http://doi.org/10.51707/2618-0529-2024-29-03
УДК 004.56.53

О. М. Башкиров,
О. П. Крушеницький,
А. Ю. Дмитренко

НОВІТНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ДЛЯ ПІДГОТОВКИ ФАХІВЦІВ КІБЕРОБОРОНИ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ

Анотація. *За останні роки спецслужби росії продемонстрували, що спроможні подолати заходи безпеки навіть добре захищених компаній і урядових мереж по всьому світу, зокрема систему безпеки військової бази США на острові Гуам. За оцінками Служби безпеки України нині росія здійснює близько 10 кібератак на Україну щоденно. Тому підготовка фахівців із кібернетичної безпеки для нашої держави, особливо для сфери сектору безпеки і оборони, є нагальним і актуальним завданням. Організація надійної системи інформаційної безпеки об'єктів критичної інфраструктури є суттєвим елементом оборонної стратегії будь-якої країни. Згідно зі Стратегією воєнної безпеки України, яка затверджена Указом Президента України від 25 березня 2021 р., серед заходів з надійної оборони України окремим пріоритетом є нарощування спроможностей Збройних сил України, Сил територіальної оборони, інших складових сил оборони щодо виконання покладених завдань. Одним із напрямів практичної реалізації цього пріоритету має бути виконання певних завдань з розвитку спроможностей щодо забезпечення кібербезпеки, кіберзахисту та кібероборони, відбиття агресії в кіберпросторі під час підготовки та ведення всеосяжної оборони України. Крім цього, Закон України «Про освіту» визначає, що інформаційно-комунікаційна компетентність є однією з ключових компетентностей сучасної людини. Тому стаття присвячена актуальній темі покращення організації підготовки керівного складу Міністерства оборони України в галузі забезпечення кібернетичної безпеки держави. За прикладом деяких закладів вищої освіти України запропоновано створити кіберполігон на базі Національного університету оборони України для підготовки фахівців кібероборони для ЗСУ та проведення з ними кібернавчань. У статті аналізуються завдання кіберполігона і розробляються пропозиції стосовно його функціональної структури.*

Ключові слова: *кібернетична оборона, навчання фахівців кібербезпеки, кіберполігон.*

Постановка проблеми. Як повідомляли спецслужби США у 2020 р., Служба зовнішньої розвідки росії довела, що спроможна подолати заходи безпеки навіть добре захищених компаній і урядових мереж по всьому світу, коли використала модуль безпеки SolarWinds для проникнення в ланцюжки поставок програмного забезпечення для десятків тисяч цілей по всьому світу [1]. Це був аналог більш агресивного вірусу NotPetya 2017 р., коли російські хакери завдали збитків у розмірі мільярдів доларів компаніям по всьому світу від використання програми-вимагача, застосовуючи ушкоджене програмне забезпечення для оформлення фінансово-економічних документів.

Також відомо, що і кіберзлочинці з Китаю провели хакерську атаку з кодовою назвою «Hafnium» на початку 2021 р. Для цього вони використали чотири «вразливості нульового дня», тобто неусунені вразливості системи облікових записів електронної пошти Microsoft Exchange для збору інформації з пріоритетних

серверів, скомпрометувавши понад 30 000 серверів тільки в Сполучених Штатах і сотні тисяч по всьому світу. З цією метою Пекін багато років аналізував інформацію, проводив кібероперації і накопичував досвід проведення кібератак по всьому світу. Кіберстратегія Пентагону попереджає, що Пекін готовий здійснити кібератаки на критично важливу інфраструктуру й оборонні мережі в разі початку війни. Альянс із обміну розвідданими Five Eyes, до якого належать Австралія, Канада, Нова Зеландія, Великобританія та США, у травні 2023 р. заявив, що китайська шпигунська група подолала систему кібернетичного захисту військової бази на Гуамі та в інших підрозділах армії США, що було виявлено компанією «Microsoft» та ідентифіковано з групою, відомою як Volt Typhoon [2].

Практика останнього десятиріччя переконливо доводить, що побудова системи безпеки об'єктів критичної інфраструктури є суттєвим елементом оборонної стратегії будь-якої країни [3].

Найбільш розвинені країни світу створили кібернетичну спільноту країн-однодумців для узгодження дій у сфері кібернетичного захисту критично важливих інформаційних ресурсів. Для цього був розроблений проєкт «Google Project Shield» для захисту новинних, правозахисних та спостережних організацій від потужних атак на кшталт «відмова в обслуговуванні» державних установ. Із початком прямої військової агресії росії у 2022 р. цей проєкт почав надавати безкоштовні послуги Україні. Інші компанії, які запропонували допомогу Києву, мають аналогічні програми, які, з одного боку, допомагають забезпечити кібернетичну безпеку народу України, а з іншого — сприяють посиленню кіберзахисту всіх учасників кіберальянсу. Наукові, дослідницькі, виробничі установи й армія США активізували обмін розвідданими про кіберзагрози з мережевими захисниками в Україні, допомагаючи зупинити деякі з найгірших кібератак росії з метою позбавлення доступу до критично важливих інформаційних послуг [4].

