DOI 10.33099/2618-1614-2021-15-2-42-49
УДК: 004.056

А. Д. Білюга,
ад'юнкт кафедри історії війн і воєнного мистецтва, Національний університет оборони України імені Івана Черняховського, підполковник

Кіберзброя: сучасні загрози національній безпеці та шляхи протидії

Функціонування сучасного суспільства визначається низкою факторів, які, зокрема, пов'язані з розвитком комп'ютерних технологій. З поглибленням комп'ютеризації суспільства з'явилась якісно нова сфера обміну інформацією – кіберпростір. Світовий досвід показує, що захист кіберпростору (кібербезпека), поряд із боротьбою з таким негативним феноменом, як тероризм, став чи не найголовнішою проблемою людства.

Потужним засобом проведення незаконних дій та боротьби в кіберпросторі стала кіберзброя. Провідні країни світу розглядають кіберзброю як фактор, потенційно здатний впливати на перебіг воєнних дій і завдавати збитки економіці, порушувати управлінські функції конкретних держав тощо. Ураховуючи різноманітність дефініцій кіберзброї, автором запропоноване власне визначення цього виду зброї, проведений історіографічний опис кіберзброї, розглянутий досвід застосування кіберзброї в різних сферах людської діяльності. Надані пропозиції щодо подальшого поглиблення відносин України з НАТО в боротьбі з кіберзброєю.

Ключові слова: кіберзброя, кіберпростір, комп'ютерні системи, кібератаки, національна безпека, кібербезпека, НАТО.

Постановка проблеми в загальному вигляді. Протягом останніх 5 тис. років від становлення перших держав і до сьогодення неодмінним супутником цивілізації є війни та збройні конфлікти. У них застосовувалися найрізноманітніші види зброї – від мечів і списів до сучасного озброєння та військової техніки. Починаючи з 80-х рр. XX ст. зброя фізичного впливу поступово трансформувалась у кіберзброю, розпочався перехід від кінетичного ураження до інформаційного. Руйнівні наслідки від застосування кіберзброї почали зростати в геометричній прогресії. Наприклад, у журналі *Cybercrime Magazine* зазначено, що кіберзлочинність у світі зростатиме на 15% щороку і до 2025 р. збитки становитимуть 10,5 трлн дол. США порівняно з 3 трлн дол. США у 2015 р. [1]. Тобто за наявності могутнього військового потенціалу кіберзброя поступово набуває більш руйнівного та критично небезпечного характеру, аніж класичні види озброєння та військової техніки.

Аналіз останніх досліджень і публікацій. З розвитком інформаційних технологій міждержавне протиборство набуває нових форм, пов'язаних з боротьбою в кіберпросторі, що в перспективі може трансформуватись у кібервійну. Різні аспекти зазначеної тематики у своїх наукових працях розкривали П. Біленчук, М. Гуцалюк, Ю. Даник, Д. Дубов, М. Козир, В. Костенко, О. Кравчук, П. МакБарні (P. McBurney), С. Меле (S. Mele), Т. Рід (T. Rid.), Т. Ткачук та ін. Зокрема, в монографії Д. Дубова зазначено, що у 2010 р. США вже були готові завдати воєнного удару у відповідь на кібератаки на американські комп'ютерні системи [2, с. 51]. Однак, попри значну кількість наукових праць, присвячених кіберзброї, її визначенню та застосуванню, це питання залишається недостатньо розкритим і потребує подальших наукових досліджень.

Метою статті є аналіз визначень поняття «кіберзброї», визначення потенційних напрямів протидії цьому різновиду зброї та авторські пропозиції щодо вжиття відповідних заходів у сфері забезпечення кібернетичної безпеки України.

Виклад основного матеріалу

Із середини XX ст. за швидких темпів розвитку інформаційно-технічних систем мали місце злочини, пов'язані з незаконним отриманням інформації, порушенням роботи комп'ютерів тощо. Загалом статистику комп'ютерних злочинів вели від 1958 р., злочинами вважали випадки псування і розкрадання комп'ютерного устаткування; крадіжку інформації; шахрайство чи крадіжку грошей, вчинені із застосуванням комп'ютерів, або крадіжку машинного часу. Комп'ютер уперше був використаний як інструмент для пограбування банку в 1966 р. у Міннесоті. У 1968 р. у США було зафіксовано 13 подібних злочинів; у 1975 р. – 85 [3, с. 5–6].

