https://doi.org/10.31891/2219-9365-2026-85-43
УДК 004.056:621.397.3:004.942

КЛЬОЦ Юрій
Хмельницький національний університет
https://orcid.org/0000-0002-3914-0989
e-mail: klots@khmnu.edu.ua
ДЖУЛІЙ Володимир
Хмельницький національний університет
https://orcid.org/0000-0003-1878-4301
e-mail: dzhuliivm@khmnu.edu.ua
ЧОРНЕНЬКИЙ Святослав
Хмельницький національний університет
https://orcid.org/0009-0000-4882-2001
e-mail: chornenkyisv@khmnu.edu.ua
ЗАПОРОЖЧЕНКО Михайло
Хмельницький національний університет
https://orcid.org/0009-0005-1775-4671
e-mail: zaporozhchenkom@khmnu.edu.ua
ШКРЕБЕТА Владислав
Хмельницький національний університет
https://orcid.org/0009-0005-3283-4688
e-mail: shkrebetav@khmnu.edu.ua

МЕТОД ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ДО КОМПЛЕКСНИХ КІБЕРЗАГРОЗ

У статті запропоновано практичний метод забезпечення стійкості корпоративних інформаційних систем до комплексних кіберзагроз. Метод об'єднує чотири взаємопов'язані контури: багатоджерельний моніторинг подій, оцінювання ризиків у реальному часі, адаптивне реагування на інциденти та кероване відновлення сервісів. Наведено математичну модель для інтегральної оцінки стійкості, референтну архітектуру, алгоритми виконання. Показано, що впровадження методу скорочує середній час виявлення та відновлення, а також підвищує індекс стійкості системи. Робота орієнтована на практичне застосування в організаціях різного масштабу.

Ключові слова: кіберстійкість, корпоративна інформаційна система, комплексні загрози, моніторинг, інцидент, ризик, реагування, відновлення.

YURIY Klots, DZHULIY Volodymyr, CHORNENSKY Sviatoslav,
ZAPOROZHCHENKO Mykhailo, SHKREBETA Vladyslav
Khmelnytsky National University

METHOD OF ENSURING RESILIENCE OF CORPORATE INFORMATION SYSTEMS TO COMPLEX CYBER THREATS

The article proposes a practical method for ensuring the resilience of corporate information systems to complex cyber threats in modern digital environments. The proposed approach is based on the integration of four interconnected operational circuits: multi-source security event monitoring, real-time risk assessment, adaptive incident response, and managed service recovery. The combination of these components makes it possible to form an integrated cyber resilience management framework that supports the continuous functioning of information systems even under conditions of intensive cyber threat exposure. Within the study, a mathematical model for integrated resilience assessment of a corporate information system is developed. The model takes into account threat characteristics, the current state of the protection mechanisms, the time parameters of incident detection, and service recovery processes. In addition, a reference architecture and execution algorithms for implementing the proposed method in practical information and communication infrastructures are presented.

The results of the study demonstrate that the implementation of the proposed approach reduces the average detection and recovery time for cyber incidents and significantly improves the overall system resilience index. An important advantage of the method is the possibility of quantitative assessment of the processes occurring within the protected corporate information system. This capability enables a higher level of formalization of security management processes and improves the justification of decision-making in cybersecurity management. The developed models and methods can be effectively applied for high-level formalization of operational processes of corporate information systems in production enterprises, social institutions, transport facilities, shopping centers, and other organizations where the continuity and reliability of information infrastructure are critically important.

Furthermore, the proposed models and methods can be successfully used in planning and selecting countermeasures against cyber threats within organizational networks. The validity of the proposed approach is justified by the correctness of the initial assumptions, the consistency of the modeling results with general principles of complex information system functioning, and the possibility of practical implementation within modern cybersecurity management frameworks.

Keywords: cyber resilience, corporate information system, complex threats, monitoring, incident, risk, response.

Стаття надійшла до редакції / Received 30.12.2025
Прийнята до друку / Accepted 02.02.2026
Опубліковано / Published 05.03.2026

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Сучасні корпоративні інформаційні системи складаються з великої кількості компонентів: сервери застосунків і баз даних, віртуальна інфраструктура, хмарні сервіси, мережеве обладнання, мобільні та віддалені робочі місця. За таких умов зростає кількість векторів атак і складність їх комбінацій. Традиційний підхід «захист периметру» поступово втрачає ефективність: атаки заходять через фішинг і скомпрометовані облікові записи, використовують вразливості ланцюга постачання, латеральний рух усередині мережі, приховані канали ексфільтрації даних. На перший план виходить стійкість: здатність КІС підтримувати критичні функції під час інцидентів, зменшувати їх вплив на бізнес-процеси та швидко повертатися до нормального стану. Такий підхід вимагає не лише технічних засобів, а й налаштованих процесів і показників ефективності [1,2,3].

Одним із найбільш значущих класів систем, що підлягають захисту від деструктивних впливів, виступають корпоративні інформаційні системи (КІС). Від їхнього успішного функціонування багато в чому залежить ефективність багатьох сучасних підприємств та організацій. Це масштабовані системи, призначені для комплексної автоматизації всіх видів господарської діяльності підприємств, і навіть корпорацій, потребують єдиного управління [1,4,5,8]. Такі системи часто ґрунтуються на поглибленому аналізі даних, широкому використанні систем інформаційної підтримки прийняття рішень, електронному документообігу та діловодстві. КІС організуються на основі комп'ютерних мереж і схильні до мережних атак, але також мають певну специфіку як об'єктів захисту від деструктивних інформаційних впливів, які постійно вчиняються [6,7,11].

Не є рідкістю масштабні мережеві атаки на інформаційну інфраструктуру підприємств і держав. Інша мета зловмисників – хмарна інфраструктура. Хмарні технології використовуються в освіті, науці, банківській сфері. Такі сервіси, як Amazon, GoogleDrive, Dropbox, Яндекс.Диск, не тільки налічують сотні мільйонів приватних користувачів, але і пропонують корпоративні акаунти організаціям. Несанкціонований доступ зловмисника до хмарних сховищ дозволяє йому отримати не лише дані про користувачів (включно з такою інформацією, як реквізити платіжних карток, паролі від акаунтів, копії посвідчень особи), а й дані, що становлять комерційну та навіть, можливо, державну таємницю [9,10,13, 24,25].

Поняття стійкості корпоративної інформаційної системи є здатністю системи залишатися функціональною та доступною, продовжувати працювати без збоїв, навіть якщо відбуваються атаки та інші передбачувані й непередбачувані події. Тобто, попри несприятливі зовнішні чи внутрішні впливи, стійкість корпоративної ІС дозволяє системі забезпечувати безперервність бізнес-процесів. І це є дуже важливим тому, що її порушення може призвести до катастрофічних наслідків для компанії. Цими наслідками можуть бути фінансові втрати, втрата репутації та довіри, порушення операційної діяльності, втрата даних та юридичні ризики [3,13,14].

