Вплив кіберзагроз на безпеку військових об’єктів в умовах збройної агресії росії проти України

Підтинний Дмитро Леонідович[1]

Опубліковано	Секція	УДК
18.06.2024	Соціальні та поведінкові науки	327.004.056

DOI: https://doi.org/ 10.5281/zenodo.12097014

Анотація. Представлена стаття відображає результати дослідження впливу кіберзагроз на безпеку військових об’єктів в умовах збройної агресії росії проти України. Доведено, що повномасштабне вторгнення рф в Україну призвело до значних змін у сфері кібербезпеки. Діяльність військових та цивільних об’єктів перейшла в режим воєнного стану, що змусило спеціалістів із забезпечення кібербезпеки адаптуватися до нових умов, зокрема опановувати нові техніки протистояння кіберзагрозам. Важливою професією в умовах війни є фахівець (спеціаліст) із кібербезпеки, оскільки захист від інформаційних загроз є не менш важливим, ніж захист від ракетних ударів, для успішного функціонування військових об’єктів та критичної інфраструктури. Сучасне інформаційне поле України й світу активно використовується для виведення з ладу різних пристроїв та викрадення секретних даних. Запобігання цьому передбачає впровадження інновацій у реалізацію змісту та методики викладання дисципліни «Кібербезпека», що присвячена протидії кіберзагрозам. Перманентний розвиток Збройних сил України зумовив розширення та ускладнення змісту функцій фахівців із кібербезпеки та створив для них велику кількість серйозних викликів. Проблема впливу кіберзагроз на безпеку військових об’єктів в умовах збройної агресії росії проти України часто привертає увагу вітчизняних та закордонних учених. З’ясовано, що розв’язання наукового завдання щодо анонсованої проблеми потребує подальшого розгляду, оскільки характер ведення інформаційних операцій постійно змінюється, і те, що було актуальним ще донедавна, сьогодні вже є застарілим або навіть шкідливим для використання. Результати здійсненого дослідження дозволяють зробити висновок, згідно з яким саме підвищення кваліфікації фахівців із кібербезпеки в контексті взаємодії закладів вищої освіти і військових структур може стати ключем для забезпечення високого рівня кібербезпеки для військових об’єктів та критичної інфраструктури в умовах збройної агресії росії проти України. Відповідно до сфери професійної діяльності фахівців із кібербезпеки запропоновано низку заходів для розвитку їх методичних навичок, які допоможуть підготувати спеціалістів високої кваліфікації.

Ключові слова: кібербезпека, військова стратегія, інформаційні загрози, захист даних, критична інфраструктура.

[1] Старший викладач Національної академії Служби безпеки України, dmytro3214@gmail.com, https://orcid.org/0009-0003-1784-2079.

Interaction Between Higher Educational Institutions and Military Structures in the Field of Training Specialists in Fire Training

Annotation. The presented article reflects the results of a study of the impact of cyber threats on the security of military facilities in the conditions of Russia's armed aggression against Ukraine. It was determined that the full-scale invasion of the Russian Federation into Ukraine led to significant changes in the field of cyber security. The activities of military and civilian facilities have gone into martial law mode, which has forced cyber security specialists to adapt to new conditions, namely to start mastering new techniques for countering cyber threats. An important profession, in the conditions of war, is a specialist (specialist) in cyber security, since protection against information threats is no less important than protection against missile attacks for the successful functioning of military facilities and critical infrastructure. The modern information field of Ukraine and the world is actively used to disable various devices and steal secret data. Prevention of this requires the introduction of innovations in the implementation of the content and teaching methodology of the cyber security discipline, which is dedicated to countering cyber threats. The permanent development of the Armed Forces of Ukraine has led to the expansion and complication of the functions of cyber security specialists and created a large number of serious challenges for them. The problem of the influence of cyber threats on the security of military facilities in the conditions of Russia's armed aggression against Ukraine often attracts the attention of domestic and foreign scientists. It becomes clear that the solution of the scientific task regarding the announced problem requires further consideration, since the nature of conducting information operations is constantly changing and what was relevant recently is now obsolete or even harmful for use. The results of the conducted research allow us to conclude that the advanced training of cyber security specialists, in the context of the interaction of higher educational institutions and military structures, can become the key to ensuring a high level of cyber security for military facilities and critical infrastructure in the conditions of Russia's armed aggression against Ukraine. Also, in accordance with the field of professional activity of cyber security specialists, a number of measures have been proposed to develop their methodological skills, which will help prepare highly qualified specialists.

Keywords: cyber security, military strategy, information threats, data protection, critical infrastructure.

Вступ

Актуальність дослідження впливу кіберзагроз на безпеку військових об'єктів в умовах збройної агресії росії проти України зумовлена низкою таких факторів, як:

-втрати техніки та особового складу через використання ворожими спеціалістами прогалин у вітчизняній кібербезпеці;

-необхідність забезпечувати конфіденційність та секретність планів ведення бойових дій (військової стратегії);

-військово-цивільна співпраця сприяє розробці та впровадженню професійних стандартів у галузі кібербезпеки, що допомагає підвищити загальну оборонну готовність України;

-подолання ворожих кіберзагроз зменшить можливості ворога в контексті атаки на військові й цивільні об'єкти, об'єкти критичної інфраструктури. Це сприятиме наближенню перемоги ЗСУ й високому моральному духу населення в тилу;

-недостатній розвиток кібербезпеки як навчальної дисципліни в Україні (більш ефективна передача знань та навичок майбутнім спеціалістам із кібербезпеки можлива тільки за умови глибокого розуміння самої сутності поняття та його складових).

