DOI: https://doi.org/10.26565/1992-2337-2024-1-26
УДК 355/359

Живило Євген Олександрович,
кандидат наук з державного управління,
докторант кафедри публічної політики
навчально-наукового інституту "Інститут державного управління"
Харківського національного університету імені В. Н. Каразіна,
майдан Свободи, 4, м. Харків, 61022, Україна,
e-mail: zhivilka@i.ua https://orcid.org/0000-0003-4077-7853

МІЛІТАРИЗАЦІЯ ВИКЛИКІВ ТА ЗАГРОЗ В КІБЕРПРОСТОРІ ЯК ОПЕРАЦІЙНОМУ СЕРЕДОВИЩІ

Анотація. Цільові вектори захисту фундаментальних національних інтересів України у кіберпросторі орієнтуються не тільки на колективну кібербезпеку, які реалізується за допомогою держав-партнерів і союзників, але і на власну систему кібероборони, яка не тільки здатна конкурувати в умовах гібридних загроз, але й стримувати їх агресивну і нецивілізовану спрямованість та протидіяти їм в кіберпросторі.

Сучасний кіберпростір – це набагато більше, ніж просто мережа Інтернет чи сукупність будь-яких інших комп'ютерних мереж, доступ до яких можливий лише через певні програмні застосунки, налаштування чи авторизацію, або використання стандартних і нестандартних комунікаційних протоколів чи портів. Всі елементи мереж (системи), доступ до яких відкриває кіберпростір, можуть бути потенційними цілями та потенційними загрозами.

Кіберпростір надає відповідні можливості як для дружніх чи нейтральних сил (військ), так і для противника (потенційного противника). Залежність збройних сил від кіберпростору пов'язана з певними ризиками, однак вона також формує потребу щодо створення і розвитку відповідних спроможностей військ (сил).

Отже, в статті розкривається суть операційного середовища, яке являє собою сукупність умов, обставин та чинників, що впливають на застосування сил і засобів. Обґрунтовано, його складові які пов'язані з конкретним фізичним або віртуальним простором, а також набір спроможностей військ (оперативних, бойових, спеціальних) та навичок, необхідних для планування і проведення операцій.

Ключові слова: операційне середовище, кіберпростір, кібербезпека, кіберзагрози, кібервплив, кібероперація.

Як цитувати: Живило Є. О. Мілітаризація викликів та загроз в кіберпросторі як операційному середовищі. *Державне будівництво.* 2024. № 1 (35). С. 344–359. DOI: https://doi.org/10.26565/1992-2337-2024-1-26

In cites: Zhyvylo, Ye.O. (2024). Militarization of challenges and threats in cyberspace as an operational environment. *State Formation, no. 1 (35), 344–359.* DOI: https://doi.org/10.26565/1992-2337-2024-1-26 [in Ukrainian].

Постановка проблеми. Сучасний етап технологічного розвитку демонструє, що динаміка освоєння кіберпростору (далі – КП) лише набирає обертів. Завдяки цьому його розвиток, включаючи "мілітаризацію", стає все стрімкішим, тоді як фізичні простори залишаються відносно стабільними і майже не змінюються.

Щоб повністю реалізувати потенціал технологій, провідні держави співставляють своє національне економічне бачення з пріоритетами національної безпеки. При цьому якщо ризики для безпеки, пов'язані з поширенням інфраструктури та інтернет-додатків на основі інформаційно-комунікаційних технологій, належним чином не збалансовані з комплексними національними стратегіями кібербезпеки (далі – КБ) та планами забезпечення стійкості, то країни не зможуть досягти економічного зростання та цілей національної безпеки, яких вони прагнуть. У відповідь на це країни розвивають як наступальні, так і оборонні спроможності для захисту від незаконної і протиправної діяльності в КП і попередження інцидентів до того, як вони зможуть завдати шкоди їхнім країнам.

Зважаючи на зазначене необхідно зауважити, що практично всі держави світу безперервно збільшують свої арсенали кіберзброї, застосування якої може призвести до незворотніх та руйнівних наслідків. Як правило, її застосування на першочергових етапах спрямовується на інформаційно-комунікаційні системи державних органів влади та об'єкти критичної інформаційної інфраструктури з метою виведення їх з ладу, отримання прихованого доступу і контролю [7], здійснення розвідувальної та розвідувально-підривної діяльності. В подальшому вона активно використовується агресором як елемент спеціальних інформаційних операцій з метою маніпулятивного впливу на населення, втручання у виборчі процеси та дискредитації ознак державності.

Перше виважене політичне рішення про необхідність проведення скоординованих заходів з кібероборони України та формування військової кіберскладової, а саме кіберсил Збройних Сил України (далі – ЗС України) було прийняте на засіданні Ради національної безпеки і оборони України 14 травня 2021 року. Це рішення було введене в дію указом Президента України [1].

Вважається що основною метою створення військової кіберскладової у складі ЗС України є стримування кібератак з боку противника, приватних військових компаній або організованих хакерських угрупувань, які здійснюють агресивні дії в КП, спрямовані на порушення суверенітету та недоторканності України. Іншим завданням нового роду військ є відсіч воєнної агресії у КП, протидія гібридним загрозам та захист від кібератак (ведення кібероборони).

За цих умов визначення та подальша пріоритизація інвестицій і ресурсів для нашої держави є критично важливою для успішного управління ризиками в такій всеосяжній сфері, як КБ.

