УДК 004.056.55:004.312.2
DOI https://doi.org/10.32782/2663-5941/2025.6.2/31

Мельник Р.П.
Національного університету цивільного захисту України

Мельник О.Г.
Національного університету цивільного захисту України

МЕТОДИКА ОЦІНКИ КРИПТОСТІЙКОСТІ ТА ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ В УМОВАХ СУЧАСНИХ КІБЕРЗАГРОЗ

У статті представлено результати дослідження, спрямованого на розробку та апробацію інтегрованої методики кількісної оцінки криптостійкості та захищеності інформаційно-комунікаційних систем у сучасних умовах. Актуальність дослідження зумовлена військовою агресією проти України, що супроводжується масштабними кібератаками на державні установи та об'єкти критичної інфраструктури, а також стрімким розвитком новітніх технологій, зокрема штучного інтелекту та постквантових обчислень. У роботі наголошено на проблемі недосконалості чинної нормативно-правової бази у сфері захисту інформації, яка не враховує специфіки воєнного часу і потребує адаптації до нових викликів.

Запропонована методика передбачає використання інтегрального показника, що об'єднує криптографічні, організаційні, технічні та експлуатаційні параметри в єдину формулу. Оцінювання здійснюється на основі нормування ключових характеристик: довжини криптографічного ключа, стійкості алгоритмів, ефективності політики безпеки, рівня фізичного захисту, своєчасності оновлення програмного забезпечення, готовності до реагування на інциденти, кількості та часу відкритості вразливостей, а також ефективності потенційних атак. Запропоновано шкалу інтерпретації результатів, що дозволяє визначати рівень захищеності системи від низького до дуже високого.

Апробація методики проведена на прикладі трьох сценаріїв, які відображають різний рівень організації захисту: державного центру обробки даних, муніципальної інформаційної системи та підприємства критичної інфраструктури в умовах воєнного часу. Отримані результати підтвердили ефективність запропонованої моделі та її чутливість до змін ключових параметрів. Було встановлено, що найбільший вплив на рівень безпеки мають своєчасність оновлення програмного забезпечення, кількість вразливостей і тривалість їх існування, а також готовність до реагування на інциденти.

Практичне значення дослідження полягає у створенні інструменту, придатного для використання державними органами, підприємствами критичної інфраструктури та експертними установами з метою проведення аудиту, сертифікації і вдосконалення політик захисту інформації. Запропонований підхід може стати основою для оновлення національних стандартів і гармонізації їх з міжнародними вимогами, що є критично важливим у контексті сучасних кіберзагроз і війни.

Ключові слова: *криптостійкість, захищеність, інформаційна система, кібератаки, штучний інтелект, постквантові обчислення, вразливості, кіберзахист, інформаційна безпека, воєнний час.*

Постановка проблеми. Сучасні інформаційно-комунікаційні системи (ІКС) є фундаментом функціонування державного управління, сектору безпеки й оборони, фінансових установ та критичної інфраструктури. В умовах повномасштабної збройної агресії російської федерації проти України питання їхньої захищеності набуває особливої актуальності. Хакерські атаки, які здійснюють російські угруповання проти органів державної влади, енергетичних компаній, транспортних і комунікаційних систем, стали невід'ємною складовою гібридної війни. Вони спрямовані на дестабілізацію суспільних процесів, порушення роботи критичної інфраструктури та підрив національної безпеки.

Додатковим викликом стає стрімкий розвиток новітніх технологій. По-перше, це квантові обчислення, які ставлять під загрозу стійкість класичних криптографічних алгоритмів. По-друге, це широке впровадження штучного інтелекту, який з одного боку відкриває нові можливості для захисту інформації (інтелектуальні системи вияв-

лення атак, прогнозування ризиків), а з іншого – надає зловмисникам інструменти для автоматизації кібератак і підвищення їхньої ефективності.

Важливою проблемою залишається і недосконаліть нормативної бази у сфері захисту інформації в Україні. Наявні документи здебільшого зосереджуються на формальних вимогах до організації інформаційної безпеки або містять критерії, які не дозволяють здійснювати комплексну кількісну оцінку рівня криптостійкості та захищеності ІКС. Це ускладнює як порівняння різних систем між собою, так і визначення слабких місць у їхній архітектурі.

