Моделі прогнозування були успішно верифіковані шляхом проведення натурних експериментів. Результати валідації довели високу точність розробленого апарату: середня квадратична похибка (RMSE) склала 0.21 с, а максимальна відносна похибка не перевищила 3.2 %. Встановлено, що розмір файлу та апаратна продуктивність мають визначальний вплив на час шифрування, тоді як вплив типу медіаконтенту є вторинним. Практична значущість роботи підтверджується розробкою програмного забезпечення – інтерактивного веб-калькулятора, який інкапсулює математичний апарат під інтуїтивно зрозумілим інтерфейсом. Цей програмний засіб реалізовано як односторінковий застосунок (SPA), що може генерувати динамічні поради, наприклад, щодо доцільності переходу до алгоритму ChaCha20 на малопотужних пристроях. Створений інструмент призначений для практичного використання фахівцями з інформаційної безпеки і може бути ефективно інтегрований у процеси DevSecOps, а також застосований архітекторами під час проектування систем відеоспостереження, платформ потокової передачі та медичних баз даних PACS.

Ключові слова: *шифрування медіаконтенту, симетричні алгоритми шифрування, AES, ChaCha20, математична модель, багатокритеріальна оптимізація, безпека даних, калькулятор шифрування.*

Svynarenko M. S., Bondarenko Y. V., Lytvynenko Y. M. Mathematical model and software calculator for evaluating media content encryption parameters

In the context of the rapid development of digital technologies and the growing volume of multimedia content transmitted over open telecommunication channels, fundamental issues of information security are of critical importance. Multimedia data regularly become targets of cyberattacks and unauthorized access. The practical application of encryption requires consideration of numerous technical factors, as media content fundamentally differs from transactional data due to its specific entropy characteristics and varying compression potential. Despite the existence of theoretical research, there is currently a

shortage of comprehensive mathematical models capable of organically combining performance evaluation, data size variation, and security levels into a single predictive system adaptable to the content type. The article presents a mathematical model and a software calculator for a comprehensive evaluation of multimedia data encryption parameters. The developed predictive model covers four types of media data (video, audio, images, documents) and five popular symmetric encryption algorithms (AES-128, AES-256, ChaCha20, Blowfish, Twofish). Symmetric encryption is considered an indispensable choice for the mass processing of large multimedia files due to its high performance speed. The proposed mathematical apparatus allows for accurate forecasting of the encrypted file size, encryption time, security level, and computational resource requirements with an average error of less than 5 %. To account for the stochastic nature of the processing, a corresponding component was introduced into the model, which allowed the formation of realistic confidence intervals. In addition, the study formulates and solves the problem of multi-criteria optimization for algorithm selection. By applying the Pareto optimality method and normalized weighted sums, the ability to flexibly balance cryptographic security and hardware performance is provided. The forecasting models were successfully verified through full-scale experiments. The validation results proved the high accuracy of the developed apparatus: the root mean square error (RMSE) was 0.21 s, and the maximum relative error did not exceed 3.2 %. It was established that the file size and hardware performance have a decisive influence on the encryption time, while the impact of the media content type is secondary. The practical significance of the work is confirmed by the development of software – an interactive web calculator that encapsulates the mathematical apparatus under an intuitive interface. This software tool is implemented as a single-page application (SPA) capable of generating dynamic recommendations, such as the feasibility of switching to the ChaCha20 algorithm on low-power devices. The created tool is intended for practical use by information security specialists and can be effectively integrated into DevSecOps processes, as well as applied by architects when designing video surveillance systems, streaming platforms, and PACS medical databases.

Key words: *media content encryption, symmetric encryption algorithms, AES, ChaCha20, mathematical model, multi-criteria optimization, data security, encryption calculator.*

Постановка проблеми. В умовах стрімкого розвитку цифрових технологій, впровадження високошвидкісних мереж зв'язку (5G/6G) та зростаючого обсягу мультимедійного контенту, що передається відкритими телекомунікаційними каналами, фундаментальні питання захисту інформації набувають критичного значення. Мультимедійні дані, зокрема відеопотоки високої роздільної здатності, цифрові медичні зображення, конфіденційні аудіозаписи та корпоративні документи, регулярно стають об'єктами кібератак та несанкціонованого доступу. Шифрування виступає одним з основних, математично надійних механізмів забезпечення конфіденційності та цілісності даних. Проте його практичне застосування в сучасних гетерогенних інформаційних системах вимагає врахування численних технічних, архітектурних та організаційних чинників. Вибір криптографічного алгоритму, об'єктивна оцінка його впливу на загальну продуктивність апаратно-програмної системи та точне прогнозування фізичних характеристик захищених файлів є складними інженерними задачами. Це зумовлено тим, що мультимедійний контент принципово відрізняється від транзакційних даних. Відео- та аудіофайли, растрові й векторні зображення мають специфічні характеристики ентропії, ступінь структурної надмірності та різний потенціал до стиснення. Зазначені параметри безпосередньо впливають на обчислювальну ефективність, споживання енергії та накладні витрати пам'яті під час виконання криптографічних перетворень [1].