У 1980-х роках з розвитком мережі Інтернет інтерес людства до цифрового (віртуального) простору

кардинально зріс. Це спонукало до створення інститутів, шкіл, курсів і навчальних програм, метою яких було всебічне опанування комп'ютерних систем та Інтернету. Удосконалення інформаційних технологій створило умови для ефективного розвитку суспільства: комунікаційні засоби стали невід'ємною складовою діяльності людей у всіх сферах, комп'ютери розширили комунікаційні, просторові та часові межі. Водночас мережа Інтернет стала засобом отримання величезних прибутків, зокрема й нелегальних. Цей процес стимулював дії шахраїв-хакерів, які активізували злочинну діяльність із використанням комп'ютерів у мережі Інтернет. Так, у 1981 р. у мас-медіа з'явилась інформація про появу комп'ютерного вірусу та його вплив на комп'ютерні системи [4, с. 92], у 1985 р. за допомогою комп'ютерного вірусу було виведено з ладу систему голосування Конгресу США [5, с. 11]; 2000 р. – вірус Jer розмістили на одному із сайтів, що поклало початок новій технології поширення вірусів у мережі Інтернет і мало «епідемічний» характер [6, с. 21]. Починаючи від 1970-х рр. і до початку XXI ст. кіберзброю визначали як комп'ютерні віруси, метою яких було викликати несправність у певній операційній системі чи окремій сервісній програмі (*табл. 1–2*) [7, с. 7–15].

З розвитком Інтернету речей (англ. Internet of Things, IoT – система речей, що під'єднані до мережі Інтернет), зокрема промислового Інтернету (англ. Industrial Internet of Things, IioT – система об'єднаних комп'ютерних мереж) спостерігається тенденція зростання впливу комп'ютерних вірусів не лише на окремі комп'ютери, а й на комп'ютерні системи загалом, що інколи набувало руйнівного характеру державних масштабів (*табл. 2*).

Однією з характерних особливостей кінця XX ст. стало підвищення функціонування обчислювальної техніки та інформаційно-комунікаційних систем на якісно новий рівень. Прогрес таких технологій спонукав військово-політичне керівництво провідних країн світу зосередити увагу на забезпеченні безпеки кібернетичного середовища від впливу кіберзброї. Так, у США протягом 1994 р. було зафіксовано більш ніж 300 тис. випадків несанкціонованого втручання злочинців у федеральні комп'ютерні мережі; приблизно 30 країн, зокрема Іран, активно вели розробки технологій, цільовим призначенням яких було ведення інформаційної війни, яка могла би стати для США «кібернетичним Чорнобилем» [8, с. 696]. Такі дії злочинних структур і радикально налаштованих країн стали «сигналом» для провідних країн до забезпечення належного рівня національної безпеки.

Сучасний цифровий простір і швидкий розвиток інформаційних технологій створили новітнє середовище обміну інформацією та застосування кіберзброї, який прийнято називати кіберпростір. В українському законодавстві «кіберпростір» визначається як середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних [9].

Інший підхід до кіберпростору пропонують у Північноатлантичному альянсі. У Доктрині ведення операцій у кіберпросторі зазначено, що кіберпростір – це глобальний домен з'єднаних між собою комунікаційних, інформаційних та інших електронних систем, мереж та їхніх даних, у яких обробляється, зберігається та передається інформація [10]. Фахівці НАТО наголошують на тому, що кіберпростір є ширшим, ніж Інтернет. Засоби, досяжні

Таблиця 1

Вплив вірусів на комп'ютери

	Назва комп'ютерного вірусу						
	Creeper	Rabbit	Elk Cloner	Brain	Virus Hoax	One Half	I Love You
Рік	поч. 1970-х	1974	1981	1986	1988	1994	2000
Цільове призначення	Збій системи	Зниження продуктивності системи	Перевертання зображення, повідомлення з погрозами	Виведення з ладу дискет	Зміна конфігурації портів і напряму обертання дисководів	Повна втрата даних на дисках	Увімкнення за замовчуванням обробника скриптів і приховування розширень приєднаних файлів

Таблиця 2

Вплив вірусів на працездатність комп'ютерних систем

	Назва комп'ютерного вірусу			
	Backdoor	Slammer	P2P ботмережі	Троянські програми
Рік	Початок 2000-х	2003	2007	2008 – теперішній час
Цільове призначення	Самостійне під'єднання зловмисників до комп'ютерів та їх зараження	Сповільнення швидкості мережі Інтернет, знищення мережі Інтернет у країні	Незаконне проникнення через мережу Інтернет, WAP/GPS та шахрайське заволодіння інформацією	Ураження комп'ютерних систем державного масштабу, отримання інформації про користувачів, отримання доступу до мобільних телефонів, смартфонів тощо

через кіберпростір, можуть бути об'єктами застосування кіберзброї, зокрема технічні прилади, що не під'єднанні до мережі Інтернет.