Таким чином, виникає потреба у створенні методики, яка б дозволила поєднати технічні, алгоритмічні та організаційно-технічні аспекти захисту інформації в єдину інтегральну модель. Її застосування має забезпечити можливість кількісного оцінювання рівня безпеки, визначення вразливих компонентів і підвищення загальної стійкості українських ІКС до кіберзагроз у сучасних умовах війни та швидкої еволюції технологій.

Аналіз останніх досліджень і публікацій. У 2020-2025 рр. українська та зарубіжна наукова література активно розвивала тематику оцінки інформаційної безпеки й криптостійкості в умовах швидких технологічних змін та загострення геополітичних ризиків. Українські дослідники приділяли особливу увагу проблемам практичної імплементації постквантових рішень, якості генераторів псевдовипадкових чисел (ГПВЧ/CSPRNG), а також адаптації процесів управління ключами і процедур оновлення ПЗ під умови воєнного часу й атак на критичну інфраструктуру [1-5].

Дослідження щодо генераторів псевдовипадкових чисел та їх оцінки (кількісні критерії ентропії, стійкість до криптоаналізу) є численними у вітчизняних публікаціях 2021-2025 рр. Автори розглядають як алгоритмічні (програмні) підходи, так і використання фізичних джерел ентропії для вбудованих/IoT-систем, де слабкий ГПВЧ може стати «однією з найслабших ланок» захисту навіть при застосуванні сучасних шифрів [6-8]. Це підкреслює необхідність включення компонентних метрик у загальну оцінку криптостійкості.

Воєнний контекст, зокрема повномасштабна агресія росії проти України, значно змінив пріоритети наукових та прикладних досліджень. Моніторинги та аналітичні звіти документують постійні операції по підриву функціонування держустанов і критичної інфраструктури через кібератаки – від DDoS і компрометації вебсервісів до складних операцій з руйнуванням даних та впливом на енергосистеми [9-12]. Це створює вимогу до оцінки не тільки криптографічної «теоретичної» стійкості, але й оперативної резильєнтності системи в умовах тривалих атак і фізичних загроз.

Міжнародна література і стандарти також еволюціонують: систематичні огляди постквантової криптографії, звіти NIST і практичні роботи з імплементації PQC підкреслюють, що перехід буде поетапним і потребує інструментів для оцінки ризиків і пріоритетності міграції [13-14]. У той самий час міжнародні огляди ризиків і оцінки безпеки показують розбіжність методів (кількісні проти якісних), що ускладнює міжнародну гармонізацію практик і їхню адаптацію у національних умовах [15].

Окрему проблему становить швидкий розвиток штучного інтелекту (ШІ): з одного боку, ШІ-методи істотно посилюють можливості систем виявлення аномалій і автоматизації реагування; з іншого – вони дають зловмисникам інструменти для автоматичної генерації експлойтів, інтелектуального фішингу й оптимізації атак [16-17]. Це вимагає врахування впливу моделей ML/AI на ефективність атак при моделюванні ризиків і тестуванні стійкості.

Нормативна база в Україні (й інструменти оцінки за національними документами) частково відстає від сучасних загроз: нормативи часто орієнтовані на формальні процедури та контроль доступу, але дають недостатньо вимірних критеріїв для оцінки криптостійкості компонентів (наприклад, CSPRNG, менеджмент ключів, апаратні HSM) або для врахування постквантових ризиків. Окремі вітчизняні роботи закликають до модернізації підходів і інтеграції кількісних показників у процедури аудиту й сертифікації [18-19].

Аналіз літератури виявляє такі ключові проблеми:

1. Відсутність єдиної кількісної методики, яка б інтегрувала алгоритмічні, компонентні та організаційно-технічні показники у вимірний індекс криптостійкості.

2. Недостатнє врахування воєнного контексту у більшості моделей ризику: потрібна інтеграція показників оперативної резильєнтності, готовності реакції та тривалості експозиції вразливостей.

3. Потреба в методах пріоритизації переходу на постквантові рішення, які б базувалися на кількісній оцінці ризику (включно з економічними та експлуатаційними обмеженнями).

