http://doi.org/10.26565/1727-6667-2024-2-05
УДК 351.865

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

ІНТЕГРАЦІЙНІ ЗАСАДИ КІБЕРНЕТИЧНОГО ТА ЕЛЕКТРОМАГНІТНОГО СЕРЕДОВИЩА

Анотація. В світі останні десять років відбулась трансформація поглядів в питанні створення систем кібербезпеки, інформаційної безпеки та електромагнітної активності які у поєднанні використовуються для придушення, або взагалі блокування роботи випромінюючих комплексів/засобів, подавлення функціонування систем управління та зброєю, взаємодіючих систем, комунікаційних та сервісних платформ.

Це відбулось на тлі прискорення розвитку технологій, а кіберактивність у всесвіті створила складний стан постійної міждержавної конкуренції чи війни. Як слідство, необхідно зробити наголос на тому, що досягнення переваги в такому середовищі, може відбутись лише за умов чіткого осмислення ситуації яка склалась, та за умов постійної адаптації та вдосконалення самої системи.

В Україні продовжується активна робота з удосконалення форм і способів реалізації активних кібердій, а також розвитку механізмів для побудови національної системи кібербезпеки. У сучасному цифровому середовищі кіберзагрози, які постають, стають дедалі складнішими та різноманітнішими, тому забезпечення надійного захисту інформаційної інфраструктури країни є пріоритетним завданням.

Одним із основних напрямків цієї роботи є вдосконалення існуючих технологій і стратегій кібероборони, а також створення нових методів для ефективного реагування на кіберзагрози. У цьому контексті велика увага приділяється розбудові координаційних механізмів між державними органами, приватним сектором і міжнародними партнерами, що дозволяє швидко виявляти та нейтралізувати кіберінциденти.

Важливим аспектом є також розвиток національної системи кібербезпеки, яка включає в себе створення нових нормативно-правових актів, удосконалення кадрової політики та підвищення рівня технічної підготовленості спеціалістів. Це дозволяє не лише забезпечити ефективний захист від зовнішніх та внутрішніх кіберзагроз, але й підвищити стійкість критично важливої інфраструктури України.

Таким чином, удосконалення форм і способів кібердій, а також реалізація механізмів побудови національної системи кібербезпеки, є ключовими елементами стратегії забезпечення національної безпеки України в умовах сучасних викликів.

Ключові слова: *інформаційно-комунікаційні технології, кібернетичне та електромагнітне середовище, інформаційні технології, інформаційна безпека, кібербезпека, кібервплив, активні кібердії.*

Як цитувати: Живило Є. О. Інтеграційні засади кібернетичного та електромагнітного середовища. *Теорія та практика державного управління*. 2024. Вип. 2 (79). С. 99–114. http://doi.org/10.26565/1727-6667-2024-2-05

Вступ. Сьогодні всі країни стикаються з інтенсивною глобальною конкуренцією за вплив, а також із постійно змінним кіберпростором (далі – КП), який несе з собою зростаючі ризики та загрози з боку як державних, так і недержавних акторів. Це змушує посилювати зусилля з метою забезпечення стабільного зв'язку та захисту військових у КП. Провідні держави світу все більше зосереджуються на розвитку та захисті своїх інформаційних ресурсів (далі – ІР), а також на здатності впливати на ІР інших країн, що в цілому становить проблему забезпечення національної кібербезпеки (далі – КБ).

У світі глобалізації жодна держава не може ефективно протистояти сучасним кіберзагрозам (далі – КЗ) без активного інформаційного обміну з іншими країнами. Тому в нормативно-правовій базі України велика увага приділяється співпраці з ЄС, НАТО та іншими міжнародними акторами для забезпечення безпеки КП та спільного захисту від КЗ, зокрема в галузі оборони та військових сфер.

Так провідні країни світу постійно вдосконалюють свої зусилля щодо забезпечення КБ за двома ключовими напрямами, а саме: удосконалення власного законодавства, впровадження власної стратегії КБ та об'єднання у відповідні безпекові організації; створення та нарощування спроможностей власних кібервійськ та національних команд реагування на комп'ютерні інциденти, з одночасним удосконаленням ними форм і способів кібердій (далі – КД) в рамках підготовки до кібервійни (далі – КВ).

В цілому, слід зазначити, що світові тенденції розвитку нормативно-правових документів (далі – НПД) сфери КБ, здійснюються у відповідності до:

- рекомендацій Міжнародного союзу електрозв'язку (ITU), які висвітлюють загальну уяву. Зазначені рекомендації формулюють теоретичні засади розвитку електронних інформаційно-комунікаційних систем/архітектур (далі – ІКС), захисту інформації (далі – ЗІ), інформаційної безпеки (далі – ІБ) та КБ;

- сімейства міжнародних стандартів ISO/IEC 27000, що включають стандарти з ІБ, опубліковані спільно Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC). Обумовлена лінійка міжнародних стандартів розкриває змістовні особливості щодо практичних методів побудови архітектур ІКС, порядку об'єднання та взаємодії ІКС та проведення аудиту з управління ІБ мережі та системи в цілому;

- стандартів (рекомендацій) Національного інституту стандартів і технологій США – NIST та стандартів та специфікацій національного інституту стандартів (ANSI). Ці стандарти (рекомендації) детально розглядають сфери ЗІ, ІБ та КБ, зокрема з практичним акцентом на питання криптографії, організацію

освітніх заходів у сфері КБ та підготовку фахівців, оцінку рівня захищеності КБ-систем, управління ідентифікацією та доступом до мереж, забезпечення конфіденційності, управління ризиками, захист новітніх технологій, а також підтримку надійності мереж та платформ;

- міжнародних нормативних актів і галузевих стандартів, федеральних законів, розпоряджень та політик (PCI-DSS, SOX, MAS-TRM, GDPR Article та інші) [1].