Критерії оцінювання стійкості для цих систем є дуже важливими для забезпечення стійкості корпоративної інформаційної системи. Вони дозволяють компаніям не просто реагувати на збої, а активно запобігати їм і планувати ефективне відновлення. Що в свою чергу дозволяє планувати безперервність бізнесу, ефективно інвестувати та підвищувати рівень конкурентоздатності [14,16,27].

Оцінювання стійкості корпоративної ІС відбувається за кількома ключовими критеріями, що дозволяють визначити її слабкі місця та потенціал для відновлення. До цих критеріїв належить безвідмовність, надійність, відновлюваність, масштабованість, безпека, гнучкість. Безвідмовність визначає, наскільки система доступна для використання та вимірюється, як правило, у відсотках часу, протягом якого система працює без збоїв. Надійність стосується здатності системи виконувати свої функції стабільно та без помилок протягом певного періоду часу. Відновлюваністю це є швидкість і ефективність, з якою система може повернутися до нормального стану після збою. Масштабованість це здатність системи ефективно адаптуватися до зростання навантаження, наприклад, збільшення кількості користувачів або обсягу даних, не втрачаючи при цьому своєї продуктивності та стабільності. Безпекою є рівень захищеності від несанкціонованого доступу, кібератак, вірусів та інших загроз. Цей критерій є основою стійкості, бо запобігає збоям, спричиненим зловмисниками. Гнучкість є можливістю системи адаптуватися до змін, гнучка система легше інтегрується з новими інструментами та оновлюється без значних перерв [3,21,22,26,27]. Усі ці критерії зображені на рис. 1.

Наведені критерії не існують окремо, а вони тісно взаємопов'язані та формують єдину систему. Оцінювання стійкості, що враховує всі ці взаємозв'язки, дозволяє компаніям не просто реагувати на збої, а будувати проактивну стратегію. Це дає можливість мінімізувати ризики, зменшити потенційні фінансові втрати та забезпечити стабільну роботу ІТ-інфраструктури [5,12,13].

Загрози для інформаційних систем можна класифікувати за кількома критеріями. За джерелом походження вони поділяються на природні (пожежі, повені і т. д.), техногенні (збої обладнання чи програмні помилки) та людські. Людські загрози можуть бути ненавмисними, тобто помилки користувачів, а також можуть бути умисними, а саме зовнішніми (хакерські атаки, фішинг), так і внутрішніми (недобросовісні співробітники) [12,14,21,22]. Схема поділу джерел походження загроз зображено на рис. 2.

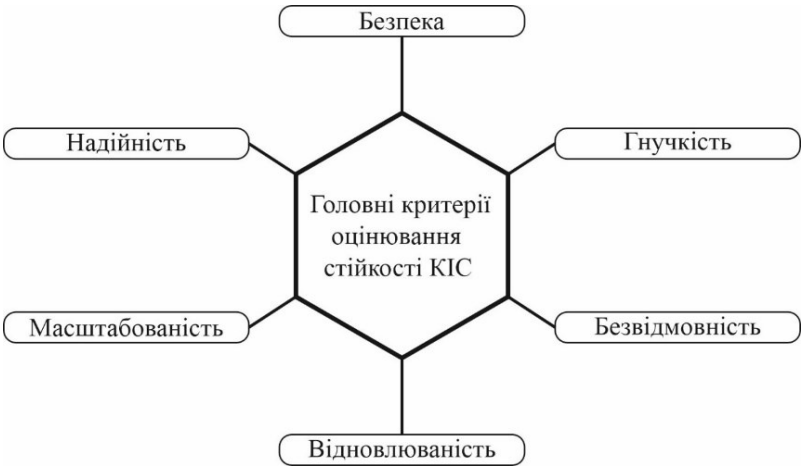

Рис. 1. Головні критерії оцінювання стійкості КІС

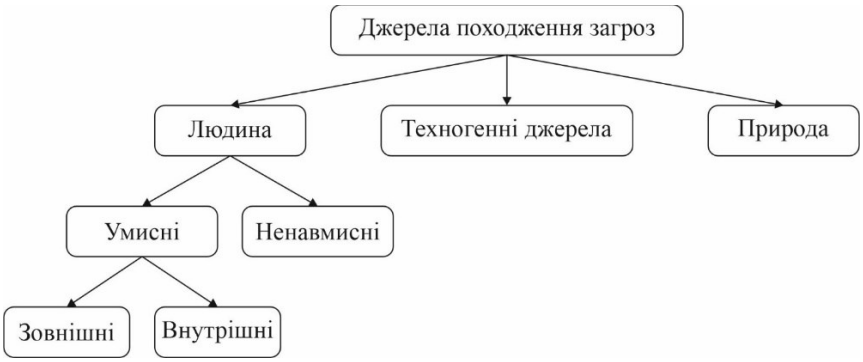

Рис. 2. Джерела походження загроз

За способом реалізації загрози поділяються на фізичні (крадіжка, пожежа), технічні (збої в апаратному забезпеченні), програмні (віруси, трояни) та організаційні (слабкі паролі, відсутність політик безпеки). І, нарешті, за наслідками для системи загрози можуть призвести до порушення конфіденційності (несанкціонований доступ до даних), порушення цілісності (зміна або знищення інформації) та порушення доступності (відмова в доступі до ресурсів) [11, 12,21,22,23].

Але можуть бути і складніші загрози, такими загрозами є комплексні загрози. Комплексними загрозами є не просто окремі атаки, а поєднання кількох, часто незалежних, факторів, які, взаємодіючи, створюють значно більший ризик, ніж кожен з них окремо. Такі загрози можуть призвести до системного збою, витоку даних, фінансових втрат, пошкодження репутації та навіть повного припинення діяльності компанії. Тобто, в порівнянні з окремими загрозами, комплексні є більш багатовимірні та є взаємозалежні між собою. Можна на багато елементів класифікувати комплексні загрози, але основними можна виділити це поєднання програмних і організаційних загроз, фізичних і програмних загроз, технічних і організаційних загроз. Прикладом взаємодії програмної та організаційної загрози є отримання доступу до ситеми зловмисником через недостатню обізнаність персоналу (погані паролі чи відкривання фішингово листа). Прикладом взаємодії фізичної та програмної загрози є випадок крадіжки фізичного обладнання, що перетворюється на несанкціонований доступ до конфіденційної інформації без необхідності складних кібератак. Прикладом взаємодії технічної та організаційної загрози є технічна несправність через відсутність належних організаційних процедур.

Дані загрози у різних випадках можуть по різному поєднуватись та по різному взаємодіяти між собою. Це не обов'язко пара загроз, це можуть бути декілька загроз, що в сукупності певним чином проявилися [13, 14, 15].

Незважаючи на спроби захисту корпоративних інформаційних систем від комплексних деструктивних інформаційних впливів, вони не мають тенденцій до зниження. До причин цього відноситься поява нових видів загроз, невисока адаптивність методів і систем захисту до умов функціонування корпоративних інформаційних систем, що змінюються. Необхідний пошук нових методів і моделей захисту корпоративних інформаційних систем від таких впливів.

