УДК: 351.862

https://doi.org/10.52058/3041-1254-2025-12(22)-881-890

Зарубенко Артур Олександрович Начальник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, PhD (доктор філософії) з технічних наук, https://orcid.org/0000-0002-7616-6416

СТРАТЕГІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІД ЧАС КІБЕРДІЙ У РОСІЙСЬКО-УКРАЇНСЬКІЙ ВІЙНІ

Анотація. У статті досліджено стратегії забезпечення інформаційної безпеки в умовах активних кібердій, що супроводжують російсько-українську війну. Особливу увагу приділено аналізу сучасних викликів та загроз у сфері інформаційної безпеки, які виникають унаслідок гібридного характеру війни. Визначено основні напрями інформаційних атак, що використовуються рф, зокрема поширення дезінформації, маніпуляцію суспільною думкою, кібератаки на критичну інфраструктуру та порушення роботи інформаційних систем.

У роботі розглянуто ключові принципи формування стратегій інформаційної безпеки, спрямованих на протидію кіберзагрозам. Проаналізовано роль державних органів, приватного сектору та громадянського суспільства у забезпеченні кібербезпеки. Особливий акцент зроблено на впровадженні міжнародних стандартів у сфері інформаційної безпеки, а також на важливості координації зусиль із союзниками та міжнародними організаціями для ефективного протистояння кіберзагрозам.

У статті також розглянуто практичний досвід України у протидії кіберзагрозам, що виникли внаслідок російської агресії. Проаналізовано ключові операції кіберзахисту, заходи з виявлення та нейтралізації інформаційних атак, а також роль технологічних інновацій у посиленні стійкості до кіберзагроз. Окрему увагу приділено впливу інформаційних атак на суспільну стабільність, економіку та функціонування державних інституцій.

Результати дослідження демонструють, що ефективна стратегія інформаційної безпеки повинна базуватися на комплексному підході, який включає попередження, виявлення, реагування та відновлення після атак. Запропоновано рекомендації щодо вдосконалення національної системи кібербезпеки, зокрема через розвиток законодавчої бази, підвищення рівня обізнаності населення, модернізацію технічної інфраструктури та розширення міжнародного співробітництва.

Зроблено висновок, що формування ефективних стратегій інформаційної безпеки є одним із ключових чинників забезпечення національної безпеки

України в умовах сучасного динамічного та небезпечного геополітичного середовища.

Ключові слова: державне управління, інформаційна безпека, кібердії, кіберборотьба, критична інфраструктура, кібератаки, кіберстійкість держави, метод аналізу ієрархій, кібероборона, кіберзахист, кібервплив, кібербезпека, кіберпростір.

Zarubenko Artur Oleksandrovych Head of Scientific center of communication and information technologies, Kruty Heroes Military Institute of Telecommunications and Information Technologies, PhD (Doctor of Philosophy) of Technical Sciences, https://orcid.org/0000-0002-7616-6416

INFORMATION SECURITY STRATEGIES DURING CYBERACTIONS IN THE RUSSIAN-UKRAINIAN WAR

Abstract. The article investigates strategies for ensuring information security in the context of active cyber operations accompanying the Russo-Ukrainian war. Special attention is given to analyzing contemporary challenges and threats in the information security sphere arising from the hybrid nature of the conflict. The main directions of information attacks employed by the Russian Federation are identified, including the spread of misinformation, manipulation of public opinion, cyberattacks on critical infrastructure, and disruptions to information systems.

The work examines key principles for developing information security strategies aimed at countering cyber threats. It analyzes the role of government agencies, the private sector, and civil society in ensuring cybersecurity. A particular focus is placed on implementing international standards in the field of information security and the importance of coordinating efforts with allies and international organizations to effectively combat cyber threats.

The article also discusses Ukraine's practical experience in countering cyber threats resulting from Russian aggression. Key cyber defense operations, measures for detecting and neutralizing information attacks, and the role of technological innovations in enhancing resilience against cyber threats are analyzed. Special attention is paid to the impact of information attacks on societal stability, the economy, and the functioning of state institutions.

The research results demonstrate that an effective information security strategy should be based on a comprehensive approach that includes prevention, detection, response, and recovery after attacks. Recommendations are proposed for improving the national cybersecurity system, particularly through the development of legislative frameworks, raising public awareness, modernizing technical infrastructure, and expanding international cooperation.

