DOI: 10.58254/viti.6.2024.11.146

УДК 004.946.5

канд. техн. наук Міхєєв Ю. І. ORCID: 0000-0002-6239-2324 (НУОУ)
Павленко М. М. ORCID: 0000-0002-1011-5042 (ЖВІ ім. С. П. Корольова)
Лобода В. В. ORCID: 0000-0002-3535-0233 (ЖВІ ім. С. П. Корольова)
Войтко Т. М. ORCID: 0000-0002-4326-0633 (НУОУ)

ВИМОГИ ДО ПЕРСПЕКТИВНОГО КІБЕРОЗБРОЄННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ

Аналіз досвіду виконання завдань відповідними підрозділами Сил оборони України під час відбиття широкомасштабної збройної агресії російської федерації проти України свідчить про те, що отримання переваги в кіберпросторі можливе лише за наявності власної сучасної кіберзброї. Завдання зі створення кіберзброї передбачає розроблення вимог до неї. Актуальність цього завдання також підтверджується зростанням кількості кібератак на військові об'єкти з боку російської федерації, що відображено у звітах оперативного центру реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України за останні роки. Отже, метою статті є дослідження існуючих шляхів створення сучасного кіберозброєння в інтересах Збройних сил України та висування вимог до нього.

У статті наведені результати аналізу застосування кіберзброї та тенденції щодо її розвитку. Розглянуто класифікацію кіберзброї за принципом її застосування. Запропоновано складові кіберозброєння Збройних сил України, які ґрунтуються на підставі аналізу тактики дій хакерських угруповань, інформаційних загроз, спрямованих на Україну з боку російської федерації.

У статті зазначаються об'єкти (цілі), які мають вражати перспективне кіберозброєння Збройних сил України з врахуванням його цільового призначення та завдань. Серед основних об'єктів кібервпливу визначені: критична інфраструктура держави противника; системи бойового управління, системи (мережі) зв'язку та автоматизації противника; системи (платформи) управління зброєю та військовою технікою противника; інформаційні та медіаресурси противника; окремі персони (посадові особи); групи осіб, верстви населення противника.

Надано системні та функціональні і нефункціональні вимоги до перспективного озброєння видів Збройних сил України. Запропоновані результати досліджень, у подальшому, можуть стати підґрунтям для розроблення відповідних оперативно-тактичних вимог до перспективного кіберозброєння видів Збройних сил України.

Ключові слова: *кіберозброєння, кібератака, Збройні сили України, шкідливе програмне забезпечення, озброєння та військова техніка, оперативно-тактичні вимоги.*

Y. Mikhieiev, M. Pavlenko, V. Loboda, T. Voitko Requirements for advanced cyber weapons of the Armed Forces of Ukraine

An analysis of the experience of the relevant units of the Ukrainian Defense Forces in repelling the large-scale armed aggression of the Russian Federation against Ukraine shows that gaining an advantage in cyberspace is possible only if Ukraine has its own modern cyber weapons. The task of creating cyber weapons involves the development requirements for them. The relevance of this task is also confirmed by the growing number of cyberattacks on military facilities by the russian federation, as reflected in the reports of the Cyber Incident Response Center of the State Center for Cyber Defense of the State Service for Special Communications and Information Protection of Ukraine in recent years. Thus, the purpose of the article is to study the existing ways of creating modern cyber weapons in the interests of the Armed Forces of Ukraine and to put forward requirements for them.

In the article, results are presented of the analysis process regarding cyber weapons use and trends in their development. Classification of cyber weapons by principle is considered. Components of cyber weapons in the Armed Forces of Ukraine are proposed, based on the analysis tactics by hacker groups and information threats directed at Ukraine by the russian federation.

The article specifies the objects (targets) that should be hit by the advanced cyber weapons of the Armed Forces of Ukraine, taking into account their purpose and tasks. The main objects of cyber influence include: critical infrastructure of the enemy state; combat control systems, communication and automation systems (networks) of the enemy; systems (platforms) for controlling enemy weapons and military equipment; information and media resources of the enemy; individuals (officials); groups of individuals, segments of the enemy population.

The systemic and functional and non-functional requirements for advanced weapons of the Armed Forces of Ukraine are presented. The proposed research results can further serve as a basis for the development of relevant operational and tactical requirements for advanced cyber weapons of the Armed Forces of Ukraine.