З цієї точки зору, вважається необхідним узгодити пріоритети КБ з іншими цілями, пов'язаними з інформаційно-комунікаційними технологіями, оскільки вона відіграє центральну роль у досягненні соціально-економічних

цілей сучасної економіки. Національна стратегія повинна відображати, як КБ підтримує ці цілі. Це можна зробити шляхом посилання на існуючі політики, спрямовані на реалізацію цифрового порядку денного або порядку денного розвитку країни, або оцінюючи, як КБ може бути включена в ці політики.

Нарешті, бачення уряду необхідно зосередити на послідовну і здійсненну політику, яка допоможе йому досягти поставлених цілей в сфері захисту національного сегменту КП [6]. Сюди входять не лише кроки, програми та ініціативи, які необхідно здійснити, але й ресурси, виділені для цих зусиль, а також те, як ці ресурси мають бути використані. Аналогічно, процес має визначити показники, які будуть використовуватися для забезпечення досягнення бажаних результатів у рамках встановлених бюджетів і термінів.

Аналіз останніх досліджень і публікацій. Розвиток інформаційного середовища в XXI–му столітті в якості пріоритетного напрямку внутрішньої політики більшості держав світу визначає розвиток інформаційних і комунікаційних технологій, формування насиченого інформаційного середовища і нарощування відповідної інфраструктури. Усі комунікаційні мережі, комп'ютерні системи, обмін інформацією в яких здійснюється на основі використання єдиної системи стандартів і протоколів, дозволяють здійснювати перетворення вихідної інформації в певний інформаційних продукт для конкретного користувача, утворюють базис КП.

Проведений аналіз існуючої національної нормативно-правової бази, наукових робіт які були спрямовані на теоретико-методологічне обґрунтування даної сфери, а також принципи та стандарти які використовуються в збройних силах держав-членів НАТО підтверджує що самі "країни-партнери" ще остаточно не визначили критерії класифікації кібератак (кібероперацій (далі – КО)) як поріг для збройного нападу, що є юридичним наслідком початку здійснення колективної оборони відповідно до статті 5 Північноатлантичного договору.

Так, в стандартах НАТО КП представлений у вигляді трирівневої моделі, кожен з яких характеризує певну площину для планування, проведення або оцінювання операцій [12].

При цьому провідні світові науковці та військові аналітики розуміють та усвідомлюють що сутність КП в контексті операційної діяльності військ (сил) полягає в наступному:

– межі КП не можливо звести до меж будь-якого фізичного простору;

– межі КП можуть рухатися і трансформуватися;

– КП охоплює всю планету і при цьому не позначений на жодній карті світу;

– КП фізично не можливо поділити, аналогічно до адміністративного поділу територій держав, однак принцип адміністративного поділу КП має важливе значення з точки зору юрисдикції та національної відповідальності за дії в КП;

– КП надає спроможності для дружніх сил (військ), нейтральних сил, а також для противника та потенційного противника одночасно;

– основні елементи КП, на відміну від інших фізичних просторів, створені людиною, і тому ризиками в КП можна управляти, здійснюючи маніпулятивні дії в кіберсфері.

Взагалі, представники як цивільного сектору, так і сектору оборони держав-партнерів зазначають, що КП через свої функціональні властивості дає певний простір для маневру, який необхідний для полегшення контролю в усіх операційних середовищах (далі – ОС) (суша, море, повітря, космос) і який впливає на всі етапи операції. Саме тому, свобода дій в КП (в межах дозволених законодавством вимог) є необхідною передумовою для успішного проведення операції і отримання ефектів в усіх (інших) складових ОС.

Метою статті є чітке визначення взаємозв'язку операційного кіберсередовища з іншими ОС та цілісне його сприйняття що має важливе значення для планування і проведення КО.

Виклад основного матеріалу. Операційне кіберсередовище (як підвид ОС) утворюється як визначена частина КП, яка охоплює можливості інформаційно-комунікаційних мереж та інформаційних цифрових технологій (включаючи відповідні ділянки радіочастотного спектру, Інтернет та інші комунікаційні і комп'ютерні мережі, системи) та придатна для планування і проведення КО (ведення активних кібердій), а також створення сприятливих умов для ефективної операційної діяльності і досягнення бажаної мети (рисунок 1).