Незважаючи на наявність глибоких теоретичних досліджень у галузі криптоаналізу, наразі спостерігається дефіцит комплексних математичних моделей. Більшість існуючих підходів пропонують фрагментарні рішення: вони або аналізують суто криптографічну міцність алгоритмів, або розглядають виключно апаратну швидкодію на специфічних мікроконтролерах, ігноруючи морфологію вхідних даних [2]. Практично відсутні універсальні моделі, здатні органічно поєднувати оцінку продуктивності, зміну розміру даних та рівень безпеки в єдину предиктивну систему, що динамічно адаптується до типу контенту [3]. Заповнення цієї науково-практичної прогалини є основним мотивом дослідження.

Інтеграція предиктивного моделювання з інструментами багатокритеріального прийняття рішень (MCDM) відкриває нові перспективи для створення адаптивних систем кібербезпеки [4]. Практична значущість роботи підтверджується розробкою програмного забезпечення – веб-калькулятора, який інкапсулює математичний апарат під інтуїтивно зрозумілим інтерфейсом. Цей інструмент може бути інтегрований у процеси DevSecOps та застосований архітекторами під час проектування систем відеоспостереження, медичних баз даних PACS та платформ потокової передачі.

Аналіз останніх досліджень та публікацій. Дослідженню алгоритмів симетричного та асиметричного шифрування присвячено значну кількість наукових праць. Сучасний науковий дискурс зосереджений на пошуку оптимального балансу (trade-off) між математичною стійкістю шифру та його обчислювальною ефективністю, що є критично важливим для мобільних пристроїв та мереж Інтернету речей (IoT), де ресурси жорстко лімітовані [5]. Симетричне шифрування, завдяки високій швидкодії, залишається безальтернативним вибором для масової обробки об'ємних мультимедійних файлів. Стандарт AES (Advanced Encryption Standard), прийнятий NIST у 2001 році [6], залишається найбільш застосовуваним алгоритмом блокового шифрування завдяки збалансованому поєднанню рівня безпеки та ефективності апаратної реалізації. Алгоритм AES-256 вважається де-факто стандартом для захисту даних вищого рівня. Потоковий шифр ChaCha20, запропонований Д. Дж. Бернштейном у 2008 році [7], базується на функції Salsa20. Завдяки ефективній

програмній реалізації та стійкості до атак сторонніми каналами, ChaCha20 набув широкого застосування в мобільних архітектурах. Порівняльний аналіз демонструє суттєві переваги ChaCha20 [8] на пристроях без апаратної підтримки інструкцій AES-NI. Алгоритм Blowfish, розроблений Б. Шнаєром у 1993 році [9], відрізняється змінною довжиною ключа до 448 біт та 16-раундовою мережею Фейстеля. Він забезпечує високу продуктивність під час шифрування великих обсягів даних. Його наступник, алгоритм Twofish [10], характеризується гнучкістю керування ключами. У сфері оцінки продуктивності варто виокремити роботи [11, 12], присвячені аналізу накладних витрат під час обробки потокового відео та стиснутих аудіоформатів. Встановлено, що характеристики ентропії вхідних даних суттєво впливають на загальну ефективність шифрування. Фундаментальний апарат аналізу стійкості наведено в роботі Менезеса та ін. [13], тоді як праця Фергюсона та Шнаєра [14] систематизує інженерні принципи проектування захищених інформаційних систем. Водночас у зазначених працях не представлено інтегрованого підходу до оцінки параметрів із урахуванням типу медіаконтенту, що підкреслює актуальність даного дослідження і свідчить про наявність невирішеної частини загальної проблеми. Незважаючи на наявність глибоких теоретичних досліджень у галузі криптоаналізу, наразі спостерігається дефіцит комплексних математичних моделей. Більшість існуючих підходів пропонують фрагментарні рішення: вони або аналізують суто криптографічну міцність алгоритмів, або розглядають виключно апаратну швидкодію на специфічних мікроконтролерах, ігноруючи морфологію вхідних даних [2]. Практично відсутні універсальні моделі, здатні органічно поєднувати оцінку продуктивності, зміну розміру даних та рівень безпеки в єдину предиктивну систему, що динамічно адаптується до типу контенту [3]. Заповнення цієї науково-практичної прогалини є основним мотивом дослідження. Інтеграція предиктивного моделювання з інструментами багатокритеріального прийняття рішень (MCDM) відкриває нові перспективи для створення адаптивних систем кібербезпеки [4].

