КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.1203
УДК 004.056.55: 003.26

Шевченко Світлана Миколаївна
кандидат педагогічних наук, доцент,
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

Жданова Юлія Дмитрівна
кандидат фізико-математичних наук, доцент,
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0002-9277-4972
y.zhdanova@kubg.edu.ua

Стороженко Валерія Андріївна
студентка Факультету інформаційних технологій та математики
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0009-0004-7726-9670
vastorozhenko.fitm23@kubg.edu.ua

Рашевська Валерія Олександрівна
студентка Факультету інформаційних технологій та математики
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0009-0008-1921-5104
vorashevska.fitm23@kubg.edu.ua

Горбач Володимир Володимирович
студент Факультету інформаційних технологій та математики
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0009-0005-7431-9879
vvhorbach.fitm23@kubg.edu.ua

ІНТЕГРОВАНЕ ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОСНОВІ БАЄСІВСЬКИХ МЕРЕЖ ТА АУДИТУ ЗРІЛОСТІ

Анотація. Фундаментальним елементом будь-якої архітектури безпеки є оцінка ризиків, що дозволяє систематизувати потенційні загрози та прогнозувати їхній вплив на конфіденційність, цілісність і доступність інформаційних активів. У даному дослідженні висвітлено питання ймовірнісного моделювання ризиків із застосуванням спеціалізованого інструментарію, зокрема баєсівських мереж (BN) та програмного рішення Microsoft Security Assessment Tool (MSAT). Такий підхід дозволяє не лише візуалізувати топологію загроз, а й математично обґрунтувати причинно-наслідкові зв'язки між уразливостями та можливими втратами. Проведений аналіз наукових джерел дозволив систематизувати існуючі методики, від класичних анкетних опитувань до складних математичних моделей для оцінки ризиків інформаційної безпеки, зокрема SWOT-аналіз, експертний метод, нормативний метод, теорія ігор, нечіткі когнітивні карти, а також використання нейромережевих моделей. Практична значущість дослідження полягає у розробці та апробації комплексної методики оцінки безпеки умовної організації. Дана методика базується на кількісному моделюванні за допомогою програмного комплексу GeNIe Modeler та якісним аудитом зрілості системи захисту Microsoft Security Assessment Tool. Порівняльний аналіз показав, що MSAT виступає надійним інструментом для виявлення прогалин у комплаєнсі та організаційному захисті, тоді як баєсівські мережі забезпечують глибший кількісний аналіз критичності ризиків, дозволяючи моделювати ефективність впровадження конкретних контрзаходів. Результати дослідження мають як теоретичне, так і прикладне значення. Розроблені моделі

та методичні рекомендації були впроваджені в освітній процес при підготовці фахівців зі спеціальності F5 «Кібербезпека та захист інформації» в Київському столичному університеті імені Бориса Грінченка. Це підтверджує доцільність використання комбінованих інтелектуальних систем для прийняття обґрунтованих рішень у сфері управління ризиками цифрової інфраструктури.

Ключові слова: інформаційна безпека; кібербезпека; ризики інформаційної безпеки; кіберризики; захист інформації; Microsoft Security Assessment Tool (MSAT); програмний комплекс GeNIe Modeler; баєсівські мережі (BN).

ВСТУП

Постановка проблеми. Динаміка розвитку сфери кібербезпеки характеризується безперервною технологічною еволюцією та стрімким зростанням її економічної значущості. У центрі цієї трансформації перебуває штучний інтелект (ШІ), який став «зброєю подвійного призначення». З одного боку, ШІ надає фахівцям із безпеки потужні інструменти для автоматизованого виявлення аномалій, предиктивного аналізу уразливостей та миттєвого реагування на інциденти. З іншого – зловмисники дедалі частіше використовують алгоритми машинного навчання для створення витонченого фішингу, генерації поліморфного шкідливого коду та автоматизації пошуку «слабких ланок» у периметрі захисту корпоративних мереж. У таких умовах для компаній стає критично важливим не лише зміцнення «цифрових стін», а й чітке розуміння алгоритму дій у разі неминучого прориву захисту. Питання полягає не в тому, чи відбудеться інцидент, а в тому, коли він станеться і наскільки організація готова мінімізувати його наслідки. Саме тут фундаментального значення набуває ризико-орієнтований підхід. Замість розпилення ресурсів на захист від усіх можливих загроз одночасно, цей підхід дозволяє ідентифікувати найбільш критичні активи, кількісно та якісно оцінити ймовірні ризики та вибудувати стратегію стійкості. Це дає змогу не лише ефективно протидіяти атакам, а й забезпечити безперервність бізнес-процесів навіть у разі успішної кібератаки.

Аналіз останніх досліджень і публікацій. Проведений теоретичний аналіз наукових і практико-орієнтованих досліджень засвідчив, що серед проблем впровадження ризик-орієнтованого підходу особливої актуальності набуває оцінка ризику інформаційної безпеки. Цим підтверджується важливість даної роботи і значною кількістю наукових розробок у цій сфері.

- Серед методів для якісної та кількісної оцінки ризику пропонують застосовувати:
  - SWOT-аналіз та експертний метод [1-3];
  - нормативний та експертний метод [4];
  - нечіткі когнітивні карти та експертний метод [5-10];
  - баєсівські мережі та їх доповнення та удосконалення [11-15];
  - теорію ігор, нейромережеві моделі, машинне навчання [16-18].
- У практичній діяльності організації застосовують різні програмні засоби для аналізу ризиків інформаційної безпеки. Кожен із таких інструментів має власну специфіку, сильні сторони та певні недоліки. Частина з них орієнтована на анкетування спеціалістів і використання контрольних переліків, тоді як інші ґрунтуються на застосуванні більш складних математичних моделей, зокрема баєсівських мереж або статистичних підходів.
- У цій роботі розглядаються два програмні засоби оцінювання ризиків ІБ, що реалізують різні принципи аналізу: програмний комплекс GeNIe Modeler [19,20], який використовує ймовірнісне моделювання на основі баєсівських мереж, та Microsoft

Security Assessment Tool [21] – експертно-анкетний інструмент оцінювання рівня безпеки організацій, розроблений компанією Microsoft. Обидва інструменти широко застосовуються на практиці, проте орієнтовані на різні рівні формалізації та зрілості процесів управління ІБ.