У процесі розвитку національної системи КБ в Україні залишаються кілька ключових питань, які ускладнюють формалізацію безпекової політики в КП. Зокрема, досі бракує системних міжнародних НПД, які б чітко визначали КП та всі його аспекти, пов'язані з безпекою. Крім того, відсутнє визначення правового статусу КП, а на міжнародному рівні не досягнуто консенсусу щодо правил поведінки в цьому середовищі. Існує також значна проблема через відсутність єдиних методологій для оцінки наслідків кіберзлочинів і їхнього розгляду як об'єкта міжнародних норм, зокрема в контексті визнання кібератак (далі – КА) як актів війни.

Аналіз наявних законодавчих актів і НПД України, Європейського Союзу, НАТО та провідних країн, зокрема США, свідчить про значну термінологічну, дефініційну та нормативно-правову невизначеність, а також розбіжності в трактуванні низки понять, що складають базовий термінологічний набір сфери КБ та кібероперацій (далі – КО). Така невизначеність ускладнює розробку єдиних стандартів і підходів до управління КЗ, що, в свою чергу, створює додаткові труднощі у формуванні єдиної політики в цій сфері. Враховуючи ці обставини, вагомою особливістю в реалізації удосконалення форм і способів активних КД є розуміння того, що досягти успіху в цій сфері можна лише за умови ефективного поєднання зусиль Збройних Сил України (далі – ЗС України), складових сил оборони та безпеки держави (далі – СОБД), а також приватного сектору. Лише за умови належної координації між цими елементами можна забезпечити обороноздатність країни у КП. Це передбачає застосування сучасних активних КД у кібернетичному та електромагнітному середовищі (далі – КЕС), зокрема через радіоелектронне протистояння, управління радіочастотним ресурсом і електромагнітним спектром (далі – ЕС), що є основою операцій у КП.

За таких умов, необхідним є нарощування в Україні спроможностей військових підрозділів КБ, зокрема через створення функцій постійного удосконалення форм і способів активних КД. Це повинно супроводжуватися одночасним розвитком національної нормативно-правової бази у сфері КБ відповідно до вимог міжнародного права. Такий комплексний підхід дозволить ефективно реагувати на новітні КЗ, посилити обороноздатність та забезпечити стійкість національної кіберінфраструктури.

Огляд літератури. Сучасний етап технологічного розвитку людства демонструє швидке зростання та трансформацію КП, що стає все більш значущим елементом у глобальній конкуренції і конфліктах. У той час як фізичні простори залишаються відносно стабільними, КП, навпаки, швидко розвивається, зокрема в аспектах його "мілітаризації" [2]. Завдяки технологічному прогресу, можливості його використання в збройних конфліктах (далі – ЗК) значно збільшились, і сьогодні КП є одним з ключових компонентів сучасних військових

операцій. У цьому контексті важливо зазначити, що КП набуває статусу бойового простору, де активно застосовуються методи КВ і агресії, спрямовані на підрив суверенітету інших держав.

Одним з яскравих прикладів такого використання КП є війна Росії проти України, починаючи з 2014 року. Російська Федерація, що є визнаною державою-терористом, активно використовує КЗ як частину своєї гібридної агресії, застосовуючи кібертерористичні методи проти України. З початку конфлікту Росія регулярно нарощує свої кіберспроможності, використовуючи їх для атак на критичну інфраструктуру, державні органи, а також для ведення пропаганди і дезінформації.

Враховуючи постійну загрозу з боку РФ, Україна активно працює над створенням національної системи КБ, зокрема через формування військової кіберскладової. Важливим кроком у цьому напрямку стало рішення Ради національної безпеки і оборони України від 14 травня 2021 року щодо формування Кіберсил ЗС України. Це рішення стало основою для створення організаційної структури, яка повинна забезпечити кіберстримування агресора та протидіяти загрозам в КП. Метою цієї складової є не тільки захист суверенітету України, а й активне протистояння агресії в КП, відбиття гібридних атак і забезпечення кібероборони на всіх етапах ЗК.

Важливою складовою цієї роботи є створення та реалізація ефективних механізмів інтеграції КО із іншими елементами національної безпеки (далі – НБ), такими як радіоелектронна боротьба (далі – РЕБ) та традиційні військові сили. Крім того, Україна активно співпрацює з міжнародними партнерами, зокрема з державами-членами НАТО, для забезпечення колективної КБ.

Доктрина кібероборони України враховує сучасні міжнародні принципи і стандарти, зокрема ті, що застосовуються в НАТО. Однак слід зазначити, що на момент видання Доктрини "Кібероперації ЗС України", травень 2024 року, держави-члени НАТО ще не визначили чіткі критерії класифікації КА як "червоної лінії" для початку ЗК згідно зі статтею 5 Північноатлантичного договору, що залишає певну юридичну невизначеність щодо застосування колективної оборони у випадку КА.