4. Вплив компонентних факторів (CSPRNG, менеджмент ключів, апаратні модулі) на загальну стійкість, підтверджений експериментальними роботами українських науковців.

5. Зростання ролі ШІ як двозначного фактора (захист/атака), що вимагає нових критеріїв при моделюванні ефективності атак і стійкості детекторів.

Отже, з теоретичного й практичного погляду існує обґрунтована потреба в розробці комплексної кількісної методики оцінки криптостійкості та загальної захищеності ІКС, яка б ураховувала алгоритмічні та компонентні метрики, експлуатаційну резильєнтність у воєнному середовищі, вплив ШІ та вимоги до постквантової міграції. Саме ця проблема становитиме предмет подальшого дослідження в роботі.

Постановка завдання. Метою даного дослідження є розробка інтегрованої методики кількісної оцінки криптостійкості та загальної захищеності ІКС, яка враховує сучасні виклики – військову агресію проти України, масштабні кібератаки на критичну інфраструктуру, швидкий розвиток штучного інтелекту та постквантових обчислень, а також недосконаліть чинної нормативно-правової бази. Запропонована методика повинна забезпечувати можливість об'єктивного вимірювання рівня безпеки ІКС, виявлення вразливих компонентів і формування практичних рекомендацій щодо підвищення їхньої стійкості.

Для досягнення мети дослідження передбачається вирішити такі завдання:

1. Систематизація наукових підходів до оцінки криптостійкості та інформаційної безпеки за останні роки (2020–2025), зокрема українських і міжнародних напрацювань.

2. Визначення ключових критеріїв оцінки, які охоплюють алгоритмічні, компонентні та організаційно-технічні фактори, а також показники резильєнтності системи в умовах воєнних загроз.

3. Формалізація інтегрального показника захищеності у вигляді математичної моделі, що поєднує зазначені фактори в єдиний індекс.

4. Розробка методики нормування параметрів і градацій для коректної інтерпретації результатів оцінки.

5. Апробація запропонованої методики на прикладних сценаріях, що відображають умови воєнного часу в Україні (атаки на державні органи та критичну інфраструктуру).

6. Порівняння результатів оцінки з існуючими методами, а також аналіз практичної доцільності інтеграції підходу в аудит, сертифікацію та практику управління інформаційною безпекою.

7. Формування рекомендацій для вдосконалення нормативно-правової бази України у сфері захисту інформації та узгодження її з міжнародними стандартами.

Таким чином, дослідження спрямоване не лише на розробку теоретичної моделі, а й на створення практичного інструментарію, придатного для застосування у вітчизняних умовах. Його результати можуть бути використані державними органами, підприємствами критичної інфраструктури та експертними організаціями для кількісної оцінки рівня безпеки та визначення пріоритетів у підвищенні криптостійкості інформаційних систем.

Виклад основного матеріалу. Для кількісного визначення рівня захищеності ІКС запропоновано інтегральний показник S, що враховує ключові параметри системи:

$$S = \frac{K \times A \times P \times F \times U \times R}{V \times E \times L}. \quad (1)$$

де K – довжина криптографічного ключа (біт);
A – надійність алгоритму (0–1), яка визначається за результатами криптоаналізу та експертних оцінок;
P – ефективність політики безпеки (0–1), що включає процедури контролю доступу, управління ключами та аудит;
F – рівень фізичного захисту (0–1), включно з організаційними заходами;
U – своєчасність оновлення програмного забезпечення (0–1);
R – готовність системи до реагування на інциденти (0–1);
V – кількість виявлених вразливостей (шт.);
E – ефективність потенційних атак (1–10);
L – час відкритості вразливостей до усунення (дні).

Для забезпечення коректності розрахунку всі параметри моделі приводяться до безрозмірних величин у діапазоні [0;1] або мають дискретні інтервали оцінки. Зокрема, нижче представлена таблиця градації параметрів (вхідних коефіцієнтів) (табл. 1).

Для аналізу отриманих значень інтегрального показника S пропонується шкала (табл. 2).