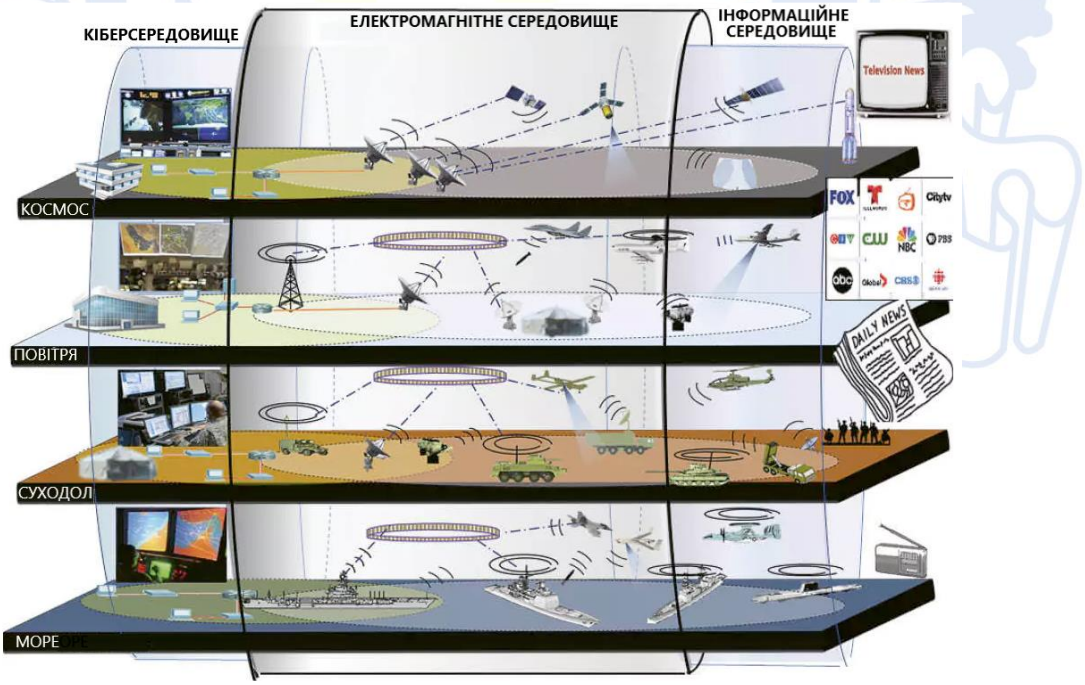

Рисунок 1 – Комплексне ОС
Figure 1 – Complex OS

Операційна діяльність у КП може носити як “індивідуальний” характер, так і “колективний” – на підтримку операцій, що проводяться іншими або об’єднаними силами. В обох випадках, операційне кіберсередовище може використовувати комунікаційні можливості КП, орієнтовані саме на інтеграцію задіяних військових бойових (інтегрованих) спроможностей. Тому, чітке розуміння взаємозв’язку операційного кіберсередовища з іншими підвидовими ОС та цілісне сприйняття ОС має важливе значення для планування і проведення КО.

Складність контролю КП полягає в тому, що він присутній у всіх фізичних просторах (середовищах), і одночасно виходить за визначені командувачем географічні межі операційної зони (військово-сухопутні, військово-повітряні чи військово-морські зони), що в результаті може ускладнити ведення операційної діяльності.

При цьому домінування у КП має виходити за рамки комунікаційних та інформаційних технологій і потребує переваги у всіх його складових: соціальній, технічній, комунікаційній, інформаційній, мережевій та у всьому електромагнітному спектрі.

Власне до суб’єктів, які можуть впливати на операційну діяльність ЗС України у КП, відносяться:

1) дружні сили (війська), у тому числі сили складових сектору національної безпеки і оборони, а також збройні сили інших держав, з якими укладено міжнародні договори про колективну оборону;

2) нейтральний або потенційно дружній національний цивільний компонент (оператори мереж електронних комунікацій, надавачі хмарних послуг і послуг обробки даних, споживачі послуг електронних комунікацій, тощо) [3];

3) інші нейтральні суб’єкти (у тому числі збройні сили держав, які у своїй діяльності є нейтральними по відношенню до ЗС України);

4) ворожі суб’єкти (державні та недержавні органи/організації, збройні сили вороже налаштованих держав, окремі фізичні особи та групи осіб, які ведуть кіберзлочинну або кібертерористичну діяльність).

В рамках існуючих кіберзагроз необхідно зауважити, що основною рисою сучасного технологічного розвитку людства є процес всеохоплюючої цифровізації та насичення різних сфер життя і діяльності суспільства (у тому числі і військової складової) сучасними цифровими засобами, системами зв’язку, “розумними” і роботизованими пристроями, засобами дистанційного управління, телеметрії, навігації, персональних супутникових комунікацій. Більшість таких систем, засобів, пристроїв компілюються, об’єднуються в мережі і все в більшій мірі стають залежними від КП.

Внаслідок такої залежності і шкідливої (ворожої) діяльності в КП (кібератаки, КО) всі ці системи, засоби і пристрої стають функціонально вразливими, що є особливо важливим для військового сегменту, оскільки внаслідок такої залежності і функціональної вразливості війська (сили) можуть втратити частину своїх основних спроможностей [4].

Така шкідлива діяльність дозволяє провести певну класифікацію і сформувати базис кіберзагроз, дій, метою яких є нанесення шкоди або порушення роботи комп'ютерних систем, систем зв'язку і комунікацій, викрадення даних або заволодіння інформацією.

У загальному вигляді до них відносяться:

– кіберзагрози національного характеру;

– кіберзагрози зовнішнього характеру;

– кіберзагрози індивідуального характеру;

– кіберінциденти і природні кіберзагрози.

Насамперед вразливими до кіберзагроз є, військові об'єкти, функціонування яких базується на застосуванні комп'ютерних систем та які з'єднуються через КП (Інтернет чи інші комунікаційні мережі).

Також вразливими є системи, доступ до яких здійснюється з використанням електромагнітного спектру (радіочастотного чи інших діапазонів електромагнітного випромінювання) [13].

