КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (17), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2022.17.3145

Байдур Олексій Володимировичович
аспірант кафедри комп'ютерних систем, мереж та кібербезпеки НУБіП України
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID ID 0000-0001-7036-1264
alexvb1981@gmail.com

ВДОСКОНАЛЕННЯ КІБЕРЗАХИСТУ ЗБРОЙНИХ СИЛ З УРАХУВАННЯМ ДОСВІДУ ПРОТИДІЇ ВІЙСЬКОВИМ КІБЕРОБЕРАЦІЯМ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ В 2022 РОЦІ

Анотація. у статті розглянуто можливості вдосконалення системи кібероборони Збройних Сил України та Міністерства оборони України відповідно до цілей і завдань визначених у рішеннях Ради національної безпеки і оборони України та Законів України. Здійснено огляд вимог нормативних документів з інформаційної та кібербезпеки України та аналогічних документів Сполучених Штатів Америки. Розглянуто алгоритм розбудови системи управління ризиками за напрямом інформаційної безпеки викладений у національних стандартах США. Наукова новизна роботи полягає в тому, що було запропоновано в процесі розбудови системи управління ризиками в інформаційно-комунікаційних системах (далі ІКС) Збройних Сил України та Міністерства оборони України створити автоматизовану систему підтримки рішень, що буде спиратися на спеціалізовану базу знань, здатну накопичувати досвід отриманий як під час проведення заходів кібероборони ІКС, так і під час здійснення кібервливів на ІКС противника. Здійснено огляд відкритих міжнародних способів стандартизації та відповідних баз знань, що можуть бути використані з метою актуалізації інформації про вразливості і контрзаходи в ІКС системах Потенційно спільно використання відкритих баз знань і спеціалізованої бази знань може створити нові можливості не тільки під час кібероборони, а і під час здійснення кібервпливів на ІКС противника, тому даний напрям дослідження є перспективним і відповідає національним інтересам України.

Ключові слова: кібероборона, контрзаходи, інформаційна безпека, кібербезпека, система управління ризиками, система підтримки прийняття рішень

ВСТУП

24 лютого 2022 року відбулася масштабна та багатовекторна кібератака з боку російської федерації на інформаційно-комунікаційні системи (далі — ІКС) Збройних Сил України. Саме в цей день можна було спостерігати дію широкого спектру наступальної кіберзброї російської федерації. В цілому цю російську кібератаку на ІКС Збройних Сил України можна оцінити, як таку, що мала частковий успіх. Детальна інформація про дії ворожої сторони та проведені контрзаходи в короткотерміновій перспективі не буде доступною для публічного обговорення, але вже зараз отриманий досвід можна використати для вдосконалення кібероборони Збройних Сил України.

Незважаючи на те, що протягом останніх років увага до проблем кібербезпеки в Україні значно зросла і був прийнятий ряд ключових нормативно-правових актів за цим напрямом, деякі системні проблеми в організації кіберзахисту інформаційно-комунікаційних системи Збройних Сил стали очевидними лише після початку відкритої фази агресії російської федерації в лютому 2022 року. Так, станом на початок 2022 року, за напрямом інформаційнішої безпеки в цілому та зокрема кібербезпеки в Збройних Силах були добре регламентовані питання організації технічного захисту інформації та частково моніторингу кіберінцидентів, але при цьому не приділялася достатня увага питанням захисту самої електронно-комунікаційної мережі, вибору оптимального

набору контрзаходів та превентивного тестування безпеки шляхом часткового моделювання дій зовнішніх зловмисників. Ця стаття — спроба започаткувати розробку нового комплексного підходу до вдосконалення системи кіберзахисту ІКС Збройних Сил з використанням кращих світових практик та набутого досвіду ведення активної протидії атакам російської федерації в кіберпросторі з другої половини 2021 року і по цей час.

На даний час в Україні існує багато перспективних наукових розробок та ведеться активна наукова робота над системами моніторингу [1] та розпізнавання кібератак [2]. Попри те, що праці цих учених мають значну наукову та практичну цінність, здійснене дослідження і отриманий в ході ведення активної кібероборони досвід дає підстави стверджувати, що чимало питань, пов'язаних із переходом від пасивної стратегії кібероборони до проактивної досі є дискусійними (недостатньо дослідженими). В умовах інтенсивного застосування противником кіберзброї в комбінації із активними військовими діями пасивна стратегія кібероборони в ІКС військового призначення є недостатньою, так само як і загальновійськова стратегія, що покладається виключно на оборонні дії — є очевидним шляхом зазнати поразку на полі бою. Досвід протидії сучасній військовій агресії, що відбувається одночасно в кіберпросторі та реальному світі, показав, що єдиним дієвим варіантом протидії є проактивна стратегія кібероборони, коли методи розпізнавання кібератак та моніторингу інцидентів кібербезпеки компонуються із заздалегідь розробленою деталізованою моделлю контрзаходів, що покривають весь спектр наслідків можливих кібератак та застосуванням методів оцінювання безпеки ІКС шляхом часткового моделювання дій зовнішніх і внутрішніх зловмисників із проникненням в систему. В цьому випадку практики застосовані при моделюванні атак, навички пошуку вразливостей отримані персоналом можуть бути застосовані в реальних умовах для атаки на ІКС противника.

В цій роботі буде застосований метод порівняльно-правового аналізу стандартів та методологій побудови комплексного кіберзахисту систем Сполучених Штатів Америки (далі - США) та нормативної-правової бази України щодо кібербезпеки. Проведено узагальнення опрацьованих матеріалів з метою формування пропозицій щодо доопрацювання нормативно-правової бази в Збройних Силах України та Міністерстві Оборони України та застосований діалектичний метод для первинного пошуку оптимальних шляхів переходу до стратегії проактивної кібероборони в ІКС Збройних Сил.