Запропонована формула дозволяє поєднати в єдиному показнику різні аспекти інформаційної безпеки: криптографічні (довжина ключа, стійкість алгоритму), організаційно-технічні (політика безпеки, фізичний захист, оновлення ПЗ, реагування на інциденти) та експлуатаційні (кількість і час відкритості вразливостей, ефективність атак). Такий підхід забезпечує комплексність оцінки та дозволяє проводити як порівняльний аналіз різних систем, так і виявлення «вузьких місць» у конкретній ІКС.

Таким чином, матеріали та методи дослідження спрямовані на формування уніфікованої системи критеріїв, здатної об'єктивно оцінювати стан захищеності ІКС у сучасних умовах воєнних загроз та швидкої технологічної еволюції.

Таблиця 1

Градація параметрів (вхідних коефіцієнтів)

Позначення	Параметр	Значення	Оцінка
K	Довжина ключа	≤128	Низька криптостійкість
		192	Середня криптостійкість
		≥256	Висока криптостійкість
A	Надійність алгоритму (0–1)	≤0.4	Ненадійний
		0.5–0.8	Помірно надійний
		0.9–1.0	Високонадійний
P	Політика безпеки (0–1)	≤0.5	Слабка
		0.6–0.8	Середня
		0.9–1.0	Сильна
F	Фізичний захист (0–1)	≤0.5	Мінімальний
		0.6–0.8	Помірний
		0.9–1.0	Високий
U	Рівень оновлення ПЗ (0–1)	≤0.5	Рідкі оновлення
		0.6–0.8	Часткове оновлення
		0.9–1.0	Своєчасне оновлення
R	Реакція на інциденти (0–1)	≤0.5	Немає системи реагування
		0.6–0.8	Частково готова система
		0.9–1.0	Повноцінна реакція
V	Кількість вразливостей	≥10	Високий ризик
		5–9	Середній ризик
		0–4	Низький ризик
E	Ефективність атаки (1–10)	≥7	Дуже ефективна атака
		4–6	Потенційно ефективна
		1–3	Низька ефективність
L	Дні відкритості вразливості	≥30	Критична вразливість
		7–29	Середньої тривалості
		≤6	Швидко закривається

Таблиця 2

Градація результату (показника S)

Значення S	Класифікація захищеності
S < 0.5	Низький рівень захисту
0.5 ≤ S < 1.5	Середній рівень
1.5 ≤ S < 3.0	Достатній рівень
3.0 ≤ S < 5.0	Високий рівень
S ≥ 5.0	Дуже високий рівень

Для практичного використання інтегральної формули для кількісної оцінки рівня захищеності ІКС необхідно деталізувати алгоритм застосування формули, визначити порядок збору даних для параметрів, встановити механізми нормування та продемонструвати приклади її використання на реальних сценаріях.

Методика оцінки передбачає послідовність таких дій:

1. Визначення початкових параметрів системи (ключі, алгоритми, політики, інфраструктурні засоби).
2. Оцінка параметрів за допомогою експертних або автоматизованих методів (сканери вразливостей, аудит політик безпеки, тестування стійкості алгоритмів).
3. Нормування отриманих значень до єдиної шкали відповідно до критеріїв.
4. Підстановка даних у формулу інтегрального показника (1).
5. Інтерпретація результату за шкалою (від низького до дуже високого рівня захищеності).
6. Формування рекомендацій для підвищення безпеки системи, базованих на найбільш слабких параметрах.

Джерела даних для оцінки параметрів:

- **K, A:** визначаються шляхом аналізу застосованих криптографічних алгоритмів і довжини ключів; враховуються міжнародні рекомендації (NIST, ENISA).
- **P:** оцінюється через аудит політики доступу, управління ключами, фіксація подій.
- **F:** визначається за стандартами фізичного захисту приміщень і обладнання (наприклад, ISO/IEC 27001).
- **U:** оцінюється частотою та своєчасністю оновлень ПЗ.

• **R:** визначається наявністю планів реагування на інциденти та відпрацьованістю процедур CSIRT/CERT.

• **V, E, L:** встановлюються за результатами сканування вразливостей (наприклад, Nessus, OpenVAS), статистикою зловживань і часовими даними про закриття уразливостей.

Розглянемо приклади сценаріїв застосування.