У США кіберпростір не пов'язують виключно з комунікаційними, інформаційними та іншими електронними системами, зокрема у Стратегії національної кібербезпеки США кіберпростір згадується як компонент фінансового, соціального, державного та політичного життя Америки [11, с. 1].

Виходячи із цього, можемо дійти висновку, що кіберпростір перетворився не лише на окрему, поряд із традиційними – «земля», «море», «повітря» та «космос» – сферу збройної боротьби, а й став невід'ємною частиною повсякденної людської діяльності.

Разом з тим, опанування кіберпростору кіберзлочинцями призвело до масштабніших проявів застосування вірусних програм, унаслідок чого на урядових порталах мали місце «викрадення» чи пошкодження службової інформації, світові економічні компанії та об'єкти атомної енергетики зазнавали величезних збитків. Наприклад, у червні 2017 р. кібератака на Україну за допомогою вірусу Petya завдала значних збитків державному сектору і бізнесу, заморозивши бізнес-процеси в країні на кілька днів. Серед постраждалих державних інституцій – Кабінет Міністрів України, КП «Київський метрополітен», Національний поштовий оператор «Укрпошта», Міжнародний аеропорт «Бориспіль» тощо.

Фактично кіберзброя стала зброєю першого удару, метою якої є системні порушення управління та функціонування держави противника; як цілі для ураження чи взяття під контроль почали розглядатися не лише збройні сили, їхні системи управління, інфраструктура та комунікації, а й об'єкти економіки, населення та керівництво держави [12, с. 14]. Отже, розвиток ІТ-технологій, активне використання мережі Інтернет і незаконні дії кіберзлочинців призвели до появи абсолютно нового виду зброї, який отримав назву «кіберзброя».

Світова практика свідчить, що не існує єдиного визначення «кіберзброї», оскільки вона постійно функціонально модифікується та вдосконалюється. Проте деякі національні та міжнародні документи дають зрозуміти сутність цього явища. Міжнародною групою вчених у Керівництві із застосування норм міжнародного права в кібервійнах зазначено, що кіберзброя є засобом ведення кібервійни, що має наступальний характер. За своїм задумом та призначенням вона здатна пошкоджувати, знищувати, спричиняти тяжкі наслідки в процесі застосування. До кіберзасобів можна віднести будь-який пристрій, прилад чи механізм, обладнання чи програмне забезпечення, що використовується для ведення кібератак [13, с. 141–142]. Результатом впливу на інформаційні системи можуть стати людські жертви, вплив на інфраструктуру, «параліч» певної сфери економіки, банківської системи чи дезорганізація системи управління під час ведення воєнних дій.

У статті «Кіберзброя» (Cyber-Weapons) американські вчені Т. Рід та П. МакБарні розглядають кіберзброю як один з видів зброї: комп'ютерний код, який використовується з метою погрози чи заподіяння фізичної, функціональної та психологічної шкоди структурам, системам чи фізичним особам [14].

Італійський спеціаліст із кібербезпеки Стефано Мелє пропонує визначення кіберзброї в міжнародно-правовій площині. На думку автора, кіберзброєю може бути пристрій чи будь-який набір інструкцій для комп'ютера, що використовується в конфліктах між державними та недержавними суб'єктами з метою заподіяння (прямо чи опосередковано) фізичних збитків людям чи предметам, а також пошкодження та/або виведення з ладу інформаційних систем [15, с. 7].

Фахівці з питань боротьби в кіберпросторі А. Медін та С. Марінін стверджують, що кіберзброя – це спецзасоби, які мають руйнівний вплив на комп'ютерні системи та мережі противника. Нею може бути будь-який інструмент нанесення збитків противнику, що володіє стандартизованим спеціальним програмним забезпеченням [16, с. 3].

Загальновідомим прикладом застосування кіберзброї стало використання комп'ютерного вірусу «Stuxnet». Вірус набув поширення у 2010 р. як перша програма, що була скерована проти енергосистем Ірану [17]. Метою вірусу стали комп'ютерні системи, які контролювали атомні електростанції. Фактично Stuxnet вважається різновидом кіберзброї, створеним за підтримки певної держави (держав). Створення комп'ютерного вірусу «Stuxnet» стало можливим завдяки масштабній розвідувальній операції на об'єкті критичної інфраструктури, де були порушені основні принципи побудови системи безпеки комп'ютерних систем.

