

[DOI 10.28925/2663-4023.2026.35.1422](https://doi.org/10.28925/2663-4023.2026.35.1422)

УДК 004.056:351.86

Волинець Віталій Володимирович

аспірант кафедри захисту інформації

Вінницький національний технічний університет, м. Вінниця, Україна

ORCID: 0009-0006-7999-1290

volynets1026@gmail.com

Войтович Олеся Петрівна

к.т.н., доцент, доцент кафедри захисту інформації

Вінницький національний технічний університет, м. Вінниця, Україна

ORCID: 0000-0001-8964-7000

voytovych.olesya@vntu.edu.ua

МЕХАНІЗМ АДАПТИВНОГО ПЛАНУВАННЯ АУДИТУ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВА НА ОСНОВІ КОМПЛЕКСНОГО ОЦІНЮВАННЯ СТАНУ ТА КРИТИЧНОСТІ АКТИВІВ

Анотація. У статті запропоновано механізм адаптивного планування аудиту кібербезпеки підприємства на основі комплексного оцінювання стану та критичності інформаційних активів. Механізм розглядається як засіб підтримки етапу планування аудиторських процедур і призначений для визначення пріоритетності перевірок інформаційних активів у межах установленої програми аудиту. Для комплексного оцінювання стану активу поєднуються оцінка формальної відповідності вимогам кіберзахисту, поточного динамічного стану безпеки та експертна оцінка аудитора або профільного фахівця. Бізнес-значущість активу враховується за допомогою коефіцієнта критичності. На основі зазначених показників формується узагальнена оцінка стану та розраховується індекс пріоритетності аудиту, який використовується для ранжування активів і адаптивного уточнення черговості їх перевірки за обмеженого аудиторського ресурсу. Передбачено можливість повторного обчислення пріоритетів у разі появи нових вразливостей, аномалій, інцидентів, змін конфігурації або інших чинників кіберризиків. Для забезпечення відтворюваності результатів фіксуються джерела та момент отримання вхідних даних, правила нормування, шкали оцінювання і вагові коефіцієнти. Проведено сценарну апробацію механізму на прикладі восьми інформаційних активів умовного підприємства. Після моделювання погіршення стану окремих активів індекси пріоритетності було повторно обчислено, що спричинило зміну черговості першочергових перевірок. За обмеження аудиторського ресурсу трьома перевірками середній індекс пріоритетності активів першочергової перевірки збільшився з 0,307 для початкового порядку до 0,344 для адаптивно оновленого. Отримані результати демонструють працездатність механізму як засобу підтримки прийняття рішень і потребують подальшої перевірки на реальних даних підприємства.

Ключові слова: кібербезпека; аудит кібербезпеки; інформаційні активи; критичність активів; кіберризик; пріоритизація; прийняття рішень; адаптивне планування.

ВСТУП

Постановка проблеми. У межах реалізації програми аудиту безпеки підприємства виникає задача встановлення черговості перевірки інформаційних активів в умовах обмеженого аудиторського ресурсу. Якщо нормативні вимоги, бізнес-цілі та загальне оцінювання ризиків задають загальну періодичність та обсяг аудиту, то поточний стан і критичність конкретних активів у цій роботі використовуються як основа для адаптивного уточнення пріоритетності окремих аудиторських перевірок.

Для чіткої окресленості предмета дослідження доцільно розмежувати аудит інформаційної безпеки підприємства та аудит кібербезпеки (кібераудит). Аудит інформаційної безпеки охоплює ширший контур - систему управління, політики, процеси та внутрішній контроль. Аудит кібербезпеки розглядається як його спеціалізована складова, зосереджена на інформаційно-комунікаційних системах, технічних заходах кіберзахисту та відповідних кіберризиках, які й формують поточний стан оцінюваних активів.

Ризик-орієнтований принцип визначення об'єктів, що потребують підвищеної уваги аудитора, застосовується й у сучасних інтелектуальних системах підтримки внутрішнього аудиту, де оцінювання



ризиків, виявлення аномалій та моніторинг використовуються для підтримки прийняття аудиторських рішень [1].

Необхідність такого адаптивного уточнення зумовлена динамічністю чинників кіберризиків. У цифровому середовищі з'являються нові вразливості, фіксуються аномалії в журналах подій, змінюються конфігурації інформаційних систем, а інциденти можуть впливати на пов'язані сервіси та бізнес-процеси [2]. За даними аналітичного звіту Unit 42 (Palo Alto Networks), у 25% найшвидших кібератак час від початкового проникнення зловмисників до моменту викрадення даних скоротився до рекордних 72 хвилин, тоді як роком раніше цей показник становив 285 хвилин [3]. За таких умов заздалегідь визначена послідовність перевірок інформаційних активів не завжди дає змогу своєчасно зосередити аудиторський ресурс на тих об'єктах, для яких потреба в перевірці стала більш актуальною [3], [4]. Тому доцільним є розроблення механізму адаптивного уточнення пріоритетності перевірок інформаційних активів відповідно до змін чинників кіберризиків та поточного стану їх кібербезпеки.

Аналіз останніх досліджень і публікацій. Сучасні дослідження у сфері аудиту кібербезпеки дедалі частіше акцентують увагу на переході від статичних періодичних перевірок до ризик-орієнтованих і більш гнучких підходів. Це пов'язано з тим, що чинники кіберризиків підприємства можуть змінюватися швидше, ніж завершується традиційний аудиторський цикл: з'являються нові вразливості, фіксуються інциденти, змінюються конфігурації систем, а окремі порушення можуть впливати на пов'язані сервіси та бізнес-процеси. У попередніх дослідженнях також підкреслено, що застосування штучного інтелекту в аудиті кібербезпеки підприємства відкриває можливості для автоматизації аналізу ризиків, виявлення аномалій і підтримки прийняття рішень аудитора [2].