Таким чином, КП став одним із основних бойових просторів, де розвиваються нові методи ведення війни. В Україні особливу увагу приділяють розвитку кібероборони, що включає формування Кіберсил ЗС України та забезпечення інтеграції КО з іншими компонентами НБ.

Отже, технологічні зміни в світі, а також постійні загрози з боку агресивних держав, вимагають швидкої адаптації та розвитку ефективних систем КБ для захисту національних інтересів у КП.

Метою статті є визначення і розкриття шляхів реагування на майбутні виклики сучасного КП, з одночасним наданням загального огляду КО та РЕБ, їх планування, інтеграцію та координацію в рамках кіберелектромагнітної діяльності.

Методологія дослідження полягає в оцінці спроможностей кібервійськ щодо проведення КО та РЕБ в рамках спільних операцій СОБД, зокрема їх ефективної координації та інтеграції у процесі підтримки наземних бойових дій. Дослідження також має на меті визначити фундаментальні зміни в методах і процедурах, які забезпечують синергію між КО та іншими видами боротьби, такими як РЕБ.

Очікувані результати дослідження включають визначення найбільш ефективних методів інтеграції КО та РЕБ в спільні операції, розробку рекомендацій щодо вдосконалення процесів координації між різними підрозділами СОБД, а також оцінку впливу нових методів на підвищення обороноздатності України в КП.

У підсумку, результати цього дослідження повинні сприяти розробці стратегії інтеграції КО та РЕБ в загальний контекст військових операцій, що дозволить підвищити ефективність захисту країни від КЗ і забезпечити координацію СОБД на всіх рівнях.

Основні результати дослідження. Поглиблений ЗІ є де-факто підходом до захисту державних і комерційних мереж протягом більше десяти років. Однак така зосередженість на захисті електронно-комунікаційних мереж та ресурсів призвела до експоненційного зростання витрат на КБ, захисне програмне забезпечення (далі – ПЗ), апаратне забезпечення та навчання для підвищення обізнаності. Поширення КЗ продовжує стимулювати величезне зростання витрат, пов'язаних із безпекою, що споживає більший відсоток корпоративних ресурсів.

Всесвітнє націлювання на критично важливу інфраструктуру та основні послуги становить зростаючу загрозу економічній стабільності та НБ [4]. Поточні умови КЗ вимагають іншого, більш агресивного курсу дій для боротьби з цими зростаючими ризиками. Країни, які мають сили реагування та противаги у безпековому національному сегменті КП, повинні ефективно координувати активні наступальні заходи, щоб заборонити злочинним групам доступ до комп'ютерних ресурсів та мереж.

Більшість розвинутих країн мають добре налагоджені елементи КВ, які цілком здатні виконувати наступальні КО [5]. Більшість цих міжнародних федеральних ресурсів зосереджено виключно на цілях НБ. Разом ці країни могли б застосувати весь спектр своїх наступальних кіберпотенціалів проти злочинних елементів, як це було зроблено для перешкоджання торгівлі наркотиками та глобальному тероризму. Зростаюча загроза секторам критичної інфраструктури створює загрозу міжнародній безпеці, особливо враховуючи, що цільовими є базові послуги.

Існуючі кіберугрупування, як правило, добре організовані і добре фінансуються, володіють широким асортиментом найсучаснішої кіберзброї. Ці злочинні угруповання мають міжнародне охоплення. Тому вкрай важливо утворити коаліцію противаги на міжнародному рівні, щоб боротися з цими злочинними групами [2]. Окремі компанії та країни не можуть ефективно боротися з цією глобальною загрозою лише за допомогою індивідуальних методів захисту. Ця глобальна загроза вимагатиме ефективного міжнародного державно-приватного партнерства, яке створюватиме узгоджений підхід, залучатиме всю силу, можливості та співпрацю відповідних урядів і галузей для надання допомоги у спільній обороні.

Сучасне суспільство у своєму повсякденному житті суттєво залежить від ЕС, ми знаходимся в ньому під час спілкування, користування Інтернетом, під час прослуховування музики і використання багатьох інших бездротових функцій та сервісів. Те саме стосується і військових користувачів. КЕС пронизує всі аспекти військових операцій у всіх сферах, а це означає, що, щоб використовувати його якнайкраще, необхідно розглядати та застосовувати дані складові

комплексно [6]. Тому військовим користувачам необхідно вміти приймати чіткі рішення, діяти, постійно адаптуватися і вдосконалюватися в умовах маніпуляцій, обмана і відмови в доступі в умовах розгалуженого та активного КЕС.

Здатність керувати цим дедалі складнішим і перевантаженим середовищем буде мати вирішальне значення для досягнення та збереження переваги над противником. Враховуючи такі умови необхідно звернути увагу на те, як забезпечена та організована кібер- та електромагнітна активність.

Міжнародні безпекові організації протягом багатьох років проводять збір, обробку та аналіз розгалуженості та розповсюдженість КЕС шляхом впровадження, модернізації технологічних спроможностей радіолокаційних, електрооптичних комплексів зондування та зв'язку. При цьому відомо, що зазначені системи використовуються для перевірки безпеки власних ІКС і їх побудова доволі розгалужена і не однотипна з визначеними зв'язками між ними та об'єднаних єдиним керівництвом.