Отже, мінімізація чи навіть повне усунення впливу кіберзагроз на безпеку військових об'єктів в умовах збройної агресії росії проти України є важливою складовою підвищення мотивації військовослужбовців Збройних Сил України.

Проблеми впливу кіберзагроз на безпеку нашої держави та військових об'єктів як однієї з ланок її загальної кібербезпеки в умовах збройної агресії росії проти України є предметом досліджень багатьох сучасних як вітчизняних, так і закордонних науковців. Так, С. Онищенко та А. Глушко [1] в їх спільній праці довели необхідність впровадження комплексних та скоординованих заходів на національному й міжнародному рівнях для запобігання реалізації кіберінцидентів із боку органів влади, бізнесу та суспільства. У роботі А. Омельченка [2] визначено органи координації та контролю за діяльністю суб'єктів сектору безпеки й оборони, які забезпечують кібербезпеку в Україні.

Є. Колосовський, А. Калюжна та О. Матвієнко [3] здійснили дослідження, яке виявило, що рф фактично веде комплексну перманентну кібервійну проти України. До того ж науковці запропонували ідею щодо створення новітнього органу протидії кібератакам – кіберсили. О. Сичов [4] здійснив ситуаційний аналіз кібербезпеки Міністерства Оборони України, який показав, що наявні суб'єкти кібербезпеки постійно функціонують у різних умовах, а це, відповідно, має вплив на можливість реалізації їх спроможностей. Колектив дослідників під керівництвом А. Плахотного [5] розглянув актуальні аспекти кібербезпеки під час воєнного конфлікту та ролі кіберзагроз у воєнному контексті, що дозволило зрозуміти необхідність запровадження належних засобів захисту. Дослідження Л. Мазника та З. Двуліта [6] допомогло визначити зміст діяльності фахівців із кібербезпеки відповідно до основних концепцій кібербезпеки в умовах повномасштабної війни. М. Кулешов [7] визначив особливості формування переліку об'єктів критичної інфраструктури як об'єктів забезпечення кібербезпеки.

Праця В. Поліщука [8] дозволила проаналізувати досвід США та КНР щодо забезпечення необхідного рівня кібербезпеки. С. Островський [11] вважає першочерговим завданням для ЗСУ – наблизити систему військ зв'язку та кібербезпеки до стандартів НАТО.

Г. Бондар [9] довів, що ворожі хакери використовували шкідливе програмне забезпечення в українських мережах ще задовго до вторгнення в Україну 24 лютого 2022 року. У науковій праці Б. Васильківа [10] запропоновано співпрацю між усіма зацікавленими сторонами для подолання кіберзагроз та подальшого розвитку України. Колектив учених на чолі з О. Пономаровим [13] сформував ідею щодо необхідності створення гібридної системи кібербезпеки на основі військово-цивільної співпраці. В. Фесьоха, Д. Кисиленко та О. Нестеров [12] досліджують можливість виявляти нове шпигунське програмне забезпечення на основі ідентифікації поліморфних структур раніше відомих вірусів.

D. Strucl [14] здійснив аналіз кібероперацій рф проти України та виявив потенційний глобальний вплив кіберпростору на збройний конфлікт у майбутньому. I. Aviv та U. Ferri [15] визначили важливість парадигми «цифрового суверенітету» як складової кібербезпеки.

М*етою даної статті* є дослідження впливу кіберзагроз на безпеку військових об'єктів в умовах збройної агресії росії проти України

Для досягнення зазначеної мети були сформульовані такі завдання: визначити поняття «кіберзагроза» та «кібербезпека»; розглянути приклади сценаріїв кібервійни; виокремити основні складові компоненти кібербезпеки; описати основні з наявних кіберзагроз; розглянути законодавство України про кібербезпеку; з'ясувати напрями протидії кіберзагрозам рф в умовах війни; запропонувати низку заходів (рекомендацій) у межах закладів вищої освіти, що допоможуть фахівцям із кібербезпеки покращувати їхні навички та підготувати спеціалістів високої кваліфікації для майбутнього.

Матеріали та методи

Інформаційною базою нашого дослідження стала наукова література за тематичним спрямуванням та науково-аналітичні публікації українських і зарубіжних учених із досліджуваної проблематики. Теоретичною основою дослідження є положення закордонної й вітчизняної військової науки та інформатики.

Для реалізації визначених завдань було використано низку методів наукового дослідження, відображених на рис. 1.