СУЧАСНИЙ СТАН НОРМАТИВНО-ПРАВОВОЇ БАЗИ УКРАЇНИ

Основними документами, що регламентують питання інформаційної безпеки є Закон України "Про захист інформації в інформаційно-комунікаційних системах" [3] де визначені ключові поняття віднесені до захисту інформації та встановлені повноваження державних органів у цій сфері та Закон України "Про основи національної безпеки України" [4] в якому питання інформаційної безпеки, кібербезпеки та кіберзахисту віднесені до питань національної безпеки.

Відповідно до вимог згаданих законів Указом Президента України від 26 серпня 2021 року № 447/2021 "Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" [5], була затверджена згадана Стратегія в якій, зокрема, визначені і такі завдання:

- створення національної системи управління інцидентами, розроблення та впровадження стандартних операційних процедур для реагування на різні види

подій у кіберпросторі з визначенням критеріїв для оцінки критичності подій та пріоритетності реагування залежно від визначеного рівня критичності;

- розроблення базових (визначатимуть мінімальний обов'язковий рівень) вимог та рекомендації з питань забезпечення кібербезпеки для державного і приватного секторів з урахуванням кращих світових практик.

За цим напрямом Україна вже має прийняті Національні стандарти з питань інформаційної безпеки, що аналогічні за змістом відповідним міжнародним стандартам, а саме:

- ДСТУ ISO/IEC 27000:2019 “Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник”;
- ДСТУ ISO/IEC 27001:2015 “Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги”;
- ДСТУ ISO/IEC 27002:2015 “Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки”;
- ДСТУ ISO/IEC 27005:2019 “Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки”;
- ДСТУ ISO/IEC TS 27008:2019 “Інформаційні технології. Методи захисту. Настанова щодо оцінювання захисту інформаційної безпеки”;

які прийняті наказами Державного підприємства "Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості" [6] та [7].

Водночас Законом України «Про внесення змін до деяких законів України щодо військових стандартів», який було прийнято Верховною Радою України 6 червня 2019 року [8], об’єкти військової стандартизації було виключено з під дії Закону України “Про стандартизацію”. Таке рішення законодавець обґрунтував тим, що загальний закон зокрема поширюється виняткова на стандарти, які стосуються товарів, виробничих процесів та способів виробництва, які можуть створювати технічні бар’єри у торгівлі. Водночас, військова стандартизація передбачає визначення військової термінології, вимог до систем документації, процесів та процедур управління, дії, взаємодії військового командування та органів військового управління. Об’єкти військової стандартизації є значно ширшими ніж об’єкти стандартизації, на які розповсюджується дія Закону України "Про стандартизацію".

Саме тому питання прийняття військового стандарту, аналогічно за змістом стандартам групи ДСТУ ISO/IEC 27000 із врахуванням вимог та специфіки військової стандартизації, є актуальним питанням, як і згадані вище завдання Стратегії кібербезпеки України щодо розроблення базових вимог та рекомендації з питань забезпечення кібербезпеки та стандартних операційних процедур для реагування на різні види подій у кіберпросторі за напрямом організації кіберзахисту ІКС військового призначення.

На виконання даного Закону Міністерством оборони України 24 лютого 2020 року було прийнято наказ № 56 «Про питання військової стандартизації» [9], яким затверджено як Положення про військову стандартизацію, так і Порядок розроблення, прийняття, внесення змін, скасування, відновлення дії, оприлюднення , запровадження та застосування військових стандартів.

Також варто зазначити що питання кібербезпеки від січня 2019 року відповідним рішенням уряду було покладено на Міністерство оборони України, а саме доповненням до Положення про Міністерство оборони України ще одним пунктом: “117-1) відповідно до компетенції вживає заходів до забезпечення інформаційної безпеки, кібербезпеки та кіберзахисту, а також підготовки держави до відбиття воєнної агресії у кіберпросторі

(кібероборони)"[10]

Отже, можна зробити висновок що зміни внесені до нормативних актів за останні три роки зумовили необхідність перегляду структури, підходів, регулювання та впровадження стандартів, водночас враховуючи чітку позицію держави щодо наближення до вимог НАТО.

СВІТОВІ ПРАКТИКИ РЕГУЛЮВАННЯ ПИТАНЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗА ПРИКЛАДОМ НОРМАТИВНО-ПРАВОВОЇ БАЗИ США

Як зазначено у статті [11] до стандартів інформаційної безпеки зосереджених на проблемах безпеки відносяться такі документи, як серія ISO 27000, ISF SOGP, серія NIST 800, SOX та Risk IT. Автори статті [12] також відзначають стандарти групи National Institute of Standards and Technology (далі - NIST), як такі що містять найбільш детально описані показники, спрямовані на вимірювання різних атрибутів безпеки, включаючи вразливості, атаки, витрати та ймовірнісні показники. Враховуючи, що розробки групи NIST також спрямовані на автоматизацію процесів безпеки, далі будуть розглядатися національні стандарти інформаційної безпеки США, як провідної країни світу, що є ключовим безпековим партнером України, та як такі, що мають найбільш детально описані процедури побудови кібероборони на рівні держави. Провідну роль США в розробці стандартів за напрямом інформаційної безпеки визнають автори багатьох профільних наукових публікацій світу.

Основі засади системи інформаційної безпеки були визначені в Законі про електронне врядування США 2002 року № 107-347 [13]. Також в цьому законі було визначено NIST як організацію, що:

1. Основною місією якої є розробка стандартів, настанов, відповідних методик та інструкцій для інформаційних систем;
2. Розробка стандартів та настанов, включаючи мінімальні вимоги, для операційних систем, що використовуються та впроваджуються агенціями або їх підрядниками, або іншими організаціями від імені агенцій, які не використовуються в системах пов'язаних із національною безпекою;
3. Розробка стандартів, настанов, що включають мінімальні вимоги для достатню інформаційну безпеку для всіх операцій та активів агенцій, але ці стандарти та настанови не застосовуються для систем пов'язаних із національною безпекою.

