КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.1101
УДК 004.056:519.61:338

Гладка Олена Миколаївна
к.т.н, доцент, доцент кафедри комп'ютерних технологій та економічної кібернетики
Національний університет водного господарства та природокористування, Рівне, Україна
ORCID: 0000-0003-4728-0663
o.m.hladka@nuwm.edu.ua

Карпович Іван Миколайович
к.ф.-м.н, доцент, доцент кафедри комп'ютерних технологій та економічної кібернетики
Національний університет водного господарства та природокористування, Рівне, Україна
ORCID: 0000-0002-4601-0541
i.m.karpovich@nuwm.edu.ua

Паламарчук Андрій Сергійович
здобувач вищої освіти Навчально-наукового інституту кібернетики, інформаційних технологій та інженерії
Національний університет водного господарства та природокористування, м. Рівне, Україна
palamarchuk_ak24@nuwm.edu.ua

ЕКОНОМІЧНИЙ АСПЕКТ МОДЕЛЮВАННЯ СИСТЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ З ВИКОРИСТАННЯМ МЕТОДІВ МАТЕМАТИЧНОЇ ОПТИМІЗАЦІЇ

Анотація. В умовах стрімкої цифровізації захист інформаційних активів набуває пріоритетного значення, оскільки зростаюча інтенсивність кіберзагроз вимагає розробки дієвих механізмів мінімізації потенційних збитків. В роботі розглянуто можливі підходи до визначення ефективності та економічної обґрунтованості створення систем захисту інформації. Проаналізовано основні складові політики безпеки компанії та роль керівників вищої ланки в організації кібербезпеки. Оскільки проблема управління інформаційними ризиками стає дедалі критичнішою, це зумовлює необхідність пошуку стратегій, спрямованих на оптимізацію витрат та скорочення економічних втрат від деструктивних кібервпливів. В статті також розглянуто особливості зовнішніх зловмисних впливів і проаналізовано мотивацію зловмисників. Використано запропоновану раніше математичну модель максимізації ефективності засобів захисту інформації при обмеженнях на обсяг витрат і наведено їх економічне обгрунтування. Застосування математичного моделювання трансформує процес прийняття рішень у сфері кіберзахисту з інтуїтивного на доказовий. Це дозволяє обґрунтувати інвестиції в систему інформаційної безпеки як чинник зростання прибутковості через запобігання втратам, а також розв'язати задачу вибору оптимального комплексу засобів захисту в умовах дефіциту ресурсів. Математична модель у цьому контексті виступає об'єктивним інструментом верифікації ефективності системи протидії актуальним загрозам. В роботі також проведено аналіз нових трендів у розробці систем інформаційної безпеки.

Ключові слова: інформаційна безпека; інформаційні ризики; математична модель; інформаційна загроза; ефективність системи інформаційної безпеки.

ВСТУП

У сучасному цифровому світі, де інформація стала стратегічним ресурсом, забезпечення кіберстійкості інформаційних систем (ІС) трансформувалося з чисто технічного завдання у фундаментальну економічну проблему. Стрімке зростання кількості кіберзагроз та їхня дедалі більша витонченість змушують компанії інвестувати значні кошти в системи інформаційної безпеки. Проте ресурси будь-якої організації є

обмеженими, що породжує критичну потребу в обґрунтованому розподілі бюджету між різними векторами захисту.

Згідно з нормативними документами (зокрема, ISO/IEC 27000:2009) інформаційна безпека (ІБ) містить три основні складові: конфіденційність (захист інформації від несанкціонованого доступу); цілісність (захист повноти і точності інформації та програмного забезпечення); доступність (забезпечення своєчасної доступності інформації і основних послуг для всіх авторизованих користувачів). Порушення нормального функціонування інформаційної системи в результаті деструктивних факторів погіршують значення основних показників інформаційної безпеки для цієї ІС.

Постановка проблеми. Забезпечення інформаційної безпеки є самостійним, складним і витратним напрямом діяльності організацій. Розгляду питань, пов'язаних із забезпеченням захищеності інформації, присвячено багато наукових досліджень. Створено широку базу нормативних і методичних документів, які регламентують діяльність у цій галузі. Проте, завдання забезпечення ІБ, зазвичай, не має тривіальних рішень для її практичної реалізації. Проблеми тут пов'язані із визначенням ефективності та економічної обґрунтованості створення систем інформаційної безпеки.