Актуальність дослідження. Згідно зі статтею 12 Закону України «Про освіту» інформаційно-комунікаційна компетентність визначена однією з ключових компетентностей [5]. Питання кібербезпеки є важливими складниками цієї компетентності й відображають загальні підходи, сформульовані в Рамках цифрової компетентності для громадян ЄС [6]. Навіть більше, під час упровадження концепції віддаленого доступу до інформаційних ресурсів закладів вищої освіти виникає низка завдань, які необхідно вирішити в процесі забезпечення інформаційної та кібернетичної безпеки: запобігання несанкціонованому доступу до приміщень закладу та його локальної мережі; виконання вимог і рекомендацій чинної політики інформаційної та кібербезпеки; контроль підключених до корпоративної мережі пристроїв на предмет відповідності чинній політиці; логічний поділ корпоративної мережі на зони безпеки без зміни наявної інфраструктури тощо [7].

Одна з основних причин наявності недоліків в організації протидії дезорганізації роботи інформаційних систем і телекомунікаційних мереж та порушенню функціонування критично важливих об'єктів полягає в «незадовільному кадровому забезпеченні відомств відповідними фахівцями у сфері інформаційної безпеки», як наголошується в аналітичній доповіді Національного інституту стратегічних досліджень при Президентові України на тему «Кібербезпека: світові тенденції та виклики для України» [8]. Отже, нині найбільшу кіберзагрозу для вітчизняних установ і відомств становить відчутна нестача фахівців сфери інформаційної та кібернетичної безпеки. Тому питання підготовки фахівців кібербезпеки і набуття відповідних спроможностей Міністерства оборони України є не тільки актуальними для підтримання інформаційної та кібербезпеки власне закладів військової освіти України, а й дуже важливими для підготовки військових фахівців сфери кібероборони.

У серпні 2023 р. на конференції «AFCEA TechNet» у Джорджії посадові особи Збройних сил США наголосили на важливості підготовки службовців до протистояння та протидії кіберзагрозам і необхідності проведення навчань щодо можливостей кіберборотьби навіть для вищого військового керівництва, а також порадили, щоб національні навчальні центри дедалі частіше охоплювали такі теми, як наступальна кібернетика, т. зв. інформаційна перевага та електронна війна [9]. Військове керівництво США наполягає на тому, що раннє і безперервне навчання має вирішальне значення для ознайомлення з кіберпростором та безпечного його використання в майбутньому. Тому в США розробляється навчальна

ISSN 2786-4510 (Online)

програма для вивчення сфери захисту даних та цифрової грамотності, яка стане частиною професійної військової освіти кожного військового. Вже тепер завданням кіберцентру у Форт-Гордоні є підготовка і розвиток висококваліфікованих фахівців кібервійськ, інформатизації та радіоелектронної боротьби. Наприкінці серпня 2023 р. розпочалися курси з підвищення кваліфікації командування армії США у сфері кібероборони.

У грудні 2023 р. в Естонії країни НАТО завершили одні з найважливіших навчань «Кіберкоаліція 2023» (Cyber Coalition) для покращення кібербезпеки, запросивши на них Південну Корею та Японію, оскільки офіційні особи альянсу шукають уряди-однодумці для зміцнення свого колективного віртуального захисту [10]. Україна також взяла участь у наймасштабніших за всю історію навчань НАТО з кіберзахисту [11]. Навчання у столиці країни Таллінні були зосереджені на обміні розвідданими про погрози та реагування на сценарії кібератак на національну критично важливу інфраструктуру, а також на цілі та структури військового характеру.

Отже, цей досвід є важливим і для впровадження в Збройних силах України. Зокрема, за час відсічі збройній агресії росії кількість кібератак зросла в декілька разів порівняно з попередніми роками, наприклад: від 24 лютого 2022 р. зафіксовано понад 4500 кібератак, у 2020 р. їх було всього 800, а у 2021 — близько 2000. Як повідомляє українське інтернет-видання «Лівий берег» з посиланням на слова голови Служби безпеки України Василя Малюка, щоденно росія здійснює в середньому по 10 кібератак на Україну [12]. Саме тому підготовка спеціалістів із кібербезпеки є своєчасним, важливим і актуальним питанням з точки зору підготовки військових фахівців.

Мета статті — на підставі аналізу досвіду деяких закладів вищої освіти України розробити пропозиції стосовно покращення підготовки військових фахівців сфери кібероборони та проведення з ними кібернавчань.