В 2014 році з метою впровадження реформи в Федеральну інформаційну безпеку були прийняті зміни до згаданого закону. Ці зміни отримали окрему назву, як Federal Infration Security Modernization Act of 2014 (далі — FISMA) [14].

Перше завдання встановлене згаданим федеральним законом, а саме завдання розробити стандарти для категоризації інформації та інформаційних систем було реалізовано за допомогою публікації Federal information processing standards publication (скорочена назва - FIPS) 199 Standards for Security Categorization of Federal Information and Information Systems [15]. Пропоновані виданням стандарти категоризації безпеки для інформації та інформаційних систем забезпечують загальну структуру та розуміння для вираження безпеки, що, з точки зору федерального уряду США, сприяє ефективному управлінню та нагляду за програмами інформаційної безпеки, включаючи координацію зусиль у сфері інформаційної безпеки в цивільних системах, системах національної безпеки, готовності до надзвичайних ситуацій та правоохоронних органів, а також послідовному звітуванню Адміністративно-бюджетному управлінню США (Office of Management and Budget - OMB) і Конгресу США про адекватність і ефективність політики, процедур і практики інформаційної безпеки.

Документом FIPS 200 Minimum Security Requirements for Federal Information and Information Systems [16] були оприлюднені федеральні стандарти щодо категоризації безпеки федеральної інформації та інформаційних систем на основі цілей забезпечення відповідних рівнів інформаційної безпеки відповідно до низки рівнів ризику та мінімальних вимоги безпеки для інформації та інформаційних систем у кожній такій категорії. Ця публікація стосується специфікації мінімальних вимог безпеки для федеральної інформації та інформаційних систем.

В системах національної безпеки США (National Security System, далі - NSS) застосовуються інструкції прийняті Комітетом систем національної безпеки (Committee on National Security Systems - CNSS), зокрема інструкція - Categorization and control selection for National Security Systems № 1253 від 29 липня 2022 року [17]. Ця інструкція ґрунтується на наступних документах:

1. NIST Special Publication (SP) 800-37 Revision 2, Risk Management for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy [18], в якому описується структура управління ризиками (Risk Management Framework, далі - RMF) і надаються вказівки щодо застосування RMF до інформаційних систем і організацій. RMF забезпечує дисциплінований, структурований і гнучкий процес управління ризиками безпеки та конфіденційності, який включає категоризацію інформаційної безпеки; відбір, реалізацію та оцінку контролю; систему та повноваження здійснення загального контролю; постійний моніторинг;
2. NIST SP 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations [19], який містить каталог заходів безпеки та конфіденційності для інформаційних систем і організацій, що призначені захисту операцій в організаціях та їх активів, окремих осіб та нації в цілому від різноманітних загроз і ризиків, що включають ворожі атаки, людські помилки, стихійні лиха, структурні невдачі, дії органів іноземної розвідки та ризики конфіденційності.
3. NIST SP 800-53B, Control Baselines for Information Systems and Organizations [20], що представляє базові показники безпеки та контролю конфіденційності для федерального уряду. В ній викладені три базові рівні контролю безпеки (по одному для кожного рівня впливу на систему — низький, помірний і сильний), а також базовий рівень конфіденційності, який застосовується до систем незалежно від рівня впливу.

При цьому між Інструкцією CNSSI № 1253 і згаданими вище стандартами NIST є наступні відмінності:

- Інструкція не використовує концепцію високорівневих позначок (HWM — high-water mark) із стандарту FIPS 200;
- зв’язки конфіденційності, цілісності та/або доступності засобів контролю в базових лініях NSS чітко визначені в додатку D цієї Інструкції;
- використання контрольних накладень, як визначено в додатку E цієї Інструкції, та узгоджується зі стандартом NIST SP 800-53B, але є специфічним для завдань національної безпеки;
- базовий рівень контролю конфіденційності NSS представляє засоби контролю конфіденційності, необхідні агентству для управління ризиками конфіденційності підприємства;
- засоби керування, специфічні для систем, які створюють, збирають, використовують, обробляють, зберігають, підтримують, поширюють, розкривають або позбавляються конфіденційної інформації, було вилучено з базового рівня

контролю конфіденційності NIST та включено до окремого розділу Privacy Overlays;

- таблиці у Додатку D включають стовпець «Міркування щодо впровадження конфіденційності», який визначає засоби контролю, не включені в базову лінію контролю конфіденційності NSS, але якщо такі засоби контролю запроваджено, вони можуть створювати ризики для конфіденційності, а тому вимагають координації з уповноваженими особами.

Серед розроблених NIST Computer security Division документів існує загальний огляд під назвою Summary of NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations [21], в якому надана послідовність впровадження процедури управління ризиками в інформаційній системи (в тому числі із посиланням на CNSS Instruction № 1253). Зазначена вище процедура наведена на Рис. 1

Короткий огляд документів FISP 199, FISP 200, NIST SP800-37, NIST SP800-53 та CNSS Instruction № 1253 вже був наведений вище, тому наведемо аналогічну інформацію по іншим згаданим у Рис. 1 стандартам:

4. NIST SP 800-60 Volume I Revision 1: Guide for Mapping Types of Information and Information [22], який містить основні вказівки щодо віднесення типів інформації та інформаційних систем до категорій безпеки;
5. NIST SP 800-60 Volume II Revision 1: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories [23], який містить додатки до першого тому, включаючи рекомендації щодо категоризації безпеки для типів інформації, що базуються на розумінні місії, та обґрунтування рекомендацій щодо категоризації безпеки.
6. NIST SP 800-160 Volume I: Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems [24], розглядає інженерну перспективу та дії, необхідні для розробки більш надійних і живучих систем, включаючи машинні, фізичні та людські компоненти, які складають системи, а також можливості та послуги, що надаються цими системами. Вона починається з набору добре встановлених міжнародних стандартів системної та програмної інженерії, опублікованих Міжнародною організацією зі стандартизації (ISO), Міжнародною електротехнічною комісією (IEC) та Інститутом інженерів з електротехніки та електроніки (IEEE). впроваджує методи, практики та прийоми інженерної безпеки систем у ці системи та діяльність з розробки програмного забезпечення;
7. NIST SP 800-53A Revision 5, Assessing Security and Privacy Controls for Information Systems and Organizations [25], де наведено методологію та набір процедур для проведення оцінки засобів контролю безпеки та конфіденційності, які застосовуються в системах і організаціях у рамках ефективного управління ризиками;
8. NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations [26], що визначає безперервний моніторинг інформаційної безпеки (Information security continuous monitoring — ISCM), як підтримку постійної обізнаності про інформаційну безпеку, вразливості та загрози для підтримки організаційних рішень щодо управління ризиками та описує шляхи впровадження подібного моніторингу.

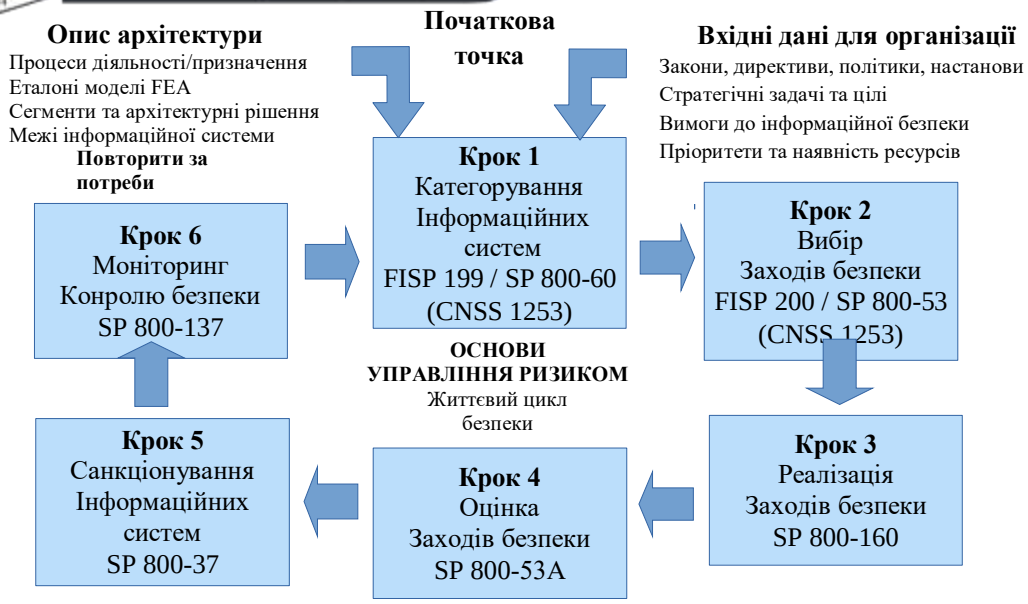

Рис. 1. Основи управління ризиками

В третій частині статті був проведений загальний огляд ключових нормативно-правових документів, що стосуються інформаційної безпеки в США і розглянуто рекомендовану послідовність впровадження системи управління ризиками в федеральних та системах національної безпеки США. В наступному розділі будуть розглянуті пропозиції щодо початкових кроків розбудови системи кібероборони Збройних Сил України із врахуванням як досвіду США, так і досвіду відсічі агресії російської федерації у кіберпросторі проти України.

ПРОПОЗИЦІЇ ЩОДО ПОЧАТКОВИХ КРОКІВ РОЗБУДОВИ СИСТЕМИ КІБЕРОБОРОНИ ЗБРОЙНИХ СИЛ УКРАЇНИ

Першим кроком в процесі розбудови системи управління ризиками в ІКС має бути Категорування інформаційних систем, що відповідає підходу запропонованому на Рис. 1. Категорування відбувається за наявності всіх необхідних вхідних даних, та є добре описаним в наведених на малюнку стандартах США. Вимоги до захисту інформації та класифікація інформації, що обробляється у військових ІКС України вже визначені у відповідних нормативно-правових документах Державної служби спеціального зв'язку та захисту інформації України та Міністерства оборони України та частково мають обмеження доступу. Питання категорування інформаційних систем не є проблемним, з точки зору впровадження системи управління ризиками інформаційної безпеки, тому слід переходити до другого кроку.

Другий крок, а саме - вибір заходів безпеки, є визначальним, та впливає на систему захисту в цілому. Цей крок є цікавим для проведення ґрунтовного дослідження, так як в України, на даний час, не існує військових стандартів, які визначають порядок проведення подібних заходів. Особливістю даного кроку саме у військовій сфері є те, що під час військових дій та агресії у кіберпросторі у кіберпросторі підрозділи відповідальні за кібероборону мають вести постійну боротьбу як проти ворожих кібердій [12], так і боротися із загрозами системам ІКТ з боку агентів, що можуть діяти маючи внутрішній доступ. Тобто, особливу загрозу можуть становити ті, хто має привілейований доступ до мереж і активів певної системи [27]. У такому сценарії вирішальне значення має вибір оптимальних контрзаходів для протидії вищезгаданим кіберзагрозам, спрямований на

забезпечення найбільш ефективного, але з найменшим негативним впливом виправлення [11]. Ключовою у цьому напрямку є роль експертів з безпеки, оскільки вони відповідають за балансування згаданого компромісу між ефективністю та наслідком контрзаходів, завжди маючи справу з обмеженими ресурсами. Їхнє знання безпеки є необхідним для вибору правильних дій із відновлення та оперативного реагування під час кібератак, спрямованих на зниження загального ризику, якому піддається система [28]. Крім того, у військовій екосистемі, правильний вибір контрзаходів вимагає організувати взаємодії з метою отримання узагальненої інформації про кіберситуацію, що має на меті забезпечити швидке реагування, ефективне застосування захисних можливостей та підтримку прийняття рішень для кінцевих користувачів військових ІКТ [29].