Сценарій 1. Добре захищена система (державний центр обробки даних).

• K = 256; A = 1.0; P = 0.9; F = 0.9; U = 0.95; R = 1.0;

• V = 2; E = 3; L = 7.

Результат:

$$S = \frac{256 \times 1.0 \times 0.9 \times 0.9 \times 0.95 \times 1.0}{2 \times 3 \times 7} \approx 5.2$$

що відповідає дуже високому рівню захисту.

Сценарій 2. Система з низьким рівнем оновлення ПЗ (муніципальна ІКС).

• K = 192; A = 0.8; P = 0.7; F = 0.7; U = 0.4; R = 0.6;

• V = 6; E = 5; L = 25.

Результат:

$$S = \frac{192 \times 0.8 \times 0.7 \times 0.7 \times 0.4 \times 0.6}{6 \times 5 \times 25} \approx 0.51$$

що відповідає середньому рівню захисту, з критичною вразливістю у параметрі U (оновлення).

Сценарій 3. Система з високою кількістю вразливостей (енергетична компанія у воєнний час).

• K = 256; A = 0.9; P = 0.8; F = 0.6; U = 0.7; R = 0.8;

• V = 12; E = 7; L = 30.

Результат:

$$S = \frac{256 \times 0.9 \times 0.8 \times 0.6 \times 0.7 \times 0.8}{12 \times 7 \times 30} \approx 0.19$$

що відповідає низькому рівню захисту, з основним ризиком через велику кількість невиправлених вразливостей.

Таким чином, методика дозволяє:

– кількісно оцінювати рівень захищеності різних систем;

– ідентифікувати критичні слабкі параметри;

– проводити порівняльний аналіз у динаміці (наприклад, до і після впровадження заходів безпеки);

– формувати рекомендації для вдосконалення політик та технічних рішень.

Запропонований підхід має прикладне значення для державних установ, підприємств критичної інфраструктури та приватного сектору, забезпечуючи об'єктивність і прозорість у процесі аудиту й сертифікації інформаційної безпеки.

Для перевірки запропонованої методики було проведено апробацію на низці умовних сценаріїв, які відображають різні рівні організації захисту ІКС в Україні. Дослідження охоплювало державні установи, муніципальні інформаційні системи та підприємства критичної інфраструктури, що дозволило протестувати модель на різних класах об'єктів.

Для трьох сценаріїв (див. попередній розділ) було сформовано узагальнені дані з розрахунком показника *S* табл 3.

Отже, державний центр обробки даних продемонстрував дуже високий рівень захисту (S > 5), що забезпечується поєднанням сучасних криптоалгоритмів, надійної політики безпеки та мінімальної кількості вразливостей. Муніципальна ІКС отримала лише середній рівень захисту, при цьому головним чинником зниження стійкості стала відсутність системних оновлень та недостатня готовність до реагування на інциденти. Енергетична компанія у воєнних умовах виявила найнижчий показник (S = 0.19), що пояснюється великою кількістю невиправлених вразливостей, високою ефективністю атак і тривалим часом їх відкритості.

Таблиця 3

Узагальнені дані перевірки запропонованої методики

Сценарій	Характеристика	Основні параметри	Значення S	Рівень захисту	Ключові проблеми
1. Державний центр обробки даних	Високий рівень безпеки, застосування сучасних криптоалгоритмів та процедур	K=256; A=1.0; P=0.9; F=0.9; U=0.95; R=1.0; V=2; E=3; L=7	5.2	Дуже високий	Практично відсутні
2. Муніципальна ІКС	Обмежені ресурси, несвоєчасні оновлення ПЗ	K=192; A=0.8; P=0.7; F=0.7; U=0.4; R=0.6; V=6; E=5; L=25	0.51	Середній	Відсутність оновлень, слабка реакція
3. Енергетична компанія (воєнний час)	Висока кількість невиправлених вразливостей, активні кібератаки	K=256; A=0.9; P=0.8; F=0.6; U=0.7; R=0.8; V=12; E=7; L=30	0.19	Низький	Вразливості, тривале їх існування

Було проведено оцінку впливу зміни окремих параметрів на інтегральний показник. Для сценарію 2 (муніципальна ІКС) підвищення параметра U (оновлення ПЗ) з 0.4 до 0.9 дало приріст значення S з 0.51 до 1.14, що перевело систему з нижнього порогу середнього рівня захисту ближче до достатнього. Це підтверджує ключову роль оновлень у сучасних умовах. У сценарії 3 (енергетична компанія) зменшення кількості вразливостей з 12 до 5 (за рахунок своєчасних оновлень і патчів) дозволило підвищити S з 0.19 до 0.45, що хоч і не виводить систему з категорії низького рівня, проте істотно покращує її позицію.