Результати досліджень. Нині готовність керівного складу Міністерства оборони України до протидії кібератакам можна оцінити як «умовно задовільну». Причиною цього є слабка обізнаність військових, насамперед оперативного та стратегічного рівня, стосовно особливостей проведення кібератак та недостатність навичок для оперативного реагування на них, тому що регулярних тренувань для оволодіння прийомами протидії таким атакам у військах не проводиться. Попри те, що нині комп'ютери в ЗС України є майже на кожному робочому місці, питаннями кібероборони займається тільки вузьке коло спеціалістів нижньої та середньої ланки управління, решта володіє тільки початковими знаннями в цій сфері. Відсутність повноцінного моніторингу інформаційних небезпек і кібератак у військових частинах та органах військового управління призводить до неможливості подальшого розслідування кібернетичного інциденту. Саме для покращення цієї ситуації доцільно проаналізувати досвід певних закладів освіти України з підготовки фахівців з кібероборони і розробити пропозиції щодо покращення підготовки військових спеціалістів цієї сфери. Відомо, що з метою підготовки фахівців сфери кібероборони в деяких закладах освіти України почали створювати кіберполігони. З точки зору функціонального призначення кіберполігон — це віртуальна лабораторія, де спеціалісти мають можливість реалізувати мережеві атаки і здійснювати їх відбиття, виявляти вразливості й відпрацьовувати свої дії в умовах, максимально наближених до реальних атак.

Зокрема, такий кіберполігон функціонує на кафедрі кібербезпеки та інформаційних технологій Харківського національного економічного університету імені Семена Кузнеця [13]. Розгортання кіберполігона на базі університету має за мету відпрацювання студентами, дослідниками та спеціалістами тактик відбиття кібератак на об'єкти критичної інфраструктури, а також симуляції кібератак з одночасним відпрацюванням методик кібернападів. Відпрацювання кібернетичних дій здійснюється в замкненому віртуальному середовищі, яке не має виходу в інтернет. Головним елементом кіберполігона є програмне забезпечення та системи віртуалізації, за допомогою яких відбувається моделювання кібератак на комп'ютерні мережі. Це дає можливість зменшити (або унеможливити) витрати на придбання ресурсів хмарних обчислень та зайве залучення пропускної здатності загальних комунікаційних каналів щодо виконання завдань роботи кіберполігона.

Своєю чергою, навчальний кіберполігон дасть змогу імітувати кібернапади на інфраструктуру серверів, що є доцільним для пошуку

вразливих місць та налагодження кращої системи захисту своїх ресурсів. У процесі підготовки бакалаврів відпрацьовуються механізми протидії сучасним загрозам на основі вебтехнологій та вебзастосунків. На другому (магістерському) рівні підготовки здобувачів освіти ці навички застосовуються під час відпрацювання практичних дій для забезпечення мережевої та хмарної безпеки, мобільної безпеки та безпеки серверних систем.

Для вдосконалення навичок студентів спеціальності «Кібербезпека» в Хмельницькому національному університеті також функціонує віртуальна лабораторія — кіберполігон [14]. За допомогою кіберполігона студенти мають можливість самостійно реалізовувати мережеві атаки й оволодівати навичками їх відбиття, виявляти вразливості програмного забезпечення, відновлювати уражену інфраструктуру і досліджувати механізми подолання наслідків кібервпливів та відновлення системи після атак, особливості життєвого циклу шкідливого програмного забезпечення та інші питання кібербезпеки. На рис. 1 показана структура цього кіберполігона.

Кіберполігон має у своєму складі три ділянки (зони згідно з термінологією [15]): на ділянці 1 (недовірена зона) розгорнута локальна мережа АРМ користувачів, що здійснюють навчання; на ділянці 2 (довірена, але вразлива зона) — сервер доступу до інформаційних ресурсів і сервер управління віртуальними комп'ютерами; ділянка 3 (довірена зона) містить робочі станції адміністраторів кіберполігона, а також ізольовані експериментальні сервери, до яких відсутній доступ із зовнішнього інформаційного простору. На останніх зберігаються сценарії кібератак для проведення занять щодо дій в умовах кібернетичних впливів і відпрацювання заходів із подолання їх наслідків.

Крім того, в Україні запустили кіберполігон Unit Range, який створений для практичного тренування спеціалістів із кібербезпеки державних органів в умовах, максимально наближених до реальних [16]. Як повідомив популярному українському онлайн-журналу про IT-бізнес, стартапи, технології та підприємництво «AIN.UA» засновник полігона Єгор Аушев, у системі вже накопичено понад 150 сценаріїв кібератак [17].

Використання кіберполігонів дає можливість підвищувати якість кіберекспертиз, проводити наукові дослідження, розуміти особливості боротьби із загрозами та впливами в кіберпросторі, забезпечувати якісне навчання військових і цивільних експертів у кіберсфері, а також проводити кібернавчання в умовах інформаційного та кібернетичного впливу, вдосконалити систему підготовки та підвищення кваліфікації у галузі інформаційної та кібербезпеки з впровадженням комплексних підходів і стандартів НАТО.

