ISSN 2076-1546

УДК 004.4 DOI: 10.46972/2076-1546.2025.28.09

В. В. Охрімчук, І. А. Охрімчук

МЕТОД ПОБУДОВИ ПОТЕНЦІЙНОГО ВЕКТОРА КІБЕРАТАКИ НА ОСНОВІ ТЕОРІЇ МНОЖИН

Стрімке впровадження інформаційних технологій у ключові сфери діяльності людини та держави, зокрема в енергетику, транспорт, військову справу та економіку, спричиняє підвищення ефективності функціонування сучасного суспільства. Водночас зростає кількість та складність кіберзагроз, що зумовлює необхідність постійного вдосконалення систем інформаційної безпеки. Однак модернізація чинних систем інформаційної безпеки не гарантує належного рівня захисту через зростання складності атак та неефективне використання наявних засобів захисту. Більшість наукових досліджень зосереджені на розробці нових способів виявлення атак, тоді як питання їх запобігання залишається менш дослідженим.

У статті запропоновано метод побудови потенційного вектора кібератаки, що дозволяє оцінити ефективність чинної системи інформаційної безпеки або провести її оптимізацію шляхом перерозподілу ресурсів. Основою методу є побудова множин ресурсів системи на кожному рівні захисту та відповідних множин вразливостей, а також булевої матриці суміжності між цими множинами, подальший її аналіз для формування векторів атаки. Розглянуто два підходи до формування таких векторів: перший – через найвразливіший ресурс, другий – через найпоширенішу вразливість. Об'єднання частинних векторів на всіх рівнях дозволяє отримати повний вектор потенційної кібератаки.

Застосування методу дає змогу виявити критичні ресурси системи інформаційної безпеки, визначити універсальні або найвразливіші її елементи та запропонувати шляхи підвищення стійкості: вилучення слабких або надлишкових компонентів, усунення поширених вразливостей, посилення ключових вузлів. Метод має прикладне значення для проєктування, тестування та вдосконалення систем інформаційної безпеки, а також створює підґрунтя для подальших досліджень, спрямованих на врахування динаміки змін у вразливостях та адаптивних стратегій зловмисників.

***Ключові слова**: кібербезпека; кіберзахист; кібератака; вектор кібератаки; множина; вразливість.*

Постановка проблеми в загальному вигляді. Стрімкий розвиток інформаційних технологій та їх інтеграція в різні сфери, наприклад, економічну, військову, енергетичну, транспортну тощо, суттєво впливає на ефективність діяльності не тільки окремо взятої людини, але й суспільства та держави в цілому. Проте, окрім усіх позитивних ефектів від їх упровадження в діяльність сучасного суспільства, суттєво й не в кращий бік змінюється ситуація з кібербезпекою. Саме тому на сучасному етапі одним із пріоритетних векторів наукових досліджень у цій сфері є розроблення інноваційних та ефективних методів

і засобів протидії кібератакам (КбА), що спрямовані на їх своєчасне детектування й нейтралізацію.

Модернізація ж чинних систем інформаційної безпеки (СІБ) не забезпечує повної гарантії захисту інформаційно-комунікаційних систем (ІКС) від різних типів КбА. Така ситуація зумовлена, з одного боку, технологічною складністю останніх, а з іншого – неефективним розподіленням засобів захисту ІКС від КбА.

Отже, пошук нових підходів до підвищення рівня кіберзахисту ІКС залишається актуальним завданням як у теоретичному, так і в прикладному вимірах.

Аналіз останніх досліджень і публікацій. У результаті аналізу доступних джерел [1–6] встановлено, що більшість досліджень у цій сфері направлені на розроблення нових методів виявлення КбА або побудову математичних моделей для дослідження реакцій системи на неї, оцінювання заподіяної шкоди. Метою цих методів є підвищення ефективності СІБ для виявлення нетипових й аномальних КбА за рахунок розроблення нових шаблонів КбА та внесення їх до баз сигнатур СІБ, тобто основна увага спрямована на питання, яким чином виявити КбА та захиститися від неї.

З урахуванням викладеного вище постає питання про попередження потенційних КбА в ході проєктування та розгортання СІБ. Вирішити цю проблему можливо за допомогою всебічного дослідження наявних засобів захисту, встановлення їх слабких місць та побудови найімовірнішого вектора КбА.