Keywords: *cyber weapon, cyberattack, malware, Armed Forces of Ukraine, operational and tactical requirements.*

Постановка проблеми у загальному вигляді. Результати аналізу досвіду з питань кібербезпеки, що отриманий під час російсько-української війни, свідчить про зростання значущості кіберпростору для досягнення цілей військових операцій [1]. Об'єктами кібератак, з боку противника, здебільшого стали вебресурси урядових установ, міністерств, Збройних сил (ЗС) України, банків та інші об'єкти критичної інфраструктури нашої держави [2]. Враховуючи наслідки, які були спричинені кібератаками на Україну, актуальним постає завдання з організації відповідних контрзаходів у кіберпросторі та розроблення кіберзброї, яка може бути використана не тільки для захисту власних інформаційних ресурсів, а й для впливу на об'єкти противника під час проведення кібероперацій.

Тому актуальним постає завдання зі створення кіберзброї, яке передбачає розроблення відповідних вимог до неї.

Аналіз останніх публікацій. На сьогодні питанню забезпечення кібербезпеки держави та об'єктів критичної інфраструктури приділяється значна увага. Тенденція до збільшення кількості наукових публікацій та аналітичних дайджестів, у цій галузі, свідчить про наявність актуальних проблемних питань, вирішення яких ґрунтується на отриманому практичному досвіді під час російсько-української війни [1–4]. Разом з тим, питанню особливостей створення та розвитку кіберозброєння, а саме розробленню вимог до нього з метою подальшого розроблення та застосування кіберозброєння підрозділами видів ЗС України, приділено недостатньо уваги. У цьому аспекті існують проблеми, пов'язані з визначенням дефініцій поняття "кіберзброї", що зумовлено із певним періодом її постійної модифікації.

Так у [4] автором розглядаються особливості застосування кіберзброї з врахуванням норм міжнародного права. Зазначається її призначення та вказується, що кіберзброя є засобом ведення кібервійни. Однак вимоги щодо її використання саме у ЗС України не зазначаються.

У Військовому стандарті ВСТ 01.114.001 − 2023 (01) "Електромагнітна та кіберборотьба. Глосарій термінів і визначень" подано визначення кіберзброї, в якому стисло вказується її призначення, але вимоги, щодо її розроблення та сфери подальшого використання при цьому не зазначаються [5].

У [6] авторами приділено увагу питанню сутності та призначення кіберзброї, класифікації, характеристикам, базовим принципам її побудови. Класифікувати кіберзброю пропонується за наступними базовими ознаками: призначення; масштабність застосування; характер вражаючої дії; спосіб доставки; керованість; деструктивний вплив; оперативність; місце базування; рівень маскування; спосіб виготовлення; спектр дії; об'єкти ураження; рівень впливу на об'єкти ураження; прицільні властивості; інтегральний ефект; тип зв'язків та рівень взаємодії; наслідки; принцип генерування; самоорганізація; тривалість ефекту; латентність. Запропоновані підходи ґрунтуються на певній аналогії із відомим зразком озброєння. За такий зразок було обрано ракетоносій. Такий підхід, на нашу думку, не в повній мірі дозволяє створити підґрунтя для розроблення вимог до сучасного кіберозброєння.

Отже, **метою статті** є обґрунтування вимог до перспективного кіберозброєння ЗС України, що мають містити опис його складу, призначення, об'єкти, на які воно має бути спрямоване.

Виклад основного матеріалу дослідження

Кіберзброя набула активного розвитку в США. Це пов'язано із підтримкою керівництвом країни програм розвитку обчислювальних мереж військового призначення Arpanet [3]. Відповідно до керівних документів НАТО дії в кіберпросторі розглядаються на тактичному та стратегічному рівнях. Основна відмінність проведення дій на тактичному чи

стратегічному рівні полягає у виборі об'єктів для здійснення кібервпливу. На тактичному рівні – можуть виконуватися завдання з ускладнення чи часткового призупинення діяльності обраних об'єктів (телекомпаній, операторів стільникового зв'язку, провайдерів Інтернету, відомих локальних обчислювальних мереж тощо). На стратегічному рівні основними об'єктами впливу виступають державні структури та критичні об'єкти інфраструктури держав. З огляду на аналіз зафіксованих фактів впливу на об'єкти критичної інфраструктури країн Близького Сходу в країнах НАТО було запропоновано основний вид кіберзброї – шкідливе програмне забезпечення (ПЗ) основу якого становить комп'ютерний вірус [9].