Такий навчально-тренувальний комплекс кібербезпеки функціонує також на кафедрі

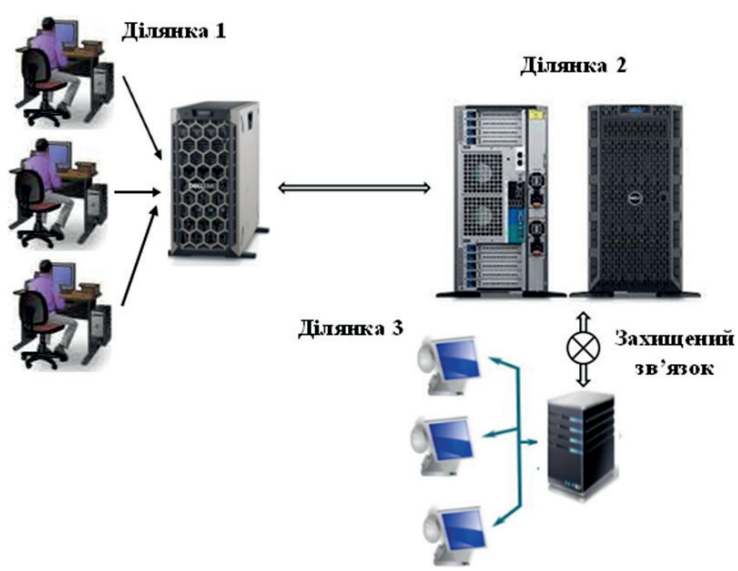

Рис. 1. Організаційно-технічна структура кіберполігона

ISSN 2786-4510 (Online)

кібербезпеки Військового інституту телекомунікацій та інформатизації імені Героїв Крут [18]. До складу комплексу входять програмно-технічні засоби, ситуаційний центр, комплекс технічних засобів, який забезпечує стале функціонування програмно-апаратного ядра, надання можливості створення, модифікації і реалізації сценаріїв та контролю проведення навчальних занять, тренувань із кібербезпеки.

Проблемним питанням залишається підготовка фахівців сфери кібероборони для оперативного та стратегічного рівня управління Збройних сил України, яких треба навчати керувати діями підлеглих у таких ситуаціях. З метою підготовки таких спеціалістів (військових кадрів за ступенями вищої освіти «бакалавр», «магістр», «доктор філософії») для потреб Збройних сил України та проведення з ними навчань із відпрацювання навичок подолання наслідків кібератак пропонується створити кіберполігон на базі Національного університету оборони України.

З технічної точки зору кіберполігон — це сукупність спеціалізованих програмно-апаратних комплексів, об'єднаних за допомогою засобів зв'язку в єдину систему моніторингу, дослідження впливу на систему управління об'єктами і захисту власної системи управління від кібератак.

Крім «звичайних» завдань забезпечення інформаційної і кібернетичної безпеки інформаційно-комунікаційних систем можна визначити такі основні завдання кіберполігона:

- практична апробація та випробовування спеціалізованого програмного забезпечення для забезпечення безпеки мережевих структур;
- моніторинг зареєстрованих даних щодо подій, які стосуються забезпечення безпеки, для аналізу їх на наявність порушень політики безпеки;
- виявлення несанкціонованих змін в управлінні, менеджменті, політиці і процедурах безпеки;
- дослідження різних методів захисту і проведення експериментів у сфері мережевих технологій захисту та програмних засобів критичних об'єктів мережевої інфраструктури;
- симуляція кібератак і процесів кіберзахисту на об'єкти з критичною мережевою інфраструктурою тощо;
- розроблення методів нейтралізації кіберзагроз;
- відпрацювання практичних навичок протидії кібератакам під час командно-штабних навчань.

Функціональну структуру комплексу засобів кібероборони кіберполігона можна представити в спосіб, показаний на рис. 2.

До складу функціональної структури кіберполігона мають входити два комплекти спеціалізованих програмно-апаратних засобів: комплекс засобів кібероборони і комплекс засобів аудиту й моніторингу кібернетичних впливів, які взаємодіють із користувачами та зовнішнім оточенням в інтернеті через дата-центр.

Комплекс засобів кібероборони призначений для забезпечення типових функцій захисту сервісів та служб дата-центру кіберполігона. Він містить антивірусні засоби, засоби криптографічного захисту, засоби контролю цілісності системи, засоби контролю доступу користувачів до ресурсів та інформації шляхом авторизації, автентифікації та розподілу прав доступу, а також засоби захисту периметра системи в складі міжмережних екранів для запобігання витоку даних і засобів менеджменту контенту.

Комплекс засобів аудиту і моніторингу кібернетичних впливів, своєю чергою, має у своєму складі підсистеми моніторингу кібернетичних впливів, моделювання кібератак і тестування на кіберзахищеність.

Підсистема моніторингу кібернетичних впливів має виконувати такі функції: аналіз кіберпростору з метою виявлення, реєстрації та обліку подій, а також аналіз особливостей кібератак, і в такий спосіб сприяти запобіганню вторгненням. Підсистема моніторингу містить такі програмно-технічні компоненти: засоби аналізу та супроводу актуальних баз даних кіберінцидентів і кіберзагроз, засоби виявлення кіберзагроз на системи управління, засоби мережевої топології, засоби програмно-апаратного забезпечення сервісів та служб дата-центру, а також засоби аналізу технологій кібервпливу.

Підсистема тестування має здійснювати діагностику кіберзахищеності всієї системи. Вона об'єднує такі програмно-технічні складові: засоби тестування сервісів та служб дата-центру на кіберзахищеність, засоби аналізу активності в соціальних мережах та електронні ЗМІ, засоби виявлення та аналізу інформаційного впливу на операторів дата-центру через кіберпростір.

