УДК: 004.056.5:519.2 DOI 10.33111/mise.105.5

Джалладова І. А.
д. ф.-м. н., професор кафедри системного аналізу та кібербезпеки
КНЕУ імені Вадима Гетьмана
Камінський О. Є.,
д. е. н., професор кафедри системного аналізу та кібербезпеки
КНЕУ імені Вадима Гетьмана
Лютий О.І.
к.т.н., доц., доцент кафедри системного аналізу та кібербезпеки
КНЕУ імені Вадима Гетьмана

Dzhalladova I. A.,
Doctor of Science, Professor at the Department of Systems Analysis and Cybersecurity KNEU named after V. Hetman
Kaminsky O. E, Doctor of Economics, Professor of the Department of System Analysis and Cybersecurity, KNEU named after V. Hetman
Lyuty O.I.
Ph.D., Associate Professor, Department of System Analysis and Cybersecurity,
KNEU named after V. Hetman

ОЦІНКА РИЗИКІВ КІБЕРЗАГРОЗ ЕМПІРІЧНИМИ ТА АНАЛІТИЧНИМИ МЕТОДАМИ

ASSESSMENT OF CYBER THREAT RISKS USING EMPIRICAL AND ANALYTICAL METHODS

Анотація. *У дослідженні аналізується питання реагування на кіберінциденти безпеки, використовуючи передові технології. Акцент робиться не лише на експертних оцінках, оскільки збільшення складності та непередбачуваності кіберзагроз ставить під сумнів ефективність традиційних методів.У зв'язку з цим, запропонована інтеграція кількісних досліджень реальних випадків кіберінцидентів з інструментами формалізованого моделювання загроз, що дає змогу створити сучасну систему управління ризиками. Проведено аналіз провідних наукових досліджень у цій сфері, де були розглянуті такі інструменти, як стандарт ISO/IEC 27000, методології STRIDE, STPA-Sec та CORAS, а також статистичні моделі пріоритезації вразливостей. У практичній частині наведено симуляційну модель на основі марковських процесів для прогнозування змін рівня безпеки підприємства в умовах переходу між різними станами системи (нормальний, загроза, атака). Візуалізовано зміни рівня безпеки підприємства в залежності від динаміки очікуваних витрат/прибутків. Застосування нового авторського підходу з компонентами апарату стохастичної математики, методів смарт-аналітики, бібліотек Python враховує особливості функціонування системи за умов невизначеності. Отримані результати показали перспективи автоматизації процесу оцінювання ризиків шляхом використання методів машинного навчання та побудови на їх основі адаптивних моделей, здатних швидко реагувати на зміну характеру загроз.*

Ключові слова: *кіберзагрози, оцінка ризиків, емпіричні методи, смарт-аналітика, марковські процеси*

Abstract. *The study analyzes the issue of responding to cyber security incidents using advanced technologies. The emphasis is not only on expert assessments, since the increase in the complexity and unpredictability of cyber threats calls into question the effectiveness of traditional methods. In this regard, the integration of quantitative studies of real cases of cyber incidents with tools for formalized threat modeling is proposed, which makes it possible to create a modern risk management system. An analysis of leading scientific research in this area was conducted, where such tools as the ISO/IEC 27000 standard, STRIDE, STPA-Sec and CORAS methodologies, as well as statistical models for prioritizing vulnerabilities were considered. The practical part presents a simulation model based on Markov processes for predicting changes in the level of enterprise security in conditions of transition between different system states (normal, threat, attack). Changes in the level of enterprise security are visualized depending on the dynamics of expected costs/profits. The application of a new author's approach with components of the apparatus of stochastic mathematics, smart analytics methods, Python libraries takes into account the peculiarities of the system's functioning under conditions of uncertainty. The results obtained showed the prospects for automating the risk assessment process by using machine learning methods and building adaptive models based on them, capable of quickly responding to changing threats.*
Keywords: *cyber threats, risk assessment, empirical methods, smart analytics, Markov processes.*

Вступ. Моніторинг кіберінцидентів за певні фіксовані періоди (тижні, місяці, рокі) фіксує зростання рівня кіберзагроз, що порушує стабільність безпеки структур в державі. Кібератаки спричиняють значні фінансові збитки, шкоду репутації, втрати на об'єктах критичної інфраструктури.

