КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.31.1056
УДК 004.056.5:303.732.4:004.421.2

Савченко Тетяна Віталіївна
Кандидат технічних наук, доцент, доцент кафедри інформатики
Національний університет «Києво-Могилянська академія», Київ, Україна
ORCID: 0000-0002-8884-5360
tsavchenko@ukma.edu.ua

Власенко Лідія Олександрівна
Кандидат технічних наук, доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Державний торговельно-економічний університет, Київ, Україна
ORCID: 0000-0002-2003-6313
vlasenko.lidia1@gmail.com

Пілат Михайло Іванович
Студент спеціальності «Комп'ютерні науки»
Національний університет «Києво-Могилянська академія», Київ, Україна
m.pilat@ukma.edu.ua

СИСТЕМНИЙ АНАЛІЗ ДИНАМІКИ КІБЕРАТАК І ПРОЦЕСІВ ПЕНТЕСТИНГУ НА ОСНОВІ МОДЕЛІ РИЗИКУ ТА ГРАФОВИХ СТРУКТУР

Анотація. У статті представлено цілісний системний підхід до моделювання, аналізу та оцінювання динаміки кібератак, що поєднує подієву симуляцію, графові структури мережевої інфраструктури, багаторівневу модель ризику, методологію MITRE ATT&CK та часові показники ефективності реагування. Запропонована модель дозволяє формалізувати поведінку зловмисника, відтворити ключові етапи атакувальних сценаріїв та оцінити вплив кожної дії на загальний стан інформаційної системи. Використання графових структур забезпечує можливість виявлення критичних вузлів, аналізу латерального руху та визначення потенційного blast radius у разі успішної атаки. Багаторівнева модель ризику дає змогу поєднати локальні події, стан окремих вузлів та глобальні показники стійкості в єдиному аналітичному просторі. Особливу увагу приділено ролі пентестингу як ключового інструменту проактивного забезпечення кібербезпеки. Отримані результати демонструють, що інтеграція даних пентесту в динамічні моделі аналізу ризику значно підвищує інформативність і точність оцінювання стану захищеності, а також забезпечує можливість оперативного реагування на зміну загрозового ландшафту. Практична реалізація моделі виконана у середовищі Node-RED, яке використано як платформу для автоматизованої обробки подій, побудови графів, генерування візуалізацій та обчислення ключових метрик безпеки. Node-RED забезпечує інтеграцію даних пентестингу з аналітичними потоками, перетворюючи статичні результати тестування на адаптивну систему моніторингу та оцінювання ризиків. Отримані результати свідчать про перспективність поєднання системного аналізу, графових моделей та подієвої симуляції для розвитку інтелектуальних підходів до оцінювання кіберзахисту. Застосування Node-RED як гнучкого середовища для моделювання пентестингових даних формує новий напрям у дослідженні автоматизованих систем аналізу безпеки та потребує подальшої стандартизації та розширення. Запропонована модель може бути використана для побудови більш ефективних систем прогнозування поведінки зловмисника, оптимізації мережевої архітектури та формування адаптивних механізмів управління кіберризиками.

Ключові слова: системний аналіз; пентестинг; моделювання кібератак; багаторівнева модель ризику; графові структури; Node-RED; оцінювання кіберризиків; візуалізація безпеки; симуляція атак; мережеві загрози; динамічний моніторинг.

ВСТУП

Зростання числа кібератак на українські сервіси та критичну інфраструктуру обумовлює перегляд наявних рішень із забезпечення захисту інформації, а також аналіз досліджень, пов'язаних із кількісним оцінюванням захищеності інформаційних систем (ІС) засобами деструктивного інформаційного впливу. Тестування на проникнення (пентестинг) використовується як окремий етап аудиту кібербезпеки в багатьох міжнародних стандартах, проте чинна нормативна база України не встановлює процедуру тестування як обов'язкову, що залишає питання інтеграції технічної та організаційної складової малодослідженим.

Тестування на проникнення виступає одним із ключових методів перевірки реального рівня захищеності інформаційних ресурсів та своєчасного виявлення слабких місць. Актуальні сценарії загроз ІС, зокрема атаки на інфраструктуру й несанкціоноване розкриття даних, постійно ускладнюються, що змушує організації застосовувати проактивні підходи до кіберзахисту. У цьому контексті пентестинг набуває особливої ваги, адже дозволяє практично оцінити стійкість системи до несанкціонованих дій та визначити потенційні точки компрометації [1]. Головною метою процесу проникнення під час пентестингу є виправлення вразливостей до атаки в матеріальних та нематеріальних ресурсах [2].

Сучасні кіберзагрози характеризуються високою динамічністю, багатовекторністю та здатністю швидко адаптуватися до засобів захисту. У таких умовах пентестинг перетворюється з разового аудиту на складний системний процес, що включає аналіз технологічної інфраструктури, поведінкових патернів зловмисників, сценаріїв латерального руху та взаємодію компонентів мережі. Одним із ключових завдань сучасної кібербезпеки є формування багатовимірних моделей, здатних відтворювати реалістичну динаміку атак та забезпечувати комплексне оцінювання ризику й ефективності реагування.

У запропонованому дослідженні використано підхід до моделювання кібератак на основі симульованих подій пентестингу, що поєднує формальні графові структури, багаторівневу модель ризику, таксономію MITRE ATT&CK і часові метрики SOC. Такий підхід дає змогу здійснити системний аналіз процесів проникнення, руху атакувальника всередині мережі та вразливості окремих компонентів.

Постановка проблеми. Розглянуті нормативні рішення та сучасні дослідження моделей оцінювання ефективності захисту інформації свідчать про розвиток аналізу систем безпеки із врахуванням деструктивних впливів та свідомої організації процесів оцінювання. Однак малодослідженими залишаються способи інтеграції обох підходів в цілісний комплекс оцінювання безпеки інформаційної системи.

Зростання кількості кіберінцидентів, зафіксоване CERT-UA, підкреслює потребу в комплексних інструментах оцінки, що поєднує кількісний аналіз із застосування деструктивних впливів та планування таких заходів на рівні організації. Для вирішення цієї проблеми необхідно розробити модель взаємодії зацікавлених сторін, яку можна інтегрувати в існуючі процеси оцінювання захисту інформації компаній.

Пентестинг (penetration testing) є ключовим інструментом забезпечення інформаційної безпеки, оскільки дозволяє виявляти приховані або неочевидні вразливості та моделювати реальні сценарії атак. Сучасні дослідження підкреслюють важливість не лише виявлення вразливостей, а й операційної інтеграції результатів пентесту у системи моніторингу, реагування та управління ризиками. Саме тому питання

оцінки ефективності захисту на основі даних пентестингу набуває стратегічного значення.

Традиційні методи пентестингу переважно орієнтовані на виявлення вразливостей та оцінювання можливостей їх експлуатації. Проте такі підходи здебільшого охоплюють лише статичний аспект аналізу, залишаючи поза увагою часові характеристики виявлення й реагування, особливості латерального руху та розширення впливу в мережі. Вони не забезпечують достатньої підтримки для кількісного порівняння технік за MITRE ATT&CK, формування інтегрального індексу ризику системи чи побудови динамічної моделі поведінки атакувальника.

Попри значні результати у кожному з цих напрямів, бракує комплексного аналізу, що інтегрує всі перелічені методи в єдину системну модель аналізу кібератак і пентестингових процесів. Існує потреба у комплексній моделі, яка поєднає симуляцію кібератак, графову репрезентацію мережі, багатовимірний ризик, ATT&CK-класифікацію, SOC-метрики, та надасть можливість здійснювати системний аналіз стану кіберстійкості.

Аналіз останніх досліджень і публікацій.

У сфері пентестингу спостерігається зростання нових тенденцій та викликів, що впливають на ефективність зміцнення кібербезпеки. Сучасні підходи тестування на проникнення – від класичних мануальних технік [3] до автоматизованих рішень [4] та моделей, що використовують штучний інтелект, охоплюють широкий спектр методик і практик, які дозволяють комплексно оцінити захищеність інформаційних систем.

Окрему увагу приділяють проблемним аспектам, які супроводжують процес тестування на проникнення: еволюції загроз, необхідності дотримання етичних та юридичних норм, питанням достовірності отриманих результатів, а також ризикам, пов’язаним із доступом до конфіденційних даних під час перевірки [5]. Веб-додатки часто стають ціллю атак, оскільки помилки в їхній роботі можуть відкрити шлях до витоку даних або захоплення користувацьких облікових записів [6]. За останні роки спостерігається суттєве зростання кількості вразливостей у таких системах, переважно через недостатню перевірку та фільтрацію даних, що надходять від користувачів. Зростаюча кількість пристроїв з операційною системою Android та їх розвиток спричинили стрімке зростання мобільних застосунків, що, попри свою функціональність, містять численні вразливості, які досліджуються за методологією OWASP Mobile Top Ten з метою виявлення типових ризиків, оцінювання безпеки реальних застосунків із служби цифрової дистрибуції (Google Play) та формування рекомендацій щодо їхнього усунення [7]. Через стрімкий розвиток Інтернету речей (IoT) та промислового Інтернету речей (IIoT) пристрої IoT та пристрої IIoT нерідко стають мішенню для кіберзловмисників, які можуть намагатися отримати контроль над ними або збирати дані їхніх власників, тоді як перевірка безпеки шляхом оцінювання вразливостей і проведення пентестингу дає змогу визначити, наскільки дієвими є впроваджені механізми захисту [8].