Для встановлення цільового призначення перспективного кіберозброєння ЗС України, пропонується розглянути підхід до здійснення кібератаки за моделлю Cyber Kill Chain, яка складається з таких етапів [10] (рис. 1)

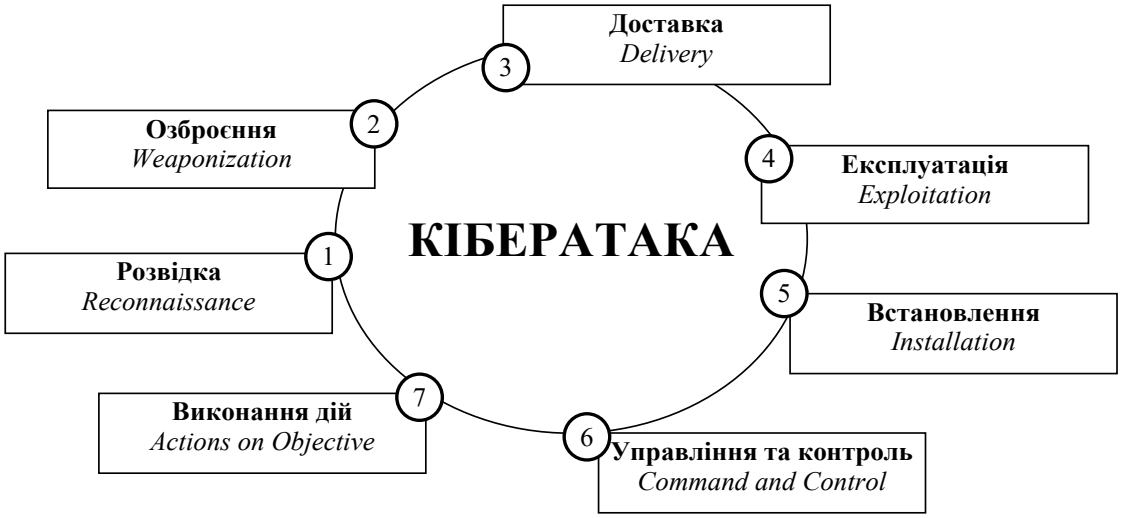

Рис. 1. Алгоритм здійснення кібератаки за моделлю Cyber Kill Chain

В алгоритмі здійснення кібератаки визначальними є етапи "розвідки" та "озброєння". На цих етапах визначаються вразливості об'єктів кібератак, проводиться підбір інструментарію, встановлюється механізм створення експлойтів та оснащення файлів шкідливим вмістом. Для максимального ефекту шкідливе ПЗ, яке створюється атакуючою стороною та застосовується під час кібератаки, має використовувати нові, раніше не виявлені вразливості (експлойти Zero-day). Враховуючи зазначене, пропонується таке цільове призначення перспективного кіберозброєння ЗС України:

збір інформації про об'єкти, на які планується здійснити вплив, під час проведення кіберрозвідки (несанкціонований доступ до інформації та даних);

виявлення уразливостей автоматизованих систем управління (АСУ) ЗС противника та інших об'єктів, які об'єднані комп'ютерною мережею;

вплив на визначені об'єкти ЗС противника (зміна, перешкодження або порушення функціонування інформаційних систем, здійснення кібератак, фішинг, розповсюдження вірусів, поширення дезінформації, вплив на громадську думку та маніпулювання подіями);

захист власних АСУ та персоналу від кібервпливу противника (запобігання атакам та забезпечення цілісності, конфіденційності та доступності інформації та ресурсів, ідентифікація потенційних ризиків та вразливостей в інфраструктурі, забезпечення сталого функціонування власних систем та інфраструктури).

Враховуючи цільове призначення та завдання, можна визначити такі об'єкти в якості цілей для перспективного кіберозброєння ЗС України:

критична інфраструктура держави противника;

системи управління військами (органи управління, системи зв’язку, інформаційні системи) видів та родів ЗС противника;

системи управління бойовими засобами противника;

інформаційні та медіаресурси противника;

окремі персони (посадові особи);

групи осіб, верстви населення противника;

тощо.