Формулювання завдання дослідження. Сьогодні для протидії КбА в ІКС розгортають СІБ. Відповідно, для досягнення своєї мети зловмиснику необхідно подолати всі механізми захисту цієї системи. У такий спосіб відбуваються постійні “змагання” між тими, хто створює СІБ, та тими, хто намагається їх подолати. Перемога перших прямо залежить від правильного вибору засобів і механізмів СІБ та розподілення їх в ІКС. Отже, знаючи слабкі сторони СІБ та ІКС в цілому, можна з високою ймовірністю визначити потенційний вектор проведення зловмисником КбА, а це, у свою чергу, може зумовити підвищення рівня кібербезпеки.

Метою статті є розроблення методу побудови потенційного вектора КбА, який може бути використаний для аналізу ефективності СІБ або перерозподілу її ресурсів.

Виклад основного матеріалу. Відповідно до [7] об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення (ПЗ), призначене для цього. Для забезпечення захисту зазначених об’єктів у системі розробляються та впроваджуються СІБ. Як показує практика, використання багаторівневих СІБ значно посилює захист [8]. Так, наприклад, він може здійснюватися на рівнях даних, додатків (ПЗ), хоста, мережі тощо. Характерним є те, що на кожному рівні використовуються певні механізми захисту, притаманні саме йому. У цілому таку систему можна подати у вигляді моделі Деннінга (рис. 1) [9, 10].

Отже, для досягнення своєї мети зловмиснику необхідно подолати всі рівні захисту СІБ. Для цього він буде використовувати наявні вразливості як у СІБ, так і в ПЗ, тому під вектором атаки розумітимемо упорядковану множину точок докладання зусиль зловмисника для подолання механізмів захисту СІБ. Враховуючи це твердження, метод

побудови потенційного вектора КбА повинен бути направлений на визначення ймовірних точок докладання зусиль зловмисника, які, у свою чергу, формуються з множин ресурсів СІБ на кожному рівні захисту, а також відповідних множин уразливостей.

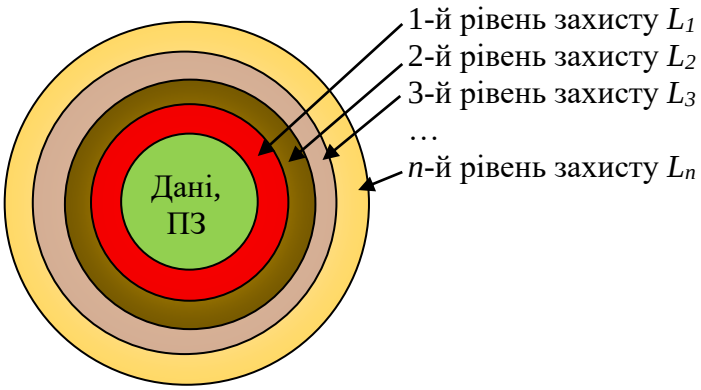

Рис. 1. Модель багаторівневого захисту (за Деннінгом)

У загальному випадку множина ресурсів СІБ L_i-го рівня може бути подана таким виразом:

$$R_{L_i} = \{r_{i1}, r_{i2}, ..., r_{i3}\}, \left|R_{L_i}\right| = k, \tag{1}$$

де i – рівень СІБ;

k – кількість ресурсів СІБ, якими можуть бути ресурси користувача, системні ресурси, ресурси баз сигнатур, обчислювальні ресурси тощо [9]. Як відомо з [11–13] немає жодної системи, зокрема і СІБ, ресурси яких не мали б вразливостей, тому кожен ресурс r_{ik} множини R_{L_i} можна подати кортежем загального вигляду:

$$\exists r_{ik} \in R_{L_i}, r_{ik} = \langle r_{ik}, V_{ik} \rangle, \tag{2}$$

де r_{ik} – k-й ресурс;

V_{ik} – множина вразливостей цього ресурсу, причому $V_{ik} \subseteq V$ та $\left|V_{ik}\right| \geq 0$, а V – множина всіх відомих вразливостей СІБ та ІКС, тобто $V = \{v_1, v_2, ..., v_s\}$.

Елементами множини V можуть бути вразливості та дефекти, об’єднані в одній із найбільш відомих баз даних загальновідомих вразливостей інформаційної безпеки *CVE* [14]. Крім неї можуть бути використані такі бази, як *Common Weakness Enumeration* (*CWE*) [15], *National Vulnerabilities Database* (*NVD*) [16], *Vulnerability Notes Database* (*VND*) [17] та інші [18].