У сучасному середовищі кібербезпеки важливо чітко і системно розуміти вразливості, оскільки навіть одна з них може спричинити серйозні наслідки для всієї системи. З огляду на зростання кількості загроз та масштаб інфраструктур виникає потреба у впорядкованих і уніфікованих знаннях про кіберризики. Для цього MITRE розробила матрицю Enterprise ATT&CK, яка дозволяє класифікувати дії зловмисників і відповідні заходи захисту, хоча повне поєднання цієї системи з іншими джерелами даних про вразливості досі залишається відкритим завданням для кіберспільноти [9]. MITRE ATT&CK є універсальною та широко застосовуваною базою знань про дії зловмисників,

однак попри її популярність бракує систематизованих досліджень щодо практичного використання, що зумовлює потребу в узагальненні наявної літератури та окресленні напрямів подальших досліджень для кожної предметної області [10]. Для протидії зростаючим кіберзагрозам організації створюють Центри операцій безпеки, і даний аналіз узагальнює ключові етапи їх побудови, вибір технологій та процеси роботи, підкреслюючи їхню важливу роль у підвищенні стійкості та ефективності кіберзахисту [11]. Наукові праці демонструють, що поєднання організаційних та індивідуальних чинників культури кібербезпеки можуть впливати на виникнення вразливостей і прояви певних моделей поведінки зловмисників, що можна відстежувати за допомогою матриці MITRE ATT&CK [12].

Дослідження кібербезпеки вимагають постійного моніторингу динамічного ландшафту загроз для виявлення нових атак. Для вирішення цієї задачі в різних сферах добре себе зарекомендували графові моделі (attack graphs, attack trees). Зокрема, в [13] графове моделювання та автоматичний аналіз дозволяють підсилити стійкість кіберфізичних систем до кібератак і підвищити ефективність оцінювання ризиків, робота [14] демонструє ефективність глибокого графового навчання для своєчасної ідентифікації атак у енергетичних мережах, що підвищує загальну кіберстійкість, а модель, представлена в [15], забезпечує глибший аналіз реальних атак завдяки графовим структурам, інструментам візуалізації та алгоритмам мережевої аналітики на основі даних, зібраних honeynet-системами.

У науковій літературі наголошується, що ефективність роботи SOC значною мірою визначається метриками реагування, зокрема, MTTD, MTTA та MTTR. Наприклад, порівняння Splunk Enterprise, Graylog Open і Syslog-ng показує суттєві відмінності у швидкості виявлення, підтвердження та стабільності обробки подій, що прямо впливає на реальну результативність SOC у реагуванні на інциденти [16]. В зв'язку з розвитком штучного інтелекту активно формується напрямок, що досліджує вплив AI та машинного навчання на сучасні операції SOC (MTTD, MTTA та MTTR), виділяючи переваги, реальні варіанти використання та стратегії впровадження [17, 18].

Багато науковців і практиків приділяють увагу застосуванню Heatmap для візуалізації порушень кібербезпеки та визначення кореляції, наприклад, між кількістю постраждалих осіб та місцем розташування викраденої інформації [19], для візуалізації кількості атак, класифікованих за типом атаки та періодом доби, коли вони сталися, допомагаючи в аналізі шаблонів атак [20], для пошуку прихованих кореляцій у великому наборі даних, які потім використовуються як вхідні дані для згорткової нейронної мережі (CNN) для виявлення та класифікації мережевих атак [21] тощо.

Для підвищення ефективності системи захисту можна використовувати підхід, який забезпечує спеціальне середовище для кіберзахисників для створення нових векторів та шляхів атак, розширюючи огляд ландшафту атак та покращуючи оцінку захисту з мінімальними ресурсами [22]. Платформи моделювання, розроблені для автоматизованого тестування на проникнення (AutoPT) зазвичай пропонують комплексний підхід до моделювання мережевих середовищ, зловмисників та захисників. [23].

Незважаючи на окремі успіхи, досі майже немає рішень, які б інтегрували всі ці методи в одну узгоджену систему для всебічного аналізу атак та проведення пентесту.

Мета статті. Метою роботи є формування системного підходу до аналізу динаміки кібератак і процесів пентестингу шляхом інтеграції багаторівневої моделі ризику, графових структур мережевої інфраструктури та симуляційно-аналітичних методів дослідження поведінки зловмисника. У роботі передбачається розроблення єдиної

аналітичної моделі, що поєднує характеристику атакувальних технік, часові параметри реагування, взаємодію мережевих компонентів і зміну ризикових показників у часі.

Для досягнення поставленої мети слід вирішити наступні задачі, пов'язані із проведенням аналізу структурних та динамічних особливостей атак, побудовою багаторівневої моделі ризику, формалізацією графового представлення мережі для опису латерального руху та визначення критичних вузлів, а також із створенням інтегральних показників оцінювання стану кіберзахисту на основі даних симульованого пентестингу. Додатково увагу зосереджено на узгодженні ризикових, часових і поведінкових параметрів у єдиній аналітичній структурі, яка дозволяє оцінити ефективність атак і захисних механізмів.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У сучасному інформаційному середовищі кіберзагрози стають дедалі витонченішими, тому активне виявлення вразливостей через пенетраційне тестування (пентестування) є критично важливим компонентом захисної стратегії. Пентестинг є проактивним методом оцінювання захищеності інформаційних систем, що передбачає імітацію дій потенційного зловмисника з метою виявлення слабких місць у програмно-апаратних комплексах та мережевій інфраструктурі. Такий підхід дає змогу своєчасно ідентифікувати та усувати вразливості до моменту їх можливого використання реальними нападниками, отже, підвищувати стійкість систем і забезпечувати безперервність їх функціонування. Регулярне проведення пентестингу є ключовим елементом сучасних практик кіберзахисту.

Пентестинг охоплює комплекс санкціонованих заходів, спрямованих на моделювання атак із застосуванням методів етичного хакінгу. Фахівці з тестування на проникнення виконують пошук вразливостей, перевіряють дієвість засобів захисту й формують рекомендації щодо їх підсилення. Результати таких робіт оформлюються у звіт, який містить опис виявлених недоліків, оцінку потенційних наслідків атак та пропозиції з удосконалення системи безпеки.