Водночас NIST Cybersecurity Framework 2.0 розглядає управління кіберризиками як безперервний процес, що охоплює ідентифікацію, оцінювання, пріоритизацію та комунікацію ризиків у межах організації [4]. Такий підхід створює передумови для врахування актуального ризикового контексту під час планування аудиторських перевірок.

Окремим аспектом є нормативно-регуляторне середовище проведення аудиту кібербезпеки. Як показано у [4], підходи до аудиту кібербезпеки в різних регіонах світу відрізняються за законодавчими вимогами, рівнем формалізації процедур та очікуваннями щодо відповідності, що також впливає на планування аудиторських перевірок.

У межах ISO/IEC 27001:2022 аудит і контроль відповідності розглядаються як складові системи управління інформаційною безпекою, що має підтримувати постійне вдосконалення та ризик-орієнтоване управління захистом інформації [6]. Водночас ISO/IEC 27005:2022 описує підхід до управління інформаційними ризиками, що охоплює ідентифікацію, оцінювання, оброблення, моніторинг і перегляд ризиків [7]. Це є важливим для планування аудиту, оскільки рівень кіберризиків, пов'язаного з активами підприємства, не є сталим і може змінюватися внаслідок появи нових вразливостей і загроз, виникнення інцидентів, зміни конфігурацій або бізнес-критичності окремих сервісів.

Структурованість і відтворюваність аудиторських процедур є важливими умовами організації аудиту інформаційної безпеки, зокрема на етапах управління програмою аудиту, його планування та проведення [8]. Відповідно, запропонований у цій роботі механізм не розглядається як самостійна методика проведення аудиту та не замінює встановлених процедур визначення критеріїв аудиту, збирання аудиторських доказів, оцінювання відповідності й формування висновків. Його функція обмежується підтримкою етапу планування шляхом визначення пріоритетності перевірок інформаційних активів у межах прийнятої в організації програми аудиту.

У наукових і практичних підходах значна увага приділяється оцінюванню ризиків інформаційної безпеки, визначенню критичності активів, використанню даних систем моніторингу, засобів виявлення інцидентів, сканерів вразливостей і баз конфігурацій. Такі джерела дають змогу отримувати актуальну інформацію про стан активів підприємства. Водночас наявність цих даних сама собою не визначає, як саме слід змінювати порядок аудиторських перевірок за умов обмежених ресурсів.

Окремим напрямом досліджень є визначення пріоритетності вразливостей з урахуванням технічних індикаторів кіберризиків. Традиційні підходи, що спираються лише на формальний рівень серйозності вразливості, поступово доповнюються контекстними та динамічними показниками, які враховують можливість її експлуатації, особливості середовища організації, критичність активу та обмеженість ресурсів на усунення вразливостей [9] - [11]. Огляд сучасних досліджень із визначення пріоритетності вразливостей (vulnerability prioritization) також показує актуальність переходу до контекстно орієнтованих підходів (context-aware approaches), які поєднують рівень серйозності вразливості (severity), можливість її експлуатації (exploitability), прогностичні показники (predictive indicators) та особливості середовища організації (organizational context) [12].

Отже, наявні дослідження і стандарти створюють основу для ризик-орієнтованого проведення аудиту, оцінювання критичності активів, використання оперативних даних безпеки та пріоритизації



вразливостей. Водночас недостатньо дослідженим залишається питання формалізованого адаптивного визначення черговості перевірки інформаційних активів у межах установленої програми аудиту, коли їх пріоритетність може переглядатися у відповідь на появу нових вразливостей, інцидентів, аномалій і змін конфігурації з урахуванням критичності активів та доступного аудиторського ресурсу. Саме на розв'язання цієї задачі спрямоване дослідження.

Мета статті. Метою статті є розроблення та сценарна апробація механізму адаптивного визначення пріоритетності перевірок інформаційних активів у межах аудиту кібербезпеки підприємства на основі комплексного оцінювання їх стану та критичності, що дає змогу уточнювати черговість аудиторських процедур відповідно до змін чинників кіберризиків за обмеженого аудиторського ресурсу.

Для досягнення поставленої мети необхідно формалізувати складові комплексного оцінювання стану інформаційних активів, визначити правило розрахунку індексу пріоритетності їх перевірки з урахуванням критичності, описати логіку адаптивного оновлення черговості перевірок за обмежених аудиторських ресурсів, а також продемонструвати працездатність запропонованого механізму на сценарному прикладі зміни чинників кіберризиків та стану кібербезпеки активів.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Для формалізованого опису задачі адаптивного визначення пріоритетності перевірок інформаційна інфраструктура підприємства представляється множиною активів $A = \{a_1, a_2, \dots, a_n\}$, які входять до області відповідного аудиторського завдання. Таке представлення використовується виключно для формалізації задачі визначення черговості перевірок інформаційних активів і не зводить аудит кібербезпеки підприємства загалом до оцінювання стану активів. Кожен актив характеризується рівнем відповідності встановленим вимогам кіберзахисту, поточним динамічним станом безпеки, експертною оцінкою та критичністю для діяльності підприємства [4]–[7].

Для комплексного оцінювання стану кожного активу використовуються три часткові оцінки: C_i - оцінка формальної відповідності активу встановленим вимогам кіберзахисту; D_i - оцінка поточного динамічного стану його безпеки; E_i - експертна оцінка аудитора або профільного фахівця.

Оцінка формальної відповідності C_i може визначатися на основі результатів внутрішніх перевірок, вимог системи управління інформаційною безпекою (Information Security Management System, ISMS), контрольних процедур і статусів виконання заходів безпеки, узгоджених з ISO/IEC 27001:2022 або іншими прийнятими в організації наборами заходів контролю [6]. Наприклад, повністю виконаному заходу контролю може відповідати значення 1,0; частково виконаному – 0,5; запланованому – 0,2; невиконаному – 0 [13]. Для критично важливих заходів контролю доцільно застосовувати вагові коефіцієнти.