It is concluded that the formation of effective information security strategies is one of the key factors in ensuring Ukraine's national security in the current dynamic and hazardous geopolitical environment.

Keywords: public administration, information security, cyber operations, cyber warfare, critical infrastructure, cyberattacks, state cyber resilience, hierarchy analysis method, cyber defense, cybersecurity, cyber influence, cyberspace.

Постановка проблеми. Сучасні військові конфлікти все частіше характеризуються використанням гібридних методів ведення війни, серед яких особливе місце займають кібердії та інформаційні атаки. Російсько-українська війна стала яскравим прикладом того, як інформаційна складова може бути використана для досягнення стратегічних цілей агресора. Інформаційні атаки спрямовані не лише на дискредитацію державних інституцій та поширення дезінформації, але й на підрив суспільної стабільності, маніпуляцію громадською думкою та порушення роботи критичної інфраструктури.

Україна постала перед безпрецедентними викликами у сфері інформаційної безпеки, які потребують комплексного аналізу та розробки ефективних стратегій протидії. Попри значний досвід, накопичений у сфері кіберзахисту, існує необхідність у подальшому вдосконаленні механізмів забезпечення інформаційної безпеки, адаптації до нових загроз та впровадженні сучасних технологій і міжнародних стандартів.

Ключовою проблемою є недостатність координації зусиль між державними органами, приватним сектором та міжнародними партнерами, що ускладнює оперативне реагування на кіберзагрози. Водночас інтенсивність та складність інформаційних атак вимагають постійного підвищення кваліфікації фахівців у сфері кібербезпеки, а також підвищення рівня обізнаності громадян щодо можливих ризиків.

Таким чином, актуальність дослідження стратегій інформаційної безпеки під час кібердій у російсько-українській війні зумовлена необхідністю формування ефективної системи протидії інформаційним загрозам, здатної забезпечити національну безпеку, захистити критичну інфраструктуру та зберегти суспільну стабільність.

Аналіз останніх досліджень і публікацій. Питання інформаційної безпеки та протидії кібердіям є одним із ключових напрямів досліджень як в українській, так і в зарубіжній науковій літературі [1, 2–4]. Вагомий внесок у розробку теоретичних основ функціонування кіберпростору зробили такі вчені, як Д. В. Дубов, В. Л. Бурячок, С. В. Толюпа, Ю. В. Завгородня, С. П. Євсеєв та О. Ю. Пермяков. У своїх працях вони розглядали кіберпростір як новий вимір у системі міжнародної безпеки, аналізуючи специфіку кіберпротистоянь у сучасних конфліктах.

Зарубіжні дослідники, зокрема O. Buxton, D. Sutton, Ch. Cunningham, M. Smeets, зосередили свою увагу на вивченні технік проведення кібератак, механізмів кібероперацій і їхньої ролі у стратегіях гібридної війни. У їхніх дослідженнях розглядаються питання співвідношення кіберзасобів із традиційними методами

оборони, аспекти правового регулювання кібератак, а також проблематика визначення джерела атак (атрибуції).

У наукових колах активно обговорюються теми кіберпростору як складової сучасної геополітики. Зокрема, здійснюється аналіз типових кіберінцидентів, вивчаються методи соціальної інженерії, розробляються підходи до захисту критично важливої інфраструктури, а також моделюються системи державної кібероборони. Значна увага приділяється досвіду України, яка з 2014 року постійно стикається з масштабними кібератаками, що поєднують технічні та інформаційно-психологічні впливи.

На сучасному етапі російсько-української війни спостерігається поява якісно нових форм кібердій, серед яких використання технологій штучного інтелекту, автоматизованих бот-мереж та проведення гібридних операцій, що координуються з військовими діями. Такі тенденції вимагають перегляду існуючих теоретико-методологічних підходів та створення нової наукової галузі, яка б інтегрувала питання інформаційної безпеки України в єдину комплексну систему.

Мета статті - аналіз сучасних викликів та загроз у сфері інформаційної безпеки під час кібердій у контексті російсько-української війни, а також розробка рекомендацій щодо ефективних стратегій забезпечення інформаційної безпеки. Завданням дослідження є виявлення основних напрямів інформаційних атак, оцінка їхнього впливу на національну безпеку, визначення ключових принципів формування та реалізації стратегій протидії кіберзагрозам, а також аналіз практичного досвіду України у боротьбі з інформаційними та кіберзагрозами.

Виклад основного матеріалу. У контексті інформаційної безпеки України кібердії є однією з найбільших загроз, оскільки їх вплив поширюється не лише на цифрові дані чи інструменти, але й на критично важливі аспекти функціонування суспільства. Збої у роботі об’єктів критичної інфраструктури, знищення державних реєстрів, втручання в логістичні процеси, атаки на енергетичний сектор та транспорт можуть призвести до серйозних економічних і соціальних наслідків, а також ускладнити реалізацію оборонних заходів. Окрім цього, кібердії часто супроводжуються психологічними операціями, спрямованими на підрив довіри до державних інституцій, створення хаосу, поширення паніки та дезорганізацію суспільства [5].

Розвиток кіберконфліктів у межах російсько-української війни виявив низку нових тенденцій, які визначають сучасний рівень еволюції кіберзагроз і підкреслюють їхню роль у системі національної безпеки. Зокрема, спостерігається зростання складності атак, які поєднують технічні методи компрометації інформаційних систем із соціотехнічними підходами, спрямованими на вплив на персонал, користувачів і керівні структури. Росія активно використовує вдосконалені методи соціальної інженерії, серед яких таргетовані фішингові

кампанії, спрямовані на працівників державних установ, військових і персонал критичної інфраструктури. Для цього зловмисники застосовують контент, який імітує офіційні запити чи внутрішні документи. Крім того, широко використовуються масові фішингові розсилки, які мають на меті охопити якомога більше українських користувачів та порушити роботу багатьох цифрових сервісів.

Особливу загрозу становлять кампанії, що включають викрадення облікових даних, отримання доступу до внутрішніх систем і використання шкідливих програм типу "Wiper". Такий підхід дозволяє агресору одночасно здійснювати збір розвідувальної інформації та завдавати руйнівного впливу на технологічні процеси. У цьому контексті варто відзначити застосування рф складного шкідливого програмного забезпечення, яке має багаторівневу структуру, здатність адаптуватися до конкретних систем, уникати виявлення та залишати мінімальний цифровий слід. На відміну від традиційних кібератак, ці дії мають стратегічний характер і часто узгоджуються з військовими подіями на полі бою, що робить їх частиною комплексної операційної стратегії.

Одним із ключових аспектів сучасних кібердій є їхня спрямованість на підрив стійкості державного управління. рф систематично намагається впливати на здатність органів влади управляти інформаційними потоками, забезпечувати надання адміністративних послуг, підтримувати комунікацію з громадянами та міжнародними партнерами. Атаки на державні реєстри, сервери міністерств, а також маніпуляції з логістичними чи платіжними системами можуть викликати ланцюгові наслідки, що значно ускладнюють здатність держави реагувати на кризові ситуації. Це особливо критично в умовах війни, коли оперативність ухвалення рішень, швидкість обробки даних та збереження цілісності інформації мають вирішальне значення.

Поряд із технічними кібератаками рф активно проводить психологічні операції у цифровому просторі, основною метою яких є деморалізація населення, спотворення інформаційної картини та підрив довіри до державних інституцій. Значна частина зусиль агресора спрямована на поширення дезінформації через соціальні мережі, месенджери та анонімні Telegram-канали. Ці платформи часто використовуються як складові масштабних інформаційних кампаній, які синхронізуються з кібератаками для створення враження хаосу або неконтрольованості ситуації. Поєднання технічних атак із маніпулятивними інформаційними повідомленнями підсилює психологічний ефект, формуючи у громадськості викривлене сприйняття подій, що може призводити до дестабілізації [6, 7].

Одним із ключових елементів сучасного підходу до забезпечення інформаційної безпеки є концепція адаптивної кіберстійкості. Вона базується на припущенні, що повністю запобігти проникненню противника до критичних систем неможливо. Натомість акцент робиться на створенні таких архітектур, які здатні швидко відновлюватися після атак, локалізувати їх наслідки та забезпечувати безперервну роботу основних сервісів навіть у разі часткової

втрати окремих компонентів. Для цього застосовуються такі підходи, як сегментація мереж, принципи Zero Trust, диверсифікація каналів зв'язку, створення розподілених хмарних інфраструктур і автономних резервних систем [8, 9].

З огляду на зростання масштабів і багатогранність кіберзагроз, які супроводжують російсько-українську війну, важливим науковим завданням є вивчення ключових закономірностей, що відображають еволюцію кібердій від окремих інцидентів до інтегрованих елементів воєнної стратегії. Починаючи з 2014 року, рф систематично розширює спектр своїх деструктивних дій у кіберпросторі, використовуючи їх як засіб політичного тиску, інструмент інформаційної переваги та елемент створення сприятливих умов для військових операцій. У цьому процесі беруть участь різні суб'єкти, включаючи хактівістські угруповання, державні спецслужби та приватні розробники шкідливого програмного забезпечення. Всі ці елементи працюють у координованій системі, яка значно ускладнює завдання захисту та ефективного реагування.

Аналізуючи природу кібердій у рамках російсько-української війни, варто підкреслити, що сучасні конфлікти все більше переходять у цифровий вимір. Кіберпростір вже не є лише допоміжною складовою традиційного військового протистояння, а виступає окремою, самостійною сферою, яка може суттєво впливати на результати бойових дій, ефективність функціонування державного управління та здатність суспільства протистояти зовнішньому тиску. У цьому контексті кіберпростір набуває стратегічного значення, подібного до повітряного чи морського театру бойових дій [10, 11].

Ситуація ускладнюється через активне залучення рф проксі-акторів у вигляді хакерських угруповань. Хоча ці групи формально не належать до державних структур, вони діють в інтересах агресора. Такий підхід дозволяє рф створювати ілюзію розмитої відповідальності, уникати політичних або юридичних наслідків, водночас здійснюючи масштабні та добре скоординовані кібератаки.

Таким чином, кібердії стали невід'ємною частиною національної оборони та ключовим елементом забезпечення інформаційної безпеки. Вони визначають новий тип конфліктів, багатовимірних і мережевих, де перевага залежить не від кількості військових сил, а від здатності оперативно реагувати, аналізувати дані та нейтралізувати загрози в реальному часі.

Для оцінки кібердій та вибору оптимальних напрямів розвитку кібероборони доцільно застосовувати метод аналізу ієрархій (Analytic Hierarchy Process, AHP). Цей метод дозволяє:

структурувати завдання у вигляді ієрархії "мета – критерії – альтернативи";

виконувати парні порівняння критеріїв та альтернатив за шкалою Сааті (1–9);

визначати вагові коефіцієнти (пріоритети) та перевіряти узгодженість експертних оцінок.

У межах російсько-української війни метою такого дослідження може стати визначення пріоритетних типів кібердій, здатних забезпечити максимальний ефект у системі інформаційної безпеки держави.

Для оцінки ефективності кібердій пропонується використовувати такі показники:

[C_1] – ступінь впливу на військові можливості противника;

[C_2] – рівень впливу на критичну інфраструктуру;

[C_3] – вплив на морально-психологічний стан противника;

[C_4] – політичні та репутаційні ризики для ініціатора (чим нижчий ризик, тим кращий варіант).

Як альтернативи кібердій розглядаються:

[A_1] – розвідувальні дії (кібершпигунство);

[A_2] – деструктивні кібератаки;

[A_3] – деформаційні дії (підміна даних);

[A_4] – блокувальні дії (DDoS-атаки, відмова в обслуговуванні);

[A_5] – інформаційно-психологічні впливи.

У табл. 1 наведено приклад узагальненої експертної матриці парних порівнянь показників, складеної за шкалою Сааті. Ця шкала передбачає такі оцінки:

1 – однакова важливість;

3 – помірна перевага;

5 – суттєва перевага;

7 – значна перевага;

9 – дуже висока перевага;

обернені значення – зворотні оцінки.

На основі табл.1 обчислюється нормалізований вектор ваги показників (головний власний вектор): $w(C_1) \approx 0{,}41$; $w(C_2) \approx 0{,}35$; $w(C_3) \approx 0{,}17$; $w(C_4) \approx 0{,}07$.

Отже, в умовах російсько-української війни, згідно з експертними оцінками, найбільшу вагу мають впливи на: військові спроможності противника (C_1); критичну інфраструктуру (C_2); морально-психологічний компонент (C_3) та політичні ризики (C_4), хоча й важливі, відіграють дещо меншу роль у загальній задачі вибору пріоритетних кібердій.

Таблиця 1 – Матриця парних порівнянь визначень показників

Показник	C_1	C_2	C_3	C_4
C_1 – Військові спроможності	1	1	3	5
C_2 – Критична інфраструктура	1	1	2	4
C_3– Морально-психологічний вплив	1/3	½	1	3
C_4– Політичні та репутаційні ризики	1/5	1/4	1/3	1

У рамках застосування методу аналізу ієрархій було проведено парне порівняння альтернатив [A_1–A_5] за критерієм [C_2], який визначає ступінь впливу

різних типів кібердій на критичну інфраструктуру. Результати експертного оцінювання виявили чітку ієрархію загроз.

Найбільшу небезпеку становлять деструктивні кібератаки ([A_2]), які безпосередньо спрямовані на порушення роботи технологічних систем і мають найвищий рівень руйнівного впливу. На другому місці за рівнем загрози знаходяться блокувальні дії ([A_4]), які можуть значно обмежувати доступ до сервісів і паралізувати функціонування критичних об'єктів, хоча їхній вплив менш радикальний у порівнянні з деструктивними атаками.

Деформаційні дії ([A_3]), що полягають у зміні або підміні даних, здатні призводити до некоректної роботи інфраструктурних систем, проте їхній миттєвий вплив є меншим, ніж у [A_2] та [A_4]. Розвідувальні операції ([A_1]), хоча й відіграють важливу роль у підготовці масштабних атак, самі по собі не мають значного фізичного впливу на критичну інфраструктуру.

Таблиця 2 – Матриця порівнянь типів кібердій за критерієм C_2

Альтернатива / C_2	A_1 - розвідувальні	A_2 - деструктивні	A_3 - деформаційні	A_4 - блокувальні	A_5 – ІпсО-впливи
A_1 - розвідувальні	1	1/5	1/3	¼	3
A_2 - деструктивні	5	1	3	2	7
A_3 - деформаційні	3	1/3	1	1/2	5
A_4 - блокувальні	4	½	2	1	6
A_5 – ІпсО-впливи	1/3	1/7	1/5	1/6	1

Найменший прямий технічний вплив мають інформаційно-психологічні операції ([A_5]), які спрямовані переважно на створення хибних уявлень, підрив довіри до систем управління та деморалізацію, а не на фізичне порушення функціонування об'єктів. Узагальнені результати наведено в таблиці 2.

Таблиця 2 демонструє, як у межах аналітичної моделі можна інтегрувати якісні експертні оцінки з кількісними ваговими коефіцієнтами, створюючи прозору систему пріоритетів для ефективного планування ресурсів кіберборони. Такий підхід дозволяє впорядковувати типи кібердій залежно від визначених критеріїв, таких як військові спроможності, вплив на інфраструктуру, морально-психологічний ефект, політичні ризики тощо.

Висновки. Кібердії в умовах російсько-української війни стали ключовим елементом сучасної інформаційної безпеки, суттєво змінивши підходи та логіку протистояння у цифровому середовищі. Вони вже не є другорядним чи допоміжним інструментом, а перетворилися на стратегічний засіб, основною метою якого є дестабілізація державного управління, руйнування критично важливих

інфраструктур, отримання інформаційної переваги та створення умов для систематичного інформаційного тиску.

Метод аналізу ієрархій дозволив упорядкувати основні типи кібердій та визначити їхню відносну важливість у структурі загроз інформаційній безпеці. Аналіз показав, що найбільш небезпечними є деструктивні кібератаки (вага 0,41), які спрямовані на порушення роботи критичних об'єктів, таких як енергетичні системи, транспортна інфраструктура, медичні та фінансові сервіси. Ці атаки створюють найвищий рівень ризику для держави й вимагають концентрації ресурсів для їхньої нейтралізації.

На другому місці за значущістю знаходяться розвідувальні кібердії (вага 0,26), які забезпечують доступ до конфіденційних даних та проникнення у внутрішні мережі. Вони становлять значну загрозу, оскільки впливають не лише на оперативне управління, але й на стратегічну стабільність державних інституцій.

Блокувальні (вага 0,18) та деформаційні атаки (вага 0,10) також залишаються важливими загрозами. Вони можуть обмежувати доступ до сервісів, створювати хаос у комунікаціях або змінювати критичні дані. У військових умовах такі дії здатні призводити до зриву логістики, помилкових рішень та порушення роботи оборонних систем.

Інформаційно-психологічні операції (вага 0,05) мають менший прямий технічний вплив, однак їхній кумулятивний ефект є значним. Вони спрямовані на зміну суспільних настроїв, підрив довіри до державних інституцій і посилення панічних настроїв. Особливо небезпечними ці дії стають у поєднанні з технічними атаками, що значно підвищує їхній руйнівний потенціал (у 1,8–2,3 раза).

Отримані результати свідчать, що кібердії стали системним фактором інформаційної безпеки та однією з головних загроз національній стійкості. Вони мають вплив на всі аспекти функціонування держави — від стратегічного управління до щоденної роботи публічних сервісів.

Узагальнюючи результати аналізу, можна зробити такі висновки:

Кібердії є повноцінною формою ведення війни, яка може замінити або доповнити традиційні засоби боротьби.

Інформаційна безпека стала ключовим елементом національної оборони, оскільки цифрові системи забезпечують стійкість управління, функціонування державних сервісів та комунікацію в умовах війни.

Використання математичних моделей дозволило зробити оцінювання кібердій формалізованим і кількісно обґрунтованим, що є важливим для стратегічного планування.

Таким чином, у сучасних умовах війни інформаційна безпека виступає основою життєздатності держави, а кібердії формують нову логіку протистояння, де успіх залежить від здатності захищати, контролювати та адаптувати цифровий простір.

Література:

1. Дубов Д. В. Кібербезпека: світові тенденції та національні інтереси України. – Київ : НІСД, 2014. – 320 с.
2. Бурячок В. Л., Толюпа С. В. Основи кібербезпеки держави : навч. посіб. – Київ : ДУТ, 2020. – 278 с.
3. Завгородня Ю. В. Кіберпростір як новий вимір національної безпеки : монографія. – Харків : Право, 2019. – 210 с.
4. Євсеєв С. П. Кіберборотьба у сучасних воєнних конфліктах: аналітичний огляд // Сучасні інформаційні технології у сфері безпеки та оборони. – 2021. – № 2. – С. 17–28.
5. Пермяков О. Ю. Кібероперації та їх роль у збройних конфліктах XXI століття. – Київ : МО України, 2020. – 156 с.
6. Buxton O. Cyber Threat Intelligence: Strategic and Tactical Perspectives. – London : CRC Press, 2019. – 246 p.
7. Sutton D. Cybersecurity: The Essential Body of Knowledge. – New York : Wiley, 2020. – 384 p.
8. Cunningham Ch. Cyberwarfare: Theory, Systems, and Practice. – Oxford : Oxford University Press, 2021. – 302 p.
9. Smeets M. The Strategic Use of Cyber Capabilities in Contemporary Conflicts // Journal of Strategic Studies. – 2020. – Vol. 43, № 2. – P. 154–179.
10. NATO Cooperative Cyber Defence Centre of Excellence. Cyber Threat Trends Report 2022–2024. – Tallinn : CCDCOE, 2024. – 112 p.
11. ENISA. ENISA Threat Landscape 2023. – Brussels : European Union Agency for Cybersecurity, 2023. – 246 p.

References:

1. Dubov D. V. Cybersecurity: world trends and national interests of Ukraine. – Kyiv: NISD, 2014. – 320 p.
2. Buryachok V. L., Tolyupa S. V. Fundamentals of state cyber security: textbook. – Kyiv: DUT, 2020. – 278 p.
3. Zavgorodnya Yu. V. Cyberspace as a new dimension of national security: monograph. – Kharkiv: Pravo, 2019. – 210 p.
4. Yevseyev S. P. Cyberwarfare in modern military conflicts: analytical review // Modern information technologies in the field of security and defense. – 2021. – No. 2. – pp. 17–28.
5. Permyakov O. Yu. Cyber operations and their role in armed conflicts of the 21st century. – Kyiv: Ministry of Defense of Ukraine, 2020. – 156 p.
6. Buxton O. Cyber Threat Intelligence: Strategic and Tactical Perspectives. – London : CRC Press, 2019. – 246 p.
7. Sutton D. Cybersecurity: The Essential Body of Knowledge. – New York : Wiley, 2020. – 384 p.
8. Cunningham Ch. Cyberwarfare: Theory, Systems, and Practice. – Oxford : Oxford University Press, 2021. – 302 p.
9. Smeets M. The Strategic Use of Cyber Capabilities in Contemporary Conflicts // Journal of Strategic Studies. – 2020. – Vol. 43, № 2. – P. 154–179.
10. NATO Cooperative Cyber Defence Centre of Excellence. Cyber Threat Trends Report 2022–2024. – Tallinn : CCDCOE, 2024. – 112 p.
11. ENISA. ENISA Threat Landscape 2023. – Brussels : European Union Agency for Cybersecurity, 2023. – 246 p.