- Метою роботи є проведення порівняльного аналізу програмних засобів оцінювання ризиків інформаційної безпеки на прикладі GeNIe Modeler та Microsoft Security Assessment Tool з використанням єдиного модельного сценарію функціонування інформаційно-телекомунікаційної системи.
- Для досягнення поставленої мети в роботі передбачається розв’язання таких завдань: розглянути теоретичні основи використання баєсівських мереж в оцінюванні ризиків ІБ; описати принципи функціонування Microsoft Security Assessment Tool; виконати практичне моделювання ризиків у програмному середовищі GeNIe Modeler; здійснити їх порівняльний аналіз.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Метод оцінювання ризиків на основі баєсівських мереж. Розробка реалістичних моделей у сфері кібербезпеки гальмується через брак емпіричних даних про минулі порушення. Однак стандартні (або класичні) баєсівські мережі (BN) мають потенціал для вирішення цієї проблеми завдяки комбінуванню різнорідних знань [15].

Баєсівська мережа – це аналітична модель, що дозволяє структурувати взаємозв’язки між випадковими подіями у вигляді орієнтованого ациклічного графа (DAG). У цій системі кожен вузол (вершина) уособлює конкретну змінну – наприклад, фактор ризику чи очікуваний результат. Зв’язки між ними (дуги) наочно демонструють, як саме ці явища впливають одне на одне, відображаючи прямі причинно-наслідкові або статистичні залежності [22]. Кількісна частина має форму умовних ймовірностей, які кількісно визначають залежності між пов'язаними вузлами в DAG, вказуючи умовний розподіл ймовірностей для кожного вузла [15].

Створення моделі ризиків на базі баєсівських мереж – це структурований процес, який можна представити як послідовність логічних етапів [15, 19, 20, 22, 23].

Етап 1. Визначення змінних і їхніх станів, на якому здійснюється початкове формування моделі шляхом виокремлення всіх релевантних факторів і загроз, подій, засобів контролю та можливих наслідків. Для кожної змінної встановлюються допустимі дискретні стани такі як: «низький», «середній», «високий» або «так», «ні». Змінні також можуть бути неперервними, а потім виконується їх подальша дискретизація.

Етап 2. Побудова графової структури. На основі експертних знань або даних встановлюються причинно-наслідкові зв’язки між змінними. Дуги (стрілки) додаються вручну, спрямовуючись від причини до наслідку. Для типових сценаріїв можна використовувати шаблонні моделі. В результаті формується орієнтований ациклічний граф, який візуалізує залежності в системі.

Етап 3. Оцінка параметрів – це етап, що передбачає кількісне встановлення взаємозв’язків у моделі. Для кожної вершини мережі визначаються відповідні ймовірнісні характеристики:

1) для кореневих вершин задаються апріорні ймовірності кожного стану;
2) для дочірніх вершин формується таблиця умовних ймовірностей, яка задає ймовірність кожного можливого стану цієї вершини для всіх допустимих комбінацій станів її батьківських вершин.

Значення параметрів можуть визначатися на основі експертних думок або шляхом навчання моделі з використанням наявних даних, тому що баєсівські мережі є ефективним інструментом для поєднання різних типів інформації, зокрема експертних оцінок і кількісних статистичних даних.

Етап 4. Валідація, аналіз та підсумовування. Механізм ймовірнісного висновку дозволяє прогнозувати та обчислювати ймовірність наслідків при заданих причинах. Здійснюється діагностика та обчислення ймовірностей причин за умови спостереження певних наслідків, а також аналіз чутливості й впливу з метою визначення факторів, що мають найбільший внесок у формування цільової змінної ризику. Крім того, виконується аналіз цінності інформації, який дає змогу встановити, які додаткові дані найбільше зменшують рівень невизначеності, а також виявлення аномалій для контролю відповідності моделі новим спостереженням і даним.

Ефективне практичне впровадження моделей оцінювання ризиків на основі баєсівських мереж вимагає використання спеціалізованого програмного забезпечення, що дозволяє наочно конструювати складні мережеві структури, задавати ймовірнісні параметри, виконувати розрахунки та здійснювати аналітичні дослідження.

Одним із найбільш відомих і функціонально потужних рішень у цій сфері є GeNIe Modeler. GeNIe Modeler – це графічний редактор для створення, навчання та аналізу графових ймовірнісних моделей, зокрема баєсівських мереж. Розробка цього інструмента здійснюється компанією BayesFusion з 1998 року, і за цей час він здобув широке визнання як у науковому середовищі, так і в промислових застосуваннях. У контексті моделювання ризиків GeNIe надає набір критично важливих можливостей, ключовою з яких є принцип повної свободи моделювання – здатність описувати практично будь-які системи без обмежень, що накладаються самим програмним засобом. Платформа підтримує різні типи вузлів і мереж, зокрема дискретні, неперервні та гібридні моделі, а також динамічні баєсівські мережі, що має особливе значення для аналізу й моніторингу ризиків у часовому вимірі. Окрім цього, GeNIe включає вузли прийняття рішень і аналізу корисності, які є необхідними для обґрунтованого вибору стратегій управління ризиками. Інструмент характеризується тісною інтеграцією з даними, підтримує імпорт із зовнішніх джерел, повну сумісність із MS Excel та містить алгоритми автоматичного навчання як структури, так і параметрів мережі безпосередньо на основі даних. Розширений аналітичний функціонал охоплює вбудовані діагностичні засоби, зокрема розрахунок цінності інформації, що дозволяє оцінювати та ранжувати можливі дії або перевірки за їх здатністю зменшувати рівень невизначеності [20]. У таблиці 1 наведено ключові характеристики GeNIe Modeler.

Таблиця 1

Ключові характеристики GeNIe Modeler

Характеристика	Опис
Тип програмного забезпечення	Графічний редактор моделей (GUI) для SMILE Engine
Основне призначення	Інтерактивна побудова, навчання та аналіз баєсівських мереж та інших графових ймовірнісних моделей
Ключові функції для ризиків	Динамічні BN, мережі впливу, алгоритми навчання, аналіз чутливості, розрахунок цінності інформації
Інтеграція та сумісність	Повна інтеграція з Excel, підтримка всіх основних форматів файлів BN, можливість вбудовування в застосунки через SMILE
Ліцензія та доступність	Комерційний продукт з безкоштовною академічною ліцензією та trial-версією.

Microsoft Security Assessment Tool як інструмент оцінювання ризиків. Після аналізу спеціалізованих середовищ, зокрема GeNIe Modeler, призначених для побудови складних баєсівських мереж, логічним наступним кроком є звернення до інструментів, які пропонують уже готовий і структурований підхід до оцінювання ризиків. Одним із таких рішень є Microsoft Security Assessment Tool (MSAT) – безкоштовний програмний засіб, розроблений компанією Microsoft для підтримки організацій у виявленні уразливостей IT-середовища та формуванні пріоритетного переліку рекомендацій з підвищення рівня безпеки.

