DOI:**10.33099/2311-7249/2021-42-3-37-44**

УДК 621.396

Євген Олександрович Живило *(кандидат наук з державного управління)* [1]
Дмитро Георгійович Шевченко *(кандидат військових наук)* [1]
Олександр Олександрович Черноног [2]

[1] ***Національний університет оборони України імені Івана Черняховського, Київ, Україна***
[2] ***Міністерство оборони України, Київ, Україна***

ТИПОЛОГІЯ СИСТЕМ КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ВІЙСЬКОВОГО (СПЕЦІАЛЬНОГО) ПРИЗНАЧЕННЯ

В статті розглянуте актуальне питання щодо підходів визначення типології систем кібербезпеки в інформаційно-телекомунікаційних системах військового (спеціального) призначення. Проаналізовані останні дослідження і публікації з цього питання. Проведений аналіз та досвід провідних країн світу, свідчить про те, що в умовах сучасних бойових дій ефективне функціонування системи кібербезпеки в інформаційно-телекомунікаційних системах військового (спеціального) призначення буде в умовах постійного впливу противника. За цих умов трансформація поглядів на питання створення систем кібербезпеки і кібероборони та, відповідно, розвиток їх структур та типологій в провідних країнах світу відбувається під впливом розвитку технологій, змін у безпековому середовищі, формах, способах та технологіях ведення війн і нових досягнень в цьому. В статті запропоновано підхід типологізації систем кібербезпеки в інформаційно-телекомунікаційних системах військового (спеціального) призначення.

В статті визначені об'єкти кібервпливу: технічні системи, соціум протиборчої сторони, соціотехнічні системи і когнітивний простір. Розглянуті сфери і галузі що підлягають кіберзахисту та кібероборонні та надана їх коротка характеристика. Запропонована типологія систем кібербезпеки в інформаційно-телекомунікаційних системах військового (спеціального) призначення за її функціональним призначенням і складовим. Проаналізована система кібербезпеки в ІТС військового (спеціального) призначення провідних країн світу та країн-членів НАТО розкриті її функціональні підсистеми.

В статті розглянуто методичний підхід для вирішення прикладної задачі, яка полягає у визначенні підходів для створення типології зазначених систем.

Запропонована типологія систем кібербезпеки в інформаційно-телекомунікаційних системах військового (спеціального) призначення враховує об'єкти кібервпливу, які обумовлені особливостями кібердій у кіберпросторі в сучасних умовах. Це дає можливість втілити типологію системи кібербезпеки в інформаційно-телекомунікаційних системах військового (спеціального) в цілому, окремих елементів та її складових. Запропоновано найбільш раціональний варіант створення типології систем кібербезпеки, якій відповідно до сучасних тенденцій розвитку, з урахуванням військово-політичної обстановки, національних інтересів та законодавства, забезпечить інформаційну, кібернетичну та когнітивну перевагу над противником та буде сприяти практичній реалізації прийнятої в країнах членах НАТО концепції "смарт-оборони".

Ключові слова: *зв'язок, інформаційно-телекомунікаційна мережа, кібербезпека.*

Вступ

Постановка проблеми. За наявними оцінками та аналізом публікацій і статей з відкритих джерел спроможності суб'єктів сектору безпеки та оборони стосовно забезпечення кібербезпеки провідними країнами-членами НАТО, по визначенню формалізованої типології відповідних систем в інформаційно-телекомунікаційних системах (далі – ІТС) військового (спеціального) призначення тримаються в таємниці.

При цьому відомо, що зазначені системи використовуються для перевірки безпеки власних ІТС і їх побудова спрямована на створення реалістичного середовища для навчань оборонних підрозділів. Слід зауважити, що найбільш сучасною і одночасно перспективною формою реалізації політики блоку НАТО за напрямом забезпечення кібербезпеки у воєнній сфері вважається створення та забезпечення ефективного функціонування системи кібероборони, як організованої сукупності суб'єктів та об'єктів кібероборони з визначеними зв'язками між ними та об'єднаних єдиним керівництвом.

За цих умов трансформація поглядів на питання створення систем кібербезпеки і кібероборони та, відповідно, розвиток їх структур

та типологій в провідних країнах світу відбувається під впливом розвитку технологій, змін у безпековому середовищі, формах, способах та технологіях ведення війн і нових досягнень в цьому.

Аналіз останніх досліджень і публікацій. На теперішній час в світі існує біля 40 ключових макротехнологій, які за думкою провідних експертів визначають рівень економіки та обороноздатності країн в сучасних умовах.