Оцінка динамічного стану D_i формується на основі актуальних технічних даних: результатів сканування вразливостей, даних систем управління інформацією та подіями безпеки (Security Information and Event Management, SIEM), засобів виявлення та реагування на кінцевих точках і розширеного виявлення та реагування (Endpoint Detection and Response / Extended Detection and Response, EDR/XDR), подій автентифікації, змін конфігурації, стану управління встановленням виправлень (patch management), показників Загальної системи оцінювання вразливостей (Common Vulnerability Scoring System, CVSS), Системи прогнозування експлуатації вразливостей (Exploit Prediction Scoring System, EPSS) та інших джерел телеметрії [9]–[11]. Оскільки наведені дані характеризують наявність і серйозність вразливостей, можливість їх експлуатації та своєчасність встановлення виправлень, їх необхідно привести до єдиної шкали оцінювання. У запропонованій моделі застосовується обернена шкала: що вищою є актуальна небезпека для активу, то нижчим є значення D_i .

Експертна оцінка E_i формується аудитором або профільним фахівцем і призначена для врахування факторів, які не завжди повністю відображаються у формалізованих контрольних процедурах або технічній телеметрії. До таких факторів належать роль активу у бізнес-процесах, чутливість даних, наявність компенсувальних заходів, локальні винятки, особливості експлуатації або результати попередніх перевірок [9].

Коефіцієнт критичності K_i відображає бізнес-значущість активу, його роль у забезпеченні безперервності процесів, вплив на конфіденційність, цілісність і доступність інформації, а також можливі фінансові, репутаційні та пов'язані з невідповідністю нормативним вимогам наслідки компрометації. Коефіцієнт доцільно визначати на основі класифікації активів, аналізу впливу на бізнес (Business Impact Analysis, BIA), вимог власників бізнес-процесів і результатів оцінювання інформаційних ризиків відповідно до ISO/IEC 27005:2022 та підходів до оцінювання критичності активів (asset criticality assessment) [7], [14]–[15].



Для забезпечення відтворюваності результатів усі часткові оцінки нормуються до інтервалу $[0;1]$, а для кожного циклу планування фіксуються критерії оцінювання, джерела та момент отримання вхідних даних, правила їх нормування, шкали часткових оцінок і значення вагових коефіцієнтів. Для складових C_i , D_i та E_i більше значення відповідає кращому стану активу, тоді як для коефіцієнта критичності K_i більше значення відповідає вищій бізнес-значущості активу. За однакового набору вхідних даних та параметрів механізму розрахунок узагальненої оцінки стану, індексу пріоритетності та підсумкового ранжування є детермінованим і може бути повторений іншим аудитором. Експертна складова E_i визначається відповідно до попередньо встановлених критеріїв, а присвоєне значення та його обґрунтування мають документуватися.

$$S_i = \alpha C_i + \beta D_i + \gamma E_i, \quad (1)$$

де S_i - узагальнена оцінка стану активу; C_i - оцінка формальної відповідності активу вимогам кіберзахисту; D_i - оцінка поточного динамічного стану безпеки; E_i - експертна оцінка; α , β , γ - вагові коефіцієнти відповідних складових, для яких виконується умова:

$$\alpha + \beta + \gamma = 1. \quad (2)$$

У межах цієї статті для сценарної апробації використано такий експертно заданий набір ваг:

$$\alpha = 0,3; \beta = 0,5; \gamma = 0,2. \quad (3)$$

Такий вибір відображає припущення, що в умовах адаптивного планування аудиту найбільший вплив на зміну пріоритетів має поточний динамічний стан активу D_i , оскільки саме він відображає нові вразливості, аномалії, інциденти, зміни конфігурації та інші актуальні технічні індикатори кіберризiku. Формальна відповідність C_i залишається важливою базовою характеристикою стану захисту, тоді як експертна оцінка E_i виконує коригувальну функцію і дає змогу врахувати чинники, які не повністю відображаються автоматизованими засобами моніторингу.

Зазначений набір ваг не є універсальним для всіх підприємств. У практичному застосуванні він може бути уточнений на основі експертного опитування, методу аналізу ієрархій, історичних даних інцидентів або аналізу чутливості. З огляду на це запропонований механізм слід розглядати як параметризовану модель, у якій вагові коефіцієнти можуть адаптуватися до галузі, регуляторних вимог, зрілості процесів кібербезпеки та доступності телеметрії.

Однак для визначення пріоритетності аудиту недостатньо враховувати лише поточний стан захищеності активу. Актив із помірними технічними проблемами може бути більш пріоритетним для перевірки, якщо він є критично важливим для підприємства. Тому в межах запропонованого механізму використовується коефіцієнт критичності K_i , який належить інтервалу $[0;1]$ і відображає бізнес-значущість активу, його роль у забезпеченні безперервності процесів, наслідки невідповідності нормативним вимогам, а також потенційний фінансовий або репутаційний збиток.

У межах цієї статті R_i розглядається як нормований індекс пріоритетності аудиту активу, призначений для порівняння та ранжування активів. Він не характеризує абсолютну ймовірність виникнення інциденту і не є повною кількісною оцінкою кіберризiku. Значення індексу відображає поєднання критичності активу та поточного рівня послаблення його захищеності: що вищою є критичність активу і що гіршим є стан його захищеності, то більш нагальною є потреба в аудиторській перевірці. Запропонована логіка використовує загальний ризик-орієнтований принцип урахування значущості об'єкта та актуального стану ризiku, тоді як конкретний спосіб обчислення індексу є складовою розробленого в цій роботі механізму [7], [16].

Базовий індекс пріоритетності аудиту активу пропонується визначати за формулою

$$R_i = K_i(1 - S_i), \quad (4)$$

де R_i - базовий індекс пріоритетності аудиту активу; K_i - коефіцієнт критичності активу; S_i - узагальнена оцінка стану активу. Якщо стан захищеності активу погіршується, значення $1 - S_i$ зростає. Якщо водночас актив має високу критичність, збільшується і його індекс пріоритетності аудиту. Отже, активи з найбільшими значеннями R_i мають перевірятися першочергово.

У розширеному варіанті механізму доцільно враховувати залежності між активами, оскільки порушення роботи одного компонента може впливати на функціонування пов'язаних сервісів. Додатково

актуальність урахування комплексного характеру інцидентів підтверджується даними Unit 42, відповідно до яких 87 % досліджених кібератак охоплювали кілька поверхонь атаки одночасно [3]. Наприклад, порушення роботи сервера автентифікації може впливати на доступ до прикладних систем, баз даних або файлових ресурсів.

Для врахування впливу залежностей між активами може бути використаний розширений індекс пріоритетності аудиту:

$$R_i^* = R_i + \lambda \sum_{j \neq i}^n \omega_{ji} R_j, \quad (5)$$

де R_i^* - розширений індекс пріоритетності аудиту активу з урахуванням залежностей; R_i - базовий індекс пріоритетності аудиту активу; ω_{ji} - коефіцієнт впливу активу a_j на актив a_i ; λ - коефіцієнт чутливості до поширення впливу між активами.

Якщо карта залежностей між активами відсутня або є недостатньо достовірною, механізм може працювати на основі базового індексу R_i . Якщо така карта доступна, доцільно використовувати розширений індекс R_i^* , що дає змогу врахувати можливе поширення впливу між пов'язаними активами [17]-[18]. На відміну від базового індексу R_i , значення R_i^* без додаткового нормування не обов'язково обмежується інтервалом $[0;1]$, тому розширений індекс використовується насамперед для порівняння та ранжування активів.

Адаптивне визначення пріоритетності перевірок інформаційних активів реалізується як циклічний процес. На кожному циклі оновлюються значення формальної відповідності, динамічного стану, експертної оцінки та критичності активів. Після цього обчислюється узагальнена оцінка стану активу, визначається його індекс пріоритетності аудиту та формується оновлений порядок аудиторських перевірок. Якщо ресурс аудиту обмежений і за один цикл можливо перевірити лише m активів, у межах запропонованого механізму першочергово обираються активи з найбільшими значеннями індексу пріоритетності R_i .

Загальну послідовність реалізації запропонованого механізму подано на рис. 1. Схема передбачає формування множини активів підприємства, збір і нормування вхідних показників, розрахунок узагальненої оцінки стану, визначення базового або розширеного індексу пріоритетності, ранжування активів і формування плану аудиторських перевірок з урахуванням обмеженого ресурсу. Циклічний характер схеми забезпечує регулярне оновлення пріоритетів аудиту відповідно до змін чинників кіберризиків та поточного стану кібербезпеки активів.



Рис. 1. Схема адаптивного визначення пріоритетності перевірок інформаційних активів у межах аудиту кібербезпеки підприємства

Якщо трудомісткість перевірки різних активів відрізняється, задачу можна подати як задачу вибору активів за обмеженого ресурсу:

$$\max \sum_{i=1}^n R_i x_i, \quad (6)$$

за умови:

$$\sum_{i=1}^n t_i x_i \leq B, \quad (7)$$

де $x_i \in \{0,1\}$ - змінна вибору активу для включення до плану аудиту; t_i - трудомісткість перевірки активу; B - загальний доступний ресурс аудиторської групи. Така постановка дає змогу не лише ранжувати активи за індексом пріоритетності аудиту, а й формувати практично придатний план перевірок з урахуванням обмежених ресурсів.

Відтак запропонований механізм поєднує оцінювання стану активів, їхньої критичності та можливих залежностей між ними. Його результатом є уточнений порядок перевірок інформаційних активів у межах установленної програми аудиту з урахуванням їх поточного стану кібербезпеки та критичності. Для демонстрації логіки роботи такого підходу в наступному розділі проведено сценарну апробацію на прикладі умовного набору активів підприємства.



МЕТОДИКА ДОСЛІДЖЕННЯ

Методика сценарної апробації механізму. Для демонстрації працездатності запропонованого механізму проведено сценарну апробацію на прикладі умовного підприємства, інформаційна інфраструктура якого містить декілька взаємопов'язаних активів. Такий підхід не є повноцінною емпіричною перевіркою на реальних даних підприємства, однак дає змогу продемонструвати логіку роботи механізму в умовах зміни чинників кіберризиків. Основна увага приділяється тому, чи здатний механізм змінювати порядок аудиторських перевірок після оновлення оцінок стану активів.

У межах сценарної апробації розглянуто вісім активів підприємства: ERP/DB-сервер, VPN-шлюз, поштовий шлюз, файловий сервер, сервер автентифікації, CRM-систему, вебпортал підприємства та робочі станції фінансового відділу. Такий набір активів дає змогу відобразити як критичні серверні компоненти, так і мережеві, прикладні та користувацькі елементи інфраструктури.

Сценарії апробації сформовано з урахуванням актуальних тенденцій, наведених у Global Incident Response Report 2026 компанії Unit 42. Зокрема, у звіті підкреслено прискорення життєвого циклу атак, зростання ролі слабких місць у керуванні ідентифікаційними даними, поширення інцидентів на декілька поверхонь атаки одночасно, а також підвищення значущості хмарних середовищ і програмного забезпечення як послуги (Software as a Service, SaaS). Наведені сценарії не відтворюють конкретних інцидентів, а використовуються як узагальнені приклади зміни чинників кіберризиків [3].

Для кожного активу використовуються визначені у попередньому розділі показники C_i , D_i , E_i , коефіцієнт критичності K_i , узагальнена оцінка стану S_i та відповідний індекс пріоритетності аудиту.

