РОЗДІЛ ІІІ. КОМП'ЮТЕРНІ НАУКИ

УДК 004.056
DOI https://doi.org/10.26661/2786-6254-2025-1-11

МАТЕМАТИЧНА МОДЕЛЬ ОЦІНКИ РИЗИКІВ КІБЕРБЕЗПЕКИ У РАЗІ ВІДСУТНОСТІ ФІНАНСОВИХ ДАНИХ ПРО ВТРАТИ

Байдур О. В.
аспірант
Національний університет біоресурсів і природокористування України
вул. Героїв Оборони, 15, Київ, Україна
orcid.org/0000-0001-7036-1264
alexvb1981@gmail.com

Ключові слова: *інформаційно-комунікаційні системи військового призначення, кібербезпека, метод Монте-Карло, оцінка ризиків, час неготовності системи, кібератаки.*

У статті розглянуто особливості оцінки ризиків кібербезпеки в інформаційно-комунікаційних системах військового призначення (ІКС ВП) в умовах війни, коли неможливо оцінити потенційні фінансові втрати від кібератак. Запропоновано математичну модель оцінки ризиків кібербезпеки в ІКС ВП, яка базується на методі Монте-Карло та враховує специфіку ІКС ВП, таку як особливості комбінованих атак з використанням конвекційної та кіберзброї в умовах гібридної війни, та неможливість оцінити потенційні фінансові втрати внаслідок успішних кібератак. Розроблено математичний апарат для оцінки частоти подій втрат та часу неготовності ІКС ВП внаслідок кібератак, що дозволяє врахувати невизначеність в оцінках та випадковий характер кібератак. У статті проведено детальний огляд наявних кількісних методів оцінки ризиків кібербезпеки, таких як метод Баєсових мереж, аналіз дерева атак, кількісна оцінка ризиків (QRA) та метод Монте-Карло. Показано, що метод Монте-Карло має низку переваг у контексті оцінки ризиків в ІКС ВП, таких як гнучкість, можливість врахування невизначеності, та здатність адаптуватися до динамічних змін у ландшафті загроз. Проведено аналіз можливості використання різних видів статистичних розподілів у процесі моделювання методом Монте-Карло і наведено типові сценарії їх застосування під час проведення оцінки ризиків кібербезпеки з урахуванням їх недоліків і переваг. Наведено приклади застосування розробленої моделі для різних сценаріїв кібератак на ІКС ВП, включаючи DDoS-атаки, фішингові атаки, атаки програм-вимагачів та APT-атаки. Запропонований підхід може бути використаний для прийняття рішень щодо розподілу ресурсів на кіберзахист ІКС ВП в умовах війни. Подальші дослідження дозволять автоматизувати оцінку ризиків в ІКС ВП, що дозволить здійснювати моделювання загроз у реальному часі і швидко розробляти пакети контрзаходів, які значно підвищать стійкість ІКС ВП в умовах ведення агресивної війни в кіберпросторі.

MATHEMATICAL MODEL FOR CYBERSECURITY RISK ASSESSMENT IN THE ABSENCE OF FINANCIAL DATA ON LOSSES

Baidur O. V.
Postgraduate Student
National University of Life and Environmental Sciences of Ukraine
Heroiv Oborony str., 15, Kyiv, Ukraine
orcid.org/0000-0001-7036-1264
alexvb1981@gmail.com

Key words: *military information and communication systems, cybersecurity, Monte Carlo method, risk assessment, system downtime, cyberattacks.*

This article examines the specifics of cybersecurity risk assessment in military information and communication systems (MICS) in wartime conditions, where it is impossible to assess potential financial losses from cyberattacks. A mathematical model for cybersecurity risk assessment in MICS is proposed, based on the Monte Carlo method and considering the specifics of MICS, such as the peculiarities of combined attacks using conventional and cyber weapons in hybrid warfare, and the impossibility of assessing potential financial losses resulting from successful cyberattacks. A mathematical apparatus has been developed to assess the frequency of loss events and system downtime of MICS due to cyberattacks, which allows accounting for uncertainty in estimates and the random nature of cyberattacks. The article provides a detailed review of existing quantitative methods for cybersecurity risk assessment, such as the Bayesian network method, attack tree analysis, quantitative risk assessment (QRA), and the Monte Carlo method. It is shown that the Monte Carlo method has several advantages in the context of risk assessment in MICS, such as flexibility, the ability to account for uncertainty, and the ability to adapt to dynamic changes in the threat landscape. An analysis of the possibility of using various types of statistical distributions in the Monte Carlo simulation process is conducted, and typical scenarios for their application during cybersecurity risk assessment are presented, considering their advantages and disadvantages. Examples of applying the developed model to various scenarios of cyberattacks on MICS are provided, including DDoS attacks, phishing attacks, ransomware attacks, and APT attacks. The proposed approach can be used to make decisions regarding the allocation of resources for the cybersecurity of MICS in wartime. Further research will allow automating risk assessment in MICS, which will enable real-time threat modeling and rapid development of countermeasures, which will significantly increase the resilience of MICS in the context of aggressive warfare in cyberspace.

Вступ. Безперервні та багатовекторні кібератаки, що здійснюються з 2022 року російською федерацією на інформаційно-комунікаційні системи військового призначення (ІКС ВП) України, змушують переглядати усталені підходи до оцінки ризиків кібербезпеки, актуальні для мирного часу. Як було зазначено в [1; 2], якісні методології оцінки ризиків кібербезпеки, що спираються на суто експертну оцінку, не можуть бути повноцінно застосовані у разі оцінки ризиків ІКС ВП України у зв'язку з унікальністю поточної ситуації та відсутністю відповідного досвіду у експертів. Насамперед ситуацію вирізняють майже щоденні спроби вмотивованих російською федерацією кіберзлочинців здійснити вплив на ІКС ВП України, що дозволило накопичити дані щодо розподілу зусиль та частоти дій кіберзлочинців у статистично значущих кількостях. Також протидія такій високій інтенсивності кібератак потребує швидкої адаптації захисту системи до змін ландшафту у кіберпросторі, що своєю чергою створює запит на перегляд ризиків кібербезпеки буквально у режимі реального часу. Все це створює сприятливі умови для застосування саме кількісних методологій і відповідних методів математичної статистики під час оцінки ризиків кібербезпеки ІКС ВП. При цьому слід врахувати, що в умовах ведення війни і інтеграції кібератак у загальну військову стратегію неможливо правильно оцінити потенційний негативний економічний ефект від кібератаки ворога, що досягне часткового або повного успіху. У попередньо проведеному огляді сучасних методологій оцінки ризиків кібербезпеки [2] було виявлено, що попу-

лярні кількісні методології не дозволяють задовільнити потреби в оцінці ризиків кібербезпеки ІКС ВП в умовах ведення бойових дій. У цих умовах недоліком розглянутих кількісних методологій є те, що вони орієнтовані на оцінку негативного економічного ефекту внаслідок успішної кібератаки з метою підтримки прийняття рішення щодо розподілу наявного фінансового ресурсу на організацію ефективного кіберзахисту системи. Тому постає завдання адаптувати математичний апарат методики оцінки ризиків кібербезпеки в ІКС ВП таким чином, щоб чинником, який впиває на прийняття рішення з розподілу фінансового ресурсу на організацію кіберзахисту системи, були не потенційний негативний економічний ефект, а інший показник, наприклад, потенційний час неготовності системи, як це було запропоновано у згаданому огляді. Проведений огляд також дозволив описати алгоритм оцінки ризиків кібербезпеки в ІКС ВП (скорочено АОРІКС-В), що задовольняє озвученим вище вимогам, і тепер постає завдання на основі цього алгоритму сформувати відповідний математичний апарат.

Аналіз останніх досліджень і публікацій. Останні огляди методів оцінки ризиків кібербезпеки [3; 4; 5] виділяють чотири основних підходи до створення математичних моделей, до яких можна віднести використання методів на основі Баєсових мереж [6], аналізу дерева атак [7], Кількісної оцінки ризиків (QRA) [8] та Монте-Карло [9]. Вибір конкретного методу залежить від основного завдання оцінки ризиків та залежить від кінцевої мети, що має бути досягнута в результаті проведеного аналізу. Стаття [6] присвячена огляду методу аналізу на основі Байєсових мереж, автори методу акцентують увагу на порівнянні з методом Монте-Карло, що пропонується в методології FAIR [10], і вони доходять висновку, що створена ними модель з використанням Баєсових мереж видає результати, подібні до використання методу Монте-Карло у загальних випадках, однак методика на основі Баєсових мереж досягає вищої точності у випадках, коли розподіли мають довгий хвіст або коли частота події втрат та величина втрат мають розподіли, відмінні від трикутних, які використовуються в традиційній моделі FAIR. Наприклад, частота події втрат може слідувати логнормальному розподілу або розподілу Вейбулла, а величина втрат може слідувати гамма-розподілу. Огляд методів аналізу дерева атак [7] розкриває основні переваги цього методу, до яких можна віднести насамперед їх наочність, позаяк вони дають чітке візуальне уявлення про потенційні загрози та їх взаємозв'язки та можливість визначити найбільш критичні загрози і зосередити ресурси на їх усуненні. При цьому слід відзначити, що дерева атак можуть бути суб'єктивними та залежати від знань та досвіду експертів, неефективними для аналізу складних систем з великою кількістю взаємопов'язаних компонентів і не враховувати динамічних змін у загрозах та вразливостях. Описаний у роботі [8] метод кількісної оцінки ризиків (QRA) використовує аналіз сценаріїв ризику для визначення ймовірності та впливу небажаних подій. При цьому QRA враховує широкий спектр факторів, включаючи загрози, вразливості та вплив та надає структурований процес для оцінки ризиків, що забезпечує послідовність та повноту. Головними недоліками QRA є суб'єктивність, яка пов'язана з тим, що метод спирається на експертні судження та його обмеженість доступністю даних, особливо для нових або незвичайних загроз. Популярна методологія FAIR [10], яка є основою деяких стандартів оцінки ризиків кібербезпеки [11], як математичний інструмент використовує метод Монте-Карло, який має здатність обробляти складні системи і залежності та дає можливість враховувати невизначеність та випадковість, але при цьому потребує великої кількості даних для точних результатів і може бути складним у реалізації та інтерпретації.