Мета статті. Метою дослідження є розробка математичної моделі для комплексної оцінки параметрів шифрування медіаконтенту, яка враховує тип даних, обраний алгоритм, характеристики апаратного забезпечення та розмір файлу.

Виклад основного матеріалу. Оптимізацію логістичних та обчислювальних рішень здійснюють на основі всебічного аналізу комплексу взаємозалежних чинників. Для формалізації задачі введено систему позначень. Нехай задано множину вхідних параметрів, де S_{orig} – розмір оригінального файлу (у МБ); $M \in$ {video, audio, image, document} – тип медіаконтенту. Також $A \in$ {AES-128, AES-256, ChaCha20, Blowfish, Twofish} позначає алгоритм шифрування, а $P \in$ {low, medium, high} – рівень продуктивності пристрою. Вихідними параметрами моделі визначено: S_{enc} – розмір зашифрованого файлу (у МБ); T_{enc} – час шифрування (у секундах); L_{sec} – рівень безпеки; R_{comp} – вимоги до обчислювальних ресурсів. Для кожного алгоритму A_i визначається вектор характеристик $C_A = \{k_A, \sigma_A, \omega_A, \lambda_A\}$, де k_A – довжина ключа (у бітах), σ_A – коефіцієнт безпеки в діапазоні [0, 5], ω_A – коефіцієнт накладних витрат в діапазоні[1.0, 1.1], λ_A – коефіцієнт швидкості обробки в діапазоні[0.5, 2.0]. Базові характеристики наведено у таблицях 1 та 2.

Таблиця 1

Характеристики алгоритмів шифрування

Алгоритм	k_A (біт)	σ_A	ω_A	λ_A	Тип шифру
AES-128	128	4.0	1.01	1.2	Блоковий
AES-256	256	5.0	1.02	1.0	Блоковий
ChaCha20	256	4.5	1.01	1.3	Потоковий
Blowfish	448	3.5	1.03	1.5	Блоковий
Twofish	256	4.5	1.02	1.1	Блоковий

Таблиця 2

Характеристики типів медіаконтенту

Тип медіа	Overhead (ω_M)	Час. множник (τ_M)	Рекомендований алгоритм
Video	1.01	1.1	AES-256
Audio	1.02	1.0	ChaCha20
Image	1.03	0.9	AES-256
Document	1.05	0.8	AES-256

Розмір зашифрованого файлу обчислюється як добуток оригінального обсягу даних на коефіцієнти накладних витрат алгоритму та типу медіа:

$$S_{enc} = S_{orig} \cdot \omega_A \cdot \omega_M \cdot (1 + \varepsilon),$$

де ε – коефіцієнт додаткових метаданих (вектор ініціалізації IV, код автентифікації MAC, заголовки):

$$\varepsilon = \alpha + \beta \cdot \frac{\log_2(k_A)}{S_{orig}},$$

де $\alpha = 0.016$ МБ – базовий розмір заголовків, $\beta = 0.002$ МБ – розмір даних, що залежить від довжини ключа. Відносне збільшення розміру файлу визначається як:

$$\Delta S = \frac{S_{enc} - S_{orig}}{S_{orig}} \times 100\ \%.$$

Аналітичні розрахунки свідчать, що для файлів обсягом від 1 МБ відносне збільшення не перевищує 5–6 %. Час шифрування моделюється у вигляді функції від розміру файлу, швидкості алгоритму та продуктивності пристрою:

$$T_{enc} = S_{orig} \cdot \lambda_A \cdot \mu_P \cdot \left(\frac{\tau_M}{\gamma} \right),$$

де $\gamma = 10$ МБ/с – базова швидкість шифрування, а $\mu_P \in \{3.0_{low}, 1.0_{medium}, 0.5_{high}\}$ – множник продуктивності пристрою. Час дешифрування апроксимується як $T_{dec} \approx 0.9 \cdot T_{enc}$. Для врахування стохастичної природи процесу T_{enc} розглядається як нормально розподілена величина з $\sigma_T = 0.15 \cdot \mu_T$ та довірчим інтервалом:

$$CI_{95\ \%} = [\mu_T - 1.96 \cdot \sigma_T,\ \mu_T + 1.96 \cdot \sigma_T].$$

Рівень безпеки формалізується як комбінація криптографічної стійкості алгоритму та ефективної довжини ключа:

$$L_{\text{sec}} = \sigma_A \cdot \left(1 + \frac{\log_2(k_A)}{256} \right).$$

Класифікація: $L_{sec} < 3.0$ – Низький; $3.0 \le L_{sec} < 4.0$ – Середній; $4.0 \le L_{sec} < 4.8$ – Високий; $L_{sec} \ge 4.8$ – Дуже високий. Стійкість до атак повним перебором оцінюється через ймовірність успішного злому за час t:

$$P_{break}(t) = 1 - \exp\left(-t \cdot \frac{v}{2^{k_A}} \right),$$

де $v \approx 10^{12}$ ключів/с. Для AES-256 досягнення 50 % ймовірності злому становить близько 1.26×10^{53} років. Вимоги до обчислювальних ресурсів моделюються за допомогою виразу:

$$R_{comp} = \lambda_A \cdot \mu_P \cdot \left(\frac{S_{orig}}{10} \right).$$

Рівні: $R_{comp} < 0.5$ (дуже низькі), $0.5 \le R_{comp} < 1.0$ (низькі), $1.0 \le R_{comp} < 2.0$ (середні); $2.0 \le R_{comp} < 5.0$ (високі), $R_{comp} \ge 5.0$ (дуже високі). Просторова складність становить $\mathcal{O}(B + k_A)$, де $B = 16$ байт; часова складність є лінійною: $\mathcal{O}(S_{orig})$.

Визначається вектор критеріїв оптимізації $f(A, P) = [T_{enc}, S_{enc} - S_{orig}, -L_{sec}]^T$, де перші два критерії мінімізуються, а третій максимізується. Розв'язок визнається Парето-оптимальним, якщо не існує іншого розв'язку, здатного покращити принаймні один критерій без погіршення решти. Застосовується метод нормалізованих зважених сум:

$$f_i' = \frac{f_i - f_i^{\min}}{f_i^{\max} - f_i^{\min}}.$$

Агрегація цільової функції набуває вигляду:

$$F_{agg}(A, P) = w_1 \cdot f_1' + w_2 \cdot f_2' + w_3 \cdot f_3', \quad \text{де } \sum w_i = 1.$$

Оптимізаційна задача розв'язується методом повного перебору по всіх 15 комбінаціях. Верифікацію здійснено шляхом натурних експериментів (Intel Core i5, 16 ГБ ОЗП, Ubuntu 22.04 LTS). Результати подано у таблиці 3.

Середня квадратична похибка (RMSE) склала 0.21 с, а максимальна відносна похибка не перевищила 3.2 %. Розмір файлу та продуктивність мають визначальний вплив на час шифрування; вплив типу медіа є вторинним. Програмний засіб реалізовано як односторінковий застосунок (SPA) з використанням нативного JavaScript без сторонніх залежностей. Архітектура побудована за модульним принципом. Структура даних algorithmInfo містить параметри алгоритмів, mediaTypeFactors – характеристики медіа, а performanceMultipliers – вагові коефіцієнти. Інтерфейс (див. рис. 1) включає панель конфігурації, панель результатів, гістограму, вкладку детальної статистики та рекомендацій. Підсистема генерує динамічні

Таблиця 3

Порівняння модельних та експериментальних значень

Тип медіа	Розмір (МБ)	Алгоритм	T_{model} (с)	T_{exp} (с)	Похибка (%)
Video	100	AES-256	10.0	9.8	2.0
Audio	50	ChaCha20	6.5	6.3	3.2
Image	25	AES-256	2.25	2.3	2.2
Document	10	AES-256	0.8	0.82	2.4

поради (наприклад, перехід до ChaCha20 на малопотужних пристроях). Цей інструмент може бути інтегрований у процеси DevSecOps та застосований архітекторами під час проектування систем відеоспостереження, медичних баз даних PACS та платформ потокової передачі.

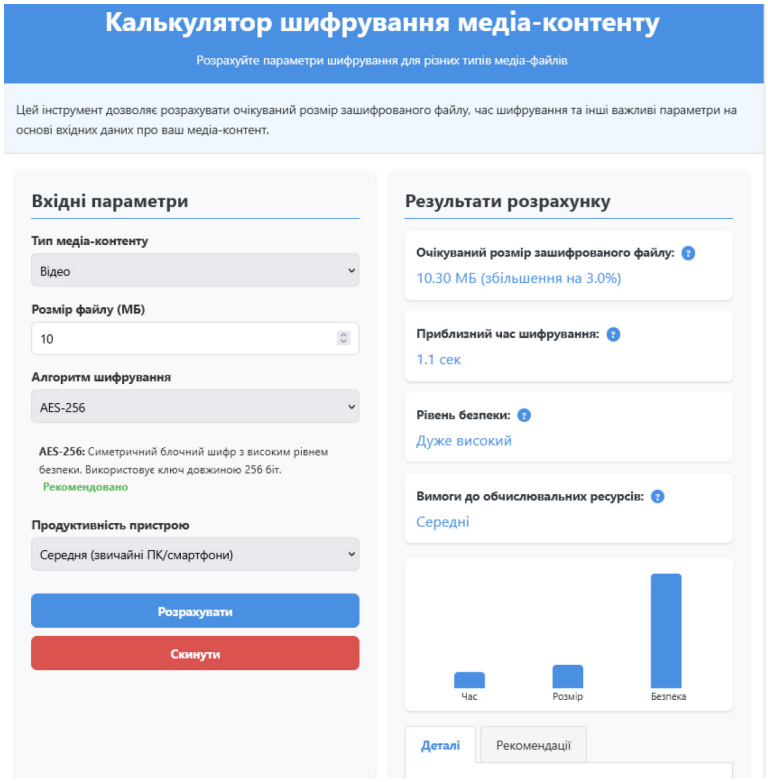

Рис. 1. Інтерфейс програмного засобу

Висновки з дослідження і перспективи подальших розвідок у цьому напрямі. У дослідженні розроблено математичну модель для оцінки параметрів шифрування медіаконтенту, що покриває п’ять алгоритмів та чотири типи даних. Моделі прогнозування розміру, часу виконання, безпеки та вимог успішно верифіковані (максимальна похибка 3.2 %). Розв’язано задачу багатокритеріальної оптимізації. Використання методів Парето-оптимальності та зважених сум надає можливість балансувати між безпекою та швидкодією. Введення стохастичної складової дозволило сформувати реалістичні довірчі інтервали. Створено програмний продукт (веб-калькулятор), який дозволяє оптимізувати параметри шифрування в режимі реального часу. Перспективні напрями подальших досліджень:

– Інтеграція методів машинного навчання для адаптивного уточнення коефіцієнтів.

– Розширення для підтримки асиметричних криптографічних схем та імплементація постквантових алгоритмів.

– Адаптація під специфіку хмарних архітектур.

Список використаних джерел:

1. Shifa A. et al. Lightweight Cipher for H.264 Videos in the Internet of Multimedia Things with Encryption Space Ratio Diagnostics. *Sensors*. 2019. Vol. 19, No. 5. Art. 1228. DOI: https://doi.org/10.3390/s19051228

2. Martínez Guevara L. M. et al. Analysis and comparison of encryption and verification algorithms. *Journal of Information and Telecommunication*. 2024. Vol. 9, No. 2. P. 173–189. DOI: https://doi.org/10.1080/24751839.2024.2411884

3. Kadakia Y. A. et al. Encrypted Model Predictive Control of a Nonlinear Chemical Process Network. *Processes*. 2023. Vol. 11, Iss. 8. Art. 2501. DOI: https://doi.org/10.3390/pr11082501

4. Zhou Y., Asano A. A Two-Layer Model for Complex Multi-Criteria Decision-Making. *Applied System Innovation*. 2025. Vol. 8, Iss. 5. Art. 148. DOI: https://doi.org/10.3390/asi8050148

5. Dungog J. M. A Python-Based Simulation and Security Analysis of ChaCha20 and AES. *IJFMR*. 2025. Vol. 7, Iss. 6. Art. 61473. DOI: https://doi.org/10.36948/ijfmr.2025.v07i06.61473

6. NIST. Advanced Encryption Standard (AES). *FIPS PUB 197*. Gaithersburg, 2001. DOI: https://doi.org/10.6028/NIST.FIPS.197

7. Bernstein D. J. ChaCha, a variant of Salsa20. *Workshop Record of SASC*. 2008. P. 1–6.

8. Nir Y., Langley A. ChaCha20 and Poly1305 for IETF Protocols. RFC 7539. *IETF*. 2015. DOI: https://doi.org/10.17487/RFC7539