Вважаємо, що термін «кіберзброя» (англ. cyber-weapons) слід розуміти як поєднання двох понять, де «кібер» (англ. cyber) характеризує процес, що відбувається в інформаційних мережах зв'язку, переважно в Інтернеті; «зброя» (англ. weapon) – засіб для нападу на когось (щось) [18].

У Законі України «Про основні засади забезпечення кібербезпеки України» зазначено, що кібератака – це спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти

кіберзахисту [9]. Тобто у вузькому розумінні кібератака – це замах на комп'ютерну безпеку інформаційної системи, а в широкому вона розглядається як пошук рішень, методів, кінцевою метою яких є отримання контролю над віддаленою системою для дестабілізації її працездатності. Таким чином, кібератаки проводяться із застосуванням кіберзброї (інформаційно-комунікаційних технологій, програмного забезпечення, комп'ютерного технічного обладнання тощо), яка застосовується переважно спеціально підготовленими особами в галузі кібернетики та інформаційних технологій.

У процесі дослідження розвитку кіберзброї автором виявлені деякі суперечності, наявні в чинних документах США. Наприклад, у Стратегії національної кібербезпеки США (2018) зазначено, що противники (Росія, Китай, Іран та Північна Корея) безперервно виготовляють нову та ефективну кіберзброю [11, с. 2–3]. Водночас у Словнику військових та суміжних термінів Міністерства оборони США (зі змінами від січня 2021 р.), який є основним документом у військовій термінології збройних сил США, термін «кіберзброя» (cyber-weapon) не згадується; запропоновані лише визначення «кіберпростір» (cyberspace), «кібератака» (cyberspace attack), «можливості кіберпростору» (cyberspace capability), «кібероборона» (cyberspace defense), «використання кіберпростору» (cyberspace exploitation), «операції в кіберпросторі» (cyberspace operations), «кібербезпека» (cybersecurity) та «перевага в кіберпросторі» (cyberspace superiority) [19, с. 55–56].

У Національній стратегії з кібербезпеки Великої Британії на 2016–2021 рр. відсутнє формулювання визначення «кіберзброї», проте зазначені дефініції «кіберзалежних злочинів» (cyber-dependent crimes) та «кіберзлочинів із застосуванням кіберпростору» (cyber-enabled crimes). Далі пояснюється, що «кіберзалежні злочини» – це злочини, які можуть бути вчинені тільки використовуючи інформаційно-комунікаційні пристрої, котрі можуть виступати як інструментом злочину, так і його ціллю (наприклад розробка та поширення шкідливих програм з метою фінансового збагачення, злом з метою викрадення, пошкодження, викривлення або знищення даних та/або мережі чи діяльності); «злочини із застосуванням кіберпростору» – «традиційні» злочини (наприклад шахрайство чи викрадення даних), масштаб яких можна збільшити за рахунок комп'ютерів, комп'ютерних мереж та інших інформаційно-комунікаційних технологій [20, с. 17]. Аналіз дефініцій «кіберзалежні злочини» та «злочини із застосуванням кіберпростору» в кримінально-правовій площині дає підстави стверджувати, що будь-які злочинні дії в кіберпросторі відбуваються безпосередньо із застосуванням кіберзброї. У свою чергу, такі дії є проявом суспільно-небезпечного явища, яке прийнято називати «кібертероризмом».

Для уточнення сутності поняття «кіберзброї» пропонується порівняльна таблиця (*табл. 3*).

Отже, виходячи з наведеного вище, автор пропонує таке визначення:

Кіберзброя – технічно-технологічний комплекс, що складається зі спеціального комп'ютерного обладнання, технологій та програм, призначених для цілеспрямованого порушення роботи інформаційно-технічних систем, викривлення, пошкодження, заволодіння або знищення критично важливої інформації, що може призвести до катастрофічних наслідків техногенного характеру.

Кіберзброя є важливим, ефективним і відносно економним компонентом проведення нелегальних операцій у кіберпросторі, що породжує такий негативний феномен, як кіберзлочинність. Кіберзлочини як складова організованої злочинності мають тенденцію до зростання і набули транснаціонального характеру.