В такому сенсі, найбільш вразливими військовими об'єктами є військові інформаційно-комунікаційні системи, електронні комунікаційні мережі, які забезпечують ЗС України послугами електронних комунікацій та постачання мереж, а також об'єкти критичної інфраструктури, які входять чи забезпечують діяльність ЗС України (субпідрядники, логістичне забезпечення, тощо) [5], для яких реалізація кіберзагроз може призвести до:

1) виникнення надзвичайних ситуацій;

2) знищення, блокування або руйнування стратегічно важливих сегментів безпеки держави, систем життєзабезпечення та об'єктів підвищеної небезпеки;

3) порушення або унеможливлення діяльності державних органів, органів військового управління та підрозділів ЗС України в цілому;

4) втручання і порушення сталого функціонування автоматизованих систем управління озброєнням та військовою технікою;

5) порушення безпечного функціонування системи ресурсного забезпечення Міністерства оборони України;

6) розголошення державної або розвідувальної таємниці, інформації з обмеженим доступом [15].

Розглядаючи загальну характеристику операційної діяльності сил (військ) у КП або через КП слід розуміти, що це чітко спланована діяльність визначених військ (сил), пов'язана з використанням засобів впливу (кіберозброєння) на КП (елементи КП), основною метою якої є створення необхідних ефектів для досягнення визначених військових цілей.

Операційна діяльність сил (військ) у КП стикається з тими самими викликами, що і операційна діяльність військ (сил) в інших фізичних доменах. Відповідно, базові принципи операційної діяльності у різних фізичних доменах застосовуються і до операційної діяльності у КП, однак інтерпретація цих принципів може відрізнятися через певні особливості кібердіяльності. Наприклад, діяльність різних складових збройних сил/сил оборони у фізичних

доменах зазвичай обмежена законами природи. Подібно до цього, діяльність у КП має свої специфічні обмеження, визначені властивостями КП як фізичного, так і віртуального характеру.

Характерною рисою сучасної операційної діяльності у КП є те, що повноцінними сторонами конфлікту, окрім державних військових формувань, можуть бути також приватні військові компанії, організовані (координовані) злочинні групи та окремі кіберзлочинці (кібертерористи), що робить перелік суб'єктів операційної діяльності у КП значно ширшим.

У стратегічному розумінні операційна діяльність військ (сил) у КП має вплив на глобальні процеси в соціальному, економічному та фінансовому сегментах, на промисловість та стратегічні системи управління військами та озброєнням, процеси у суспільстві [2], воєнну логістику, що за відповідною спрямованістю та скоординованістю заходів призведе до ефекту (наслідків) загальної або суттєвої втрати противником (потенційним противником) спроможностей розпочати або підтримувати у середньостроковій або довгостроковій перспективі розпочату збройну агресію (застосування сили) проти України, у тому числі в КП.

У рамках планування та здійснення операційної діяльності в КП, останній розділяють на:

1) власний захищений КП – так званий "синій сегмент КП", в якому можна досягти повної юрисдикції ЗС України та інших складових національної системи КБ чи держав-союзників або партнерів України;

2) КП противника (потенційного противника) – так званий "червоний сегмент КП", в якому противник (потенційний противник) може досягнути/досягає повної юрисдикції;

3) нейтральний КП – так званий "сірий сегмент КП", в якому неможливо визначити чи досягти чіткої юрисдикції будь-якою із сторін або меж юрисдикції іншими суб'єктами, які можуть впливати на військову операційну діяльність у КП.

За цих умов будь-які дії (кібердії) в рамках операційної діяльності військ у КП, представляють собою особливий специфічний вид військових дій асиметричного характеру, насамперед, у форматі застосування військової сили.

Асиметричність характеру таких дій визначається спроможностями однієї, більш розвиненої військової кіберскладової, значно послабити спроможності противника (потенційного противника), у тому числі якщо останній суттєво переважає його у чисельності особового складу, розвиненості та вогневих (бойових) спроможностях збройних сил.

У загальному розумінні основною метою КО є створення визначальних умов для досягнення бажаних ефектів у КП або з його використанням, які дозволяють отримати стратегічну, оперативну (операційну), а в окремих випадках оперативно-тактичну перевагу над противником, звести нанівець або значно послабити його спроможності до прояву військової агресії та/або продовження ведення бойових дій, а також зберегти свободу дій і забезпечити

ефективну реалізацію спроможностей своїх та дружніх військ (сил) у збройному протистоянні.

Водночас КО не є альтернативою застосуванню засобів вогневого ураження, оскільки передбачає зміну вирішальних умов та досягнення ефектів на стратегічному та оперативному напрямках і має бути скоординована з іншими заходами військового характеру. Більшість КО (кіберкампаній) проводять приховано та анонімно, завдяки чому сплановані спеціальні заходи в інтересах підготовки та проведення КО важко визначити, розпізнати і проаналізувати.

За замислом, КО поділяються на стратегічні та оперативні. Кожна з них спрямована на вирішення конкретних завдань відповідного рівня, серед яких виділяються наступні:

1) вплив на воєнно-політичну систему противника для суттєвого зниження його воєнних та економічних спроможностей для військової агресії, оперативного прийняття ефективних рішень тощо;

2) вплив на системи управління або супутні системи забезпечення функціонування стратегічно важливих об’єктів противника/потенційного противника (у т.ч. подвійного призначення) з метою їх блокування, зведення нанівець їх функціоналу, або взагалі – функціональне знищення;

3) унеможливлення запуску, зміна польотних завдань стратегічних ракет, ударних безпілотних літальних апаратів стратегічного рівня чи комбінованого впливу на системи управління таких засобів повітряного ураження з метою їх функціонального/фізичного знищення або перенацілювання, в ідеальних умовах – на об’єкти подвійного чи військового призначення;

4) приховане проникнення у системи управління стратегічною зброєю противника, перехоплення контролю і управління цими системами;

5) блокування систем управління військами, інформаційно-комунікаційних систем противника, передача заздалегідь помилкових команд, наказів і розпоряджень (особливо у ході активної фази ведення бойових дій) тощо.