Сучасні підходи до захисту корпоративних систем (рис. 3) виходять за межі простого антивірусу та фаєрвола. Вони зосереджені на побудові багаторівневої, адаптивної та проактивної оборони. Ключові концепції включають багаторівневий захист, модель Zero Trust та використання систем виявлення/запобігання вторгненням (IDS/IPS), використання системи управління інформацією та подіями

безпеки (SIEM), використання аналізу поведінки користувачів і об'єктів (UEBA) та використання центру управління безпекою (SOC) [17,18,19].

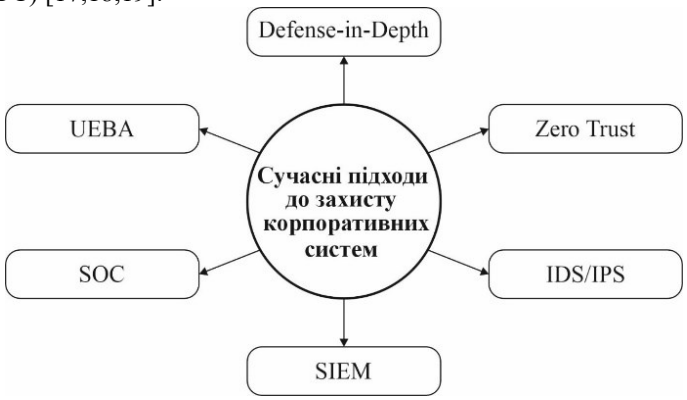

Рис. 3. Сучасні підходи до захисту корпоративних систем

Багаторівневим захистом (Defense-in-Depth) є стратегія, що передбачає використання декількох шарів захисту, щоб у разі злому одного шару інші залишалися ефективними. Кожен шар допомагає уповільнити атаку та надає системі час для виявлення та реагування. Цими шарами можуть бути фізичний захист (замки, охорона, відеоспостереження, обмеження доступу до серверних приміщень), мережевий захист (фаєрволи, сегментація мережі, VPN), захист хостів (антивірусне програмне забезпечення, персональні фаєрволи, системи виявлення загроз на кінцевих точках (EDR)), захист даних (шифрування даних під час зберігання та передачі) та організаційні заходи (політика безпеки, навчання персоналу, регулярні аудити) [9,11,15,16].

Сучасні підходи до кібербезпеки будуються на трьох принципах: запобігати, виявляти та реагувати на загрози. Це означає, що недостатньо просто встановити захист, потрібно постійно його перевіряти. Такий підхід вимагає, щоб захист був комплексним. Це включає не тільки технічні інструменти, а й освіту працівників та постійне управління ризиками. Лише постійно оновлюючи ці методи, можна ефективно боротися з найскладнішими сучасними кіберзагрозами [9,11,12,13,15].

Більшість організацій мають розрізнені засоби безпеки: окремо моніторинг, окремо копії даних, окремо інцидент-респонс. Немає узгодженого механізму, який би автоматично оцінював ризик, запускав потрібні дії та контролював відновлення. Слабке місце — відсутність інтегрованого циклу. Детекція не завжди автоматично переходить у реагування, а відновлення часто запускається вручну і не прив’язане до оцінки ризику. Запропонований метод якраз «зшиває» ці частини в одну керовану послідовність.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Формальні моделі загроз, сценаріїв атак, засобів захисту корпоративних ІС це є структуровані підходи, які допомагають компаніям систематично ідентифікувати, аналізувати та протидіяти комплексним кіберзагрозам. Вони дозволяють перетворити абстрактні ризики на конкретні, зрозумілі дії. Дані моделі є важливим елементом проактивного захисту, оскільки дають змогу не чекати атаки, а прогнозувати її можливий розвиток і заздалегідь підготувати засоби для оборони.

На етапі розвідки зловмисник пасивно збирає інформацію про ціль, не вступаючи в пряму взаємодію з її системами. На етапі озброєння зловмисник створює інструмент для атаки. На етапі доставки зловмисник передає створений інструмент до цілі. Після доставки зловмисник використовує вразливість у системі, щоб виконати шкідливий код (етап експлуатації). На етапі встановлення відбувається встановлення постійних присутності в системі для довгострокового доступу. На етапі командування та контролю хакер встановлює канал зв’язку зі своїм програмним забезпеченням. І фінальним етапом (дії за ціллю) є момент досягання зловмисником своєї кінцевої мети (викрадення даних, саботаж чи фінансова вигода) [25,26,27]. Cyber Kill Chain є ключовою моделлю для розуміння того, як відбуваються кібератаки та як від них захиститися. Попри деякі обмеження, вона добре адаптується до сучасних загроз. Завдяки інтеграції з новими інструментами, як MITRE ATT&CK, компанії можуть ефективно протистояти атакам, що постійно змінюються.

MITRE ATT&CK, є не зовсім традиційною моделлю сценарів атак, а більше базою знань, яка допомагає фахівцям з кібербезпеки створювати реалістичні сценарії атак. MITRE ATT&CK є більш деталізованою та гнучкою моделлю в порівнянні з Cyber Kill Chain. Також MITRE ATT&CK є фреймворком. MITRE ATT&CK надає детальний, нелінійний огляд конкретних технік, які зловмисник може використати в будь-який момент атаки. Тобто ця база масивно каталогізує тактику, методи та процедури кіберзлочинців на кожному етапі життєвого циклу кібератаки (від початкового збору інформації та планування дій зловмисника до остаточного виконання атаки). Дана система складається з двох основних елементів: тактики та техніки. Тактики представляють цілі зловмисника на високому рівні, наприклад, початковий доступ, виконання, закріплення та переміщення по мережі. Техніки описують конкретні методи (наприклад, технікою для тактики "Початковий доступ" може бути "Фішинг"), які зловмисник використовує для досягнення тактичної мети.

Фреймворк також включає субтехніки для більш детального опису та процедури, які є реальними прикладами того, як конкретні хакери реалізують ці техніки. MITRE ATT&CK організований у вигляді матриці. Матриця MITRE ATT&CK розділена на три основні частини, що відповідають різним сферам атак. Матриця підприємства охоплює методи атак на корпоративну інфраструктуру, включаючи операційні системи (Windows, MacOS, Linux), хмарні сервіси та контейнерні технології. Вона також містить матрицю підготовчих технік, що використовуються перед атакою. Мобільна матриця зосереджена на атаках, спрямованих на мобільні пристрої, а також на мережевих атаках, які їх використовують. Вона розділена на окремі підматриці для платформ iOS та Android. Матриця ICS (Industrial Control Systems) включає методи атак на промислові системи управління. Ці атаки спрямовані на обладнання та мережі, що використовуються для автоматизації заводів, комунальних послуг та інших критично важливих об'єктів. MITRE ATT&CK підтримує низку заходів та технологій (сортування сповіщень, виявлення загроз та реагування; полювання на загрози; аналіз прогалин у безпеці та оцінка зрілості Центру операцій безпеки (SOC); емуляція зловмисників), які організації використовують для оптимізації своїх операцій безпеки та покращення загального стану безпеки [23, 24].

Таким чином, є досить багато різних моделей загроз та сценаріїв атак й засобів захисту корпоративних ІС від комплексних кіберзагроз. Головне є те як їх буде застосовано, адже вони між собою зв’язані, і є багато прикладів як одна іншу вдало доповнює. Це є дуже важливим аспектом через те що загрози розвиваються, і відповідно потрібні досить гнучкі підходи для кібербезпеки.