За цих умов, трансформація поглядів у всьому світі на питання створення систем КБ, ІБ та електромагнітної активності відбулась з прискоренням розвитку технологій, а кіберактивність у світі створила складний стан постійної міждержавної конкуренції чи війни. Як слідство, необхідно зробити наголос на тому, що досягнення переваги в такому середовищі, може відбутись лише за умов чіткого осмислення ситуації яка склалась, та за умов постійної адаптації та вдосконалення самої системи.

Інтеграція КЕС є ключовою для того, щоб держава захищала та підтримувала інформаційні переваги. Концептуально це є поєднання складових що функціонально перетинаються, а саме: кібернетична мережа, електронна обробка та безпека, які зосереджені на системних функціях, отримання доступу і використання даних, захист, збір та маніпулювання, які доповнено інтеграцією різних ІТ-платформ та персоналом.

Кібер складова включає захисні та наступальні КД та бездротові КД, де мають місце знання та можливі маніпуляції на рівні даних або вище. Електронна боротьба стосується розуміння та використання КЕС. Він відрізняється від бездротових КД тим, що працює на рівні нижче декодованих даних. Зв'язок, гідролокатори і електрооптика можуть бути розміщені саме в цій складовій. Безпека охоплює захист спроможностей. Вона включає в себе елементи ЗІ, КБ, виявлення і реагування на КЗ, КО та активного КЗ. Платформи, на яких фізично розгорнуті або розміщені (наприклад, база даних, хмара) відповідні засоби КЗ. Персонал повинен бути повністю інтегрованим в систему операцій.

Жоден із цих компонентів не можна відокремити від інших. Імовірно у разі, порушення зазначеного функціонального поєднання передбачається порушення безпеки, сталого, надійного та штатного режиму функціонування ІКС та/або технологічних систем. При цьому, щоб утримувався сталий режим функціонування комунікативного середовища, спроможності зазначених складових повинні ґрунтуватися на базових принципах відкритих архітектур і стандартів [7]. Це забезпечує гнучкість і адаптивність системи, гарантує стійкі переваги і підтримує необхідність роботи з декількома доменами на декількох розподілених платформах.

Під загальним терміном активне КЕС мається на увазі низка військових операцій яка має бути синхронізована та скоординована. В свою чергу вони характеризуються застосуванням електронних та електромагнітних засобів, захистом, підтримкою, моніторингом, управлінням спектром і безпосередньо активними діями у КП та КО. Щоб зберегти стратегічні переваги та забезпечити успіх проведення операцій, потрібно скоординувати багатофункціональні сфери в космосі, повітрі, на землі та на морі. Противники продовжують шукати нові можливості для використання областей кібер- та ЕС та пов'язаної з ними інфраструктури, особливо в умовах поширення та розгалуженості засобів електронних комунікацій на полі бою.

Загалом кажучи, активні дії в КЕС включають радіоелектронне протистояння, керування радіочастотним ресурсом чи ЕС, що є основою операцій у КП (рис. 1).

Рисунок 1. Активні дії в КЕС
Figure 1. Active Actions in CES

Активне КЕС використовуються військовими для захоплення, збереження, використання та панування над супротивниками як у КП, так і в ЕС. Крім того, КЕС використовується для придушення, або взагалі блокування роботи випромінюючих комплексів/засобів, подавленя функціонування систем управління та зброєю та взаємодіючих систем та комунікаційних, сервісних платформ.

Ключем до всієї роботи КЕС є інтеграція та синхронізація. Інтеграція була розкрита вище. Стосовно синхронізації необхідно зазначити, що вона складається з організації військових дій у часі та просторі, метою якої є досягнення максимальної противаги та потужності у конкретному місці та часі.

Метою КЕС є надання СОБД відповідних спроможностей для підвищення обізнаності про радіочастотний спектр, ситуаційну обізнаність та живучість системи управління. В цілому активне КЕС забезпечує безпечний і безперебійний потік даних та інформації, який дозволяє СОБД швидко реагувати на мінливе поле бою та синхронізуватися з іншими об'єднаними спроможностями відповідних суб'єктів.

Виклики в КП вимагають від держави захистити ІКС всіх форм власності, об'єкти критичної інформаційної інфраструктури, даних/трафіку, включаючи

Інтернет, вбудовані процесори та контролери (бездротові і дротові), комунікаційні системи, які використовуються для задоволення суспільних потреб [8]. Доречи, програмно-апаратні та портативні комплекси (засоби) радіозв'язку також потрапляють у цю категорію, які, по суті, є пристроєм, який поєднує всі попередні технології в одному виконанні.

Окрім цього необхідно зазначити, що за останні роки Війська зв'язку та кібербезпеки ЗС України значно просунулися у вдосконаленні своїх спроможностей та адаптації до швидко мінливого ландшафту загроз у КП [9].

Так одними із найважливіших складових відповідних спроможностей цього роду військ ЗС України є здатність виявляти загрози в КП та реагувати на них, захищатися від КА та їх наслідків [16]. Це особливо важливо, оскільки Україна постійно стикається з КА зі сторони РФ, які(им) часто важко виявити та протистояти [9]. Щоб впоратися з цим викликом, Україна протягом останніх років зробила значні інвестиції в розширення та вдосконалення своїх спроможностей КЗ. Це включає впровадження нових технологій і навчання фахівців, міжнародна співпраця з партнерами, обмін досвідом, проведення навчань та інше [17]. Це дає змогу переконатися, та впевнено стверджувати, що фахівці кіберсфери здатні ідентифікувати та реагувати на останні загрози в КП.