До високих технологій та технологій подвійного призначення (high technology, hi-tech – англ.) частіше за все відносять такі технології: штучний інтелект, космічні, робототехнічні, інформаційні та кібер-технології; нано-, квантові, нейронні, біотехнології, генну інженерію, інноваційну електромеханіку, електроніку, матеріалознавство, створення нових напівпровідникових матеріалів, генерування, акумулювання та передача енергії, "чисті" (cleantech) та енергозберігаючі технології, телекомунікаційні, інфокомунікаційні технології та технології управління і автоматизації.

В цих сферах прогнозуються проривні досягнення перш за все у штучному інтелекті, хмарних технологіях, інтернеті речей, продуктивності та природі обчислювальних засобів, можливостях зберігання обробки та передачі великих масивів даних та інформації (Big Data), засобах і технологіях їх реалізації на кардинально нових принципах. Можливості і вразливості практично всіх сучасних інфокомунікаційних та кібернетичних систем все більше залежать, крім того, від зростання взаємозв'язків різноманітних інформаційних систем та систем управління між собою в багатопараметричному та багатовимірному кіберпросторі та їх інформаційно-кібернетичного взаємопроникнення, взаємодії і взаємозалежності тощо.

Таким чином, **метою статті є** аналіз типологій систем кібербезпеки в інформаційно-телекомунікаційних системах військового (спеціального) призначення.

Виклад основного матеріалу дослідження

Державами членами Європейського Союзу схвалено рішення щодо розширення оборонного співробітництва в Європі в рамках програми щодо Постійного структурного співробітництва з питань безпеки і оборони PESCO, в якій беруть участь 25 країн: Австрія, Бельгія, Болгарія, Чехія, Хорватія, Кіпр, Естонія, Фінляндія, Франція, Німеччина, Греція, Угорщина, Італія, Ірландія, Латвія, Литва, Люксембург, Нідерланди, Польща, Португалія, Румунія , Словенія, Словаччина, Іспанія і Швеція.

Стосовно визначення уніфікації побудови систем кібербезпеки було прийнято два проекти: платформа обміну інформацією по кіберзагрозам і реагування на інциденти, а також команди швидкого реагування на кіберзагрози (Security Operation Center, SOC) і взаємодопомоги в області кібербезпеки.

Ці проєкти визначили два стратегічних напрямки розвитку системи колективної кібербезпеки Європи. Перший – заходи кіберзахисту стратегічного рівня, а саме створення загальної мережної платформи для обміну інформацією про кіберзагрози між державами. Другий – це створення єдиної розгалуженої системи центрів реагування та протидії загрозам в кіберпросторі – системи колективного реагування на кіберінциденти, яка буде в змозі проводити різноманітні операції в рамках зміцнення загальної політики безпеки і оборони в кіберпросторі [6].

Приєднання до цих проєктів та інтеграція в систему колективної кібербезпеки Європи означає необхідність створення відповідної системи кібербезпеки в державі з урахуванням вимог Європейської комісії стосовно кібезахисту об'єктів критичної інфраструктури та доведення її можливостей виконувати всі завдання з кіберзахисту на відповідному рівні. В зв'язку з чим виникає питання щодо потенційних можливостей країни стосовно досягнення та підтримки необхідного рівня забезпечення та спроможностей в сфері кіберзахисту [2]. При цьому в ході проведення даного аналізу зазначається, що є необхідним проводити оцінку потенційних можливостей країн в сфері кіберзахисту.

Аналіз теорії, практики і досвіду побудови систем кібербезпеки та кібероборони (військового, спеціального призначення) США та країнами блоку НАТО свідчить, що основною тенденцією при їх формуванні стало поєднання в єдиній структурі, яка відповідає за кібероборону, відповідно до мети, завдань, доцільних форм та способів забезпечення кібербезпеки у воєнній сфері, різних напрямів діяльності (та відповідно, підрозділів, які її здійснюють) поєднаних їх відношенням до кіберпростору [8]. Визначним чином на ці процеси вплинуло безпосередньо особливості формування та постійний розвиток і трансформація кіберпростору.

Зважаючи на зазначене вище та враховуючи офіційні вислови представниками Групи урядових експертів ООН з питань інформаційної безпеки (UNGGE) та експертами в галузі кібербезпеки провідних міжнародних компаній одностайно визнається, що завдання кібербезпеки та кібероборони в цілому можуть розглядатися в межах трьох основних підсистем: кіберрозвідки, кіберзахисту, дій (операцій) у кіберпросторі.