Мета статті – розробка математичного апарату оцінки ризиків кібербезпеки в інформаційно-комунікаційних системах військового призначення з послідовністю кроків, описаною в алгоритмі оцінки ризиків кібербезпеки в ІКС ВП [2]. При цьому має бути враховано специфіку ІКС ВП, особливості гібридної війни, неможливість оцінити потенційні фінансові втрати внаслідок успішних кібератак.

Вибір методу оцінки ризиків в ІКС ВП. Обґрунтування вибору методу почнемо з проведення порівняльного аналізу перерахованих вище чотирьох методів кількісної оцінки ризиків кібербезпеки, а саме методів Баєсових мереж, аналізу дерева атак, кількісної оцінки ризиків (QRA) та Монте-Карло в контексті їх потенційного застосування під час оцінки ризиків в ІКС ВП.

Перший метод для розгляду метод Баєсових мереж. Автори роботи [6] розглядають його як послідовність дій, яка описана в методології FAIR. Вони зазначають, що оцінка ризику за допомогою моделі FAIR включає дві процедури, що потребують застосування апарату математичної статистики, це оцінка частоти подій втрат та агрегування величин втрат з використанням оцінених частот для обчислення загального збитку [6]. На першому кроці процедури оцінки частоти подій втрат у цій роботі пропонується здійснити розбудову Баєсової мережі, яка є орієнтованим ациклічним графом та являє собою факторизацію спільного розподілу ймовірностей і складається з вузлів (представляють змінні) та дуг (представ-

ляють причинно-наслідкові ймовірнісні зв'язки з ймовірнісними вагами, змодельованими за допомогою статистичних детермінованих функцій). У Баєсовій мережі кожен вузол має пов'язану таблицю ймовірностей $P\left(X_i \vee pa\left(X_i\right)\right)$, яка називається таблицею умовної ймовірності змінних X_i з урахуванням його батьківських змінних $pa\left(X_i\right)$ та визначає ймовірність кожного стану вузла за умови всіх можливих комбінацій станів його батьківських вузлів [13]. При цьому для кожного вузла X_i без батьків таблиця являє собою граничний розподіл ймовірностей $X_i, P\left(X_i\right)$. Якщо умовно зважити зв'язок між змінними незалежними у Баєсовій мережі, то слабкі зв'язки можна представити відсутністю дуг та значно спростити спільний розподіл ймовірностей, представивши його за допомогою добутку. Крім того, можна отримати граничний розподіл дочірньої змінної шляхом маргіналізації її батьківських змінних у спільному розподілі. Ці припущення дозволили авторам роботи [6] вивести таку формулу об'єднаного розподілу в Баєсовій мережі:

$$P\left(X_1, ..., X_n\right) = \prod_{i=1}^{n} P\left(X_i \vee pa\left(X_i\right)\right), \qquad (1)$$

де $P\left(X_i\right)$ – граничний розподіл ймовірностей, n – будь-яке число від 0 до верхньої межі N, а $P\left(X_i \vee pa\left(X_i\right)\right)$ – таблиця умовної ймовірності змінних X_i з урахуванням його батьківських змінних $pa\left(X_i\right)$.

При цьому розрахунок розподілу втрат L_P відбувається за припущення, що за певний період подія втрат може статися n разів, де n – будь-яке число від 0 до верхньої межі N, ця подія має фіксований розподіл величини втрат LM_p. За цих припущень основний розподіл можна обчислити за допомогою n-кратної згортки:

$$L_p = P(0)\, LP_0 + P(1)\, LP_1 + ... + P(N)\, LP_n, \qquad (2)$$

де LP_n – n-кратний розподіл величини втрат LM_p, $LP_0 = 0, a\, LP_n = LP_{n-1} + LM_p$ для n від 1 до N та $P(n)$, що є ймовірністю для частоти події втрат $F_p = n$.

Такий підхід дозволяє гнучко використовувати різні розподіли для описання подій втрат і підбирати з них той, що найкраще описує реальний стан речей.

Загальні втрати L_T описуються шляхом агрегування ризиків та їх агрегованої частоти:

$$L_T = RA_2\left(F_{p\cup s}, LM_p, LM_s\right), \qquad (3)$$

де $F_{p\cup s}$ – агрегована частота втрат, а LM_p та LM_s – величини втрат.

Автори роботи [6] пропонують спростити цю залежність до формули n-кратної згортки:

$$L_T = \sum_{n=0}^{N}\left[\sum_{m=0}^{n} P\left(F_p, F_s\right) \times \left(LP_n + LS_m\right)\right], \qquad (4)$$

де LP_n – n-кратний розподіл величини втрат LM_p, $LP_0 = 0, a\, LP_n = LP_{n-1} + LM_p$ для n від 1 до N та $P(n)$, що є ймовірністю для частоти події втрат $F_p = n$, LS_n – n-кратний розподіл величини втрат LM_s, де $LS_0 = 0, a\, LS_m = LS_{m-1} + LM_s$ для m від 1 до n та $P(n)$, а функція $P\left(F_p, F_s\right)$ є об'єднаною частотою втрат для подій n та m з ймовірністю $F_p = n$ та $F_s = m$.

Загальний вигляд Баєсової мережі для агрегації ризиків представлений на рис. 1 [6]. Наведені Баєсові мережі моделюють статичні зв'язки між подіями, при цьому адаптацію моделі пропонується проводити шляхом розширення та/або заміни вузлів у побудовані мережі, щоб забезпечити більшу гнучкість.

Підсумовуючи сказане по методу Баєсових мереж, слід зазначити, що в контексті завдання оцінки ризиків в ІКС ВП переваги методу пов'язані із можливістю використання різних розподілів для описання частоти подій втрат і нівелюються статичністю зв'язків у побудованій моделі, де адаптація під нові виявлені залежності вимагає зусиль експертів – людей, пов'язаних із перебудовою Баєсової мережі та її адаптацією. Ці зусилля значно ускладнюють використання моделі, що в умовах високої інтенсивності кібератак на ІКС-ВП може призвести до необґрунтованого навантаження на залучених експертів, яке пов'язане із необхідністю постійної адаптації моделі.

Наступний метод, а саме метод аналізу дерева атак, детально описаний у роботі [7]. Цей метод передбачає створення деревоподібної структури, яка відображає можливі шляхи атаки на систему. Послідовність дій сторони, що атакує, описується за допомогою ланцюга знищення, розробленого компанією Lockheed Matrin [12]. Кількісні показники оцінюються за допомогою матриці оцінки ризиків – візуального інструменту, який відображає потенційні ризики, що впливають на систему (таблиця 1).

Матриця оцінки ризику визначає ризик на основі двох пересічних елементів: ймовірності того, що подія ризику (атака) відбудеться, і потенційної тяжкості шкоди, яку подія ризику завдає системі. Залежно від імовірності атаки та тяжкості атаки ризик атаки можна класифікувати як низький, середній і високий, як це показано у Таблиці 1, або на більш детальному рівні залежно від вимог конкретного аналізу ризику. У цій дослідницькій роботі використовують матрицю оцінки ризику та таке рівняння:

$$\text{Ризик} = \text{Ймовірність} \times \text{Ступінь}, \qquad (5)$$

де отриманий Ризик може бути низький, середній або високий, Ступінь атаки – низький, середній та високий, а Ймовірність відповідно – низька, середня та висока.