Протидія незаконній діяльності у кіберпросторі стала нагальною проблемою для суспільства та потребує рішучих заходів. Проведений аналіз наступальної дії кіберзброї надає можливість сформулювати підходи до розв'язання цієї проблеми. Міжнародний досвід протидії кіберзброї має відносно давню історію. У 1947 р. США, Канада, Велика Британія, Австралія та Нова Зеландія як члени Англосаксонського клубу створили секретну систему «ECHELON» – першу систему, яка на початковій стадії свого функціонування забезпечувала уряди зазначених країн розвідувальною інформацією, переважно військового характеру, про країни Варшавського договору. На той час не існувало комп'ютерних систем та Інтернету, але керівництво країн об'єктивно оцінювало реальні та потенційні загрози й урахувало існуючий науково-технічний прогрес [21]. На цей час система «ECHELON» трансформована в інші структури, але продовжує виконувати безперервний моніторинг операцій, які ведуться в комп'ютерних системах: банківські перекази, перехоплення інформації кримінального характеру, прослуховування та перехоплення телефонних розмов, відстежування локації кіберзброї, запобігання кібертероризму тощо. Отже, *ця система виконує функції кіберрозвідки та є надзвичайно важливим механізмом протидії кіберзброї в усьому світі.*

Науковці факультету комп'ютерних наук Університету Бундесвера (ФРН) Р. Кох та М. Голлінг досліджували вплив кіберзброї на складні системи зброї [22]. У результаті досліджень вони встановили, що її функціональність базується передусім на аналізі та ідентифікації кібератак, установленні джерел кіберзброї та її знешкодження (*рис. 1*):

- планування на випадок надзвичайної ситуації (*Emergency Planning*) – передбачає наявність плану дій у таких випадках;
- управління ризиками (*Risk Management*) – необхідність створення єдиної системи управління ризиками, пов'язаними із застосуванням кіберзброї;
- система постачання (*Supply Chain*) – особлива увага зосереджена на виробленні єдиних вимог щодо закупівлі «надійних» комплектуючих частин та програмного забезпечення;

Таблиця 3

Порівняльна таблиця кіберзброї та її впливу

№ з/п	Автор/джерело	Складові кіберзброї, її призначення та вплив		
		Компоненти/суб'єкти застосування	Призначення	Об'єкт впливу
1.	Керівництво із застосування норм міжнародного права в кібервійнах	Пристрій, прилад, механізм, обладнання, програмне забезпечення	Пошкодження, знищення, тяжкі наслідки	Системи зброї, системи управління, цивільні та військові особи тощо
2.	Т. Рід та П. МакБарні	Комп'ютерний код	Погроза, заподіяння шкоди	Структури, системи, фізичні особи
3.	С. Меле	Пристрій чи будь-який набір інструкцій для комп'ютера	Заподіяння фізичних збитків; пошкодження та/або виведення з ладу	Люди, предмети, інформаційні системи
4.	А. Медін, С. Марінін	Спецзасоби	Руйнівний вплив, нанесення збитків	Комп'ютерні мережі, стандартизоване спеціальне програмне забезпечення
5.	Закон України «Про основні засади забезпечення кібербезпеки України» (визначення «кібератака»)	Засоби електронних комунікацій (включно з інформаційно-комунікаційними технологіями, програмними, програмно-апаратними засобами, іншими технічними й технологічними засобами та обладнанням)	Порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту	Безпека інформаційної системи
6.	Національна стратегія з кібербезпеки Великої Британії (визначення «кіберзалежні злочини»)	Пристрої на основі інформаційно-комунікаційних технологій	Розробка та поширення шкідливих програм, злом з метою викрадення, пошкодження, викривлення чи знищення даних та/або мережі або діяльності	Інформаційно-комунікаційні пристрої
7.	Національна стратегія з кібербезпеки Великої Британії (визначення «злочини із застосуванням кіберпростору»)	Пристрої на основі інформаційно-комунікаційних технологій	Шахрайство чи викрадення даних	Фізичні особи, комерційні компанії, організації

• *Hardware Regeneration by Design* – забезпечення стабільної роботи основної системи зброї (з довгим життєвим циклом) при заміні комерційних електронних комплектуючих (з коротким життєвим циклом), тому пропонується під час замовлення нових систем зброї визначати вимоги до таких замін ще на стадії проєктування зазначених систем;

• виробничі потужності (*Production Capabilities*) – розвиток оборонної технологічної та промислової бази ЄС, зокрема виробництво власних електронних компонентів для найважливіших систем зброї;

• аналіз загроз (*Threat Analysis*), на підставі якого визначаються заходи за всіма визначеними компонентами протидії.