Отже, питання щодо побудови та забезпечення мілітаризованих систем кібербезпеки країн-партнерів умовно розглядаються за:

напрямками – захист громадянина і суспільства, захист держави;

об'єктами кібервпливу – соціальні, технічні, соціотехнічні системи наведені на рис. 1 [9];

рівнями – державний (стратегічний), регіональний (оперативний), місцевий

(тактичний);

завданнями – запобігання, стримування, протидії;

сферами та галузями – економіка (виробничий та невиробничий сектори, критична інфраструктура держави), сфери зовнішньої та внутрішньої політики, державного управління, освіти, науки, безпеки і оборони (рис. 2);

кіберзахист (боротьба з кіберзлочинністю, кібершпигунством, кібертероризмом);

кібероборона (дії в IT-мережах та програмно-комп'ютерні дії, дії в електромагнітному спектрі випромінювання, дії в соціокіберпросторі, кіберпросторі та через кіберпростір: інформаційні, психологічні, когнітивні) (рис. 3);

формами і способами кіберзахисту та активних кібердій;

суб'єктами, що здійснюють кіберзахист та кібероборону.

Рис. 1. Об'єкти кібервпливу

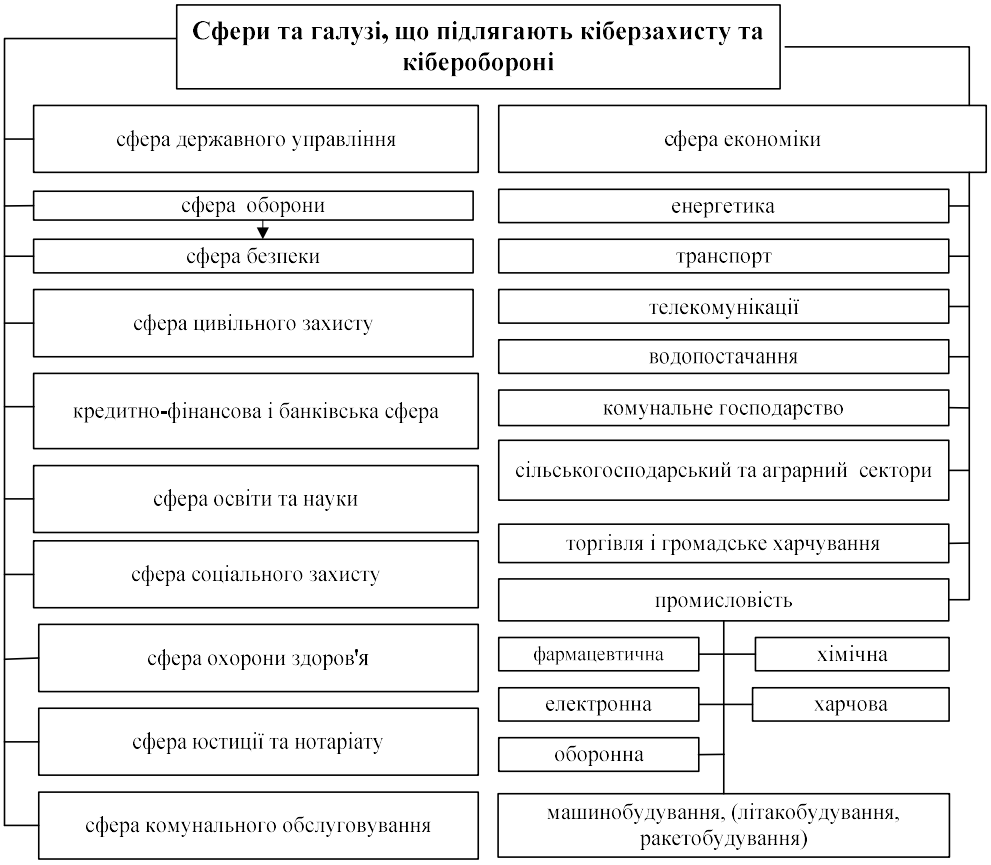

Рис. 2. Сфери та галузі, що підлягають кіберзахисту та кібероборонні

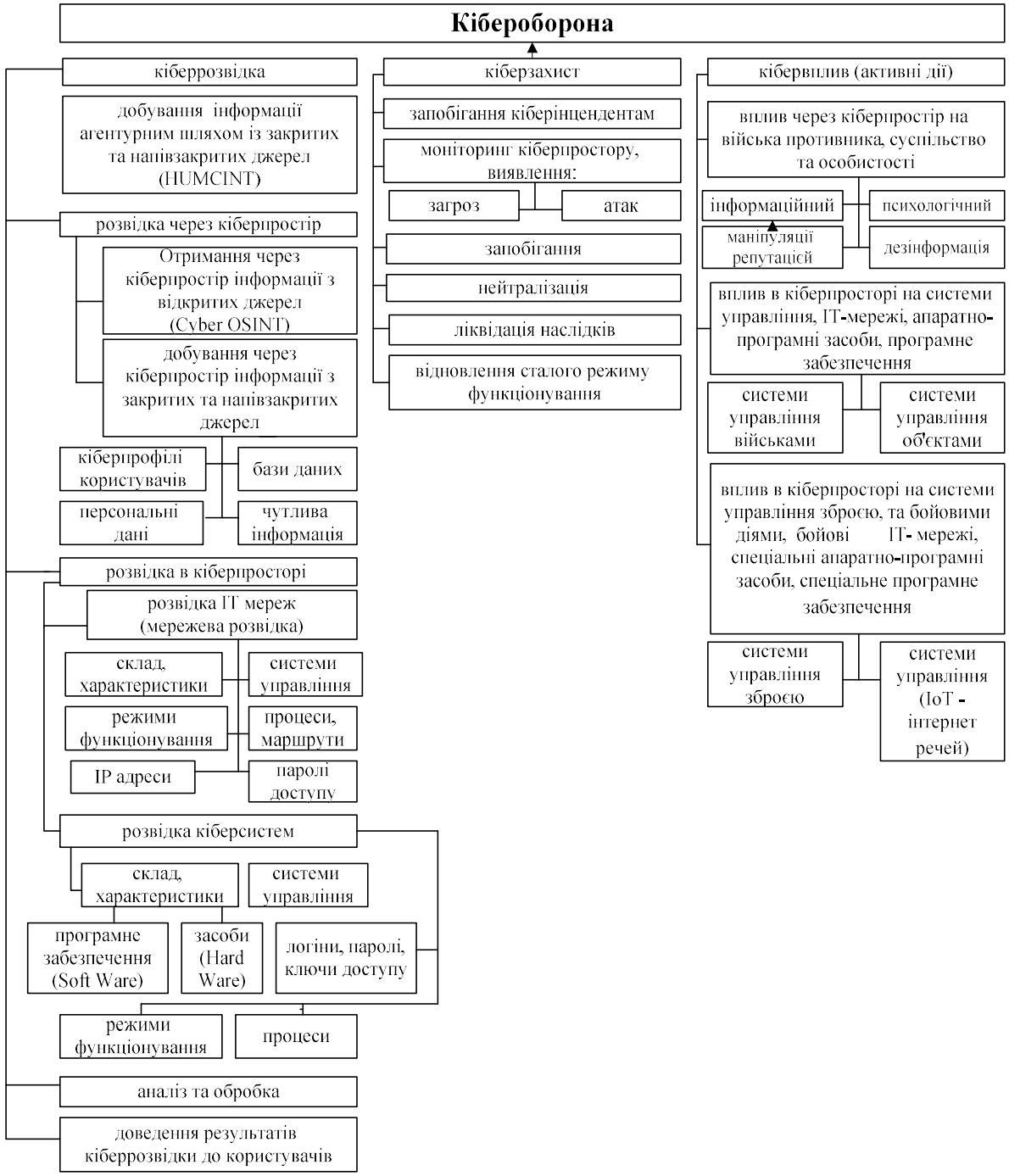

Рис. 3. Складові кібероборони