На відміну від високої гнучкості та глибини моделювання, притаманних GeNIe, MSAT використовує стандартизований анкетний підхід, що базується на міжнародних стандартах інформаційної безпеки і загальновизнаних галузевих практиках. Основним призначенням інструмента є оперативне формування узагальненого уявлення про профіль ризиків організації та поточний рівень її захищеності.

MSAT ґрунтується на комплексній методології оцінювання, яка охоплює три ключові складові:

- персонал, процеси та технології;
- профіль бізнес-ризиків (Business Risk Profile Assessment);
- оцінка захисту в глибину (Defense in Depth Assessment).

Після заповнення анкети MSAT формує детальний звіт із рекомендаціями щодо підвищення рівня безпеки та надає унікальну можливість зіставити власні показники з анонімними агрегованими даними організацій аналогічного розміру та галузі [21].

Переваги і недоліки MSAT наведені у таблиці 2.

Таблиця 2

Переваги і недоліки MSAT

Переваги	Недоліки
Комплексний підхід – інструмент забезпечує оцінювання не тільки технічної складової, а й людського фактора та організаційних процесів.	Обмежена актуальність – інструмент оновлюється рідко та може не враховувати сучасні типи загроз.
Відповідність міжнародним стандартам – питання та рекомендації побудовані на загальновизнаних практиках безпеки (ISO/IEC 17799, NIST SP 800-53).	Відсутність автоматичного аудиту – система базується на анкетуванні, а не на технічному скануванні інфраструктури.
Простота використання – програма безкоштовна, має невеликий розмір і не потребує великих ресурсів.	Залежність від точності введених даних – результат оцінки напряму залежить від правильності відповідей користувача.
Надає рекомендації – після аналізу продукт формує звіт що включає: висновки, рівні ризику та порадами щодо покращення безпеки.	Не замінює повноцінний аудит – забезпечує загальний огляд без глибокого технічного аналізу.
Універсальність – підходить для організацій із різним рівнем зрілості системи безпеки.	Потребує адаптації під локальні умови – надані рекомендації мають узагальнений характер і потребують урахування специфіки конкретної організації.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Опис об’єкта дослідження. В рамках проведення експериментального дослідження об’єктом аналізу було обрано інформаційно-телекомунікаційну систему умовної IT-компанії «TechSecure Solutions». Вибір саме такого типу організації був зумовлений високими вимогами до забезпечення конфіденційності, цілісності та доступності інформації, що є відповідно, характерними для сучасних цифрових

підприємств, які працюють з критичними даними. Компанія спеціалізується на розробці програмного забезпечення для фінансового сектору, що визначає підвищену цінність її інформаційних активів. У межах діяльності обробляються як об'єкти інтелектуальної власності, зокрема вихідний код програмних продуктів, так і персональні дані клієнтів та фінансова інформація. Сукупність таких даних дозволяє віднести їх до категорії критичних, а саму інформаційно-телекомунікаційну систему – до об'єктів із підвищеними вимогами до інформаційної безпеки.

Параметри досліджуваної системи адаптовано відповідно до типових характеристик підприємства середнього масштабу [24]. Організаційна структура компанії налічує близько 230 співробітників, переважна частина яких технічні спеціалісти. Особливістю є наявність у значної кількості працівників розширених прав доступу до внутрішніх інформаційних ресурсів, що безпосередньо впливає на загальний рівень ризиків.

Система має у собі гібридну архітектурну модель. У хмарній інфраструктурі провідних провайдерів розміщені виробничі середовища розробки та тестування програмного забезпечення, тоді як у локальному офісному середовищі функціонує адміністративний сегмент, а також сховища критично важливих даних.

Поточний стан системи захисту інформації характеризується наявністю базових технічних засобів безпеки, зокрема міжмережевих екранів, антивірусного програмного забезпечення на кінцевих пристроях та використанням VPN-технологій для забезпечення віддаленого доступу. Водночас, попередній експрес-аудит засвідчив недостатній рівень зрілості процесів управління інформаційною безпекою, що проявляється у відсутності формалізованих політик та процедур.

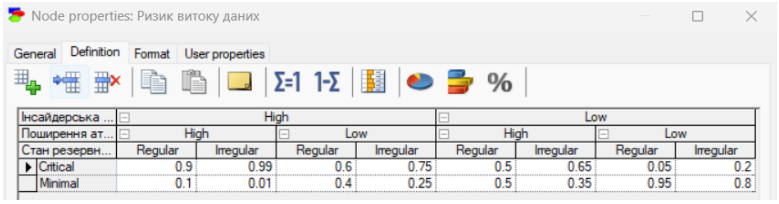
Аналіз виявив серйозні прогалини в безпеці: резервне копіювання проводиться хаотично, а відновлення системи після збоїв ніколи не перевіряли на практиці. Це створює реальну загрозу втрати даних при будь-якому інциденті. Ще однією слабкою ланкою є те, що більшість розробників мають права адміністраторів на своїх комп'ютерах. Це значно спрощує завдання для фішингових атак або дій зловмисників усередині компанії. До того ж, через відсутність нормального поділу мережі, до найважливіших баз даних можна дістатися навіть із загального Wi-Fi.

Усі ці фактори разом створюють ідеальні умови для витоку конфіденційної інформації. Саме цей сценарій було взято за основу для подальшого аналізу ризиків, який буде проведено за допомогою інструментів Microsoft Security Assessment Tool та GeNIe Modeler.

3.2 Побудова байєсівської моделі ризиків у програмному комплексі GeNIe Modeler. На основі ідентифікованих характеристик IT-інфраструктури об'єкта дослідження було розроблено топологію мережі (рис. 1), яка структурно відображає механізм розвитку потенційного інциденту. Граф моделі побудовано за ієрархічним принципом, де вхідними вузлами виступають зафіксовані під час аудиту фактори ризику: стан процедур резервного копіювання, рівень привілеїв користувачів та наявність сегментації мережі. Логіка моделі передбачає, що вплив всіх цих базових факторів на фінальний ризик не просто є прямим, а опосередковується через проміжні стани системи, а саме можливість неконтрольованого поширення атаки у корпоративній мережі та ймовірність реалізації інсайдерської загрози.

Рис. 1. Топологія розробленої баєсівської мережі у середовищі GeNIe Modeler

Критично важливим етапом налаштування моделі стала її параметризація шляхом формування таблиць умовних ймовірностей. Значення ймовірностей визначалися експертним методом, виходячи з припущення про кумулятивний ефект уразливостей, характерний для підприємств середнього масштабу з обмеженими ресурсами моніторингу. Зокрема, для цільового вузла «Ризик витоку даних» було змодельовано сценарій найгіршого випадку (рис. 2), де поєднання високого рівня інсайдерської загрози, широкого вектора поширення атаки та нерегулярного резервного копіювання призводить до критичних наслідків з імовірністю 0.99, що відображає неможливість відновлення цілісності активів за таких умов.