Ураховуючи досвід провідних країн та міжнародних організацій щодо протидії кіберзброї, нам необхідно критично оцінювати боротьбу в кіберпросторі, вирішувати питання протидії кіберзброї, тобто переходити до активних принципів оборони. У цьому контексті необхідно підкреслити важливість функціонування Національного координаційного центру кібербезпеки, який є робочим органом Ради національної безпеки і оборони України

Рис. 1. Методи запобігання та захисту від кіберзброї [22]

[23]. Діяльність цього органу базується на забезпеченні координації діяльності суб'єктів національної безпеки та оборони України під час реалізації Стратегії кібербезпеки України, підвищенні ефективності системи державного управління у формуванні та реалізації державної політики у сфері кібербезпеки.

Поряд із цим, в Україні ефективно діє урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA (*Computer Emergency Response Team of Ukraine*), яка функціонує в рамках Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України [24]. Основною метою діяльності CERT-UA є системний захист діяльності державних інститутів та громадян України від незаконного доступу в кіберпростір нашої держави, протидія кіберзброї тощо. *Проте цей орган не має повноважень слідчого органу і не може здійснювати слідчі дії та притягати до відповідальності кіберзлочинців*.

На виконання спільних Директив Міністерства оборони України та Генерального штабу Збройних Сил України завершився черговий етап реформування Збройних Сил України, в результаті якого в загальнодержавній системі боротьби з кіберзброєю в лютому 2020 р. створено новий орган військового управління – Командування Військ зв'язку та кібернетичної безпеки Збройних Сил України [25]. Проте, на нашу думку, термін «кібернетична безпека» не повною мірою відповідає чинному законодавству. Відповідно до змін, внесених у Закон України «Про оборону», зазначено, що «Підготовка держави до оборони в мирний час включає... здійснення заходів з кібероборони (активного кіберзахисту) для захисту суверенітету держави та забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройній агресії...» [26]. Отже, *доцільним було би визначення «Командування Військ зв'язку та кібернетичної оборони Збройних Сил України»*.

Значним кроком у забезпеченні кібербезпеки України стало ухвалення Радою національної безпеки і оборони України Стратегії кібербезпеки України на 2021–2025 роки [27]. Важливим стратегічним завданням зазначеного документа є створення у складі Збройних Сил України окремого роду військ – сил кібероборони, забезпечивши його належними фінансовими, кадровими і технічними ресурсами для стримування збройної агресії в кіберпросторі та відсічі агресору.

З 2014 р. Російська Федерація веде гібридну війну проти України, проте масштаби цієї війни поширюються не лише на політичну, економічну, військову та інформаційну сфери, а й на війну в кіберпросторі, що супроводжується регулярними кібератаками. У зв'язку із цим в Україні вже створена система протидії кіберзброї та боротьби з нею. Водночас вважаємо, що ця система має певні вразливості:

- недостатньо розвинені виробничі потужності, що забезпечують розроблення та виготовлення електронно-обчислювальних машин, переважно комплектуючі частини та програмне забезпечення забезпечуються іноземними постачальниками;
- закупівля імпортного програмного забезпечення створює ризики щодо наявності шпигунських складових, які можуть дестабілізувати роботу комп'ютерної мережі та бути об'єктом кібератак;
- державні органи та суб'єкти забезпечення кібербезпеки не спроможні повністю контролювати процеси, які відбуваються в мережі Інтернет, адже вузли управління цією «павутиною» розташовані, як правило, поза межами України;
- рівень фінансування кібернетичної галузі не дає змоги надійно забезпечувати захист від кіберзброї, що значно підвищує ризики кібератак.

Розв'язання зазначених проблем є вкрай важливою складовою забезпечення національної безпеки України та потребує підтримки, насамперед з боку НАТО, де питанням боротьби в кіберпросторі приділяється велика увага.

У Північноатлантичному альянсі значна увага приділяється питанню захисту мереж зв'язку та інформаційних систем, а також надається сприяння союзникам щодо підвищення кіберзахисту на національному рівні [28, с. 19]. Створено групу кіберзахисту швидкого реагування, щорічно проводяться навчання «Кіберлокація» з метою вироблення інноваційних рішень у сфері кіберзахисту.

Пріоритетними цілями партнерства України з НАТО у військовій сфері, зокрема у сфері кіберзахисту, є розвиток спроможностей органів державної влади та військового управління. Виконавши всі військово-політичні процедури, у червні 2020 р. Україна отримала статус партнера НАТО з розширеними можливостями [29], що надало можливість Україні долучитися до спільних програм, зокрема в боротьбі з кібертероризмом. На цей час триває переговорний процес щодо участі України в аналітичному процесі (NATO reflection process) для формування Стратегічної концепції НАТО-2030 [30]. У результаті подальшої співпраці Україна матиме можливість отримати досвід боротьби країн – членів НАТО в протидії кіберзброї та брати безпосередню участь у міжнародних заходах у сфері кібербезпеки.