Слід наголосити, що при плануванні та проведенні КО необхідно враховувати, що противник (потенційний противник) може діяти у відповідь, а його кібердіяльність може бути спрямована як на послаблення спроможностей дружніх військ (сил), так і на здійснення кібервпливу на конкретні елементи “синього сегменту КП” або інші сили (засоби), залежні від КП. Саме тому, постійність, всебічність та цілеспрямованість ситуаційної обізнаності про стан КП в мирний час, ворожу діяльність противника (потенційного противника) у КП, “сірий і червоний сегменти КП” має важливе значення для належного оцінювання загроз і ризиків.

Так при проведенні КО основним способом впливу прийнято вважати “безпосередній”, який здійснюється на військові комп’ютерні системи (у тому числі комп’ютеризовані системи подвійного призначення, мережу Інтернет та інші комунікаційні/комп’ютерні мережі) через військових субпідрядників

противника (потенційного противника) [12], або в інший спосіб експлуатації вразливостей його комп'ютерних систем та персоналу, які тісно пов'язані з будь-якими ланками управління збройних сил і забезпеченням спроможностей (наприклад, воєнно-промисловий комплекс, навчальні заклади і установи, громадяни та громадські організації, які беруть участь у забезпеченні чи підтриманні збройної агресії противника тощо).

Як правило, під час підготовки та проведення КО може виникнути потреба в залучені цивільних осіб, які мають спеціальні знання та навички, з метою формування парадигми кіберстримування, програмування бажаних ефектів чи цілевказівок, досягнення визначальних точок КО, проникнення в мережі/системи тощо [10].

Схема проведення КО структурує операційне кіберсередовище і проблему, а також визначає або уточнює операційні лінії та фази, які формують цілісну логіку КО.

Процес управління КО поетапно переводить сформовану схему до безпосередніх дій шляхом інтеграції, координації, синхронізації, визначення пріоритетів і розподілу спроможностей між функціональними операційними одиницями.

Слід зауважити, що попри чітку спланованість заходів для відповідного сценарію будь-який план КО у процесі реалізації потребує уточнення з урахуванням змін у ОС.

Так КО завжди передбачає діяльність на логічному рівні мереж в КП, а їх реалізація здійснюється шляхом введення різноманітних даних, послідовності команд та/або кодів, з метою досягнення замислу та визначених цілей (досягнення вирішальних умов та створення ефектів).

Всупереч цьому, кінетичні удари (атаки), наслідком яких є фізичне знищення об'єкту (наприклад, фізичне знищення центру управління або обробки даних, кабелів та ліній зв'язку тощо), не відносяться до кібердій (кібервпливу), але можуть бути сплановані як кінетичні заходи в рамках конкретної КО.

Основними цілями оборонних КО є збереження можливості використання властивостей власного захищеного КП ("синього сегменту КП") та захист мереж, систем та пристроїв, залежних від КП та даних, шляхом протидії шкідливій діяльності суб'єктів, які можуть впливати на операційну діяльність збройних сил у КП.

Основна мета оборонної КО полягає у протистоянні чи нейтралізації конкретної кіберзагрози та повернення скомпрометованого елементу КП (мережі, системи, об'єкту) в безпечний і повнофункціональний стан.

Отже, будь-яка оборонна КО ґрунтується на комплексному застосуванні кіберспроможностей відповідних складових ЗС України та суб'єктів національної системи КБ, а також на можливому використанні спроможностей інших недержавних постачальників послуг та мереж, приватних дослідників потенційних вразливостей [14], з метою своєчасного виявлення,

супроводження, аналізу, припинення дії та протидії кібератакам противника (потенційного противника).

При цьому типовими заходами активного захисту власного сегменту КП, які реалізуються в рамках оборонної КО є:

1) створення окремих ресурсів-приманок (т.зв. Honeypot), які дозволять визначити мету та/або вектор кібератаки/ворожої КО, вивчити стратегію, перелік засобів та методів кібератак тощо;

2) створення пасток (приманок), які інтегровані між існуючими інформаційно-комунікаційними ресурсами (т.зв. Deception technology) для створення помилкового сприйняття противником (нападником) успішності проведення кібератаки шляхом перенаправлення на оманливий ресурс у внутрішньому периметрі;

3) активний пошук слідів компрометації (злому, проникнення у внутрішній периметр, тощо) або функціонування шкідливого програмного забезпечення, які не виявляються стандартними засобами захисту (т.зв. Threat hunting).

Додатковими заходами, які також можуть бути реалізовані в рамках оборонної КО цього типу, є заходи пасивного захисту у власному “захищеному сегменті КП”, зокрема:

1) перевірка (аудит) адміністрування прав доступу, профайлів доступу до ресурсів в інформаційно-комунікаційних системах та автоматизованих системах управління технологічними процесами [16], перевірка оновлення антивірусних програм на усіх комп’ютерах та серверах, перевірка мережевих екранів (фаєрволів) тощо;

2) сканування на вразливості (т.зв. Vulnerability scanning), яке здійснюється програмними та апаратними засобами з метою діагностики та моніторингу мережевих комп’ютерів і програм для виявлення можливих проблем безпеки, оцінювання та усунення відомих вразливостей;

3) пошук та виявлення потенційних вразливостей інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем та електронних комунікаційних мереж із залученням зовнішніх координаторів та команд дослідників (т.зв. Penetration testing) [8].