Разом з тим, формування систем кібербезпеки та кібероборони провідних країн світу відбуваються спираючись на загальні принципи, позитивні риси яких можуть та повинні бути використані при побудові системи кібербезпеки в ІТС військового (спеціального) призначення України, основні з них, а саме:

інтегрованість системи кібероборони в багаторівневу систему кібербезпеки держави (коаліції);

безперервність функціонування системи кібероборони;

відповідність рівня всебічного забезпечення кіберсил потребам оборони;

оптимальність (раціональність) побудови сил кібероборони;

відповідність рівня всебічного забезпечення кіберсил потребам оборони;

оптимальність (раціональність) побудови сил кібероборони;

керованість з єдиного координуючого органу з питань забезпечення кібербезпеки;

науково обґрунтовані законодавче, нормативно-правове, дефініційно-термінологічне супроводження;

державно-приватне та міжнародне партнерство;

узгодженість та взаємодія різних відомств у сфері забезпечення кібероборони держави;

інтегрованість закладів освіти до

високотехнологічних навчально-наукових, дослідно-випробувальних комплексів, уніфікованість вимог щодо підготовки військового й цивільного персоналу кібербезпеки;

однозначність критеріїв (індикаторів) загроз у сфері кібероборони держави, рівня готовності систем КБ та КО, тощо.