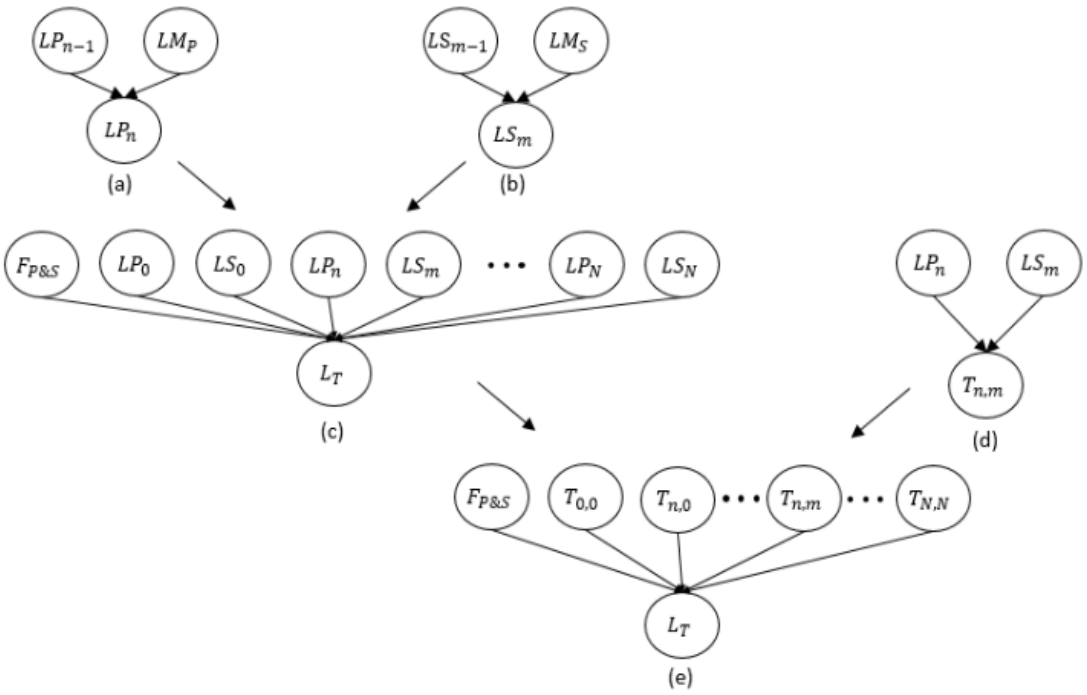

Рис. 1 Баєсова мережа, що ілюструє процес агрегації ризиків

Таблиця 1

Матриця оцінки ризику

Ступінь атаки	Ймовірність атаки		
	Низька	Середня	Висока
Високий	Ризик середній	Ризик високий	Ризик високий
Середній	Ризик низький	Ризик середній	Ризик високий
Низький	Ризик низький	Ризик низький	Ризик середній

Авторами роботи [7] пропонується проведення аналізу побудованого дерева атак здійснювати таким чином, щоб акцентувати увагу на тих елементах, які мають найбільш високі ризики. Цей метод має такі переваги, як наочність, простота використання, яка допомагає визначити критичні точки вразливості, але в контексті завдання оцінки ризиків в ІКС ВП ключовим недоліком цього методу є те, що ця модель не враховує всі можливі фактори та повністю залежить від досвіду і компетентності запрошених експертів. Використання розглянутої моделі явно не дозволяє враховувати накопичені статистичні дані щодо кібератак.

Метод кількісної оцінки ризиків (QRA) представлений у вигляді документа NATO Sciences and Technology Organization MP-IST-166 [8], що детально описує відповідну процедуру. Оцінки ризиків відбуваються за допомогою матриці QRA (таблиця 2). Ризик, пов'язаний з небажаною подією, є наслідком серйозності події та ймовірності її виникнення, при цьому матриця QRA створена на основі військового стандарту США, розробленого в Лос-Аламоській Національній лабораторії, U.S.MIL-STD 882e [13], та використовується для розрахунку рейтингу ризику зваженим способом. Категорії серйозності небажаних подій представлені в таблиці 2 та категорії ймовірності небажаної події представлені в таблиці 3 разом із матрицею оцінки ризиків (таблиця 4) є стандартизованим рейтингом, який характеризує систему оцінки ризику у форматі, який вимагає певних управлінських дій для контролю ризику (представлений рівнями 1–4 у таблиці 4).

Стандарт передбачає різні варіанти управлінських дій для деяких випадків, коли ймовірність виникнення не буде оцінюватися як часта, а потенційна серйозність небажаних подій вимагає вжиття дій для мінімізації ризику. Наведені в матриці оцінки ризику значення можуть бути використані під час прийняття рішення щодо того, чи слід усунути чи контролювати окремі вразливі місця, щоб зменшити виникнення конкретної небажаної події, чи слід прийняти пов'язаний із цим ризик. Наприклад, якщо небажаній події «втрата критично важливої секретної інформації» було присвоєно категорію ризику захисту та безпеки (SSRC) IC (найвищий рівень серйозності, випадкова ймовірність) та індекс ризику та безпеки (SSRI) 1, що вимагає управління дії для зниження ризику до наступного нижчого рівня.

Таблиця 2

Категорії серйозності небажаних подій

Рівень	Характеристики ступеня
I	Втрата життя, втрата важливої конфіденційної інформації, втрата критичних активів, значне погіршення місії, втрата системи.
II	Тяжкі травми працівника або іншої особи, втрата конфіденційної інформації та фізичного обладнання, що є результатом непоміченого доступу, неприйнятних затримок місії, неприйнятного збою системи та операцій.
III	Незначна травма, яка не вимагає госпіталізації, невиявлене або невчасно виявлене несанкціоноване проникнення, що призвело до обмеженого доступу до активів або конфіденційних матеріалів, відсутність погіршення завдання, незначний збій системи та зрив операцій.
IV	Менше ніж незначне ушкодження, невиявлене або невчасно виявлене несанкціоноване проникнення без втрати активів або доступу до конфіденційних матеріалів, без збоїв у системі чи роботі.

Таблиця 3

Категорії ймовірності небажаної події

Категорія ймовірності	Рівень	Опис події
A	Часто	Можливість повторення інцидентів
B	Можливо	Можливість ізольованих інцидентів
C	Випадково	Можливість трапитися коли-небудь
D	Рідкісний	Можливо ніколи не відбудеться
E	Неймовірний	Практично неможлива

Тому, припускаючи правильну оцінку, необхідно вжити заходів для усунення або контролю ризику, пов'язаного з цією подією. Інші ризики, які підпадають під цю категорію, представлені в IA, IB, IC, IIA, IIB і IIIA. Часто слід також вживати заходів для мінімізації ризику небажаних подій із значеннями SSRC2. Ризики цієї категорії включають ID, IIC, IID, IIIB та IIIC. Такі ризики вимагають коригувальних дій, хоча передбачається певний розсуд керівництва [8].

Розглянутий метод кількісної оцінки ризиків (QRA) схожий на метод аналізу дерева атак з використанням матриці оцінки ризиків для визначення ступеня ризику. Матриця має більшу деталізацію і явно передбачені управлінські дії для кожного рівня ризику, але в контексті завдання оцінки ризиків в ІКС ВП недоліки методу ті самі, що і для попереднього методу. Цей метод не дає можливості використати накопичені статистичні дані щодо кібератак і повністю залежить від досвіду і компетентності залучених для оцінки експертів.

Метод Монте-Карло для оцінки ризиків кібербезпеки використовує статистичні дані та ймовірнісні розподіли для розрахунку ймовірності та величини втрат, що дозволяє за допомогою математичного апарату порівнювати різні сценарії і створювати прогнози втрат, при цьому підбираючи оптимальну стратегію протидії [9]. Головною перевагою методу є здатність обробляти складні системи та враховувати невизначеність. При цьому математичний апарат методу дозволяє покращувати результати прогнозів із накопиченням реальних даних щодо атак, що є критично важливим у контексті поставленого завдання. Недоліком методу Монте-Карло можна назвати високі вимоги до обчислювальних ресурсів, а також складність інтерпретації результатів.

На тлі розглянутих методів Баєсових мереж, аналізу дерева атак та кількісної оцінки ризиків використання методу Монте-Карло можна вважати найбільш доцільним у контексті поставленого в цій роботі завдання оцінки ризиків в ІКС ВП. Так методи аналізу дерева атак та кількісної оцінки ризиків не дозволяють задіяти накопичені статистичні дані та орієнтовані на експертну оцінку, що робить їх дуже залежними від суб'єктивної думки експертів, а з огляду на безпрецедентний масштаб агресії російської федерації в кіберпросторі, спрямований проти ІКС ВП України, така залежність методів від експертних оцінок не дозволяє ефективно їх застосувати в умовах, що розглядаються. Головним недоліком методу Баєсових мереж є необхідність перебудовувати мережу з отриманням нового досвіду кібератак, який не вкладається в побудовану раніше модель. Як показує досвід протидії кібератакам рф з 2022 року, такі події трапляються доволі часто (до декількох разів на рік), враховуючи трудомісткість процесу перебудови Баєсової мережі,

Таблиця 4

Матриця оцінки ризику (SSRC)

Категорії серйозності	Категорії ймовірності				
	(A) Часто	(B) Можливо	(C) Випадково	(D) Рідкісний	(E) Неймо-вірний
I	I A	I B	I C	I D	I E
II	II A	II B	II C	II D	II E
III	III A	III B	III C	III D	III E
IV	IV A	IV B	IV C	IV D	IV E

це нівелює переваги методу, пов'язані із кращим прогнозуванням за деяких специфічних видів розподілу вхідних даних. Математичний апарат методу Монте-Карло буде розглянуто в наступних розділах у процесі адаптації методу під потреби завдання оцінки ризиків в ІКС ВП на базі вже розробленого алгоритму оцінки ризиків кібербезпеки АОРІКС-В [2].