Підсистема моделювання кібератак заходів і засобів кіберзахисту системи управління, мережевої топології, програмно-апаратного забезпечення сервісів та служб дата-центру містить

такі програмно-технічні засоби: засоби моделювання та імітації дій у кіберпросторі, засоби моделювання технологій інфозахисту операторів дата-центру, засоби моделювання заходів і засобів кіберзахисту мереж дата-центру, засоби моделювання кібератак на криптосистеми дата-центру, засоби моделювання соціотехнічних кібератак через кіберпростір на операторів дата-центру.

Висновки. Отже, аналіз подій останнього десятиріччя й особливо досвід нашої відсічі збройній агресії росії, під час якої вона активно використовує засоби ведення гібридної війни, свідчить, що кібербезпека будь-якої військової частини та органу військового управління ЗС України всіх рівнів є нині принципово важливим питанням. З метою отримання практичних навичок керування заходами протидії кібератакам слухачами Національного університету оборони України оперативного та стратегічного рівня доцільно створити кіберполігон. Це дасть змогу фахівцям у процесі експлуатації глибоко розуміти методи, які використовуються передовими групами хакерів і навчити їх приймати своєчасні рішення для відсічі кібератакам і подолання їх наслідків. Створення кіберполігона для оволодіння технологіями дій у кіберпросторі дасть змогу офіцерам ЗС України оволодіти організаційними й управлінськими заходами щодо забезпечення кібербезпеки. Крім удосконалення навичок керування заходами кібернетичної безпеки в частинах, установах та органах

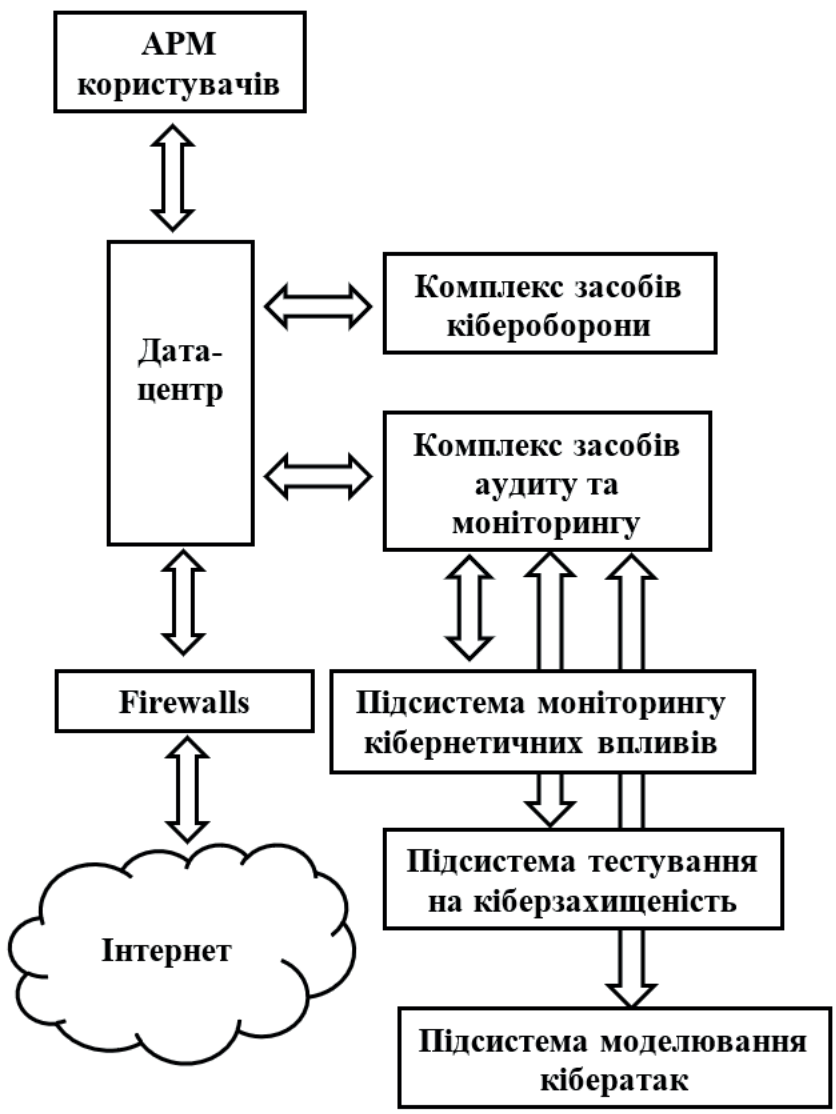

Рис. 2. Функціональна структура кіберполігона

ISSN 2786-4510 (Online)

військового управління ЗС України, кіберполігон може використовуватися і для підвищення кваліфікації посадових осіб інших підрозділів сектору безпеки й оборони України.