За функціональним призначенням типологія таких систем в її класичному виді розглядається за такими складовими [3]:

запобігання (англійською – "Prevention") – заходи щодо завчасного виявлення, уникнення, стримування, запобігання можливих (потенційних) кіберзагроз чи кібератак, припинення підготовки до них;

захист (англійською – "Protection") – заходи щодо забезпечення випереджувального захисту від можливих кібератак (кібервпливу) противника, в першу чергу в інтересах всебічного та стійкого забезпечення у кіберпросторі процесів управління власними військами та зброєю;

попередження (англійською – "Mitigation") – заходи щодо безпосереднього виявлення, відвернення загрози, зменшення можливих втрат (збитків, пошкоджень) у разі безпосередньої загрози проведення кібератак. При певних умовах в межах зазначеного можуть проводитися випереджувальні (зустрічні) заходи активного кіберзахисту;

реагування (англійською – "Response") – заходи комплексного реагування та впливу на противника, у т.ч. шляхом активного кіберзахисту в умовах безпосереднього проведення ним кібератак з одночасним проведенням заходів захисту власної інфраструктури, особового складу, ресурсів тощо від впливу противника;

відновлення (англійською – "Recovery") – заходи, направлені на відновлення інформаційної та іншої інфраструктури, яка стала об'єктом кібератак противника, стабілізацію ситуації та ліквідації інших негативних наслідків.

Деталізуючи зазначену вище класичну систему кібербезпеки в ІТС військового (спеціального) призначення провідних країн світу та країн-членів НАТО є необхідним розкрити її наступні функціональні підсистеми.

Основні:

1. Моніторинг кіберпростору та розвідувальна діяльність, у т.ч.:

розвідувальна діяльність щодо виявлення загроз національній безпеці в кіберпросторі, інших подій і обставин що стосуються сфери кібербезпеки [7].

моніторинг соціальних мереж щодо виявлення негативного інформаційно-психологічного впливу на особовий склад через кіберпростір [5].

моніторинг безпеки інформації щодо виявлення та попередження порушень в експлуатації телекомунікаційних систем та спроб несанкціонованого витоку інформації з обмеженим доступом.

моніторинг роботи радіоелектронних систем, в тому числі ведення радіоелектронної розвідки.

2. Кіберзахист, у т.ч.:

моніторинг кіберзагроз та кіберінцидентів ІТС військового (спеціального) призначення.

моніторинг кіберзагроз на об'єктах критичної інфраструктури ІТС військового (спеціального) призначення.

кіберзахист ІТС військового (спеціального) призначення.

криптографічний, криптоаналітичний та технічний захист інформації, спрямований на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідація їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних та інформаційно-телекомунікаційних систем [1].

захист інформації з обмеженим доступом, до якої може бути отримано доступ через кіберпростір.

кіберзахист в системах супутникової навігації та топогеодезичного забезпечення, які використовують космічні інформаційні технології.

участь у кіберзахисті об'єктів критичної інфраструктури держави, інших визначених об'єктів (ресурсів).

3. Участь у заходах діяльності інших суб'єктів забезпечення кібербезпеки держави (відповідно до компетенції суб'єктів сектору безпеки та оборони), у т.ч. [4, 10]:

щодо боротьби з кібертероризмом;

щодо боротьби з кіберзлочинністю;

під час участі в операціях (бойових діях) у складі коаліційних сил (щодо встановлення спеціального режиму роботи телекомунікаційних засобів).

4. Активної кібероборони (активних заходів впливу в кіберпросторі), у т.ч.:

кіберрозвідки ІТС противника;

кібердії, кібероперації та інші активні заходи впливу в кіберпросторі;

правові, організаційні та технічні заходи впливу на роботу телекомунікаційних засобів національного сегменту кіберпростору (Інтернет-провайдерів тощо);

фізичний вплив на кіберінфраструктуру противника (у т. ч. ведення радіоелектронної боротьби, вогневого ураження, проведення спеціальних операцій тощо);

боротьба у кіберпросторі із негативним інформаційно-психологічним впливом на особовий склад.

5. Керівництво (у т.ч. оперативне управління) діяльністю в кіберпросторі, у т.ч.:

участь у формуванні та реалізації державної політики щодо кібербезпеки та кібероборони;

формування та координація реалізації політики суб'єктами сектору безпеки та оборони щодо кібероборони та дій (операцій) у кіберпросторі;

оперативне управління реагуванням на кіберінциденти та кіберзагрози (у т.ч. в форматі відомчого CSOC);

підтримання взаємодії з системою інших

відомчих CERT.

Допоміжні підсистеми, у т.ч.:

6. Підсистема кадрового забезпечення.

7. Підсистема наукового забезпечення.

8. Підсистема підготовки особового складу та підрозділів.

9. Підсистема міжнародного співробітництва щодо кібербезпеки.