Методика дослідження. Методологічною основою цього дослідження є системний підхід до аналізу проблем кібербезпеки, що дозволяє розглядати ІКС ВП як складні об'єкти, що функціонують в умовах гібридної війни із широкомасштабним застосуванням противником засобів кібервпливу в умови високої інтенсивності таких дій. Для досягнення поставленої мети були використані аналіз літературних джерел та нормативних документів з питань кібербезпеки, оцінки ризиків та управління інформаційною безпекою, включаючи стандарти ISO/IEC 27000, NIST, MP-IST-166 та інші, порівняльний аналіз наявних методів кількісної оцінки ризиків кібербезпеки, таких як методи Баєсових мереж, аналізу дерева атак, кількісної оцінки ризиків (QRA) та Монте-Карло, з метою виявлення їхніх переваг та недоліків у контексті оцінки ризиків кібербезпеки у системах військового призначення, математичне моделювання процесів оцінки ризиків за методів математичної статистики. За результатом застосування вказаних методів була здійснена математична модель оцінки ризиків кібербезпеки, адаптована до специфіки інформаційно-комунікаційних систем військового призначення та реалій гібридної війни з деталізацією кроків цього алгоритму.

Застосування згаданих методів дослідження дозволило провести комплексний розгляд проблеми оцінки ризиків кібербезпеки в умовах гібридної війни та запропонувати новий комплексний підхід із застосуванням методів математичної статистики в комбінації із проведенням експертних оцінок, що дозволяє повною мірою врахувати специфіку військових інформаційно-комунікаційних систем у контексті неможливості використання традиційного підходу з оцінкою потенційних фінансових втрат. Запропонований метод оцінки ризиків може стати основою застосування ефективних стратегій кіберзахисту та підвищення кіберстійкості інформаційно-комунікаційних систем військового призначення.

Математична модель оцінки ризиків кібербезпеки в ІКС ВП. У роботі [2] був описаний перспективний алгоритм оцінки ризиків кібербезпеки в ІКС ВП (АОРІКС-В), зображений на рис. 2, що відповідає вимогам оцінки ризиків в умовах ведення агресивної війни та чинним в Україні державним стандартам. Наступним кроком, що дозволяє підійти до вирішення завдання з оцінки ризиків кібербезпеки в ІКС ВП, є розробка мате-

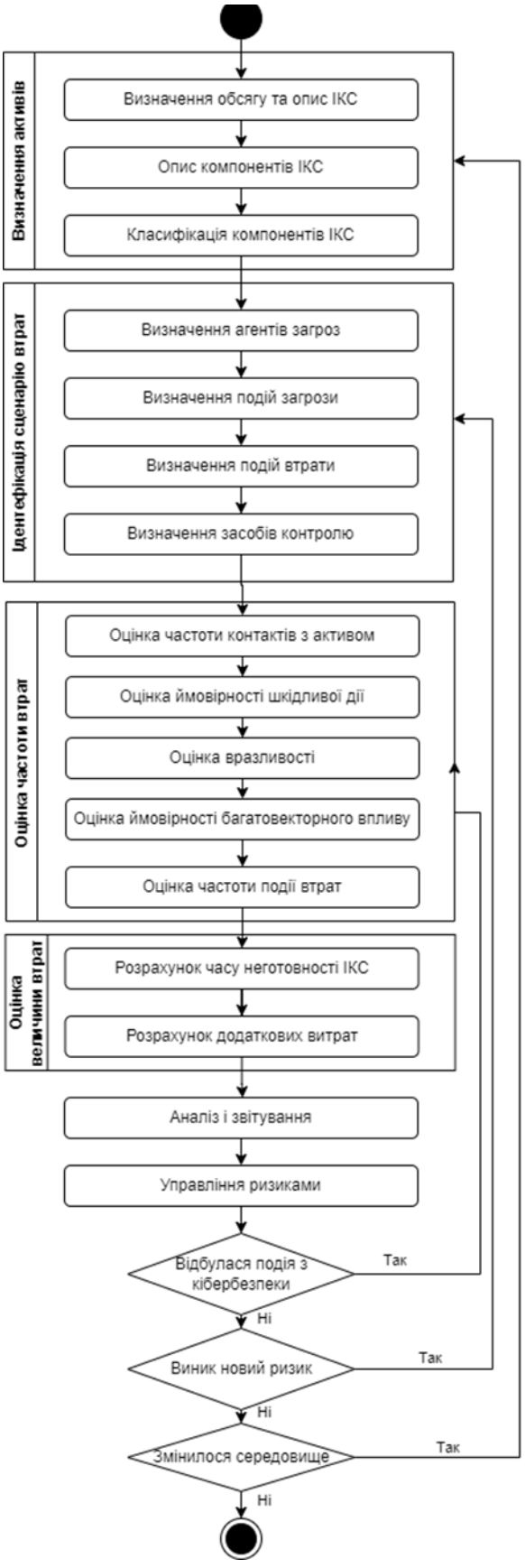

Рис. 2. Алгоритм АОРІКС-В

матичної моделі, яка має бути використана у разі виконання кроків, передбачених зазначеним алгоритмом. Але, на відміну від описаного в популярних кількісних методологіях підходу, де оцінка ймовірних втрат здійснюється з використанням фінансових показників, розроблена математична модель буде використовувати оцінку потенційного часу неготовності системи, як показника більш прийнятного для систем військового призначення, де неможливо здійснити оцінку потенційних втрат, виражену у фінансовому еквіваленті. При цьому передбачається проведення розрахунків вартості впровадження контрзаходів і порівняння потенційного часу неготовності системи, що дозволить особам, які приймають рішення, діяти в межах виділеного бюджету і здійснювати обґрунтування виділення фінансування, необхідного для розбудови кіберзахисту в ІКС ВП. В основі математичної моделі, яка пропонується для здійснення кроків оцінки ризиків в ІКС-ВП, передбачених алгоритмом АОРІКС-В, будемо застосовувати метод Монте-Карло [9]. Вибір цього методу зумовлений його гнучкістю, можливістю врахувати невизначеність під час здійснення оцінки та порівняною універсальністю, що вирізняє його від можливо більш точного, але прив'язного до статичної моделі здійснення кібератак методу Баєсових дерев.

Оцінка частоти подій втрат. Розглянемо, як можна використати метод Монте-Карло у контексті оцінки ризиків в ІКС ВП. Відповідно до діаграми діяльності алгоритму АОРІКС-В[2] (рисунок 2) першим кроком, який потребує використання математичних розрахунків, є «Оцінка частоти втрат». У результаті цього кроку має бути визначений числовий показник частоти подій втрат (ЧПВ). У методології OpenFAIR частота подій втрат (Loss Event Frequency) визначається як імовірнісна частота настання певної небажаної події протягом визначеного періоду часу [11]. При цьому ЧПВ не є фіксованим значенням, а оцінкою ймовірності того, як часто може відбуватися небажана подія. До небажаних подій відносять ті, які можуть призвести до втрат або збитків. Слід зазначити, що ЧПВ завжди прив'язана до певного періоду часу, наприклад, року, місяця або доби, та при цьому вона є ключовим фактором у кількісному аналізі ризиків, оскільки безпосередньо впливає на загальний рівень ризику. Чим вища ЧПВ, тим вищий ризик, пов'язаний з цією подією [11].

Залежно від виду активу, для якого відбувається оцінка ризику, оцінка ЧПВ може проводитися різними способами. Найпростіший варіант, а саме пряма оцінка, застосовується у разі якщо доступні історичні дані та/або ймовірнісні показники задані у вигляді характеристик активу. Використання прямої оцінки обмежено тим, що не враховує невизначеність, тому воно може бути застосовано тільки у разі, коли дані про ймовірність подій, пов'язаних із втратами, можна вважати сталими. Якщо наявні історичні дані про подію не дозволяють вважати її ймовірність сталою, то можна використати розподіл Бернулі (для разових подій), Біноміальний розподіл (для подій, що можливо описати за допомогою двох станів), Бета-розподіл або розподіл Пуасона (у разі коли важливо врахувати невизначеність).

У разі, коли оцінка проводиться для разового випадку втрат і відомою вірогідністю події, пов'язаної із цими втратами, доцільно використати розподіл Бернуллі [12] із параметром p настання події втрат A, якщо ймовірність настання цієї події протягом заданого інтервалу часу є P(A)=p, тоді дискретна випадкова величина ξ буде мати закон розподілу:

$$\xi = \begin{pmatrix} 0 & 1 \\ q & p \end{pmatrix}, \tag{5}$$

де p – ймовірність настання події втрат, p∈[0,1], а q=1-p.

Для випадку оцінки ЧПВ в ІКС ВП можна навести приклад подій втрат, пов'язаних із відмовою сервера, для якого вірогідність відмови є величиною, що може бути розрахованою із показників надійності, наданих виробником.