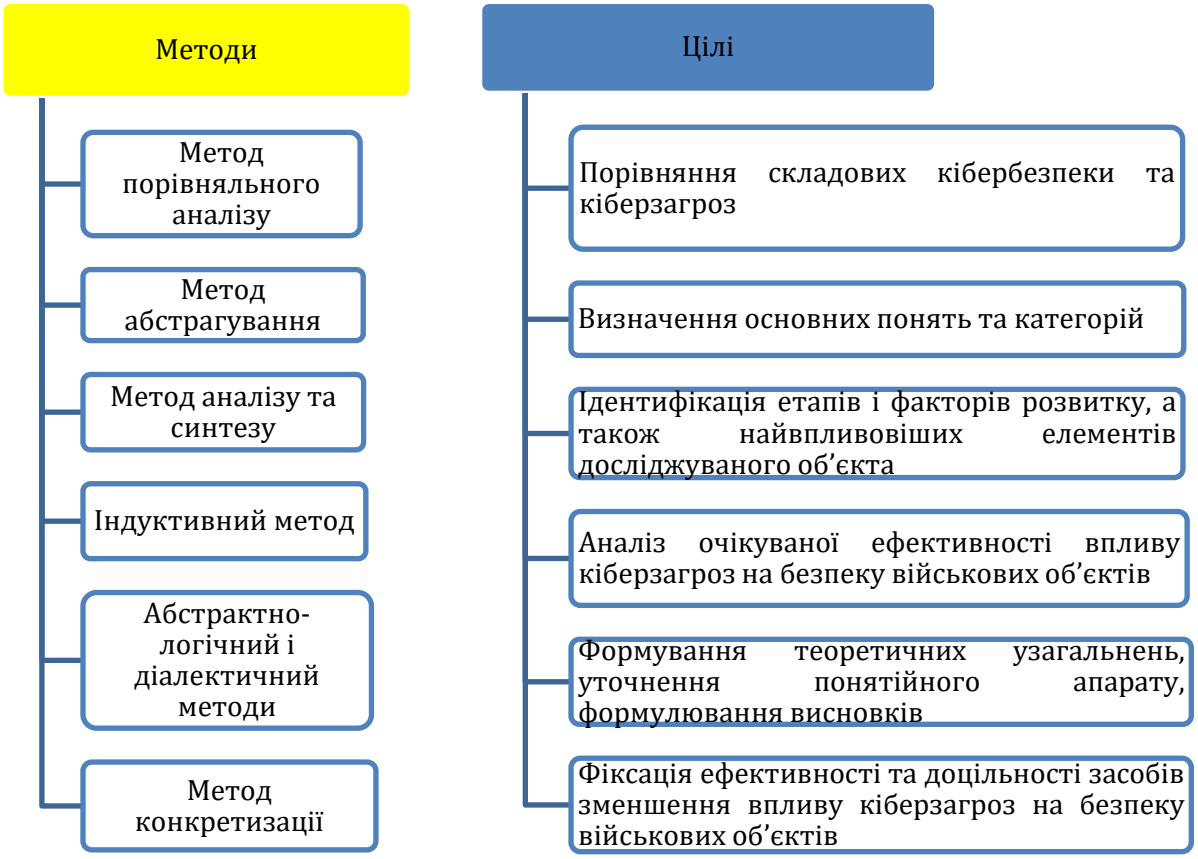

Рис. 1. Використані методи наукового дослідження

Джерело: власна розробка автора

Результати

Для досягнення сформульованої мети дослідження доцільно уточнити його понятійно-категоріальний апарат у даному контексті, зокрема терміни «кібербезпека» та «кіберзагроза». Кібербезпека (цифрова безпека або безпека інформаційних технологій) – це захист комп'ютерних систем і мереж від атак зловмисників, які можуть призвести до несанкціонованого розкриття інформації, крадіжки або пошкодження обладнання та програмного забезпечення чи даних, а також від порушення або неправильного спрямування послуг, які вони надають [16].

До того ж потрібно зауважити, що рівень і деталізація запобіжних заходів залежать від системи, яку необхідно захистити. Домашній персональний комп'ютер, банк і секретна військова мережа стикаються з дуже різними загрозами, навіть якщо базові технології, що використовуються, схожі [17].

Кіберзагроза або загроза кібербезпеці – це зловмисна дія, яка спрямована на пошкодження чи викрадення даних або ж на порушення функціонування інформаційної системи загалом [18].

Усього існує сім основних складових компонентів кібербезпеки (рис. 2).

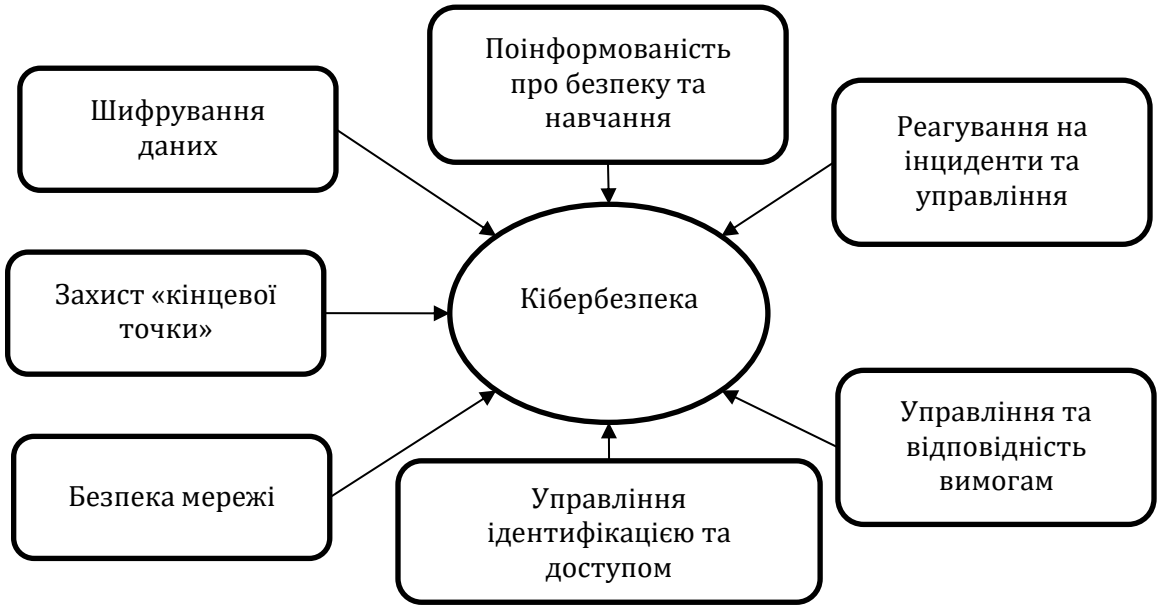

Рис. 2. Складові компоненти кібербезпеки

Джерело: власна розробка автора

Вважаємо за доцільне розкрити кожен із наведених на рис. 2 компонентів більш детально.