Формалізація процесу пентестингу за допомогою EPC-діаграми

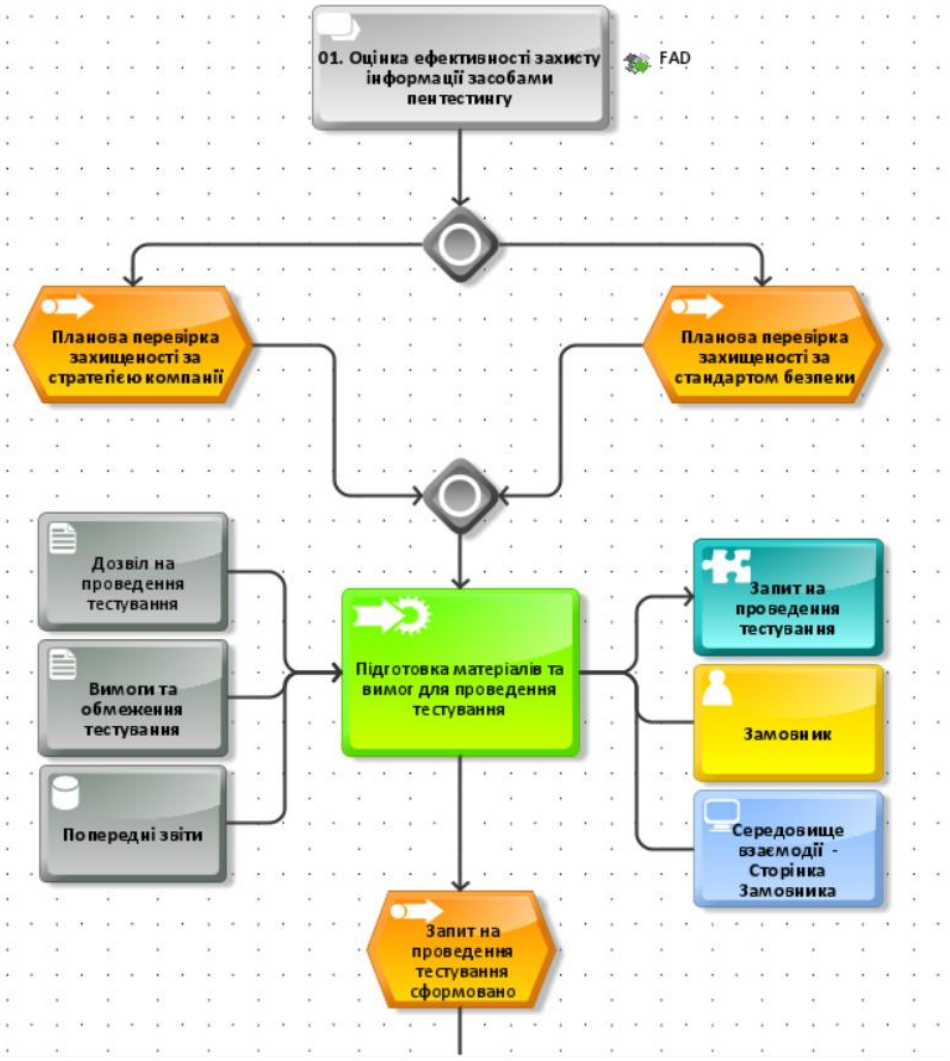
Незважаючи на різноманіття методів і стандартів, процес пентестингу зазвичай включає кілька базових етапів. Перший етап – збір інформації та планування, що передбачає отримання даних про структуру, архітектуру та особливості цільового об'єкта. Другий етап – реалізація атакувальних сценаріїв, що дозволяє перевірити ефективність побудованих векторів атаки та оцінити дієвість засобів захисту. В ході випробувань можуть бути виявлені додаткові вразливості, що підкреслює циклічний характер процесу та взаємозалежність між етапами збору інформації та експлуатації. Третій етап – формування підсумкового звіту, який містить детальний опис виконаних дій, реакції системи, застосованих методів експлуатації, а також рекомендацій щодо підвищення рівня безпеки. Документування перебігу тестування є важливою складовою, оскільки результати можуть бути використані замовником, аудиторами або іншими відповідальними сторонами для подальшої оцінки рівня захищеності.

Процес пентестингу може бути формалізований і представлений за допомогою EPC-діаграми, що дає змогу інтегрувати його в загальну модель управління кібербезпекою організації. Такий процес охоплює підготовку та узгодження вимог, подання запиту на проведення тестування, його оцінку тестувальником, погодження або

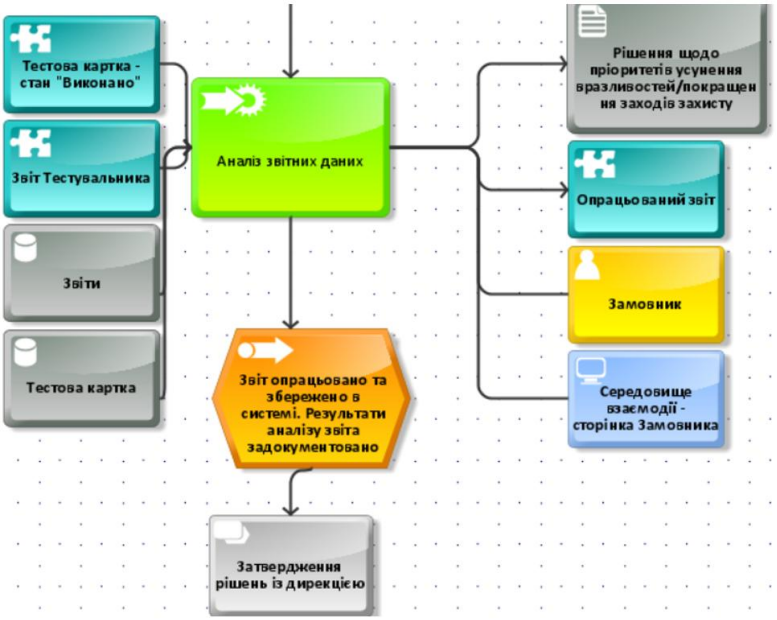
відхилення, виконання робіт із тестування, формування фінального звіту та документування прийнятих рішень на основі отриманих результатів.

На рис. 1 представлено фрагменти моделі процесу, розробленої в середовищі ARIS Express у вигляді EPC-діаграми, що забезпечує можливість подальшої інтеграції пентестингового середовища в існуючі системи оцінювання безпеки. Даний підхід створює основу для подальших досліджень із формалізації процесів тестування на проникнення та їх використання в автоматизованих моделях управління ризиками та кіберстійкістю.

Аналіз методів тестування на проникнення свідчить про їхню високу адаптивність для оцінки захищеності ІС. Розроблено низку спеціалізованих технік, які враховують особливості об’єктів тестування, таких як вебзастосунки, мобільні платформи, мережева інфраструктура тощо. Перевагою цих методів є їхня цільова орієнтація, що забезпечує ефективне виявлення вразливостей, специфічних для певного типу об’єктів. Водночас складна багатокомпонентна архітектура сучасних ІС вимагає комплексних підходів із врахуванням особливостей взаємодії множини об’єктів.



а)



б)

Рис. 1. Фрагменти EPC діаграми процесу взаємодії сторін із використанням програмного середовища для пентестингу

Інтеграція пентестингових даних у динамічну модель у середовищі Node-RED

Поряд із процесною формалізацією пентестингу у вигляді EPC-моделі постає потреба в інструменті, здатному не лише описувати етапи тестування, а й відтворювати їхню динаміку в обчислюваному середовищі. Це особливо актуально для складних інформаційних систем, де взаємодія між компонентами, часові залежності та кумулятивні ефекти атак формують багаторівневу поведінку ризиків.

Сучасні підходи до пентестингу дедалі частіше передбачають не лише формування статичного звіту, а й операційну інтеграцію результатів тестування у системи моніторингу та реагування. Одним із ефективних інструментів для такої інтеграції є середовище Node-RED – низькокодовий фреймворк для обробки подій, автоматизації та побудови візуальних потоків обробки даних. Його застосування дозволяє створити адаптивні механізми захисту, що працюють із результатами пентестів у напівавтоматичному або автоматичному режимі.

Node-RED інтегрується з більшістю інструментів пентестингу та безпеки, що дозволяє автоматично імпортувати знайдені вразливості, оформити потоки обробки даних, перетворювати результати пентесту у структуровані сценарії реагування. Node-RED може не лише обробляти дані пентесту, але й інтегрувати їх з оперативними логданими, що суттєво підсилює ефективність захисту. Система захисту стає контекстно-орієнтованою, тобто відстежує саме ті типи загроз, які були виявлені під час пентесту. Це підвищує ймовірність своєчасного виявлення реальної атаки у декілька разів, що підтверджується практикою використання адаптивних систем моніторингу в SOC.

Node-RED-Dashboard дозволяє створити інтерактивні панелі, внаслідок чого пентест перетворюється зі статичного документу у динамічну модель безпеки, яка живе й оновлюється. Таким чином, Node-RED виступає не просто інструментом візуалізації [24] – [25], а центральним механізмом інтерактивного захисту, що посилює результати пентестингу та робить кіберзахист організації значно більш ефективним, гнучким і стійким. Усе це формує інтелектуальну систему підтримки прийняття рішень, що працює в реальному часі.

Застосування системного підходу дозволяє розглядати пентестинг як складну динамічну систему, що функціонує під впливом низки взаємопов'язаних факторів: топології мережевої інфраструктури, логіки розвитку атакувальних сценаріїв, часових залежностей та механізмів реагування. На рис. 2 наведено структуру потоків даних у середовищі Node-RED, яка реалізує повний цикл обробки подій: від ініціювання атакувальних дій і накопичення історії до розрахунку ключових SOC-метрик, побудови теплових карт технік атак, формування мережевих графів та інтегральних ризикових показників. Модель побудована таким чином, що її поведінка визначається взаємодією структурних, процесних і динамічних характеристик, притаманних реальним кібернетичним системам.

У межах цього підходу мережева інфраструктура була формалізована як множина взаємопов'язаних вузлів, об'єднаних у графову структуру, що дозволило презентувати можливі шляхи латерального руху та оцінити ступінь критичності кожного компонента відповідно до його структурної ролі. Потоки даних у Node-RED синхронізовано з логікою функціональних процесів системи, що відтворюють послідовність обробки атакувальних подій, їх агрегацію та інтерпретацію у вигляді інтегральних ризикових характеристик. Така формалізація забезпечує відповідність моделі принципам процесного системного аналізу, в якому кожен елемент середовища відіграє певну функціональну роль у загальній поведінці системи.