Більш складний випадок прямої оцінки ЧПВ для випадку незалежних подій із фіксованою кількістю спроб, які можна описати двома станами, такими як «подія відбулася» та «подія не відбулася». При цьому використовується біноміальний розподіл, де кількість спроб задана параметром n, а кількість «успіхів», коли подія відбулася, задана параметром k. Тоді дискретна випадкова величина ξ має біноміальний розподіл ймовірності P, що задається формулою:

$$P\left(\xi = k\right) = C_n^k p^k q^{n-k}, \tag{6}$$

де p – ймовірність настання окремої незалежної події, q=1-p, n – кількість спроб, а k – кількість успіхів.

Біноміальний розподіл у контексті оцінки ризиків кібербезпеки ІКС ВП можна використати, наприклад, для оцінки події втрат, пов'язаної з успішними фішинговими атаками. Будемо вважати ймовірність успіху атаки сталою величиною (припустимо це ймовірність того, що користувач у разі отримання фішингового повідомлення перейде за наданим у повідомленні посиланням), тоді за умови розсилки фішингових повідомлень усім зареєстрованим користувачам поштового сервісу (загальна кількість користувачів – це відома і стала величина) біноміальний розподіл дозволяє оцінити, скільки користувачів із загальної кількості отримувачів повідомлення перейдуть за наданим зловмисниками посиланням.

Велике практичне значення саме в контексті оцінки ризиків кібербезпеки в ІКС ВП грає бета-розподіл. У разі коли необхідно мати можливість зробити оцінку ЧПВ із спостереження кількості успіхів s у серії n випробувань можливо застосувати теорему Байєса, а розподіл імовірностей визначається бета-розподілом заданою для випадкової величини X густиною ймовірності f_X:

$$f_X(x) = \frac{1}{B(\alpha,\beta)} x^{\alpha-1}(1-x)^{\beta-1}, \qquad (7)$$

де α,β – фіксовані параметри, а бета-функція задана, як $B(\alpha,\beta) = \int x^{\alpha-1}(1-x)^{\beta-1}\,dx$.

Розглянемо приклад використання бета-розподілу в контексті оцінки ризиків кібербезпеки. Проведемо оцінку ризику витоку конфіденційних даних з інформаційної системи компанії. Припустимо для оцінки ймовірності успішної атаки використовуються експертні оцінки і думка експертів складається з найменш песимістичних оцінок x_{min}, найбільш ймовірних значень – x_μ та найбільш песимістичних оцінок – x_{max}. Визначити параметри α і β бета-розподілу можна за допомогою методу моментів. Для цього слід розрахувати середнє значення μ та дисперсію σ^2 на основі наведених експертних оцінок, тоді для розрахунку параметрів α і β можна використати формули:

$$\alpha = \mu\left(\frac{\mu(1-\mu)}{\sigma^2} - 1\right) \text{ та}$$

$$\beta = (1-\mu)\left(\frac{\mu(1-\mu)}{\sigma^2} - 1\right) \qquad (8)$$

де α і β – параметри бета розподілу, μ – середнє значення та σ-дисперсія.

Після розрахунку параметрів α і β можна згенерувати випадкові числа з бета-розподілу. Ці випадкові числа будуть представляти різні можливі значення ймовірності успішної атаки, що дозволяє врахувати невизначеність в експертних оцінках та в моделі ризиків під час симуляції Монте-Карло.

Для події втрат, що мають достатню велику кількість історичних даних під час розрахунку ЧПВ, зручно використовувати розподіл Пуассона. Відоме середнє значення кількості подій, що призвели до втрат за заданий період часу, позначається як параметр λ розподілу Пуассона, тоді оцінка кількості подій, що можуть відбутися, позначається як параметр k, а розподіл Пуассона ймовірності P буде мати вигляд:

$$P(X = k) = \frac{\lambda^k}{k!} e^{-\lambda}, \qquad (9)$$

де P – ймовірність, λ – параметр розподілу Пуассона, k – кількість подій, що можуть відбутися.

Властивість процесу Пуассона пов'язана з тим, що він не залежить від попередніх подій, що дозволяє значно спростити деякі розрахунки в процесі оцінки ризиків. Наприклад, якщо середня кількість подій відповідає передбачуваним місячним коливанням протягом року, а підрахунки протягом кожного місяця відповідають пуассонівським процесам, тоді загальна кількість подій за рік відповідатиме розподілу Пуассона із середнім рівним сумі середніх підрахунків за кожен місяць.

$$P(\lambda t) = P(\lambda t_1) + P(\lambda t_2) + \ldots + P(\lambda t_n), \qquad (10)$$

де P – ймовірність, λ – параметр розподілу Пуассона, а $t_1, t_1, \ldots, t_n$ – різні часові інтервали.

Для двох незалежних подій відмов А та В за умови їх оцінки за розподілом Пуассона загальна частота відмов буде дорівнювати:

$$P(A + B) = P(A) + P(B), \qquad (11)$$

де $P(A + B)$ – ймовірність настання події А або В, де P (А) та де $P(B)$ – ймовірність настання події А та В відповідно.

Розглянемо застосування розподілу Пуассона для оцінки ризиків кібербезпеки в ІКС ВП на прикладі оцінки ЧПВ недоступності онлайн-сервісу через DDoS-атаки. Припустимо, що DDoS-атаки відбуваються випадково та незалежно одна від одної, тоді середнє значення (λ) можна розрахувати як середню кількість атак на місяць, а розподіл Пуассона із параметром λ використати для моделювання кількості DDoS-атак на місяць. При цьому використання розподілу Пуассона дозволяє врахувати випадковий характер DDoS-атак та оцінити цей ризик для прийняття рішень щодо організації захисту онлайн-сервісу від подібних атак.

У випадках, коли розрахувати ЧПВ за допомогою прямої оцінки неможливо, розрахунок проводиться з декомпозицією цього показника. Можна доповнити вже наведений приклад фішингової розсилки листів елементом декомпозиції. Припустимо, що, окрім переходу за посиланням, у фішинговому листі є ще відмінна від одиниці ймовірність введення облікових даних у формі за цим посиланням, вважатимемо ці події незалежними тоді:

$$\text{ЧПВ} = \text{ЙВЛ} * \text{ЙВД}, \qquad (12)$$

де ЧПВ – частота подій втрат, ЙВЛ – ймовірність відкриття листа, ЙВД – ймовірність введення облікових даних.

Наведений приклад показує, що декомпозиція дозволяє врахувати різні фактори, що впливають на ЧПВ і здебільшого спрощує оцінку так, як оцінювати окремі компоненти ЧПВ може бути простіше.

Попередня формула була справедлива для випадків, коли події є незалежними, якщо між компонентами ЧПВ є залежності, то їх необхідно врахувати під час розрахунку. Однак під час проведення багатовекторних кібератак кожен наступний крок залежить від успіху виконання попереднього кроку. Для розгляду подібних атак доцільно використовувати декомпозицію ЧПВ

та симуляцію Монте-Карло. Розглянемо декілька прикладів пошуку ЧПВ для події, які не можна вважати незалежними.

Перший приклад декомпозиції – це випадок із підсумовування подій Бернуллі з розподілом Пуассона. До прикладу проаналізуємо ризик виходу з ладу серверів у компанії. Припустимо, що кожен сервер має певну ймовірність вийти з ладу протягом року. Це можна розглядати як подію Бернуллі, де «успіх» – це вихід сервера з ладу. Тоді кількість серверів, що виходять з ладу кожного року, може варіюватися. Варіативність виходу з ладу серверів моделюється за допомогою розподілу Пуассона із параметром λ, який буде описувати середню кількість серверів, що виходять з ладу щороку. Щоб оцінити загальний ризик, пов'язаний з виходом серверів з ладу, слід розрахувати, скільки серверів можуть вийти з ладу в найгіршому випадку. Використаємо для цього симуляцію Монте-Карло, підсумовуючи випадкову кількість подій Бернуллі (вихід кожного сервера з ладу) згідно з розподілом Пуассона. Для цього багаторазово (зазвичай десятки тисяч разів) генеруються випадкові числа із розподілу Пуассона з параметром λ та проведенням симуляції для кожного з цих серверів і підсумовуванням кількості серверів, що вийшли з ладу в цій симуляції, що дозволить знайти верхню оцінку кількості серверів, які можуть вийти з ладу протягом року.

Декомпозиція із підсумовуванням подій Бернуллі з розподілом Пуассона використовується у випадках, коли ЧПВ складається з багатьох незалежних подій з двома можливими результатами («успіх» та «невдача»), а кількість цих подій, що відбуваються, є випадковою величиною, яку можна змоделювати за допомогою розподілу Пуассона. Це може бути кількість хакерських атак на систему, які є успішними (кожна атака розглядається як подія Бернуллі, а загальна кількість атак підпорядкована розподілу Пуассона), або кількість співробітників, які відкривають фішинговий лист (дії кожного співробітника розглядаються як подія Бернуллі, а загальна кількість відкритих фішингових листів підпорядкована розподілу Пуассона).

Як другий приклад наведемо порядок оцінки ЧПВ для багатовекторної кібератаки на вебдодаток, використовуючи симуляцію Монте-Карло. Нехай сценарій кібератаки, для якої оцінюється ЧПВ, складається із фішингу, спрямованого на отримання облікових даних співробітників з доступом до адміністративної панелі вебдодатка, DDoS-атаки, спрямованої на перевантаження серверів вебдодатка та експлуатації вразливості в коді вебдодатка для отримання несанкціонованого доступу до даних. Для кожного вектора атаки визначимо вхідні змінні та їх розподіли ймовірностей.