На першому етапі сценарної апробації формується початковий порядок перевірок інформаційних активів, що відповідає умовно статичному підходу. Порядок перевірок визначається на початку аудиторського циклу та фіксується до появи нових результатів оцінювання. Для кожного активу обчислюються узагальнена оцінка стану S_i та базовий індекс пріоритетності аудиту R_i відповідно до формул (1) та (4).

На наступному етапі моделюється зміна чинників кіберризиків. Для VPN-шлюзу передбачається поява критичної вразливості та аномальних спроб автентифікації, для поштового шлюзу - збільшення кількості фішингових повідомлень і підозрілої активності, а для сервера автентифікації - помірне погіршення динамічного стану, що може впливати на пов'язані сервіси. Для інших активів передбачено відсутність суттєвих змін або незначні коливання оцінок.

Після оновлення даних про чинники кіберризиків для кожного активу повторно обчислюються узагальнена оцінка стану S_i та індекс пріоритетності аудиту R_i . На основі отриманих значень активи повторно ранжуються і формується адаптивно оновлений порядок перевірок. Якщо після оновлення оцінок значення R_i певного активу зростає, цей актив переміщується вище в порядку перевірок. Таким чином перевіряється здатність запропонованого механізму змінювати порядок перевірок відповідно до поточного стану кібербезпеки активів, а не лише зберігати початково визначену послідовність.

Для наближення сценарної апробації до практичних умов встановлено обмеження аудиторського ресурсу: у межах одного циклу аудиторська група може перевірити лише три активи. За таких умов порівнюються два варіанти визначення черговості перевірок: початковий порядок, сформований до зміни чинників кіберризиків, та адаптивно оновлений порядок, сформований після повторного обчислення індексів пріоритетності й ранжування активів.

Для порівняння початкового та адаптивно оновленого порядків перевірок використовуються сума індексів пріоритетності аудиту активів, включених до першочергової перевірки, і середнє значення індексу пріоритетності цих активів. Сума індексів характеризує сукупну пріоритетність активів, включених до першочергової перевірки, і може перевищувати 1, оскільки утворюється шляхом додавання значень для декількох активів. Середнє значення індексу належить інтервалу $[0;1]$ і забезпечує нормоване порівняння початкового та адаптивно оновленого порядків перевірок.

Запропонована методика сценарної апробації дає змогу порівняти початковий та адаптивно оновлений порядок перевірок інформаційних активів.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Результати сценарної апробації механізму. Для сценарної апробації розглянуто умовний набір активів підприємства, до якого включено ERP/DB-сервер, VPN-шлюз, поштовий шлюз, файловий сервер, сервер автентифікації, CRM-систему, вебпортал підприємства та робочі станції фінансового відділу. Для кожного активу визначено узагальнену оцінку стану та індекс пріоритетності аудиту відповідно до формул, наведених у попередньому розділі.



Результати повторного обчислення індексів після зміни чинників кіберризиків засвідчили зміну пріоритетності окремих активів. Індекс пріоритетності VPN-шлюзу зріс з 0,243 до 0,404, унаслідок чого він перемістився з другого на перше місце у плані перевірок. Для сервера автентифікації індекс зріс з 0,229 до 0,321, а його пріоритет змінився з п'ятого на друге місце. Для поштового шлюзу значення індексу збільшилося з 0,212 до 0,308, що зумовило його переміщення із шостого на третє місце. Таким чином, після оновлення даних про чинники кіберризиків порядок першочергових перевірок було скориговано відповідно до актуальних значень показників стану та критичності активів.

Таблиця 1

Зміна індексів пріоритетності аудиту після оновлення даних про чинники кіберризиків

Актив	Основна зміна чинників кіберризиків	R_i до зміни	Пріоритет до зміни	R_i після зміни	Пріоритет після зміни
VPN-шлюз	Критична вразливість, аномальні спроби автентифікації	0,243	2	0,404	1
Сервер автентифікації	Підозрілі події доступу	0,229	5	0,321	2
Поштовий шлюз	Зростання фішингової активності	0,212	6	0,308	3
Вебпортал підприємства	Незначне погіршення динамічного стану	0,246	1	0,261	4
Робочі станції фінансового відділу	Помірне погіршення стану	0,242	3	0,256	5
CRM-система	Несуттєві зміни	0,234	4	0,242	6
ERP/DB-сервер	Незначне погіршення стану	0,203	7	0,222	7
Файловий сервер	Без суттєвих змін	0,154	8	0,161	8

Для ілюстрації розглянемо розрахунок індексу пріоритетності аудиту VPN-шлюзу, який після оновлення даних про чинники кіберризиків отримав найвищий пріоритет у порядку перевірок. До відповідних змін для цього активу задано такі значення:

$$C_i = 0,80; D_i = 0,67; E_i = 0,70; K_i = 0,85. \quad (8)$$

Тоді узагальнена оцінка стану активу становить:

$$S_i = 0,3 \cdot 0,80 + 0,5 \cdot 0,67 + 0,2 \cdot 0,70 = 0,715. \quad (9)$$

Базовий індекс пріоритетності аудиту дорівнює:

$$R_i = 0,85 \cdot (1 - 0,715) = 0,242 \approx 0,243. \quad (10)$$

Після появи критичної вразливості та аномальних спроб автентифікації оцінка динамічного стану VPN-шлюзу знижується до:

$$D_i = 0,29. \quad (11)$$

За незмінних значень формальної відповідності, експертної оцінки та критичності отримаємо:

$$S_i = 0,3 \cdot 0,80 + 0,5 \cdot 0,29 + 0,2 \cdot 0,70 = 0,525. \quad (12)$$



Відповідно індекс пріоритетності аудиту становить:

$$R_i = 0,85 \cdot (1 - 0,525) = 0,404. \quad (13)$$

Отже, погіршення поточного динамічного стану безпеки VPN-шлюзу призводить до зростання індексу пріоритетності аудиту:

$$0,243 \rightarrow 0,404.$$

Це обґрунтовує переміщення VPN-шлюзу на перше місце в оновленому плані аудиту.