Боротьба з цими викликами їде по всім фронтам: технічні засоби захисту інформації, системні та превентивні підходи ло управління та оцінювання ризиків тощо.

Аналіз великих обсягів різноманітних даних в кіберпросторі, застосування методів смарт аналітики дають змогу значно знизити рівень загроз. Впровадження таких підходів вже створило ефективну систему управління ризиками в області кібербезпеки.

Але незважаючи на значний обсяг наукових досліджень з управління кіберризиками, існують складнощі у впровадженні цих знань у практичну діяльність, а також в обробці даних випадкової структури. Вихід знаходять у розвитку методів штучного інтелекту та машинного навчання, які здатні аналізувати великі масиви даних для виявлення та прогнозування потенційних слабких місць у кіберзахисті. Моделі машинного навчання можуть прогнозувати, які вразливості з найбільшою ймовірністю будуть використані зловмисниками, що дає змогу фахівцям з кібербезпеки усувати недоліки у системі безпеці.

Актуальним напрямом у формуванні стратегії боротьби з цими недоліками є напрям наукових досліджень, пов'язаний з теорією і практикою прийняттям рішень в умовах невизначеності (у тому числі військовий стан, умови кібервійни тощо), що безпосередньо приводить до побудові теоретичних і експериментальних моделей, параметри яких залежать від випадкових процесів. Результати у запропонованої статті сприятимуть розвитку як академічної, так і практичної складової з питань управління кібербезпекою.

Аналіз останніх досліджень і публікацій. Враховуючи важливість сфери, обсяг наукових досліджень різиків в кіберпросторі зростає, але зростання складності атак, їх масштаби та потенційні ризики для державної безпеки вимагають постійно удосконалювати інструментарій, в тому числі із застосуванням розвинутих математичних моделей [14].

У роботі [1] було застосовано теорію стохастичних диференційних рівнянь та рівняння Колмогорова для оцінки ймовірності переходів між станами (нормальний, загроза, атака), що забезпечує формалізоване прогнозування ризику. Визначено концептуально інший підхід до оцінювання ефективності ведення кібероборотьби, який зводиться до її математичного моделювання як випадкового (стохастичного) процесу та отримання ймовірнісних показників, за якими є можливим аналізувати величину прогнозованого ефекту від кібердій.

В дослідженні [2] було розроблено моделі захисту на базі великих даних і методів машинного навчання; наведений автором досвід формального моделювання кібербезпеки представляє практичний інструментарій для інтеграції з кількісними підходами.

В роботі [3] було досліджено систему масового обслуговування під час кібератак із імітаційним моделюванням. Розраховані середні характеристики та показники варіативності (дисперсія, ймовірності режимів) для оцінки ефективності груп реагування та адаптації системи в реальному часі, отримані результати дозволяють прогнозувати появу режиму перевантаження, породженого відсутністю ергодичної властивості функціонування системи, в умовах якого діяльність системи перестає бути ефективною.

У дослідженні [4] було розглянуто граничну поведінку марковських процесів із локальними. Основна увага приділена побудові функціональних граничних теорем та вивченню умов, за яких марковський процес збігається до узагальненого броунівського руху з особливостями у точці збурення. Отримані результати мають важливе значення для моделювання стохастичних систем із неоднорідностями, до яких відносяться і системи кіберзахисту.

Так, у дослідженні [5] було представлено систематичний огляд інструментів, що автоматизують етапи оцінювання ризиків кібербезпеки. Автори ідентифікували 35 інструментів на базі 40 наукових досліджень, опублікованих у період з 2012 по 2020 роки. Більшість інструментів базуються на стандартах ISO/IEC 27000 та NIST 800-30. Дослідження виявило, що хоча якісні інструменти широко використовуються, експерти надають перевагу кількісним методам через їхню об'єктивність. В межах дослідження було представлено модель оцінювання ризиків, яка охоплює базові параметри та структурні компоненти відповідного процесу.

Модель, здатна оцінювати кіберзагрози, використовуючи ланцюги Маркова та графи атак, була запропонована Айсою та ін. [6]. Наведений в роботі підхід поєднує показники кібербезпеки на основі часу разом з ймовірностями загроз для побудови матриці переходів, яка визначає ймовірність переходів станів між безпечним та скомпрометованим станами для кожного компонента системи. Інтегруючи ці елементи, модель забезпечує ймовірнісну основу для оцінки стану безпеки окремих компонентів системи.