Актуальність теми зумовлена суперечністю між необхідністю мінімізації ризиків та прагненням до економічної ефективності бізнес-діяльності підприємства. Традиційні підходи до побудови систем інформаційної безпеки часто фокусуються лише на технологічних показниках, ігноруючи фінансові наслідки: вартість впровадження заходів, витрати на їх підтримку та потенційні збитки від реалізації інцидентів. Економічний аспект моделювання дозволяє розглядати інформаційну безпеку не як “центр витрат”, а як інструмент управління ризиками, що впливає на капіталізацію та стабільність компанії.

Аналіз останніх досліджень і публікацій. В роботі [1] детально викладено аналіз різних типів моделювання загроз та ризикоорієнтовану методологію, спрямовану на застосування контрзаходів безпеки з використанням стратегічного підходу до систематичного виявлення та усунення загроз на основі аналізу ризиків, вразливостей та шаблонів атак. Крім того, пропонуються кроки для боротьби із загрозами для бізнесу, розглянуто реальні інциденти порушення безпеки даних та рекомендації із управління ризиками. Інформаційна безпека асоціюється з мінімізацією ризиків загроз функціонування компанії, зокрема, зовнішні втручання в документообіг і технологічні процеси, відмови апаратного, програмного забезпечення, відмови працездатності систем, пов'язані з недостатньою кваліфікацією персоналу тощо.

Функціонування інформаційних систем пов'язане з певними ризиками. Основою проектування та використання системи захисту інформації є аналіз ризиків, механізм реалізації якого детально описується в [2]. У стандарті зазначено, що ризик вимірюється, виходячи з комбінації наслідків, які випливають з небажаної події та ймовірності виникнення цієї події.

Вирішення питання про рівень захисту конкретної системи потребує аналізу, пов'язаного з оцінкою та управлінням інформаційними ризиками. Такий підхід для дослідження загроз безпеці інформаційних систем, оцінювання рівня їх захищеності, аналізу ефективності функціонування систем захисту інформації рекомендують діючі міжнародні стандарти [2-4].

Управління ризиками складається з трьох етапів: пошук, виявлення та подальший аналіз; класифікація за ступенем критичності та можливості виникнення; дії щодо нейтралізації, мінімізації наслідків від їх виникнення або переадресації, наприклад, через укладання страхової угоди. Передумови страхування ризиків ІБ як один із варіантів

опрацювання ризиків та економічно вигідний метод захисту інформації проаналізовано в роботах [5], [6].

Проведений аналіз показав, що управління ризиками інформаційної безпеки – це циклічний та неперервний процес, тому керівництво підприємства має враховувати ці аспекти під час планування бюджету на його реалізацію. Це дасть можливість надійно захищати дані та мінімізувати ризики можливих фінансових втрат і репутаційної шкоди.

Метою статті є аналіз і дослідження можливих підходів до вирішення взаємозалежних завдань забезпечення інформаційної безпеки, що пов'язані із визначенням ефективності та економічної обґрунтованості створення систем кіберзахисту, з використанням моделювання інформаційної безпеки. Інструментарій математичної оптимізації дозволяє представити інформаційну безпеку не як статтю витрат, а як засіб захисту капіталізації компанії. Завдяки моделюванню стає можливим раціональний розподіл обмеженого бюджету та формування переконливої доказової бази для керівництва щодо здатності обраної стратегії захисту нейтралізувати критичні кіберризики.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Первинна мета аналізу ризиків – оптимізація бюджету на організацію інформаційної безпеки. Це необхідно для дотримання важливого принципу, коли вартість розгортання системи ІБ не повинна перевищувати вартість активів, які потрібно захистити. В результаті аудиту ризиків визначаються потенційно вразливі інформаційні активи. Аналіз ризиків розглядається для ІС у її початковому стані, оцінюється розмір очікуваних втрат від інцидентів, пов'язаних із інформаційною безпекою за певний період. Після цього робиться оцінка того, як запропоновані засоби та заходи забезпечення безпеки впливають на зниження ризиків і яка їх вартість.

Встановлення значення ризику може бути якісним, кількісним чи комбінованим. Рекомендується використовувати якісні значення для отримання загальних відомостей про рівень ризику і потім переходити до кількісних оцінок як до більш детальних. Спочатку проводяться якісні оцінки наслідків із врахуванням цінності активів та ймовірності виникнення загрози, потім їм у відповідність ставляться числові значення за заздалегідь визначеною шкалою.