Оскільки вагові коефіцієнти в цій статті задано експертно, отримані числові значення слід інтерпретувати як демонстраційні. Водночас логіка роботи механізму не залежить від конкретного набору ваг: за зміни α , β та γ перерахунок S_i і R_i може бути повторений, а порядок перевірок активів може бути перевірений на стійкість. У подальших дослідженнях доцільно провести аналіз чутливості для кількох наборів ваг і визначити, наскільки стабільним залишається ранжування активів.

За початкового порядку до першочергової перевірки було б включено вебпортал підприємства, VPN-шлюз і робочі станції фінансового відділу. Після адаптивного повторного обчислення до першочергової перевірки включаються VPN-шлюз, сервер автентифікації та поштовий шлюз. Отже, запропонований механізм дає змогу змінити порядок перевірок відповідно до поточного стану кібербезпеки активів, а не зберігати початково визначену черговість.

Якщо аудиторський ресурс обмежений трьома перевітками протягом одного циклу, для порівняння двох порядків перевірок використовується сума індексів пріоритетності аудиту активів, включених до першочергової перевірки. Цей показник не є ймовірністю настання інциденту або кількісною оцінкою ризику, а характеризує сукупну пріоритетність активів, охоплених планом.

Для коректного порівняння обидва варіанти порядку перевірок оцінюються за актуальними значеннями індексів після оновлення даних про чинники кіберризiku.

Для початкового порядку перевірок:

$$R_{\Sigma}^{static} = 0,261 + 0,404 + 0,256 = 0,921. \quad (14)$$

Для адаптивно оновленого порядку перевірок:

$$R_{\Sigma}^{adaptive} = 0,404 + 0,321 + 0,308 = 1,033. \quad (15)$$

Оскільки R_{Σ} є сумою індексів пріоритетності декількох активів, його значення може перевищувати 1. За трьох активів теоретичний інтервал суми становить $[0;3]$. Тому значення 1,033 не суперечить умові $R_i \in [0; 1]$, яка застосовується до індексу окремого активу.

Для нормованого порівняння додатково розраховано середнє значення індексу пріоритетності аудиту активів першочергової перевірки:

$$R_{static} = \frac{0,921}{3} = 0,307, \quad (16)$$

$$R_{adaptive} = \frac{1,033}{3} = 0,344. \quad (17)$$

Отже, адаптивно оновлений порядок забезпечує вище середнє значення індексу пріоритетності аудиту активів, включених до першочергової перевірки. Це свідчить про спрямування обмеженого аудиторського ресурсу на активи, які на момент планування мають вищі значення розрахованого індексу пріоритетності.

Отримані результати свідчать, що запропонований механізм реагує на зміну чинників кіберризiku не шляхом ручного коригування плану, а через повторне обчислення індексів пріоритетності аудиту активів. Найбільш показовим є приклад VPN-шлюзу, який після появи критичної вразливості та аномальних спроб автентифікації переміщується на перше місце у плані аудиту. Це демонструє здатність механізму підвищувати пріоритет активів, поточний стан кібербезпеки яких суттєво погіршується.

Важливим також є зростання пріоритету сервера автентифікації та поштового шлюзу. У першому випадку це пояснюється високою критичністю активу для забезпечення доступу до інших сервісів



підприємства, у другому - збільшенням фішингової активності, що може призвести до компрометації облікових записів і подальшого поширення інциденту [3]. Отже, механізм враховує не лише формальний рівень відповідності активу вимогам безпеки, а й актуальні технічні індикатори кіберризиків.

Порівняння початкового та адаптивно оновленого порядків перевірок показує, що за обмежених аудиторських ресурсів адаптивне оновлення дає змогу першочергово перевіряти активи з вищими актуальними значеннями індексу пріоритетності аудиту. Це є важливим для практичної діяльності аудиторської групи, оскільки в реальних умовах неможливо одночасно перевірити всі активи підприємства. Тому порядок перевірок має визначатися не лише попередньо сформованим календарним планом, а й поточним станом кібербезпеки та критичністю активів.

Водночас результати сценарної апробації слід розглядати як демонстрацію методики роботи механізму, а не як підтвердження його ефективності на реальному підприємстві. Для практичного впровадження необхідно забезпечити якісні джерела даних, коректне нормування показників, регулярне оновлення оцінок і налаштування вагових коефіцієнтів відповідно до особливостей конкретної організації. Однак навіть у такому вигляді механізм зберігає важливу перевагу - він є прозорим і пояснюваним, оскільки аудитор може визначити, за рахунок яких саме факторів актив отримав вищий пріоритет.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті обґрунтовано доцільність адаптивного уточнення пріоритетності перевірок інформаційних активів у межах аудиту кібербезпеки підприємства з урахуванням змін чинників кіберризиків, поточного стану та критичності активів. Запропонований механізм поєднує оцінку формальної відповідності вимогам кіберзахисту, поточний динамічний стан безпеки та експертну оцінку в єдину узагальнену оцінку стану активу, на основі якої визначається індекс пріоритетності аудиту.

Показано, що для визначення пріоритетності аудиту недостатньо враховувати лише рівень відповідності активу вимогам безпеки. Важливими є також критичність активу для діяльності підприємства, актуальні технічні індикатори кіберризиків та, за наявності відповідних даних, взаємозалежності між активами інформаційної інфраструктури. Це дає змогу формувати порядок аудиторських перевірок не за інерційним або суто календарним принципом, а відповідно до поточного стану кібербезпеки та критичності активів.

Проведена сценарна апробація показала, що після зміни чинників кіберризиків запропонований механізм забезпечує повторне обчислення індексів пріоритетності активів і відповідне оновлення порядку аудиторських перевірок. Це демонструє потенційну практичну застосовність механізму для підтримки прийняття рішень в умовах обмежених аудиторських ресурсів.