У статті розглянута організаційно-технічна структура кіберполігона, визначені його завдання і запропонована функціональна структура. Це є першим кроком з розроблення загальних вимог до кіберполігона згідно з Інструкцією з формування оперативно-стратегічних, оперативно-тактичних та загальних вимог до перспективних (нових, модернізованих) систем (комплексів, зразків) озброєння та військової техніки Збройних Сил України або розроблення тактико-технічного завдання на створення інформаційно-комунікаційної системи кіберполігона.

Згідно зі Стратегією розвитку штучного інтелекту в Україні нині настав час впроваджувати у сферу кібербезпеки держави методи і технології штучного інтелекту, щоб забезпечити своєчасне запобігання й ефективне стримування викликів і загроз, які виникають у кіберпросторі, а також ефективну боротьбу з кіберзлочинністю та кібертероризмом, удосконалювати розвідувальну та контррозвідувальну діяльність відповідних державних служб, що є напрямом подальших досліджень актуальних питань кібербезпеки в сучасному світі.

Список використаних джерел

1. Porter Ch. Protecting those below the cyber-poverty line is critical to everyone. *C4ISRNET*. 2024. Jan 4. URL: https://www.c4isrnet.com/opinion/2024/01/04/protecting-those-below-the-cyber-poverty-line-is-critical-to-everyone/ (дата звернення: 29.02.2024).
2. Demarest C. Cyberattacks on Guam could sap US forces in Indo-Pacific, Nakasone says. *C4ISRNET*. 2024. Feb 1. URL: https://www.c4isrnet.com/cyber/2024/01/31/cyberattacks-on-guam-could-sap-us-forces-in-indo-pacific-nakasone-says/ (дата звернення: 29.02.2024).
3. Development of a concept for building a critical infrastructure facilities security system / S. Yevseiev et al. *Eastern-European Journal of Enterprise Technologies*. 2021. Vol. 3. № 9 (111). Pp. 63–83. DOI: https://doi.org/10.15587/1729-4061.2021.233533.
4. Demarest C. Pentagon seeks to rapidly build up information-warfare force. *C4ISRNET*. 2023. Nov 21. URL: https://www.c4isrnet.com/information-warfare/2023/11/21/pentagon-seeks-to-rapidly-build-up-information-warfare-force/ (дата звернення: 29.02.2024).
5. Про освіту : Закон України від 05.09.2017 р. № 2145-VIII. URL: https://zakon.rada.gov.ua/laws/show/2145-19#Text (дата звернення: 29.02.2024).
6. Биков В. Ю., Буров О. Ю., Дементієвська Н. П. Кібербезпека в цифровому навчальному середовищі. *Інформаційні технології і засоби навчання*. 2019. Т. 70. № 2. С. 313–331. URL: http://nbuv.gov.ua/UJRN/ITZN_2019_70_2_25 (дата звернення: 29.02.2024).
7. Технологія забезпечення інформаційної і кібербезпеки в закладах вищої освіти України / А. Ю. Нашинець-Наумова та ін. *Інформаційні технології і засоби навчання*. 2020. Т. 77. № 3. С. 337–354.
8. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект : підручник / за заг. ред. В. Б. Толубка. Київ : ДУТ, 2015. 288 с.
9. Shank E. Skinner urges need to 'simplify the complexity of our environment'. 2023. August 17. URL: https://disa.mil/en/NewsandEvents/2023/Simplify-the-complexity-of-our-environment (дата звернення: 29.02.2024).
10. Gosselin-Malo E. NATO deepens cyber coalition with Asian partners. *C4ISRNET*. 2023. Dec 1. URL: https://www. c4isrnet.com/cyber/2023/12/01/nato-deepens-cyber-coalition-with-asian-partners/ (дата звернення: 29.02.2024).
11. 03.12.23 Україна і світ — проти російської агресії. Санкції в дії. URL: https://szru.gov.ua/news-media/publications/031223-ukraina-i-svit--proty-rosiiskoi-ahresii-sanktsii-v-dii (дата звернення: 29.02.2024).
12. Лисогор І. Росія щоденно здійснює близько 10 кібератак проти України. URL: https://lb.ua/society/2023/02/28/547362_rosiya_shchodenno_zdiysnyuie_blizko_10.html (дата звернення: 29.02.2024).
13. Кіберполігон. URL: https://www.kafcbit.hneu.edu.ua/кіберполігон/ (дата звернення: 29.02.2024).
14. Кіберполігон. URL: https://kb.khmnu.edu.ua/kiberpoligon/ (дата звернення: 29.02.2024).
15. Кібербезпека мереж наступних поколінь : навч. посіб. / О. О. Вараксін ; за ред. чл.-кор. МАЗ В. Г. Кононовича. Одеса : ОНАЗ ім. О. С. Попова, 2012. 240 с.
16. Житкевич А. В Україні запустили кіберполігон для тренування спеціалістів. URL: https://speka.media/v-ukrayini-zapustili-kiberpoligon-dlya-trenuvannya-specialistiv-9ejemp (дата звернення: 29.02.2024).
17. Сабадишина Ю. Єгор Аушев запустив кіберполігон для тренування спеціалістів — там вже є понад 150 сценаріїв атаки і захисту. URL: https://dou.ua/lenta/news/about-unit-range/ (дата звернення: 29.02.2024).
18. У ЗСУ функціонуватиме надсучасний кіберполігон VITIsecurity: на кафедрі кібербезпеки розгорнуто навчально-тренувальний комплекс. URL: https://www.viti.edu.ua/news/3247 (дата звернення: 29.02.2024).