Дослідження [7] присвячене порівнянню трьох методів оцінки ризиків: STPA-Sec, STRIDE і CORAS, на прикладі моделі системи CyberShip. Порівняльний аналіз показав, що кожен підхід має свої переваги: STRIDE забезпечує ефективну ідентифікацію загроз на рівні окремих компонентів, тоді як STPA-Sec та CORAS краще охоплюють взаємозв'язки між елементами системи. Було зроблено висновок про доцільність комбінування цих методів задля отримання більш комплексної оцінки ризиків.

У статті [8] запропоновано підхід, що створює передумови для ухвалення рішень у сфері кіберзахисту на основі моделі медіанної регресії, яка функціонує з порядковими оцінками ризиків і забезпечує надійне ранжування загроз у ситуаціях з обмеженим обсягом даних.

Моніторінг літератури показує, що створений математичний аппарат дає змогу практичного застосування для розв'язання поставленої задачи (але фактично не застосовується), а також не зважаючи на розробки методів оцінки ризиків, наявні підходи не беруть до уваги стохастичну динаміку загроз та пов'язані з ними ризики впродовж певних періодів часу.

Метою дослідження є оцінювання ризиків, пов'язаних із кіберзагрозами, з особливою увагою на синтез емпіричних спостережень і аналітичного моделювання за допомогою запропонованого авторами підходу на основі інтеграції апарату випадкових процесів, смарт-аналітики та ПЗ.

Виклад основного матеріалу. Актуальним і дієвим з точки зору отримання оцінок, зокрема, визначення розміру можливих втрат, впливу різноманітних кіберзагроз в умовах їхньої випадкової природи є застосування марковських процесів для моделювання станів системи кібербезпеки. Розглянемо це на прикладі модельної задачі.

Модельна задача. Для моделювання оцінки ризику кіберзагроз на діяльність оборонного підприємства можна використовувати концепції, схожі на те, що ми розглядали в попередніх розрахунках з марковськими ланцюгами та процесами.

Розробимо формальний опис моделі оцінювання ризику кіберзагроз. Модель визначається рівнянням:

$$x(n+1) = a(b_n)x(n)$$

де:

- $x(n)$ — показник, що відображає стан безпеки підприємства (ефективність захисту інформаційних систем або рівень безпеки інформації на певному кроці часу n).
- $a(b_n)$ — коефіцієнт, який залежить від стану b_n (де b_n є марковським процесом, що описує ймовірності переходу між різними станами безпеки: нормальний, під загрозою, атакований).

Моделювання ризику включає наступні компоненти:

1. Стани:

— Стан θ_0: Нормальний стан безпеки.

— Стан θ_1: Стан, коли інформаційні системи перебувають під загрозою.

— Стан θ_2: Стан, коли система зазнає кібернападу або іншої загрози.

2. Матриця переходів P містить ймовірність переходів від одного стану системи до іншого (від нормального стану до стану загрози, від стану загрози до стану атаки).

3. Показники $a(b_n)$ можуть залежати від рівня загрози, наприклад:

— Стан θ_0: (нормальний), показник a дорівнює 1 (без змін).

— Стан θ_1: (загроза), показник а дорівнює 0,8 (ефективність захисту знижується).

— Стан θ_2: (атака), показник а приймає значення 0,5 (критичне зниження ефективності).

Визначення ризику. Ризик можна оцінити за наступним алгоритмом:

1. Небезпека збитків від кіберзагрози оцінюється як різниця між початковим рівнем безпеки $x(0)$ та величиною рівня захисту на певному етапі функціонування системи $x(N)$, і залежить від ймовірності переходу й кількості етапів.

2. Загальний рівень ризику розраховується як середнє значення $x(n)$.

Покрокова реалізація:

1. Визначимо ймовірності переходу між станами

Матриця переходів P для трьох станів (нормальний, під загрозою, атака) виглядає наступним чином:

$$P = \begin{pmatrix} 0.9 & 0.1 & 0 \\ 0.2 & 0.7 & 0.1 \\ 0.0 & 0.3 & 0.7 \end{pmatrix}$$

Тобто:

— 90 % ймовірність залишитись в нормальному стані.