Ще однією важливою складовою частиною спроможностей цих спеціальних військ є їхня здатність щодо запровадження та додержання об'єднаного підходу в побудові та використанні систем зв'язку та інформаційних систем, яка на основі єдиного захищеного інформаційного середовища одночасно поєднує і синхронізує застосування сучасних систем управління, обміну інформацією (розвідки), засобів ураження та нелетального впливу (радіоелектронного, інформаційного впливу, дій у КП тощо) [3].

Загалом, спроможності Військ зв'язку та кібербезпеки ЗС України повинні бути поділені на три основні напрямки: наступальний, оборонний і розвідувальний. Наступальна складова передбачає здатність здійснювати КА на ворожі цілі. Оборонні можливості охоплюють здатність захищати мережі та системи країни від КЗ. Розвідувальний напрямок включає збір, обробку та аналіз інформації щодо КЗ з метою забезпечення раннього виявлення та оперативного реагування на них.

Незважаючи на це, ще у 2021 році Президент України Володимир Зеленський порушив питання створення нового окремого роду військ – Кіберсил ЗС України. Однак до сьогодні цей рід військ не має офіційного юридичного статусу [10]. Ситуація може змінитися у 2025 році, оскільки відповідний законопроєкт (№12349 від 19.12.2024) вже перебуває на завершальних етапах розгляду [11].

Все ж таки Кіберсили ЗС України після завершення етапів формування, повинні мати у своєму розпорядженні низку інструментів і технологій для виконання своїх завдань, включаючи інструменти аналізу зловмисного ПЗ, системи виявлення вторгнень, сканери мережевої безпеки та ПЗ для аналізу даних.

Однією з першочергових проблем, які стоять перед новоствореним органом військового управління, що входить до визначеної законом структури ЗС України, є брак ресурсів і фінансування. Це обмежовує їх здатність отримувати новітні технології та залучати висококваліфікований персонал. Крім того, різні урядові уста-

нови, яким доручено наглядати за операціями в КП в Україні, часто працюють ізольовано, що перешкоджає координації та обміну ресурсами та інформацією [12].

Підсумовуючи, необхідно зробити наголос, що як існуючий, а в подальшому внов сформований рід військ мають/будуть мать певні можливості в наступальних, оборонних і розвідувальних операціях, вони все одно будуть стикаться з кількома викликами, які необхідно вирішити для подальшого підвищення їх спроможностей. Ці виклики включають недостатні ресурси, обмежене фінансування та відсутність координації між різними "суб'єктами", залученими до операцій у КП.

Тому, у рамках КЕС операції в КП пропонується мати трьохрівневу структуру, а саме: наступальні операції в КП, оборонні операції в КП і захист внутрішніх комунікаційних систем та ІР спеціальних користувачів загальнодержавного рівня. Важливим для наступальних операцій в КП є проведення атак у КП. Вони складаються з дій, які створюють різноманітні прямі та непрямі КЗ критичній інформаційній інфраструктурі (порушення, збій або знищення) [15], і маніпуляції, які призводять до відмови в обслуговуванні, яка є прихованою або проявляється у фізичному домені мережі.

Унікальним для КП є те, наскільки він взаємопов'язаний із космічним простором, насамперед через те, що супутники відіграють вирішальну роль у військових телекомунікаціях і мережах, особливо для величезної кількості вимог щодо розташування, навігації та просторово-часових показників. Крім того, взаємозв'язок між КП і космічним простором (обмін даними супутниковими каналами зв'язку в військовому діапазоні) в межах ЕС значно розширює та ускладнює оперативну структуру, перетворюючи концентроване фізичне поле бою на повністю інтегроване глобальне поле бою.

Наприклад, комп'ютерні віруси чи зловмисне ПЗ, запущене в КП, може досягти цільової мети, а в багатьох випадках вражати і підсистеми, на які покладаються інші суб'єкти СОБД [19]. Зазначені взаємозв'язки є важливими міркуваннями при плануванні КЕС в глобальному масштабі.

У КП існують численні проблеми, особливо коли йдеться про використання стеків мережевих протоколів. Часто комунікації базуються на моделі взаємозв'язку відкритої системи (OSI), де часто Інтернет-протокол (IP) поєднується з протоколом керування передачею (TCP) для формування TCP/IP. Ця система розроблена для пакетного обміну критичними даними/інформацією між операціями КЕС, але вона також є однією з причин руйнування архітектури та КА.

Виклики, що зумовлені радіоелектронним протиборством, яке інтегроване через КЕС в основному складається з трьох функцій: активне електронне подавлення, електронний захист і підтримка РЕБ.

На рисунку 2 показані загальні функції радіоелектронного протиборства. Ці функції реалізовуються та застосовуються з повітря, землі, моря, космосу та через КП пілотованими (тобто літаками спостереження) і безпілотними (тобто дронами) або системами без нагляду (тобто автономними БПЛА/сенсорами).

Зараз засоби РЕБ є одними з провідних елементів сучасних війн і ЗК і не випадково мають чи не найбільшу серед усіх сучасних видів озброєнь динаміку розвитку. Ці засоби повноцінно формують та змінюють оперативне середовище на свою користь.

Рисунок 2. Загальні функції радіоелектронного протиборства
Figure 2. General Functions of Electronic Warfare

Проведений аналіз підтверджує, що роль сенсорних систем відіграє доволі важливу роль в сучасних умовах. З твердістю можливо зазначити, що більшість сучасних систем озброєння та підтримки базується саме на них [20].