Висновки

Ураховуючи поточну ситуацію в Україні у сфері запобігання впливу кіберзброї, на нашу думку, було б доцільно:

- підвищити рівень кіберзахисту об'єктів критичної інфраструктури держави та приватного сектору, насамперед тих, які розташовані в районі проведення операції Об'єднаних сил і належать до юрисдикції Міністерства оборони України та Збройних Сил України;
- ужити заходів для вдосконалення комплексної системи кібербезпеки, яка виконувала би функції на випередження кібератак, ідентифікації джерел кіберзброї та її фінансування;

• провести критичний аналіз кадрового забезпечення підрозділів кібербезпеки, їхньої вкомплектованості, перспектив проходження військової служби майбутніх офіцерів за спеціальністю «Кібербезпека»;

• внести пропозиції щодо створення міжнародних підрозділів з кібербезпеки, що значно підвищить ефективність їхньої діяльності в боротьбі з кіберзброєю;

• удосконалити нормативно-правове забезпечення у сфері кібербезпеки з урахуванням сучасних загроз національній безпеці України.

Таким чином, забезпечення кібербезпеки, запобігання кібератакам та знищення кіберзброї противника повинні бути пріоритетом для України. Навіть попри позитивні зміни в питаннях забезпечення кібербезпеки ця система потребує подальшого вдосконалення. Держава повинна володіти необхідними інструментами та можливостями з нейтралізації реальних і потенційних загроз національній безпеці України. Вважаємо, що найефективніший спосіб протидії кіберзброї – це збільшення інвестування в кібербезпеку, координація дій складових сектору безпеки та оборони у сфері кібербезпки та їх інтеграція в єдину структуру, подібну до кібервійськ країн – членів НАТО.

Перелік літератури

1. *Morgan S.* 2021 Report: Cyberwarfare in the C-Suite [Електронний ресурс] : Cybercrime facts and statistics : Jan 21, 2021 / S. Morgan ; Cybersecurity Ventures // Cybercrime Magazine. – Режим доступу : https://cybersecurity ventures.com/wp-content/uploads/2021/01/ Cyberwarfare-2021-Report.pdf.

2. *Дубов Д. В.* Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. – К. : НІСД, 2014. – 328 с.

3. Комп'ютерний тероризм: суперхакери, кібер-терористи, кібер-криміналісти / П. Д. Біленчук, М. В. Гуцалюк, О. В. Кравчук, М. В. Козир ; за заг. ред. П. Д. Біленчука. – К. : Наука і життя, 2008. – 291 с.

4. *Расторгуев С. П.* Инфицирование как способ защиты жизни. Вирусы: биологические, социальные, психические, компьютерные / С. П. Расторгуев. – М. : Яхтсмен, 1996. – 332 с.

5. *Безруков Н. Н.* Компьютерные вирусы / Н. Н. Безруков. – М. : Наука, 1991. – 160 с.

6. *Цветков В. Я.* Технологии и системы информационной безопасности : аналитический обзор / В. Я. Цветков. – М. : ВНТИЦ, 2001. – 89 с.

7. Комп'ютерна вірусологія : навч. посібник / за заг. ред. Б. В. Наркіна. – К., 2012. – 309 с.

8. *Антипенко В. Ф.* Борьба с современным терроризмом: международно-правовые подходы / В. Ф. Антипенко. – К. : ЮНОНА-М, 2002. – 723 с.

9. Про основні засади забезпечення кібербезпеки України [Електронний ресурс] : Закон України № 2163-VIII від 5 жовтня 2017 р. / Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2163-19#Text.

10. Allied Joint Doctrine for Cyberspace Operations [Електронний ресурс] : NATO Standard AJP-3.20 : Edition A Version 1 : January 2020 // NATO Standardization Office. – Режим доступу : https://nso.nato.int/nso/zPublic/ap/PROM/AJP-3.20%20EDA%20V1%20E.pdf.

11. National Cyber Strategy of the United States of America [Електронний ресурс] : September 2018 // The White House. – Режим доступу : https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

12. *Даник Ю. Г.* Кібербезпека до кібероборони / Ю. Г. Даник, С. І. Вдовенко // Оборонний вісник. – 2020. – № 10. – С. 10–15.