Наступальна КО – це форма ведення активних військових дій в КП, які проецирують силу для досягнення цілей, створення вирішальних умов та досягнення бажаних ефектів, що задовольняють визначені ключові показники ефективності.

Відтак, за своєю цільовою спрямованістю наступальна КО орієнтована переважно на “червоний сегмент КП” і проводиться з метою створення ефектів першого порядку, які дозволяють отримувати каскадні ефекти у фізичних доменах шляхом кібервпливу на системи управління військами і зброєю, командування, логістику, високопріоритетні цілі противника (потенційного противника).

Проведення наступальної КО, що має стратегічний замисел, допускається лише за умови ухвалення відповідного рішення вищим командуванням ЗС України під час дії правового режиму воєнного стану, а у мирний час – вищим військово-політичним керівництвом держави [9].

За своєю суттю КО можуть мати прямий і непрямий вплив на противника (потенційного противника). Основна направленість таких впливів включає (але не обмежується) наступними ефектами:

– Захищеність. Провести компрометацію конфіденційності, цілісності та доступності визначених частин КП, а також даних, що зберігаються або обробляються у противника (потенційного противника).

– Ізоляція. Блокування комунікацій, які використовує противник для здійснення спрямованої діяльності в його уражених системах.

– Стримування. Поширення шкідливого коду/послідовності команд/діяльності, які деградують функціонування систем.

– Нейтралізація. Поширення шкідливого коду/послідовності команд/діяльності для унеможливлення здатності противника (потенційного противника) протягом певного часу впливати на відновлення, конфіденційність, цілісність та доступність відповідних частин системи.

– Маніпуляція. Контроль, змінення або порушення конфіденційності, цілісності та доступності інформації, систем та/або мереж противника з метою сприяння досягненню цілей операцій дружніх сил і задуму командувача.

– Просочування. Збір, завантаження, розкриття або заволодіння інформацією через несанкціонований доступ.

– Погіршення. Заборона доступу або істотне зниження експлуатаційних показників певного сегменту його систем до найнижчого рівня його пропускної здатності та/або продуктивності. Зазвичай бажаний рівень таких заборон і зниження визначається заздалегідь.

– Виведення з ладу. Повна заборона доступу до системи, або до її використання на певний період часу. Зазвичай, визначається бажаний час початку та закінчення такого часового проміжку. Виведенням з ладу можна вважати окремий випадок деградації системи, якщо рівень деградації становить 100 відсотків на визначений період часу.

– Знищення. Повна і безповоротна відмова в доступі до системи (інформації) або її експлуатації, причому система (інформація) в такому випадку зазнає максимального впливу, як з точки зору часу простою, так і з точки зору заподіяної шкоди.

Підсумовуючи необхідно зазначити, по-перше, що будь-які кібердії в рамках операційної діяльності військ у КП повинні вибудовуватись на всеосяжному розумінні та аналізу загального цифрового середовища, але при цьому вони мають бути адаптовані до обставин та пріоритетів країни.

По-друге, КБ – це не лише технічний виклик, але й складне багатогранне питання, аспекти якого виходять за межі економічного та соціального

процвітання і стосуються таких сфер, як правоохоронна діяльність, національна та міжнародна безпека, міжнародні відносини, торговельні переговори та сталий розвиток.

По-третє, важливо розуміти всі аспекти КБ і те, як вони взаємопов'язані, потенційно доповнюючи або конкуруючи один з одним. На основі цього розуміння та аналізу конкретного контексту країни можна визначити пріоритети відповідно до цілей і визначених часових показників. При цьому пріоритети дозволять встановити конкретні цілі і терміни, а також розподілити необхідні ресурси.

Вкрай важливо зрозуміти що цифрове середовище стало критично важливим для урядів, організацій та приватних осіб. Ці групи стикаються з ризиками КБ і несуть певну відповідальність за управління ними залежно від своєї ролі. З цієї причини урядам доцільно налагоджувати партнерські відносини та механізми співпраці, щоб залучити приватний сектор і громадянське суспільство до реалізації визначених завдань [11]. Хоча це може бути доволі складним завданням. Але виконавши його, в подальшому це допоможе зрозуміти потреби зацікавлених сторін, їхні унікальні знання та досвід, що сприятиме співпраці для досягнення мети та цілей в ході проведення КО.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямку.

Беззаперечно, що цифрове середовище має потенціал для прискорення економічного зростання та соціального прогресу, просування ключових суспільних цінностей, покращення надання державних послуг та зміцнення потенціалу, сприяння міжнародній торгівлі та розвитку належного врядування.

За цих умов постає зростаюча залежність функціонування суспільства від цифрового середовища. Однак КБ не є самоціллю. Слід звернути увагу на свободу вираження поглядів, конфіденційність комунікацій та захист персональних даних.

Разом з тим, глобальність, взаємозв'язок, віртуальність, швидкість обміну інформацією виступає ключовим компонентом сучасного світу, функціонуючи як унікальне ОС, яке інтегрує цифрові, інформаційні та комунікаційні технології. Це середовище охоплює широке коло інформаційних систем, мереж та інфраструктур, які забезпечують безперервний потік даних і комунікацій між користувачами, організаціями та державами.