Ризиком у сфері інформаційної безпеки вважається потенційна можливість зазнати збитків через порушення безпеки інформаційної системи. Ймовірні втрати від реалізації окремої загрози можна обчислити за методикою, описаною раніше в роботі [7], з допомогою формули розрахунку вартості ризику:

$$R_i = \sum_{k=1}^{k1} \omega_i \, p_i y_i c(a_k)$$

де $k1$ – кількість активів, на які спрямована i-та загроза, i=1..n; ω_i – частота виникнення i-ї загрози; p_i – ймовірність реалізації загрози, наприклад, внаслідок успішного використання деякої вразливості; $c(a_k)$ – вартість активу a_k, $a_k \in A_i$, A_i – набір активів або ресурсів, на які спрямована i-та загроза.

Коефіцієнт пошкодження (руйнування) $y_i \in [0; 1]$, що виражає міру руйнівної дії загрози на актив чи активи, може служити критерієм відбору тих активів, на які поширюється руйнівна дія i-ї загрози. Такий підхід відповідає стандарту [8], де ризик

визначається як функція ймовірності реалізації окремим джерелом загрози певної потенційної вразливості та результуючого впливу цієї ворожої дії на організацію чи індивіда.

Аналіз політики безпеки ІС. Система інформаційної безпеки є складовою частиною інформаційної системи компанії і не повинна порушувати функціональних параметрів ІС. Захищеність інформаційної системи, зазвичай, формулюється під час її проектування у вигляді політики безпеки. Політика безпеки – це перелік зафіксованих документально рішень, які стосуються всіх співробітників компанії, спрямованих на безпеку інформаційних активів. Документ, у якому повинні бути детально відображені напрямки роботи, завдання, принципи та методи забезпечення інформаційної безпеки підприємства, може містити наступні блоки.

- Основні положення, в яких описані загальні проблеми організації безпеки інформації та способи їх вирішення, нормативно-правові засади, роль працівників тощо.
- Сфера використання, де перелічені основні активи підприємства, які потрібно захищати (зазвичай, це дані, програмне забезпечення, інформаційна система, персонал, нематеріальні ресурси (репутація і імідж компанії) тощо).
- Цілі, завдання та критерії організації безпеки інформації, що визначаються специфікою галузі, у якій функціонує підприємство. Зокрема, для режимних об'єктів пріоритетним є збереження конфіденційності інформаційних активів; для інформаційних сховищ важливо зберігати цілісність даних; для сервісних організацій актуальним є забезпечення доступності підсистем тощо.
- Ролі, обов'язки та відповідальність у випадку порушень інформаційної безпеки. Тут детально описують організацію системи доступу до інформаційних активів.

Політику безпеки поділяють на верхній, середній та нижній рівні. Верхній рівень носить загальноорганізаційний характер та описує політику інформаційної безпеки компанії в цілому, зокрема, мету та завдання у сфері забезпечення інформаційної безпеки; виділення бюджету на організацію безпеки інформації; способи, ресурси, процеси для забезпечення ІБ; комунікації компанії з контрагентами, клієнтами тощо.

Середній рівень політики інформаційної безпеки підприємства виділяють за високої складності архітектури підприємства чи у випадках, коли є потреба позначити специфічні підсистеми підприємства. Зазвичай, середній рівень регулює питання, пов'язані з експлуатацією компанією різних систем.

Нижній рівень політики ІБ регулює роботу конкретних служб та підрозділів і конкретизує заходи, передбачені на верхніх рівнях політики.

Захист від кібератак не можна розглядати як проблему, що належить виключно ІТ-відділу або відділу кібербезпеки. Системний підхід до комплексу питань захисту інформації повинен охоплювати все, що робить організація – від її бізнес-операцій, моделей та стратегій до її продуктів та інтелектуальної власності. В роботі [9] на основі практичного досвіду запропоновано рекомендації, як керівникам вищої ланки та членам ради директорів стати розпорядниками діяльності своїх компаній у сфері кібербезпеки. Рекомендації містять тлумачення кіберризиків та способів їх контролю; планування та підготовку до інформаційних атак, а також шляхи подолання їх наслідків; перетворення кібербезпеки на загальнокорпоративну ініціативу та відповідальність; особливості нетехнічної динаміки, яка впливає на ефективність заходів кібербезпеки; узгодження пріоритетів діяльності ради директорів, виконавчого керівництва та команд з кібербезпеки.