Дуже важливою є оцінка ефективності захисту корпоративних ІС. Це дозволяє чітко оцінити захист систем, щоб зрозуміти чи є достатніми заходи щодо захисту інформаційних систем. І якщо захист є недостатнім, то потрібно буде його покращувати. Ефективність захисту корпоративних ІС від комплексних кіберзагроз вимірюється за допомогою комбінації кількісних і якісних показників, які показують здатність системи запобігати, виявляти, реагувати та відновлюватися після інцидентів. Ці показники допомагають оцінити поточний стан кібербезпеки, виявити слабкі місця та обґрунтувати інвестиції в захисті [24,26,27].

Якісні показники ґрунтуються на експертних оцінках і аудитах, вони допомагають оцінити готовність організації до комплексних загроз. Якісні показники не є чіткими, які можна виміряти, а є суб’єктивною оцінкою. Попри все, оцінка через якісні показники є дуже важливою частиною загальної оцінки. До якісних показників можна віднести результати пентестів (тестування на проникнення), рівень обізнаності співробітників та відповідність стандартам. Тестування на проникнення потрібне для ефективного оцінювання захисту і відбувається через імітацію реальної кібератаки. Даний показник є один з найважливіших тому, що при наявності добре обізнаних співробітників з кібербезпекою, компанія суттєво підвищує всю безпеку.

Показник відповідності стандартам є також важливим, оскільки вказує на ступінь дотримання різних стандартів з кібербезпеки (наприклад, ISO 27001, NIST). Цей показник не тільки допомагає підігнати рівень безпеки під стандарти визначенні спеціалістами, а й несе репутаційний вплив на компанію, показує на якому рівні знаходиться компанія в плані кібербезпеки [25,26,27].

Наступний тип показників є кількісні показники, ці показники є об'єктивними, і їх можна вимірювати та відстежувати. Такі показники кібербезпеки різняться від кількості заблокованих спроб порушення до швидкості реагування організації на інциденти. Першим показником є (еталон для оцінки надійності), середній час між збоями (MTBF). Взагальному, цей показник показує середній часовий інтервал, який відбувся між двома послідовними збоями системи чи її компонента. Другим показником є середній час до виявлення (MTTD). Показник вимірює середню тривалість часу, необхідну для виявлення потенційного інциденту. оцінює, наскільки ефективно і швидко системи можуть виявляти загрози. Чим коротший MTTD, тим швидше виявлення, що дозволяє оперативніше реагувати на ризики. Третім показником є середній час до підтвердження (MTTA). MTTA вимірює середню тривалість між початковим виявленням інциденту та його офіційним підтвердженням або реєстрацією. Показник є критично важливим, показує рівень готовності почати вирішення проблем безпеки. Четвертим показником є середній час до локалізації (MTTC). Показник відображає, наскільки швидко можна ізолювати та усунути загрозу, мінімізуючи її потенційну шкоду. MTTC оцінює ефективність процедур локалізації інцидентів. П’ятим показником є середній час до вирішення (MTTR). Даний показник вимірює, наскільки швидко організація може виявити, відреагувати та повністю відновитися після інциденту, оцінює ефективність та швидкість в усуненні загроз та відновленні після них. Наступним, шостим, показником є час на виправлення (Days to patch), що вказує на швидкість усунення вразливостей. Сьомим показником є ефективність запобігання втраті даних (DLP). Даний показник оцінює здатність системи запобігати несанкціонованому доступу або витоку даних. Показник вказує кількісну оцінку ефективності DLP-системи (Data Loss Prevention) через співвідношення успішно зупинених інцидентів до загальної кількості спроб. Восьмим показником є кількість спроб вторгнення. Даний показник показує кількість спроб зловмисників зламати мережі організації, надає представлення про рівень інтересу з боку кіберзлочинців та допомагає оцінити стійкість заходів кібербезпеки [15,16,17].

Взагальному, щоб комплексно оцінити ефективність захисту необхідно аналізувати ці показники разом, оскільки вони доповнюють один одного, надаючи повну картину стану кібербезпеки організації.

Модель функціонування корпоративної ІС можна відобразити при використанні марківських моделей. Марківські моделі є стохастичними моделями у теорії ймовірностей. Взагальному стохастичні моделі враховують випадковість з одною або більше випадкових величин. Стохастичні моделі допомагають передбачати чи пояснювати явища в моментах де результат не завжди однаковий, навіть при схожих умовах. Головною суттю марківських моделей це є використання марківських процесів (випадкові процеси без післядії), це означає, що в деякій системі S з дискретними станами $S_1, S_2, S_3 ...$ в будь-який моменту часу ймовірність будь-яких майбутніх станів системи залежить від її стану в теперішньому і не залежить від того як і скільки часу розвивався поточний випадковий процес (марківський процес) в минулому.

Для більшості практичних випадків процес функціонування корпоративної інформаційної системи в умовах комплексних деструктивних інформаційних впливів пропонується формалізувати у вигляді графа станів на рис. 4.

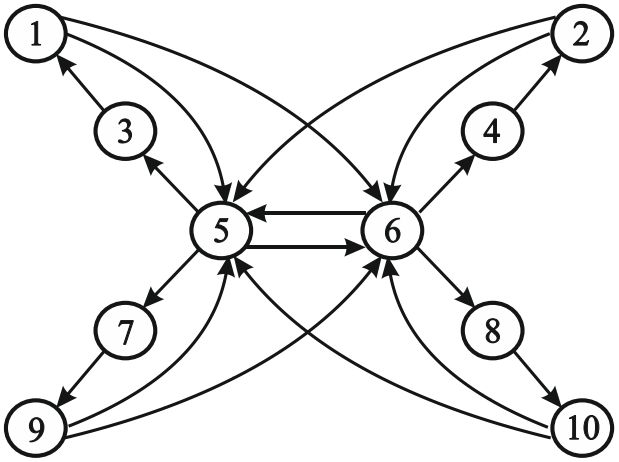

Рис. 4. Модель функціонування захищеної КІС

Вершини графа позначають стани процесу, дуги - переходи з одних станів в інші. Виділяються 10 станів ($S_1 ... S_{10}$) розглянутого процесу, які перераховуються в табл. 1. Відмінності цих станів полягають в умовах, у яких функціонує система в заданий момент часу. Наведена множина станів є повною групою подій. Переходи між станами, показані на рис.4, визначаються на основі характеру аналізованого процесу.

Переходи $S_5. \to S_6, S_6. \to S_5$ можуть відбуватися при посиленні чи ослабленні активності зловмисників, реконфігурації системи, зміні її контрагентів, а також модифікації інших умов функціонування системи. Зміна цих умов суттєво впливає на процеси актуалізації та деактуалізації загроз.

Беручи до уваги потоковий характер, властивий процесам функціонування КІС, а також орієнтуючись на граничну теорему для сумарних потоків, розглянутому вище графу відповідає система з 10 лінійних диференційних рівнянь. Кожне з рівнянь описує залежність ймовірностей знаходження системи у відповідному стані $S_1 ... S_{10}$ від часу та інтенсивностей переходів λ_{ij} з одних станів до інших.