Тому КП як ОС є невід'ємною частиною сучасного життя, забезпечуючи численні можливості для розвитку, але при цьому також вимагає постійної уваги до питань безпеки та захисту від загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про рішення Ради національної безпеки і оборони України від 14.05.2021 р. “Про Стратегію кібербезпеки України” : Указ Президента України від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 30.03.2024);

2. Onyshchenko Svitlana, Zhyvylo Yevhen, Cherviak Anna, Bilko Stanislav. Determining the patterns of using information protection systems at financial institutions in order to improve the level of financial security. *Eastern-European Journal of Enterprise Technologies*. 2023. Vol. 5 (13 (125). P. 65–76.

3. Порядок реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі : Постанова Кабінету Міністрів України від 04.04.2023 р. № 299. Дата оновлення: 04.04.2023. URL: https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#n12 (дата звернення: 10.04.2024).

4. Koval M., Sova O., Orlov O., Zhyvylo Y., Zhyvylo I. Improvement of complex resource management of special-purpose communication systems. *Eastern-European Journal of Enterprise Technologies*. 2022. 5(9-119). P. 34–44.

5. Mahdi Q. A., Zhyvotovskyi R., Kravchenko S., Borysov I., Orlov, O., Panchenko I., Zhyvylo Y., Koltovskov D., Boholii S. Development of a method of structural-parametric assessment of the object state. *Eastern-European Journal of Enterprise Technologies*. 2021. 5 (4 (113)). C. 34–44. DOI: https://doi.org/10.15587/1729-4061.2021.240178

6. Живило Є. О., Орлов О. В. Сутність кібербезпеки національного сегменту кіберпростору держави в умовах кризового управління. *Збірник наукових матеріалів XXII Міжнародного науково-го конгресу “Публічне управління XXI століття в умовах гібридних загроз”* 27 квітня 2022 р. Київ : Харківський національний університет імені Василя Назаровича Каразіна, 2022. С. 248–254.

7. Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом : Постанова Кабінету міністрів України від 11 листопада 2020 р. № 1176. URL: https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#Text

8. Special Publication 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS) URL: https://csrc.nist.gov/pubs/sp/800/94/final

9. Живило Є.О. Геостратегічні гравці сучасного кіберпростору. Загрози, виклики, наслідки : монографія. C91 Moderní aspekty vědy: XLV. Díl mezinárodní kolektivní monografie / Mezinárodní Ekonomický Institut s.r.o.. Česká republika: Mezinárodní Ekonomický Institut s.r.o., 2024. P. 29–63. URL: http://perspectives.pp.ua/public/site/mono/mono-45.pdf (дата звернення: 30.03.2024).

10. Zhyvylo Y. Exploring and Acquiring Modern Human Resource Competencies in Cybersecurity Amidst State Digital Transformation. Pressing Problems of Public Administration. 2023. 2(63), 111–127. DOI: https://doi.org/10.26565/1684-8489-2023-2-08 (дата звернення: 30.03.2024).

11. Zhyvylo Y. O., Zhyvylo I. O. Joint training of the cyber security defense forces personnel in the conditions of total state defense. Theory and Practice of Public Administration. 2021. 2(73). 144–153. DOI: https://doi.org/10.34213/tp.21.02.16

12. NATO Standard, Allied Joint Publication No 3.20 Allied Joint Doctrine For Cyberspace Operations, 2020, (AJP–3.20), STANAG 6514. URL: https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

13. Joint Doctrine Note 1/18 – Cyber and Electromagnetic Activities, 2018, UK, (JDN 1/18). URL: https://assets.publishing.service.gov.uk/media/667d6471c7f64e23420900d6/ARCHIVE-JDN_1_18_Cyber_and_electromagnetic_activities.pdf

14. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2469-VIII. Дата оновлення: 28.07.2022. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 30.03.2024).

15. Про державну таємницю : Закон України від 21.01.1994 р. № 3855-XII. Дата оновлення: 01.01.2024. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 30.03.2024).

16. О. Данілов: Кіберзахист державних інформаційних ресурсів – важлива складова у процесі цифрової трансформації країни, 2020. [Електронний ресурс]. URL: https://www.rnbo.gov.ua/ua/Diialnist/4606.html (дата звернення: 30.03.2024).

Стаття надійшла до редакції 06.04.2024 р.
Стаття рекомендована до друку 15.05.2024 р.

Zhyvylo Y.O.,
doctoral candidate of the Department of Economic Policy and Management
Educational and Scientific Institute «Institute of Public Administration»
of V. N. Karazin Kharkiv National University,
4 Svobody Sq., Kharkiv, 61022, Ukraine
e-mail: zhivilka@i.ua https://orcid.org/0000-0003-4077-7853

MILITARIZATION OF CHALLENGES AND THREATS IN CYBERSPACE AS AN OPERATIONAL ENVIRONMENT

Annotation. The target vectors for the protection of fundamental national interests of Ukraine in cyberspace are oriented not only to collective cyber security, which is implemented with the help of partner states and allies, but also to its own cyber defense system, which is not only able to compete in conditions of hybrid threats, but also to deter their aggressive and uncivilized orientation and countering them in cyberspace.

