КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (19), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.19.109121
УДК 177 +17.03 + 378

Пономарьов Олександр Анатолійович
начальник факультету бойового застосування систем управління та зв'язку
Військовий інститут телекомунікацій і інформатизації імені Героїв Крут, Київ, Україна
ORCID ID: 0009-0008-2320-1549
aleksan_bimer3@ukr.net

Пивоварчук Сергій Андрійович
начальник кафедри бойового застосування підрозділів зв'язку
Військовий інститут телекомунікацій і інформатизації імені Героїв Крут, Київ, Україна
ORCID ID 0000-0001-9410-5951
sergij.pyvovarchuk@viti.edu.ua

Козубцова Леся Михайлівна
кандидат технічних наук,
завідувач кафедри математики та фізики
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID 0000-0002-7866-8575
lesia.kozubtsova@viti.edu.ua

Козубцов Ігор Миколайович
доктор педагогічних наук, кандидат технічних наук, старший науковий співробітник,
професор кафедри бойового застосування підрозділів зв'язку
Військовий інститут телекомунікацій і інформатизації імені Героїв Крут, Київ, Україна
ORCID ID 0000-0002-7309-4365
kozubtsov@gmail.com

Бондаренко Тетяна Василівна
старший науковий співробітник науково-дослідного відділу кібернетичної безпеки в інформаційно-телекомунікаційних системах
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID ID 0000-0002-2879-2041
tanjusha170393@gmail.com

Терещенко Тетяна Павлівна
старший науковий співробітник науково-дослідного відділу кібернетичної безпеки в інформаційно-телекомунікаційних системах
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID ID 0000-0002-9659-7897
tany-83@ukr.net

ГІБРИДНА ПОБУДОВА СИСТЕМИ КІБЕРБЕЗПЕКИ: АДМІНІСТРАТИВНО-ПРАВОВІ ЗАСАДИ ВІЙСЬКОВО-ЦИВІЛЬНОГО СПІВРОБІТНИЦТВА

Анотація. Національна безпека держави є одним з основних факторів стабільного розвитку суспільства. Проте Україна та Збройні сили України змушені протидіяти гібридній війні із застосуванням кіберпростору. Встановлено, що на даний час відсутнє єдине бачення щодо методології протидії війнам за гібридною формою. Відсутність методології протидії вимагає перегляду існуючих підходів до гарантування та підтримки державної безпеки. Мета статті. Обґрунтування необхідності створення гібридної системи кібербезпеки для нейтралізації кіберзагроз Збройним Силам України та способи її реалізації на засадах військово-цивільного співробітництва. Матеріали й методи. Для вирішення поставлених завдань використовувалася сукупність методів теоретичного дослідження: історичного аналізу та узагальнення наукової літератури щодо проблеми дослідження; структурно-генетичного аналізу та синтезу при уточненні об'єкта та предмета дослідження; метод сходження від

© О.А. Пономарьов, С.А. Пивоварчук, Л.М. Козубцова, І.М. Козубцова, Т.В. Бондаренко, Т.П. Терещенко, 2023

абстрактного до конкретного; метод аналітично-порівняльного аналізу при аналітично-порівняльному оцінюванні новизни результатів дослідження; синтез та узагальнення – для обґрунтування методологічних та методичних засад дослідження; узагальнення – формулювання висновків та рекомендацій щодо продовження подальших досліджень. Результат. Сформовано ключову гіпотезу, що ефективним інструментом у протидії з веденням війною за гібридною формою можна досягнути за рахунок застосування гібридних військ. Розвиваючи цю гіпотезу обґрунтовано філософську ідею необхідності у створенні гібридної системи кібербезпеки на основі військово-цивільного співробітництва. Зарубіжний досвід підтверджує високу ефективність військово-цивільного співробітництва. На підставі діючих нормативно-правових актів запропоновано спосіб реалізації. Практичне значення дослідження полягає у можливості отримання переваг у кіберпросторі ЗС України в час активних гібридних війн за рахунок формування підрозділів військово-цивільного співробітництва як нової (гібридної) форми підрозділу Збройних Сил України.

Ключові слова: гібридний, військово-цивільне співробітництво, кібербезпека, нейтралізація, кіберзагрози, Збройні Сили України.

ВСТУП

Національна безпека держави є одним з основних факторів стабільного розвитку суспільства. Проте Україна та Збройні Сили України зіткнулися з веденням гібридної війни проти себе із застосуванням кіберпростору, а це вимагає перегляду існуючих підходів до гарантування та підтримки державної безпеки. Аналіз публікацій ЗМІ за напрямком дослідження засвідчує думку, що “клин клином вибивають”, тобто для протидії викликам гібридної війни необхідно створювати гібридні війська.

Постановка завдання. Згідно положень Стратегії національної безпеки України, Воєнної доктрини України та Концепції розвитку сектору безпеки і оборони України визначено оперативну ціль “1.5. Удосконалення системи кібербезпеки та захисту інформації” [1, с. 33], Закону України “Про основні засади забезпечення кібербезпеки України” [2]; Стратегії кібербезпеки України [3]; Рішення Ради національної безпеки і оборони України від 10.07.17 “Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року” “Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації” [4] визначено кібербезпеку як пріоритетний напрямком. Без сумніву, що для реалізації вимог зазначених в документах [1-4] необхідно першочергово визначити шляхи з нейтралізації кіберзагроз Збройним Силам України. Тому існує об’єктивне наукове завдання щодо необхідності обґрунтування філософія створення гібридних військово-цивільних формувань для ефективної протидії кіберзагрозам у сучасному безпековому середовищі Збройним Силам України.