1. Безпека мережі: захист конфіденційності та безпеки даних, якими обмінюються через мережі, є надзвичайно важливим компонентом. Це передбачає встановлення надійних засобів захисту, таких як віртуальні приватні мережі (VPN) для створення безпечних з'єднань через загальнодоступні мережі, системи виявлення атак (IDS) для моніторингу й аналізу мережевого трафіку на ознаки злочинної діяльності та брандмауери для фільтрації вхідного й вихідного мережевого трафіку.

2. Захист кінцевої точки: підтримання загального рівня безпеки організації вимагає захисту окремих пристроїв або цілей від різноманітних кібератак. Це означає використання технологій виявлення та реагування кінцевих точок (EDR) для моніторингу та реагування на поведінку кінцевих точок у режимі реального часу, антивірусне програмне забезпечення для виявлення та видалення шкідливого програмного забезпечення та захист пристрою для захисту даних кінцевої точки від несанкціонованого використання.

3. Шифрування даних: конфіденційність і цілісність вимагають захисту конфіденційних даних шляхом кодування їх у нечитабельний код. Такі методи безпеки, як симетричне та асиметричне шифрування, гарантують безпеку інформації під час обробки, передачі й зберігання, навіть якщо вона потрапляє в чужі руки.

4. Поінформованість про безпеку та навчання: створення культури безпеки всередині організації вимагає навчання користувачів і персоналу найкращим практикам кібербезпеки. Це передбачає інформування про фішингові електронні листи та використання методів соціальної інженерії через навчальні сесії й надання порад щодо виявлення та подолання кіберзагроз.

5. Реагування на інциденти та управління: щоб мінімізувати наслідки порушень і зберегти безперервність роботи, необхідно встановити політики та процедури для виявлення, обробки й відновлення інцидентів кібербезпеки. Це означає формування групи реагування на інциденти, завданням якої є виявлення та припинення порушень безпеки й розробка детального плану реагування на інциденти, який визначає, що треба робити у випадку кібератаки.

6. Управління та відповідність вимогам: вимога щодо дотримання стандартів і законодавчих норм має вирішальне значення для зниження ризиків і збереження відповідальності. Для ефективного управління ризиками необхідне запровадження правил безпеки, процедур і засобів контролю. Це передбачає регулярний аудит та аналіз відповідності, щоб знайти сфери, які потребують розвитку та коригування.

7. Управління ідентифікацією та доступом: уникнення небажаного доступу до систем і даних здебільшого залежить від керування онлайн-ідентифікаціями, перевірки та контролю доступу. Щоб отримати доступ, користувачі повинні спочатку надати кілька форм перевірки за допомогою такого методу, як багатофакторна автентифікація (MFA). Подібним чином контроль доступу на основі ролей (RBAC) гарантує, що користувачам надаються дозволи відповідно до їхніх посад і обов'язків в організації [19].

Найнебезпечнішими загрозами для кібербезпеки є кібершпигунство та кібертероризм. Використання методів злому та шкідливого програмного забезпечення, включно з троянськими програмами та шпигунським програмним забезпеченням, які призначені для викрадення секретної інформації щодо окремих осіб, груп і урядів для власної вигоди з використанням незаконних методів отримання доступу до інформації без дозволу власника, називається кібершпигунством. Такі дії можуть бути вчинені онлайн-професіоналами (хакерами) [20].

Кібертероризм – це процес використання мережі інтернет для здійснення насильницьких дій, які пов'язані з небезпекою для життя й здоров'я людей або настанням інших тяжких наслідків з метою досягнення політичних чи ідеологічних переваг шляхом погроз або залякування. Акти навмисного, великомасштабного порушення роботи комп'ютерних мереж, особливо персональних комп'ютерів, підключених до мережі інтернет за допомогою таких інструментів, як комп'ютерні віруси, комп'ютерні хробаки, фішинг, шкідливе програмне забезпечення, методи апаратного забезпечення та сценарії програмування – усе це є формами інтернет-тероризму [21].

З початком військової агресії на Сході України та анексії Криму рф розв'язала проти України повноцінну кібервійну. Кібервійна відрізняється від кібертероризму тим, що це організовані зусилля однієї національної держави для проведення операцій у кіберпросторі проти інших держав. Найбільш популярним інструментом кібервійни є використання мережі інтернет для збору розвідувальних даних [22].

Потенційними наслідками кібервійни є:

1.Повалення системи державної влади або катастрофічна загроза національній безпеці.

2. Велика шкода для іміджу країни на міжнародному рівні.

3. Катастрофічне руйнування або пошкодження політичних та економічних зв'язків країни.

4. Значні людські жертви або загроза здоров'ю й безпеці населення.

5. Руйнування суспільної довіри чи релігійних та національних переконань.

6. Пошкодження чи знищення об'єктів інфраструктури та національного господарства країни.

7. Дезорганізація оборони шляхом викрадення військових планів і порушення систем функціонування військових об'єктів.

Зазвичай кібервійна відбувається за попереднім сценарієм, але можливе й використання ворогом унікального сценарію, що залежить від його можливостей та особливостей країни, проти якої він реалізується. Найпоширенішими сценаріями кібервійни можна вважати такі:

-Спонсороване урядом кібершпигунство з метою збору інформації для планування майбутньої кібератаки;

-Кібератака, спрямована на формування основи для будь-яких заворушень і поширення популярності ідей бунтів та повстання;

-Кібератака, спрямована на виведення обладнання з ладу та сприяння фізичній агресії;

-Кібератака як доповнення до фізичної агресії;

-Кібератака для повсюдного знищення інфраструктури або дезорганізації як остаточної мети [23].