Таблиця 1

Стан процесу функціонування системи

Номер стану	Умови функціонування
1	Реалізація захисних заходів для усунення виявленої загрози
2	Коректна оцінка ситуації за відсутності загрози
3	Отримання справжньої інормації про наявність загрози
4	Отримання справжньої інормації про відсутність загрози
5	Відсутність інформації про загрози за наявності загрози
6	Відсутність інформації про загрози за відсутності загрози
7	Пропуск загрози за її наявності
8	Хибне розпізнавання загрози за її відсутності (хибна тривога)
9	Сприйняття неправдивої інформації як істинної
10	Реалізація помилкових заходів захисту за відсутності загрози

Рішення конкретної системи рівнянь дозволяє розраховувати ймовірності, знаходження системи на момент часу, що цікавить, у можливих станах при захисті від конкретної загрози за допомогою конкретної програми захисту PRG_k . Якщо інтенсивності переходів та початкові умови відомі, система диференціальних рівнянь легко вирішується відомими методами чисельно чи аналітично. Розпізнавання актуального стану системи визначення початкових умов може виконуватися модулем аналізу ефектів системи захисту. Крім того, для кожного типу загроз і програм захисту, модель матиме свої початкові значення та параметри. За

наявності можливості розпізнавання актуального стану системи та відомих інтенсивностях λ_{ij} поява загроз може бути передбачена.

Алгоритм оцінювання ефективності захисту КІС за інтегральним показником із застосуванням розробленої марківської моделі включає наступні кроки:

1. Розрахунок ймовірностей $P_z^*(t), P_{zk}(PRG_k, t)$ знаходження КІС у виділених станах без застосування заходів захисту та з цими заходами на заданий момент часу.

2. Оцінювання $t_z^*(t)$ і $t_{zk}(PRG_k)$ сумарного часу знаходження КІС у станах $S_z \in \{S_1 ... S_{10}\}$ у разі відсутності та реалізації захисної програми PRG_k (1):

$$t_z^k = \int_0^T P_z(t)dt,\ t_{zk}(PRG_k) = \int_0^T P_{zk}(PRG_k, t)dt, \tag{1}$$

де $P_{zk}(PRG_k, t)$ означає ймовірність знаходження системи в стані z при реалізації цієї захисної програми PRG_k; T – аналізований період часу.

3. Кожному стану z ставиться у відповідність величина ефекту V_z, пов'язана з показниками якості обслуговування, що доставляється користувачеві в одиницю часу.

4. Розраховуються сукупні ефекти $L^*, L(PRG_k)$ КІС без заходів захисту та з ними (2):

$$L^* = \sum_{z=1}^{Z} V_z \cdot t_z^*,\ L(PRG_k) = \sum_{z=1}^{Z} V_z \cdot t_{zk}(PRG_k), \tag{2}$$

де Z - Число всіх станів КІС. Слід врахувати, що значення ефектів V_z можуть бути як додатніми, так і від'ємними (за наявності шкоди). Враховуючи, що показники якості обслуговування залежать від часу, розрахунок сукупного ефекту може виконуватися за формулами (3,4):

$$L^* = \sum_{z=1}^{Z} L_z^*,\ L(PRG_k) = \sum_{z=1}^{Z} L_z(PRG_k) \tag{3}$$

$$L_z^* = \int_0^T V_z(t) P_z^*(t)dt,\ L_z(PRG_k) = \int_0^T V_z(t) P_{zk}(PRG_k, t)dt \tag{4}$$

5. Розрахунок приросту $\Delta L = L_z(PRG_k) - L_z^*$ ефективності КІС за рахунок реалізованих заходів захисту.

Пропонований метод оцінювання ефективності захисту корпоративних інформаційних систем від комплексних деструктивних впливів може бути використаний для широкого кола різних за призначенням і структурним особливостями КІС.

На основі розробленого методу запропоновано структуру системи захисту корпоративної інформаційної системи від деструктивних впливів. Структура системи наведено на рис. 5. Відмінна риса даної системи полягає в новій множині функціональних блоків і зв'язків між ними. Вона дозволяє підвищити здатність прикладної системи виявляти та усувати деструктивні інформаційні впливи в автоматичному режимі.

Задача системи – забезпечення високої адаптивності від гетерогенних деструктивних інформаційних впливів на комп'ютерні мережі, зокрема – мережевих атак. Адаптація системи до актуальних умов функціонування виконується за допомогою її реконфігурування. Реконфігурування передбачає підналаштування блоків системи до поточної ситуації, а також вибір відповідних методів захисту.

У процесі конфігурування системи захисту визначається склад застосовуваних методів та систем захисту, а також їх параметри. Конфігурування повинно виконуватися з урахуванням як активних, так і можливих загроз, а також стану системи, що захищається. У загальному випадку необхідно вирішувати оптимізаційну задачу для знаходження відповідного способу захисту від розглянутих загроз.

Для оптимізації такої конфігурації потрібно знайти оптимальну програму PRG_{opt} для конфігурації системи захисту від вибраних загроз, при реалізації якої досягається максимум сукупного ефекту $L_{opt}(PRG_{opt})$ на інтервалі часу $[0;T]$ (5):

$$L_{opt}(PRG_{opt}) = \max_k \sum_{z=1}^{Z} \int_0^T V_z(t) P_{zk}(PRG_k, k)dt \tag{5}$$

при наступних обмеженнях: $t_k(PRG_k) \le t_D, PRG_k \in R, z = \overline{1, Z}, k = \overline{1, K}$,

де R - кінцева множина результативних програм конфігурації системи захисту (програма, яка досягає мети за кінцеве число кроків); K – кількість програм у множині R; Z – кількість станів у моделі системи, що захищається; $V_z(t)$ – ефект, що досягається системою в момент часу t за умови, що система перебуває у стані z; $P_{zk}\left(PRG_k, t\right)$ – ймовірність знаходження системи, що захищається, в стані z в момент часу t за умови, що програма PRG_k реалізована; T – інтервал часу, протягом якого оцінюються сукупні ефекти; $t_k(PRG_k)$ - час виконання програми PRG_k; t_D – максимально допустимий час виконання програми.