Іншим варіантом застосування є блокування радарів противника або електронних систем командування та управління. Виконання заходів "електронної омани", метою яких є прояв для розвідки противника хибних випромінюючих засобів, застосування зброї спрямованої дії для виведення з ладу обладнання або засобів противника.

Наскрізність спектру також часто класифікується як частина електронного захисту. Швидка координація потрібна для таких завдань, як деконфлікт ресурсів спектру, виділених різними технічними аспектами.

З розвитком ІТ-технологій та радіочастотних технологій виникла низка проблем із виявленням ворожих джерел випромінення. Це включає в себе здатність методів швидкої псевдовипадкової зміни частоти, метою якої є уникнення режиму передачі радіо засобів, різних технологій фокусування/керування електромагнітним променем, а також розробка важко виявлених форм радіочастотної хвилі, тривалість якої дуже коротка за часом [18].

ЕС та його взаємозв'язок з оперативними спроможностями військових є ключовим елементом у управлінні радіочастотним ресурсом під час проведення операцій. Цей комплекс організаційних, технічних та правових заходів складається з взаємопов'язаних функцій, що охоплюють: управління спектром, визначення смуг частот, координацію та різні політики, які дозволяють планувати, управляти та реалізовувати активні дії в електромагнітному середовищі на всіх етапах операцій.

Врешті-решт, управління радіочастотним ресурсом та ефективне використання спектру забезпечують координацію доступу до ЕС між цивільними, об'єднаними та багатонаціональними партнерами в межах всього операційного середовища.

Дискусії в управлінні радіочастотним спектром доволі часто зводяться до того, що він є надзвичайно проблематичним і перевантаженим. Сутність цього управління полягає у цілеспрямованому посилені електромагнітного поля з боку противника, яке порушує здатність використовувати спектр для проведення військових операцій. При цьому поєднання глобальної індустрії бездротового широкосмугового зв'язку та комерційних супутників також має суттєвий вплив на виконання зазначених заходів, які постійно намагаються перерозподілити спектр та ресурс від оборонних заходів до задоволення запитів споживачів до більшої мобільності, з'єднання та обміну даних.

Таким чином, завдання, з якими стикаються всі радіочастотні технології, які використовуються у військових операціях – від радарів до супутників, а також тактичних радіостанцій – полягають у забезпеченні ефективності, адаптивності та гнучкості у використанні ресурсів радіочастотного спектру.

Висновки з даного дослідження і перспективи подальших досліджень. Впевнено можна стверджувати, що поширення та комерціалізація інструментів для проведення КА суттєво змінили баланс сил у КП. Сучасні технології надають широкому колу суб'єктів, від держав до неурядових організацій і навіть окремих осіб – можливість використовувати ці інструменти для досягнення геополітичного впливу та економічної вигоди [2]. Це створює нові загрози та виклики, зокрема для НБ, адже КА можуть бути спрямовані не лише на окремі держави, а й на критичну інфраструктуру, економіку та соціальну сферу [13].

Україна, враховуючи сучасні виклики, все більше зосереджується на розвитку та захисті власних ІР. В рамках цієї стратегії активно реалізуються заходи з побудови національної системи КБ, створюються і реформуються відповідні державні органи та структури, які повинні забезпечити ефективну протидію КЗ. Однак ці кроки здійснюються на тлі повномасштабного вторгнення Російської Федерації на територію України, що значно ускладнює завдання та посилює тиск на національну систему безпеки [14].

Враховуючи поточну ситуацію, визначення організаційно-правового статусу Кіберсил ЗС України є ключовим етапом у процесі трансформації системи управління СОБД. Однак, існуючі проблеми в нормативно-правовому полі, зокрема невизначеність щодо виконання завдань суб'єктами забезпечення КБ у рамках заходів з КО, залишаються суттєвими бар'єрами для формалізації безпекової політики в КП. Це ускладнює координацію дій між різними структурами і не дозволяє досягти належного рівня інтеграції КО у загальну стратегію НБ.

Отже, на основі вищевикладеного можна зробити висновок, що в найближчому майбутньому рівень обороноздатності держави буде визначатися здатністю СОБД ефективно протистояти воєнній агресії в КП та КО. Це потребуватиме не тільки суттєвого вдосконалення організаційно-правового статусу Кіберсил, але й розробки нових механізмів інтеграції КО з іншими складовими НБ, такими як РЕБ та традиційні військові сили.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Onyshchenko S., Zhyvylo Y., Cherviak A., Bilko S. 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. 5 (13 (125)), 65–76. doi: https://doi.org/10.15587/1729-4061.2023.288175

2. Живило Є.О. Геостратегічні гравці сучасного кіберпростору. Загрози, виклики, наслідки : монографія. С91 Moderní aspekty vědy: XLV. Díl mezinárodní kolektivní monografie / Mezinárodní Ekonomický Institut s.r.o.. Česká republika: Mezinárodní Ekonomický Institut s.r.o., 2024. pp. 29–63. URL: http://perspectives.pp.ua/public/site/mono/mono-45.pdf

3. Koval M., Sova O., Orlov O., Shyshatskyi A., Artabaiev Y., Shknai O., Veretnov A., Koshlan 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), 34–44. https://doi.org/10.15587/1729-4061.2022.266009

4. Onyshchenko S., Zhyvylo Ye., Hlushko A., Bilko S. Cyber risk management technology to strengthen the information security of the national economy. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*. 2024, No 5. C. 136-142.