Україна є не першою жертвою кібервійни. Вперше про кібервійну заговорили ще у 2007 році, коли з території рф були здійснені кібератаки проти Естонії. Кібератаки на Естонію у 2007 році були широко відображені в ЗМІ та названі першою в історії кібервійною. Це показало, як нову технологію можна використати для нападу на сучасну країну. Атака відбулась із території росії – більшість DDoS-атак здійснювалися з російських IP-адрес. Багато зловмисників використовували комп'ютери з Естонії – це була російська меншина в цій країні. Незважаючи на те, що експерти Європейської комісії та НАТО не знайшли доказів того, що російська влада здійснила ці атаки, останні були дуже вигідні кремлівському режиму.

Головними цілями рф у випадку кібератаки на Естонію було:

-вплинути на владу Таллінна, щоб вона відмовилася від свого рішення про демонтаж радянського пам'ятника;

-перевірити можливості в кібервійні та подивитися на реакцію НАТО;

-показати естонському суспільству його беззахисність і залякати його.

Жодну з цілей не було досягнуто, радянський пам'ятник демонтували, а Естонія стала лідером у сфері кібербезпеки. Організація НАТО прискорила розвиток своїх проєктів кіберзахисту та створила Спільний центр передового досвіду кіберзахисту поблизу Таллінна [24].

Найвідомішими кібератаками проти України до початку повномасштабного вторгнення були «Fancy Bear», атаки на енергетику, що викликали блекаут, та використання вірусу «NotPetya».

Імплантат «FANCY BEAR X-Agent» таємно поширювався на українських військових форумах у легальному Android-додатку з кінця 2014 до початку 2016 року. Згідно з даними з відкритих джерел, за два роки конфлікту українські артилерійські підрозділи втратили більше половини своєї артилерії, понад 80% гаубиць Д-30, що є найбільшою втратою серед інших артилерійських систем на озброєнні України. Це стало наслідком їх відстеження за допомогою цього імплантату [25]. Також ця російська хакерська група вважається відповідальною за кілька інших резонансних кібератак, включаючи атаку на німецький парламент у 2015 році та Всесвітнє антидопінгове агентство (WADA) у 2016 році.

У грудні 2015 року жителі України пережили серію відключень електроенергії, які тривали по декілька годин. Збій стався через кібератаку на енергомережу України. Хакери успішно відключили електрику багатьом українцям у Києві та інших містах. Вони використовували шкідливу частину спеціально створеного програмного забезпечення, призначеного для автоматичного запуску процесу відключення електроенергії, надаючи швидкі команди автоматичним вимикачам в утиліті жертви під назвою Crash

Override [26]. Це була перша кібератака, яка спричинила відключення електроенергії. Багато хто звинувачував у нападі росію, але офіційні представники кремля заперечували будь-яку причетність.

NotPetya – вірус-вимагач, який уперше був виявлений у червні 2017 року. Вірус швидко поширився Україною, а потім і іншими країнами, зокрема Великою Британією та США. NotPetya спочатку був замаскований під програмне забезпечення під назвою Petya, яке використовується для шифрування файлів на комп'ютері жертви. Після встановлення вірус поширювався на інші комп'ютери в тій же мережі. Вірус відрізнявся від інших програм-вимагачів тим, що був розроблений для знищення даних, а не для їх постійного шифрування. Це зробило його більш руйнівним і завдало збитків на мільярди доларів. Вважається, що NotPetya створило російське головне розвідувальне управління (ГРУ) [27].

З наведених вище даних стає очевидним, що кібератаки рф проти України відбувались одразу на кількох напрямах, таких як оборонна готовність держави, критична інфраструктура, економічна діяльність та національне господарство.

Для зменшення успіху кібератак злочинних груп та потенційно ворожих держав на Україну було розроблено плани протидії кіберзагрозам та забезпечення належного рівня кібербезпеки вітчизняних інформаційних мереж. Головними документами, що регулюють питання кібербезпеки в Україні, є Закон «Про основні засади забезпечення кібербезпеки України» та Указ Президента № 447.

Закон «Про основні засади забезпечення кібербезпеки України» містить правові основи забезпечення кібербезпеки України, визначення об'єктів та суб'єктів забезпечення кібербезпеки. Також він утверджує основні принципи забезпечення кібербезпеки та створену на їх основі національну систему кібербезпеки. У контексті війни найважливішим його пунктом є пункт 22, що регламентує здійснення воєнно-політичних, військово-технічних та інших заходів для розширення можливостей воєнної організації держави, сектору безпеки й оборони з використанням кіберпростору, створення й розвитку сил, засобів та інструментів можливої відповіді на агресію в кіберпросторі, яка може застосовуватися як засіб стримування воєнних конфліктів та загроз із використанням кіберпростору [28].

Указ Президента № 447 надає чинності рішенню Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» та затверджує Стратегію кібербезпеки України, яка є надважливою для мінімізації наслідків кіберзагроз та протистояння кібератакам із таких причин:

1. Кібербезпека визначена одним із пріоритетів у системі національної безпеки України.

2. Кіберпростір разом з іншими фізичними просторами визнано одним із можливих театрів воєнних дій.

3. Основною загрозою для кібербезпеки України визначено діяльність рф, яка активно реалізує концепцію інформаційного протиборства.

4. Здійснено огляд стану вітчизняного інформаційного поля.

5. Розглянуто основні виклики й загрози. У військовому контексті основною загрозою визначено мілітаризацію кіберпростору та розвиток кіберзброї, що дає можливість приховано здійснювати кібератаки для підтримки бойових дій і розвідувально-підривної діяльності в кіберпросторі.