— 20 % ймовірність переходу з нормального в загрозу.

— 70 % ймовірність залишитись у стані загрози, 30 % — ймовірність переходу в атаку.

2. Коефіцієнти ефективності $a(b_n)$:

— Нормальний стан: $a(0) = 1$;

— Загроза: $a(1) = 0.8$;

— Атака: $a(2) = 0.5$.

3. Далі моделюємо процес і оцінюємо ризик за допомогою програмного коду [13].

4. Аналізуємо та робимо опис результатів: Отриманий графік (див.рис.1.) відображає, як змінюється рівень безпеки підприємства на кожному кроці часу. 95 % довірчі інтервали показують варіацію ризику залежно від змін ймовірностей переходів між станами. Графік показує, що ризик зниження безпеки підвищується в міру того, як система перебуває у стані загрози або атаки.

5. Подальші кроки: для точнішої оцінки можна додати більше реальних сценаріїв та параметрів для кожного стану (наприклад, додаткові типи атак, варіації в ефективності заходів безпеки) [9, 10].

Подана модель є елементом авторської методики оцінювання ризиків для підприємства оборонної галузі, котру можливо буде поліпшити або налаштувати, зважаючи на особливості конкретного підприємства. Додамо варіативність для визначення суми збитків на кожному стані. Для цього ми введемо випадкову величину для кожного стану, яка буде визначати величину збитків залежно від поточного стану системи:

Для вдосконалення програми виконаємо наступні кроки:

1. Визначимо варіативність для суми збитків на кожному стані.

— Нормальний стан: збитки низькі (наприклад, від 0 до 10 умовних одиниць).

— Загроза: збитки помірні (наприклад, від 10 до 50 умовних одиниць).

— Атака: високі збитки (наприклад, від 50 до 100 умовних одиниць).

2. Величини ймовірних збитків створюємо за допомогою генератора випадкових чисел.

3. Використаємо ці дані для обчислення загальних збитків на кожному кроці для кожної симуляції, та оцінюватимемо сумарні збитки підприємства в результаті атак. Результати роботи програми [13] наведено на рисунку 1 та рис. 2.

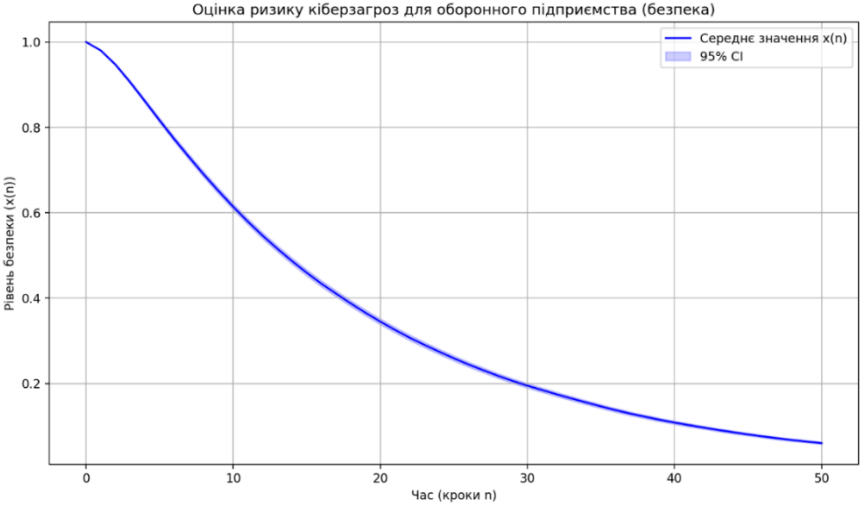

Рис. 1. Графік оцінки ризику кіберзагроз
для оборонного підприємства

Джерело: розроблено авторами

Визначення варіативності для збитків:

— Нормальний стан: збитки генеруються випадковим чином у межах [0, 10].

— Загроза: збитки генеруються випадковим чином у межах [10, 50].

— Атака: збитки генеруються випадковим чином у межах [50, 100].