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

6. 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

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

8. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2469-VIII.URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

9. Живило Є.О., Докіль В.М. Модель методики оцінювання спроможностей військ зв'язку та кібербезпеки Збройних Сил України щодо виконання завдань з відбиття воєнної агресії в кіберпросторі. *Сучасні інформаційні технології у сфері безпеки та оборони*. К.: Національний університет оборони України імені Івана Черняховсько, 2023. №1 (46). С. 32-41.

10. 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

11. Про Кіберсили Збройних Сил України : проект Закону України від 19.12.2024 № 12349. – URL: URL:https://ips.ligazakon.net/document/ji12124a?an=2

12. Живило Є. О., Докіль В. М. Нормативно-правові шляхи вирішення існуючих колізій у сфері кібербезпеки в умовах створення кіберсил Збройних Сил України. *Теорія та практика державного управління*. 2024, *1*(78), 183-196. https://doi.org/10.26565/1727-6667-2024-1-11

13. The EY/IIF global risk management survey results surface new challenges faced by today's CRO as their strategic and tactical remit expands. URL: https://www.ey.com/en_gl/industries/banking-capital-markets/ey-iif-global-bank-risk-management-survey

14. Живило Є.О., Докіль В.М. Організаційно-функціональні трансформації кіберсил геостратегічних гравців світового кіберпростору. С91 Moderní aspekty vědy: XLIX. Díl mezinárodní kolektivní monografie / Mezinárodní Ekonomický Institut s.r.o.. Česká republika: Mezinárodní Ekonomický Institut s.r.o., 2024. pp. 218 – 263. URL: http://perspectives.pp.ua/public/site/mono/mono-49.pdf

15. Kashkevich S., Kashkevych I., Kuvshynov O., Kuzavkov V., Zhyvylo Y., Dmytriieva O., Lebedynskyi A., Pysarenko A., Zudikhin Y., & Shyshatskyi A. (2024). Development of a method for assessing the state of dynamic objects using a population algorithm. *Eastern-European Journal of Enterprise Technologies*, 4(3 (130), 29–36. DOI: https://doi.org/10.15587/1729-4061.2024.308389

16. Порядок реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі : Постанова Кабінету Міністрів України від 04.04.2023 р. № 299. URL: https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#n12

17. 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

18. Deloitte (2021) Global cyber executive briefing: high technology. Case studies, DeloitteDevelopment LLC. URL: https://www2.deloitte.com/ba/en/pages/risk/articles/High-Technology-Sector

19. Навігатори AgriTech, CyberTech, EdTech і FinTech представлені на Генеральній асамблеї ITU 2024. URL: https://itukraine.org.ua/en/home/

20. Mahdi Q. A., Zhyvotovskyi R., Kravchenko S., Borysov I., Orlov O., Panchenko I., Zhyvylo Y., Kupchyn A., 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), Pp. 34–44. https://doi.org/10.15587/1729-4061.2021.240178

Стаття надійшла до редакції 20.11.2024
Стаття рекомендована до друку 20.12.2024

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

INTEGRATION PRINCIPLES OF THE CYBERNETIC AND ELECTROMAGNETIC ENVIRONMENT

Abstract: Over the past ten years, there has been a transformation in the views on the creation of cybersecurity systems, information security, and electromagnetic activity. These elements are now used in combination to suppress or even completely block the operation of emitting complexes/devices, disable the functioning of control systems and weapons, as well as interacting systems, communication, and service platforms. This change has occurred against the backdrop of accelerating technological development, while cyber activity in the global arena has created a complex state of constant interstate competition or war. As a

result, it is essential to emphasize that achieving superiority in such an environment can only be accomplished through a clear understanding of the current situation and through continuous adaptation and improvement of the system itself.

In Ukraine, active work continues to improve the forms and methods of conducting active cyber operations, as well as the development of mechanisms for building the national cybersecurity system. In the modern digital environment, emerging cyber threats are becoming increasingly complex and diverse, which makes securing the country's information infrastructure a priority task.

One of the main directions of this work is the enhancement of existing cybersecurity technologies and strategies, as well as the creation of new methods for effective response to cyber threats. In this context, significant attention is given to building coordination mechanisms between government agencies, the private sector, and international partners, which enables the rapid detection and neutralization of cyber incidents.

An important aspect is also the development of the national cybersecurity system, which includes the creation of new regulatory acts, improvement of personnel policies, and raising the level of technical training of specialists. This not only ensures effective protection against external and internal cyber threats but also enhances the resilience of Ukraine's critical infrastructure.

Thus, improving the forms and methods of cyber operations, as well as implementing mechanisms for building the national cybersecurity system, are key elements of Ukraine's national security strategy in the face of modern challenges.

Keywords: *information and communication technologies, cybernetic and electromagnetic environment, information technologies, information security, cybersecurity, cyber influence, active cyber operations.*

In cites: Zhyvylo, Ye. O. (2024). Integration Principles of the cybernetic and electromagnetic environment. *Theory and Practice of Public Administration*, 2 (79), 99–114. http://doi.org/10.26565/1727-6667-2024-2-05 [in Ukrainian].