6. Виокремлено кіберзагрози саме від рф: нарощування арсеналу кіберзброї наступального призначення, застосування якої може викликати невиправні, незворотні руйнівні наслідки; спрямування кібератак насамперед на інформаційно-комунікаційні системи державних органів України та об'єкти критичної інформаційної інфраструктури з метою виведення їх із ладу (кібердиверсії); здійснення розвідувальної

та розвідувально-підривної діяльності; перманентна дискредитація української державності.

7. Визначено пріоритети забезпечення кібербезпеки України та стратегічні цілі й завдання.

8. Запропоновано метрики (виміри успіху стратегії) [29].

31 травня 2021 року Президент України Володимир Зеленський підписав указ про створення президентського Університету інформаційної та кібербезпеки. Як зазначив глава держави, «студенти навчатимуться безкоштовно, а потім реалізовуватимуться і працюватимуть в Україні для захисту держави». У ЗВО можна буде отримати наукові ступені бакалавра, магістра і навіть доктора філософії. До участі в програмі навчання запрошуватимуть іноземних викладачів та дослідників [30]. На жаль, через повномасштабне вторгнення рф на територію України та епідемію COVID-19 університет досі не був створений.

Вплив кібератак на ведення воєнних дій залишається дискусійним питанням. Попри те, що, як раніше було зазначено, імплантат «FANCY BEAR X-Agent» і допоміг рф знищувати українську артилерію під час проведення АТО на сході України, дослідження Н. Костюк та Ю. Жукова [31], яке базується на прикладах війни в Україні та Сирії й використовує дані про невеликі кібератаки на Україну, зібрані з 2013 по 2016 та по Сирії з 2011 по 2016 роки, визначає, що кібератаки (поки що) не є ефективними як інструменти впливу на війні.

Перед повномасштабним вторгненням підрозділи хакерів з рф активізувалися. Наприклад, можна згадати що в період з 2021 по 2022 роки цілями росії стали близько 150 військових і урядових установ із доменами gov.ua та mil.gov.ua. Цілі включали військові й дипломатичні організації та урядові агенції, які управляють критичною інфраструктурою.

Протидіяти кіберзагрозам та кібератакам тоді почали вітчизняні фахівці з кібербезпеки, що отримали підготовку в українській мережі закладів освіти системи підготовки кадрів у сфері кібербезпеки, яка складається з:

-53 закладів освіти, що здійснюють підготовку бакалаврів, та 25 закладів освіти, які готують магістрів за спеціальністю «Кібербезпека»;

-51 закладу вищої освіти, що організовують підвищення кваліфікації фахівців із питань інформаційних технологій і кібербезпеки;

-133 навчальних центрів, які здійснюють комплексну підготовку ІТ-фахівців з інформаційних технологій та кібербезпеки;

-62 ІТ-шкіл, які здійснюють навчання підлітків програмуванню, а також створенню власних проєктів у сфері кібербезпеки [32].

Для якісної підготовки й діяльності спеціалістів у питаннях протидії кіберзагрозам необхідно навчати їх за сучасними методиками, розуміючи специфіку їх майбутньої діяльності. Особливості, притаманні сучасній освіті та підготовці фахівців із кібербезпеки, наведені на рис. 3.

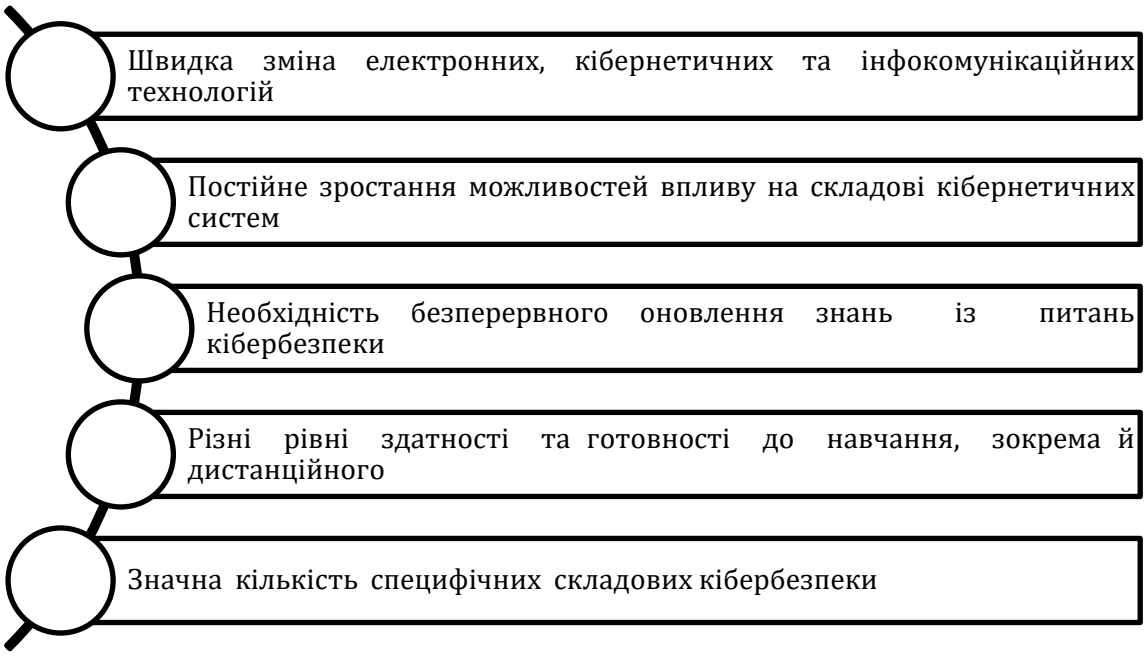

Рис. 3. Особливості підготовки кіберфахівців у сучасних умовах
Джерело: складено автором за [33]

Реалізація підготовки фахівців із кібербезпеки повинна бути здійснена й удосконалена на основі відповідних технічних навичок (hard skills) та, так званих, адаптивних навичок (transferable skills) як частини soft skills. Soft skills і transferable skills є важливими для фахівців із кібербезпеки, але вони мають свої відмінності, які наведено в табл. 1.