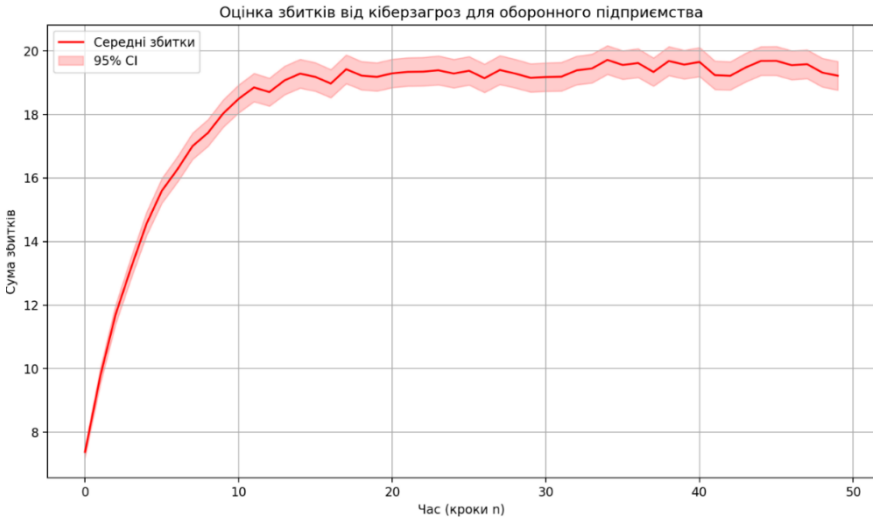

Рис. 2. Графік оцінки збитків від кіберзагроз
для оборонного підприємства

Джерело: розроблено авторами

Симуляція: для кожного стану на кожному кроці n генерується випадкова сума збитків, яка додається до загальних збитків підприємства.

Ризик розраховується наступним чином:

1. Оцінюємо середні збитки на кожному кроці часу та їх варіативність.
2. Підраховуємо загальні збитки за всі симуляції для кожного сценарію.

На основі оцінювання створюємо наступні графіки:

— Графік для рівня безпеки підприємства.

— Графік для середніх збитків, що визначає як змінюється ризик на кожному етапі.

Візуалізація збитків показує, як змінюється фінансові витрати в кожному з можливих станів і те, що зменьшується поступово стійкість системи.

Доповнимо модель оцінки розрахунком дисперсії, який дозволяє кількісно оцінити, наскільки фактичні або змодельовані значення ризиків (наприклад, рівень вразливості, ймовірність атаки, збитки) відхиляються від середнього значення. Це особливо важливо при аналізі динамічних кіберзагроз, які мають непередба-

чуваний характер [11]. Наприклад, у моделі оцінки ймовірності успішного злому різних систем, висока дисперсія вказує на високий ступінь невизначеності – одні системи надзвичайно вразливі, інші майже неуразливі.

1. Дисперсія процесу x(n) розраховується за формулою:

$$D[x(n)] = E[x(n)^2] - (E[x(n)])^2 = m_2(n) - \left(m_1(n)\right)^2$$

2. Коефіцієнт варіації (CV) розраховується за формулою:

$$CV[x(n)] = \frac{\sqrt{D[x(n)]}}{E[x(n)]}$$

Показує рівень розсіювання щодо середнього значення. В результаті ми отримаємо 3 графіки: перший момент, дисперсію та коефіцієнт варіації. Але кіберзагрози часто моделюються на основі історичних даних, емпіричних вимірів або симуляцій Оскільки жоден із цих методів не гарантує абсолютну точність, застосування довірчих інтервалів дасть змогу оцінити діапазон, у якому з певною ймовірністю (наприклад, 95 %) знаходиться істинне значення ризику.

1. Довірчі інтервали для $(E[x(n)])$ для кожного n з симуляцій розраховується за формулою:

$$CI = \overline{x_n} \pm z \cdot \frac{s_n}{\sqrt{M}}$$

де:

$(\overline{x_n})$ – середнє значення;

(s_n) – стандартне відхилення;

($z \approx 1.96$) — для 95 % інтервалу;

(M) – кількість симуляцій.

2. Для розподілу $x(n)$ на конкретному кроці (наприклад, n = 20) включає можна також побудувати логарифмічну шкалу, якщо розкид дуже великий. Код програми наведено в [13]. Результати наведено на рис. 3 та 4.