Особливості і мотивації зовнішніх зловмисників. Як відомо, порушення інформаційної безпеки відбувається з ініціативи зловмисника. Особливості мотивації

внутрішнього зловмисника проаналізовано в роботі [7]. Узагальнюючи інформацію з відкритих джерел, можна сформулювати основні положення та принципи, які характеризують зовнішнього зловмисника:

- для кожної реалізації загрози існує зловмисник, який заради досягнення своєї мети намагається виконати завдання, використовуючи можливості, що надаються інфраструктурою;
- існують зловмисники, які шукають способи для компрометації хостів та мереж з метою просування своїх намірів та задоволення власних потреб;
- будь-яка система, а значить і будь-який цільовий актив, має вразливості або слабкі місця;
- кожна шкідлива активність складається з фаз, успішне виконання яких за певних умов призводить до успіху активності загалом;
- практично завжди існують стосунки між зловмисником та жертвою, навіть якщо вони неявні чи непрямі;
- зловмисники, які мають мотивацію, ресурси та можливості, можуть підтримувати шкідливу присутність протягом тривалого часу, очікуючи сприятливого моменту для подолання заходів із протидії.

Економічною складовою мотивації зловмисника реалізувати конкретну загрозу щодо певного інформаційного ресурсу є його "надбання" $g - D$ отримане в результаті успішної атаки, де g – цінність інформаційного ресурсу для зловмисника; D – загальна вартість витрат атакуючої сторони на реалізацію конкретної загрози. Ймовірність загрози можна оцінити співвідношенням [10]:

$$p = 1 - \frac{D}{g}.$$

Бачимо, що якщо цінність ресурсу для атакуючої сторони висока, зловмисники вимушені йти на значні витрати для реалізації загрози. З іншого боку, ймовірність застосування високовитратних атак для реалізації загроз низька.

Для підвищення рівня безпеки необхідно мінімізувати вразливості ІС, підвищивши ефективність функціонування системи захисту інформації, що сприятиме збільшенню витрат на реалізацію загроз зловмисниками і зменшить ймовірність їх застосування.

Математична оптимізаційна модель. Одним із підходів до вирішення завдання захисту інформації є аналіз проблеми з економічної точки зору і розробка та тестування відповідних математичних моделей. Завдання забезпечення ІБ інформаційної системи розглядається тут як інвестиційний проект із вкладення коштів у її вирішення. У розробці будь-якого проекту, що потребує фінансових витрат на його реалізацію, важливо вже на початковій стадії визначити, як будуть оцінюватися результати виконання. Для завдань, пов'язаних з інформаційною безпекою, це теж актуально, адже витрати на забезпечення високого рівня безпеки можуть бути невиправданими. Здебільшого переважає відомий принцип розумної достатності, застосований до сфери забезпечення ІБ, який описується набором тверджень:

- абсолютно неперебірного захисту створити неможливо;
- необхідно дотримуватися балансу між витратами на захист та одержуваним ефектом;
- вартість засобів захисту не повинна перевищувати вартості інформації, що захищається;

• витрати порушника на несанкціонований доступ до інформації повинні перевищувати той ефект, який він отримає, здійснивши такий доступ.

Для розрахунку оптимальних витрат, необхідних для побудови ефективної системи захисту інформації, можна використати постановку задачі у вигляді [6]:

$$\sum_{j=1}^{m}\sum_{i=1}^{n} r(i,j)y(i,j) \to \max$$

за обмежень

$$\sum_{i=1}^{n} q(i)\sum_{x_j \in T} y(i,j) \le Q;$$

$$\{y(i,j)\} = \{0;1\},$$

де *r(i,j)* – ефективність нейтралізації *i*-м засобом захисту *j*-ї інформаційної загрози; *y(i,j)* дорівнює 1, якщо *j*-а загроза нейтралізується за допомогою *i*-го засобу захисту, і дорівнює нулю в іншому випадку; *q(i)* – витрати на розробку чи придбання *i*-го засобу захисту.