Аналіз досліджень та публікацій. Аналіз досліджень показав, що дане питання привернуло увагу достатню кількість зарубіжних та вітчизняних науковців.

В роботі [5] автором досліджено генезис, семантичні зміщення та сучасну роль терміну “гібридна війна (гібридні військові дії)” у когнітивній сфері. Основною метою статті є визначення можливих причин та наслідків імовірної семантичної надмірності терміну “гібридна війна (гібридні військові дії)”. В результаті проведеного аналізу було встановлено, як вживання терміну “гібридна війна (гібридні військові дії)” діє на користь поширення “туману війни”: він замінює загальновизнану концепцію конвенційної війни та спрямовує увагу суспільства до семантичної нечіткості, що неявно призводить до ігнорування основних рис звичайного збройного конфлікту. Це створює когнітивне упередження, яке досі належним чином непроаналізоване та незрозуміле.

В роботі [6] автором здійснюється спроба проаналізувати сутність та ключові

складові війни нового типу, "гібридної війни". Акцентовано увагу, що єдиного визначення природи гібридної війни ще немає. Попри те, що цей термін не є поширеним у військово-теоретичних розвідках, він є цілком придатним для опису нових форм та характеру воєн у постіндустріальному суспільстві. Визначаються характерні риси гібридної війни – використання інформаційної зброї, участь у протистоянні недержавних акторів, використання терористичних методів, нехтування військовим правом та етикою, використання методів економічного та психологічного тиску, пропаганди тощо.

Для розуміння у потребі формування військово-цивільного співробітництва та протидії повномасштабній агресії Російської Федерації проти України, вважаємо за потребу ознайомитися і з публікаціями та ідеям и для адекватної протидії.

В роботі [7] автором досліджено модель гібридної війни. Розкрито послідовність розробки моделі гібридної війни. Описані системні компоненти моделі гібридної війни. Формула Клаузевіца в наші дні могла б звучати в дзеркальному варіанті – "політика є продовженням війни іншими засобами".

В роботі [8] автор приходить до висновку, що бінарна схема "Війна і Мир" не працює. Миру немає ніколи, є тільки зміна форми війни, а мир – обманний трюк. Це внаслідок відсутності адекватної теорії воєн і миру. Мир вважався відсутністю війни. Виходячи з цього автор робить акцент на необхідності:

1. Модернізації теорії війни і миру, оскільки миру немає ніколи, змінюються лише форми протистояння і боротьби. Це значить необхідно народу чітко говорити про зміну військового регістра. Миром може називатися тимчасова пауза рекогносцировки.

2. Ввести чітке тлумачення дефініцій "холодних, гібридних, мережецентричних, інтелектуальних" воєн – для формування бойової свідомості у всіх сферах діяльності.

3. Створення професійних гібридних військ – в усіх напрямках ведення (сучасних війн) – від лінгвістичних до церемоніальних і хронологічних.

4. Для ведення гібридних воєн необхідно інтелектуальне оснащення з режимом постійного інноваційного оновлення, адже новий фронт – інтелектуальний.

Як можна встановити з [5 – 7] питання «гібридної війни» є актуальним, але наразі немає розуміння як їй протистояти. Безумовно війни майбутнього мають бути об'єктом наукових досліджень [9].

Раціональне зерно виявилось в роботі [8], автор якої дійшов до висновку про необхідність формування гібридних військ для протистоянню "гібридній війні". Таким чином, зорієнтуємо наше дослідження на доцільність формування гібридних військ для потреб ЗС України.

Формулювання мети та завдань статті. Обґрунтувати необхідності створення гібридної системи кібербезпеки для нейтралізації кіберзагроз Збройним Силам України та способи її реалізації на засадах військово-цивільного співробітництва.

Для досягнення мети поставлено такі задачі:

1. Проаналізувати сучасний стан досліджень та публікацій.

2. Обґрунтувати необхідності створення гібридної системи кібербезпеки для нейтралізації кіберзагроз Збройним Силам України та способи її реалізації на засадах військово-цивільного співробітництва.

3. Обговорити адміністративно-правові засади гібридного військово-цивільного співробітництва для ефективної нейтралізації кіберзагроз Збройним Силам України.

МЕТОДИ ДОСЛІДЖЕННЯ

Основні інструменти дослідження:

- методи теоретичного історичного аналізу й узагальнення наукової літератури (в т.ч. з інтернет-джерел), за темою дослідження;
- метод аналітично-порівняльного аналізу при оцінюванні новизни результатів дослідження;
- узагальнення – для формулювання висновків і рекомендацій щодо результативності.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Адміністративно-правові засади військово-цивільного співробітництва в країнах ЕС та НАТО в сфері кібербезпеки для нейтралізації кіберзагроз. Основи гібридного військово-цивільного співробітництва з нейтралізації кіберзагроз зазначені в положеннях Договору про Європейський Союз та Лісабонського договору (2009 р.) передбачає створення:

- сфери постійного оборонного співробітництва в Європі;
- постійного структурного співробітництва (PESCO) в області оборони.

В програмі PESCO задіяні учасники 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.

Програма PESCO охоплює 2 проєкти пов’язані з кібербезпекою [10].

Перший проєкт передбачає функціонування платформи обміну інформацією про кіберзагрози і рекомендації щодо реагування на інциденти. Проєкт спрямований на створення проактивних заходів захисту, а також на розробку загальної мережевої платформи для обміну інформацією про кіберзагрози. Відповідальною країною виступає Греція, оскільки в неї знаходиться Європейське агентство з мережевої та інформаційної безпеки (ENISA), яке надає практичні поради та рішення державному і приватному сектору, здійснює обмін інформацією та поширення передового досвіду.

Другий проєкт передбачає функціонування команди швидкого реагування на кіберзагрози і взаємна допомога в області кібербезпеки. Проєкт дозволяє державам-членам спільно забезпечити більш високий рівень кіберстійкості і колективно реагувати на кіберінциденти. Команди швидкого реагування використовують для надання допомоги іншим державам-членам та інститутам ЄС, країнам-партнерам, а також в операціях, що проводяться в рамках загальної політики безпеки і оборони. Основною метою цього проєкту є інтеграція досвіду держав-членів в області кібероборони. Відповідальною країною за організацію виступає Литва, оскільки вона запропонувала і просувала ідею створення кіберпідрозділів швидкого реагування.

Гібридна співпраця між НАТО і ЄС, на думку Генерального секретаря НАТО Й. Столтенберга, має ключове значення для реагування на зростаючі кіберзагрози.

Гібридна співпраця між НАТО і ЄС розвивається на основі підписаної в 2016 р спільної Декларації, в якій визначено пріоритетний напрямок взаємодії у сфері кібербезпеки та кібероборони. З метою перевірка здібностей гібридного військово-цивільного співробітництва НАТО і ЄС з протидії кібератакам і відпрацювання взаємодії на внутрішньодержавному і міжнародному рівнях в Естонії 28 листопада 2017 року відбулися сумісні навчання “Di-Si Cannabis Koalishn”.

Подальший розвиток гібридного військово-цивільного співробітництва НАТО з державами, що не входять до Альянсу набуло за результатами участі японських фахівців в Естонії в дослідженнях з кібербезпеки. За результатами навчань в 2018 році були переглянуті основні напрямків національної оборонної програми Японії, і в рамках цього процесу в Міністерстві Оборони створено командний центр для управління операціями в космосі і кіберпросторі. Він має взаємодіяти з НАТО і відповідними структурами США. При цьому чисельність підрозділів кібербезпеки складе приблизно 1000 чоловік.

За даними джерела [11; 8] зазначається, що компетенція бізнеса, приватного сектора незамінні і необхідні для створення ефективного гібридного механізму захисту об'єктів критичної інфраструктури.

Розглянемо адміністративно-правові засади та підстави до створення і функціонування нового формування гібридних кібервійськ на основі військово-цивільного співробітництва для доповнення Збройних Сил України.

Адміністративно-правові засади військово-цивільного співробітництва в Україні. Аналогічну гібридну співпрацю до НАТО та ЄС в Україні пропонується організувати функціонування і взаємодію Збройних Сил України з державними організаціями та приватним сектором для нейтралізації кіберзагроз можна на підставі Закону України "Про основні засади забезпечення кібербезпеки України" [12], а саме:

Стаття 10. Державно-приватна взаємодія у сфері кібербезпеки в якій визначено:

1. Державно-приватна взаємодія у сфері кібербезпеки здійснюється шляхом:

1) створення системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій;

2) підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських проєктів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту;

3) обміну інформацією між державними органами, приватним сектором і громадянами щодо кіберзагроз об'єктам критичної інфраструктури, інших кіберзагроз, кібератак та кіберінцидентів;

4) партнерства та координації команд реагування на комп'ютерні надзвичайні події;

5) залучення експертного потенціалу, наукових установ, професійних об'єднань та громадських організацій до підготовки ключових галузевих проєктів та нормативних документів у сфері кібербезпеки;

6) надання консультативної та практичної допомоги з питань реагування на кібератаки;

7) формування ініціатив та створення авторитетних консультаційних пунктів для громадян, представників промисловості та бізнесу з метою забезпечення безпеки в мережі Інтернет;

8) запровадження механізму громадського контролю ефективності заходів із забезпечення кібербезпеки;

9) періодичного проведення національного саміту з професійними постачальниками бізнес-послуг, включаючи страховиків, аудиторів, юристів, визначення їхньої ролі у сприянні кращому управлінню ризиками у сфері кібербезпеки;

10) створення системи підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки;

11) тісної взаємодії з фізичними особами, громадськими та волонтерськими організаціями, ІТ-компаніями з метою виконання заходів кібероборони в кіберпросторі.

2. Державно-приватна взаємодія у сфері кібербезпеки застосовується з урахуванням встановлених законодавством особливостей правового режиму щодо окремих об'єктів та окремих видів діяльності.

Отже, на підставі абзаців 1, 3 та 11 пункту 1 статті 10 Закону України [12] нами запропоновано для нейтралізації можливих кіберзагроз Збройним Силам України та державі реалізувати на практиці пункт 2 статті 10 та Закону України [12] шляхом державно-приватної взаємодія не лише під час проведення інформаційної операції, але на постійній основі для забезпечення кібербезпеки [13].

Розглянемо можливу взаємодію у сфері кібербезпеки Збройних Сил України із фахівцями з приватного сектору.

Підготовка військових фахівців з кібербезпеки у Військовому інституті телекомунікацій та інформатизації імені Героїв Крут та інших ВВНЗ націлена на формування навиків менеджменту (військового управління) у майбутніх офіцерів здібних до виконання окремих завдань за призначення пов'язаних з військовою службою та високим ризиком для життя [14].

Потреби у фахівцях з кібербезпеки для інших сфер як правило поповнюються за рахунок підготовки зазначених фахівців у цивільних ВНЗ.

Оскільки випускники ВВНЗ та ВНЗ мають абсолютно різне уявлення про перспективу професійної діяльності та індивідуальну мотиваційну характеристику [15], то необхідно при допуску до кібернетичного протистояння з'ясовувати їх мотиваційну характеристику [16].

Сучасна практика підтверджує низьку вмотивованість фахівців з освітньо-кваліфікаційним рівнем (бакалавр, магістр) у сфері кібербезпеки до підписання контракту та проходження військової служби в Збройних Силах України через низку факторів, а саме:

- низький рівень грошового забезпечення;
- режим роботи та обмеження пов'язані зі специфікою військової служби;
- відсутність вирішення проблеми у забезпеченні постійним або службовим житлом військовослужбовців та систематичного порушення соціальних гарантій військовослужбовцям та членів їх сімей [17];
- інші переконання, в тому числі пов'язані з віросповіданням.

Метою формування гібридних кібервійськ Збройних Сил України на основі військово-цивільного співробітництва є максимальне залучення мотивованих, цілеспрямованих і наполегливих фахівці-практики у вузькій сфері кібербезпеки подібних до тих, що ідентифікують себе до угрупування "Хакер" [15].

Розглянемо можливий формат військово-цивільного співробітництва.

Поштовхом до вибору оптимального формату військово-цивільного співробітництва став безпрецедентний виклик всього світу пандемія COVID 19 [18].

В умовах жорсткого національного карантину в Збройних Силах України успішно була апробована форма дистанційної роботи працівниками (цивільними) та військовослужбовцями.

Військово-цивільне співробітництво за дистанційною формою можливе з адміністративно-правової (пункт 1 статті 10 Закону України [12]) та мотиваційної точки зору пропонувати фахівцям цивільних ВНЗ і всім зацікавленим з приватного сектора як один з варіантів проходження альтернативної служби.

Альтернативний варіант проходження служби у Збройних Силах України [19] є формою виконання громадянином України військового обов'язку щодо захисту Вітчизни, незалежності та територіальної цілісності України, шанування її державних

символів відповідно статті 65 Конституції України [20].

Пропонування альтернативного варіанту проходження служби у Збройних Силах України – це дійсно дієвий механізм реалізації державно-приватної взаємодії у сфері кібербезпеки із залучення фахівців із цивільних ВНЗ і всіх зацікавлених з приватного сектора.

Обговорення попередніх результатів

Очікуваний ефект від впровадження військово-цивільного співробітництва за дистанційною формою:

1) збільшиться потенціал сил та засобів Збройних Сил України у сфері кібербезпеки наполегливими фахівцями-практиками з високим рівнем мотивації, цілеспрямованості за рахунок підписання контрактів з різними термінами проходження альтернативної військової служби;

2) сформувати актуальну кваліфіковану "пісочницю" фахівців-практиків з кібербезпеки, що спроможні оперативно реагувати на кіберзагрози та інциденти;

3) економія на військовому забезпеченні (обмундировані, котловому та інших видах) фахівців, які підписали контракти на проходження альтернативної військової служби.

Теоретичні результати одержані в процесі наукового пошуку прогнозують, що сформовані гібридні війська спроможні будуть протидіяти складовій гібридній формі ведення війни в соціальних мережах [21]. Цікавим та перспективним напрямком подібних досліджень є перевірка узгодженості децентралізації управління військами (силами) в гібридній війні [22].

Для досягнення позитивного ефекту, Збройні Сили України мають взяти зобов'язання і бути гарантом військово-цивільного співробітництва:

- не залучати фахівців до виконання функціональних обов'язків не пов'язаних з профілем діяльності;
- надавати фахівцям офіційного статусу працівників Збройних Сил України з відповідним соціальним пакетом;
- надання фахівцям можливості займатися науковою, науково-педагогічною, науково-технічною та інноваційною діяльністю;
- гарантувати відпустку згідно порядку проходження альтернативної військової служби [19];
- гарантувати час перебування громадянина на альтернативній військовій службі зараховувати до його страхового стажу. Цей час також зараховується до безперервного стажу роботи і стажу роботи за спеціальністю за умови, якщо громадянин не пізніше ніж протягом трьох календарних місяців після звільнення з альтернативної служби приступить до роботи;
- надавати за необхідності фахівцям у тимчасове розпорядження озброєння та військову техніку за профілем професійної діяльності;
- виступати гарантом інших зобов'язань згідно чинного законодавства.

Зобов'язання, що покладаються на фахівців за умови військово-цивільного співробітництва:

- наполегливо, на високому професійному рівні виконувати покладені посадові функціональні обов'язки у сфері кібербезпеки, оперативна реагувати на кіберзагрози та інциденти, виробляти практичні рекомендації з їх нейтралізації;

– проводити інформаційно-роз'яснювальну агітаційну роботу серед знайомих колег до залучення (вибору) альтернативної військової служби у Збройних Силах України;
– вести превентивну (попереджувальну) роботу серед знайомих колег, що ідентифікують себе до угрупування "Хакер" про адміністративну та кримінальну відповідальність у разі вчинення втручання у функціонування складові системи кібербезпеки Збройних Сил України та/або держави, бездіяльність у разі, якщо стали відомі такі факти.

Досвід військово-цивільного співробітництва неформальних груп України проти військової агресії Російської Федерації.

З початком повномасштабної військової агресії Російської Федерації проти України, визначені Державні органи та організаційні структури, з носіями спроможностей виявились не спроможними виконувати завдання за призначенням.

Адміністративно-правовою основою, для організації військово-цивільного співробітництва у проведенні активних та пасивних заходів в кіберпросторі, слід вважати подію "затвердження у 2016 р. Президентом України Стратегії кібербезпеки України". Вперше в оборонну термінологію було введено поняття "кібероборона" [23].

У проєкті Указу Президента України від 2021 "Про рішення Ради національної безпеки і оборони України", "Про Стратегічний оборонний бюлетень України", з яким можна ознайомитися за посиланням [25] запропоновано доповнити термінологію поняттям "кібердорозвідка – збір інформації щодо вразливостей програмного забезпечення, телекомунікаційного обладнання, автоматизованих систем управління силами, зброєю та/або технологічними процесами визначеної цілі".

У затвердженому Указі Президента України від 17.09.2021 №473/2021 [25] під кібердорозвідкою розуміють діяльність щодо виявлення вразливостей програмного забезпечення, телекомунікаційного обладнання, автоматизованих систем управління силами, зброєю та/або технологічними процесами визначеної цілі (об'єкта кіберінфраструктури).

У додатку 3. Стратегічного оборонного бюлетеня України "Матриця основних спроможностей сил оборони" систематизовані Інституційні спроможності центральних органів виконавчої влади та інших державних органів, які здійснюють керівництво, спрямовують та координують діяльність військових формувань, що входять або виділяють відповідні сили і засоби до складу сил оборони, та оперативні, бойові і спеціальні спроможності сил оборони. Так згідно якого за реалізацію здатності ведення кіберрозвідки та кібердорозвідки в інформаційно-телекомунікаційних мережах та системах державного, приватного і військового призначення (об'єктів критичної інфраструктури) противника для здобуття інформації про кіберінфраструктуру противника, їх призначення, місцезнаходження, технологічних процесів, уразливості, встановлення прихованого контролю, перехоплення та дешифрування керуючих і ресурсних даних та інформації покладаються на: Головне управління розвідки Міноборони, Збройні Сили України, Державна прикордонна служба України.

В перші дні повномасштабної військової агресії Російської Федерації в контексті військово-цивільного співробітництва, потужну і превентивну допомогу в реалізації кібердорозвідки, реалізовано на базі кафедри кібербезпеки та комп'ютерної інженерії, Київський національний університет будівництва і архітектури (під керівництвом завідувача кафедри д.т.н., проф. Хлапонін Ю.І.). Отримані практичні успіхи підтвердили гіпотезу про ефективність і необхідності створення гібридних підрозділів військово-цивільного співробітництва.

Відсутність пропозицій зі сторони Збройних Сил України до військово-цивільного співробітництва, небайдужими фахівцями ІТ галузі та кібербезпеки в екстреному односторонньому порядку створювалися Телеграм-канали для виконання широкого спектру завдань із запобігання кібервтручання Російської Федерації в об'єкти критичної інформаційної інфраструктури України.

Так, наприклад, станом на 18:00 25.02.2022 р. Телеграм-канал "Кібер Армія", "Stop Russian Channel MRIYA" нараховували понад 250 тисяч активних учасників.

Звичайні люди, поряд із професіоналами сфери ІТ, наносять нищівний удар атакуючи ворога у кіберпросторі, завдають йому збитків та зривають плани [26, с. 41].

Адміністратори періодично і за результатами обстановки в кіберпросторі формували дозовані завдання небайдужими фахівцями в галузі ІТ та кібербезпеки:

- пошуку та виявлення вразливостей програмного забезпечення, телекомунікаційного обладнання, автоматизованих систем управління силами, зброєю та/або технологічними процесами визначеної цілі (об'єкта кіберінфраструктури) Російської Федерації та Республіки Білорусь;
- блокування інтернет ресурсів, що поширювали інформацію про насилля, шляхом подачі відповідних заявок адміністраторам відповідних ресурсів;
- реалізація через VPN проникнення та вивчення архітектури об'єктів критичної інформаційної інфраструктури Російської Федерації та Республіки Білорусь;
- реалізація активних заходів впливу на порушення правильності функціонування об'єктів критичної інформаційної інфраструктури Російської Федерації та Республіки Білорусь;
- підготовка "відео снарядів" інформаційно-роз'яснювальної пропаганди для користувачів Російської Федерації, Республіки Білорусь та країн НАТО про стан і супротив населення та Збройних Сил України повномасштабній військовій агресії Російської Федерації проти України.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Таким чином, виходячи з вище розглянутого дослідження сформулюємо нові висновки.

1 Для протистояння гібридній війні та нейтралізації кіберзагроз Збройним Силам України та держави необхідно створити гібридні підрозділи на основі військово-цивільного співробітництва.

2. На основі альтернативної військової служби залучити до військово-цивільного співробітництва мотивованих, цілеспрямованих і наполегливих фахівців-практиків у сфері кібербезпеки.

Перспективи подальших досліджень. Представлене дослідження не вичерпує всіх аспектів зазначеної проблеми. Теоретичні та практичні результати, що одержані в процесі наукового пошуку, становлять підґрунтя для подальшого дослідження у обраному напрямку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Петренко, А.Г. (2016). *План дій щодо впровадження оборонної реформи у 2016-2020 роках (дорожня карта оборонної реформи)*. ДВПСП та МС МО України.

2 Закон України «Про основні засади забезпечення кібербезпеки України» (2017). https://zakon.rada.gov.ua/laws/show/2163-19.
3 Указ Президента України «Про Стратегію кібербезпеки України». (2016). https://zakon5.rada.gov.ua/laws/show/96/2016.
4 Указ Президента України «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації». (2017). https://zakon.rada.gov.ua/laws/show/n0006525-17.
5 Лобода, Ю.О. (2020). Поняття «гібридна війна (гібридні військові дії)»: походження та складність. *Наука і оборона*, 20–23.
6 Магда, Є.М. (2014). Гібридна війна: сутність та структура феномену. *Міжнародні відносини: Серія. «Політичні науки», 4*. http://journals.iir.kiev.ua/index.php/pol_n/article/viewFile/2489/2220.
7 Бартош, А.А. (2019). Модель гибридной войны. «*Военная мысль» Военно-теоретический журнал МО РФ*. https://vm.ric.mil.ru/Stati/item/191517.
8 Магнитов, С.Н. (2021). Что между войной и миром? *Академия Тринитаризма*. Эл №77-6567. http://www.trinitas.ru/rus/doc/0012/001g/00125039.htm.
9 Ільяшов, О.А. (2008). Війни майбутнього як об'єкт наукових досліджень. *Наука і оборона*, *2*, 36–40.
10 NATO and the European Union work together to tackle growing cyber threats. (2018). North Atlantic Treaty Organization. https://www.nato.int/cps/uk/natohq/news_161570.htm?selectedLocale=en.
11 Демидов, О. (2016). *Глобальное управление интернетом и безопасность в сфере использования ИКТ: ключевые вызовы для мирового сообщества.* Интеллектуальная Литература.
12 Закон України «Про основні засади забезпечення кібербезпеки України». (2017).
13 Мазниченко, Ю.А., Живило, Є.О., Козубцов, І.М., Машталір, В.В. (2015). Взаємодія Збройних Сил України, інших військових формувань та правоохоронних органів, органів державної влади під час проведення інформаційної операції. У *VIII науково-практична конференція «Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення з урахуванням досвіду АТО»*, (с. 27–30).
14 Козубцовб І.М., Хлапонинб Ю.І., Процюкб Ю.О. (2013). Методологічні основи підготовки фахівців інформаційної безпеки в технічних ВНЗ: філософсько-технічний аспект. *Інформаційна безпека. Науковий журнал. Східноукраїнський національний університет ім. Володимира Даля*, 35–41.
15 Козубцовб І.М. (2015). Про мотиваційний портрет учасники кібернетичного протистояння. *Матеріали першої міжнародної науково-технічної конференції «Актуальні проблеми розвитку науки і техніки»*, 208–211.
16 Козубцов, І.М., Козубцова, Л.М., Живило, Є.О., Куцаєв, В.В. (2016). Про необхідність дослідження мотиваційної характеристики військовослужбовців при допуску їх до кібернетичного протистояння. *Науково-практична конференція «Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку»*, 35–36.
17 Козубцов, І.М., Радченко, М.М., Артемчук, М.В. (2021). Проблема забезпечення житлом військовослужбовців: сутність, причини, наслідки та шляхи її рішення. *І Міжнародна науково-практична конференція «Соціальні аспекти військово-професійної діяльності сектора безпеки і оборони: виклики сьогодення»*, 33–35.
18 Schwab, K., Malleret, T. (2020). *COVID-19: The Great Reset. Edition 1.0*. Switzerland. Cologny/Geneva.: Forum publishing World Economic Forum.
19 Закон України «Про альтернативну (невійськову) службу» (1991).
20 Конституція України. Закон України (1996).
21 Куцаєв, В.В., Терещенко, Т.П., Козубцов, І.М. (2017). Інформаційне протистояння в соціальних мережах. *Науково-практична конференція «Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку»*, 21–22.
22 Корендович, В.С., Чірікалов, О.С. (2020). Проблема децентралізації управління військами (силами) в гібридній війні. *Наука і оборона*, *3*, 32 – 40.
23 Указ Президента України «Про Стратегію кібербезпеки України». (2016). https://zakon.rada.gov.ua/laws/show/96/2016/ed20210828.
24 Проект Указу Президента України «Про Стратегічний оборонний бюлетень України». (2021). https://www.mil.gov.ua/content/pdf/up_rrnb.pdf.
25 Указ Президента України «Про Стратегічний оборонний бюлетень України». (2021). https://zakon.rada.gov.ua/laws/show/473/2021.
26 Мальцева, І., Черниш, Ю., Штонда, Р. (2022). Аналіз деяких кіберзагроз в умовах війни. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *4*(16), 37-44. https://doi.org/10.28925/2663-4023.2022.16.3744.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (19), 2023
ISSN 2663 - 4023

Oleksandr A. Ponomarov
head of the Faculty of combat use of control and communication systems
Military Institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine
ORCID ID: 0009-0008-2320-1549
aleksan_bimer3@ukr.net

Serhii A. Pyvovarchuk
head of the Department of combat use of communications units
Military Institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine
ORCID ID 0000-0001-9410-5951
sergij.pyvovarchuk@viti.edu.ua

Lesya M. Kozubtsova
candidate of Technical Sciences,
head of the Department of mathematics and physics
Military Institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine
ORCID 0000-0002-7866-8575
lesia.kozubtsova@viti.edu.ua

Igor M. Kozubtsov
Doctor of Pedagogical Sciences, Candidate of Technical Sciences, Senior researcher
professor of the Department of combat use of communication units
Military Institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine
ORCID ID 0000-0002-7309-4365
kozubtsov@gmail.com

Tetiana V. Bondarenko
senior researcher at the research department of cyber security in information and telecommunications systems
Military Institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine
ORCID ID 0000-0002-2879-2041
tanjusha170393@gmail.com

Tetiana P. Tereshchenko
senior researcher at the research department of cyber security in information and telecommunications systems
Military Institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine
ORCID ID 0000-0002-9659-7897
tany-83@ukr.net

HYBRID CONSTRUCTION OF CYBER SECURITY SYSTEM: ADMINISTRATIVE AND LEGAL PRINCIPLES OF MILITARY-CIVIL COOPERATION

Abstract. National security of the state is one of the main factors of stable development of society. However, Ukraine and the Armed Forces of Ukraine are forced to counter a hybrid war using cyberspace. It has been established that currently there is no unified vision regarding the methodology of countering wars in a hybrid form. The lack of a countermeasure methodology requires a review of existing approaches to guaranteeing and maintaining state security. The purpose of the article. Justification of the need to create hybrid troops to neutralize cyber threats to the Armed Forces of Ukraine and methods of its implementation on the basis of military-civilian cooperation. Materials and methods. To solve the tasks, a set of theoretical research methods was used: historical analysis and generalization of scientific literature on the research problem; structural and genetic analysis and synthesis when specifying the object and subject of research; the method of going from the abstract to the concrete; the method of analytical and comparative analysis in the analytical and comparative evaluation of the novelty of research results; synthesis and generalization - to justify the methodological and methodical foundations of the research; generalization – formulation of conclusions and recommendations regarding the continuation of further research. Result. A key hypothesis was formed that an effective tool in countering hybrid warfare can be achieved through the use of hybrid troops. Developing this hypothesis substantiates the philosophical idea of the need to create hybrid cyber armies on the basis of military-civilian formations. Foreign experience

confirms the high efficiency of military-civilian formations. On the basis of the current legal acts, a method of implementation is proposed. The practical significance of the study lies in the possibility of obtaining advantages in the cyberspace of the Armed Forces of Ukraine during active hybrid wars due to the formation of units of hybrid troops of the Armed Forces of Ukraine.

Keywords: hybrid; military-civilian formations; neutralization; cyber threats; Armed Forces of Ukraine.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 Petrenko, A.H. (2016). *Plan dii shchodo vprovadzhennia oboronnoi reformy u 2016-2020 rokakh (dorozhnia karta oboronnoi reformy)*. DVPSP ta MS MO Ukrainy.
2 Zakon Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy» (2017). https://zakon.rada.gov.ua/laws/show/2163-19.
3 Ukaz Prezydenta Ukrainy «Pro Stratehiiu kiberbezpeky Ukrainy». (2016). https://zakon5.rada.gov.ua/laws/show/96/2016.
4 Ukaz Prezydenta Ukrainy «Pro zahrozy kiberbezpetsi derzhavy ta nevidkladni zakhody z yikh neitralizatsii». (2017). https://zakon.rada.gov.ua/laws/show/n0006525-17.
5 Loboda, Yu.O. (2020). Poniattia «hibrydna viina (hibrydni viiskovi dii)»: pokhodzhennia ta skladnist. *Nauka i oborona*, 20–23.
6 Mahda, Ye.M. (2014). Hibrydna viina: sutnist ta struktura fenomenu. Mizhnarodni vidnosyny: Seriia. «Politychni nauky», *4*. http://journals.iir.kiev.ua/index.php/pol_n/article/viewFile/2489/2220.
7 Bartosh, A.A. (2019). Model gibridnoi voiny Voennaia mysl Voenno-teoreticheskii zhurnal MO RF. https://vm.ric.mil.ru/Stati/item/191517.
8 Magnitov, S.N. (2021). Chto mezhdu vojnoj i mirom? *Akademiia Trinitarizma.* El 77-6567. http://www.trinitas.ru/rus/doc/0012/001g/00125039.htm.
9 Iliashov, O.A. (2008). Viiny maibutnoho yak ob'iekt naukovykh doslidzhen. *Nauka i oborona*, *2*, 36–40.
10 NATO and the European Union work together to tackle growing cyber threats. (2018). North Atlantic Treaty Organization. https://www.nato.int/cps/uk/natohq/news_161570.htm?selectedLocale=en.
11 Demidov, O. (2016). Globalnoe upravlenie internetom i bezopasnost v sfere ispolzovaniia IKT kliuchevye vyzovy dlia mirovogo soobshchestva Intellektualnaia Literatura.
12 Zakon Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy». (2017).
13 Maznychenko, Yu.A., Zhyvylo, Ye.O., Kozubtsov, I.M., Mashtalir, V.V. (2015). Vzaiemodiia Zbroinykh Syl Ukrainy, inshykh viiskovykh formuvan ta pravookhoronnykh orhaniv, orhaniv derzhavnoi vlady pid chas provedennia informatsiinoi operatsii. In VIII naukovo-praktychna konferentsiia «Priorytetni napriamky rozvytku telekomunikatsiinykh system ta merezh spetsialnoho pryznachennia z urakhuvanniam dosvidu ATO», 27–30.
14 Kozubtsov, I.M., Khlaponyn, Yu.I., Protsiuk, Yu.O. (2013). Metodolohichni osnovy pidhotovky fakhivtsiv informatsiinoi bezpeky v tekhnichnykh VNZ: filosofsko-tekhnichnyi aspekt. Informatsiina bezpeka. Naukovyi zhurnal. Skhidnoukrainskyi natsionalnyi universytet im. Volodymyra Dalia, 35–41.
15 Kozubtsov, I.M. (2015). Pro motyvatsiinyi portret uchasnyky kibernetychnoho protystoiannia. Materialy pershoi mizhnarodnoi naukovo-tekhnichnoi konferentsii «Aktualni problemy rozvytku nauky i tekhniky», 208–211.
16 Kozubtsov, I.M., Kozubtsova, L.M., Zhyvylo, Ye.O., Kutsaiev, V.V. (2016). Pro neobkhidnist doslidzhennia motyvatsiinoi kharakterystyky viiskovosluzhbovtsiv pry dopusku yikh do kibernetychnoho protystoiannia. Naukovo-praktychna konferentsiia «Zastosuvannia informatsiinykh tekhnolohii u pidhotovtsi ta diialnosti syl okhorony pravoporiadku», 35–36.
17 Kozubtsov, I.M., Radchenko, M.M., Artemchuk, M.V. (2021). Problema zabezpechennia zhytlom viiskovosluzhbovtsiv: sutnist, prychyny, naslidky ta shliakhy yii rishennia. I Mizhnarodna naukovo-praktychna konferentsiia «Sotsialni aspekty viiskovo-profesiinoi diialnosti sektora bezpeky i oborony: vyklyky sohodennia», 33–35.
18 Schwab, K., Malleret, T. (2020). COVID-19: The Great Reset. Edition 1.0. Switzerland. Cologny/Geneva.: Forum publishing World Economic Forum.
19 Zakon Ukrainy «Pro alternatyvnu (neviiskovu) sluzhbu». (1991).
20 Konstytutsiia Ukrainy. Zakon Ukrainy. (1996).
21 Kutsaiev, V.V., Tereshchenko, T.P., Kozubtsov, I.M. (2017). Informatsiine protystoiannia v sotsialnykh

merezhakh. Naukovo-praktychna konferentsiia «Zastosuvannia informatsiinykh tekhnolohii u pidhotovtsi ta diialnosti syl okhorony pravoporiadku», 21–22.

22 Korendovych, V.S., Chirikalov, O.S. (2020). Problema detsentralizatsii upravlinnia viiskamy (sylamy) v hibrydnii viini. Nauka i oborona, 3, 32 – 40.

23 Ukaz Prezydenta Ukrainy «Pro Stratehiiu kiberbezpeky Ukrainy». (2016). https://zakon.rada.gov.ua/laws/show/96/2016/ed20210828.

24 Proekt Ukazu Prezydenta Ukrainy «Pro Stratehichnyi oboronnyi biuleten Ukrainy». (2021). https://www.mil.gov.ua/content/pdf/up_rrnb.pdf.

25 Ukaz Prezydenta Ukrainy «Pro Stratehichnyi oboronnyi biuleten Ukrainy». (2021). https://zakon.rada.gov.ua/laws/show/473/2021.

26 Maltseva, I., Chernysh, Yu., Shtonda, R. (2022). Analiz deiakykh kiberzahroz v umovakh viiny. Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnika», 4(16), 37-44. https://doi.org/10.28925/2663-4023.2022.16.3744.

This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.