Оскільки кожний ресурс r_{ik} можна подати у вигляді (2), то множина ресурсів, які потенційно можуть бути атакованими, становитиме відношення R'_{L_i}, задане на декартовому добутку множин ресурсів R_{L_i}, та відомих вразливостей V [19]. У формалізованому вигляді воно може бути описане булевою матрицею суміжності:

R'_{L_i}	v_1	v_2	v_3	$\cdots$	v_s
r_{i1}	1	0	1	$\cdots$	1
r_{i2}	0	0	0	$\cdots$	1
r_{i3}	0	0	1	$\cdots$	1
$\vdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
r_{ik}	1	1	0	$\cdots$	0

. (3)

Отже, множина R'_{L_i} містить упорядковані пари (див. (3)). Першим елементом упорядкованої пари є ресурс r_{ik} множини R_{L_i}, що має вразливість, а другим – відповідна йому вразливість $v_s \in V_{ik}$, тобто

$$R'_{L_i} \subseteq R_{L_i} \times V = \left\{ \langle r_{ik}, v_s \rangle \mid r_{ik} \in R_{L_i}, v_s \in V_{ik}, |V_{ik}| \neq 0, r_{ik} R'_{L_i} v_s \right\}. \quad (4)$$

Аналізуючи вираз (4), можна розглядати два потенційні вектори КбА для подолання механізмів захисту СІБ на L_i-му рівні.

1. *Атака через найбільш вразливий ресурс*. Зловмисник обирає для атаки той ресурс r_{ik}, для якого потужність множини його вразливостей є максимальною, тобто

$$r_{ik} = \arg\max_{r_{ik} \in R_{L_i}} |V_{ik}|. \quad (5)$$

Цей підхід логічний з погляду атакуючого, оскільки більше вразливостей означає вищу ймовірність успішного вторгнення. На думку сторони, що захищається, цей принцип дозволяє ідентифікувати найбільш вразливі елементи системи й вжити заходи для посилення захисту.

2. *Експлуатація найбільш розповсюдженої вразливості*. Інший підхід полягає у виборі тієї вразливості, яка є спільною для найбільшої кількості ресурсів, тобто

$$v_s = \arg\max_{v_s \in V} \left| \left\{ r_{ik} \in R_{L_i} : v_s \in V_{ik} \right\} \right|. \quad (6)$$

Такий підхід дозволяє зловмиснику атакувати максимальну кількість ресурсів одночасно, використовуючи одну й ту саму вразливість. Для сторони, що захищається, цей аналіз є критично важливим для виявлення точок концентрації ризику – універсальних слабких місць системи.

Оскільки точками докладання зусиль зловмисником є ресурси СІБ та ІКС, то загальний вектор атаки для L_i-го рівня СІБ можна подати у вигляді множини, елементами якої є ресурс, визначений за виразом (5), та ресурси, що входять до виразу (6).

Відповідно, для побудови повного вектора КбА слід побудувати частинні вектори для кожного рівня СІБ, він буде містити об’єднану множину ресурсів усіх рівнів, що з високою ймовірністю будуть використані для здійснення КбА.

Отже, з урахуванням наведеного математичного апарату метод побудови потенційного вектора КбА складається з таких кроків.

Крок 1. Визначення структури системи. Здійснюється аналіз СІБ та розбиття її механізмів захисту на рівні, після чого відбувається ідентифікація всіх ресурсів кожного рівня R_{L_i} (1) та їх вразливостей V_{ik}.

Крок 2. Побудова булевої матриці суміжності. За визначеними на першому кроці ресурсами та їх вразливостями будується таблиця, де рядки – ресурси, стовпці – вразливості (див. (3)).

Крок 3. Підготовка даних до аналізу на підставі (4) здійснюється в два етапи: для кожного ресурсу обчислюються потужності множин притаманних їм вразливостей, тобто $|V_{ik}|$; для кожної вразливості визначається кількість ресурсів, у яких вона присутня.

Крок 4. Вибір стратегії атаки. На основі аналізу даних, отриманих на попередньому кроці, та за виразами (5), (6) визначають дві стратегії зловмисника: перша – використання ресурсу, що має найбільшу кількість вразливостей; друга – множинний вхід, застосування однієї універсальної вразливості, що притаманної найбільшій кількості ресурсів.