Пропонується об’єкти критичної інфраструктури держави противника, їх інформаційні та медіаресурси, верстви населення противника, розглядати цілями для усіх видів ЗС України. Основну відмінність для видів ЗС України будуть становити такі об’єкти (цілі):

елементи систем управління військами видів, родів, сфер діяльності ЗС противника (органи управління, системи зв’язку, інформаційні системи);

системи управління бойовими засобами противника зі складу систем управління військами;

окремі персони, посадові особи, що приймають рішення (групи осіб).

Окремими об’єктами впливу перспективного кіберозброєння, наприклад, Сухопутних військ (СВ) ЗС України, можуть бути:

1) системи управління СВ ЗС противника:

органи управління СВ ЗС;

системи зв’язку СВ ЗС;

інформаційні системи СВ ЗС;

2) системи управління бойовими засобами СВ ЗС противника:

системи дистанційного управління озброєнням та військовою технікою (ОВТ) СВ ЗС;

системи навігації ОВТ СВ ЗС;

канали телеметрії ОВТ СВ ЗС;

інші системи зі складу систем управління бойовими засобами, на які можливо здійснити вплив;

офіційні сайти СВ ЗС, акаунти соціальних мереж, електронні поштові скриньки особового складу СВ ЗС противника.

Для забезпечення виконання завдань з кіберрозвідки, кібервпливу, кіберзахисту, враховуючи цільове призначення, пропонується у складі перспективного кіберозброєння розглядати такі основні елементи: технічні засоби, програмне забезпечення та спеціальні програмні засоби впливу (шкідливе ПЗ) (рис. 2).

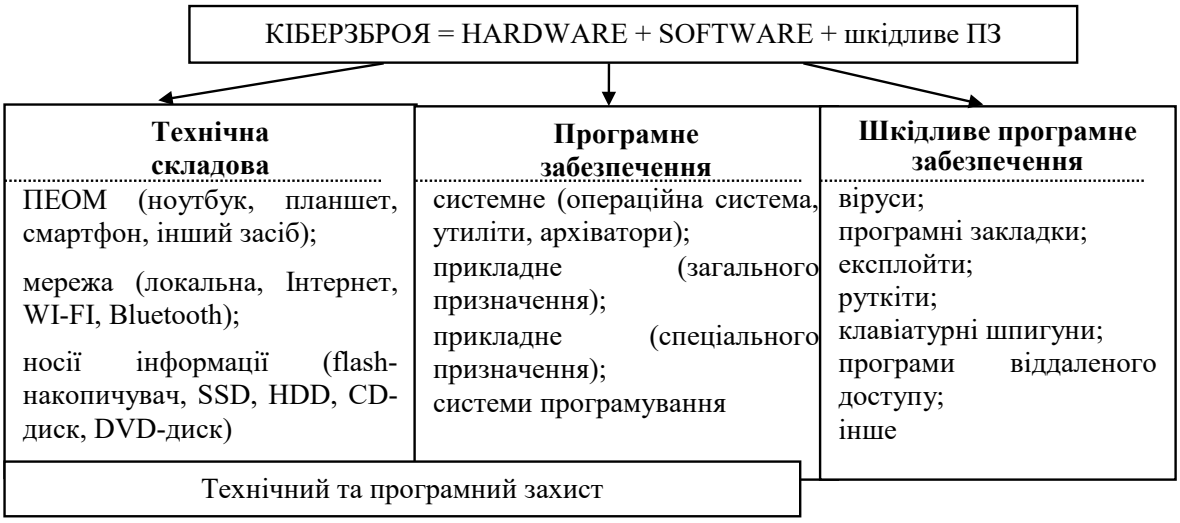

Рис. 2. Складові перспективного кіберозброєння

Запропонований склад перспективного кіберозброєння передбачає наявність універсальної структури та можливість використання для різних видів ЗС України. Відмінність буде полягати у формуванні складу шкідливого ПЗ, що визначатиметься об’єктами впливу.

До характеристик програмних компонентів кіберозброєння (SOFTWARE) пропонується віднести:

призначення;

принцип дії;

спосіб поширення;

обсяг файлу;

розмір програмного коду;

можливість самодублювання і самознищення;

алгоритм маскування;

тип операційної системи, яку здатен вражати бойовий програмний агент.