Вектор 1 (фішинг) включає такі параметри: кількість надісланих фішингових листів (N_1) та розподіл Пуассона з λ_1, що показує середню кількість листів за місяць, в яких користувач переходить за надісланим посиланням, при цьому ймовірність відкриття листа (p_{11}) підпорядкована бета-розподілу з параметрами α_{11}, β_{11}, які знаходяться внаслідок проведення експертної оцінки, а ймовірність введення облікових даних (p_{12}) підпорядкована бета-розподілу з параметрами α_{12} та β_{12} (визначеними за допомогою експертної оцінки).

Вектор 2 (DDoS) включає параметри: кількість DDoS-атак (N_2) із розподілом Пуассона з λ_2 (що відповідає середній кількості атак на місяць) та ймовірність успішної атаки (p_2), що підпорядкована бета-розподілу з параметрами α_2, β_2 (які отримані внаслідок проведення експертної оцінки).

Вектор 3 (експлуатація вразливості) включає такі параметри, як частота спроб експлуатації вразливості (N_3), розподіл Пуассона з λ_3 (що відповідає середній кількості спроб на місяць) та ймовірність успішної експлуатації вразливості (p_3), підпорядковану бета-розподілу з α_3 та β_3, які отримані внаслідок проведення експертної оцінки.

Проведення симуляції Монте-Карло починається із генерації великої кількості (десятки тисяч) випадкових значень для кожної вхідної змінної згідно з їх розподілами. В кожній симуляції проводиться розрахунок кількості успішних атак для кожного вектора атаки. Оцінка кількості успішних атак по вектору 1:

$$N_{1усп} = B(N_1, p_{11} \cdot p_{12}), \tag{13}$$

де N_1 – кількість надісланих фішингових листів, p_{11} – ймовірність відкриття листа, а p_{12} – ймовірність введення облікових даних.

Оцінка кількісті успішних атак по вектору 2:

$$N_{2усп} = B(N_2, p_2), \tag{14}$$

де N_2 – кількість DDoS атак, p_2 – ймовірність успішної DDoS атаки.

Оцінка кількості успішних атак по вектору 3:

$$N_{3усп} = B(N_3, p_3), \tag{15}$$

де $B(N_3, p_3)$ – біноміальний розподіл з параметрами, N_3 – частота спроб експлуатації вразливості та p_3 – ймовірність успішної експлуатації вразливості.

Подія втрат вважається такою, що відбулася, якщо хоча б один з векторів атаки був успішним, а ЧПВ розраховується як відношення кількості ітерацій, в яких відбулася подія втрат, до загальної кількості ітерацій.

Показані приклади ілюструють переваги симуляції Монте-Карло в проведенні аналізу бага-

товекторних атак. Використання методу Монте-Карло дозволяє врахувати невизначеність в оцінках вхідних параметрів та складні залежності між векторами атак. При цьому можна легко змінювати вхідні параметри та розподіли для дослідження різних сценаріїв атак.

Підсумовуючи викладене щодо кроку алгоритму АОРІКС-В «Оцінка частоти втрат», можна сказати таке. Здебільшого виконання оцінки частоти втрат потребує декомпозиції цієї події з окремим аналізом для частоти контактів зловмисника з активом та оцінки ймовірності шкідливої дії внаслідок контактів. У випадку коли події контакту та шкідливої дії можна розглядати як незалежні для пошуку ЧПВ, використовується простий добуток отриманих ймовірностей (при цьому слід слідкувати, щоб згадані оцінки були проведені для однакового часового проміжку). У разі, якщо аналізуються залежні події, такі як послідовні сценарії атак або багатовекторні атаки для оцінки ЧПВ, використовується симуляція Монте-Карло, що дозволяє врахувати невизначеність в оцінках вхідних параметрів та складні залежності між векторами атак.

Оцінка величини втрат. Наступним кроком, що потребує виконання математичних розрахунків із передбачених алгоритмом АОРІКС-В, є оцінка величини втрат. На цьому кроці для ІКС ВП пропонується проводити оцінку не фінансових втрат, а часу неготовності системи. Це є ключовою відмінністю алгоритму від традиційного підходу методології FAIR, де пропонується для оцінки величини фінансових втрат використовувати триточкову оцінку, логнормальний розподіл та узагальнений розподіл Парето (слід зазначити, що методологія також передбачає і інші розподіли, але детальний опис застосування у супровідній документації описано саме для цих трьох). При цьому логнормальний розподіл та узагальнений розподіл Парето вибрані розробниками методології [10] за можливість моделювати ситуації, коли втрати можуть мати дуже великі значення. Наприклад, логнормальний розподіл підходить для моделювання ситуацій, коли втрати можуть приймати дуже великі значення, але з малою ймовірністю, а узагальнений розподіл Парето добре підходить для моделювання екстремальних подій, таких як кібератаки з катастрофічними наслідками, що несуть великі фінансові втрати та або ведуть до природних катастроф [14]. Ці два розподіли не підходять для моделювання часу неготовності ІКС, позаяк, на відміну від величин фінансових втрат, час неготовності ІКС не може прямувати до дуже великих значень. Це виходить із того факту, що практичний зміст оцінки втрачає сенс після певних часових показників, коли прогнозований час відновлення працездатності системи стає порівняним із часом, необхідним на розбудову її з нуля. Слід зазначити, що в деяких роботах, присвячених моделюванню відмови інформаційно-комунікаційної системи, іноді пропонується використовувати логнормальний розподіл для моделювання ситуацій, коли час непрацездатності може приймати дуже великі значення, але з малою ймовірністю [15], але це у випадку з ІКС ВП не можна застосувати на практиці, а ось головний недолік логнормального розподілу, а саме його непридатність для моделювання коротких часів непрацездатності [15], змушує відмовитись від його застосування в контексті поставленого завдання.

Розглянемо приклади оцінки часу неготовності ІКС ВП у контексті виконання етапу оцінка часу неготовності ІКС кроку «Оцінка величини втрат» із використанням згаданих розподілів. Отримання функції розподілу ймовірності дозволить у майбутньому скористатися симуляцією Монте-Карло для формування остаточної оцінки ризику кібербезпеки в ІКС ВП. Згідно з даними, наведеними в роботах [16; 17], для формування розподілу ймовірності часу простою інформаційно-комунікаційних систем використовують експоненціальний розподіл, розподіл Вейбулла та гамма-розподіл, а у разі недостатньої кількості експериментальних даних і наявності тільки експертних оцінок можливе використання триточкової оцінки. Опишемо типові сценарії оцінки ризиків кібербезпеки в ІКС ВП і процес вибору відповідного розподілу для оцінки ймовірності часу неготовності системи.

Розглянемо приклад, коли вебсервер компанії, що забезпечує доступ до критично важливих онлайн-сервісів, щойно запущено в роботу. З огляду на той факт, що сервер тільки розпочав роботу, історичних даних, які дозволять сформувати оцінку часу його непрацездатності внаслідок здійснення DDoS-атаки, не існує. В таких умовах для оцінки величини втрат, згідно з алгоритмом АОРІКС-В, використовуються експертні оцінки та триточковий розподіл. Завдання експертів – сформувати оцінки мінімального часу неготовності системи a, найбільш ймовірного m та максимального часу b, тоді очікуваний час неготовності системи буде розраховуватися за формулою:

$$T = \frac{a + 4m + b}{6}, \qquad (16)$$

де a – мінімальний час неготовності системи, m – найбільш імовірний час неготовності системи та b – максимальний час неготовності системи, при цьому стандартне відхилення розраховується як

$$\sigma = \frac{b - a}{6}, \qquad (17)$$

де a – мінімальний час неготовності системи та b – максимальний час неготовності системи.

Розглянемо попередній приклад з неготовністю системи внаслідок DDoS атаки за умови, коли сервер уже попрацював деякий час і є наявні історичні дані про час його відновлення після подібних атак. Найбільш оптимальним розподілом, що підходить для оцінки часу неготовності ІКС ВП, буде експотенціальний розподіл, позаяк він добре підходить для випадків, коли система може бути швидко відновлена після атаки (експоненціальний розподіл припускає, що система миттєво відновлюється після збою) [16]. В такому випадку слід задати тільки один параметр $\lambda = \frac{1}{t_a}$, де t_a – розрахований на основі історичних даних середній час неготовності системи під час здійснення DDoS-атаки. Функція розподілу щільності ймовірності матиме вигляд:

$$F(x) = 1 - e^{-\lambda t}, \qquad (18)$$

де λ – параметр розподілу, t – час тривалості оцінки.

Моделювання часу неготовності ІКС ВП за допомогою експотенціального розподілу доцільно використовувати в умовах, коли кібератаки відбуваються випадково та незалежно одна від одної, частота атак є приблизно постійною протягом часу, а система може бути швидко відновлена після атаки. Але також є низка суттєвих обмежень на застосування експоненціального розподілу, оскільки він бути неточним, якщо частота атак не є постійною або час відновлення не є експоненціально розподіленим і цей розподіл не підходить для оцінки часу неготовності системи внаслідок атак різного типу з різними частотами та часом відновлення.