10. Підсистема матеріально-технічного забезпечення.

При цьому функціонування системи дій в кіберпросторі здійснюється у відповідності до нормативно-правових актів (національних кіберстратегій, програм, планів, стандартів і т.ін.) та формату узгодженої діяльності визначених організаційно-штатних структур суб'єктів сектору безпеки та оборони до повноважень яких віднесені питання кібербезпеки (кібероборони).

Перевагами побудови таких типологій систем кібербезпеки в ІТС військового (спеціального) призначення є гнучкість структури, визначення та залучення відповідних сил і засобів під конкретні задачі.

В свою чергу недоліком такої системи є організація підпорядкованості відповідних сил призначених для дій в кіберпросторі не тільки міністерству оборони (агенцій, центрів і т.ін.) але і розвідувальним структурам, що може призвести до розпорошення сил.

Висновки й перспективи подальших досліджень

Таким чином, аналізуючи типологію систем кібербезпеки ІТС військового (спеціального) призначення розвинутих країн світу вбачається, що побудова даних систем безпосередньо залежить від їх потенційних можливостей, фінансування та чисельності ІТ-фахівців і спеціалістів в галузі кібербезпеки. Найбільш розгалуженою та гнучкою системою на сьогодні є топологія Сполучених Штатів Америки. Однак, якщо взяти до уваги створення Європейської колективної системи кібербезпеки, до якої входить 25 країн, то ця система за чисельністю ІТ-фахівців, їх рівнем освіченості і підготовки та фінансуванням буде найпотужнішою з усіх сьогодні відомих.

Результати проведеного аналізу дозволяють стверджувати, що створення колективних систем протидії кіберзагрозам є перспективним напрямком подальших досліджень з метою створення потужних систем кібервпливу.

При цьому, якщо провести паралель з існуючими підходами створення системи колективної безпеки у військовій сфері, створення колективних систем протидії кіберзагрозам віддалено нагадує створення колективних систем безпеки країн, за розміщення яких поблизу кордонів іншої держави постійно йде боротьба.

Література

1. Закон України (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403) // Про основні засади забезпечення кібербезпеки України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

2. Чевардін В. Є. Аналіз структур кіберкомандувань озвинутих країн / В. Є. Чевардін, О. Є. Мазулевський // Збірник наукових праць ВІТІ № 2. – 2020. – URL: http://www.viti.edu.ua/files/zbk/2020/12_2_2020.pdf.

3. Віктор Петров. Підходи до концептуальних засад проєкту Стратегії кібербезпеки України на 2021–2025 роки// Незалежний аналітичний центр геополітичних досліджень. 11.02.2021. URL: https://bintel.org.ua/analytics/voenni-voprosy/armii-voorugenie/konceptualni-zasadu-proyektu-strategii-kiberbezpeki-ukraini-na-2021-2025-roki/

4. Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України". URL: https://www.rnbo.gov.ua/ua/Ukazy/417.html?PRINT

5. Інформаційний вимір гібридної війни: досвід України: матеріали міжнародної науково-практичної конференції. – Київ: НУОУ, 2017. – 104 с. URL: https://nuou.org.ua/assets/documents/zbirn-gibr-mizhn-konf.pdf **6. А. Деркаченко**. Сектор безпеки і оборони. Напрями розвитку зовнішньої розвідки України // Незалежний аналітичний центр геополітичних досліджень. 02.02.2020. URL: https://bintel.org.ua/nukma/sektor-bezpeki-i-oboroni/

7. Указ Президента України Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України". URL: https://www.rnbo.gov.ua/ua/Ukazy/4974.html

8. Всеохоплююча оборона України: стан, проблеми та заходи щодо зміцнення кібероборони держави і створення кібервійськ. Оборонно-промисловий кур'єр. 15:19 01.11.2021. URL: http://opk.com.ua/%d0%b2%d1%81%d0%b5%d0%be%d1%85%d0%be%d0%bf%d0%bb%d1%8e%d1%8e%d1%87%d0%b0-%d0%be%d0%b1%d0%be%d1%80%d0%be%d0%bd%d0%b0-%d1%83%d0%ba%d1%80%d0%b0%d1%97%d0%bd%d0%b8-%d1%81%d1%82%d0%b0%d0%bd-%d0%bf%d1%80/