13. Tallinn Manual on the International Law Applicable to Cyber Warfare [Електронний ресурс] // Cambridge University Press. – Режим доступу : https://doi.org/10.1017/CBO9781139169288.

14. *Rid T.* Cyber-Weapons [Електронний ресурс] / T. Rid, P. McBurney // The RUSI Journal. – 2012. – Volume 157, Issue 1. – P. 6–13. – Режим доступу : https://doi.org/10.1080/03071847.2012.664354.

15. *Mele S.* Legal Considerations on Cyber-Weapons and Their Definitions [Електронний ресурс] / S. Mele // Journal of Law & Cyber Warfare. – 2014. – Vol. 3, № 1. – P. 52–69. – Режим доступу : https://www.jstor.org/stable/26432559.

16. *Мелин А. В.* Использование киберпространства террористическими и экстремистскими организациями / А. В. Мелин, С. О. Маринин // Зарубежное военное обозрение. – 2012. – № 10 (787). – С. 3–8.

17. Stuxnet – перша цифрова зброя-вірус? [Електронний ресурс] // BBC News Україна. – Режим доступу : https://www.bbc.com/ukrainian/news/2011/02/110215_stuxnet_virus_oh.

18. Definition of weapon noun from the Oxford Advanced Learner's Dictionary [Електронний ресурс] // Oxford Learner's dictionaries – Режим доступу : https://www.oxfordlearnersdictionaries.com/definition/english/weapon?q=weapon.

19. DOD Dictionary of Military and Associated Terms [Електронний ресурс] : as of January 2021 // Joint Chiefs of Staff. – Режим доступу : https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

20. National Cyber Security Strategy 2016–2021 [Електронний ресурс] // UK Government. – Режим доступу : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

21. *Perrone J.* The Echelon spy network [Електронний ресурс] / J. Perrone // The Guardian. – Режим доступу : https://www.theguardian.com/world/2001/may/29/qanda.janeperrone.

22. *Koch R.* Weapons systems and cyber security – a challenging union / R. Koch, M. Golling // Proceedings of 2016 8th International Conference on Cyber Conflict: Cyber Power, 31 May – 03 June 2016, Tallinn, Estonia / NATO CCD COE Publications. – Tallinn, 2016. – P. 191–203.

23. Про Національний координаційний центр кібербезпеки [Електронний ресурс] : Указ Президента України № 242/2016 від 07 червня 2016 р. / Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/242/2016#Text.

24. Computer Emergency Response Team of Ukraine. – Режим доступу: https://cert.gov.ua/about-us.

25. Перший етап реформування Збройних Сил суттєво наблизив їх до набуття взаємосумісності з НАТО, – Андрій Таран. – Режим доступу: https://www.kmu.gov.ua/news/pershij-etap-reformuvannya-zbrojnih-sil-suttyevo-nabliziv-yih-do-nabuttya-vzayemosumisnosti-z-nato-andrij-taran.

26. Про оборону України [Електронний ресурс] : Закон України № 1932-XII від 6 грудня 1991 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1932-12#Text.

27. Глава держави провів засідання РНБО, на якому застосовано санкції до злодіїв у законі та доручено провести аудит державних земель у Конча-Заспі та Пущі-Водиці [Електронний ресурс] // Офіційне інтернет-представництво Президента України. – Режим доступу : https://www.president.gov.ua/news/glava-derzhavi-proviv-zasidannya-rnbo-na-yakomu-zastosovano-68465.

28. *Голопатюк Л.* Адаптація до загроз / Л. Голопатюк, І. Пилипчук // Україна до НАТО. – 2019. – № 1 (1). – С. 16–19.

29. Програма розширених можливостей НАТО для України: у Міноборони назвали всі переваги (УНН) [Електронний ресурс] // Офіційний вебсайт Міністерства оборони України. – Режим доступу : https://www.mil.gov.ua/ministry/zmi-pro-nas/2020/07/24/programa-rozshirenih-mozhlivostej-nato-dlya-ukraini-u-minoboroni-nazvali-vsi-perevagi-(unn).

30. Ольга Стефанішина: Україна прагне долучитися до аналітичного процесу NATO reflection process для формування Стратегічної концепції НАТО-2030 [Електронний ресурс] // Урядовий портал. – Режим доступу : https://www.kmu.gov.ua/news/olga-stefanishina-ukrayina-pragne-doluchitisya-do-analitichnogo-procesu-nato-reflection-process-dlya-formuvannya-strategichnoyi-koncepciyi-nato-2030.