References

1. Porter, Ch. (2024). Protecting those below the cyber-poverty line is critical to everyone. *C4ISRNET.* Jan 4. Retrieved from https://www.c4isrnet.com/opinion/2024/01/04/protecting-those-below-the-cyber-poverty-line-is-critical-to-everyone/.
2. Demarest, C. (2024). Cyberattacks on Guam could sap US forces in Indo-Pacific, Nakasone says. *C4ISRNET*. Feb 1. Retrieved from https://www.c4isrnet.com/cyber/2024/01/31/cyberattacks-on-guam-could-sap-us-forces-in-indo-pacific-nakasone-says/.
3. Yevseiev, S., Melenti, Y., Voitko, O., Hrebeniuk, V., Korchenko, A., Mykus, S. et al. (2021). Development of a concept for building a critical infrastructure facilities security system. *Eastern-European Journal of Enterprise Technologies*, 3, 9 (111), 63–83. DOI: https://doi.org/10.15587/1729-4061.2021.233533.
4. Demarest, C. (2023). Pentagon seeks to rapidly build up information-warfare force. *C4ISRNET*. Nov 21. Retrieved from https://www.c4isrnet.com/information-warfare/2023/11/21/pentagon-seeks-to-rapidly-build-up-information-warfare-force/.
5. Zakon Ukrainy Pro osvitu vid 5 veres. 2017 roku № 2145-VIII [Law of Ukraine On education from September 5 2017, № 2145-VIII]. *zakon.rada.gov.ua.* Retrieved from https://zakon.rada.gov.ua/laws/show/2145-19#Text [in Ukrainian].
6. Bykov, V. Yu., Burov, O. Yu., & Dementiievska, N. P. (2019). Kiberbezpeka v tsyfrovomu navchalnomu seredovyshchi [Cyber security in a digital educational environment]. *Informatsiini tekhnolohii i zasoby navchannia — Information technologies and teaching aids,* 70 (2), 313–331. Retrieved from http://nbuv.gov.ua/ UJRN/ITZN_2019_70_2_25 [in Ukrainian].
7. Nashynets-Naumova, A. Yu., Buriachok, V. L., Korshun, N. V., Zhyltsov, O. B., Skladannyi, P. M., Kuzmenko, L. V. (2020). Tekhnolohiia zabezpechennia informatsiinoi i kiberbezpeky v zakladakh vyshchoi osvity Ukrainy [Technology of information and cyber security in higher education institutions of Ukraine]. *Informatsiini tekhnolohii i zasoby navchannia — Information technologies and teaching aids*, 77 (3), 337–354 [in Ukrainian].
8. Buriachok, V. L., Tolubko, V. B., Khoroshko, V. O., Toliupa, S. V. (2015). *Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt [Information and cyber security: socio-technical aspect]* V. B. Tolubko (Ed.). Kyiv : DUT [in Ukrainian].
9. Shank, E. (2023). Skinner urges need to 'simplify the complexity of our environment'. August 17. Retrieved from https://disa.mil/en/NewsandEvents/2023/Simplify-the-complexity-of-our-environment.
10. Gosselin-Malo, E. (2023). NATO deepens cyber coalition with Asian partners. *C4ISRNET*. Dec 1. Retrieved from https://www. c4isrnet.com/cyber/2023/12/01/nato-deepens-cyber-coalition-with-asian-partners/.
11. 03.12.23 Ukraina i svit — proty rosiiskoi ahresii. Sanktsii v dii. [03.12.23 Ukraine and the world are against russian aggression. Sanctions are in effect]. Retrieved from https://szru.gov.ua/news-media/publications/031223-ukraina-i-svit--proty-rosiiskoi-ahresii-sanktsii-v-dii [in Ukrainian].
12. Lysohor, I. Rosiia shchodenno zdiisniuie blyzko 10 kiberatak proty Ukrainy [Russia carries out about 10 cyberattacks against Ukraine every day]. Retrieved from https://lb.ua/society/2023/02/28/547362_rosiya_shchodenno_zdiysnyuie_blizko_10.html [in Ukrainian].
13. Kiberpolihon [Cyber range]. Retrieved from https://www.kafcbit.hneu.edu.ua/kiberpolihon/ [iт Ukrainian].
14. Kiberpolihon [Cyber range]. Retrieved from https://kb.khmnu.edu.ua/kiberpoligon/ [in Ukrainian].
15. Varaksin, O. O., Vasiliu, Ye. V., Horokhov, S. M., Kildishev, V. Y., & Kononovych, V. H. (2012). Kiberbezpeka merezh nastupnykh pokolin [Cybersecurity of next-generation networks]. V. H. Kononovych (Ed.). Odesa : ONAZ im. O. S. Popova [in Ukrainian].
16. Zhytkevych, A. V Ukraini zapustyly kiberpolihon dlia trenuvannia spetsialistiv [In Ukraine, a cyber training ground was launched for the training of specialists]. Retrieved from https://speka.media/v-ukrayini-zapustili-kiberpoligon-dlya-trenuvannya-specialistiv-9ejemp [in Ukrainian].
17. Sabadyshyna, Yu. (2023). Yehor Aushev zapustyv kiberpolihon dlia trenuvannia spetsialistiv — tam vzhe ye ponad 150 stsenariiv ataky i zakhystu [Yehor Aushev launched a cyber training ground for specialists — there are already more than 150 attack and defense scenarios]. Retrieved from https://dou.ua/lenta/news/about-unit-range/ [in Ukrainian].
18. U ZSU funktsionuvatyme nadsuchasnyi kiberpolihon VITIsecurity: na kafedri kiberbezpeky rozghornuto navchalno-trenuvalnyi kompleks [The state-of-the-art VITIsecurity cyber training ground will function in the Armed Forces: an educational and training complex has been deployed at the cyber security department]. Retrieved from https://www.viti.edu.ua/news/3247 [in Ukrainian].