9. Schneier B. Description of a New Variable-Length Key, 64-bit Block Cipher (Blowfish). *Fast Software Encryption*. Springer. 2005. P. 191–204. DOI: https://doi.org/10.1007/3-540-58108-1_24

10. Schneier B. et al. Twofish: A 128-Bit Block Cipher. *AES Submission*. 1998.

11. Priyanka M., Arun V. Performance Analysis of Symmetric Encryption Algorithms. *IJCSNS*. 2021. Vol. 21, No. 4. P. 114–120. DOI: https://doi.org/10.54938/ijemdcsai.2024.03.1.268

12. Al-Hazaimeh O. M. Chaotic based multimedia encryption: a survey for network and internet security. *Bulletin of Electrical Engineering and Informatics*. 2022. Vol. 11, No. 4. P. 2151-2159. DOI: https://doi.org/10.11591/eei.v11i4.3520

13. Menezes A. J. et al. Handbook of Applied Cryptography. CRC Press, 1997. DOI: https://doi.org/10.1201/9780429466335

14. Ferguson N., Schneier B., Kohno T. Cryptography Engineering: Design Principles and Practical Applications. Wiley Publishing, 2010. DOI: https://doi.org/10.1002/9781118722367

15. Stallings W. Cryptography and Network Security. 8th ed. Pearson, 2022.

References:

1. Shifa, A., Asghar, M. N., Noor, S., Gohar, N., & Fleury, M. (2019). Lightweight Cipher for H.264 Videos in the Internet of Multimedia Things with Encryption Space Ratio Diagnostics. *Sensors*, *19*(5), 1228. https://doi.org/10.3390/s19051228

2. Martínez Guevara, L. M., et al. (2024). Analysis and comparison of encryption and verification algorithms. *Journal of Information and Telecommunication*, 9(2), 173–189. https://doi.org/10.1080/24751839.2024.2411884

3. Kadakia, Y. A., et al. (2023). Encrypted Model Predictive Control of a Nonlinear Chemical Process Network. *Processes*, *11*(8), 2501. https://doi.org/10.3390/pr11082501

4. Zhou, Y., & Asano, A. (2025). A Two-Layer Model for Complex Multi-Criteria Decision-Making and Its Application in Institutional Research. *Applied System Innovation*, *8*(5), 148. https://doi.org/10.3390/asi8050148

5. Dungog, J. M. (2025). A Python-Based Simulation and Security Analysis of ChaCha20 and AES. *IJFMR*, 7(6), 61473. https://doi.org/10.36948/ijfmr.2025.v07i06.61473

6. NIST. (2001). Advanced Encryption Standard (AES). *FIPS PUB 197*. Gaithersburg. https://doi.org/10.6028/NIST.FIPS.197

7. Bernstein, D. J. (2008). ChaCha, a variant of Salsa20. *Workshop Record of SASC 2008*, 1–6.

8. Nir, Y., & Langley, A. (2015). ChaCha20 and Poly1305 for IETF Protocols. RFC 7539. *IETF*. https://doi.org/10.17487/RFC7539

9. Schneier, B. (2005). Description of a New Variable-Length Key, 64-bit Block Cipher (Blowfish). *Fast Software Encryption*, Springer, 191–204. https://doi.org/10.1007/3-540-58108-1_24

10. Schneier, B., et al. (1998). Twofish: A 128-Bit Block Cipher. *AES Submission*.

11. Priyanka, M., & Arun, V. (2021). Performance Analysis of Symmetric Encryption Algorithms. *IJCSNS*, 21(4), 114–120. https://doi.org/10.54938/ijemdcsai.2024.03.1.268

12. Al-Hazaimeh, O. M. (2022). Chaotic based multimedia encryption: a survey for network and internet security. *Bulletin of Electrical Engineering and Informatics* 11 (4), 2151-2159. https://doi.org/10.11591/eei.v11i4.3520

13. Menezes, A. J., et al. (1997). Handbook of Applied Cryptography. CRC Press. https://doi.org/10.1201/9780429466335

14. Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography Engineering: Design Principles and Practical Applications. Wiley Publishing. https://doi.org/10.1002/9781118722367

15. Stallings, W. (2022). Cryptography and Network Security (8th ed.). Pearson.

Дата першого надходження статті до видання: 03.03.2026
Дата прийняття статті до друку після рецензування: 10.04.2026
Дата публікації (оприлюднення) статті: 30.05.2026