Крок 5. Побудова частинного вектора КбА. У результаті обрання стратегій та об'єднання потенційних для атаки ресурсів отримаємо частинний вектор КбА для певного рівня захисту СІБ.

Далі кроки з другого по п'ятий повторюються для всіх рівнів захисту, визначених на першому кроці.

Крок 6. Побудова повного вектора КбА. Після визначення частинних векторів КбА повний вектор будується шляхом їх об'єднання.

Отже, у результаті використання запропонованого методу можна отримати множину всіх критичних ресурсів та притаманних їм вразливостей.

Ця інформація може бути використана для оптимізації СІБ, зокрема усунення недоцільних інструментів (якщо ресурс має занадто багато вразливостей і низьку критичність, то його можна виключити із системи), або ж для підсилення слабких місць (усунення вразливості, притаманної максимальній кількості ресурсів), або для створення додаткових механізмів захисту для ресурсів, що мають найбільшу кількість вразливостей.

Висновки. У статті розглянуто актуальну проблему побудови потенційного вектора КбА на ІКС. Запропонований метод базується на теорії множин і включає побудову булевої матриці суміжності між ресурсами та відомими вразливостями з використанням загальновідомих баз даних (*CVE, CWE, NVD* тощо). У межах методології проаналізовано два основні сценарії атак: через найуразливіший ресурс та через найбільш розповсюджену вразливість.

Результатом застосування методу є формування повного вектора КбА, що охоплює всі рівні захисту СІБ та дозволяє ідентифікувати критичні елементи системи, які можуть бути використані зловмисником. Його застосування сприяє підвищенню рівня кіберстійкості ІКС та створює підґрунтя для аналізу ефективності механізмів захисту СІБ, перерозподілу її ресурсів, усунення надмірно вразливих або неефективних компонентів і посилення захисту найбільш небезпечних точок.

Метод є універсальним, адаптивним та придатним як для етапу проєктування, так і для експлуатації ІКС. У подальших дослідженнях його можливо розширити з урахуванням динаміки розвитку вразливостей, нових типів атак та моделювання поведінки адаптивного противника в умовах змінного середовища загроз.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Грищук Р. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень : монографія. Житомир : Рута, 2010. 280 с.
2. Optimising Cyber Attack Detection: A Systematic Analysis of Attack Vectors and Data Sources / Harris Daniel, Miknis Marius, Smith Connor, Wilson Ian. 2023. https://doi.org/10.13140/RG.2.2.30655.89767
3. Dwivedi. Analysis of Cyber Attack Vectors // International Conference on Computing, Communication and Automation (ICCCA). 2016. https://doi.org/10.1109/CCAA.2016.7813791
4. Погасій С. С. Моделі і методи захисту інформації в кіберфізичних системах // Безпека інформації. 2022. Т. 28, № 2. С. 67–79. https://doi.org/10.18372/2225-5036.28.16951
5. Моделювання кібератак засобами теорії графів / В. А. Савченко, О. Й. Мацько, С. В. Легомінова та ін. // Сучасний захист інформації. 2019. № 4 (40). С. 6–11. https://doi.org/10.31673/2409-7292.2019.040611
6. Корченко А. О. Методи ідентифікації аномальних станів для систем виявлення вторгнень : монографія. Київ : ЦП «Компринт», 2019. 361 с.
7. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 18.05.2025).
8. Даник Ю. Г., Грищук Р. В. Основи кібернетичної безпеки : монографія / За заг. ред. проф. Ю. Г. Даника. Житомир : ЖНАЕУ, 2016. 636 с.
9. Дудикевич В., Опірський І. Аналіз моделей захисту інформації в інформаційних мережах держави // Системи обробки інформації. 2016. № 4 (141). С. 86–89.
10. Охрімчук В. В. Узагальнена диференційно-ігрова модель шаблону потенційно небезпечної кібератаки // Кібербезпека: освіта наука і техніка. Київ : Київськ. ун-т ім. Б. Грінченка. 2020. № 4 (8). С. 113–123. https://doi.org/10.28925/2663-4023.2020.8.113123
11. Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения : монография. Київ : “МК-Пресс”, 2006. 320 с.
12. Охрімчук В. В. Модель шаблону потенційно небезпечної кібератаки // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : наук.-техн. зб. 2018. № 1 (35). С. 30–37.
13. Охрімчук В. В. Метод побудови шаблонів потенційно небезпечних кібератак // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. Житомир : ЖВІ, 2019. Вип. 17. С. 173–182. https://doi.org/10.46972/2076-1546.2019.17.16
14. Common Vulnerabilities and Exposures (CVE) : офіційний сайт. URL: http://cve.mitre.org (last accessed: 16.05.2025).