Завдання вибору оптимальної системи інформаційної безпеки полягає у максимізації ефективності нейтралізації наявних інформаційних загроз засобами захисту при обмеженнях на обсяг витрат *Q*.

Визначення оптимального обсягу витрат компанії на інформаційну безпеку здійснюється, як відомо, на основі аналізу ризиків. За даними [11] про ключові показники інформаційної діяльності, організації витрачають в середньому 5,6% загального IT-бюджету на інформаційну безпеку та управління ризиками. Однак, за дослідженнями аналітиків, витрати на інформаційну безпеку варіюються в межах від 1 до 13% IT-бюджету.

Без урахування бізнес-вимог, толерантності до ризику, показник витрат на інформаційну безпеку у відсотках від IT-бюджету сам по собі не надає достовірної порівняльної інформації, яку можна використовувати для розподілу IT- або бізнес-ресурсів. Більше того, статистика витрат на інформаційну безпеку сама по собі не вимірює ефективність інформаційної безпеки і не є показником успішності IT-організацій.

Реальні витрати на безпеку зазвичай поділяються на обладнання, програмне забезпечення, послуги (аутсорсинг та консалтинг), персонал. Однак будь-яка статистика щодо явних витрат на безпеку занижує справжній масштаб інвестицій підприємства в IT-безпеку, оскільки функції безпеки вбудовуються в обладнання, програмне забезпечення, діяльність чи ініціативи, що не призначені спеціально для інформаційної безпеки [11]. Складність точного визначення витрат на кібербезпеку частково пояснюється тим, що не всі системи обліку витрат виділяють інформаційну безпеку як окремий пункт, а багато процесів, пов'язаних з безпекою, виконуються співробітниками, які займаються питаннями безпеки не повний робочий день.

У більшості випадків головний спеціаліст з інформаційної безпеки (CISO) не може оцінити витрати на безпеку в усьому підприємстві. Реальний бюджет на безпеку, в основному, складається з витрат на мережеве обладнання із вбудованими функціями безпеки, захист робочих місць, який може бути включений до бюджету підтримки кінцевих користувачів, корпоративні додатки, аутсорсингові або керовані послуги

безпеки, програми забезпечення неперервності бізнесу або конфіденційності, а також профінансоване навчання з безпеки.

Нові тренди у розробці систем інформаційної безпеки. Розглянемо нові виклики та тренди у розробці і функціонуванні систем інформаційної безпеки, які покликані підвищити рівень захисту інформації та забезпечення безпеки організацій в умовах кіберзагроз.

В сучасних умовах керівникам кібербезпеки необхідне глибоке розуміння систем штучного інтелекту (ШІ), що використовуються на їх підприємствах. Це ускладнюється тим, що кількість систем штучного інтелекту, вбудованих у підприємства, значно зросла. ШІ та машинне навчання застосовуються для автоматизації процесів виявлення та запобігання кіберзагрозам, аналізу великих обсягів даних про поведінку користувачів, моніторингу подій безпеки та виявлення можливих загроз, а також для оптимізації роботи інструментів ІБ. Керівники з кібербезпеки повинні провести виявлення та каталогізацію заходів з інформаційної безпеки на базі штучного інтелекту, перш ніж проводити обов'язкові оцінки ризиків [12]. Популярність спеціально розроблених агентів ШІ створює нові можливості для атак та ризики, які вимагають від підприємств впровадження безпечних практик розробки та реалізації заходів безпеки. Оскільки дії агентів ШІ базуються на ймовірнісних моделях, вони менш передбачувані, що ускладнює управління ризиками.

Підхід нульової довіри передбачає, що довіра до користувачів та пристроїв усередині мережі має бути мінімальною, а доступ до ресурсів повинен надаватися лише після перевірки автентичності та авторизації. Це дозволяє знизити ризики виходу за межі безпеки компанії та підвищити рівень захисту інформації.

Контейнеризація даних та контейнерна архітектура інформаційних систем потребують захисту контейнерних середовищ. Контейнери є полегшеним віртуальним середовищем, яке дозволяє запускати програми ізольовано одна від одної. Для організації безпеки контейнерних середовищ використовуються шифрування даних, захист від несанкціонованого доступу, моніторинг подій, аудит дій користувачів тощо.