Протягом останніх років в Україні було докладено значних зусиль для стандартизації та початку розбудови систем, що пов'язані з інформаційною безпекою, але питанням щодо розробки єдиного стандарту представлення інформації про вразливості, слабкі місця та атаки, даних розвідки, що оточує поле протидії, приділялося значно менше уваги. Як зазначено в статті [30], однією із значних проблем в екосистемі, що відповідальна за розробку заходів протидії є відсутність стандартного представлення контрзаходів разом із відсутністю спільної бази знань про можливі варіанти виправлення наслідків кібератаки. Введення стандартного представлення контрзаходів та частково закритої бази знань, що має на меті узагальнити досвід, як і під час здійснення заходів протидії ворожим кібератакам, так і під час тестуванням кіберзахищеності системи. База знань повинна включати в себе результати застосування власної кіберзброї проти систем противника. Враховуючи особливість застосування і військове призначення накопичених знань подібна база знань повинна бути захищеною відповідним грифом обмеження доступу. При розробці за основу можна використати вже існуючи приклади подібних баз цивільного призначення. Однієї із спроб створити базу знань заходів відновлення працездатності ІКТ систем цивільного призначення був проєкт common remediation enumeration - CRE, з невідомих причин закритий у 2011 році [12]. Автори роботи [11] зібрали в таблицю відомі стандарти безпеки (таблиця 1), розділивши їх на різні категорії. Більшість записів у таблиці 1 знайшли відображення у документах NIST та MITRE ATT&CK глобально доступної бази знань про тактику та прийоми дій противника у кіберпросторі, що заснована на реальних спостереженнях.

Таблиця 1

Спроби стандартизації для автоматизації заходів безпеки

Категорія	Акронім	Назва	Опис
Управління активами	AI	Asset identification	Метод унікальної ідентифікації активів і вказівки щодо використання ідентифікації активів
	ASR	Asset summary report	Модель даних для вираження транспортного формату підсумкової інформації про один або кілька наборів активів
	ARF	Asset reporting format	Модель даних для вказівки транспортного формату інформації про активи та зв'язки між активами та звітами
	CPE	Common platform enumeration	Стандартизований метод для опису та визначення класу додатків, операційних систем і апаратних пристроїв, наявних у

			обчислювальних активах підприємства
Таксономія атак	ATT&CK	MITRE ATT&CK	Знання тактики та прийомів противника на основі реальних фактів
	CAPEC	Common attack pattern enumeration and classification	Загальнодоступний каталог типових шаблонів атак, класифікованих інтуїтивно зрозумілим способом
Управління конфігурацією	CCE	Common configuration enumeration	Надає унікальні ідентифікатори проблем конфігурації системи для швидкого й точного співвіднесення даних конфігурації з кількох джерел інформації
	CCSS	Common configuration scoring system	Набір заходів серйозності проблем конфігурації безпеки програмного забезпечення
Обмін інформацією про кіберзагрози та аналіз	CybOX	Cyber Observable eXpression	Стандартизована мова для кодування та передачі високоточної інформації про кібер-спостереження, нещодавно інтегрована зі STIX
	OpenIOC	Open Indicator Of Compromise	Розширювана XML-схема, яка дозволяє описувати технічні характеристики, які ідентифікують докази компрометації
	STIX	Structured Threat Information eXpression	Спільні зусилля спільноти для визначення та розробки мови для представлення структурованої інформації про загрози
	TAXII	Trusted Automated eXchange of Indicator Information	Відкритий транспортний механізм, який стандартизує автоматизований обмін інформацією про кіберзагрози
	TMSAD	Trust model for security automation data	Загальна модель довіри, яку можна застосувати до специфікації в домені автоматизації безпеки
Управління подіями	CEE	Common event expression	Спроба стандартизувати опис, представлення та обмін записами подій між електронними системами розроблена спільнотою
Управління інцидентами	IDMEF	Intrusion detection message exchange format	Формати даних і процедури обміну для обміну інформацією, яка становить інтерес для IDS/IPS і систем управління
	IODEF	Incident object description exchange format	Представлення даних, яке забезпечує основу для обміну інформацією, якою зазвичай обмінюються групи реагування на інциденти комп'ютерної безпеки (CSIRT) про інциденти комп'ютерної безпеки
Керування шкідливими програмами	MAEC	Malware attribute enumeration and characterization	Стандартизована мова для кодування та передачі високоточної інформації про зловмисне програмне забезпечення на основі таких атрибутів, як поведінка, артефакти та шаблони атак
Інформація про санацію	CRE	Common remediation enumeration	Набір специфікацій санації, який забезпечує автоматизацію та розширену кореляцію дій із виправлення
	ERI	Extended remediation information	Словник із додатковими даними про кожен CRE, включаючи посилання на CPE, CVE та