15. Common Weakness Enumeration (CWE) : офіційний сайт. URL: https://cwe.mitre.org (last accessed: 16.05.2025).
16. National Vulnerabilities Database (NVD) : офіційний сайт. URL: https://nvd.nist.gov (last accessed: 16.05.2025).
17. Vulnerability Notes Database (VND) : офіційний сайт. URL: https://www.kb.cert.org/vuls (last accessed: 16.05.2025).
18. Грищук Р. В., Охрімчук В. В., Ахтирцева В. С. Джерела первинних даних для розроблення шаблонів потенційно небезпечних кібератак // Захист інформації. 2016. Т. 18, № 1. С. 21–29. https://doi.org/10.18372/2410-7840.18.10109
19. Михалін Г. О., Дюженкова Л. І. Елементи теорії множин і теорії чисел. Київ : НПУ ім. М. П. Драгоманова, 2003. 128 с.

Стаття надійшла до редакції 21.05.2025.

REFERENCES

1. Hryshchuk, R. (2010). *Teoretychni osnovy modeliuvannia protsesiv napadu na informatsiiu metodamy teorii dyferentsialnykh ihor ta dyferentsialnykh peretvoren: monohrafiia [Theoretical Foundations of Modeling Information Attack Processes Using Differential Games and Differential Transformations. Monograph]*. Zhytomyr. [in Ukrainian].
2. Harris Daniel, Miknis Marius, Smith Connor, & Wilson Ian. (2023). *Optimising Cyber Attack Detection: A Systematic Analysis of Attack Vectors and Data Sources.* https://doi.org/10.13140/RG.2.2.30655.89767
3. Dwivedi. (2016). Analysis of Cyber Attack Vectors. In *International Conference on Computing, Communication and Automation (ICCCA).* https://doi.org/10.1109/CCAA.2016.7813791
4. Pohasii, S. S. (2022). Modeli i metody zakhystu informatsii v kiberfizychnykh systemakh [Models and Methods for Information Protection in Cyber-Physical Systems]. *Bezpeka informatsii [Information Security], 28,* 2, 67–79. https://doi.org/10.18372/2225-5036.28.16951 [in Ukrainian].
5. Savchenko, V. A., Matsko, O. Y., & Lehominova, S. V. et al. (2019). Modeliuvannia kiberatak zasobamy teorii hrafiv [Modeling Cyber Attacks Using Graph Theory]. *Suchasnyi zakhyst informatsii [Modern Information Protection], 4* (40), 6–11. https://doi.org/10.31673/2409-7292.2019.040611 [in Ukrainian].
6. Korchenko, A. O. (2019). Metody identyfikatsii anomalnykh staniv dlia system vyiavlennia vtorhnen : monohrafiia [Methods for Identifying Abnormal States for Intrusion Detection Systems. Monograph]. Kyiv. [in Ukrainian].
7. *Pro zakhyst informatsii v informatsiino-komunikatsiinykh systemakh: Zakon Ukrainy vid 05.07.1994 № 80/94-VR (zi zminamy) [About Information Protection in Information and Communication Systems: Law of Ukraine № 80/94- VR of 05.07.1994 (as amended)]*. Retrived from https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text [in Ukrainian].
8. Danyk, Yu. H., & Hryshchuk, R. V. (2016). *Osnovy kibernetychnoi bezpeky: monohrafiia [Basics of cybernetic security. Monograph]*. Zhytomyr [in Ukrainian].
9. Dudykevych, V., & Opirskyi, I. (2016). Analiz modelei zakhystu informatsii v informatsiinykh merezhakh derzhavy [Analysis of information protection models in state