9. Вдовенко С.Г., Даник Ю.Г. Проблеми та перспективи забезпечення кібероборони держави. Збірник наукових праць військового інституту Київського Національного університету імені Тараса Шевченка, випуск 66, 2020 - С. 75-89. DOI: https://doi.org/10.17721/2519-481X/2020/66-08 **10. Mahdi, Q**. A., Животовський, Р. М., Кравченко, С. І., Борисов, І. В., Орлов, О. В., Панченко, І. В., Живило, Є. О., Купчин, А. В., Колтовсков, Д. Г., & Боголій, С. М. (2021). Розробка методики структурно-параметричної оцінки стану об'єкту. *Eastern-European Journal of Enterprise Technologies*, *5*(4 (113), 34–44. https://doi.org/10.15587/1729-4061.2021.240178

ТИПОЛОГИЯ СИСТЕМ КИБЕРБЕЗОПАСНОСТИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ ВОЕННОГО (СПЕЦИАЛЬНОГО) НАЗНАЧЕНИЯ

***Евгений Александрович Живило** (кандидат наук по государственному управлению)* [1]

***Дмитрий Георгиевич Шевченко** (кандидат военных наук)* [1]

Александр Александрович Черноног [2]

[1] Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина
[2] Министерство обороны Украины, Киев, Украина

В статье рассмотрен актуальный вопрос о подходах определения типологии систем кибербезопасности в информационно-телекоммуникационных системах военного (специального) назначения. Проанализированы последние исследования и публикации по этому вопросу. Проведенный анализ и опыт ведущих стран мира показывает, что в условиях современных боевых действий эффективное функционирование системы кибербезопасности в информационно-телекоммуникационных системах военного (специального) назначения будет в условиях постоянного влияния противника.

В этих условиях трансформация взглядов на вопросы создания систем кибербезопасности и кибероборонь и, соответственно, развитие их структур и типологий в ведущих странах мира происходит под влиянием развития технологий, изменений в среде безопасности, формах, способах и технологиях ведения войн и новых достижений в этом. В статье предложен подход типологизации систем кибербезопасности в информационно-телекоммуникационных системах военного (специального) назначения.

В статье определены объекты кибервоздействия: технические системы, социум противоборствующей стороны, социотехнические системы и когнитивное пространство. Рассмотрены сферы и отрасли, подлежащие киберзащите и кибероборонe, и дана их краткая характеристика. Предложена типология систем кибербезопасности в информационно-телекоммуникационных системах военного (специального) назначения по ее функциональному и составляющему назначению. Проанализированная система кибербезопасности в ИТС военного (специального) назначения ведущих стран мира и стран-членов НАТО раскрыта ее функциональные подсистемы.

В статье рассмотрен методический подход для решения прикладной задачи, заключающейся в определении подходов для создания типологий указанных систем.

Предложенная типология систем кибербезопасности в информационно-телекоммуникационных системах военного (специального) назначения учитывает объекты кибервлияния, обусловленные особенностями кибердий в киберпространстве в современных условиях. Это позволяет воплотить типологию системы кибербезопасности в информационно-телекоммуникационных системах военного (специального) в целом, отдельных элементов и ее составляющих.

Предложен наиболее рациональный вариант создания типологии систем кибербезопасности, которой в соответствии с современными тенденциями развития, с учетом военно-политической обстановки, национальных интересов и законодательства, обеспечит информационное, кибернетическое и когнитивное преимущество над противником и будет способствовать практической реализации принятой в странах членов НАТО концепции смарт-обороны.

Ключевые слова: *связь, информационно-телекоммуникационная сеть, кибербезопасность.*

TYPOLOGY OF CYBER SECURITY SYSTEMS IN INFORMATION AND TELECOMMUNICATION SYSTEMS OF MILITARY (SPECIAL) PURPOSE

Yevgen Zhyvylo (Candidate of Science in Public Administration) [1]
Dmytro Shevchenko (Candidate of military sciences) [1]
Olexandr Chernonog [2]

[1] National Defense University of Ukraine named by Ivan Cherniakhovskyi, Kyiv, Ukraine
[2] Ministry of Defense of Ukraine

The article considers the topical issue of approaches to determining the typology of cybersecurity systems in information and telecommunication systems for military (special) purposes. Recent research and publications on this issue are analyzed. The analysis and experience of the leading countries of the world show that in the conditions of modern military operations the effective functioning of the cybersecurity system in information and telecommunication systems of military (special) purpose will be in the conditions of constant enemy influence.

Under these conditions, the transformation of views on the creation of cybersecurity and cyber defense systems and, accordingly, the development of their structures and typologies in leading countries is influenced by technology, changes in the security environment, forms, methods and technologies of warfare and new advances. The article proposes an approach to the typology of cybersecurity systems in information and telecommunication systems for military (special) purposes.