			CCE
Тест безпеки	OCIL	Open checklist interactive language	Інформаційна структура для подання користувачам питань, пов'язаних із безпекою, і відповідні процедури для інтерпретації результатів
	OCRL	Open checklist reporting language	Мова для написання визначень XML, які збирають інформацію з систем і представляють її як стандартизований звіт для оцінки відповідності політикам
	OVAL	Open vulnerability and assessment language	Світова спільнота інформаційної безпеки намагається стандартизувати спосіб оцінки та звітування про стан машини комп'ютерної системи
	XCCDF	EXtensible Configuration Checklist Description Format	Мова специфікацій на основі XML для написання контрольних списків безпеки, тестів і пов'язаних документів
Гарантія програмного забезпечення	CMSS	Common misuse scoring system	Набір заходів, що описують наслідки неправильного використання функцій програмного забезпечення (припущення довіри, зроблені під час розробки функцій програмного забезпечення, зловживаних для порушення безпеки)
	CWE	Common weakness enumeration	Спільна мова для обговорення, пошуку та усунення причин вразливостей безпеки програмного забезпечення, виявлених у коді, дизайні чи архітектурі системи
	CWRAF	Common weakness risk analysis framework	Частина проекту обліку загальних слабких місць (CWE). Він забезпечує основу для оцінки слабких місць програмного забезпечення
	CWSS	Common weakness scoring system	Механізм визначення пріоритетів виправлення слабких місць програмного забезпечення послідовним, гнучким і спільним способом
	SWID	Software identification tagging	Частина ISO/IEC 19770-2:2015 забезпечує організаціям прозорий спосіб відстеження програмного забезпечення, встановленого на їхніх керованих пристроях
Управління вразливістю	CVE	Common vulnerabilities and exposures	Еталонний метод для загальновідомих вразливостей і ризиків
	CVRF	Common vulnerability report format	Мова на основі XML, яка дозволяє різним зацікавленим сторонам у різних організаціях обмінюватися важливою інформацією, пов'язаною з безпекою, в одному форматі
	NVD	National Vulnerability Database	Репозиторій уряду США стандартизованих даних про управління вразливістю, представлених за допомогою SCAP

Крім того, слід зазначити, що контрзаходи військового призначення повинні враховувати оперативну інформацію, необхідну для військового Cyber Situational Awareness - CSA (обізнаність про кіберситуацію) та належну підтримку прийняття рішень Mission-level Courses of Action - M-CoA (курси дій на рівні місії) та/або Cyber Courses of Action - C-CoAs (кіберкурси дій) [31]. Військова доктрина НАТО щодо планування операцій уже містить визначення CoA для проведення спільних операцій союзників (наприклад, Спільна доктрина НАТО щодо планування операцій [32]). Тому слід планувати також розробку відповідної системи підтримки прийняття рішень, щоб було можливо оцінити потенціал кібероборони під час проведення оборонного огляду на основі об'єктивних математичних показників [3]. Загальна оцінка кібероборони залежить від багатьох критеріїв, що мають подальший розподіл на підкритерії. Створення подібної системи можливе і для цього використовуються методи описані в теорії multiple-criteria decision-making problem — MCDM (Багатокритеріальне прийняття рішень), яка використовується при необхідності підтримати рішення за умови наявності багатьох суперечливих критеріїв.

Вимоги вибору метрики для критерів за напрямом інформаційна безпека описані у документі NIST SP800-55 Revision 1 Performance Measurement Guide for Information Security [33]. В цьому документі NIST представив свою таксономію показників безпеки, описуючи три категорії (керівні, технічні та операційні показники) і саме ці показники можуть бути використані при проєктувані та розробці згаданої вище автоматизованої системи підтримки прийняття рішень.

На основі викладеного сформулюємо пропозицію щодо початкових кроків розбудови системи кібероборони Збройних Сил України. Вибір заходів безпеки при створенні системи управління ризиками за напрямом інформаційна безпека в ІКТ Збройних Сил України має здійснюватися на основі системи, що забезпечить вибір оптимальних контрзаходів протидії, як ворожим кібердіям, так і загрозам ІКТ системам з боку агентів, що можуть діяти маючи внутрішній доступ. Зазначена система використовує базу знань, що узагальнює досвід отриманий, як і під час здійснення заходів протидії ворожим кібератакам, так і під час тестування кіберзахищеності системи. Також система здійснює підтримку прийняття рішень, яка здатна оцінити потенціал кібероборони на основі об'єктивних математичних показників математичних засобів. Вибір метрики критеріїв здійснюється за основі єдиного стандарту, що має бути розроблений із використанням досвіду провідних країн світу.

ВИСНОВКИ

В роботі розглянуті основні нормативно правові акти, що визначають вимоги до інформаційної безпеки як в України, так і В сполучених Штатах Америки. Нормативні акти України за напрямом інформаційної безпеки лише формуються і значна низка питань ще не отримала належного регулювання. В Збройних Силах України та Міністерстві оборони України, станом на момент написання цієї статті, відсутній повний комплект стандартів за напрямом інформаційна безпека, в той самий час сфера оборони держави виведена за межі дії загальнонаціональних стандартів з інформаційної безпеки. США, як провідна країна світу в галузі безпеки інформації, мають детально описану процедуру побудови системи управління ризиками за напрямом інформаційна безпека. Ця процедура викладена у відповідних національних документах, в тому числі і за напрямом національної безпеки США, до якої належать питання оборони держави.

Якщо брати досвід США, то визначальним кроком для побудови дієвої системи управління ризиками за напрямом інформаційна безпека в Україні має стати вибір

заходів безпеки. У статті запропоновано почати розбудову системи кібероборони Збройних Сил України із визначення заходів безпеки на основі автоматизованої системи, що забезпечить вибір оптимальних контрзаходів протидії ворожим кібердіям, так і загрозам ІКТ системам з боку агентів, що можуть діяти маючи внутрішній доступ та сформульвоні шляхи створення подібної системи.

СПОСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Лахно, В., Терещук, А., Петренко, Т. (2016). Совершенствование киберзащиты информационных систем за счет адаптивных технологий распознавания кибератак. *Захист інформації*, *18*(2), 99-106.
2 Beketova, G., Akhmetov, B., Korchenko, A., Lakhno, A. (2016). Design of a model for intellectual detection of cyber-attacks, based on the logical procedures and the coverage matrices of features. *Ukrainian Scientific Journal of Information Security*, *22*(3), 242-254.
3 Закон України “Про захист інформації в інформаційно-комунікаційних системах” зі змінами від 15 червня 2022 року. https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.
4 Закон України “Про національну безпеку України” зі змінами від 16 листопада 2021 року. https://zakon.rada.gov.ua/laws/show/2469-19#Text
5 Указ Президента України від 26 серпня 2021 року № 447/2021 "Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України". https://www.president.gov.ua/documents/4472021-40013
6 Наказ Державного підприємства "Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості" від 18 грудня 2015 року № 193. https://zakon.rada.gov.ua/rada/show/v0193774-15#Text
7 Наказ Державного підприємства "Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості" від 16 жовтня 2019 року № 312. https://zakon.rada.gov.ua/rada/show/v0312774-19#Text
8 Закон України «Про внесення змін до деяких законів України щодо військових стандартів» від 6 червня 2019 року. https://zakon.rada.gov.ua/laws/show/2742-19#Text
9 Наказ Міністерства оборони України «Про питання військової стандартизації» № 56 від 24 лютого 2020 року. https://www.mil.gov.ua/content/nakaz_moy/56_nm.pdf
10 Постанова Кабінету міністрів України №1 від 10 січня 2019 року. https://ips.ligazakon.net/document/KP140671?an=9
11 Nespoli, P., Marmol, F., Vidal, J. (2021). Battling against cyberattacks: towards pre-standardization of countermeasures. *Cluster Computing*, *24*, 57–81
12 Calton, J. (2017). *Evaluation of the 2015 dod cyber strategy: mild progress in a complex and dynamic military domain.* Strategic Studies Institute, US Army War College.
13 Public Law 107–347 107th Congress, E-Government Act of 2002. https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf
14 Public Law No: 113-283 113th Congress, Federal Information Security Modernization Act of 2014. https://www.congress.gov/bill/113th-congress/senate-bill/2521/text
15 FIPS PUB 199. Standards for Security Categorization of Federal Information and Information Systems. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf
16 FIPS PUB 200. Minimum Security Requirements for Federal Information and Information Systems. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf
17 CNSS № 1253 Categorization and control selection for National Security Systems 29 July 2022. https://www.cnss.gov/CNSS/issuances/Instructions.cfm
18 NIST SP 800-37 Rev. 2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
19 NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
20 NIST SP 800-53B Control Baselines for Information Systems and Organizations https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf
21 Dempsey, K., Witte, G., & Rike, D. (2014). *Summary of NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations*. National Institute of Standards and Technology. https://doi.org/10.6028/nist.cswp.02192014

22 Stine, K., Kissel, R., Barker, W., Fahlsing, J., Gulick, J. NIST SP 800-60 Vol. 1 Rev. 1 Guide for Mapping Types of Information and Information Systems to Security Categories. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf

23 Stine, K., Kissel, R., Barker, W., Fahlsing, J., Gulick J. NIST SP 800-60 Vol. 2 Rev. 1 Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf

24 Ross, R, McEvilley, M., Oren, J. NIST SP 800-160 Vol. 1 Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf

25 NIST SP 800-53A Rev. 5 Assessing Security and Privacy Controls in Information Systems and Organizations. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar5.pdf

26 Dempsey, K., Chawla, N., Johnson, L., Johnston, R., Jones, A., Orebaugh, A., Scholl, M., Stine, K. NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

27 Kaur, J., Ramkumar, K. (2022). The recent trends in cyber security: A review. Journal of King Saud University. *Computer and Information Sciences, 34*(8), 5766-5781

28 Standley, V., Nuno1, F., Sharpe, J. (2020). Fusing attack detection and severity probabilities: a method for computing minimum-risk war decisions. *Computing, 102*, 1385–1408.

29 Bhol, S., Mohanty, J., Pattnaik, P. (2020). *Cyber security metrics evaluation using multi-criteria decision-making approach.* Smart Intelligent Computing and Applications.

30 Chowdhury, N., Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review, 40*, 100361

31 Rizwan, A. (2016). Cyber Situational Awareness for the NATO alliance. *The Three Swords Magazine 30,* 72-75.

32 Ministry of Defence. (2019, 23 липня). *Allied Joint Doctrine for the Planning of Operations (AJP-5).* GOV.UK. https://www.gov.uk/government/publications/allied-joint-publication-ajp-05a-allied-joint-doctrine-for-the-planning-of-operations.

33 Chew, E., Swanson ,M., Stine, K., Bartol, N., Brown, A., Robinson, W. NIST SP 800-55 Rev. 1 Performance Measurement Guide for Information Security. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (17), 2022
ISSN 2663 - 4023

Baidur Oleksii
graduate student of the Department of Computer Systems, Networks and Cyber Security of the Ukrainian National University of Science and Technology
National University of Bioresources and Nature Management of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0001-7036-1264
alexvb1981@gmail.com

IMPROVEMENT OF THE CYBER PROTECTION OF THE ARMED FORCES TAKING INTO ACCOUNT THE EXPERIENCE OF COUNTERING MILITARY CYBER ATTACKS OF THE RUSSIAN FEDERATION IN 2022

Abstract. The article considers the possibilities of improving the cyber defense system of the Armed Forces of Ukraine and the Ministry of Defense of Ukraine in accordance with the goals and objectives defined in the decisions of the National Security and Defense Council of Ukraine and the Laws of Ukraine. A review of the requirements of normative documents on information and cyber security of Ukraine and similar documents of the United States of America was carried out. The considered algorithm for developing a risk management system in the direction of information security is outlined in the USA national standards. The scientific novelty of the work is that in the process of developing the risk management system in the information and communication systems (ICS) of the Armed Forces of Ukraine and the Ministry of Defense of Ukraine, it was proposed to create an decision support system that will be based on a specialized knowledge base capable of accumulating experience both during cyber-defense measures of the ICS and during the implementation of cyber-influences on the ICS of the enemy. An overview of open international standardization methods and relevant knowledge bases that can be used to update information on vulnerabilities and countermeasures in IC systems was carried out. The joint to use of open knowledge bases and specialized knowledge bases potentially can create new opportunities not only during cyber defense, but also during the implementation of cyber influences on the ICS of the enemy, therefore, this direction of research is promising and corresponds to the national interests of Ukraine.