information networks]. *Systemy obrobky informatsii [Information Processing Systems], 4* (141), 86–89. [in Ukrainian].
10. Okhrimchuk, V. V. (2020). Uzahalnena dyferentsiino-ihrova model shablonu potentsiino nebezpechnoi kiberataky [Generalized Differential Game Model of a Potentially Dangerous Cyber Attack Pattern]. *Kiberbezpeka: osvita nauka i tekhnika [Cybersecurity: Education, Science, and Technology], 4* (8), 113–123. https://doi.org/10.28925/2663-4023.2020.8.113123 [in Ukrainian].
11. Korchenko, A. H. (2006). *Postroenye system zashchytы ynformatsyy na nechetkykh mnozhestvakh. Teoryia y praktycheskye reshenyia : monohrafyia [Building Information Security Systems Based on Fuzzy Sets. Theory and practical solutions: Monograph]*. Kyiv [in Ukrainian].
12. Okhrimchuk, V. V. (2018). Model shablonu potentsiino nebezpechnoi kiberataky [A Model of a Potentially Dangerous Cyber Attack Pattern]. *Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini : nauk.-tekhn. zb. [Legal, Regulatory and Metrological Support of the Information Security System in Ukraine: Scientific and Technical Collection], 1* (35), 30–37 [in Ukrainian].
13. Okhrimchuk, V. V. (2019). Metod pobudovy shabloniv potentsiino nebezpechnykh kiberatak [The Method of Development a Templates of Potentially Dangerous Cyber-Attacks]. *Problemy stvorennia, vyprobuvannia, zastosuvannia ta ekspluatatsii skladnykh informatsiinykh system: zb. nauk. prats [Problems of Construction, Testing, Application and Operation of Complex Information Systems. Scientific Journal of Korolov Zhytomyr Military Institute], 17*, 173–182. https://doi.org/10.46972/2076-1546.2019.17.16 [in Ukrainian].
14. Common Vulnerabilities and Exposures (CVE): Official Website. (n.d.). Retrived from http://cve.mitre.org
15. Common Weakness Enumeration (CWE): Official Website. (n.d.). Retrived from https://cwe.mitre.org
16. National Vulnerabilities Database (NVD): Official Website. (n.d.). Retrived from https://nvd.nist.gov
17. Vulnerability Notes Database (VND): Official Website. (n.d.). Retrived from https://www.kb.cert.org/vuls
18. Hryshchuk, R. V., Okhrimchuk, V. V., & Akhtyrtseva, V. S. (2016). Dzherela pervynnykh danykh dlia rozroblennia shabloniv potentsiino nebezpechnykh kiberatak [The Sources of Primary Data for the Development Potentially Dangerous Patterns of Cyber-Attacks]. *Zakhyst informatsii [Information Protection], 18*, 1, 21–29. https://doi.org/10.18372/2410-7840.18.10109 [in Ukrainian].
19. Mykhalin, H. O., & Diuzhenkova, L. I. (2003). Elementy teorii mnozhyn i teorii chysel [Elements of Set Theory and Number Theory]. Kyiv [in Ukrainian].

V. V. Okhrimchuk, I. A. Okhrimchuk

METHOD FOR CONSTRUCTING A POTENTIAL CYBER ATTACK VECTOR USING SET THEORY

The rapid integration of information technologies into key sectors of human and state activity – including energy, transportation, defense, and the economy – enhances the efficiency

of modern society. At the same time, the number and complexity of cyber threats are increasing, necessitating the continuous improvement of information security systems. However, upgrading existing information security systems does not guarantee an adequate level of protection due to the growing sophistication of attacks and inefficient use of available security tools. Most scientific research focuses on developing new attack detection methods, while the issue of attack prevention remains relatively underexplored.

This article proposes a method for constructing a potential cyberattack vector, which enables evaluation of the effectiveness of an existing information security system or its optimization through resource redistribution. The method is based on constructing sets of system resources at each protection level, as well as the corresponding sets of vulnerabilities. A Boolean adjacency matrix is then created between these sets and analyzed to generate attack vectors. Two approaches to vector construction are considered: the first – through the most vulnerable resource, and the second – through the most widespread vulnerability. The combination of partial vectors across all levels yields a complete potential cyberattack vector.

The application of this method allows for the identification of critical information security systems resources, the determination of universal or most vulnerable system components, and the development of strategies to enhance resilience — such as removing weak or redundant components, eliminating common vulnerabilities, and strengthening key nodes. The method has practical value for the design, testing, and improvement of information security systems, and also provides a foundation for further research aimed at accounting for vulnerability dynamics and adaptive adversary strategies.

Keywords*: cybersecurity; cyberdefense; cyberattack; attack vector; set; vulnerability.*