Таким чином, застосування системного аналізу в межах розробленої моделі, що ґрунтується на поєднанні структурного, функціонального та динамічного підходів до вивчення кібернетичних процесів, дозволило створити узгоджену архітектуру, здатну не лише відтворювати сценарії багатостадійних атак, а й забезпечувати їх кількісну інтерпретацію через призму системних характеристик ризику та стійкості. Запропонована модель формує аналітичне підґрунтя для подальших досліджень, спрямованих на інтеграцію пентестингових методів у широкі системи управління кібербезпекою.

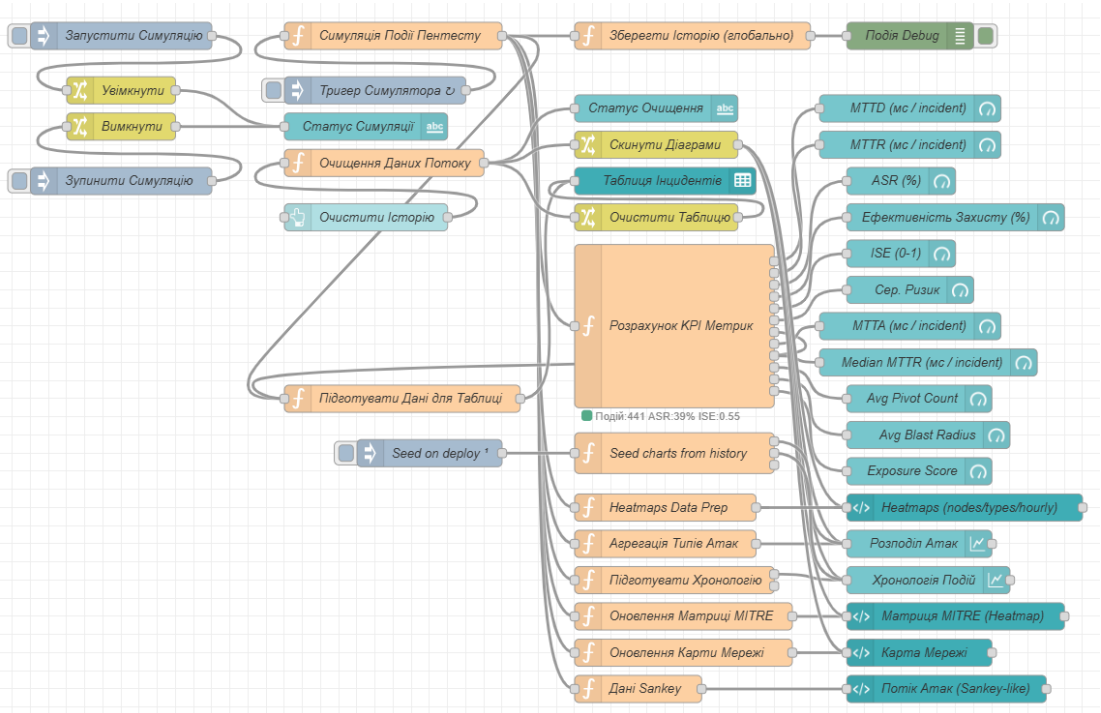


Рис. 2. Архітектура потоків даних моделі аналізу кібератак у середовищі Node-RED

Часова динаміка ризику та аналіз застосованих технік

Отримані результати демонструють комплексну динаміку розвитку атакувальних подій у мережевому середовищі та дозволяють простежити взаємозв'язок між структурними властивостями інфраструктури, характеристиками атак та інтегральними показниками ризику. На рис. 3 представлено зміну рівня ризику у часі, а також частотний розподіл технік, зафіксованих у ході моделювання. Часова крива відображає високу нерівномірність інтенсивності атак, що є характерним для багатостадійних сценаріїв із поєднанням дій розвідки, експлуатації та латерального руху. Ризиковий показник для кожної події визначався як функція її серйозності та вагових коефіцієнтів, пов'язаних із типом техніки:

$$R_i = f(S_i, \tau_i), \quad (1)$$

де S_i – рівень серйозності атаки, τ_i – тип техніки відповідно до MITRE ATT&CK.

Така формалізація дозволяє інтерпретувати часову динаміку ризику як відображення накопичення впливу локальних подій на глобальний стан системи.

Нижче подано розподіл типів атак, що узагальнюється через частотну функцію:

$$\tau k = ei : type ei = \tau k. \quad (2)$$

Отриманий розподіл засвідчує переважання технік, пов'язаних із розвідкою та початковими фазами проникнення, що формує базовий фон ризикового навантаження. Техніки експлуатації з меншими частотами, але вищою серйозністю, істотно впливають на загальну динаміку ризику, що відображається у вигляді окремих пікових значень.

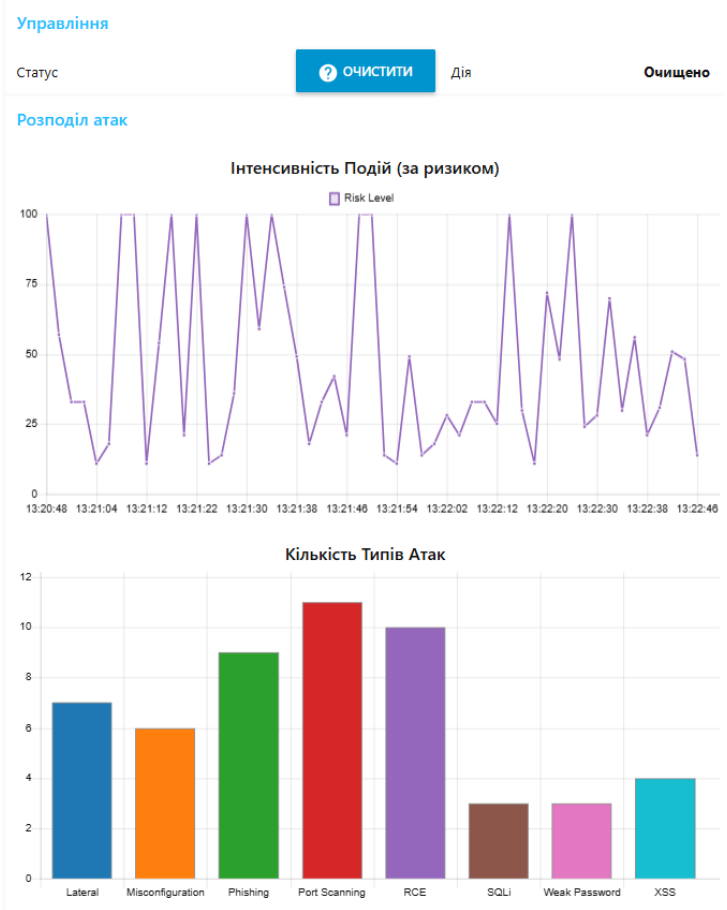


Рис. 3. Часова динаміка ризику та частотний розподіл технік атак

Матриця інцидентів та моделювання потоків атак.

На рис. 4 подано впорядковану матрицю інцидентів, сформовану за результатами моделювання атакувальних сценаріїв у мережевому середовищі. Така таблиця забезпечує реконструкцію послідовності подій, дозволяє відстежити часову динаміку розвитку інцидентів, параметри виявлення та реагування, а також дає змогу виконати кількісне оцінювання ключових показників ефективності (MTTD, MTTR, MTTA, рівень успішності атак, величину pivot-переходів тощо). Структурованість даних забезпечує можливість інтегрального аналізу стану системи, виявлення аномальних відхилень та ідентифікації критичних напрямів атакувального впливу.

Подальша інтерпретація отриманих результатів представлена нижче на рис. 4, де надано візуалізацію потоків атакувальної активності у форматі Sankey-подібного графа. Візуальна схема дозволяє визначити домінантні вектори проникнення, інтенсивність переходів між компонентами системи та структуру взаємозв'язків між атакувальними діями. Такий підхід дає змогу простежити поширення атаки у вигляді послідовності переходів між активами, що узгоджується з концепцією lateral movement та reconnaissance-to-impact ланцюжками, характерними для фреймворку MITRE ATT&CK.

Ймовірність переходу між вузлами моделі визначається як функція ваги відповідного напрямку, що враховує частоту техніки, її успішність та рівень доступності активу. Формально ймовірність переходу з вузла ϑ_i до ϑ_j описується виразом:

$$P(\vartheta_i \to \vartheta_j) = \frac{W_{ij}}{\sum_k W_{ik}}, \quad (3)$$

де W_{ij} – узагальнена вага потенційного переходу, обчислена на основі інтенсивності атак певного типу, їхніх тактичних характеристик та топологічних властивостей мережі відповідно до реалізованого у Node-RED алгоритму. Така формалізація забезпечує можливість оцінювання латерального переміщення, інтенсивності експлуатаційних дій і ступеня структурної вразливості системи з урахуванням усіх зафіксованих інцидентів.