Таблиця 1

Порівняння особистісних та адаптивних навичок для підготовки майбутніх фахівців із кібербезпеки

Складові аспекти	Особистісні навички	Адаптивні навички
Природа навичок	Пов'язані з особистісним розвитком і міжособистісними відносинами та містять такі аспекти, як комунікація, лідерство, співпраця, толерантність	Можна використовувати в різних галузях і різних ролях. Вони включають аналітичні навички, управлінські здібності, рішення, вміння працювати в команді
Застосування в кібербезпеці	Комунікація та лідерство важливі для спілкування з іншими фахівцями з кібербезпеки, клієнтами й стейкхолдерами. Вони можуть допомогти вирішувати конфлікти та сприяти побудові довіри у важливих ситуаціях	Аналітичні навички та управління проєктами можуть бути застосовані безпосередньо в аналізі кіберзагроз, розробці стратегій кібербезпеки й управлінні проєктами кібербезпеки
Типові завдання	Допомагають у вирішенні конфліктів, налагодженні співпраці й взаємодії з іншими фахівцями та стейкхолдерами в процесі подолання кіберзагроз	Допомагають у виконанні конкретних завдань, таких як аналіз логів, виявлення вразливостей, створення політик безпеки

Тривалість навчання і розвитку	Розвиваються протягом тривалого часу і можуть вимагати більших зусиль для вдосконалення	Можуть бути набуті швидше, їх можна швидко адаптувати до потреб у сфері кібербезпеки
Важливість у сфері кібербезпеки	Часто вважаються менш пріоритетними, ніж технічні навички, але все ж є необхідними для успіху в галузі кібербезпеки	Є критично важливими, оскільки вони допомагають фахівцям із кібербезпеки адаптуватися до змінних обставин та ефективно розв'язувати різні завдання

Майбутній фахівець із кібербезпеки повинен розвивати й об'єднувати обидві категорії навичок для досягнення ним максимальної ефективності в протидії кіберзагрозам.

Крім того, необхідно зазначити, що військовий вимір кібербезпеки зумовлює появу низки доволі складних етичних питань, які спеціалістам із кібербезпеки доводиться розглядати з урахуванням моральних та етичних аспектів. Необхідно розвивати етичні стандарти, щоб забезпечити відповідальне використання кіберзброї та кібератак у воєнних конфліктах і зберегти імідж держави на міжнародному рівні.

Висновки

Отже, робота спецслужб росії в інформаційному полі Україні відбувалась завжди, але ще більше активізувалася після агресії РФ проти нашої держави. Система підготовки фахівців із кібербезпеки в України є доволі розвиненою, оскільки сформована з декількох ланок.

До основних компонентів кібербезпеки належать безпека мережі, захист кінцевої точки, шифрування даних, поінформованість про безпеку та навчання, реагування на інциденти та управління, відповідність вимогам, управління ідентифікацією та доступом. Найнебезпечнішими загрозами для кібербезпеки є кібершпигунство та кібертероризм.

Основними документами, згідно з якими відбувається процес забезпечення кібербезпеки та протидії кіберзагрозам, визначено Закон «Про основні засади забезпечення кібербезпеки України» та Указ Президента № 447. Саме вони регулюють діяльність державних органів у напрямах захисту даних, подолання інформаційних загроз та запобігання пошкодженню військової та цивільної інфраструктури.

Результатом наукової роботи стали рекомендації для вдосконалення підготовки фахівців із кібербезпеки, які наголошують на важливості формування в майбутніх спеціалістів низки необхідних для роботи особистісних та адаптивних навичок. Підготовка фахівців з кібербезпеки повинна здійснюватися та вдосконалюватися на основі відповідних технічних навичок (hard skills) та так званих адаптивних навичок (transferable skills), які є частиною soft skills.

У подальших дослідженнях необхідно приділити увагу питанням навчання фахівців із кібербезпеки на основі стандартів організації НАТО, співпраці закладів вищої освіти і військових структур щодо підготовки фахівців із кібербезпеки саме в контексті захисту систем озброєнь та військових об'єктів Збройних сил України.

Список використаних джерел

1.Онищенко С. В., Глушко А. Д. Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз. *Економіка і регіон*. 2022. № 1 (84). С. 13–20.

2.Омельченко А. В. Організаційно-правові засади забезпечення кібербезпеки України. *Київський часопис права.* 2021. № 3. С. 140–145.

3.Колосовський Є., Калюжна А., Матвієнко О. Значення кібербезпеки у забезпеченні національної безпеки України в умовах воєнного стану. *Наука і техніка сьогодні*. 2024. № 2 (30). С. 90–99.

4.Сичов О. Л. Ситуаційний аналіз кібербезпеки Міністерства Оборони України. *Стратегії кіберстійкості: управління ризиками та безперервність бізнесу*: матеріали Всеукраїнської наук.-практ. конф., м. Київ, 23 лютого 2023 р. Київ, 2023. С. 27–29.

5.Смілянец Є., Білаш О., Плахотний А. Щодо кібербезпеки в умовах воєнного стану. *Інноваційна наука: пошук відповідей на виклики сучасності* : матеріали І Міжнар. наук. конф., м. Одеса, 22 грудня 2023 р. Одеса, 2023. С. 166-170.