REFERENCES:

1. Onyshchenko, S., Zhyvylo, Y., 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, 5 (13 (125)), 65–76. doi: https://doi.org/10.15587/1729-4061.2023.288175

2. Zhyvylo, Ye.O., Heostratehichni hravtsi suchasnoho kiberprostoru. Zahrozy, vyklyky, naslidky. Monohrafiia. 2024. 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 [in Ukrainian].

3. Koval, M., Sova, O., Orlov, O., Shyshatskyi, A., Artabaiev, Y., Shknai, O., Veretnov, A., Koshlan, 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. https://doi.org/10.15587/1729-4061.2022.266009

4. Onyshchenko, S., Zhyvylo, Ye., Hlushko, A., & Bilko, S. (2024). Cyber risk management technology to strengthen the information security of the national economy. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*, No 5. C. 136-142.

5. Zhyvylo, Ye.O., Orlov, O.V. (2022). Sutnist kiberbezpeky natsionalnoho sehmentu kiberprostoru derzhavy v umovakh kryzovoho upravlinnia. *Publichne upravlinnia KhKhI stolittia v umovakh hibrydnykh zahroz* : Zbirnyk naukovykh materialiv KhKhII Mizhnarodnoho naukovoho konhresu, 27 kvitnia 2022 r. Kharkivskyi natsionalnyi universytet imeni Vasylia Nazarovycha Karazina. 248-254. [in Ukrainian].

6. Zhyvylo, Ye. O. (2024). Militaryzatsiia vyklykiv ta zahroz v kiberprostori yak operatsiinomu seredovyshchi. *Derzhavne budivnytstvo*. 1 (35), 344–359. DOI: https://doi.org/10.26565/1992-2337-2024-1-26 [in Ukrainian].

7. Zhyvylo, Yt. (2023). Exploring and Acquiring Modern Human Resource Competencies in Cybersecurity Amidst State Digital Transformation. *Pressing Problems of Public Administration*, 2(63), 111-127. https://doi.org/10.26565/1684-8489-2023-2-08

8. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 05.10.2017 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].

9. Zhyvylo, Ye. O., Dokil, V. M. (2023). Model metodyky otsiniuvannia spromozhnostei viisk zviazku ta kiberbezpeky Zbroinykh Syl Ukrainy shchodo vykonannia zavdan z vidbyttia voiennoi ahresii v kiberprostori. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*. K.: Natsionalnyi universytet oborony Ukrainy imeni Ivana Cherniakhovsko. 1 (46), 32-41 [in Ukrainian].

10. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14.05.2021 r. "Pro Stratehiiu kiberbezpeky Ukrainy": Ukaz Prezydenta Ukrainy vid 26.08.2021 r. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text [in Ukrainian].

11. Pro Kibersyly Zbroinykh Syl Ukrainy : proekt Zakonu Ukrainy vid 19.12.2024 № 12349. URL: https://ips.ligazakon.net/document/ji12124a?an=2 [in Ukrainian].

12. Zhyvylo, Y., & Dokil, V. (2024). Regulatory and Legal Ways to Resolve Existing Conflicts in the Field of Cyber Security in the Context of the Creation of Cyber Forces of the Armed Forces of Ukraine. *Theory and Practice of Public Administration*, *1* (78), 183-196. https://doi.org/10.26565/1727-6667-2024-1-11 [in Ukrainian].

13. The EY/IIF global risk management survey results surface new challenges faced by today's CRO as their strategic and tactical remit expands. URL: https://www.ey.com/en_gl/industries/banking-capital-markets/ey-iif-global-bank-risk-management-survey

14. Zhyvylo, Ye.O., & Dokil, V.M. (2024). Orhanizatsiino-funktsionalni transformatsii kibersyl heostratehichnykh hravtsiv svitovoho kiberprostoru. Monohrafiia. C91 Moderní aspekty vědy: XLIX. Díl mezinárodní kolektivní monografie / Mezinárodní Ekonomický Institut s.r.o.. Česká republika: Mezinárodní Ekonomický Institut s.r.o., 218–263. URL: http://perspectives.pp.ua/public/site/mono/mono-49.pdf [in Ukrainian].

15. Kashkevich, S., Kashkevych, I., Kuvshynov, O., Kuzavkov, V., Zhyvylo, Y., Dmytriieva, O., Lebedynskyi, A., Pysarenko, A., Zudikhin, Y., & Shyshatskyi, A. (2024). Development of a method for assessing the state of dynamic objects using a population algorithm. *Eastern-European Journal of Enterprise Technologies*, 4(3 (130), 29–36. URL: https://doi.org/10.15587/1729-4061.2024.308389

16. Poriadok reahuvannia subiektamy zabezpechennia kiberbezpeky na rizni vydy podii u kiberprostori: Postanova Kabinetu Ministriv Ukrainy vid 04.04.2023 r. № 299. https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#n12 [in Ukrainian].

17. Zhyvylo, Ye. O., & Zhyvylo, I. (2021). 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

18. Deloitte (2021) Global cyber executive briefing: high technology. Case studies, Deloitte Development LLC. URL: https://www2.deloitte.com/ba/en/pages/risk/articles/High-Technology-Sector

19. Navihatory AgriTech, CyberTech, EdTech i FinTech predstavleni na Heneralnii asamblei ITU 2024. URL: https://itukraine.org.ua/en/home/ [in Ukrainian].

20. 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. https://doi.org/10.15587/1729-4061.2021.240178

The article was received by the editors 20.11.2024
The article is recommended for printing 20.12.2024