 ISSN 2786-4510 (Online)

O. M. Bashkyrov,
O. P. Krushenytskyi,
A. Yu. Dmytrenko

ADVANCED INFORMATION TECHNOLOGIES FOR THE TRAINING OF CYBER DEFENCE SPECIALISTS OF THE SECURITY AND DEFENCE SECTOR OF UKRAINE

Abstract. *In recent years, russian intelligence agencies have demonstrated the capability to overcome security measures even in well-protected companies and government networks worldwide, including the security system of the U. S. military base on Guam. According to estimates from the Security Service of Ukraine, russia is currently carrying out around 10 cyber attacks on Ukraine daily. Therefore, the training of cybersecurity professionals for our country, especially in the sector of security and defense in Ukraine, is now an urgent and relevant task. Establishing a robust information security system for critical infrastructure objects is a crucial element of the defense strategy of any country. According to the Military Security Strategy of Ukraine, approved by the President's Decree on March 25, 2021, enhancing the capabilities of the Armed Forces of Ukraine, territorial defense forces, and other components of defense forces to fulfill assigned tasks is a specific priority. One practical direction in implementing this priority is the development of capabilities in ensuring cyber security, cyber protection, and cyber defense, countering aggression in cyberspace during the preparation and conduct of comprehensive defense in Ukraine. Furthermore, the Law of Ukraine "On Education" defines information and communication competence as one of the key competencies of a modern individual. Therefore, this article addresses the timely topic of improving the organization of training for the leadership of the Ministry of Defense of Ukraine in the field of ensuring cyber security for the state. The article discusses the tasks of a cyber range and justifies practical ways of their implementation. The experience of some higher education institutions in Ukraine regarding the organizational and technical structure of a cyber range is presented. Using these institutions as examples, the creation of a cyber range at the National Defense University of Ukraine for the training of cyber defense specialists for the Armed Forces of Ukraine and conducting cyber exercises with them is proposed. The article develops proposals regarding its functional structure.*

Keywords: *cyber defense, cybersecurity training, cyber range.*

ІНФОРМАЦІЯ ПРО АВТОРІВ

Башкиров Олександр Миколайович — канд. техн. наук, доцент, провідний науковий співробітник науково-дослідного управління, Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України, м. Київ, Україна, bashkyrov1958@gmail.com; ORCID ID: https://orcid.org/0000-0001-9444-0653

Крушеницький Олександр Петрович — слухач, Інститут інформаційно-комунікаційних технологій та кібероборони Національного університету оборони України, м. Київ, Україна, cosmoss1@i.ua; ORCID ID: https://orcid.org/0009-0003-0202-1729

Дмитренко Андрій Юрійович — слухач, Інститут інформаційно-комунікаційних технологій та кібероборони Національного університету оборони України, м. Київ, Україна, admitrenko44@gmail.com; ORCID ID: https://orcid.org/0009-0002-9658-8488

INFORMATION ABOUT THE AUTHORS

Bashkyrov O. M. — PhD in Engineering, Associate Professor, Leading Researcher, Central Scientific Research Institute of Armament and Military Equipment of Armed Forces of Ukraine, Kyiv, Ukraine, bashkyrov1958@gmail.com; ORCID ID: https://orcid.org/0000-0001-9444-0653

Krushenytskyi O. P. — student, the Institute of Information and Communication Technologies and Cyber Defense of National Defense University of Ukraine, Kyiv, Ukraine, cosmoss1@i.ua; ORCID ID: https://orcid.org/0009-0003-0202-1729

Dmytrenko A. Yu. — student, the Institute of Information and Communication Technologies and Cyber Defense of National Defense University of Ukraine, Kyiv, Ukraine, admitrenko44@gmail.com; ORCID ID: https://orcid.org/0009-0002-9658-8488

Стаття надійшла до редакції / Received 29.02.2024