Отримані результати підтвердили, що методика є чутливою до змін ключових параметрів і дозволяє точно визначати слабкі місця в системі. Вона надає можливість:

– визначати критичні напрями підвищення безпеки;

– порівнювати рівень захищеності між різними організаціями;

– моделювати ефективність впровадження окремих заходів (наприклад, скорочення часу усунення вразливостей).

Таким чином, апробація підтвердила практичну придатність методики для використання у державному секторі, на підприємствах критичної інфраструктури та в організаціях, що працюють із чутливою інформацією.

Результати апробації показали, що розроблена методика дозволяє комплексно оцінювати стан захищеності ІКС з урахуванням як криптографічних характеристик, так і організаційно-технічних чинників. На відміну від існуючих підходів, які здебільшого фокусуються на якісному аналізі або оцінюють лише окремі аспекти (наприклад, стійкість криптоалгоритмів чи ефективність політик доступу), запропонована модель об'єднує різні параметри в єдиний інтегральний показник. Це робить її придатною для кількісного порівняння систем різного класу та різних організацій.

Особливу цінність модель має в Україні, яка з 2022 року перебуває у стані постійних кіберзагроз з боку російської федерації. Хакерські атаки на державні органи та об'єкти критичної інфраструктури засвідчили необхідність не лише підтримувати криптографічну стійкість алгоритмів, але й забезпечувати резильєнтність систем до тривалих і комбінованих атак. Результати апробації підтвердили, що саме параметри V (кількість вразливостей), L (час відкритості) та U (оновлення ПЗ) є найбільш критичними у воєнних умовах, оскільки вони напряму впливають на здатність системи протистояти атакам у реальному часі.

Порівняння з наявними зарубіжними підходами (наприклад, методиками NIST та ENISA) показує, що запропонована модель є більш гнучкою щодо адаптації до локальних умов. Якщо зарубіжні стандарти значною мірою орієнтовані на постквантові виклики й формалізовані процеси сертифікації, то український контекст вимагає урахування специфіки воєнного середовища, нестачі ресурсів і необхідності швидкого реагування на кібератаки. Саме це відображено у включенні до формули параметрів, що характеризують не лише стійкість алгоритмів, але й оперативну готовність та організаційні аспекти безпеки.

Ще одним важливим результатом є можливість використання методики як інструмента для сценарного аналізу. Чутливісний аналіз продемонстрував, що навіть незначне підвищення своєчасності оновлень ПЗ або скорочення часу відкритості вразливостей суттєво підвищує інтегральний показник S. Це надає практичним фахівцям можливість обґрунтовувати доцільність конкретних заходів безпеки, що особливо важливо в умовах обмежених ресурсів.

Таким чином, запропонована методика може стати основою для:

– вдосконалення державних підходів до сертифікації ІКС;

– розробки нових нормативних документів, що базуватимуться на кількісних критеріях;

– впровадження у системи управління ризиками та моніторингу кібербезпеки.

Водночас необхідно підкреслити, що методика потребує подальшої перевірки на розширеній вибірці реальних систем та узгодження з міжнародними стандартами. У майбутньому доцільним є також розширення моделі шляхом врахування факторів, пов'язаних із використанням штучного інтелекту як у засобах захисту, так і у зловмисних діях.

Висновки. У роботі запропоновано інтегровану методику оцінки криптостійкості та захищеності інформаційно-комунікаційних систем, яка поєднує криптографічні, організаційно-технічні та експлуатаційні параметри в єдиний інтегральний показник. Запропонована формула дозволяє кількісно оцінювати рівень захисту ІКС, виявляти критичні слабкі місця та формувати практичні рекомендації для підвищення стійкості.