Modern cyberspace is much more than just the Internet or a collection of any other computer networks, access to which is possible only through certain software applications, settings or authorization, or the use of standard and non-standard communication protocols or ports. All elements of networks (systems), access to which opens cyberspace, can be potential targets and potential threats.

Cyberspace provides appropriate opportunities for both friendly or neutral forces (armies) and for the enemy (potential enemy). The dependence of the armed forces on cyberspace is associated with certain risks, but it also creates a need for the creation and development of the corresponding capabilities of the troops (forces).

So, the article reveals the essence of the operational environment, which is a set of conditions, circumstances and factors affecting the use of forces and means. It is substantiated that its components are related to a specific physical or virtual space, as well as a set of capabilities of troops (operational, combat, special) and skills necessary for planning and conducting operations.

Keywords: operational environment, cyber space, cyber security, cyber threats, cyber influence, cyber operation.

REFERENCES

1. On the decision of the National Security and Defense Council of Ukraine dated 05/14/2021 "On the Cybersecurity Strategy of Ukraine": Decree of the President of Ukraine dated 08/26/2021 No. 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (date of application: 03/30/2024).

2. Onyshchenko, S., Zhyvylo, Ye., Cherviak, A., Bilko, S. (2023). Determining the patterns of using information protection systems at financial institutions in order to improve the level of financial security. *Eastern-European Journal of Enterprise Technologies, vol. 5 (13 (125)), 65–76.*

3. Procedure for response by cyber security entities to various types of events in cyberspace: Resolution of the Cabinet of Ministers of Ukraine dated 04.04.2023 No. 299. Date of update: 04.04.2023. https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#n12 (date of application: 07/30/2024).

4. Koval, M., Sova, O., Orlov, O., Zhyvylo, Y., Zhyvylo, I. (2022). Improvement of complex resource management of special-purpose communication systems. *Eastern-European Journal of Enterprise Technologies. 5(9-119), 34–44.*

5. Mahdi, Q.A., Zhyvotovskyi, R., Kravchenko, S., Borysov, I., Orlov, O., Panchenko, I., Zhyvylo, Y., Kupchyn, A., Koltovskov, D., Boholii, S. (2021). Development of a method of structural-parametric assessment of the object state. *Eastern-European Journal of Enterprise Technologies, 5 (4 (113)), 34–44.* DOI: https://doi.org/10.15587/1729-4061.2021.240178

6. Zhivylo, E.O., Orlov, O.V. (2022). The essence of cyber security of the national segment of the state's cyberspace in the context of crisis management. *Collection of scientific materials of the 22nd International Scientific Congress "Public administration of the 21st century in the context of hybrid threats"* April 27, 2022. Kharkiv: Kharkiv National University named after Vasyl Nazarovych Karazin, 248–254.

7. Resolution of the Cabinet of Ministers of Ukraine dated November 11, 2020 No. 1176 "On approval of the Procedure for conducting a review of the state of cyber protection of critical information infrastructure, state information resources and information whose protection is required by law". URL: https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#Text

8. Special Publication 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS). URL: https://csrc.nist.gov/pubs/sp/800/94/final

9. Zhivylo, E.O. (2024). Geostrategic players of modern cyberspace." Threats, challenges, consequences". Monograph. C91 Moderní aspekty vědy: XLV. Díl mezinárodní kolektivní monografie. Mezinárodní Ekonomický Institut s.r.o.. *Česká republika: Mezinárodní Ekonomický Institut s.r.o., 29 – 63.* URL: http://perspectives.pp.ua/public/site/mono/mono-45.pdf (date of application: 07/30/2024).

10. Zhyvylo, Y. (2023). Exploring and Acquiring Modern Human Resource Competencies in Cybersecurity Amidst State Digital Transformation. *Pressing Problems of Public Administration, 2(63), 111-127*. URL: https://doi.org/10.26565/1684-8489-2023-2-08 (date of application: 03/30/2024).

11. Zhyvylo, Y.O., & Zhyvylo, I.O. (2021). Joint training of the cyber security defense forces personnel in the conditions of total state defense. *Theory and Practice of Public Administration, 2(73), 144-153*. DOI: https://doi.org/10.34213/tp.21.02.16

12. NATO Standard, Allied Joint Publication No 3.20 Allied Joint Doctrine For Cyberspace Operations, 2020, (AJP–3.20), STANAG 6514, URL: https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

13. Joint Doctrine Note 1/18 – Cyber and Electromagnetic Activities, 2018, UK, (JDN 1/18), URL: https://assets.publishing.service.gov.uk/media/667d6471c7f64e23420900d6/ARCHIVE-JDN_1_18_Cyber_and_electromagnetic_activities.pdf

14. On the main principles of ensuring cyber security of Ukraine: Law of Ukraine dated October 5, 2017 No. 2469-VIII. Date of update: 07/28/2022. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (date of application: 03/30/2024).

15. On state secrets: Law of Ukraine dated January 21, 1994 No. 3855-XII. Date of update: 01.01.2024. https://zakon.rada.gov.ua/laws/show/3855-12#Text (date of application: 03/30/2024).

16. Danilov, O. (2020). Cyber protection of state information resources is an important component in the process of digital transformation of the country. URL: https://www.rnbo.gov.ua/ua/Diialnist/4606.html (date of application: 03/30/2024).

The article was received by the editors 06.04.2024.
The article is recommended for printing 15.05.2024.