Порівняння початкового та адаптивно оновленого порядків перевірок засвідчило, що після адаптивного оновлення до першочергової перевірки включаються активи з вищим середнім значенням індексу пріоритетності. Отже, запропонований механізм може бути використаний як прозорий та пояснюваний засіб підтримки прийняття рішень під час планування перевірок інформаційних активів у межах аудиту кібербезпеки підприємства. Він не замінює встановлених критеріїв, процедур і методик проведення аудиту, збирання аудиторських доказів та формування аудиторських висновків. Подальші дослідження доцільно спрямувати на уточнення вагових коефіцієнтів, використання реальних даних телеметрії та експериментальну перевірку механізму на прикладі інфраструктури конкретного підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Криворучко, О. В., & Гнатченко, Д. Д. (2024). Функціональні особливості інтелектуальної системи внутрішнього аудиту. *Кібербезпека: освіта, наука, техніка*, 4(24), 40–49. <https://doi.org/10.28925/2663-4023.2024.24.4049>
2. Куперштейн, Л. М., Волинець, В. В., & Войтович, О. П. (2026). Аналіз сучасних підходів та перспектив застосування штучного інтелекту в аудиті кібербезпеки підприємства. *Наукові праці Вінницького національного технічного університету*, (1). <https://praci.vntu.edu.ua/index.php/praci/article/view/923>
3. Palo Alto Networks, Unit 42. (2026). Global incident response report 2026. https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/unit42/Unit42-Global-Incident-Response-Report.pdf
4. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>



5. Войтович, О., & Волинець, В. (2025). Особливості законодавства щодо аудиту кібербезпеки в різних регіонах світу. *Вимірювальна та обчислювальна техніка в технологічних процесах*, (3), 23–29. <https://doi.org/10.31891/2219-9365-2025-83-3>
6. International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. <https://www.iso.org/standard/27001>
7. International Organization for Standardization. (2022). *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection—Guidance on managing information security risks*. <https://www.iso.org/standard/80585.html>
8. Chalyi, O., & Toliupa, S. (2025). Comparison of international audit standards for information security with automation perspectives. *Cybersecurity: Education, Science, Technique*, 3(31), 579–588. <https://doi.org/10.28925/2663-4023.2025.31.1046>
9. Souppaya, M., & Scarfone, K. (2022). *Guide to enterprise patch management planning: Preventive maintenance for technology* (NIST Special Publication 800-40 Rev. 4). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-40r4>
10. Forum of Incident Response and Security Teams. (2023). *Common Vulnerability Scoring System version 4.0: Specification document*. <https://www.first.org/cvss/v4.0/specification-document>
11. Forum of Incident Response and Security Teams. (n.d.). *Exploit Prediction Scoring System (EPSS)*. Retrieved June 30, 2026, from <https://www.first.org/eps/>
12. Jiang, Y., Oo, N., Meng, Q., Lim, H. W., & Sikdar, B. (2025). A survey on vulnerability prioritization: Taxonomy, metrics, and research challenges. arXiv. <https://arxiv.org/abs/2502.11070>
13. Адміністрація Державної служби спеціального зв'язку та захисту інформації України. (2026). *Методичні рекомендації щодо проведення самооцінювання поточного стану кіберзахисту (Додаток до наказу Адміністрації Держспецзв'язку від 16.04.2026 № 285 «Деякі питання проведення оцінювання стану кіберзахисту»*. <https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspetszv-yazku-vid-16-04-2026-285-deyaki-pitannya-provedennya-ocinyuvannya-stanu-kiberzakhistu>
14. Korobeinikova, T., Shapovalov, B., Zhuravel, I., & Romanyuk, O. (2025). A weighted expert-based method for asset criticality assessment in cyber risk evaluation. In *2025 15th International Conference on Advanced Computer Information Technologies (ACIT)*. IEEE. <https://doi.org/10.1109/ACIT65614.2025.11185835>
15. Masukume, M., Mhlanga, S., Mubvirwi, T., & Mushiri, T. (2020). Development of an asset criticality assessment tool: The case of a fertiliser manufacturing company. In *Proceedings of the 2nd African International Conference on Industrial Engineering and Operations Management*. <https://www.ieomsociety.org/harare2020/papers/117.pdf>
16. Ghazouani, M., Medromi, H., Sayouti, A., & Faris, S. (2014). Information security risk assessment: A practical approach with a mathematical formulation of risk. *International Journal of Computer Applications*, 103(8). <https://doi.org/10.5120/18097-9155>
17. Kostiuk, Y., Skladannyi, P., Samoilenko, Y., Khorolska, K., Bebesko, B., & Sokolov, V. (2025). A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps. In *Cyber Hygiene & Conflict Management in Global Information Networks 2024* (CEUR Workshop Proceedings, Vol. 3925, pp. 249–264). <https://ceur-ws.org/Vol-3925/>
18. Jiang, Y., Oo, N., Meng, Q., Lim, H. W., & Sikdar, B. (2025). *VulRG: Multi-level explainable vulnerability patch ranking for complex systems using graphs*. arXiv. <https://arxiv.org/abs/2502.11143>

**Vitalii Volynets**

Postgraduate Student, Department of Information Security
Vinnytsia National Technical University, Vinnytsia, Ukraine
ORCID: 0009-0006-7999-1290
volynets1026@gmail.com

Olesya Voytovych

Ph.D., Associate Professor, Associate Professor of Information Security Department
Vinnytsia National Technical University, Vinnytsia, Ukraine
ORCID: 0000-0001-8964-7000
voytovych.olesya@vntu.edu.ua

MECHANISM FOR ADAPTIVE PLANNING OF ENTERPRISE CYBERSECURITY AUDITS BASED ON COMPREHENSIVE ASSESSMENT OF ASSET SECURITY STATE AND CRITICALITY