У тих випадках, коли застосування експоненціального розподілу недоцільне, а саме для оцінки часу неготовності ІКС ВП внаслідок складних атак зі змінною інтенсивністю, краще використовувати розподіл Вейбула, що має два параметри. Перший з параметрів – це параметр форми k, який визначає характер частоти відмов. Для $k < 1$ це спадаюча частота відмов (ймовірність відмови з часом зменшується) $k = 1$ (постійна частота відмов, ймовірність відмови залишається сталою протягом часу і розподіл Вейбула за таких умов стає експоненціальним розподілом) та $k > 1$ – це зростаюча частота відмов (ймовірність відмови з часом збільшується). В контексті моделювання часу неготовності ІКС ВП $k < 1$ може бути застосовано для моделювання атак на нові системи або системи з новими вразливостями, де ймовірність атаки може зменшуватися з часом, коли вразливості виправляються. Параметр $k = 1$ може бути використано для моделювання атак, які відбуваються випадково та не залежать від часу, наприклад, фішингові атаки а $k > 1$ може бути застосовано для моделювання атак на системи, які з часом стають більш вразливими, наприклад, через застаріле програмне забезпечення або відсутність оновлень безпеки. Слід також враховувати, що параметр k може змінюватися з часом, тому необхідно регулярно переглядати та оновлювати його оцінку. Другий параметр аналогічний параметру експоненціального розподілу $\lambda = \frac{1}{t_a}$, де t_a – розрахований на основі історичних даних середній час неготовності системи. Функція розподілу щільності ймовірності:

$$F(x) = \frac{k}{\lambda}\left(\frac{x}{\lambda}\right)^{(k-1)} e^{-(x/\lambda)^k}, \qquad (19)$$

де k – це параметр форми, λ – параметр розподілу розрахований за допомого даних про середній час неготовності.

У випадку коли під час проведення оцінки часу неготовності ІКС слід враховувати різні фактори, такі як складність атаки, методи виявлення, ефективність реагування на інцидент, доступність резервних копій та інші, доцільно проводити цю оцінку з використанням гамма-розподілу. Основною перевагою цього розподілу є можливість моделювати широкий спектр форм розподілу часу непрацездатності, що дозволяє врахувати різні фактори та більш точну оцінку часу неготовності ІКС порівняно з простішими розподілами. При цьому його застосування більш складне і вимагає більш глибокого розуміння статистичних методів, а для точного оцінювання параметрів потрібна достатня кількість історичних даних.

Розглянемо приклад оцінки величини втрат (часу неготовності ІКС) внаслідок атаки на внутрішню мережу компанії, що містить конфіденційні дані. За допомогою APT-атаки (Advanced Persistent Threat), спрямованої на викрадення даних. До можливих втрат, що призводять до неготовності ІКС ВП, належать витрати часу на розслідування втрати даних та відновлення повної працездатності системи. Проведемо оцінку часу неготовності з гамма-розподілом. Для повноцінного застосування гамма-розподілу слід буде провести збір даних, що базується на аналізі інформації про схожі APT-атаки, дані з галузевих звітів та експертні оцінки. Слід зібрати інформацію про тривалість перебування зловмисників у мережі до виявлення та час, необхідний для повного відновлення системи після атаки. Час неготовності ІКС ВП визначається як сума часу перебування зловмисників у мережі та часу відновлення системи.

Після збору даних слід використати методи статистичного оцінювання (наприклад, метод максимальної правдоподібності або метод моментів) для визначення параметрів гамма-розподілу, а саме параметру форми α та параметру масштабу (β), що визначає середній час непрацездатності. При $\alpha < 1$ гамма-розподіл має спадаючу функцію щільності ймовірності. Це означає, що короткі часи непрацездатності є більш ймовірними, ніж

довгі. Такий розподіл може бути використаний для моделювання сценаріїв, де система швидко відновлюється після атаки, наприклад, при атаках, які блокують доступ до певних ресурсів, але не пошкоджують саму систему. При $\alpha = 1$ гамма-розподіл перетворюється на експоненціальний розподіл, який вже був розглянутий вище. При $\alpha > 1$ гамма-розподіл має «горб» і більш важкий «хвіст», що означає наявність певний «типового» часу непрацездатності, але також ймовірність дуже довгих часів відновлення. Такий розподіл може бути використаний для моделювання сценаріїв, де атаки призводять до значних пошкоджень системи, і час відновлення може бути дуже тривалим, наприклад, у разі атак, які знищують дані або пошкоджують критичні компоненти IT-інфраструктури. Наприклад, DoS-атака на вебсервер може бути описана гамма-розподілом з параметром α близьким до 1, якщо атаки призводять до випадкових збоїв, або більше 1, якщо атаки можуть призвести до перевантаження системи та тривалого часу відновлення. Для атаки програм-вимагачів параметр α розподілу може бути більше 1, оскільки час відновлення залежить від багатьох факторів, таких як наявність резервних копій, складність розшифровки даних та швидкість реагування IT-фахівців. Для складної APT-атаки параметр α може бути значно більше 1, оскільки APT-атаки можуть призводити до тривалого перебування зловмисників у мережі, що ускладнює виявлення та відновлення системи. Час неготовності ІКС ВП внаслідок атаки з використанням SQL-ін'єкції може бути оціненим з α близьким до 1 або більше 1, залежно від впливу атаки на працездатність системи та обсягу викрадених або пошкоджених даних. Вибір відповідного значення α залежить від конкретної ситуації та аналізу історичних даних про атаки та може змінюватися з часом, тому необхідно регулярно переглядати та оновлювати оцінку цього параметра. Загальний вигляд функції розподілу ймовірності для гамма-розподілу:

$$F(x) = \frac{\gamma\left(\alpha, \frac{x}{\beta}\right)}{\Gamma(\alpha)}, \qquad (20)$$

де $\gamma\left(\alpha, \frac{x}{\beta}\right) = \int_0^{\frac{x}{\beta}} t^{\alpha-1} e^{-t} dt$ – нижня неповна гамма-функція,

а $\Gamma(x) = \int_0^{\infty} t^{x-1} e^{-t} dt$ – гамма-функція, α – параметр форми та β – параметр масштабу.

Гамма-розподіл доцільно використовувати для оцінки часу неготовності ІКС ВП, коли цей час залежить від багатьох факторів і наявна достатня кількість історичних даних [17]. Його застосування дозволяє підвищити точність оцінки.

Для оцінки прогнозованого часу простою системи протягом певного періоду часу, якщо вже відома оцінка ЧПВ та оцінку часу неготовності ІКС відповідно до вибраного методу Монте-Карло для цієї події багаторазово (десятки тисяч разів із випадково згенерованими даними) виконується моделювання кількості подій втрат та моделювання часу неготовності ІКС із розрахунком загального часу простою за допомогою сумування згенерованих значень часу непрацездатності для всіх подій втрат, щоб отримати загальний час простою за цей період. Після завершення симуляції буде отриманий розподіл імовірностей для загального часу неготовності ІКС, що дозволить розрахувати середнє значення, стандартне відхилення, квантилі для оцінки очікуваного часу простою та його варіабельності із візуалізацією результатів.

Наступним етапом кроку «Оцінка величини втрат», згідно з алгоритмом АОРІКС-В, є оцінка додаткових витрат. Він здійснюється під час розробки пакета контрзаходів, які покликані зменшити вразливість системи до кібератак. На цьому кроці для пропонованих сценаріїв організації кіберзахисту ІКС ВП проводиться орієнтовний розрахунок вартості запровадження вибраних контрзаходів і виконується симуляція Монте-Карло із новими значеннями ЧПВ та оцінками часу неготовності ІКС. Таких підхід дозволить оцінити різницю в оцінках загального прогнозованого часу неготовності ІКС за умов запровадження різних пакетів контрзаходів та надати дані для прийняття оптимального рішення щодо розподілу фінансового ресурсу для організації захисту ІКС ВП. Розробка пакета контрзаходів відбувається з метою підвищення стійкості системи до кібератак, орієнтуючись на зменшення ЧПВ та часу неготовності ІКС.

Результати дослідження. В результаті проведеного дослідження було розроблено математичний апарат оцінки ризиків кібербезпеки в ІКС ВП, який враховує неможливість отримати фінансові дані про втрати для подій відмови систем внаслідок кібератак. На початку роботи проведено порівняння методу Монте-Карло з іншими методами оцінки ризиків кібербезпеки, такими як метод Баєсових мереж, аналіз дерева атак, кількісна оцінка ризиків (QRA), та виявлено, що метод Монте-Карло має низку переваг у контексті оцінки ризиків в ІКС ВП, таких як гнучкість, можливість врахування невизначеності та здатність адаптуватися до динамічних змін у ландшафті загроз. Тому запропонований у роботі підхід базується на методі Монте-Карло та дозволяє оцінити ризики кібербезпеки в умовах невизначеності, використовуючи як основний показник, що впливає на прийняття ризику, потенційний час неготовності ІКС. Дослідження спирається на розроблений у попередній роботі [2] алгоритм оцінки ризиків кібербезпеки в ІКС ВП (АОРІКС-В). Для кроку «Оцінка

частоти втрат» АОРІКС-В запропоновано використання різних розподілів ймовірностей» (розподіл Бернулі, біноміальний розподіл, бета-розподіл, розподіл Пуассона) та методу декомпозиції з обґрунтуванням вибору розподілу і прикладами застосування під час проведення оцінки ризиків в ІКС ВП. Для кроку «Оцінка величини втрат» запропоновано використання експоненціального розподілу, розподіл Вейбулла, гамма-розподіл та триточкової оцінки з оцінкою додаткових витрат на впровадження контрзаходів. Запропоновано порядок проведення порівняння різних сценаріїв організації кіберзахисту та підготовки даних, необхідних для прийняття оптимального рішення щодо розподілу фінансового ресурсу.