Резервне копіювання є важливим елементом системи ІБ. Щоб підвищити його ефективність, необхідно визначити, які дані потрібно резервувати, вибрати оптимальні методи та засоби резервного копіювання, а також гарантувати довгострокове зберігання резервних копій.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Відзначимо, що розробка системи інформаційної безпеки в організації – це складний та багатоетапний процес, що вимагає комплексного підходу. Реалізація заходів інформаційної безпеки повинна бути адаптована до умов бізнесу, що змінюються, і нових загроз. Це вимагає регулярного моніторингу та аналізу ризиків, розробки та впровадження нових механізмів захисту, а також навчання персоналу. Необхідно враховувати всі рівні захисту: адміністративний, законодавчий, процедурний та програмно-технічний. Тільки комбінований підхід, що враховує всі рівні захисту, дозволить створити надійну систему інформаційної безпеки, яка буде достатньо стійкою і зможе забезпечити ефективний захист від усіх відомих ризиків. При цьому важливо пам'ятати: система організації безпеки інформації має бути неперервною, цілодобовою і регулярно оновлюватись та вдосконалюватись з виникненням нових загроз чи внесенням змін до роботи підприємства.

Перспективи подальших досліджень можуть полягати у посиленні математичної оптимізації адаптивними алгоритмами для автоматичного коригування бюджету системи інформаційної безпеки у режимі реального часу залежно від інтенсивності кібератак; використанні методів робастної оптимізації (Robust Optimization) та теорії нечітких множин (Fuzzy Logic), що дозволить моделювати системи захисту навіть за відсутності точних вхідних даних (яких у сфері інформаційної безпеки зазвичай обмаль) і створювати економічно ефективні системи ІБ навіть за умови значних похибок у прогнозуванні ймовірності атак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. UcedaVelez, T., & Morana, M. M. (2015). *Risk-centric threat modeling: Process for attack simulation and threat analysis*. John Wiley & Sons.
2. British Standards Institution. (2008). *Information technology—Security techniques—Information security risk management (BS ISO/IEC 27005:2008)*.
3. International Organization for Standardization. (2005). *ISO/IEC 27001:2005: Information technology—Security techniques—Information security management systems—Requirements*. http://www.jtc1sc27.din.de/en
4. International Organization for Standardization. (2007). *ISO/IEC 27002:2007: Information technology—Security techniques—Code of practice for information security management*. http://www.jtc1sc27.din.de/en
5. Ksonzhyk, I., Zhovta, N., & Pavlina, A. (2021). Cybersecurity risk insurance of business entities in the modern information space. *Economy and Society, 34*. https://doi.org/10.32782/2524-0072/2021-34-90
6. Karpovych, I., Hladka, O., & Palamarchuk, A. (2025). Application of mathematical optimization methods to improve the efficiency of information security systems. *Cybersecurity: Education, Science, Technique, 4*(28), 198–205. https://doi.org/10.28925/2663-4023.2025.28.778
7. Karpovych, I. M., Hladka, O. M., & Kalashnikov, V. I. (2022). Modeling of information security risk analysis processes as a way to optimize costs. *Scientific Notes of Taurida National V. I. Vernadsky University. Series: Technical Sciences, 33*(72), 93–99. https://doi.org/10.32782/2663-5941/2022.5/13
8. National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments (NIST Special Publication 800-30 Rev. 1)*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
9. Parenty, T. J., & Domet, J. J. (2019). *The leader's guide to cybersecurity: Why boards need to lead—and how to do it*. Harvard Business Review Press.
10. Arkhypov, O. Ye. (2011). Application of economic-motivational relationships for assessing probabilistic parameters of information risks. *Information Protection, 2*, 5–11.
11. Gartner, Inc. (2016). *Gartner says many organizations falsely equate IT security spending with maturity*. https://www.gartner.com/en/newsroom/press-releases/2016-12-09-gartner-says-many-organizations-falsely-equate-it-security-spending-with-maturity
12. Henein, N. (2025). *Cybersecurity and AI: Enabling security while managing risk*. Gartner. https://www.gartner.com/en/cybersecurity/topics/cybersecurity-and-ai

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023

Olena Hladka
PhD on Engineering Science, Associate Professor, Associate Professor at the Department of Computer Technology and Economic Cybernetics
National University of Water and Environmental Engineering, Rivne, Ukraine
ORCID: 0000-0003-4728-0663
o.m.hladka@nuwm.edu.ua