До характеристик апаратної частини кіберозброєння (HARDWARE) можна віднести системні вимоги: набір характеристик, яким повинен відповідати цифровий пристрій (обчислювальний засіб, комутаційний засіб, мобільний термінал); мережа або інформаційна система для коректної роботи програмного компонента перспективного кіберозброєння. Зазначені вимоги можуть описувати, як апаратне забезпечення, так і інше ПЗ (необхідні драйвери, операційна система тощо).

Під час розроблення вимог, слід розрізняти мінімальні та рекомендовані системні вимоги. Якщо мінімальні системні вимоги вказують, яка конфігурація системи цілковито необхідна для запуску ПЗ, то рекомендовані системні вимоги повинні вказувати на те, яка конфігурація здатна забезпечити повну функціональність кіберозброєння. Системні вимоги пропонується пов’язувати із такими характеристиками:

тип операційної системи, яка необхідна для запуску шкідливого ПЗ;

тип архітектури процесора, що виконує програмний код;

кількість дискового простору;

кількість оперативної пам’яті;

необхідність доступу до мережі (локальної або Інтернет);

наявність додаткових програмних та апаратних засобів, без яких функціонування шкідливого ПЗ неможливе.

Відповідно до специфікації Software Requirements Specification (SRS), які містять множину функціональних та нефункціональних (чи додаткових) вимог до ПЗ, пропонується визначити такі вимоги до перспективного кіберозброєння ЗС України [11]:

системні;

функціональні;

нефункціональні.

Системні вимоги:

використання сучасних ОС з останніми оновленнями безпеки;

використання апаратної архітектури x86-64 та ARM-архітектури (Advanced RISC Machine) як найбільш поширених;

підтримка багатопотоковості та розподіленості завдань з використанням багатоядерних процесорів;

застосування та підтримка сучасних інтерфейсів обладнання, інтерфейсів зв’язку та комунікацій;

підтримка можливості обміну даними через інтерфейси взаємодії (сучасні програмні інтерфейси);

можливість підключення до мережі, як за допомогою дротового способу, так і бездротовим дистанційним способом (наприклад, за допомогою пристрою Wi-Fi) із забезпеченням стабільного зв’язку з мережею за такими параметрами:

мінімальна пропускна здатність – 1 Мбіт/с;

рівень втрати цільових пакетів – не більше ніж 5% (1 пакетна втрата на 25 разів обміну пакетами);

рекомендована пропускна здатність – 100 Мбіт/с.

Прикладне ПЗ повинно базуватись на використанні вільно розповсюджувального ПЗ, яке не потребує придбання ліцензій. Також доцільно використовувати ПЗ, яке має відповідні ліцензії на використання.

Функціональні вимоги:

підтримка можливості розмежування прав доступу користувачів до відповідних функцій або системних ресурсів;

ергономічний та адаптивний інтерфейс, що забезпечує зручність і зрозумілість дій для оператора;

програмні компоненти повинні розроблятися за модульним принципом, тобто система складається з окремих модулів, кожен з яких реалізує певний набір функцій, притаманних виключно йому.

Передача інформації між складовими кіберозброєння має виконуватись стандартними протоколами на рівні ПЗ або на рівні платформи (системи керування базами даних, вебсерверів, тощо). У разі позаштатних ситуацій (аварій, відмов технічних засобів, зокрема, зникнення напруги, збоїв у роботі загальносистемного ПЗ, збоїв у роботі бази даних або інших технічних проблем) кіберозброєння повинне мати можливість відтворення своєї працездатності з резервних копій за короткий проміжок часу та з мінімальними втратами інформації.

Нефункціональні вимоги:

час готовності кіберозброєння до роботи – відповідно до інструкцій з експлуатації;

експлуатаційна документація повинна бути повна та достатня для забезпечення експлуатації, обслуговування кіберозброєння, виконана державною мовою.

Під час обміну інформацією між елементами кіберозброєння має бути забезпечено:

у незахищених каналах обміну даними – використання засобів криптографічного захисту інформації, які відповідають вимогам законодавства України у сфері криптографічного захисту інформації та забезпечують шифрування даних і взаємну автентифікацію сторін обміну даними;

у разі передачі інформації, що підлягає захисту відповідно до законодавства України у сфері захисту інформації (конфіденційної інформації (персональних даних, комерційної таємниці, державних інформаційних ресурсів тощо) до іншої системи – наявність у цій системі комплексної системи захисту інформації з підтвердженою у встановленому порядку відповідністю;

у разі необхідності формування та перевірки кваліфікованого електронного підпису на даних, обмін якими здійснюється використання засобів кваліфікованого електронного підпису чи печатки, які відповідають вимогам законодавства України у сфері електронних довірчих послуг.