Таким чином, матриця інцидентів і побудована візуалізація потоків атак функціонують як взаємодоповнюючі інструменти аналітики: перша надає детальний перелік подій із параметрами, друга – агреговане відображення траєкторій проникнення та впливів на мережеві вузли. Разом вони формують цілісну основу для подальшого розрахунку ризикових показників, виявлення критичних компонентів та побудови сценаріїв реагування.

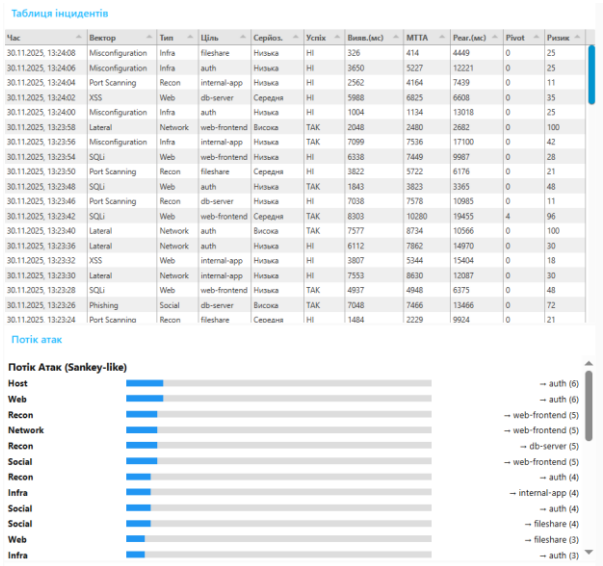


Рис. 4. Матриця інцидентів та візуалізація потоків атак

Обчислення SOC-метрик та інтегральних показників стійкості

На підставі часових атрибутів інцидентів, сформованих у ході симуляції та оброблених у середовищі Node-RED, було здійснено обчислення ключових SOC-метрик, що характеризують оперативність виявлення та реагування на атаки. Згідно з усталеною практикою кібероперацій них центрів, метрики Mean Time to Detect (MTTD), Mean Time to Respond (MTTR) та Mean Time to Acknowledge (MTTA) визначаються як середні значення різниць між відповідними часовими подіями. Формально вони описуються виразами:

$$MTTD = \frac{1}{N}\sum_{i=1}^{N}(t_{detect,i} - t_{start,i}), \quad (4)$$

$$MTTR = \frac{1}{N}\sum_{i=1}^{N}\left(t_{resolve,i} - t_{detect,i}\right), \quad (5)$$

$$MTTA = \frac{1}{N}\sum_{i=1}^{N}\left(t_{act,i} - t_{detect,i}\right). \quad (6)$$

Отримані значення MTTD, MTTR та MTTA демонструють різну тривалість фаз життєвого циклу інцидентів, що відображає часову структуру атакувальних сценаріїв, а також ефективність процесів моніторингу й реагування. Високі коливання цих метрик узгоджуються з різною складністю атак, наявністю латеральних переміщень, неоднорідністю векторів та відмінністю в часі реакції між окремими компонентами мережі.

Додатково були обчислені інтегральні індикатори стану системи – середній ризик, індекс ефективності захисту, медіанний MTTR, показник середньої кількості pivot-переходів, blast radius та інтегральна оцінка вразливості (Risk Score). Ці показники формують узагальнену характеристику кіберстійкості, відображаючи взаємозв'язок між частотою атак, їхньою складністю, топологічними властивостями мережі та сценаріями латерального руху. Зокрема, blast radius відтворює потенційний масштаб впливу успішної атаки, тоді як Risk Score оцінює ймовірність компрометації ключових активів з урахуванням накопиченого ризикового навантаження.

Представлені результати (рис. 5) свідчать про те, що запропонована модель дозволяє інтегрувати часові параметри SOC, топологічні характеристики мережі та параметри атакувальної активності в єдиному аналітичному просторі, забезпечуючи кількісно обґрунтовану оцінку динаміки кіберзагроз та поточного рівня захищеності інфраструктури.

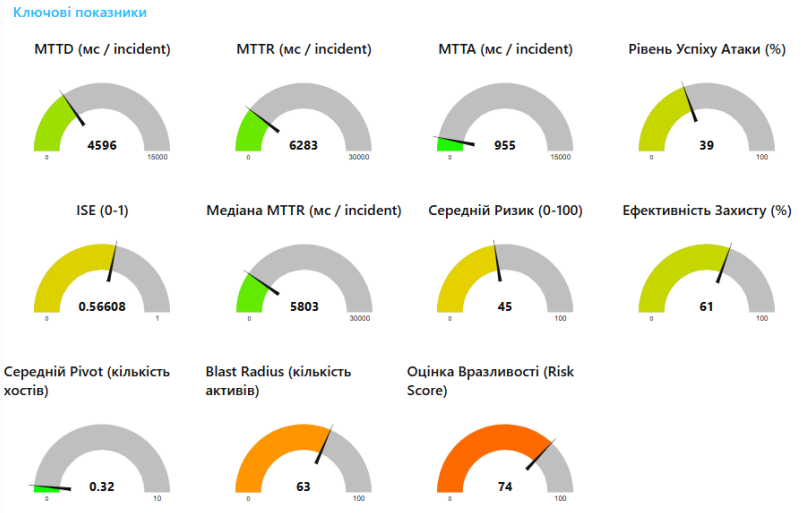


Рис. 5. Інтегральні показники моделі кібератак

Графова модель мережевих взаємодій та оцінювання структурних ризиків

Структурні властивості мережевої інфраструктури подано на рис. 6 у вигляді графової моделі, у якій вузли репрезентують мережеві активи, а ребра – канали їхньої комунікаційної взаємодії. Такий підхід відповідає усталеній практиці моделювання корпоративних мереж, де графові структури використовуються для аналізу зв'язності, виявлення критичних точок та оцінювання потенційних шляхів поширення компрометації. Топологічні характеристики, зокрема центральність вузлів та щільність з'єднань, визначають масштаби можливого впливу атакувальних дій і формують базу для обчислення показників на кшталт radius of compromise (blast radius).

Blast radius визначається як потужність множини вузлів, що можуть бути досягнуті після компрометації вузла ϑ_0:

$$BR = |reachable(\vartheta_0)|, \quad (7)$$

Цей показник відображає потенційний обсяг активів, які опиняються під загрозою за умови реалізації атаки та подальшого латерального руху. Візуалізація на рис. 6 демонструє мережу з кількома вузлами підвищеної зв'язності, що природно збільшує можливий радіус ураження в реалістичних сценаріях тестування на проникнення.

У межах дослідження використано динамічну графову модель, яка відтворює еволюцію станів мережевих активів у часі залежно від розвитку атакувальних подій. Базова структура моделі подається у вигляді неорієнтованого графа:

$$G = (V, E), \quad (8)$$

де множина вузлів *V* відповідає елементам інфраструктури, а множина ребер *E* описує їхні логічні мережеві з'єднання.

Оскільки вхідні дані симуляції не містять спрямованих каналів передачі (наприклад, політик маршрутизації або ACL), модель коректно трактує взаємодії як неорієнтовані ребра, що відповідає типовому зображенню рівня зв'язності на етапі пентестингу.

На відміну від статичної топології, динамічна модель передбачає зміну станів вузлів унаслідок подій симуляції. Для кожного вузла υ_i обчислюється часовий ризиковий індекс:

$$R_i(t) = \omega_C C_i + \omega_A A_i(t) + \omega_E E_i(t), \quad (9)$$

де C_i – критичність активу, $A_i(t)$ – акумульована дія атакувальних технік, $E_i(t)$ – ступінь експозиції, що визначається кількістю та властивостями його зв'язків.

Модель не використовує стохастичних переходів між вузлами; натомість вона спирається на детерміноване оновлення станів, що ґрунтується на зафіксованих у пентесті подіях та параметрах MITRE ATT&CK.

Динамічність моделі забезпечується тим, що кожна нова подія (експлуатація вразливості, доступ, рух між вузлами) оновлює атрибути відповідних вузлів та змінює інтегральний стан мережі. Це дозволяє отримувати часові профілі ризику, heatmap-візуалізації, статистику застосованих технік та оцінювати концентрацію впливу на окремі сегменти графа. Таким чином, модель фокусується не на зміні топології, а на динаміці кіберризику, що виникає внаслідок атакувальних дій. Обрана архітектура дозволяє інтегрувати результати пентестингу як подієві сигнали, що безпосередньо впливають на стан графа, забезпечуючи адаптивне оцінювання стану інформаційної системи. Це створює основу для подальшої автоматизації аналізу ризиків та моделювання латерального руху в умовах реалістичних пентестингових сценаріїв.