Ivan Karpovich
PhD on Physics and Mathematics Science, Associate Professor, Associate Professor at the Department of Computer Technology and Economic Cybernetics
National University of Water and Environmental Engineering, Rivne, Ukraine
ORCID: 0000-0002-4601-0541
i.m.karpovich@nuwm.edu.ua

Andrii Palamarchuk
student at the Institute of Cybernetics, Information Technologies and Engineering
National University of Water and Environmental Engineering, Rivne, Ukraine
palamarchuk_ak24@nuwm.edu.ua

ECONOMIC ASPECT OF MODELING INFORMATION SECURITY SYSTEMS USING MATHEMATICAL OPTIMIZATION METHODS

Abstract. In the context of rapid digitalization, the protection of information assets is becoming a priority, since the growing intensity of cyber threats requires the development of effective mechanisms to minimize potential losses. The paper considers possible approaches to determining the effectiveness and economic feasibility of creating information protection systems. The main components of a company's security policy and the role of senior managers in the organization of cybersecurity are analyzed. As the problem of information risk management becomes increasingly critical, this necessitates the search for strategies aimed at optimizing costs and reducing economic losses from destructive cyber impacts. The article also considers the features of external malicious influences and analyzes the motivation of attackers. The previously proposed mathematical model of maximizing the effectiveness of information protection tools with restrictions on the amount of costs is used and their economic justification is provided. The use of mathematical modeling transforms the decision-making process in the field of cyber security from intuitive to evidence-based. This allows us to justify investments in the information security system as a factor in increasing profitability through loss prevention, as well as to solve the problem of choosing the optimal set of protection tools in conditions of resource shortage. The mathematical model in this context acts as an objective tool for verifying the effectiveness of the system for countering current threats. The paper also analyzes new trends in the development of information security systems.

Keywords: information security; information risks; mathematical model; information threat; effectiveness of the information security system.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. UcedaVelez, T., & Morana, M. M. (2015). *Risk-centric threat modeling: Process for attack simulation and threat analysis*. John Wiley & Sons.
2. British Standards Institution. (2008). *Information technology—Security techniques—Information security risk management (BS ISO/IEC 27005:2008)*.
3. International Organization for Standardization. (2005). *ISO/IEC 27001:2005: Information technology—Security techniques—Information security management systems—Requirements*. http://www.jtc1sc27.din.de/en
4. International Organization for Standardization. (2007). *ISO/IEC 27002:2007: Information technology—Security techniques—Code of practice for information security management*. http://www.jtc1sc27.din.de/en

5. Ksonzhyk, I., Zhovta, N., & Pavlina, A. (2021). Cybersecurity risk insurance of business entities in the modern information space. *Economy and Society, 34*. https://doi.org/10.32782/2524-0072/2021-34-90
6. Karpovych, I., Hladka, O., & Palamarchuk, A. (2025). Application of mathematical optimization methods to improve the efficiency of information security systems. *Cybersecurity: Education, Science, Technique, 4*(28), 198–205. https://doi.org/10.28925/2663-4023.2025.28.778
7. Karpovych, I. M., Hladka, O. M., & Kalashnikov, V. I. (2022). Modeling of information security risk analysis processes as a way to optimize costs. *Scientific Notes of Taurida National V. I. Vernadsky University. Series: Technical Sciences, 33*(72), 93–99. https://doi.org/10.32782/2663-5941/2022.5/13
8. National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments (NIST Special Publication 800-30 Rev. 1)*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
9. Parenty, T. J., & Domet, J. J. (2019). *The leader's guide to cybersecurity: Why boards need to lead—and how to do it*. Harvard Business Review Press.
10. Arkhypov, O. Ye. (2011). Application of economic-motivational relationships for assessing probabilistic parameters of information risks. *Information Protection, 2*, 5–11.
11. Gartner, Inc. (2016). *Gartner says many organizations falsely equate IT security spending with maturity*. https://www.gartner.com/en/newsroom/press-releases/2016-12-09-gartner-says-many-organizations-falsely-equate-it-security-spending-with-maturity
12. Henein, N. (2025). *Cybersecurity and AI: Enabling security while managing risk*. Gartner. https://www.gartner.com/en/cybersecurity/topics/cybersecurity-and-ai

Отримано редакцією журналу / Received: 27.01.26
Прорецензовано / Revised: 18.02.26
Схвалено до друку / Accepted: 26.03.26