Для кожного запропонованого розподілу наведено приклади застосування розробленого математичного апарату для різних сценаріїв кібератак на ІКС ВП, що демонструє його практичну цінність.

Висновки. Результати дослідження свідчать, що запропонований математичний апарат та алгоритм АОРІКС-В можуть бути ефективно використані для оцінки ризиків кібербезпеки в ІКС ВП, враховуючи специфіку цих систем та особливості гібридної війни. Подальші дослідження дозволять автоматизувати оцінку ризиків в ІКС ВП, що дозволить здійснювати вплив моделювання загроз у реальному часі і швидко розробляти пакети контрзаходів, які значно підвищать стійкість ІКС ВП в умовах ведення агресивної війни в кіберпросторі.

ЛІТЕРАТУРА

1. Байдур О.В. Передумови створення моделі кіберзахисту Збройних сил України. *Прикладні системи та технології в інформаційному суспільстві* : збірник тез VII Міжнародної науково-практичної конференції, м. Київ, 29 верес. 2023 р. Київ, 2023. С. 19–22. URL: https://aistis.knu.ua/wp-content/uploads/2023/09/AISTIS_2023.
2. Байдур О.В. Кількісна методологія оцінки ризиків кібербезпеки при відсутності фінансових даних про втрати. *Кібербезпека: освіта, наука, техніка.* Том 2. № 26, м. Київ, 2024. https://doi.org/10.28925/2663-4023.2022.17.3145.
3. Leszczyna R. Review of cybersecurity assessment methods: Applicability perspective. *Computers & Security*. 2021. Vol. 108. P. 102376. https://doi.org/10.1016/j.cose.2021.102376.
4. Cheimonidis P., Rantos K. Dynamic risk assessment in cybersecurity: a systematic literature review. *Future internet.* 2023. Vol. 15, № 10. P. 324. https://doi.org/10.3390/fi15100324.
5. Devi R. Information security risk assessment (ISRA): a systematic literature review. *Journal of information systems engineering and business intelligence.* 2022. Vol. 8, № 2. P. 207–217. https://doi.org/10.20473/jisebi.8.2.207-217.
6. Wang J., Neil M., Fenton N. A Bayesian Network Approach for Cybersecurity Risk Assessment Implementing and Extending the FAIR Model. *Computers & Security.* 2020. Volume 89. https://doi.org/10.1016/j.cose.2019.101659.
7. Naik N., Grace P., Jenkins P, Naik K., Song J. An evaluation of potential attack surfaces based on attack tree modelling and risk matrix applied to self-sovereign identity. *Computers & Security*. 2022. Volume 120. https://doi.org/10.1016/j.cose.2022.102808.
8. Piper J. Risk Management Framework: Qualitative Risk Assessment through Risk Scenario Analysis, NATO Science and Technology Organization. 2019, p. 51. URL: https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-IST-166/MP-IST-166-07.pdf.
9. The Open Group Guide, The Mathematics of the Open FAIR Methodology. 2022, p. 50. URL: https://publications.opengroup.org/guides/open-fair/g180
10. Freund J., Jones J. Measuring and Managing Information Risk: A FAIR Approach. Butterworth-Heinemann, 2014. 408 p. URL: https://www.researchgate.net/publication/387512575_Measuring_and_Managing_Information_Risk_A_FAIR_Approach.
11. The Open Group Risk Analysis (O-RA) Standard, Version 2.0.1. Berkshire, United Kingdom : The Open Group, 2021. 47 p. URL: https://publications.opengroup.org/c20a.
12. Hutchins E., Cloppert M., Amin R. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Lockheed Martin Corporation, 2011, URL: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.
13. Departement of Defence. Standard practice. System safety, MIL-STD-882E, 2012. URL: https://www.nde-ed.org/NDEEngineering/SafeDesign/MIL-STD-882E.pdf.
14. Ferreira D.J., Mateus-Coelho N., Mamede H.S. Methodology for Predictive Cyber Security Risk Assessment (PCSRA). *Procedia Computer Science.* 2023. Vol. 219. P. 1555–1563. https://doi.org/10.1016/j.procs.2023.01.447.

15. Рибальченко С.А. Огляд функцій ймовірності для моделювання страхової діяльності. *Ефективна економіка*. № 3, Дніпро, 2013. URL: http://www.economy.nayka.com.ua/?op=1&z=1861.
16. Lawless J. Statistics in Reliability. *Journal of the American Statistical Association.* 2000. 95(451), p. 989–992. https://doi.org/10.1080/01621459.2000.10474291.
17. Anderson-Cook C.M., Morzinski J., Blecker K.D. Statistical Model Selection for Better Prediction and Discovering Science Mechanisms That Affect Reliability. *Systems*. 2015, 3, p. 109–132. https://doi.org/10.3390/systems3030109.

REFERENCES

1. Baidur, O.V. (2023). Prerequisites for creating a cyber defense model for the Armed Forces of Ukraine. *Applied Systems and Technologies in the Information Society:* Collection of Abstracts of the VII International Scientific and Practical Conference, Kyiv, September 29, 2023 (pp. 19–22). Retrieved from: https://aistis.knu.ua/wp-content/uploads/2023/09/AISTIS_2023.
2. Baidur, O.V. (2024). Quantitative methodology for assessing cybersecurity risks in the absence of financial loss data. *Cybersecurity: Education, Science, Technique*, *2*(26). https://doi.org/10.28925/2663-4023.2022.17.3145.
3. Leszczyna, R. (2021). Review of cybersecurity assessment methods: Applicability perspective. *Computers & Security*, *108*, 102376. https://doi.org/10.1016/j.cose.2021.102376/.
4. Cheimonidis, P., & Rantos, K. (2023). Dynamic risk assessment in cybersecurity: A systematic literature review. *Future Internet*, *15*(10), 324. https://doi.org/10.3390/fi15100324.
5. Devi, R. (2022). Information security risk assessment (ISRA): A systematic literature review. *Journal of Information Systems Engineering and Business Intelligence*, *8*(2), 207–217. https://doi.org/10.20473/jisebi.8.2.207-217.
6. 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.
7. Naik, N., Grace, P., Jenkins, P., Naik, K., & Song, J. (2022). An evaluation of potential attack surfaces based on attack tree modelling and risk matrix applied to self-sovereign identity. *Computers & Security*, *120*. https://doi.org/10.1016/j.cose.2022.102808.
8. Piper, J. (2019). *Risk Management Framework: Qualitative Risk Assessment through Risk Scenario Analysis*. NATO Science and Technology Organization. Retrieved from: https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-IST-166/MP-IST-166-07.pdf.
9. The Open Group. (2022). *The Mathematics of the Open FAIR Methodology*. Retrieved from: https://publications.opengroup.org/guides/open-fair/g180.
10. Freund, J., & Jones, J. (2014). *Measuring and managing information risk: A FAIR approach*. Butterworth-Heinemann. Retrieved from: https://www.researchgate.net/publication/387512575_Measuring_and_Managing_Information_Risk_A_FAIR_Approach.
11. The Open Group. (2021). *The Open Group Risk Analysis (O-RA) Standard*, Version 2.0.1. Retrieved from: https://publications.opengroup.org/c20a.
12. Hutchins, E., Cloppert, M., & Amin, R. (2011). *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. Lockheed Martin Corporation. Retrieved from: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.
13. Department of Defense. (2012). *Standard Practice. System Safety (MIL-STD-882E)*. Retrieved from: https://www.nde-ed.org/NDEEngineering/SafeDesign/MIL-STD-882E.pdf.
14. Ferreira, D.J., Mateus-Coelho, N., & Mamede, H.S. (2023). Methodology for predictive cyber security risk assessment (PCSRA). *Procedia Computer Science*, *219*, 1555–1563. https://doi.org/10.1016/j.procs.2023.01.447.
15. Rybalchenko, S. A. (2013). Review of probability functions for insurance activity modeling. *Effective Economics*, *(3)*. Retrieved from: http://www.economy.nayka.com.ua/?op=1&z=1861.
16. Lawless, J. (2000). Statistics in reliability. *Journal of the American Statistical Association*, *95*(451), 989–992. https://doi.org/10.1080/01621459.2000.10474291.
17. Anderson-Cook, C.M., Morzinski, J., & Blecker, K.D. (2015). Statistical model selection for better prediction and discovering science mechanisms that affect reliability. *Systems*, *3*, 109–132. https://doi.org/10.3390/systems3030109.