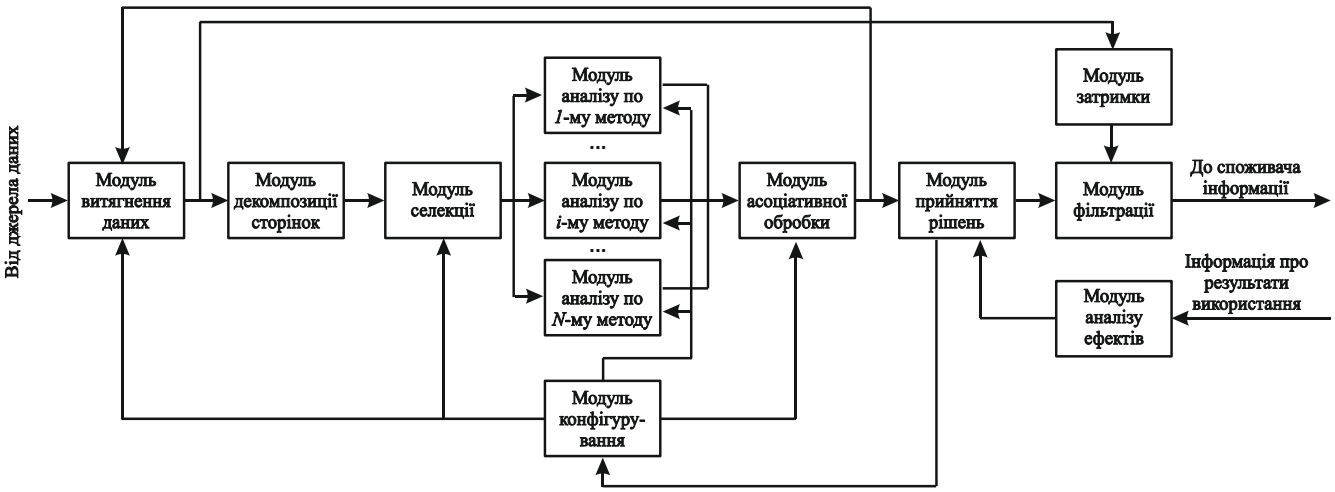

Рис. 5. Структура системи захисту корпоративної інформаційної системи від деструктивних впливів

Ця модель передбачає, що пошук оптимальної програми PRG_{opt} для конфігурації системи захисту може виконуватися лише на багатьох програмах, які відповідають наведеним обмеженням. Врахування цих обмежень істотно скорочує складність завдання.

Алгоритм вирішення сформульованої задачі пошуку оптимальної програми PRG_{opt} складається з наступних кроків:

1. Визначення початкових даних - T, Z, K, t_D, множин $V_z(t)$, $P_{zk}\left(t=0\right)$, PRG_k, $t_k(PRG_k)$, λ_{ijk} – інтенсивностей переходу в марківській моделі процесу, що захищається після реалізації конфігураційної програми PRG_k. Встановлення початкових значень: $k = 0$, $L_{opt} = 0$.

2. $k = k + 1$; $z = 0$; $L_k = 0$.

3. Якщо $k > K$, перейти до кроку 16.

4. Вибрати k- альтернативну програму з множини PRG_k.

5. Перевірити умову: $PRG_k \in R$. Якщо умова не виконується, перейти кроку 2.

6. Перевірити умову: $t_k(PRG_k) \le t_D$. Якщо умова не виконується, перейти до кроку 2.

7. Вибрати відповідні програмі PRG_k інтенсивності переходів λ_{ijk}.

8. $z = z + 1$.

9. Якщо $z > Z$, перейти до кроку 14.

10. Обчислити значення $P_{zk}\left(PRG_k, t\right)$

11. Обчислити $L_{kz} = \int_0^T V_z\left(t\right) P_{zk}\left(PRG_k, t\right) dt$

12. $L_k = L_k + L_{kz}$

13. Перейти до кроку 8.

14. Якщо $L_{opt} < L_k, L_{opt} = L_k, PRG_{opt} = PRG_k$.

15. Перейти до кроку2.

16. Вибрати програму PRG_{opt} на виконання.

Для великої кількості альтернативних програм повний пошук може бути замінений відомими методами оптимізації, наприклад, методом гілок та кордонів тощо.

Алгоритм адаптивного захисту КІС від інформаційних загроз наведений на рис. 6.

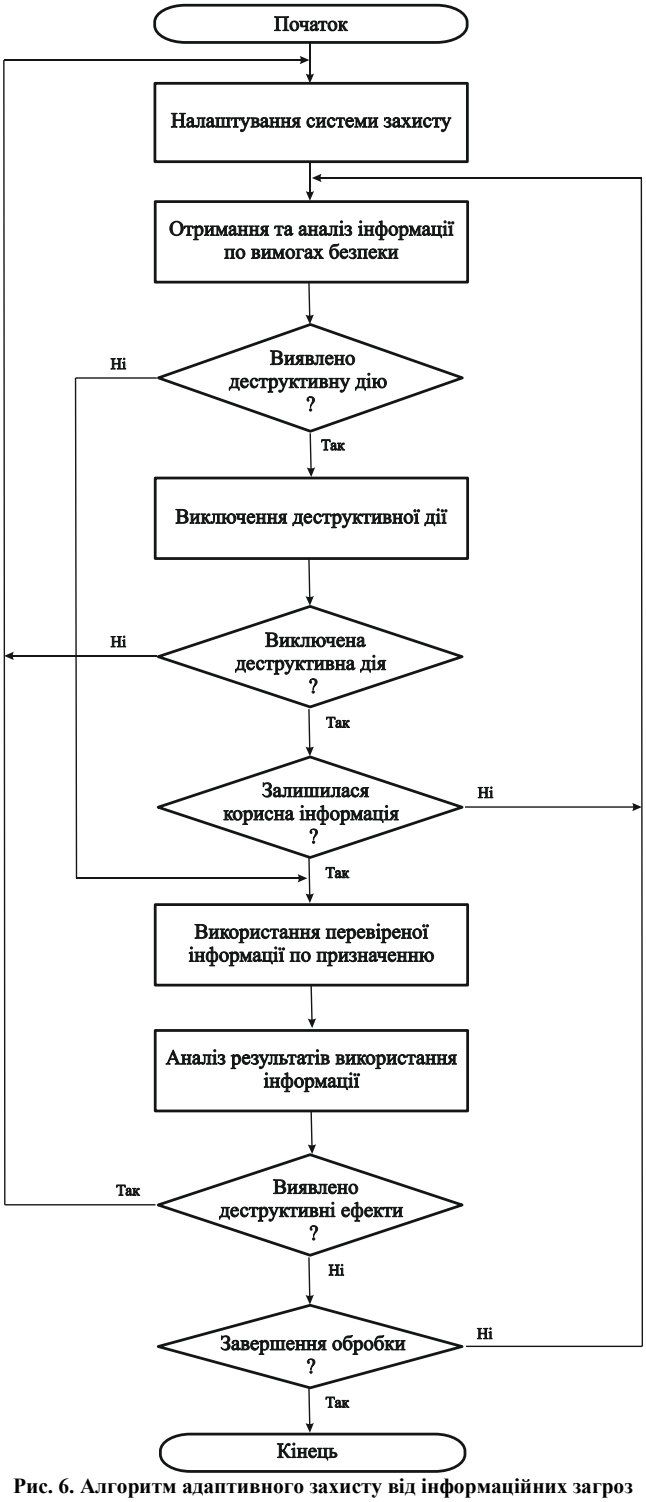

Рис. 6. Алгоритм адаптивного захисту від інформаційних загроз

Розглянутий метод оптимізації конфігурації системи захисту корпоративної інформаційної системи відрізняється від інших відомих рішень новим набором правил, що дозволяють реалізовувати адаптивний захист від інформаційних загроз. Реконфігурування системи захисту має виконуватися з метою досягнення максимального зростання сукупного ефекту або мінімальної шкоди в рамках заданого часового інтервалу з обмеженнями на час пошуку та реалізації керуючої програми.