Апробація методики на прикладі різних сценаріїв (державні, муніципальні та інфраструктурні системи) продемонструвала її ефективність і чутливість до змін ключових параметрів. Найбільш вагомий вплив на рівень безпеки у воєнних умовах мають своєчасність оновлень програмного

забезпечення, кількість та час відкритості вразливостей, а також готовність системи до реагування на інциденти. Це підтверджує актуальність комплексного підходу до оцінки, який виходить за межі виключно криптографічної стійкості.

Практичне значення методики полягає в можливості її використання державними органами, підприємствами критичної інфраструктури та експертними установами для проведення аудиту, сертифікації та управління ризиками в сфері інформаційної безпеки. Подальший розвиток дослідження передбачає розширення моделі для врахування впливу новітніх технологій, зокрема штучного інтелекту та постквантових обчислень, а також гармонізацію з міжнародними стандартами кібербезпеки.

Список літератури:

1. Храмов С., Опірський І. Аналіз сучасного стану кібератак в Україні під час війни. *Захист інформації.* 2024. Том 26, № 1. С. 187–196. https://doi.org/10.18372/2410-7840.26.18842.

2. Воробець П., Горпенюк А., Опірський І. Перехід до постквантових криптографічних систем: виклики, стандартизація та перспективи. *Безпека інформації.* 2024. Том 30, № 2. С. 303–312. https://doi.org/10.18372/2225-5036.30.19243.

3. Фесенко А., Мирошніченко М. Порівняння постквантових стандартів у розрізі впровадження у класичні алгоритми електронного підпису. *Безпека інформаційних систем і технологій*. 2024. Том 1, № 7. С. 31–38. https://doi.org/10.17721/ISTS.2024.7.31-38.

4. Корченко А., Іванченко Є., Кошкіна Н., Кузнецов О., Качко О., Потій О., Онопрієнко В., Бобух В. Сучасні комплекси пост-квантової безпеки державних електронних інформаційних ресурсів. *Безпека інформації.* 2021. Том 27, № 1. С. 27–52. https://doi.org/10.18372/2225-5036.27.15575.

5. Мельник О., Мельник Р. Актуальність забезпечення кіберстійкості телекомунікаційних мереж ДСНС України. *Публічне управління у сфері цивільного захисту: освіта, наука, практика: матеріали Міжнародної науково-практичної інтернет-конференції (16 березня 2023 р.)*. Харків: НУЦЗ України, 2023. С. 274–275.

6. Klimushyn, P., Solianyk, T., Mozhaiev, O., Gnusov, Y., Manzhai, O., & Svitlychny, V. Crypto-Resistant Methods and Random Number Generators in Internet of Things (IOT) Devices. *Сучасний стан наукових досліджень та технологій в промисловості*. 2024. № 2 (20). С. 22–34. https://doi.org/10.30837/ITSSI.2022.20.022.

7. Поперешняк С. В. Тестування датчиків псевдовипадкових чисел, вбудованих в смарт-карти. *Наукоємні технології*. 2020. № 3. С. 359–369. https://doi.org/10.18372/2310-5461.47.14934.

8. Основи криптографічного захисту інформації: електронний навчальний посібник комбінованого (локального та мережного) використання [Електронний ресурс] / Яремчук Ю. Є., Салієва О. В., Бондаренко І. О. Вінниця: ВНТУ, 2024. 139 с.

9. Гнатюк С., Сидоренко В., Скуратівський А. Модель управління вимогами кібербезпеки при впровадженні програмного забезпечення. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2025. № 4 (28). С. 715–726. https://doi.org/10.28925/2663-4023.2025.28.841.

10. Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. Статистичний звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки протягом 2022 року. TLP:WHITE. 2022. 10 с. URL: https://scpc.gov.ua/uk/articles/233?utm_source=chatgpt.com.

11. CERT-UA. Russia's War on Ukraine: One Year of Cyber Operations. TLP:CLEAR. 2023. 32 c. URL: https://cert.europa.eu/static/MEMO/2023/TLP-CLEAR-CERT-EU-1YUA-CyberOps.pdf?utm_source=chatgpt.com.