The article identifies the objects of cyber influence: technical systems, the society of the opposing party, socio-technical systems and cognitive space. Areas and areas subject to cyber defense and cyber defense are considered and a brief description is given. The typology of cybersecurity systems in information and telecommunication systems of military (special) purpose on its functional purpose and component is offered. The

functional subsystems of the leading countries of the world and NATO member states have been analyzed in the ITS military (special) cyber security system.

The methodical approach for the decision of an applied problem which consists in definition of approaches for creation of typologies of the specified systems is considered in article.

The proposed typology of cybersecurity systems in military information and telecommunication systems takes into account the objects of cyber influence, which are due to the peculiarities of cyberdia in cyberspace in modern conditions. This makes it possible to implement the typology of the cybersecurity system in the information and telecommunication systems of the military (special) as a whole, individual elements and its components.

The most rational variant of creating a typology of cybersecurity systems is proposed, which in accordance with current development trends, taking into account the military-political situation, national interests and legislation, will provide informational, cyber and cognitive advantage over the enemy and will promote the practical implementation of the concept of smart-defense.

Key words: *connection, information and telecommunication network, cyber security.*

References

1. Zakon Ukrainy (Vidomosti Verkhovnoi Rady (VVR), 2017, № 45, st.403) // Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text. **2. Chevardin V. Ye.** Analiz struktur kiberkomanduvan ozvynutykh krain / V. Ye. Chevardin, O. Ye. Mazulevskyi // Zbirnyk naukovykh prats VITI № 2. – 2020. – URL: http://www.viti.edu.ua/files/zbk/2020/12_2_2020.pdf. **3. Viktor Petrov.** Pidkhody do kontseptualnykh zasad proiektu Stratehii kiberbezpeky Ukrainy na 2021–2025 roky// Nezalezhnyi analitychnyi tsentr heopolitychnykh doslidzhen. 11.02.2021. URL: https://bintel.org.ua/analytics/voenni-voprosy/armii-voorugenie/konceptualni-zasadu-proyektu-strategii-kiberbezpeki-ukraini-na-2021-2025-roki/ **4.** Ukaz Prezydenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku "Pro Stratehiiu kiberbezpeky Ukrainy". URL: https://www.rnbo.gov.ua/ua/Ukazy/417.html?PRINT **5.** Informatsiinyi vymir hibrydnoi viiny: dosvid Ukrainy: materialy mizhnarodnoi naukovo-praktychnoi konferentsii. – Kyiv: NUOU, 2017. – 104 s. URL: https://nuou.org.ua/assets/documents/zbirn-gibr-mizhn-konf.pdf **6. A. Derkachenko**. Sektor bezpeky i oborony. Napriamy rozvytku zovnishnoi rozvidky Ukrainy // Nezalezhnyi analitychnyi tsentr heopolitychnykh doslidzhen. 02.02.2020. URL: https://bintel.org.ua/nukma/sektor-bezpeki-i-oboroni/ **7.** Ukaz Prezydenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku "Pro Stratehiiu kiberbezpeky Ukrainy". URL: https://www.rnbo.gov.ua/ua/Ukazy/4974.html **8.** Vseokhopliuiucha oborona Ukrainy: stan, problemy ta zakhody shchodo zmitsnennia kiberoborony derzhavy i stvorennia kiberviisk. Oboronno-promyslovyi kurier. 15:19 01.11.2021. URL: http://opk.com.ua/%d0%b2%d1%81%d0%b5%d0%be%d1%85%d0%be%d0%bf%d0%bb%d1%8e%d1%8e%d1%87%d0%b0-%d0%be%d0%b1%d0%be%d1%80%d0%be%d0%bd%d0%b0-%d1%83%d0%ba%d1%80%d0%b0%d1%97%d0%bd%d0%b8-%d1%81%d1%82%d0%b0%d0%bd-%d0%bf%d1%80/ **9. Vdovenko S.H.,** Danyk Yu.H. Problemy ta perspektyvy zabezpechennia kiberoborony derzhavy. Zbirnyk naukovykh prats viiskovoho instytutu Kyivskoho Natsionalnoho universytetu imeni Tarasa Shevchenka, vypusk 66, 2020 - S. 75-89. DOI: https://doi.org/10.17721/2519-481X/2020/66-08 **10. Mahdi, Q. A**., Zhyvotovskyi, R. M., Kravchenko, S. I., Borysov, I. V., Orlov, O. V., Panchenko, I. V., Zhyvylo, Ye. O., Kupchyn, A. V., Koltovskov, D. H., & Boholii, S. M. (2021). Rozrobka metodyky strukturno-parametrychnoi otsinky stanu obiektu. Eastern-European Journal of Enterprise Technologies, 5(4 (113), 34–44. https://doi.org/10.15587/1729-4061.2021.240178