Abstract. The article proposes a mechanism for adaptive planning of enterprise cybersecurity audits based on a comprehensive assessment of the security state and criticality of information assets. The mechanism is considered as a decision-support tool for the audit planning stage and is intended to determine the priority of information asset checks within an established audit program. The comprehensive assessment combines formal compliance with cybersecurity requirements, the current dynamic security state, and expert assessment performed by an auditor or a relevant specialist. Asset business significance is additionally represented by a criticality coefficient. Based on these indicators, an integrated asset security-state score is formed and an audit priority index is calculated. The index is used to rank information assets and adaptively refine the order of their checks when audit resources are limited. The mechanism allows priorities to be recalculated when new vulnerabilities, anomalous events, incidents, configuration changes, or other cybersecurity risk factors occur. To ensure reproducibility, the sources and timing of input data, normalization rules, assessment scales, and weighting coefficients are documented. A scenario-based evaluation was performed using eight information assets of a hypothetical enterprise. After the deterioration of the security state of selected assets was modeled, the priority indices were recalculated, resulting in a change in the order of first-priority checks. With the available audit resource limited to three checks per cycle, the mean priority index of the assets selected for first-priority examination increased from 0.307 for the initial order to 0.344 for the adaptively updated order. The obtained results demonstrate the operability of the mechanism as a decision-support tool for prioritizing information asset checks and require further validation using real enterprise data.

Keywords: cybersecurity; cybersecurity audit; information assets; asset criticality; cyber risk; prioritization; decision-making; adaptive planning.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Kryvoruchko, O., & Hnatchenko, D. (2024). Functional features of an intelligent internal audit support system. *Cybersecurity: Education, Science, Technique*, 4(24), 40–49. <https://doi.org/10.28925/2663-4023.2024.24.4049>
2. Kupershtein, L. M., Volynets, V. V., & Voytovych, O. P. (2026). Analysis of modern approaches and prospects for the application of artificial intelligence in enterprise cybersecurity audit. *Scientific Works of Vinnytsia National Technical University*, (1). <https://praci.vntu.edu.ua/index.php/praci/article/view/923> (in Ukrainian)
3. Palo Alto Networks, Unit 42. (2026). Global incident response report 2026. https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/unit42/Unit42-Global-Incident-Response-Report.pdf
4. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>
5. Voytovych, O., & Volynets, V. (2025). Peculiarities of cybersecurity audit legislation in different regions of the world. *Measuring and Computing Devices in Technological Processes*, (3), 23–29. <https://doi.org/10.31891/2219-9365-2025-83-3> (in Ukrainian)



6. International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. <https://www.iso.org/standard/27001>
7. International Organization for Standardization. (2022). *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection—Guidance on managing information security risks*. <https://www.iso.org/standard/80585.html>
8. Chalyi, O., & Toliupa, S. (2025). Comparison of international audit standards for information security with automation perspectives. *Cybersecurity: Education, Science, Technique*, 3(31), 579–588. <https://doi.org/10.28925/2663-4023.2025.31.1046>
9. Souppaya, M., & Scarfone, K. (2022). *Guide to enterprise patch management planning: Preventive maintenance for technology* (NIST Special Publication 800-40 Rev. 4). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-40r4>
10. Forum of Incident Response and Security Teams. (2023). *Common Vulnerability Scoring System version 4.0: Specification document*. <https://www.first.org/cvss/v4.0/specification-document>
11. Forum of Incident Response and Security Teams. (n.d.). *Exploit Prediction Scoring System (EPSS)*. Retrieved June 30, 2026, from <https://www.first.org/epss/>
12. Jiang, Y., Oo, N., Meng, Q., Lim, H. W., & Sikdar, B. (2025). *A survey on vulnerability prioritization: Taxonomy, metrics, and research challenges*. arXiv. <https://arxiv.org/abs/2502.11070>
13. Administration of the State Service of Special Communications and Information Protection of Ukraine. (2026). *Methodological recommendations for self-assessment of the current state of cyber protection (Appendix to Order No. 285 of April 16, 2026, “Some issues of assessing the state of cyber protection”)*. <https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-16-04-2026-285-deyaki-pitannya-provedennya-ocinyuvannya-stanu-kiberzakhistu> (in Ukrainian)
14. Korobeinikova, T., Shapovalov, B., Zhuravel, I., & Romanyuk, O. (2025). A weighted expert-based method for asset criticality assessment in cyber risk evaluation. In *2025 15th International Conference on Advanced Computer Information Technologies (ACIT)*. IEEE. <https://doi.org/10.1109/ACIT65614.2025.11185835>
15. Masukume, M., Mhlanga, S., Mubvirwi, T., & Mushiri, T. (2020). Development of an asset criticality assessment tool: The case of a fertiliser manufacturing company. In *Proceedings of the 2nd African International Conference on Industrial Engineering and Operations Management*. <https://www.ieomsociety.org/harare2020/papers/117.pdf>
16. Ghazouani, M., Medromi, H., Sayouti, A., & Faris, S. (2014). Information security risk assessment: A practical approach with a mathematical formulation of risk. *International Journal of Computer Applications*, 103(8). <https://doi.org/10.5120/18097-9155>
17. Kostiuk, Y., Skladannyi, P., Samoilenko, Y., Khorolska, K., Bebesko, B., & Sokolov, V. (2025). A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps. In *Cyber Hygiene & Conflict Management in Global Information Networks 2024 (CEUR Workshop Proceedings, Vol. 3925, pp. 249–264)*. <https://ceur-ws.org/Vol-3925/>
18. Jiang, Y., Oo, N., Meng, Q., Lim, H. W., & Sikdar, B. (2025). *VulRG: Multi-level explainable vulnerability patch ranking for complex systems using graphs*. arXiv. <https://arxiv.org/abs/2502.11143>

Отримано редакцією журналу / Received: 06.08.26

Прорецензовано / Revised: 24.08.26

Схвалено до друку / Accepted: 26.10.26



This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.