Захист власних інформаційних ресурсів повинен реалізовуватися з використанням апаратних та програмних засобів захисту, що відповідають вимогам законодавства України у сфері захисту інформації, а також організаційних заходів, спрямованих на керування засобами захисту, регламентацію дій користувачів і контроль за цими діями. Кожен факт доступу до системи повинен зазначатись у протоколі доступу. Протокол доступу та протокол

дій оператора (log-файл) повинен бути доступний для перегляду та аналізу адміністратору системи, підрозділу, що відповідає за інформаційну безпеку.

Висновки і перспективи подальших досліджень

Отримані результати досліджень ґрунтуються на аналізі подій у кіберпросторі, які спостерігалися протягом 2014–2023 років під час російсько-української війни та відомостей, зазначених у звітах з питань кібербезпеки країн-членів НАТО. Це дало змогу визначити цільове призначення перспективного кіберозброєння, його склад, основні завдання та об'єкти (цілі) на які воно спрямовано.

Передбачається, що розроблення та застосування кіберозброєння, в інтересах ЗС України, буде пов'язано з такими особливостями:

низькою вартістю виробництва деяких складових елементів кіберзброї;

можливістю застосування кіберзброї з мінімальним рівнем ризику;

високою ефективністю кіберзброї в умовах використання противником АСУ;

масштабністю поширення кіберзброї;

комплексним використанням ключових можливостей кіберзброї для деструктивного впливу на об'єкти противника в кіберпросторі.

Тому, пропонується зосередити **подальші наукові дослідження** на обґрунтуванні оперативно-тактичних вимог кіберозброєння видів Збройних сил України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бойовий досвід з питань кібербезпеки отриманий під час російсько-української війни (аналіз та уроки). Частина перша (січень-травень 2022 року): збірник інформаційно-аналітичних матеріалів / С. А. Микусь, О. Й. Мацько, О. В. Войтко та ін. К.: НУОУ, 2022. 92 с.

2. Звіт оперативного центру реагування на кіберінциденти ДЦКЗ. URL: https://cip.gov.ua/ua/news/kilkist-zareyestrovanikh-kiberincidentiv-zrosla-na-46-zvit-operativnogo-centru-reaguvannya-na-kiberincidenti-dckz (дата звернення: 20.10.2023).

3. Зміна тактик, цілей і спроможностей хакерських груп уряду рф та контрольованих ним угруповань: прогнози. URL: https://cip.gov.ua/ua/news/zmina-taktik-cilei-i-spromozhnostei-khakerskikh-grup-uryadu-rf-ta-kontrolovanikh-nim-ugrupovan-prognozi (дата звернення: 20.02.2023).

4. Білюга А. Д. Кіберзброя: сучасні загрози національній безпеці та шляхи протидії. Наука і оборона. 2021. № 2. С. 42–49.

5. ВСТ 01.114.001 – 2023 (01). Вид. 1. "Електромагнітна та кіберборотьба. Глосарій термінів і визначень".

6. Даник Ю. Г. Воробієнко П. П., Чернега В. М. Основи кібербезпеки та кібероборони: підручник [Видання друге, перероб. та доп.]. Одеса: ОНАЗ ім. О. С. Попова, 2019. 320 с.

7. Arpanet. URL: https://www.quora.com/topic/ARPANET (дата звернення: 20.10.2023).

8. National Cybersecurity Strategy / The White House. Washington, 2023. URL: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (дата звернення: 20.03.2023).

9. Грищук Р. В. Кібернетична зброя: класифікація, базові принципи побудови, методи та засоби застосування й захисту від неї // Сучасна спеціальна техніка. Київ, 2016. № 3 (46). С. 94–101.

10. Cyber Kill Chain. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (дата звернення: 08.09.2023).

11. IEEE Std 830-1998 IEEE Recommended Practice for Software Requirements Specifications – Description. URL: https://ieeexplore.ieee.org/document/720574/definitions#definitions (дата звернення: 08.09.2023).