Висновки. В межах проведеного дослідження було запропоновано авторську модель оцінювання кіберризиків, яка базується на синтезі емпіричних та аналітичних підходів. Використання емпіричних даних забезпечує відповідність розрахунків реальним умовам функціонування інформаційно-комунікаційних систем, тоді як аналітичні методи, зокрема моделювання на основі марковських процесів, обчислення дисперсії, довірчих інтервалів та

коефіцієнтів варіації надають можливість комплексно проаналізувати невизначеність і мінливість ризиків.

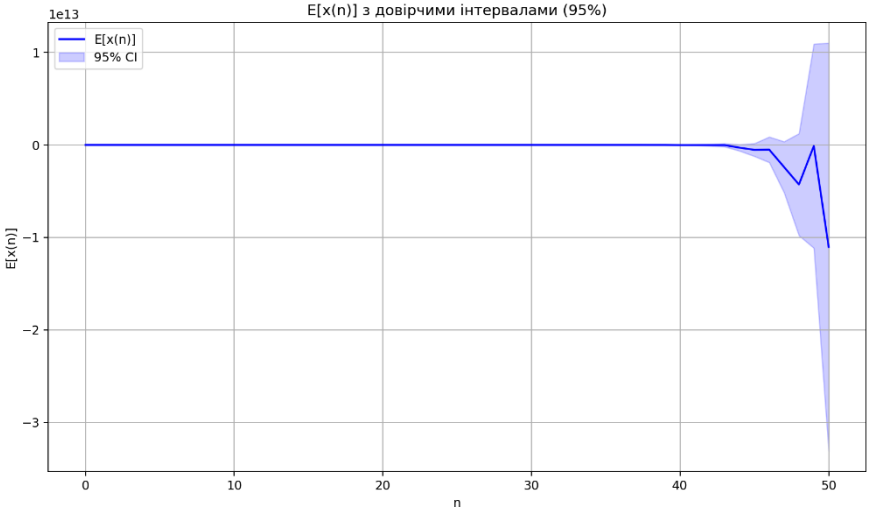

Рис. 3. Середнє значення з довірчими інтервалами

Джерело: розроблено автором

n	E[x(n)]	Var[x(n)]	CV[x(n)]	CI_lower	CI_upper
0	1.0000	0.0000	0.0000	1.0000	1.0000
1	1.2248	2.5001	1.2910	1.1938	1.2558
2	2.2896	10.7588	1.4326	2.2253	2.3539
3	2.9104	55.5351	2.5605	2.7643	3.0565
4	4.9856	231.1669	3.0496	4.6876	5.2836
5	6.4000	983.1383	4.8992	5.7854	7.0146
6	11.2128	3970.6702	5.6198	9.9777	12.4479
7	15.1552	16155.9355	8.3870	12.6639	17.6465
8	28.0064	64758.1174	9.0864	23.0187	32.9941
9	41.6768	260433.0877	12.2449	31.6744	51.6792
10	75.5712	1042969.2907	13.5139	55.5545	95.5879
11	69.2224	4189931.2525	29.5704	29.1025	109.3423
12	118.7840	16764782.8396	34.4700	38.5322	199.0358
13	127.7952	67099242.3111	64.0980	-32.7565	288.3469
14	252.3136	268398633.7106	64.9306	-68.7908	573.4180
15	910.9504	1073019295.2982	35.9591	268.9137	1552.9871

Рис. 4. Дані для кожного n: середнє $E[x(n)]$, дисперсія, коефіцієнт варіації, нижня/верхня межа 95 % довірчого інтервалу

Джерело: розроблено автором

В побудові експериментальної моделі використовувались основні статистичні характеристики: дисперсія даних, варіаційність та довірчі інтервали. Отриманий результат імітаційного моделювання дає змогу запропонувати його інтеграцію до чинних систем аналізу загроз, у випадку невизначеності середовища.

В наступних дослідженнях автори планують застосовувати дані в реальному часі. Окрім цього, перспективними напрямками майбутніх розвідок є:

— інтеграція моделей з наборами актуальних даних щодо кіберінцидентів, що відкриє можливість автоматичного навчання моделей на основі історичної інформації з ІТ-інфраструктури організації;

— удосконалення авторського підходу до оцінювання кіберзагроз в середовищах з більш невизначеною структурою, вхідними даними, часовими внтервалами виявлення атак тощо.

Синтез емпіричних та аналітичних методів, застосування теорії випадкових процесів, смарт-аналітики та Python-бібліотек дає змогу отримувати сучасні інструменти для підтримання стабільності кіберпростору.

Бібліографічні посилання

1. Горгуленко В. А. Математична модель визначення ймовірнісних станів інформаційно-комунікаційної системи в умовах ведення кібероборотьби. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2025. Т. 52, № 1. С. 77–84.

2. Адамов О. С. Моделі і методи захисту кіберпростору на основі аналізу великих даних з використанням машинного навчання : дис. … д-ра техн. наук : 05.13.05 / Харківський національний університет радіоелектроніки. Харків, 2019. 359 с.

3. Дьогтєва І. О., Шиян А. А. Моделювання роботи групи реагування на інциденти інформаційної безпеки в умовах зростання інтенсивності кібератак. *Вісник ВПІ*. 2021. Вип. 6. С. 123–130.

4. Приходько Ю. Є. Гранична поведінка локальних збурень процесів Маркова : дис. … канд. фіз.-мат. наук : 01.01.05 / Інститут математики НАН України ;Національний технічний університет України "КПІ імені Ігоря Сікорського". Київ, 2018. 213 с.

5. Sánchez-García I. D., Mejía J., San Feliu Gilabert T. Cybersecurity Risk Assessment: A Systematic Mapping Review, Proposal, and Validation. *Applied Sciences.* 2023. Vol. 13, No. 1. P. 395. URL: https://doi.org/10.3390/app13010395. (Last accessed: 04.07.2025)

6. Aissa A. B., Abdalla I., Hussein L., Elhadad A. “A novel stochastic model for cybersecurity metric inspired by Markov chain model and attack graphs,” *Int. J. Sci. Technol. Res*., 2020, vol. 9, no. 3, P. 6329-6335.

7. Sahay R., Sepulveda Estay D. A., Meng W., Jensen C. D., Barfod M. B. A Comparative Risk Analysis on CyberShip System with STPA-Sec, STRIDE and CORAS. *Computers & Security.* 2023, V. 128, URL: https://doi.org/10.1016/j.cose.2023.103179 (Last accessed: 04.07.2025)

8. Angelelli M., Arima S., Catalano C., Ciavolino E. A robust statistical framework for cyber-vulnerability prioritisation under partial information in threat intelligence. *Expert Systems with Applications.* 2024. Vol. 255. Article No. 124572. URL: https://doi.org/10.1016/j.eswa.2024.124572. (Last accessed: 04.07.2025)

9. Dzhalladova I., Kaminskyi O., Bartash O. AI and LLM Models to Analyze and Identify Cybersecurity Incidents. *Papers of the XX International Scientific Conference «Dynamical System Modeling and Stability Investigation» (DSMSI-2023).* Vol. 2. CEUR Workshop Proceedings, Vol. 3746. 2023. P. 115–123.

10. Джалладова І. А. Системний аналіз загроз соціокібернетичної безпеки в умовах пандемії. *Моделювання та інформаційні системи в економіці.* 2020. Вип. 100. С. 50–58.

11. Dzhalladova I., Ruzickova M., Diblík J. Dynamical system with Markov parameters for modelling system security of threats in cyberspace. *AIP Conference Proceedings.* 2019. Vol. 2116. Article No. 310003. URL: https://doi.org/10.1063/1.5114310 (Last accessed: 04.07.2025)

12. Камінський О. Є., Деменко І. Аналіз впливу автоматизованого тестування на якість та безпеку ПЗ. *Моделювання та інформаційні системи в економіці.* 2023. № 103. С. 91–103.

13. Джалладова І. А., Камінський О.Є. Програмний код для оцінки ризику кіберзагроз. GitHub, 2025. URL: https://github.com/olkam2022/article_2025/tree/main/prog_code (дата звернення: 04.07.2025).

14. Dzhalladova I., Ruzickova M. Dynamical system with random structure and their applications. Cambridge: Cambridge Scientific Publishers, 2020. 224 p. ISBN 978-1-908106-66-7.