Таким чином, запропонований метод адаптивного захисту корпоративної інформаційної системи від деструктивних впливів орієнтований на нову архітектуру системи захисту корпоративної інформаційної системи від деструктивних впливів. В його основі лежить розроблений алгоритм адаптивного захисту (рис. 6), а також метод оптимізації конфігурації системи такого захисту. Метод дозволяє розширити можливості систем захисту з виявлення та усунення деструктивних впливів.

Алгоритм оцінки ризику (RiskScore) включає наступні кроки:
1. Вхід: подія/інцидент, критичність сервісу, контекст користувача.
2. Нормалізувати подію (джерело, час, об’єкт впливу).
3. Призначити базовий бал загрози (за типом події).
4. Модифікувати бал з урахуванням критичності активу.
5. Врахувати наявність дублюючих контролів (зменшення ризику).
6. Рівень ризику {LOW, MED, HIGH} і бал [0;1].
7. Вибір плейбука (PlaybookSelect)
   7.1. Якщо ризик HIGH → обрати «жорсткий» плейбук (ізоляція, блокування, MFA reset).
   7.2. Якщо MED → «помірний» (посилення політик, збір форензіки, обмеження доступу).
   7.3. Якщо LOW → «спостереження/перевірка» (логування, сповіщення, відкладені дії).
8.Відновлення (ControlledRecover)
   8.1. Перевірка цілісності конфігурацій і даних.
   8.2. Відновлення з репліки/бекапу (тільки після ізоляції).
   8.3. Перевірка прикладних тестів (smoke/health-check).
   8.4. Повернення вузла в продуктивний сегмент.
   8.5. Підтвердження бізнес-власника сервісу.
9. Кінець

Архітектура системи адаптивного захисту корпоративної інформаційної системи від комплексних деструктивних інформаційних впливів, відрізняється новою сукупністю пов'язаних блоків збору, передобробки та аналізу даних та вибору контрзаходів для захисту від мережевих атак та інших деструктивних впливів, що дозволяє розширити функціональні можливості такого захисту.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Запропоновано метод забезпечення стійкості корпоративних інформаційних систем до комплексних кіберзагроз, який поєднує моніторинг, оцінювання ризику, адаптивне реагування та відновлення в єдиний керований цикл. Подано просту формулу інтегральної оцінки стійкості, референтну архітектуру, алгоритми і практичні кроки впровадження. Експериментальна перевірка показала скорочення MTTD і MTTR, а також зростання індексу стійкості. Метод придатний для організацій різного масштабу та може впроваджуватися поступово, починаючи з критичних сервісів.

Розроблені методи дозволяють кількісно оцінювати процеси, що протікають в КІС, що захищаються. Запропоновані моделі та методи можуть бути застосовані для високорівневої формалізації процесів функціонування корпоративних інформаційних систем на виробничих підприємствах, у соціальних установах, транспортних об'єктах, моллах, і т. д. Подібні моделі та методи можуть також успішно застосовуватися в завданнях планування та вибору контрзаходів для протидії загрозам у мережах цих організацій. Ця можливість може бути обґрунтована коректністю вихідних передумов, відповідністю результатів моделювання загальним закономірностям.

Подальші дослідження включають побудову приватних моделей, що відображають процеси, що протікають у сервісах КІС в умовах загроз. Також передбачається розвиток методів, що дозволяють визначати склад заходів захисту, у тому числі – формалізація захисних програм для конкретних умов функціонування КІС, аналіз та вибір найбільш ефективних методів оптимізації для пошуку захисних програм, що забезпечують кращі значення показників функціонування КІС.

Літертура

1. Корпоративна інформаційна система. URL: https://uk.wikipedia.org/wiki/ Корпоративна інформаційна система
2. A technology survival guide for resilience. URL: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/a-technology-survival-guide-for-resilience
3. Додонов О. Г., Кузнєцова М. Г., Горбачик О. С. Моделювання і оцінювання функціональної стійкості інформаційних систем. *Методи захисту інформації у комп’ютерних системах і мережах.* Київ, 2025. С. 77–82.
4. Аналіз побудови інтелектуальної інформаційної системи на основі поняття функціональної стійкості. / М. Ю. Миронюк та ін. Зв’язок. 2024. №1. С. 3–8.
5. Lakshmi Goel, Dawn Russell, Steven Williamson. Information systems security resilience as a dynamic capability. *Journal of Enterprise Information Management*. 2023. Vol. 36, № 4. P. 906–924. URL: https://doi.org/10.1108/JEIM-07-2022-0228
6. Кібератака. URL: https://uk.wikipedia.org/wiki/ Кібератака
7. Давиденко Є. А. Корпоративна безпека на українських підприємствах в умовах війни. *Економіка та суспільство*. 2023. № 58. С. 2–6.

8. Основи Кібербезпеки для бізнесу. URL: https://westelecom.ua/blog/osnovy-kiberbezopasnosti-dla-biznesa

9. Комплексний погляд на кібератаки. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-cyberattack

10. Різні типи кібератак та як не стати їх жертвою. URL: https://nordvpn.com/uk/blog/shcho-take-kiberataka/?srsltid=AfmBOoqlIfwpKtKr4GXDnwlrVkLpEH813XSEN41WC44rfi2_VqSRkZrz

11. Комплексна система захисту інформації – що це? URL: https://hostpark.ua/news-ua/kompleksna-systema-zahystu-informacziyi-shho-cze/

12. Захист корпоративних мереж від загроз: засоби та методи. URL: https://netwave.ua/blog/zahist-korporativnih-merezh-vid-zagroz-zasobi-ta-metodi/

13. В. Б. Дудикевич, Г. В. Микитин, Т. Є. Мурак. Комплексна система безпеки регіональної корпоративної мережі на основі еталонної моделі osi та моделі “Глибокого захисту”. *Computer systems and networks*. 2025. Vol. 7, № 1. P. 124–126.

14. Мехед Д. Аналіз вразливостей корпоративних інформаційних систем / Д. Мехед, Ю. Ткач, В. Базилевич, В. Гур’єв, Я. Усов // Захист інформації. 2018. Т. 20, № 1. С. 61-66. URL: http://nbuv.gov.ua/UJRN/Zi_2018_20_1_10

15. Defense in Depth: багаторівневий підхід до захисту інформації. URL: https://avolutech.com/blog/defense-in-depth-багаторівневий-підхід-до-захисту/

16. Zero Trust: Модель кібербезпеки, яка не вірить нікому – і саме тому рятує бізнес. URL: https://my-itspecialist.com/zero-trust-model-kyberbezpeky

17. Що таке IPS/IDS і де застосовується. URL: https://www.hostzealot.com.ua/blog/about-solutions/shho-take-ipsids-i-de-zastosovujetsya

18. Порівняння та вибір стандарту кібербезпеки URL: https://www.oksim.ua/porivnyannya-ta-vibir-standartu-kiberbezpeki/

19. Основні переваги сертифікації ISO/IEC 27001. URL: https://www.issp.training/post/osnovni-perevahy-sertyfikatsiyi-iso-iec-27001