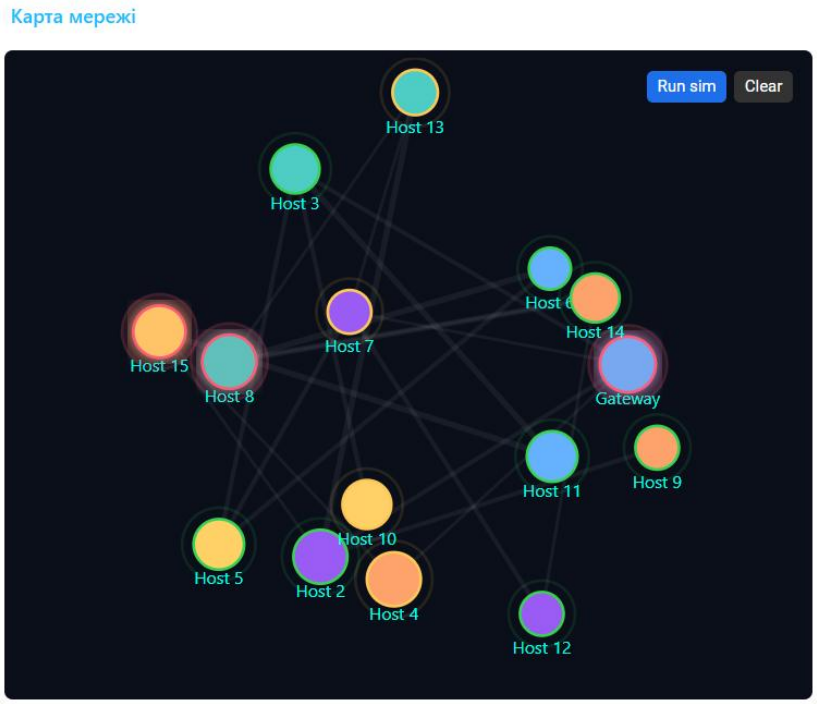


Рис. 6. Графова модель мережевих взаємодій

Теплові карти технік та ризикового навантаження

На рис. 7(а) подано теплову карту технік MITRE ATT&CK, що відображає кількість зафіксованих подій для кожної техніки. Така форма представлення дозволяє оцінити частотність активності різних тактик та технік, зіставити їх з фазами атаки (Reconnaissance, Initial Access, Execution, Lateral Movement тощо) та визначити, які техніки домінують у моделюванні. Найвищі значення частоти відповідають технікам, що становлять найбільший внесок у загальну динаміку загроз і потенційно формують основні вектори розвитку атаки.

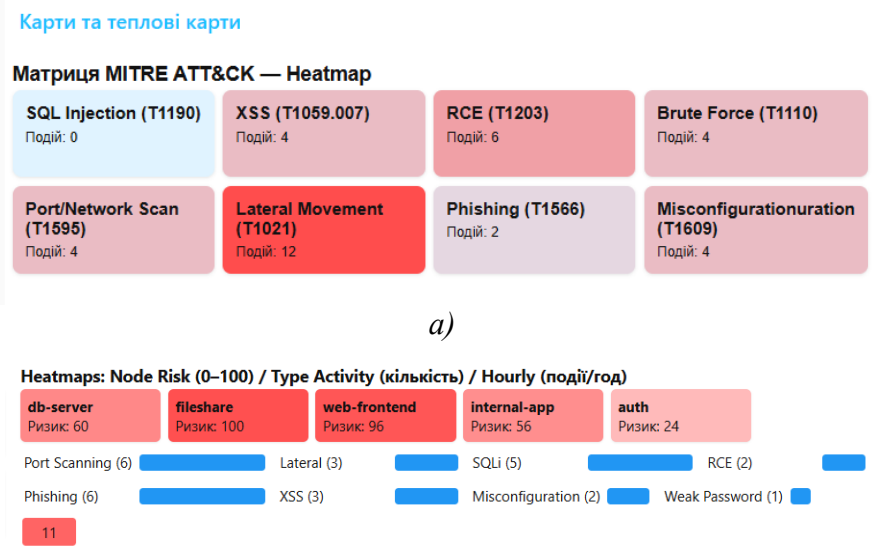
На рис. 7(б) наведено теплову карту ризикових характеристик мережевих вузлів у поєднанні з розподілом технік за їхньою активністю. Для кожного вузла локальний ризик визначався на основі агрегованої функції:

$$R(\vartheta_i) = f\left(N_{attacks}(\vartheta_j), S(\vartheta_j), C(\vartheta_j)\right), \quad (10)$$

де $N_{attacks}(\vartheta_j)$ – кількість атак на актив, $S(\vartheta_j)$ – серйозність цих атак, $C(\vartheta_j)$ – структурна значущість вузла в мережевому графі.

Таке поєднання метрик узгоджується з практиками ризик-орієнтованого моніторингу у SOC та дозволяє оцінити концентрацію впливу атак на різні сегменти інфраструктури. Теплова карта показує, які активи формують найбільше ризикове навантаження, а також які техніки домінують у їхньому профілі атак.

Узагальнення представлених результатів свідчить про внутрішню узгодженість отриманих показників та їхню придатність для комплексної оцінки динаміки кіберзагроз. Такий підхід дозволяє визначити критичні компоненти системи з погляду їхнього внеску у ризикове навантаження; ідентифікувати техніки, що є найбільш репрезентативними для поточного сценарію атак; формувати інтегральну картину ризику на основі структурних, поведінкових та частотних характеристик.



а)

б)

Рис. 7. Теплові карти технік кібератак (а)
і ризикових характеристик мережевих вузлів (б)

Таким чином, розроблена модель демонструє здатність інтегрувати процесні, структурні й динамічні компоненти пентестингу в єдине аналітичне середовище, що підтверджує доцільність системного підходу для дослідження сучасних кіберзагроз та формування адаптивних механізмів кіберзахисту. Використання платформи Node-RED дозволяє значно посилити ефективність застосування результатів пентестингу, переводячи їх зі статичної площини у динамічний аналітичний процес, який функціонує у близькому до реального часу режимі. Отже, Node-RED відіграє роль системи, що робить результати пентесту дієвими, придатними до оперативних змін і здатними реально впливати на рівень інформаційної безпеки організації.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У межах даного дослідження представлено комплексний підхід до системного аналізу динаміки кібератак і процесів пентестингу, що поєднує багаторівневу модель ризику, графові структури мережевої інфраструктури та симуляційні механізми моделювання поведінки зловмисника. Запропонована модель забезпечує інтегральне оцінювання стану інформаційної системи, враховуючи часові характеристики атак, інтенсивність взаємодій зловмисника із середовищем, а також вплив кожного етапу атаки на загальний рівень ризику.

Реалізація моделі в середовищі Node-RED підтверджує її прикладну придатність: побудовані heatmap-візуалізації, граф мережі, динамічні SOC-показники та агреговані індекси ризику дають можливість отримувати узгоджене бачення безпекового стану системи та відтворювати реалістичну динаміку атак. Використання таких структур, як blast radius, pivoting, MITRE ATT&CK-класифікація, а також середні значення MTTD, MTTA і MTTR, забезпечує можливість оцінювати ступінь захищеності як окремих вузлів, так і всієї інфраструктури в цілому.

Отже, сформована модель не лише об’єднує структурні, поведінкові та часові параметри пентестингу, але й створює підґрунтя для побудови комплексних систем

ситуаційної обізнаності в кібербезпеці. Це дозволяє підвищити достовірність оцінок, покращити процес прийняття рішень та створює умови для інтеграції пентестингових результатів у ширші системи моніторингу та аналізу ризиків.

Подальші дослідження доцільно зосередити на розвитку інтелектуальних методів автоматизації пентестингу та поглибленні аналітичних властивостей запропонованої моделі. Перспективним є використання машинного навчання для прогнозування можливих шляхів латерального руху, підвищення точності симуляцій та визначення найбільш критичних вузлів мережі. Удосконалення механізмів калібрування моделі на основі реальних кіберінцидентів дозволить підвищити її відповідність практичним умовам експлуатації.

До важливих напрямів розвитку належить інтеграція моделі з практиками неперервного тестування, зокрема впровадження елементів безперервного пентестингу у CI/CD-середовища та SOC-процеси. Таке поєднання забезпечить оперативне виявлення нових векторів атак і зменшить часові вікна, упродовж яких уразливості можуть залишатися непоміченими.

Додаткового вивчення потребують можливості оптимізації blast radius і побудови стратегій мінімізації впливу зловмисника за допомогою математичного моделювання та теорії графів. Перспективним також є дослідження поведінкових характеристик користувачів і атакувальників з метою підвищення точності оцінювання ризику. Окремої уваги заслуговує аналіз ефективності візуалізацій, зокрема heatmap-представлень, для підтримки аналітичних процесів у SOC, включно з експериментальним оцінюванням впливу таких інструментів на швидкість і точність прийняття рішень.