12. Melnyk R., Melnyk O. Improving the Cryptographic Protection of Confidential Information in the Management of Civil Protection Forces and Means. *Вісник Кременчуцького національного університету імені Михайла Остроградського*. 2022. Вип. 1 (132). С. 108–114. https://doi.org/10.32782/1995-0519.2022.1.14.

13. Chen L., Jordan S., Liu Y., Moody D., Peralta R., Perlner R., Smith-Tone D. Report on Post-Quantum Cryptography, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, 2016. 10 p. https://doi.org/10.6028/NIST.IR.8105.

14. NIST Internal Report. NIST IR 8545. Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process. 2025. 34 p. https://doi.org/10.6028/NIST.IR.8545.

15. Pan L., Tomlinson A. A systematic review of information security risk assessmen. *International Journal of Safety and Security Engineering.* 2016. Vol. 6, № 2. Pp. 270–281. https://doi.org/10.2495/SAFE-V6-N2-270-281.

16. Ваврик Ю., Опірський І. Штучний інтелект: кібербезпека нового покоління. *Безпека інформації*. 2024. Том 30, № 2. С. 244–255. https://doi.org/10.18372/2225-5036.30.19235.

17. Rjoub G., Bentahar J., Abdel Wahab O., Mizouni R., Song A., Cohen R., Otrok H., Mourad A. (2023). A Survey on Explainable Artificial Intelligence for Cybersecurity. URL: https://arxiv.org/pdf/2303.12942.pdf.

18. Шевчук М.О. Аналіз національного законодавства про інформаційну безпеку. *Юридичний науковий електронний журнал*. 2025. № 1. С. 383–386. https://doi.org/10.32782/2524-0374/2025-1/87.

19. Гедіков В. Загальний аналіз нормативно-правових актів у сфері цифровізації в Україні. *Юридичний вісник*. 2024. № 3. С. 54–61. https://doi.org/10.32782/yuv.v3.2024.7.

Melnyk R.P., Melnyk O.H. METHODOLOGY FOR THE ASSESSMENT OF CRYPTOGRAPHIC STRENGTH AND SECURITY OF INFORMATION AND COMMUNICATION SYSTEMS UNDER MODERN CYBER THREATS

The article presents the results of a study aimed at developing and testing an integrated methodology for the quantitative assessment of cryptographic strength and the overall security of information and communication systems under modern conditions. The relevance of the research is determined by the ongoing military aggression against Ukraine, accompanied by large-scale cyberattacks targeting government institutions and critical infrastructure, as well as by the rapid development of emerging technologies, including artificial intelligence and post-quantum computing. The study highlights the problem of imperfections in the current regulatory framework for information protection, which does not fully reflect the specifics of wartime and requires adaptation to new challenges.

The proposed methodology introduces an integral indicator that combines cryptographic, organizational, technical, and operational parameters into a unified formula. The evaluation is based on the normalization of key characteristics: cryptographic key length, algorithmic robustness, effectiveness of security policies, level of physical protection, timeliness of software updates, readiness for incident response, number and duration of vulnerabilities, and the effectiveness of potential attacks. A scale of interpretation of results is suggested, which allows defining the security level of the system from low to very high.

The methodology was tested through three scenarios representing different levels of security organization: a government data processing center, a municipal information system, and a critical infrastructure enterprise under wartime conditions. The results confirmed the effectiveness of the proposed model and its sensitivity to changes in key parameters. It was established that the most significant impact on the security level is caused by the timeliness of software updates, the number and duration of vulnerabilities, and the readiness to respond to incidents.

The practical significance of the study lies in creating a tool suitable for use by government bodies, critical infrastructure enterprises, and expert institutions for auditing, certification, and the improvement of information protection policies. The proposed approach can serve as a foundation for updating national standards and harmonizing them with international requirements, which is of crucial importance in the context of modern cyber threats and war.

Key words: *cryptographic strength, security, information system, cyberattacks, artificial intelligence, post-quantum computing, vulnerabilities, cybersecurity, information protection, wartime.*

Дата надходження статті: 18.11.2025
Дата прийняття статті: 10.12.2025
Опубліковано: 30.12.2025