20. What is the Plan-Do-Check-Act (PDCA) Cycle? URL: https://asq.org/quality-resources/pdca-cycle?srsltid=AfmBOorjsGZ3ClVTu2cM1OsZDFM708DI47GQxdLkVsEF2adyAQqEpajD

21. Що таке моделювання загроз і якими є його переваги? URL: https://www.issp.training/post/shcho-take-modelyuvannya-zahroz-i-yakymy-ye-yoho-perevahy

22. What Is the STRIDE Threat Model? Beginner’s Guide – 2025. URL: https://www.practical-devsecops.com/what-is-stride-threat-model/?srsltid=AfmBOooFRj5W_pOW2pZZMyk07BI-58z25VHsPzTOBjdwUMXr7e9ErIzH

23. DREAD Threat Modeling. URL: https://threat-modeling.com/dread-threat-modeling/

24. Guide to Threat Modeling using Attack Trees. URL: https://www.practical-devsecops.com/threat-modeling-using-attack-trees/?srsltid=AfmBOooQk_TLjGOcetG8OZsLF7rWu-gabZ8AA3sU5JTgSQxwTQpRbUrT

25. Cyber Kill Chain: Сучасні Загрози та Інструменти Протидії. URL: https://itorakul.com.ua/cyber-kill-chain/

26. Моделювання загроз за допомогою MITER ATT&CK Framework. URL: https://www.hostragons.com/uk/блог/моделювання-загроз-інфраструктури-mitre-attac/

27. Cybersecurity Metrics & KPIs: What to Track in 2025. URL: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cybersecurity-metrics/

References

1. Korporatyvna informatsiina systema. URL: https://uk.wikipedia.org/wiki/ Korporatyvna informatsiina systema

2. A technology survival guide for resilience. URL: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/a-technology-survival-guide-for-resilience

3. Dodonov O. H., Kuznietsova M. H., Horbachyk O. S. Modeliuvannia i otsiniuvannia funktsionalnoi stiikosti informatsiinykh system. Metody zakhystu informatsii u kompiuternykh systemakh i merezhakh. Kyiv, 2025. C. 77–82.

4. Analiz pobudovy intelektualnoi informatsiinoi systemy na osnovi poniattia funktsionalnoi stiikosti. / M. Yu. Myroniuk ta in. Zviazok. 2024. №1. S. 3–8.

5. Lakshmi Goel, Dawn Russell, Steven Williamson. Information systems security resilience as a dynamic capability. Journal of Enterprise Information Management. 2023. Vol. 36, № 4. P. 906–924. URL: https://doi.org/10.1108/JEIM-07-2022-0228

6. Kiberataka. URL: https://uk.wikipedia.org/wiki/ Kiberataka

7. Davydenko Ye. A. Korporatyvna bezpeka na ukrainskykh pidpryiemstvakh v umovakh viiny. Ekonmika ta suspilstvo. 2023. № 58. C. 2–6.

8. Osnovy Kiberbezpeky dlia biznesu. URL: https://westelecom.ua/blog/osnovy-kiberbezopasnosti-dla-biznesa

9. Kompleksnyi pohliad na kiberataky. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-cyberattack

10. Rizni typy kiberatak ta yak ne staty yikh zhertvoiu. URL: https://nordvpn.com/uk/blog/shcho-take-kiberataka/?srsltid=AfmBOoqlIfwpKtKr4GXDnwlrVkLpEH813XSEN41WC44rfi2_VqSRkZrz

11. Kompleksna systema zakhystu informatsii – shcho tse? URL: https://hostpark.ua/news-ua/kompleksna-systema-zahystu-informacziyi-shho-cze/

12. Zakhyst korporatyvnykh merezh vid zahroz: zasoby ta metody. URL: https://netwave.ua/blog/zahist-korporativnih-merezh-vid-zagroz-zasobi-ta-metodi/

13. V. B. Dudykevych, H. V. Mykytyn, T. Ye. Murak. Kompleksna systema bezpeky rehionalnoi korporatyvnoi merezhi na osnovi etalonnoi modeli osi ta modeli “Hlybokoho zakhystu”. Computer systems and networks. 2025. Vol. 7, № 1. P. 124–126.

14. Mekhed D. Analiz vrazlyvostei korporatyvnykh informatsiinykh system / D. Mekhed, Yu. Tkach, V. Bazylevych, V. Huriev, Ya. Usov // Zakhyst informatsii. 2018. T. 20, № 1. S. 61-66. URL: http://nbuv.gov.ua/UJRN/Zi_2018_20_1_10

15. Defense in Depth: bahatorivnevyi pidkhid do zakhystu informatsii. URL: https://avolutech.com/blog/defense-in-depth-bahatorivnevyi-pidkhid-do-zakhystu/

16. Zero Trust: Model kiberbezpeky, yaka ne viryt nikomu – i same tomu riatuie biznes. URL: https://my-itspecialist.com/zero-trust-model-kyberbezpeky

17. Shcho take IPS/IDS i de zastosovuietsia. URL: https://www.hostzealot.com.ua/blog/about-solutions/shho-take-ipsids-i-de-zastosovujetsya

18. Porivniannia ta vybir standartu kiberbezpeky URL: https://www.oksim.ua/porivnyannya-ta-vibir-standartu-kiberbezpeki/

19. Osnovni perevahy sertyfikatsii ISO/IEC 27001. URL: https://www.issp.training/post/osnovni-perevahy-sertyfikatsiyi-iso-iec-27001

20.What is the Plan-Do-Check-Act (PDCA) Cycle? URL: https://asq.org/quality-resources/pdca-cycle?srsltid=AfmBOorjsGZ3ClVTu2cM1OsZDFM708DI47GQxdLkVsEF2adyAQqEpajD

21. Shcho take modeliuvannia zahroz i yakymy ye yoho perevahy? URL: https://www.issp.training/post/shcho-take-modelyuvannya-zahroz-i-yakymy-ye-yoho-perevahy

22. What Is the STRIDE Threat Model? Beginners Guide – 2025. URL: https://www.practical-devsecops.com/what-is-stride-threat-model/?srsltid=AfmBOooFRj5W_pOW2pZZMyk07BI-58z25VHsPzTOBjdwUMXr7e9ErIzH

23. DREAD Threat Modeling. URL: https://threat-modeling.com/dread-threat-modeling/

24. Guide to Threat Modeling using Attack Trees. URL: https://www.practical-devsecops.com/threat-modeling-using-attack-trees/?srsltid=AfmBOooQk_TLjGOcetG8OZsLF7rWu-gabZ8AA3sU5JTgSQxwTQpRbUrT

25. Cyber Kill Chain: Suchasni Zahrozy ta Instrumenty Protydii. URL: https://itorakul.com.ua/cyber-kill-chain/

26. Modeliuvannia zahroz za dopomohoiu MITER ATT&CK Framework. URL: https://www.hostragons.com/uk/bloh/modeliuvannia-zahroz-infrastruktury-mitre-attac/

27. Cybersecurity Metrics & KPIs: What to Track in 2025. URL: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cybersecurity-metrics/