Загалом, подальший розвиток представленої моделі відкриває можливості для створення адаптивних, інтелектуально керованих систем оцінювання безпеки, здатних інтегрувати результати пентестингу в загальний цикл управління кіберризиками та забезпечувати високий рівень стійкості інформаційних систем.

ПОДЯКА

This work was supported by a grant from the Simons Foundation (SFI-PD-Ukraine-00014577; T.S.).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Mahamood, A. K., Malik, M., Ruhani, A. B., & Zolkipli, M. F. (2023). Cybersecurity strengthening through penetration testing: Emerging trends and challenges. *Borneo International Journal eISSN 2636-9826*, *6*(1), 44-52.
2. Sarker, K. U., Yunus, F., & Deraman, A. (2023). Penetration taxonomy: A systematic review on the penetration process, framework, standards, tools, and scoring methods. *Sustainability*, *15*(13), 10471. https://doi.org/10.3390/su151310471
3. Al-Sinani, H. S., & Mitchell, C. J. (2024). AI-augmented ethical hacking: A practical examination of manual exploitation and privilege escalation in Linux environments. arXiv preprint arXiv:2411.17539. https://doi.org/10.48550/arXiv.2411.17539
4. Hu, Z., Beuran, R., & Tan, Y. (2020, September). Automated penetration testing using deep reinforcement learning. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 2-10). IEEE. https://doi.org/10.1109/EuroSPW51379.2020.00010
5. Adam, H. M., & Putra, G. D. (2023, November). A review of penetration testing frameworks, tools, and application areas. In *2023 IEEE 7th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE)* (pp. 319-324). IEEE. https://doi.org/10.1109/ICITISEE58992.2023.10404397

6. Altulaihan, E. A., Alismail, A., & Frikha, M. (2023). A survey on web application penetration testing. *Electronics*, *12*(5), 1229. https://doi.org/10.3390/electronics12051229
7. Alanda, A., Satria, D., Mooduto, H. A., & Kurniawan, B. (2020, May). Mobile application security penetration testing based on OWASP. In *IOP Conference Series: Materials Science and Engineering* (Vol. 846, No. 1, p. 012036). IOP Publishing. https://doi.org/10.1088/1757-899X/846/1/012036
8. Bella, G., Biondi, P., Bognanni, S., & Esposito, S. (2023). Petiot: Penetration testing the internet of things. *Internet of Things*, *22*, 100707. https://doi.org/10.1016/j.iot.2023.100707
9. Branescu, I., Grigorescu, O., & Dascalu, M. (2024). Automated mapping of common vulnerabilities and exposures to mitre att&ck tactics. *Information*, *15*(4), 214. https://doi.org/10.3390/info15040214
10. Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing mitre att&ck risk using a cyber-security culture framework. *Sensors*, *21*(9), 3267. https://doi.org/10.3390/s21093267
11. Chamkar, S. A., Maleh, Y., & Gherabi, N. (2024). Security Operations Centers: Use Case Best Practices, Coverage, and Gap Analysis Based on MITRE Adversarial Tactics, Techniques, and Common Knowledge. *Journal of Cybersecurity and Privacy*, *4*(4), 777-793. https://doi.org/10.3390/jcp4040036
12. Jiang, Y., Meng, Q., Shang, F., Oo, N., Minh, L. T. H., Lim, H. W., & Sikdar, B. (2025). MITRE ATT&CK Applications in Cybersecurity and The Way Forward. *arXiv preprint arXiv:2502.10825*. https://doi.org/10.1109/ISI58743.2023.10297134
13. Adamos, K., Stergiopoulos, G., Karamousadakis, M., & Gritzalis, D. (2024). Enhancing attack resilience of cyber-physical systems through state dependency graph models. *International Journal of Information Security*, *23*(1), 187-198. https://doi.org/10.1007/s10207-023-00731-w
14. Presekal, A., Ştefanov, A., Rajkumar, V. S., & Palensky, P. (2023). Attack graph model for cyber-physical power systems using hybrid deep learning. *IEEE Transactions on Smart Grid*, *14*(5), 4007-4020. https://doi.org/10.1109/TSG.2023.3237011
15. Rabzelj, M., Bohak, C., Južnič, L. Š., Kos, A., & Sedlar, U. (2023). Cyberattack graph modeling for visual analytics. *IEEE Access*, *11*, 86910-86944. https://doi.org/10.1109/ACCESS.2023.3304640
16. Chamkar, S. A., Maleh, Y., & Gherabi, N. (2023). SOC Analyst Performance Metrics: Towards an optimal performance model. *Edpacs*, *68*(3), 16-29. https://doi.org/10.1080/07366981.2023.2259046
17. Mohammed, A. (2024). Transforming SOC Operations: Harnessing the Power of AI and ML for Enhanced Threat Detection. *INTERNATIONAL JOURNAL OF RESEARCH CULTURE SOCIETY Monthly Peer-Reviewed, Refereed, Indexed*, *8*. https://doi.org/10.2017/IJRCS/ICCDMP01
18. Stefanov, M., Stefanov, K., Kandel, L. N., Crouse, S., & Jekov, B. (2025). Autonomous agentic ai architectures for optimizing security operations centers (SOC) KPIs: methodology, impact on detection, response, and recovery. *Land Forces Academy Review*, *30*(3). https://doi.org/10.2478/raft-2025-0046
19. Murthy, A. S. R. C., Sravani, M., Ruthmani, G., & Chandra, V. U. (2024, July). An In-Depth Analysis of Contemporary Security Breaches using Time Series Analysis. In *International Conference on Computational Innovations and Emerging Trends (ICCIET-2024)* (pp. 701-709). Atlantis Press. https://doi.org/10.2991/978-94-6463-471-6_68
20. Naidu, P. R., Laya, N., Vinay, T. R., & Satish, E. G. (2025, May). Machine Learning Based Analysis and Visualization of Cyber Security Attacks on a Company. In *2025 6th International Conference for Emerging Technology (INCET)* (pp. 1-8). IEEE. https://doi.org/10.1109/INCET64471.2025.11140330
21. Rana, A., Rawat, P., Vats, S., & Sharma, V. (2024). Heatmap-Based Deep Learning Model for Network Attacks Classification. *SN Computer Science*, *5*(8), 1113. https://doi.org/10.1007/s42979-024-03447-3
22. Ajmal, A. B., Khan, S., Alam, M., Mehbodniya, A., Webber, J., & Waheed, A. (2023). Toward effective evaluation of cyber defense: threat based adversary emulation approach. *IEEE Access*, *11*, 70443-70458. https://doi.org/10.1109/ACCESS.2023.3272629
23. Wang, Y., Liu, S., Wang, W., Zhou, C., Zhang, C., Jin, J., & Zhu, C. (2025). A unified modeling framework for automated penetration testing. *arXiv preprint arXiv:2502.11588*. https://doi.org/10.48550/arXiv.2502.11588
24. Savchenko, T., Lutska, N., Vlasenko, L., Sashnova, M., Zahorulko, A., Minenko, S., Ibaiev, E., & Tytarenko, N. (2025). Risk analysis and cybersecurity enhancement of Digital Twins in dairy production. *Technology audit and production reserves*, *2(2(82))*, 37–49. https://doi.org/10.15587/2706-5448.2025.325422
25. Savchenko, T., Lutska, N., Vlasenko, L., & Tomenko, N. (2025). Analysis of the effectiveness of border traffic anomaly detection based on machine learning models. *Cybersecurity: Education, Science, Technique*, *1*(29), 464–479. https://doi.org/10.28925/2663-4023.2025.29.898

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023

Tetiana Savchenko
Candidate of Technical Sciences, Associate Professor,
Associate Professor of the Department of Informatics
National University of Kyiv-Mohyla Academy, Kyiv, Ukraine
ORCID: 0000-0002-8884-5360
tsavchenko@ukma.edu.ua

Lidiia Vlasenko
Candidate of Technical Sciences, Associate Professor,
Associate Professor of the Department of Software Engineering and Cybersecurity
State University of Trade and Economics, Kyiv, Ukraine
ORCID: 0000-0002-2003-6313
vlasenko.lidia1@gmail.com

Mykhailo Pilat
Student majoring in «Computer Science»
National University of Kyiv-Mohyla Academy, Kyiv, Ukraine
m.pilat@ukma.edu.ua

SYSTEMS ANALYSIS OF CYBERATTACK DYNAMICS AND PENETRATION TESTING PROCESSES USING A MULTILAYER RISK MODEL AND GRAPH-BASED STRUCTURES

Abstract. This article presents a comprehensive systems-based approach to modelling, analysing, and evaluating the dynamics of cyberattacks, integrating event-driven simulation, graph-based representations of network infrastructures, a multilayer risk assessment model, the MITRE ATT&CK methodology, and time-based incident response performance indicators. The proposed model enables the formalization of adversarial behaviour, reconstruction of key stages of attack scenarios, and assessment of the impact of each attacker action on the overall security posture of an information system. The use of graph structures facilitates the identification of critical nodes, analysis of lateral movement, and estimation of the potential blast radius in the event of a successful intrusion. The multilayer risk model consolidates local events, node-level states, and global resilience indicators within a unified analytical framework. Particular attention is given to penetration testing as a core instrument of proactive cybersecurity. The findings demonstrate that integrating pentesting results into dynamic risk assessment models significantly enhances the accuracy and informational value of security evaluations while enabling timely responses to evolving threat landscapes. The practical implementation of the model was carried out in the Node-RED environment, used as a platform for automated event processing, graph construction, visualization generation, and computation of key security metrics. Node-RED supports seamless integration of pentesting outputs into analytical workflows, transforming static test results into an adaptive monitoring and risk evaluation system. The results indicate the high potential of combining systems analysis, graph-based modelling, and event-driven simulation for the development of advanced, intelligence-driven approaches to cybersecurity assessment. The use of Node-RED as a flexible environment for modelling pentesting data establishes a promising direction for research into automated security analysis systems and highlights the need for further standardization and expansion. The proposed model can be applied to develop more effective adversary behaviour prediction systems, optimize network architectures, and create adaptive mechanisms for cyber risk management.

Keywords: systems analysis; penetration testing; cyberattack modelling; multilayer risk model; graph-based structures; Node-RED; cyber risk assessment; security visualization; attack simulation; network threats; dynamic monitoring.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Mahamood, A. K., Malik, M., Ruhani, A. B., & Zolkipli, M. F. (2023). Cybersecurity strengthening through penetration testing: Emerging trends and challenges. *Borneo International Journal eISSN 2636-9826*, *6*(1), 44-52.
2. Sarker, K. U., Yunus, F., & Deraman, A. (2023). Penetration taxonomy: A systematic review on the penetration process, framework, standards, tools, and scoring methods. *Sustainability*, *15*(13), 10471. https://doi.org/10.3390/su151310471
3. Al-Sinani, H. S., & Mitchell, C. J. (2024). AI-augmented ethical hacking: A practical examination of manual exploitation and privilege escalation in Linux environments. arXiv preprint arXiv:2411.17539. https://doi.org/10.48550/arXiv.2411.17539
4. Hu, Z., Beuran, R., & Tan, Y. (2020, September). Automated penetration testing using deep reinforcement learning. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 2-10). IEEE. https://doi.org/10.1109/EuroSPW51379.2020.00010
5. Adam, H. M., & Putra, G. D. (2023, November). A review of penetration testing frameworks, tools, and application areas. In *2023 IEEE 7th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE)* (pp. 319-324). IEEE. https://doi.org/10.1109/ICITISEE58992.2023.10404397
6. Altulaihan, E. A., Alismail, A., & Frikha, M. (2023). A survey on web application penetration testing. *Electronics*, *12*(5), 1229. https://doi.org/10.3390/electronics12051229
7. Alanda, A., Satria, D., Mooduto, H. A., & Kurniawan, B. (2020, May). Mobile application security penetration testing based on OWASP. In *IOP Conference Series: Materials Science and Engineering* (Vol. 846, No. 1, p. 012036). IOP Publishing. https://doi.org/10.1088/1757-899X/846/1/012036
8. Bella, G., Biondi, P., Bognanni, S., & Esposito, S. (2023). Petiot: Penetration testing the internet of things. *Internet of Things*, *22*, 100707. https://doi.org/10.1016/j.iot.2023.100707
9. Branescu, I., Grigorescu, O., & Dascalu, M. (2024). Automated mapping of common vulnerabilities and exposures to mitre att&ck tactics. *Information*, *15*(4), 214. https://doi.org/10.3390/info15040214
10. Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing mitre att&ck risk using a cyber-security culture framework. *Sensors*, *21*(9), 3267. https://doi.org/10.3390/s21093267
11. Chamkar, S. A., Maleh, Y., & Gherabi, N. (2024). Security Operations Centers: Use Case Best Practices, Coverage, and Gap Analysis Based on MITRE Adversarial Tactics, Techniques, and Common Knowledge. *Journal of Cybersecurity and Privacy*, *4*(4), 777-793. https://doi.org/10.3390/jcp4040036
12. Jiang, Y., Meng, Q., Shang, F., Oo, N., Minh, L. T. H., Lim, H. W., & Sikdar, B. (2025). MITRE ATT&CK Applications in Cybersecurity and The Way Forward. *arXiv preprint arXiv:2502.10825*. https://doi.org/10.1109/ISI58743.2023.10297134
13. Adamos, K., Stergiopoulos, G., Karamousadakis, M., & Gritzalis, D. (2024). Enhancing attack resilience of cyber-physical systems through state dependency graph models. *International Journal of Information Security*, *23*(1), 187-198. https://doi.org/10.1007/s10207-023-00731-w
14. Presekal, A., Ştefanov, A., Rajkumar, V. S., & Palensky, P. (2023). Attack graph model for cyber-physical power systems using hybrid deep learning. *IEEE Transactions on Smart Grid*, *14*(5), 4007-4020. https://doi.org/10.1109/TSG.2023.3237011
15. Rabzelj, M., Bohak, C., Južnič, L. Š., Kos, A., & Sedlar, U. (2023). Cyberattack graph modeling for visual analytics. *IEEE Access*, *11*, 86910-86944. https://doi.org/10.1109/ACCESS.2023.3304640
16. Chamkar, S. A., Maleh, Y., & Gherabi, N. (2023). SOC Analyst Performance Metrics: Towards an optimal performance model. *Edpacs*, *68*(3), 16-29. https://doi.org/10.1080/07366981.2023.2259046
17. Mohammed, A. (2024). Transforming SOC Operations: Harnessing the Power of AI and ML for Enhanced Threat Detection. *INTERNATIONAL JOURNAL OF RESEARCH CULTURE SOCIETY Monthly Peer-Reviewed, Refereed, Indexed*, *8*. https://doi.org/10.2017/IJRCS/ICCDMP01
18. Stefanov, M., Stefanov, K., Kandel, L. N., Crouse, S., & Jekov, B. (2025). Autonomous agentic ai architectures for optimizing security operations centers (SOC) KPIs: methodology, impact on detection, response, and recovery. *Land Forces Academy Review*, *30*(3). https://doi.org/10.2478/raft-2025-0046
19. Murthy, A. S. R. C., Sravani, M., Ruthmani, G., & Chandra, V. U. (2024, July). An In-Depth Analysis of Contemporary Security Breaches using Time Series Analysis. In *International Conference on Computational Innovations and Emerging Trends (ICCIET-2024)* (pp. 701-709). Atlantis Press. https://doi.org/10.2991/978-94-6463-471-6_68

20. Naidu, P. R., Laya, N., Vinay, T. R., & Satish, E. G. (2025, May). Machine Learning Based Analysis and Visualization of Cyber Security Attacks on a Company. In *2025 6th International Conference for Emerging Technology (INCET)* (pp. 1-8). IEEE. https://doi.org/10.1109/INCET64471.2025.11140330
21. Rana, A., Rawat, P., Vats, S., & Sharma, V. (2024). Heatmap-Based Deep Learning Model for Network Attacks Classification. *SN Computer Science*, *5*(8), 1113. https://doi.org/10.1007/s42979-024-03447-3
22. Ajmal, A. B., Khan, S., Alam, M., Mehbodniya, A., Webber, J., & Waheed, A. (2023). Toward effective evaluation of cyber defense: threat based adversary emulation approach. *IEEE Access*, *11*, 70443-70458. https://doi.org/10.1109/ACCESS.2023.3272629
23. Wang, Y., Liu, S., Wang, W., Zhou, C., Zhang, C., Jin, J., & Zhu, C. (2025). A unified modeling framework for automated penetration testing. *arXiv preprint arXiv:2502.11588*. https://doi.org/10.48550/arXiv.2502.11588
24. Savchenko, T., Lutska, N., Vlasenko, L., Sashnova, M., Zahorulko, A., Minenko, S., Ibaiev, E., & Tytarenko, N. (2025). Risk analysis and cybersecurity enhancement of Digital Twins in dairy production. *Technology audit and production reserves*, *2(2(82))*, 37–49. https://doi.org/10.15587/2706-5448.2025.325422
25. Savchenko, T., Lutska, N., Vlasenko, L., & Tomenko, N. (2025). Analysis of the effectiveness of border traffic anomaly detection based on machine learning models. *Cybersecurity: Education, Science, Technique*, *1*(29), 464–479. https://doi.org/10.28925/2663-4023.2025.29.898