Інсайдерська ...	High				Low			
Поширення ат...	High		Low		High		Low	
Стан резервн...	Regular	Irregular	Regular	Irregular	Regular	Irregular	Regular	Irregular
Critical	0.9	0.99	0.6	0.75	0.5	0.65	0.05	0.2
Minimal	0.1	0.01	0.4	0.25	0.5	0.35	0.95	0.8

Рис. 2. Фрагмент таблиці умовних ймовірностей для цільового вузла моделі

Для моделювання реального стану безпеки компанії було реалізовано процедуру перерахунку ймовірностей із введенням свідчень, що відповідають результатам попереднього опису об’єкта. У модель було жорстко задано стани, виявлені під час аналізу інфраструктури: нерегулярність резервного копіювання (Irregular = 100%), надання розробникам надмірних прав доступу (Excessive = 100%) та відсутність сегментації мережі (Absent = 100%). Результати обчислення (рис. 3) продемонстрували, що за поточної конфігурації засобів захисту інтегральна ймовірність критичного витоку даних становить 89%.

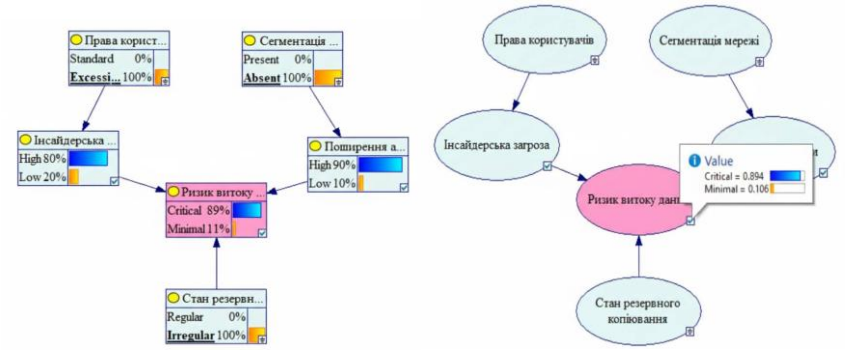


Рис. 3. Результати розрахунку ймовірності ризику для поточного стану системи

Отриманий кількісний показник свідчить про критичну уразливість досліджуваної системи, насамперед через синергетичний ефект відсутності сегментації та надмірних прав доступу. Такий рівень ризику вимагає верифікації альтернативними засобами аудиту, що зумовлює доцільність проведення наступного етапу дослідження з використанням інструментарію Microsoft Security Assessment Tool.

3.3 Проведення оцінювання ризиків у MSAT. З метою верифікації результатів імовірнісного моделювання та отримання комплексної оцінки рівня зрілості системи захисту інформації було проведено аудит компанії «TechSecure Solutions» із використанням інструментарію Microsoft Security Assessment Tool (MSAT).

На першому етапі було сформовано профіль об’єкта (рис. 4). Враховуючи специфіку діяльності, вказано належність до IT сектору та середній розмір штату (рис. 4, а). Високий базовий рівень ризику додатково обґрунтовано агресивним конкурентним середовищем (рис. 4, б) та використанням застарілого програмного забезпечення (рис. 4, в), що створює передумови для експлуатації відомих уразливостей.

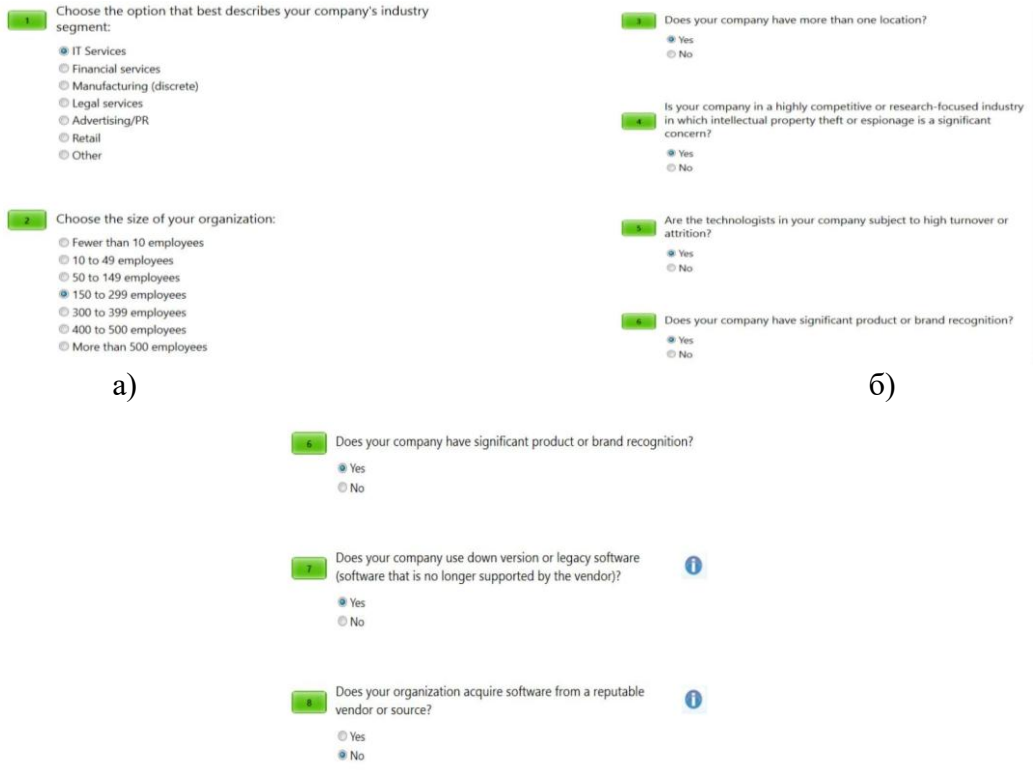
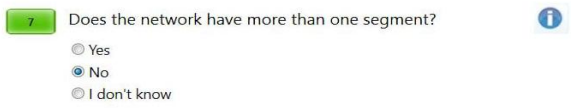
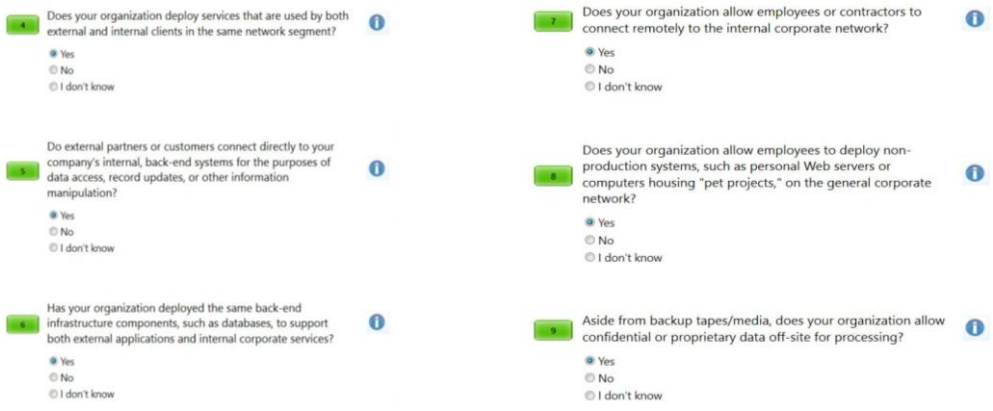


Рис. 4. Налаштування профілю об'єкта дослідження: а) галузь та розмір організації; б) фактори конкурентного середовища; в) використання застарілого ПЗ

Детальний аналіз інфраструктурної складової (рис. 5) підтвердив критичні архітектурні недоліки. Анкетування виявило відсутність сегментації внутрішньої мережі (рис. 5, а) та виділеної демілітаризованої зони для веб-сервісів (рис. 5, б), що значно спрощує горизонтальне переміщення зловмисника мережею. Ситуація ускладнюється використанням слабких механізмів автентифікації без застосування MFA (рис. 5, в).



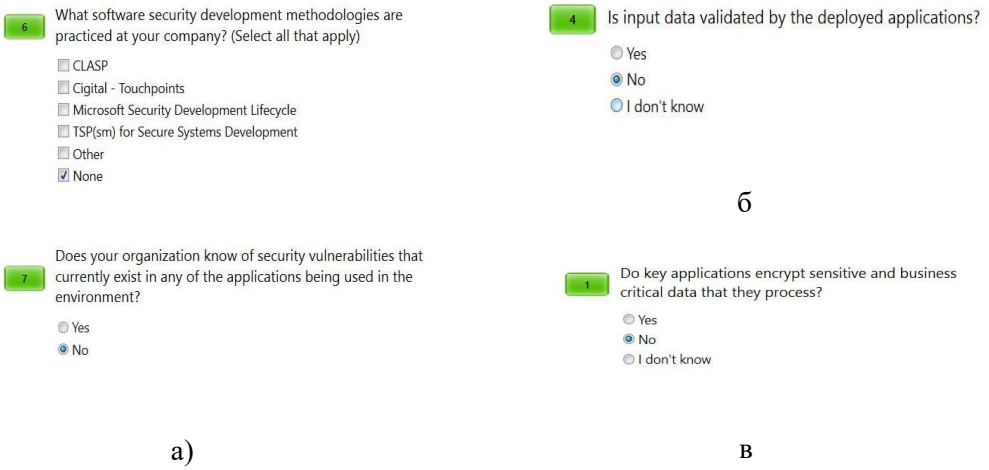
а)



б) в)

Рис. 5. Результати аудиту мережевої інфраструктури: а) відсутність сегментації мережі; б) відсутність демілітаризованої зони (DMZ); в) використання слабких паролів

У домені безпеки прикладного програмного забезпечення (рис. 6) зафіксовано повну відсутність методологій безпечної розробки (рис. 6, а). Аудит виявив, що програмні продукти не проходять валідацію вхідних даних (рис. 6, б), а критично важлива інформація зберігається у відкритому вигляді без шифрування (рис. 6, в), що створює ризики інтеграції коду та витоку даних.



а) б в

Рис. 6. Оцінювання безпеки прикладного ПЗ: а) відсутність методологій безпечної розробки; б) відсутність валідації вхідних даних; в) зберігання даних у відкритому вигляді

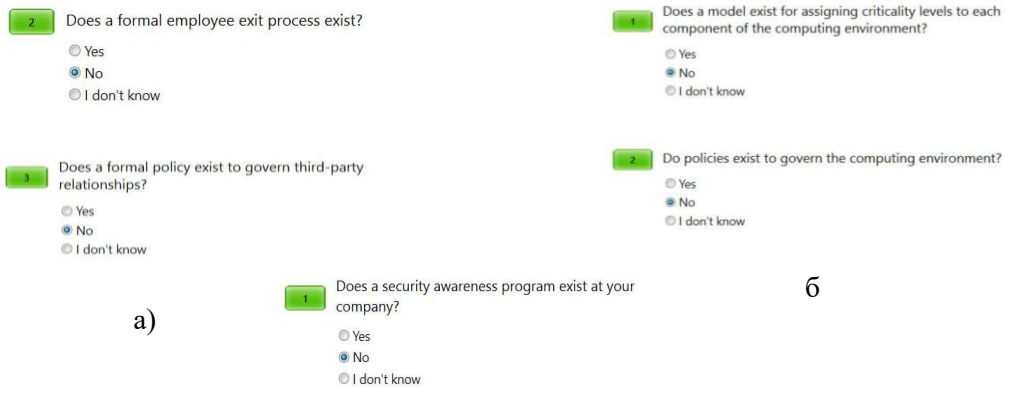
Найбільш критичні уразливості ідентифіковано у розділі операційної безпеки (рис. 7). Підтверджено, що в організації не виконується регулярне резервне копіювання критично важливих даних (рис. 7, а) та відсутній план аварійного відновлення (рис. 7,

б). Це корелює зі станом вузла «Backup_Status = Irregular» у побудованій раніше моделі. Також встановлено відсутність процедур тестування оновлень та централізованого моніторингу подій безпеки.

а) б)

Рис. 7. Недоліки операційної безпеки: а) нерегулярне резервне копіювання; б) відсутність плану аварійного відновлення

Аналіз організаційних заходів (рис. 8) засвідчив, що компанія не має формалізованої процедури анулювання прав доступу при звільненні співробітників (рис. 8, а). Відсутність затвердженої політики інформаційної безпеки (рис. 8, б) та регулярних навчань персоналу (рис. 8, в) створює сприятливі умови для соціальної інженерії.



а) б)

в

Рис. 8. Організаційні заходи безпеки: а) відсутність процедур анулювання прав доступу; б) відсутність політики інформаційної безпеки; в) відсутність програми підвищення обізнаності

За результатами анкетування сформовано підсумковий звіт (рис. 9). Графічний розподіл демонструє критичний дисбаланс, а саме: профіль бізнес-ризику (BRP) знаходиться на дуже високому рівні, тоді як індекс глибокого захисту (DiDI) є мінімальним. Це дозволяє класифікувати стан безпеки як стан високого ризику «High Risk», що повністю підтверджує результати моделювання у GeNIe (ймовірність успішної атаки 89%).

Рис. 9. Підсумковий звіт MSAT: розподіл профілю бізнес-ризику (BRP) та індексу глибокого захисту (DiDI)

Важливо розмежовувати поняття: у контексті MSAT термін "Business Risk Profile" стосується не фінансових показників чи ринкової кон'юнктури, а передусім того, наскільки глибоко IT інтегровано в бізнес і наскільки привабливими є активи компанії для хакерів. У нашому випадку цей профіль ризику є закономірно високим. Це зумовлено специфікою IT-компанії: тут зберігаються критично важливі дані (вихідний код, фінансова звітність), а будь-який простій сервісів є неприпустимим.

3.4 Порівняльний аналіз результатів. Завершальним етапом дослідження стало зіставлення результатів, отриманих двома різними методологічними підходами: кількісним моделюванням на основі баєсівських мереж довіри (GeNIe Modeler) та якісним аудитом зрілості системи захисту (Microsoft Security Assessment Tool). Метою цього етапу є взаємна верифікація отриманих даних та формування комплексного висновку щодо стану захищеності інформаційної системи компанії «TechSecure Solutions».

Попри фундаментальні відмінності в алгоритмах оцінювання, обидва інструменти продемонстрували високий рівень кореляції результатів, вказуючи на критичний стан інформаційної безпеки досліджуваного об'єкта. Узагальнена порівняльна характеристика результатів дослідження наведена в таблиці 3.

Таблиця 3

Порівняльний аналіз результатів оцінювання ризиків IT-компанії

Критерій порівняння	Імовірнісне моделювання (GeNIe Modeler)	Аудит зрілості (MSAT)
Методологічний підхід	Кількісний: розрахунок ймовірності реалізації конкретного сценарію атаки на основі причинно-наслідкових зв'язків.	Якісний: оцінювання відповідності впроваджених заходів захисту кращим практикам та стандартам (Defense-in-Depth).
Виявлені ключові уразливості	1. Відсутність сегментації мережі. 2. Нерегулярне резервне копіювання. 3. Надмірні права доступу користувачів.	1. Критичний розрив у захисті інфраструктури та операцій. 2. Відсутність політик безпеки та навчання персоналу. 3. Уразливість прикладного ПЗ (SDL).
Інтегральний показник ризику	89% (Ймовірність успішної реалізації атаки з витоком даних).	High Risk (Високий рівень ризику при мінімальному індексі захисту DiDI).
Характер висновків	Прогнозує неминучість інциденту через синергію технічних уразливостей.	Констатує системну неготовність організації до протидії загрозам через організаційні та технічні прогали.

Зіставлення результатів демонструє чітку конвергенцію обох методів. Розраховані у GeNIe 89% фактично дають математичне обґрунтування якісному вердикту «High Risk», який виставив MSAT. Глибший аналіз звітів дозволив виявити прямі паралелі між ключовими уразливостями в обох моделях.

Наприклад, критичний вузол «Backup_Status = Irregular» у байєсівській мережі повністю відповідає висновкам MSAT у блоці «Operations Security» – обидва інструменти вказують на хаотичність бекапів та брак планів відновлення. Та ж сама ситуація з мережею: статус «Segmentation = Absent» у GeNIe дзеркально відображається у розділі «Infrastructure Security» MSAT, де підсвічено відсутність DMZ. Не менш показовим є людський фактор: висока ймовірність інсайдерських загроз у моделі GeNIe корелює з прогалинами в «People Security» (MSAT), зокрема з відсутністю коректних процедур звільнення співробітників.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Поєднання інструментарію GeNIe Modeler (баєсівські мережі) та MSAT дозволило вийти за межі звичайного аудиту і створити об’ємну модель загроз. Вона не просто фіксує "дірки" в безпеці, а наочно показує, як саме архітектурні помилки чи дії персоналу можуть призвести до критичних збоїв. Головна цінність такого методу – це відмова від формальних чек-листів на користь розуміння глибинних причинно-наслідкових зв'язків. Отримана кількісна оцінка ризику витоку даних (89%) стає твердим підґрунтям для прийняття управлінських рішень в умовах невизначеності. Водночас, варто бути свідомим щодо обмежень цього підходу. Точність моделі напряму залежить від якості вхідних даних та експертних суджень, що завжди несе ризик суб’єктивізму. До того ж, статичні інструменти на кшталт MSAT дають картину лише на момент перевірки, яка швидко застаріває. Проте, для розвитку практичних компетенцій студентів використання доступного програмного забезпечення, зокрема інструментарію баєсівських мереж або безкоштовних утиліт на зразок MSAT, є критично важливим.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Shevchenko, S. M., Zhdanova, Y. D., Spasiteleva, S. O., & Skladannyi, P. M. (2020). Conducting SWOT analysis of information risk assessment as a means of forming practical skills of cybersecurity students. *Cybersecurity: Education, Science, Technique, 2*(10), 158–168. https://doi.org/10.28925/2663-4023.2020.10.158168
2. Shevchenko, H., Shevchenko, S., Zhdanova, Y., Spasiteleva, S., & Nehodenko, O. (2021). Information security risk analysis using SWOT. In *Cybersecurity Providing in Information and Telecommunication Systems* (Vol. 2923, pp. 309–317). http://ceur-ws.org/Vol-2923/paper34.pdf
3. Dziuba, L., & Chmyr, O. (2022). Information security risk assessment using mathematical statistics methods. *Bulletin of Lviv State University of Life Safety, 26*, 47–54. https://doi.org/10.32447/20784643.26.2022.06
4. Shevchenko, S., Zhdanova, Y., & Kiia, O. (2025). Semi-automated tool for multi-standard cybersecurity maturity assessment based on NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019, and CIS Controls v8. *Cybersecurity: Education, Science, Technique, 3*(31), 43–60. https://doi.org/10.28925/2663-4023.2025.31.1004
5. Shevchenko, S., Zhdanova, Y., Shevchenko, H., Nehodenko, O., & Spasiteleva, S. (2023). Information security risk management using cognitive modeling. In *Cybersecurity Providing in Information and Telecommunication Systems* (Vol. 3550, pp. 297–305). https://ceur-ws.org/Vol-3550/short15.pdf
6. Shevchenko, S., Zhdanova, Y., Kryvytska, O., Shevchenko, H., & Spasiteleva, S. (2024). Fuzzy cognitive mapping as a scenario approach for information security risk analysis. In *Cybersecurity Providing in*

Information and Telecommunication Systems II (Vol. 3826, pp. 356–362). https://ceur-ws.org/Vol-3826/short28.pdf

7. Shevchenko, S., Zhdanova, Y., Skladannyi, P., & Petrenko, T. (2024). Fuzzy cognitive maps as a tool for visualization of incident response scenarios in security systems. *Cybersecurity: Education, Science, Technique, 2*(26), 419–429. https://doi.org/10.28925/2663-4023.2024.26.707
8. Bone, J. (2024). *Cognition in cybersecurity situational awareness*. https://doi.org/10.13140/RG.2.2.23490.59842
9. Shevchenko, S. M., Zhdanova, Y. D., & Harkushenko, A. M. (2025). Cognitive modeling of scenarios for cybersecurity risk forecasting. In *Technical, agricultural and mathematical sciences: Scientific trends, problems and ways of their development* (pp. 178–196). Primedia eLaunch. https://isg-konf.com
10. Kostiuk, Y., Skladannyi, P., Samoilenko, Y., Khorolska, K., Bebeshko, B., & Sokolov, V. (2025). A system for assessing interdependencies of information system agents in risk management using cognitive maps. In *Cyber Hygiene & Conflict Management in Global Information Networks 2024* (Vol. 3925, pp. 249–264).
11. Tymoshyn, A., Kalienichenko, L., Hnusov, Y., Khavina, I., Tsuranov, M., & Dovhan, I. (2025). Integrated information security risk management model based on AHP and Bayesian networks. *Innovative Technologies and Scientific Solutions for Industries, 3*(33), 166–179. https://doi.org/10.30837/2522-9818.2025.3.166
12. Wang, J., Neil, M., & Fenton, N. (2020). A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. *Computers & Security, 89*. https://doi.org/10.1016/j.cose.2019.101659
13. Khosravi-Farmad, M., & Ghaemi-Bafghi, A. (2020). Bayesian decision network-based security risk management framework. *Journal of Network and Systems Management, 28*, 1794–1819. https://doi.org/10.1007/s10922-020-09558-5
14. Flores, M., Heredia, D., Andrade, R., & Ibrahim, M. (2022). Smart home IoT network risk assessment using Bayesian networks. *Entropy, 24*(5), 668. https://doi.org/10.3390/e24050668
15. Chockalingam, S., Pieters, W., Teixeira, A., & van Gelder, P. (2017). Bayesian network models in cybersecurity: A systematic review. In H. Lipmaa et al. (Eds.), *Secure IT Systems* (pp. 105–122). Springer.
16. Palko, D., & Myrutenko, L. (2024). Method for comprehensive cybersecurity risk assessment in distributed information systems. *Cybersecurity: Education, Science, Technique, 2*(26), 487–502. https://doi.org/10.28925/2663-4023.2024.26.731
17. Barlybayev, A., Sharipbay, A., Shakhmetova, G., & Zhumadillayeva, A. (2024). Development of a flexible information security risk model using machine learning and ontologies. *Applied Sciences, 14*(21), 9858. https://doi.org/10.3390/app14219858
18. Bebeshko, B., Malyukov, V., Lakhno, M., Skladannyi, P., Sokolov, V., Shevchenko, S., & Zhumadilova, M. (2022). Application of game theory, fuzzy logic, and neural networks for risk assessment. *Journal of Theoretical and Applied Information Technology, 100*(24), 7390–7404
19. Bayes Server. (n.d.). *Introduction to risk modeling with Bayesian networks*. https://www.bayesserver.com/docs/modeling/risk/
20. BayesFusion. (n.d.). *GeNIe Modeler: Complete modeling freedom*. https://www.bayesfusion.com/genie/
21. Microsoft. (n.d.). *Microsoft Security Assessment Tool 4.0*. https://www.microsoft.com/en-us/download/details.aspx?id=12273
22. Bidiuk, P. I., & Kuznietsova, N. V. (2007). Main stages of construction and application of Bayesian networks. *System Research & Information Technologies, 4*.
23. Moe, S. J., Carriger, J. F., & Glendell, M. (2021). Increased use of Bayesian networks in environmental risk assessment. *Integrated Environmental Assessment and Management, 17*(1), 53–61. https://doi.org/10.1002/ieam.4369
24. Verkhovna Rada of Ukraine. (1999). *Law of Ukraine "On accounting and financial reporting in Ukraine"*. https://zakon.rada.gov.ua/laws/show/996-14#Text

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

Svitlana Shevchenko
PhD, Associate Professor,
Associate Professor of the Department of Information and Cybersecurity
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

Yuliia Zhdanova
PhD, Associate Professor,
Associate Professor of the Department of Information and Cybersecurity
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0002-9277-4972
y.zhdanova@kubg.edu.ua

Valeriia A. Storozhenko
student of the Faculty of Information Technologies and Mathematics
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0009-0004-7726-9670
vastorozhenko.fitm23@kubg.edu.ua

Valeria O. Rashevska
student of the Faculty of Information Technologies and Mathematics
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0009-0008-1921-5104
vorashevska.fitm23@kubg.edu.ua

Volodymyr V. Horbach
student of the Faculty of Information Technologies and Mathematics
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0009-0005-7431-9879
vvhorbach.fitm23@kubg.edu.ua

INTEGRATED INFORMATION SECURITY RISK ASSESSMENT BASED ON BAYESIAN NETWORKS AND MATURITY AUDIT

Abstract. A fundamental element of any security architecture is risk assessment, which allows you to systematize potential threats and predict their impact on the confidentiality, integrity and availability of information assets. This study highlights the issue of probabilistic risk modeling using specialized tools, in particular Bayesian networks (BN) and the Microsoft Security Assessment Tool (MSAT). This approach allows not only to visualize the topology of threats, but also to mathematically substantiate the cause-and-effect relationships between vulnerabilities and possible losses. The conducted analysis of scientific sources allowed us to systematize existing methods, from classic questionnaires to complex mathematical models for assessing information security risks, in particular SWOT analysis, expert method, normative method, game theory, fuzzy cognitive maps, as well as the use of neural network models. The practical significance of the study lies in the development and testing of a comprehensive methodology for assessing the security of a hypothetical organization. This methodology is based on quantitative modeling using the GeNIe Modeler software package and a qualitative audit of the maturity of the security system using the Microsoft Security Assessment Tool. Comparative analysis showed that MSAT is a reliable tool for identifying gaps in compliance and organizational protection, while Bayesian networks provide a deeper quantitative analysis of the criticality of risks, allowing modeling the effectiveness of implementing specific countermeasures. The results of the study have both theoretical and applied significance. The developed models and methodological recommendations were implemented in the educational process when training specialists in the specialty F5 "Cybersecurity and Information Protection" at the Borys Grinchenko Kyiv Metropolitan

University. This confirms the feasibility of using combined intelligent systems for making informed decisions in the field of digital infrastructure risk management.

Keywords: information security; cybersecurity; information security risks; cyber risks; information protection; Microsoft Security Assessment Tool (MSAT); GeNIe Modeler software package; Bayesian networks (BN).

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Shevchenko, S. M., Zhdanova, Y. D., Spasiteleva, S. O., & Skladannyi, P. M. (2020). Conducting SWOT analysis of information risk assessment as a means of forming practical skills of cybersecurity students. *Cybersecurity: Education, Science, Technique, 2*(10), 158–168. https://doi.org/10.28925/2663-4023.2020.10.158168
2. Shevchenko, H., Shevchenko, S., Zhdanova, Y., Spasiteleva, S., & Nehodenko, O. (2021). Information security risk analysis using SWOT. In *Cybersecurity Providing in Information and Telecommunication Systems* (Vol. 2923, pp. 309–317). http://ceur-ws.org/Vol-2923/paper34.pdf
3. Dziuba, L., & Chmyr, O. (2022). Information security risk assessment using mathematical statistics methods. *Bulletin of Lviv State University of Life Safety, 26*, 47–54. https://doi.org/10.32447/20784643.26.2022.06
4. Shevchenko, S., Zhdanova, Y., & Kiia, O. (2025). Semi-automated tool for multi-standard cybersecurity maturity assessment based on NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019, and CIS Controls v8. *Cybersecurity: Education, Science, Technique, 3*(31), 43–60. https://doi.org/10.28925/2663-4023.2025.31.1004
5. Shevchenko, S., Zhdanova, Y., Shevchenko, H., Nehodenko, O., & Spasiteleva, S. (2023). Information security risk management using cognitive modeling. In *Cybersecurity Providing in Information and Telecommunication Systems* (Vol. 3550, pp. 297–305). https://ceur-ws.org/Vol-3550/short15.pdf
6. Shevchenko, S., Zhdanova, Y., Kryvytska, O., Shevchenko, H., & Spasiteleva, S. (2024). Fuzzy cognitive mapping as a scenario approach for information security risk analysis. In *Cybersecurity Providing in Information and Telecommunication Systems II* (Vol. 3826, pp. 356–362). https://ceur-ws.org/Vol-3826/short28.pdf
7. Shevchenko, S., Zhdanova, Y., Skladannyi, P., & Petrenko, T. (2024). Fuzzy cognitive maps as a tool for visualization of incident response scenarios in security systems. *Cybersecurity: Education, Science, Technique, 2*(26), 419–429. https://doi.org/10.28925/2663-4023.2024.26.707
8. Bone, J. (2024). *Cognition in cybersecurity situational awareness*. https://doi.org/10.13140/RG.2.2.23490.59842
9. Shevchenko, S. M., Zhdanova, Y. D., & Harkushenko, A. M. (2025). Cognitive modeling of scenarios for cybersecurity risk forecasting. In *Technical, agricultural and mathematical sciences: Scientific trends, problems and ways of their development* (pp. 178–196). Primedia eLaunch. https://isg-konf.com
10. Kostiuk, Y., Skladannyi, P., Samoilenko, Y., Khorolska, K., Bebeshko, B., & Sokolov, V. (2025). A system for assessing interdependencies of information system agents in risk management using cognitive maps. In *Cyber Hygiene & Conflict Management in Global Information Networks 2024* (Vol. 3925, pp. 249–264).
11. Tymoshyn, A., Kalienichenko, L., Hnusov, Y., Khavina, I., Tsuranov, M., & Dovhan, I. (2025). Integrated information security risk management model based on AHP and Bayesian networks. *Innovative Technologies and Scientific Solutions for Industries, 3*(33), 166–179. https://doi.org/10.30837/2522-9818.2025.3.166
12. Wang, J., Neil, M., & Fenton, N. (2020). A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. *Computers & Security, 89*. https://doi.org/10.1016/j.cose.2019.101659
13. Khosravi-Farmad, M., & Ghaemi-Bafghi, A. (2020). Bayesian decision network-based security risk management framework. *Journal of Network and Systems Management, 28*, 1794–1819. https://doi.org/10.1007/s10922-020-09558-5
14. Flores, M., Heredia, D., Andrade, R., & Ibrahim, M. (2022). Smart home IoT network risk assessment using Bayesian networks. *Entropy, 24*(5), 668. https://doi.org/10.3390/e24050668
15. Chockalingam, S., Pieters, W., Teixeira, A., & van Gelder, P. (2017). Bayesian network models in cybersecurity: A systematic review. In H. Lipmaa et al. (Eds.), *Secure IT Systems* (pp. 105–122). Springer.

16. Palko, D., & Myrutenko, L. (2024). Method for comprehensive cybersecurity risk assessment in distributed information systems. *Cybersecurity: Education, Science, Technique, 2*(26), 487–502. https://doi.org/10.28925/2663-4023.2024.26.731
17. Barlybayev, A., Sharipbay, A., Shakhmetova, G., & Zhumadillayeva, A. (2024). Development of a flexible information security risk model using machine learning and ontologies. *Applied Sciences, 14*(21), 9858. https://doi.org/10.3390/app14219858
18. Bebeshko, B., Malyukov, V., Lakhno, M., Skladannyi, P., Sokolov, V., Shevchenko, S., & Zhumadilova, M. (2022). Application of game theory, fuzzy logic, and neural networks for risk assessment. *Journal of Theoretical and Applied Information Technology, 100*(24), 7390–7404
19. Bayes Server. (n.d.). *Introduction to risk modeling with Bayesian networks*. https://www.bayesserver.com/docs/modeling/risk/
20. BayesFusion. (n.d.). *GeNIe Modeler: Complete modeling freedom*. https://www.bayesfusion.com/genie/
21. Microsoft. (n.d.). *Microsoft Security Assessment Tool 4.0*. https://www.microsoft.com/en-us/download/details.aspx?id=12273
22. Bidiuk, P. I., & Kuznietsova, N. V. (2007). Main stages of construction and application of Bayesian networks. *System Research & Information Technologies, 4*.
23. Moe, S. J., Carriger, J. F., & Glendell, M. (2021). Increased use of Bayesian networks in environmental risk assessment. *Integrated Environmental Assessment and Management, 17*(1), 53–61. https://doi.org/10.1002/ieam.4369
24. Verkhovna Rada of Ukraine. (1999). *Law of Ukraine "On accounting and financial reporting in Ukraine"*. https://zakon.rada.gov.ua/laws/show/996-14#Text

Отримано редакцією журналу / Received: 25.01.26
Прорецензовано / Revised: 15.02.26
Схвалено до друку / Accepted: 26.03.26