DOI:**10.33099/2311-7249/2023-46-1-41-44**

УДК: 355.45

Рустам Камілович Мурасов (*кандидат технічних наук****)***
Ярослав Вячеславович Мельник

Національний університет оборони України імені Івана Черняховського, Київ, Україна

ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ КІБЕРПРОСТОРУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Методика оцінювання захищеності кіберпростору об'єктів критичної інфраструктури України є надзвичайно важливою через посилення загроз кібербезпеці в Україні. Об'єкти критичної інфраструктури України, такі як енергетичні мережі, транспортні системи, банківські установи, медичні та військові заклади, системи зв'язку та інші, мають велике значення для життя і діяльності національної економіки та суспільства в цілому. Зокрема, збій в роботі цих об'єктів може призвести до серйозних наслідків, таких як відключення електропостачання, зупинка транспорту, порушення фінансової стабільності, порушення медичного обслуговування та ін. За таких умов, захист кіберпростору об'єктів критичної інфраструктури стає надзвичайно важливим завданням для держави та бізнесу. Для досягнення цієї мети необхідно мати ефективну методику оцінювання захищеності кіберпростору об'єктів критичної інфраструктури, яка дає змогу виявляти потенційні загрози та ризики, а також розробляти та впроваджувати заходи з підвищення кібербезпеки. В статті наведено теоретичні викладки, що пов'язують між собою розуміння державою принципів функціонування сучасних кібернетичних загроз та пошуку механізмів їх вирішення. Встановлено, що забезпечення національної (воєнної) безпеки поки не здійснюється за рахунок належної концепції. За результатами оцінювання захищеності кіберпростору об'єктів критичної інфраструктури визначено практичні шляхи зміцнення воєнної безпеки України через пошук ефективної стратегії кібербезпеки.

Ключові слова: *кібератака; кібербезпека; кібероборона; мінімізація наслідків надзвичайних ситуацій; дослідження причин виникнення надзвичайних ситуацій.*

Вступ

Методика оцінювання захищеності кіберпростору об'єктів критичної інфраструктури України є актуальною та важливою через посилення загроз у сфері кібербезпеки України, особливо у період повномасштабної російської агресії проти України. Розробка і впровадження ефективної методики оцінювання захищеності кіберпростору об'єктів критичної інфраструктури є складним завданням, що потребує врахування багатьох факторів. Для цього потрібно використовувати сучасні технології та методи аналізу, зокрема, моніторинг і аналіз кібератак, тестування на проникнення, аудит безпеки, поради фахівців тощо. Ця методика має бути адаптована до специфіки кожного об'єкта та враховувати його унікальні особливості й потенційні загрози. Важливо також враховувати міжнародні стандарти та рекомендації щодо кібербезпеки, зокрема, ISO/IEC 27001, NIST Cybersecurity Framework, ENISA Guidelines тощо. Наслідки кібератак можуть бути катастрофічними, тому важливо проводити регулярне оцінювання захищеності кіберпростору об'єктів критичної інфраструктури та приймати заходи для підвищення захищеності. Це дає змогу зменшити ризики кібератак і забезпечити безпеку функціонування критичної інфраструктури.

Постановка проблеми. Багато уваги надано вирішенню та оцінюванню кібербезпеки в закордонних провідних виданнях [2], традиційно в західних наукових виданнях, і останнім часом, дане питання, глибоко вивчається в цивільних і воєнних наукових сферах російської федерації [1]. Але методологія оцінювання кібербезпеки має закритий характер, а її складова більш орієнтована на комерційну діяльність направлена на надання послуг щодо моніторингу та оцінювання кібербезпеки суб'єктів господарювання.

Вищезазначене дозволяє створити власну методику оцінювання кібернетичної безпеки, яка буде враховувати реальний стан функціонування власної кібернетичної мережі та яку буде можливо оптимізувати, за умов виявлення нових складових. Ця методика має враховувати специфіку кожного об'єкта критичної інфраструктури і враховувати його унікальні особливості та потенційні загрози. Важливо також враховувати міжнародні стандарти та рекомендації щодо кібербезпеки, забезпечити регулярне оцінювання та підвищення захищеності кіберпростору об'єктів критичної інфраструктури для запобігання наслідків кібератак і забезпечення стабільності функціонування системи в цілому.

Крім того, необхідно враховувати, що загрози кібербезпеці постійно видозмінюються, тому

методика має бути гнучкою та здатною до оновлення відповідно до нових загроз і вразливостей.

Метою статті є проведення оцінювання захищеності кіберпростору об'єктів критичної інфраструктури України для визначення рівня захищеності кіберпростору таких об'єктів, що забезпечить виявлення та усунення вразливостей і потенційних загроз кібербезпеці, дасть змогу запобігти можливим кібератакам та забезпечити безперебійне функціонування системи в цілому.

Виклад основного матеріалу дослідження

У процесі вивчення наукових робіт провідних фахівців [4] у сфері кібербезпеки (IBM, Cisco та інших відомих фірм із забезпечення кібербезпеки), аналізу наукових даних, якими можна оперувати під час оцінювання стану кібербезпеки, оптимальною методикою, що пропонується в цій роботі, є методика на основі оцінювання імовірності стійкості системи у ході здійсненні кібератак, які здатні порушити роботу кібернетичної мережі [2].

$$P_{кб} = \{0; \dots\dots; 1\} \quad (1)$$

Доцільно буде зробити декомпозицію імовірностей типів кібератак (порушення стану функціонування), як незалежні події та застосувати математичний апарат теорії імовірності – теорему повної імовірності [1]. Таким чином отримуємо імовірнісну оцінку стану кібербезпеки. Складовими імовірностями будуть такі, що обрані відповідно до статистики методів здійснення кібератак для основних джерел загроз, що були заблоковані на комп'ютерах автоматизованої системи управління (далі – АСУ) (відсоток атакованих комп'ютерів АСУ за півріччя), наведених на рис. 1 та основні платформи, що використовує шкідливе програмне забезпечення (відсоток атакованих комп'ютерів АСУ), наведених на рис. 2.).

Рис. 1. Основні джерела загроз, що були заблоковані на комп'ютерах АСУ

Відповідно до статистичних даних кіберзагроз були обрані такі імовірності здійснення кібернетичних атак (табл. 1).

Для оцінювання ступеня захищеності кіберпростору України використано відомий математичний апарат, заснований на теоремах повної імовірності та множення імовірностей [1]. Теорема повної імовірності (англ. Law of Total Probability) – повна система подій, що дорівнює сумі добутків імовірностей гіпотез на умовні ймовірності події, обчислені відповідно до кожної з гіпотез. Теорема повної ймовірності дає змогу обчислити ймовірність події А, що цікавить дослідника, через ймовірність її здійснення за умов підтвердження гіпотез із заданою ймовірністю.

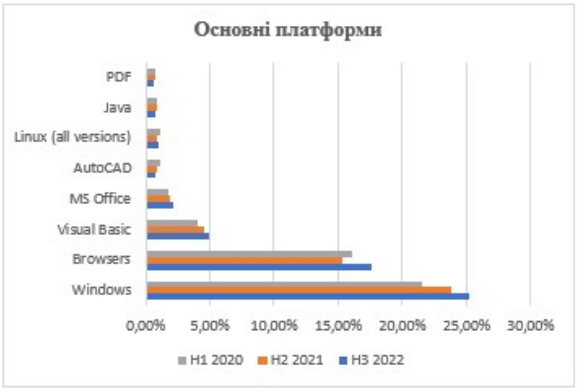

Рис. 2. Основні платформи, що використовує шкідливе програмне забезпечення у 2020, 2021 та 2022 роках

Таблиця 1

Імовірність здійснення кібернетичних атак

Вид загрози	Умовне позначення
DDoS атака	P_{DDoS}
Троян/вірус	P_{virus}
Програмне забезпечення	$P_{programm}$
Шпигунство/сторонній доступ	P_{spy}
Технічні вразливості	P_{hiker}

Формула повної ймовірності застосовується, коли необхідно отримати ймовірність настання певної події, якщо ця подія залежить від кількох умов. Наприклад, можна дізнатися про ймовірність захищеності кіберпростору, знаючи, з якою ймовірністю захищено кожен її елемент. Теорема множення ймовірностей – імовірність добутку двох подій дорівнює добутку імовірностей одного з них на умовну ймовірність іншого, обчислену за умови, що перше мало місце. Іншими словами імовірність добутку двох незалежних подій дорівнює добутку імовірностей цих подій [2]:

$$P(AB) = P(A) \cdot P(B) \quad (2)$$

Застосовуючи теорему повної ймовірності та теорему множення ймовірностей, отримуємо такий вираз для ймовірність захищеності кіберпростору

$$P_{кб} = 1 - (1 - P_{DDoS})(1 - P_{virus})(1 - P_{programm})(1 - P_{spy})(1 - P_{hiker}), \quad (3)$$

Такий підхід дає змогу враховувати нові складові кібербезпеки і додавати їх під час обчислення ймовірності. Блок-схема реалізації методики оцінювання захищеності кіберпростору об'єктів критичної інфраструктури України наведено на рис. 3.

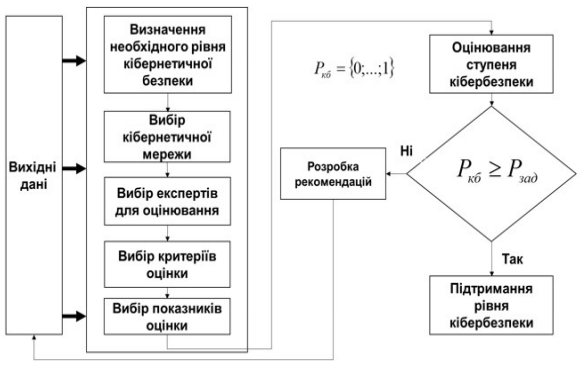

Рис. 3. Блок-схема методики оцінювання захищеності кіберпростору об'єктів критичної інфраструктури

Варто констатувати, що методи оцінювання імовірностей кіберзагроз не є доступними у загальних джерелах. Оскільки кіберсистеми мають різну архітектуру і властивості, програмне забезпечення та рівень підготовленого персоналу, доцільно застосовувати метод експертних оцінок з метою визначення ймовірностей для кожного конкретного випадку [3].

За методикою можна визначити реальний ступінь кібернетичного захисту різних систем, і як наслідок, корегувати рівень складових кібернетичного захисту, залежно від його стану, наявних кібернетичних загроз і можливостей, а також поставлених завдань.

Як приклад реалізації методики, пропонується провести практичні розрахунки оцінювання кібербезпеки кібермережі Центру імітаційного моделювання Національного університету оборони України імені Івана Черняховського. Методом експертного оцінювання пропонується обчислити значення імовірностей загроз за вихідними даними, що наведені у таблиці 2.

Таблиця 2

Обчислення значення імовірностей загроз

Вид загрози	Умовне позначення	Значення
DDoS атака	P_{DDoS}	0,7
Троян/вірус	P_{virus}	0,2
Програмне забезпечення	$P_{programm}$	0,5
Шпигунство/сторонній доступ	P_{spy}	0,1
Технічні вразливості	P_{hiker}	0,5

Обчислена ймовірність кіберзагрози за виразом (3) становить $P_{кб} = 0{,}946$, що є показником вдалої кібератаки, тому потрібно застосувати заходи щодо зменшення ймовірностей успіху кібератак. Після застосування рекомендованих в роботі заходів, маємо показники наведені у таблиці 3 [4].

За результатами проведених розрахунків, ймовірність кіберзагрози зменшилася в 2,3 рази, що графічно відображено на рис. 4. Імовірність успішної кібернетичної атаки складає 0,41 що є достатньо надійним показником.

Таблиця 3

Зменшення ймовірностей успіху кібератак

Вид загрози	Умовне позначення	Значення
DDoS атака	P_{DDoS}	0,3
Троян/вірус	P_{virus}	0,01
Програмне забезпечення	$P_{programm}$	0,1
Шпигунство/сторонній доступ	P_{spy}	0,001
Технічні вразливості	P_{hiker}	0,05

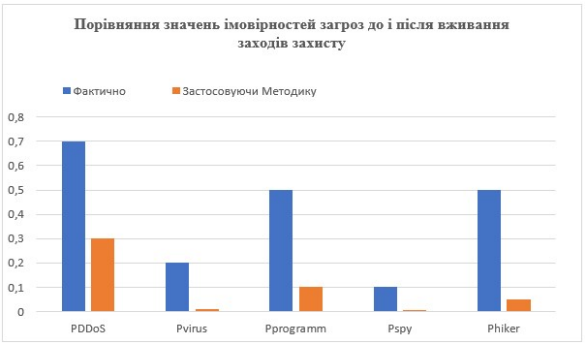

Рис. 4. Порівняння значення загроз до та після застосування заходів захисту

Після обчислень отримаємо: $P_{кб} = 0{,}41$ (рис. 5.)

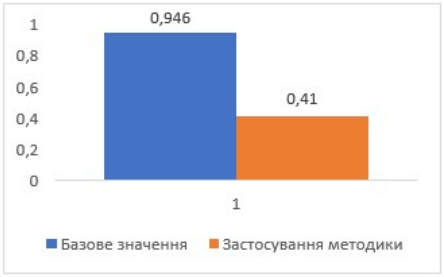

Рис. 5. Результат застосування запропонованої методики

Висновки й перспективи подальших досліджень

Таким чином, у статті проведено визначення рівня кібербезпеки підрозділу Міністерства оборони України. На основі отриманих результатів сформовано практичні рекомендації щодо забезпечення кібернетичної безпеки до необхідного рівня, які доцільно впровадити в установах та військових частинах. Використана методика дозволяє коректувати пріоритети кіберзагроз, вносити зміни щодо наявних загроз та вразливостей для забезпечення кібероборони (відбиття воєнної агресії у кіберпросторі) України. Також за допомогою зазначеної методики є можливість аналізувати стан існуючої безпеки і шляхи її підвищення, включати і враховувати нові показники, залежно від рівня технічного оснащення, та здійснювати аналіз стану критичних показників кіберзахисту об'єктів критичної інфраструктури.

Література

1. Мохор В., Гончар С., Дибах О. Методи оцінки сумарного ризику кібербезпеки об'єктів критичної інфраструктури. Ядерна та радіаційна безпека. 2019. №2(82). DOI: https://doi.org/10.32918/nrs.2019.2(82).01 (дата звернення: 12.12.2022). **2. Regulation (EU) of the European Parliament and of the Council «**On ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)» (Text with EEA relevance) of 17 April 2019 №2019/881. *Official Journal of the European Union*. L 151/15, 7.6.20193. **3. Указ Президента України «**Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"» від 26.08.2021 №447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 12.12.2022). **4. Мурасов Р. К., Мельник Я. В.** Імовірнісний метод прогнозування надзвичайних подій на потенційно-небезпечних об'єктах критичної інфраструктури. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2022. № 2(44). С. 60–64.

ASSESSMENT OF CYBER SPACE PROTECTION OF CRITICAL INFRASTRUCTURE FACILITIES OF UKRAINE

Rustam Murasov (Candidate of Technical Sciences)
Yaroslav Melnyk

National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine

The methodology for assessing the security of cyberspace of critical infrastructure objects of Ukraine is extremely important due to the strengthening of cyber security threats in Ukraine. Objects of critical infrastructure of Ukraine, such as energy networks, transport systems, banking institutions, medical and military institutions, communication systems and others, are of great importance for the life and activity of the national economy and society as a whole. In particular, a failure in the operation of these facilities can lead to serious consequences, such as power outages, traffic stoppages, disruption of financial stability, disruption of medical services, etc. Under such conditions, protecting the cyberspace of critical infrastructure objects becomes an extremely important task for the state and business. To achieve this goal, it is necessary to have an effective methodology for assessing the security of cyberspace of critical infrastructure objects, which makes it possible to identify potential threats and risks, as well as to develop and implement measures to improve cyber security. The article provides theoretical explanations that connect the state's understanding of the principles of functioning of modern cyber threats and the search for mechanisms to solve them. It has been established that the provision of national (military) security is not yet carried out at the expense of the proper concept. According to the results of the assessment of the security of the cyberspace of critical infrastructure objects, practical ways of strengthening the military security of Ukraine through the search for an effective cyber security strategy have been determined.

Key words: *cyber-attack, cyber danger, cyber defense, minimization of the consequences of emergencies, investigation of the causes of emergencies.*

References

1. Mokhor, V., Gonchar, S., Dybach, O. (2019). Methods for assessing the overall risk of cybersecurity in critical infrastructure facilitiesю Nuclear and radiation safety, 2(82). DOI: https://doi.org/10.32918/nrs.2019.2(82).01. **2. Regulation (EU) 2019/881 of 17 April 2019** on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) № 526/2013 (Cybersecurity Act). Official Journal of the European Union. L 151/15, 7.6.20193. **3. Decree of the President of Ukraine** On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine", 447/2021. **4. Murasov, R. K., Melnyk, Y. V. (**2022). A probabilistic method of forecasting emergency events at potentially dangerous objects of critical infrastructure. Modern information technologies in the sphere of security and defense, 2(44), 60–64