6.Мазник Л. В., Двуліт З. П. Управління діяльністю фахівців із кібербезпеки в умовах повномасштабного вторгнення. *Менеджмент та підприємництво в Україні: етапи становлення і проблеми розвитку*. 2023. № 2 (9). С. 54–65.

7.Кулешов М. Об'єкти критичної інфраструктури як об'єкт забезпечення кібербезпеки в умовах збройної агресії. *Вісник Пенітенціарної асоціації України*. 2022. № 4. С. 50–58.

8.Поліщук В. П. Міжнародне право і кібербезпека: визначення правового статусу кібератак та кібервійськових операцій. *Юридичний науковий електронний журнал.* 2024. № 2. С. 503–506.

9.Бондар Г. Кібервійна в Україні та виклики національній безпеці : кібернапади на цифрову інфраструктуру (державні установи, об'єкти критичної інфраструктури та організації третього сектору). *Публічне управління та регіональний розвиток*. 2022. № 15. С. 30–67.

10.Васильків Б. Л. Кібербезпека як напрямок захисту інформаційно-комунікаційного сектору в сучасних умовах. *Економіка та управління національним господарством*. 2023. Вип. 1 (71). С. 15–19.

11.Островський С. О. Правовий статус військ зв'язку та кібербезпеки в системі Збройних сил України. *Київський часопис права*. 2022. № 3. С. 86–91.

12.Фесьоха В. В., Кисиленко Д. Ю., Нестеров О. М. Аналіз спроможності існуючих систем антивірусного захисту та покладених у їхню основу методів до виявлення нового шкідливого програмного забезпечення у військових інформаційних системах. *Системи і технології зв'язку, інформатизації та кібербезпеки*. 2023. № 3. С. 143–151.

13.Пономаров О., Пивоварчук С, Козубцова Л., Козубцов І., Бондаренко Т., Терещенко Т. Гібридна побудова системи кібербезпеки: адміністративно-правові засади військово-цивільного співробітництва. *Кібербезпека: освіта, наука, техніка*. 2023. № 19. С. 109–121.

14.Strucl D. Russian aggression on Ukraine: Cyber operations and the influence of cyberspace on modern warfare. *Contemporary Military Challenges/Sodobni Vojaški Izzivi*. 2022. Vol. 2. pp. 103–123.

15.Aviv I., Ferri U. Russian-Ukraine armed conflict: Lessons learned on the digital ecosystem. International Journal of Critical Infrastructure Protection. 2023. Vol. 4. pp. 1–30.

16.Schatz D., Bashroush R., Wall J. Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*. 2017. Vol. 2/

17.Anderson R. Security engineering: a guide to building dependable distributed systems. John Wiley & Sons, 2020. 1232 p.

18.Tunggal T. What is a Cyber Threat? *UpGuard*. URL: https://www.upguard.com/blog/cyber-threat (дата звернення: 13.04.2024).

19.What are the main components of cybersecurity? *Digitdefence*. URL: https://digitdefence.com/blog/what-are-the-main-components-of-cybersecurity (дата звернення: 12.04.2024).

20.Hammi B., Zeadally S., Nebhen J. Security threats, countermeasures, and challenges of digital supply chains. *ACM Computing Surveys*. 2023. Vol. 14. pp. 1–40.

21.Mayer Lux L. Defining cyberterrorism. *Revista Chilena de derecho y tecnología*. 2018. Vol. 2. pp. 5–25.

22.De Paoli S. et al. A qualitative exploratory study of the knowledge, forensic, and legal challenges from the perspective of police cybercrime specialists. *Policing: A Journal of Policy and Practice*. 2021. Vol. 2. pp. 1429–1445.

23.Li Y., Liu Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports.* 2021. Vol. 7. pp. 8176–8186.

24.Boyte K. J. A comparative analysis of the cyberattacks against Estonia, the United States, and Ukraine: exemplifying the evolution of internet-supported warfare. *International Journal of Cyber Warfare and Terrorism (IJCWT).* 2017. Vol. 2. pp. 54–69.

25.Datta P. Hannibal at the gates: Cyberwarfare & the Solarwinds sunburst hack. *Journal of Information Technology Teaching Cases*. 2022. Vol. 2. pp. 115–120.

26.Gjesvik L., Szulecki K. Interpreting cyber-energy-security events: experts, social imaginaries, and policy discourses around the 2016 Ukraine blackout. *European Security*. 2023. Vol. 1. pp. 104–124.

27.Krasznay C. Case study: The notpetya campaign. *Információés kiberbiztonság*. 2020. pp. 485–499.

28.Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII : станом на 4 квіт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 13.04.2024).

29.Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 14.05.2021 р. №447/2021. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 13.04.2024).

30.MediaSapiens. Зеленський підписав указ про створення Університету інформаційної та кібербезпеки. *ms.detector.media*. URL: https://ms.detector.media/kiberbezpeka/post/27396/2021-05-31-zelenskyy-pidpysav-ukaz-pro-stvorennya-universytetu-informatsiynoi-ta-kiberbezpeky/ (дата звернення: 09.04.2024).

31.Kostyuk N., Zhukov Y. M. Invisible digital front: can cyber attacks shape battlefield events? *Journal of Conflict Resolution*. 2019. Vol. 2. pp. 317–347.

32.Арсенович Л. Понятійно-категоріальний апарат у сфері підготовки фахівців із кібербезпеки органів державної влади України. *Наукові перспективи (Naukovì perspektivi).* 2022. № 2 (20). С. 33–53.

33.Даник Ю. Кіберосвіта та її особливості. *Військова освіта*. 2018. № 2. С. 67–84.