Keywords: cyber defense, countermeasures, information security, cyber security, risk management system, decision support system.

REFERENCES

1 Lakhno, V., Tereshchuk, A., Petrenko, T. (2016). Improving the cyber protection of information systems due to adaptive technologies for the recognition of cyber attacks. Information Protection, 18(2), 99-106.
2 Beketova, G., Akhmetov, B., Korchenko, A., Lakhno, A. (2016). Design of a model for intellectual detection of cyber-attacks, based on the logical procedures and the coverage matrices of features. Ukrainian Scientific Journal of Information Security, 22(3), 242-254.
3 Law of Ukraine "On Protection of Information in Information and Communication Systems" as amended from June 15, 2022. https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.
4 Law of Ukraine "On National Security of Ukraine" as amended from November 16, 2021. https://zakon.rada.gov.ua/laws/show/2469-19#Text
5 Decree of the President of Ukraine dated August 26, 2021 No. 447/2021 "On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cyber Security Strategy of Ukraine". https://www.president.gov.ua/documents/4472021- 40013
6 Order of the State Enterprise "Ukrainian Research and Training Center for Standardization, Certification and Quality Problems" dated December 18, 2015 No. 193. https://zakon.rada.gov.ua/rada/show/v0193774-15#Text
7 Order of the State Enterprise "Ukrainian Research and Training Center for Standardization, Certification and Quality Problems" dated October 16, 2019 No. 312. https://zakon.rada.gov.ua/rada/show/v0312774-19#Text
8 Law of Ukraine "On Amendments to Certain Laws of Ukraine Regarding Military Standards" dated June 6, 2019. https://zakon.rada.gov.ua/laws/show/2742-19#Text
9 Order of the Ministry of Defense of Ukraine "On issues of military standardization" No. 56 of February 24, 2020. https://www.mil.gov.ua/content/nakaz_moy/56_nm.pdf
10 Resolution of the Cabinet of Ministers of Ukraine No. 1 dated January 10, 2019.

https://ips.ligazakon.net/document/KP140671?an=9

11 Nespoli, P., Marmol, F., Vidal, J. (2021). Battling against cyberattacks: towards pre-standardization of countermeasures. *Cluster Computing, 24*, 57–81

12 Calton, J. (2017). *Evaluation of the 2015 dod cyber strategy: mild progress in a complex and dynamic military domain.* Strategic Studies Institute, US Army War College.

13 Public Law 107–347 107th Congress, E-Government Act of 2002. https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf

14 Public Law No: 113-283 113th Congress, Federal Information Security Modernization Act of 2014. https://www.congress.gov/bill/113th-congress/senate-bill/2521/text

15 FIPS PUB 199. Standards for Security Categorization of Federal Information and Information Systems. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

16 FIPS PUB 200. Minimum Security Requirements for Federal Information and Information Systems. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

17 CNSS № 1253 Categorization and control selection for National Security Systems 29 July 2022. https://www.cnss.gov/CNSS/issuances/Instructions.cfm

18 NIST SP 800-37 Rev. 2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

19 NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

20 NIST SP 800-53B Control Baselines for Information Systems and Organizations https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf

21 Dempsey, K., Witte, G., & Rike, D. (2014). *Summary of NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations*. National Institute of Standards and Technology. https://doi.org/10.6028/nist.cswp.02192014

22 Stine, K., Kissel, R., Barker, W., Fahlsing, J., Gulick, J. NIST SP 800-60 Vol. 1 Rev. 1 Guide for Mapping Types of Information and Information Systems to Security Categories. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf

23 Stine, K., Kissel, R., Barker, W., Fahlsing, J., Gulick J. NIST SP 800-60 Vol. 2 Rev. 1 Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf

24 Ross, R, McEvilley, M., Oren, J. NIST SP 800-160 Vol. 1 Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf

25 NIST SP 800-53A Rev. 5 Assessing Security and Privacy Controls in Information Systems and Organizations. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar5.pdf

26 Dempsey, K., Chawla, N., Johnson, L., Johnston, R., Jones, A., Orebaugh, A., Scholl, M., Stine, K. NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

27 Kaur, J., Ramkumar, K. (2022). The recent trends in cyber security: A review. Journal of King Saud University. *Computer and Information Sciences, 34*(8), 5766-5781

28 Standley, V., Nuno1, F., Sharpe, J. (2020). Fusing attack detection and severity probabilities: a method for computing minimum-risk war decisions. *Computing, 102*, 1385–1408.

29 Bhol, S., Mohanty, J., Pattnaik, P. (2020). *Cyber security metrics evaluation using multi-criteria decision-making approach.* Smart Intelligent Computing and Applications.

30 Chowdhury, N., Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review, 40*, 100361

31 Rizwan, A. (2016). Cyber Situational Awareness for the NATO alliance. *The Three Swords Magazine 30*, 72-75.

32 Ministry of Defence. (2019, 23 липня). *Allied Joint Doctrine for the Planning of Operations (AJP-5).* GOV.UK. https://www.gov.uk/government/publications/allied-joint-publication-ajp-05a-allied-joint-doctrine-for-the-planning-of-operations.

33 Chew, E., Swanson ,M., Stine, K., Bartol, N., Brown, A., Robinson, W. NIST SP 800-55 Rev. 1 Performance Measurement Guide for Information Security. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf