СВІТОВИЙ ДОСВІД ДЕРЖАВНОГО УПРАВЛІННЯ

DOI: https://doi.org/10.26565/1684-8489-2023-2-08
УДК 351.76:347.73006.013

Живило Євген Олександрович,
кандидат наук з державного управління,
докторант кафедри публічної політики
навчально-наукового інституту "Інститут державного управління"
Харківського національного університету імені В. Н. Каразіна,
майдан Свободи, 4, м. Харків, 61022, Україна

e-mail: zhivilka@i.ua *https://orcid.org/0000-0003-4077-7853*

ПОШУК ТА ЗАСВОЄННЯ СУЧАСНИХ КАДРОВИХ КОМПЕТЕНТНОСТЕЙ СФЕРИ КІБЕРБЕЗПЕКИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ДЕРЖАВИ

Анотація: Обґрунтовано актуальність того що сучасні електронно-комунікаційні системи та мережі, а також апаратні та програмні комплекси та засоби є доволі вразливими до кібернетичних впливів. Метою статті є стисле узагальнення міжнародного досвіду сучасних кадрових компетентностей сфери кібербезпеки та виокремлено їх складові за відповідними напрямками.

Проаналізовано сучасні міжнародні тенденції щодо формування мінімально необхідного пакету зі створення, впровадження, технічної підтримки та вдосконалення системи менеджменту інформаційної безпеки і кіберзахисту. В свою чергу зазначене вище вимагає від держави розвитку обізнаного в цифровому відношенні суспільства що є найважливішою сферою її внутрішньої політики.

Акцентовано увагу на одному з беззаперечних фактів, що в умовах подальшого розвитку високотехнологічного суспільства потреба у фахівцях із кібербезпеки буде постійно зростати, а за умов тотальної оборони держави роль об'єднаної підготовки персоналу складових сил оборони та цивільного сектору в сфері кібербезпеки взагалі не піддається ніякому сумніву.

Ключові слова: цифрові технології, система захисту інформації, кібербезпека, інформаційні технології, інформаційна безпека, національна безпека, кібервплив.

Постановка проблеми. Захист інформації (*далі – ЗІ*) в сучасних умовах стає все більш складною проблемою, що зумовлено рядом обставин [2; 7; 20]. До їх числа можна віднести такі: динамічні показники розвитку засобів електронно-обчислювальної техніки; перехід систем телекомунікацій на цифрову обробку сигналів; ускладнення шифрувальних технологій; несанкціоновані дії

Як цитувати: Живило Є. О. Пошук та засвоєння сучасних кадрових компетентностей сфери кібербезпеки в умовах цифрової трансформації держави. *Актуальні проблеми державного управління*. 2023. № 2 (63). С. 111–127. DOI: https://doi.org/10.26565/1684-8489-2023-2-08

In cites: Zhyvylo, Y.O. (2023). Exploring and acquiring modern human resource competencies in cybersecurity amidst state digital transformation. *Pressing Problems of Public Administration, 2 (63), 111–127.* DOI: https://doi.org/10.26565/1684-8489-2023-2-08 [in Ukrainian].

та загрози безпеці системам електронних комунікацій, системам управління технологічними процесами; сталий розвиток інформаційного суспільства та цифрового комунікативного середовища [11; 13].

Порушення цілісності інформації в системі, її виток та втрата може призвести до тяжких наслідків, тому питання захисту інформації є дуже важливими. Необхідно зазначити, що на сьогодні системи захисту інформації та кібербезпеки корпорацій, установ (організацій) світового рівня обробляють та зберігають доволі потужний масив конфіденційних даних, таких як клієнт-транзакції, інформацію про облікові записи та приватні персональні дані платіжних карток, платіжні процесори та інше [17]. При цьому цю обставину ускладнює постійна зміна обсягу, швидкості і різноманітності атак, які варіюються від відмови в обслуговуванні до зловмисного викрадення зсередини [19]. Зі збільшенням кількості резонансних порушень систем КБ установ (організацій) у всьому світі, вона змінилася від суто питання інформаційних технологій (*далі – ІТ*), до викликів занепокоєння на рівні правління компаній. Наслідки витоку даних далекосяжні та критичні.

У таких умовах все більше організацій та установ усвідомлюють, що традиційних рішень безпеки та ручних процедур вже недостатньо для виконання та підтримки політик безпеки [12]. В цьому контексті організаціям (установам, підприємствам) не забороняється нарощувати свої спроможності з питань інформаційної безпеки (*далі – ІБ*) та кібербезпеки. Але, враховуючи загальноприйняті у міжнародній практиці принципи забезпечення інформаційної безпеки і кіберзахисту, будь-які установи повинні в своїй діяльності здійснювати управління ризиками КБ, на об'єктах критичної інформаційної інфраструктури, у відповідності до міжнародних стандартів, стандартів Європейського Союзу та НАТО [10].

У цілому, сучасні компетенції спеціаліста з кібербезпеки повинні ґрунтуватись на оволодінні сучасними ІТ, фундаментальними та прикладними науковими дисциплінами, що дозволяє одержувати високий рівень теоретичного та практичного навчання. Попередньо проведений аналіз дозволяє стверджувати, що США приділяють велику увагу посиленню національної безпеки, захисту цивільних прав та інтересів бізнесу тому, що науковий, технічний, військовий, фінансовий потенціал та потенціал високих технологій США є національним надбанням американського народу, що потребує захисту на державному рівні [12]. Концентрація найбільших фінансових компаній, науково-дослідницьких установ та корпорацій, які суттєво впливають на фінансову стабільність і економічний розвиток країни, на створення та розвиток важливих технологічних процесів підсилюють значимість управління кібербезпеки в США [5].

За цих умов, показовим є те, що до сукупності кращих світових навчальних закладів у галузі кібербезпеки належать американські вищі навчальні заклади, а саме: Каліфорнійський державний університет Сан-Бернардіно, штат Каліфорнія; Університет Карнегі-Меллона, Піттсбург, штат Пенсильванія; Університет Джорджа Вашингтона, округ Колумбія; Університет Індіани Блумінгтон, штат Індіана. Також ці питання вивчаються і в військових закладах вищої освіти, таких як: Технологічний університет ВПС (Air Force Institute of Technology, Wright-Patterson AFB, Ohio); Університет інформаційних технологій (Universiti of information Technologi, Fort Gordon, GA); Університет національної оборони (National Defense University); коледж інформаційного ме-

неджменту (Information Resources Management College-School of Information Warfare and Strategy at NDU) Fort McNair, Washington, D.C. та інших військових закладах вищої освіти.

Тому, розуміючи ситуацію, в якій перебуває наша країна, та трансформаційні процеси, що відбуваються у сфері надання освітніх послуг серед вищих навчальних закладів, вкрай необхідно керівникам та науково-педагогічним працівникам зосередитись на розбудові та нарощуванні власних спроможностей в підготовці фахівців за спеціальністю 125 "Кібербезпека" для цивільного та військового сектору. При цьому важливо враховувати у своїй діяльності аналіз досвіду сучасних активних кібердій (кібероперації/кібервійни), дані розвідки, світові шаблони та наративи, тактику та інструменти які використовує ворог та різні угрупування, а також власний національний досвід фахівців з кібербезпеки (далі – КБ).

Аналіз останніх досліджень і публікацій. Проведений аналіз наукових робіт які були спрямовані на теоретико-методологічне обґрунтування і практичне впровадження системи підготовки персоналу за спеціальністю 125 "Кібербезпека" доволі розгалужений та змістовний. Національний сегмент представлений доволі досвідченими та серйозними науковцями-дослідниками, а саме: Л. Арсенович, Б. Бистрова, В. Богуш, В. Бурячок, П. Воробієнко, С. Воскобойніков, Ю. Даник, І. Діордиця, О. Євсюкова, Т. Запорожець, О. Карпенко, І. Кулик, О. Корнейко, С. Мамченко, С. Мельник, О. Новіков, О. Оксіюк, Л. Рудник, І. Руснак, А. Семенченко, В. Телелим та ін. Їх праці вже спрямовані на вивчення сучасних підходів, закономірностей і технологій щодо формування системи підготовки фахівців у сфері кібербезпеки органів публічної влади, формування концептуальних засад професійної підготовки фахівців із кібербезпеки та удосконалення чинного законодавства, що регулює сферу інформаційної безпеки та кібербезпеки, сутності інформаційної безпеки та кібербезпеки, як складових елементів національної безпеки, а також практики підготовки до протидії та ведення війни у кібернетичному та інформаційному просторах, протидії кіберзлочинності тощо.

Проведенням досліджень «дилем» теоретичного обґрунтування ландшафту кіберзагроз та визначення практично-методологічної складової з питань кібербезпеки на міжнародному рівні, доволі якісно та змістовно продовжують досліджувати експерти Об'єднаного центру передових технологій з кібероборони НАТО, а саме: А. Хаггманробить, С. Вонг, Л. Вайсінгер, М. Деніел, Дж. Кенуя, Ш. Абрахам, С. Долтрі, Л. А. ДаСілви, Дж. Рід, С. Шетті, Дж. Парк, Д. Вій Секери, Х. Ванга, С. Соаре, Дж. Бартон, Я. Белласіо, Е. Сільфверстен, Дж. Блек, Е. Лінч, Ф.-Ш. Гаді, О. Стронелл, Дж. Черавіч, Б. Ліллі, М. Лібіцкі, О. Ткачова та ін.

Їх методологічний внесок у дискусію НАТО з питань кібербезпеки зосереджений на інструментах уяви і прогнозування майбутнього кіберконфлікту в його різних соціальних, політичних і технологічних вимірах, зокрема, щодо, посилення режиму експертної оцінки для розв'язання проблем кібербезпеки, глибшого розуміння складності архітектури мережі, в тому числі моделювання загроз і кібератак, з акцентом на надання більш ефективних і адаптованих рішень з кібербезпеки.

Взагалі, слід зазначити, що погляди представників, як цивільного сектору, так і сектору оборони держав-партнерів спрямовані на виклики пов'язані з новими руйнівними технологіями в кіберсфері наступного десятиліття, пос-

тійно розглядаються концептуальні та практичні взаємозв'язки між місцевою та наднаціональною безпекою в умовах розвитку високих технологій.

Метою статті є стисле узагальнення міжнародного досвіду сучасних кадрових компетентностей сфери кібербезпеки та виокремлено їх складові за відповідними напрямками.

Виклад основного матеріалу. Сьогодні увага всього світу прикута до подій в Україні, не слід забувати, що активні кібер-дії з боку росії також відіграють важливу роль на реальному полі бою в сучасних умовах. Росія розгорнула та застосувала свій кібер-потенціал безпосередньо перед і на початку вторгнення 24 лютого 2022 року. Багато атак були спрямовані на критичну інфраструктуру України, щоб порушити її роботу. Оскільки росія зосереджена на руйнуванні критичної інфраструктури, можна з упевненістю сказати, що кібероперації використовуються і будуть використовуватися як спільні операції для підтримки кінетичних військових операцій у майбутньому.

Проведений аналіз засвідчив, що в цілому російські активні дії в кіберпросторі спрямовані на підрив військових операцій України, економічного та урядового секторів, отримання доступу до критичної інфраструктури та обмеження доступу громадськості до інформації.

Виходячи з цього, повноцінно можливо сказати, що російські кіберзлочинні угруповання не змогли завдати критичної шкоди інфраструктурі України на тривалий період часу. При цьому українській стороні вдалось зменшити нанесення шкоди своїй інформаційній інфраструктурі. Це було реалізовано шляхом перенесення кіберфізичних активів та окремих елементів власної інфраструктури на хмарні платформи. Щоразу, коли інфокомунікаційна інфраструктура України піддавалась черговій кібер-атаці, її руйнівний вплив ставав все менш деструктивним. Однак, якщо на ранніх етапах оперативної фази бойових дій пріоритетом була оборона державного сегменту кіберпростору в частині проведення кібер-операцій із захисту інформаційної інфраструктури, то зараз українська сторона зосереджується на наступальній стратегії.

Слід відмітити, що увага національної кібер-спільноти зосереджена на деталізації етіології таких атак як DDoS-атаки, фішинг, пропагандистські і дифамаційні операції та інше. Також необхідно звернути увагу на той факт, що досі росія намагається знайти нових союзників для підтримки своїх кібервійськових операцій, що може завдати ще більшої шкоди. Майже напевно, що російські державні суб'єкти кібер-впливу продовжуватимуть діяти для досягнення стратегічних і тактичних цілей російських військ, дислокованих в Україні. Російська кібер-активність, насамперед, зосереджена на українських цілях, але широкомасштабні атаки, ймовірно, відбуватимуться і в Європі, і в країнах, що підтримують Україну ще багато років уперед.

В цих умовах, відчуваючи потребу в досвідченому персоналі, національний сегмент вишів продовжує розбудову та провадження системи підготовки фахівців з кібербезпеки для потреб сил оборони та безпеки держави. Зазначена клопітка робота проваджується упродовж останніх п'яти – семи років на державному, галузевому та відомчому рівнях згідно з програмами фундаментальних і наукових робіт МО України, СБУ, ДССЗЗІ України та інших суб'єктів сил оборони в рамках науково-дослідних робіт, що виконувались (або виконуються) в НТУ України "Київський політехнічний інститут імені Ігоря Сікорського", Національному університеті оборони України імені Івана Черняховського, Військовому інституті телекомунікацій та інформатизації імені Героїв

Крут, Житомирському військовому інституті імені Сергія Павловича Корольова, Національній академії СБ України.

Паралельно з цим пріоритетними напрямками досліджень в цій галузі наук представниками як цивільного сектору, так і сектору оборони держави були пов'язані з:

1) алгоритмами підготовки та проведенням оцінки кібероперацій у мирний час, в умовах кризи та збройних конфліктів з метою ефективного захисту інфраструктури від гібридних загроз;

2) порядком оперування реальними загрозами для критичної інфраструктури цивільного та військового сектору;

3) обміну інформацією про інциденти кібербезпеки між суб'єктами сфери кібербезпеки;

4) виявлення, аналізу та прогнозування шляхів впровадження кіберзагроз тощо [21].

Попри вагомі фундаментальні напрацювання вітчизняних науковців за вказаним напрямом, все ще залишаються далекими від завершення наукові дослідження щодо формування фахових компетентностей та стандартизації процесу підготовки персоналу зі спеціальності 125 "Кібербезпека". Тому, враховуючи зазначене, було б вкрай важливим зосередити увагу та побудувати проведення досліджень щодо набуття компетенцій в зазначеній галузі відповідно до стандартів (рекомендацій) Національного інституту стандартів і технологій США (англ. *The National Institute of Standards and Technology, NIST*). Місія інституту – "просувати" інноваційну та індустріальну конкурентоспроможність США шляхом розвитку наук про виміри, стандартизацію та технології з метою підвищення економічної безпеки та покращення якості життя суспільства.

Національний інститут стандартів та технології (NIST), разом з Американським національним інститутом стандартів (ANSI) бере участь у розробці стандартів та специфікацій до програмних рішень, які використовуються як у державному секторі США, так і мають комерційне призначення [18].

За своєю топологією дані стандарти (сфери кібербезпеки) поділяються на:

1) Безпеку та конфіденційність, у складі: криптографія; ідентифікація та керування доступом; конфіденційність; управління ризиками; загрози; безпека та політика; вимірювання безпеки; програми безпеки та операції; техніка безпеки систем;

2) Цифрові технології, у складі: штучний інтелект; обробка великих даних; біометрія; блокчейн та DLT; хмара та віртуалізація; комбінаторне тестування; складність;

3) Додатки, у складі: зв'язок і бездротовий зв'язок; кіберфізичні системи; освіта з кібербезпеки, структура кібербезпеки; адміністратори з кібербезпеки; підприємства; криміналістика; промислові системи управління; інтернет-речі; позиціонування навігації та часу; малий і середній бізнес; дистанційна робота; голосування.

4) Закони та правила, у складі: виконавчі документи; закони; нормативні акти;

5) Діяльність і продукти, у складі: річні звіти; конференції та семінари; довідкові матеріали; розробка стандартів.

6) Сектори (галузі економіки), у складі: аерокосмічний; фінансові послуги; охорона здоров'я; гостинність; матеріальне виробництво; громадська безпека; роздрібна торгівля; телекомунікації; транспортування.

Таким чином, загалом впровадження NISTів забезпечує комплексний, гнучкий, повторюваний і вимірний багатоетапний процес, який будь-яка установа, організація (підприємство) може використовувати для побудови та управління власної системи ЗІ та кібербезпеки, проведення на постійній основі, циклу навчання власного персоналу з питань інформаційної безпеки та кібербезпеки [16].

А враховуючи те, що національні стандарти NIST спрямовані на вирішення проблем з захисту комунікаційних систем і телекомунікаційної інфраструктури, що мають загальнодержавне значення, то і можна стверджувати, що кожна установа чи організація має можливість використовувати нетрадиційні підходи до виконання заходів з безпеки які передбачені зазначеними стандартами [8].

Переходячи від теорії до практики, вбачається за потрібне розглянути найпотужніший і найпопулярніший у світі дистрибутив для тестування на проникнення – це Kali Linux. Даний дистрибутив доволі широко використовується професіоналами з безпеки. Він включає: тестування на проникнення, криміналістику, зворотне проектування та оцінку вразливості. Це кульмінація багаторічних удосконалень та результат безперервної еволюції від WHoppiX до WHAX, потім до BackTrack, а тепер до повноцінного дистрибутива тестування на проникнення. У Kali застосовується багато функцій Debian GNU/Linux і враховуються цінні поради членів динамічного світового співтовариства, що працює над спеціальним програмним забезпеченням (*далі – ПЗ*) з відкритим кодом.

Загалом за допомогою Kali Linux можна провести дослідження системи щодо здійснення оцінки вразливості, оцінки системи на відповідність стандартам безпеки, традиційне тестування на проникнення та здійснити оцінку додатків. В свою чергу кожна складова може включати різні елементи і свій алгоритм черговості та ступінь застосування. У цілому ж, зазначений дистрибутив дозволяє провести критичний аналіз цільового оточення, здійснити ручний пошук вразливостей креативно та нестандартно.

Незважаючи на складність та багатоплановість традиційного тестування на проникнення, хід такого дослідження можна впорядкувати, розбивши на кілька кроків. Варто зазначити, що Kali спрощує підбір програм для кожного з таких кроків за допомогою Kali Menu, а також зосереджує увагу саме на зборі інформації, виявленні вразливостей, експлуатації вразливостей, проникненні та вилучені даних, підготовці звітів. Серед додаткових налаштувань Kali Linux, що часто зустрічаються, можна відзначити наступні:

- попереднє встановлення ліцензованих комерційних пакетів;
- попередньо налаштовану віртуальну приватну мережу із зворотним з'єднанням (VPN);
- перед встановлення інструментів та програмного забезпечення власної розробки;
- попереднє налаштування конфігурації операційної системи, у тому числі відображення імен хостів на IP-адреси, шпалер робочого столу, налаштувань проксі-серверів [9] і т.д.

Все це – підходи до виявлення додаткових вразливостей, які потребують інших інструментів, здатних знайти уразливості там, де закінчуються можливості найпотужніших автоматичних сканері . Нерідко після завершення цього кроку весь процес починають знову для того, щоб забезпечити повне та якісне виконання роботи [14].

Більшість заходів щодо оцінки захищеності систем відрізняються досить великими обсягами. Особливістю ж досліджень додатків є той факт, що вивченню підлягає конкретна програма. Подібні перевірки стають все більш поширеними через складність життєвоважливих додатків, що використовуються фінансовими компаніями [6]. Багато з таких програм створено власними силами цих підприємств та установ. Якщо необхідно, то дослідження додатків може супроводжуватись іншими видами перевірок. Серед лінійки додатків, які можуть бути проаналізовані щодо безпеки, можна назвати такі.

Веб-додатки. Стандартні тести доволі часто дозволяють виявити базові проблеми веб-додатків. Однак більш детальне дослідження, хоч і може займати чимало часу, але при цьому дозволяє знайти приховані дефекти програм. Для проведення подібних випробувань можна скористатися пакетом kali-linux-web, який містить велику кількість корисних інструментів.

Прикладні та серверні додатки. Додатки для читання pdf-файлів або відео програм які використовують інтернет-ресурси. При цьому зловмисники постійно вдосконалюють свої засоби ураження зазначених додатків на теренах інтернету. Однак все ще є безліч прикладних додатків, в яких за правильного підходу можна знайти масу вразливостей.

Мобільні застосунки. Зі зростанням популярності мобільних пристроїв ці застосунки стають постійними предметами досліджень безпеки. Такі програми дуже швидко розвиваються і змінюються, тому в даній сфері методологія досліджень поки що не досягла достатньої зрілості, що веде до регулярної, практично щотижневої, появи нових методик. Інструменти, які стосуються вивчення мобільних додатків, можна знайти у розділі меню програм Kali Linux Reverse Engineering.

Дослідження додатків можна проводити різними способами. Наприклад, для ідентифікації потенційних загроз можна застосувати автоматичні засоби, призначені для тестування конкретної програми. Ґрунтуючись на особливостях роботи додатків, подібні засоби намагаються знайти у них невідомі слабкості, замість того щоб покладатись на набір заздалегідь заданих сигнатур [1]. Інструменти для аналізу програм повинні враховувати особливості їх тактики дій. Для прикладу, сканер уразливостей веб-додатків Burp Suite (https://portswigger.net/burp/) спочатку знаходить поля для введення даних, після чого застосовує різні атаки шляхом SQL-ін'єкцій, спостерігаючи в цей час за "поведінкою" додатка, з метою виявлення атак, які виявились успішними

Існують і складніші сценарії аналізу додатків. Такі перевірки можуть бути виконані в інтерактивному режимі. При їх проведенні використовують моделі "чорної і білої скриньки" [3].

Дослідження методом чорної скриньки: так інструмент (або дослідник) взаємодіє з додатком без будь-яких спеціальних знань про додаток або спеціальних прав доступу, відмінних від прав звичайного користувача. Наприклад, у випадку веб-додатків дослідники можуть отримати доступ лише до тих функцій і можливостей, які доступні користувачам, що не увійшли в систему. Будь-які облікові записи будуть такими ж, як і ті, в яких можуть зареєструватися звичайні користувачі. Це не дозволяє зловмиснику аналізувати функції, доступні лише привілейованим користувачам, облікові записи яких має створювати адміністратор.

Дослідження методом білої скриньки: в цьому варіанті інструмент (або дослідник) часто має повний доступ до вихідного коду програми, доступ адміністратора до платформи, на якій воно виконується тощо. Це гарантує виконання повного та ретельного аналізу всіх можливостей програми незалежно від того, де саме знаходиться функціональність, що досліджується. Недолік такого дослідження полягає в тому, що воно не є імітацією реальних дій зловмисника.

Звичайно, між білим та чорним є і відтінки сірого – комбінований спосіб. Зазвичай такий алгоритм дослідження роботи додатку буде проводиться в залежності від поставленої мети. Якщо вона полягає у визначені того, що може статися з додатком, який виявиться предметом цілеспрямованої зовнішньої атаки, то, ймовірно, найкраще підійде тестування методом чорної скриньки. Якщо ж мета полягає в ідентифікації та усуненні як найбільшої кількості проблем з безпекою, за порівняно короткий час, то дослідження методом білої скриньки здатне виявитися ефективнішим.

В інших випадках можна застосувати гібридний підхід, коли дослідник не має повного доступу до вихідного коду програми для платформи, на якій воно виконується, але виданий йому обліковий запис підготовлений адміністратором і відкриває доступ до максимально можливої кількості функцій програми. Kali – це ідеальна платформа для всіх підходів дослідження додатків. Після встановлення стандартного дистрибутива можна застосувати безліч сканерів, розрахованих на конкретні програми. Також Kali має інструменти для більш розвинених досліджень. Серед них – редактори вихідного коду та сценарні оточення.

Отже, сьогодні вищим військовим навчальним закладам (військовим навчальним підрозділам вищих навчальних закладів) та закладам вищої освіти, які здійснюють підготовку на певних рівнях вищої освіти підготовки курсантів (слухачів, студентів), ад'юнктів для подальшої служби на посадах офіцерського (сержантського, старшинського) або начальницького складу з метою задоволення потреб складових сил оборони та цивільного сектору необхідно скорегувати свою систему підготовки персоналу у сфері захисту інформації та кібербезпеки у відповідності до сучасних умов динамічного розвитку світової цифрової обізнаності.

Паралельно з попередньо розглянутим дистрибутивом Kali Linux та короткою методикою його практичного застосування на мій погляд доречно було б зупинитись ще на одному розгалуженому інструменті аналізу даних, а саме – OSCINT.

Зазначений інструмент є одним з вагомих інструментів аналізу даних відкритого мережевого трафіку. Сьогодні доступність до різних типів мережевих активів і користь від отриманих даних засобами розвідки на основі відкритих джерел залежать від району проведення операції, що розглядається та інших факторів, а саме – від рівня активності та динамічності ведення бойових дій, від цілей конфлікту сторін, від рівня бойового потенціалу та від району застосування засобів розвідки.

Загалом, OSCINT має доволі вагомий потенціал як джерело розвідки, є життєво важливим для командирів (начальників) всіх рівнів, експертів та користувачів і служить основою для "наповнення та розповсюдження бойового простору", а також відтворення єдиної Common Operating Picture [15].

Застосування OSCINT впроваджено на:

1) стратегічному рівні і спрямовано на:

- здійснення індикації та попередження про ворожі наміри та його спроможності;

- проведення культурної та демографічної розвідки, узагальнення та аналіз отриманих даних;

- надання несекретних даних про існуючі загрози, що використовуються під час проведення навчань, мобілізаційних заходів та логістичних потреб.

2) оперативному рівні і спрямовано на:

- регіональне узагальнення даних за напрямками (районами), виконання заходів планування на застосування на основі спроможностей видів (родів) військ (сил);

- оперативне вирішення питань, які виникнуть щодо використання цивільної інфраструктури (інженерні споруди, економічна інфраструктура, електронні комунікації та обчислювальні ресурси);

- координацію спільних дій в районах ведення бойових дій (бою) на принципах об'єднаного застосування.

3) тактичному рівні і спрямовано на:

- протидію тероризму, розповсюдженню негативних наративів серед місцевого населення, протидію "прямим діям" миротворчих операцій;

- формування цифрових карт та поточної географічної інформації з урахуванням розташування аеродромів, шляхів, дорожніх сполучень і мостів.

4) технічному рівні і спрямовано на:

- узагальнення даних про цивільні електронно-комунікаційні системи, технічні спроможності щодо обробки та передачі даних, мережевого обладнання, архітектуру та розгалуженість телекомунікаційної інфраструктури в цілому;

- залучення цивільної авіації, управління повітряним рухом, планування протиповітряної оборони з використанням цивільних платформ, заправку озброєння та військової техніки та інші логістичні заходи.

Зазначене вище розкриває лише загальну концепцію та ідею використання OSCINT, відтворює узагальнену картинку щодо застосування зазначених систем. У своїй роботі я хотів би звернути увагу на розкритті певних технічних спеціальних інструментів, а саме на спеціальне програмне забезпечення, яке може аналізувати відкриті дані мережевого трафіку.

На відміну від розвідувальних даних, отриманих з прихованих джерел, таких як Dumpster diving, Dump бази даних веб-сайтів та соціальна інженерія, розвідувальні дані OSCINT збираються з легальних джерел, таких як публічні документи та соціальні мережі. Хотілось наголосити, що найчастіше успіх пентесту часто залежить від результатів етапу збору інформації, тому далі пропонується розглянути кілька інструментів для отримання корисної інформації з відкритих джерел.

У відкритій мережі існує доволі велика кількість програмного забезпечення за даною спрямованістю. Але, на мій погляд пропонується розглянути лише декілька з них, а саме – *Netcraft.* Іноді інформація, яку веб-сервери та хостингові компанії збирають і роблять загальнодоступною, може багато чого розповісти про веб-сайт. Наприклад, компанія Netcraft реєструє час безвідмовної роботи і робить запити про програмне забезпечення, що лежить в основі веб-сайту. Netcraft також надає інші послуги, а їхні антифішингові пропозиції становлять особливий інтерес для КБ.

На рисунку 1 показано результат запиту http://www.netcraft.com/ для http://www.bulbsecurity.com. Як ви можете бачити, сайт bulbsecurity.com вперше з'явився в березні 2012 року. Він був зареєстрований через GoDaddy, має IP-адресу 50.63.212.1 і працює під управлінням Linux з веб-сервером Apache.

Site title	Bulb Security	**Date first seen**	March 2012
Site rank	186317	**Primary language**	English
Description	Bulb Security LLC was founded by Georgia Weidman, specializing in Information Security, Research and Training.		
Keywords	georgia weidman, bulb security, smartphone pentest framework, spf, DARPA Cyber Fast Track, metasploit training, security research, computer security training		

Network

Site	http://www.bulbsecurity.com	**Netblock Owner**	GoDaddy.com, LLC
Domain	bulbsecurity.com	**Nameserver**	ns65.domaincontrol.com
IP address	50.63.212.1	**DNS admin**	dns@jomax.net
IPv6 address	*Not Present*	**Reverse DNS**	p3nlhg344c1344.shr.prod.phx3.secureserver.net
Domain registrar	godaddy.com	**Nameserver organisation**	whois.wildwestdomains.com
Organisation	Domains By Proxy, LLC, Scottsdale, 85260, United States	**Hosting company**	GoDaddy Inc
Top Level Domain	Commercial entities (.com)	**DNS Security Extensions**	*unknown*
Hosting country	US		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
GoDaddy.com, LLC 14455 N Hayden Road Suite 226 Scottsdale AZ US 85260	50.63.212.1	Linux	Apache	1-Nov-2013
GoDaddy.com, LLC 14455 N Hayden Road Suite 226 Scottsdale AZ US 85260	50.63.202.81	-	Microsoft-IIS/7.5	22-Dec-2012
GoDaddy.com, LLC 14455 N Hayden Road Suite 226 Scottsdale AZ US 85260	50.63.212.1	-	Apache	18-Dec-2012

Рис. 1: Результати Netcraft для bulbsecurity.com
Fig. 1: Netcraft results for bulbsecurity.com
**Джерело: розробка автора.*

Озброївшись цією інформацією, можна почати тестування bulbsecurity.com з виключення уразливостей, які впливають лише на сервери Microsoft IIS. Або, з використанням соціальної інженерії, можна отримати облікові дані для входу на сайт, шляхом написання електронного листа від імені GoDaddy з проханням до адміністратора увійти в систему і перевірити деякі налаштування безпеки.

Пошук Whois. Усі реєстратори доменів зберігають записи про домени, які вони обслуговують. Ці записи містять інформацію про власника, включно з контактними даними. Наприклад, якщо ми запустимо інструмент командного рядка Whois на машині Kali Linux, щоб отримати інформацію про bulbsecurity.com, як показано в лістингу 1, то побачимо, що я використовував приватну реєстрацію, тому ми не дізнаємося багато нового.

Цей сайт має приватну реєстрацію, тому і реєстрант (1), і технічний контакт (2) є доменами за дорученням. Домени за проксі пропонують приватну реєстрацію, приховуючи ваші особисті дані в інформації Whois для доменів, якими ви володієте. Однак ми бачимо сервери домену (3) для bulbsecurity.com.

Запуск Whois-запитів для інших доменів покаже більш цікаві результати. Наприклад, якщо виконати пошук Whois для georgiaweidman.com, то можна отримати цікаву інформацію з минулого, включаючи номери телефонів.

```
root@kali:~# whois bulbsecurity.com
  Registered through: GoDaddy.com, LLC (http://www.godaddy.com)
   Domain Name: BULBSECURITY.COM
      Created on: 21-Dec-11
      Expires on: 21-Dec-12
      Last Updated on: 21-Dec-11

   Registrant: ❶
   Domains By Proxy, LLC
   DomainsByProxy.com
   14747 N Northsight Blvd Suite 111, PMB 309
   Scottsdale, Arizona 85260
   United States

  Technical Contact: ❷
     Private, Registration  BULBSECURITY.COM@domainsbyproxy.com
     Domains By Proxy, LLC
     DomainsByProxy.com
     14747 N Northsight Blvd Suite 111, PMB 309
     Scottsdale, Arizona 85260
     United States
     (480) 624-2599      Fax -- (480) 624-2598

  Domain servers in listed order:
     NS65.DOMAINCONTROL.COM ❸
     NS66.DOMAINCONTROL.COM
```

Рис. 2. Інформація Whois для bulbsecurity.com
Fig. 2. Whois information for bulbsecurity.com
**Джерело: розробка автора.*

Розпізнавання DNS. Також можна використовувати сервери системи доменних імен (DNS), щоб дізнатися більше про домен. Сервери DNS перетворюють людську URL адресу www.bulbsecurity.com в IP-адресу.

Nslookup. Використання інструменту командного рядка, Nslookup, наведено на рисунку 3.

```
root@Kali:~# nslookup www.bulbsecurity.com
Server:     75.75.75.75
Address:    75.75.75.75#53

Non-authoritative answer:
www.bulbsecurity.com    canonical name = bulbsecurity.com.
Name:    bulbsecurity.com
Address: 50.63.212.1 ❶
```

Рис. 3: Інформація про Nslookup для www.bulbsecurity.com
Fig. 3: Nslookup information for www.bulbsecurity.com
**Джерело: розробка автора.*

Як можна бачити на ❶ – Nslookup повернув IP-адресу www.bulbsecurity.com. Також за допомогою Nslookup можна знайти поштові сервери для цього ж веб-сайту, шукаючи MX-записи (DNS-записи електронної пошти) (рисунок 4).

```
root@kali:~# nslookup
> set type=mx
> bulbsecurity.com
Server:     75.75.75.75
Address:    75.75.75.75#53

Non-authoritative answer:
bulbsecurity.com    mail exchanger = 40 ASPMX2.GOOGLEMAIL.com.
bulbsecurity.com    mail exchanger = 20 ALT1.ASPMX.L.GOOGLE.com.
bulbsecurity.com    mail exchanger = 50 ASPMX3.GOOGLEMAIL.com.
bulbsecurity.com    mail exchanger = 30 ALT2.ASPMX.L.GOOGLE.com.
bulbsecurity.com    mail exchanger = 10 ASPMX.L.GOOGLE.com.
```

Рис. 4. Інформація Nslookup для поштових серверів bulbsecurity.com
Fig. 4. Nslookup information for bulbsecurity.com mail servers
**Джерело: розробка автора.*

Nslookup показує, що bulbsecurity.com використовує Google Mail для своїх поштових серверів, що є вірно, оскільки використовувався Google Apps.

Хост. Ще однією утилітою для DNS-запитів є Host. Наприклад, можна запитати Host про сервери імен для домену за допомогою команди «host -t ns domain». Також гарним прикладом для запитів до домену є zoneedit.com – це той домен, який був створений для демонстрації вразливостей передачі зон, як показано нижче. Цей результат показує нам всі DNS-сервери для zoneedit.com (рисунок 5).

```
root@kali:~# host -t ns zoneedit.com
zoneedit.com name server ns4.zoneedit.com.
zoneedit.com name server ns3.zoneedit.com.
--snip--
```

Рис. 5. Стисло зведений результат, який представляє DNS-сервери для zoneedit.com
Fig. 5. Brief summary of the result representing the DNS servers for zoneedit.com
**Джерело: розробка автора.*

Переміщення між зонами. Перенесення зон DNS дозволяє серверам імен реплікувати всі записи про домен. На жаль, багато системних адміністраторів налаштовують передачу DNS-зони ненадійно, тому будь-хто може передати записи DNS для конкретного домену. Існуючі сторінки DNS-записів дають чітке уявлення про те, з чого необхідно почати пошук уразливостей.

Пошук адрес електронної пошти. Зовнішні тести на проникнення часто виявляють менше вразливих сервісів, ніж внутрішні. Належна практика безпеки полягає в тому, щоб відкривати лише ті сервіси, до яких необхідно отримати віддалений доступ, наприклад, веб-сервери, поштові сервери, VPN-сервери, а також SSH або FTP. Такі сервіси є поширеними об'єктами атак, і якщо персонал не використовує двофакторну автентифікацію, то доступ до веб-пошти установи може бути простим. Для цього можна скористатися інструментом Python під назвою theHarvester, щоб швидко переглянути тисячі результатів пошукових систем у моніторингу можливих адрес електронної пошти. Інструмент theHarvester може автоматизувати пошук адрес електронної пошти в Google, Bing, PGP, LinkedIn та інших сервісах.

Maltego. Це інструмент для аналізу даних, призначений для візуалізації збору розвідувальної інформації з відкритих джерел. Maltego використовує інформацію, яка є загальнодоступною в Інтернеті, тому цілком законно проводити розвідку будь-якого суб'єкта.

Запустивши інтерфейс Maltego→права, кнопка миші на іконці домену→запуск трансформації (рисунок 2), можна провести дослідження визначених інтернет-слідів.

Сканування портів. Отримати гарне уявлення про мережеву поверхню атаки, можна склавши карту діапазону мережі та здійснивши пошук портів для прослуховування. Також зазначене можна зробити вручну підключившись до портів за допомогою таких інструментів, як Telnet, Netcat або Nmap.

Синхронне сканування, сканування версій, сканування UDP, сканування певного порту, все це можливо зробити за допомогою SYN-сканування, а саме SYN – SYN-ACK – ACK. Необхідно відмітити, що в цілому зазначене сканування відбувається комплексно, у поєднані з вже вище зазначеним ПЗ.

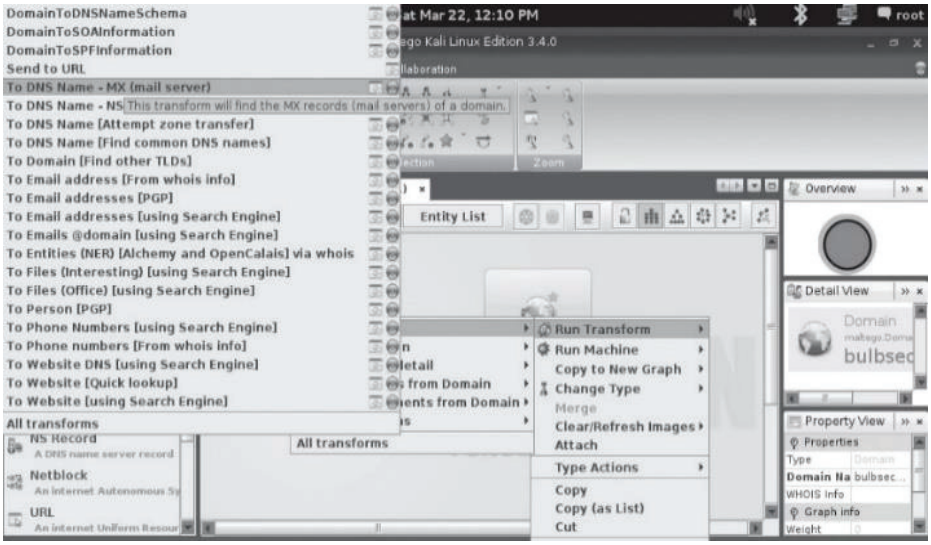

Рис. 6. Трансформації Maltego
Fig. 6. Maltego transformations
**Джерело: розробка автора.*

Реалізація такого комплексного підходу дозволяє повноцінно відтворити реальний стан технічних параметрів, порівняти отриману детальну інформацію, здійснити пошук потенційних вразливостей у подальшому та отримати звіт з результатами сканування (його запис).

Як підсумок необхідно зазначити що OSCINT завжди був частиною процесу національної та військової розвідки. При цьому в останні десятиліття підвищений акцент до технічних систем і систем ЗІ мав тенденцію до різкого зменшення обсягу фінансування та чисельності залученого до цієї сфери діяльності персоналу, зайнятого збиранням та обробкою загальнодоступної інформації. Отже, на жаль реальність сьогодні така, що більшість розвідувальних служб підготовлені, оснащені і організовані для збору і обробки секретної інформації [4]. За цих умов деякі уряди недооцінюють можливості OSCINT

як у цивільному, так і у військовому секторах. Водночас технічний розвиток ІТ-галузі та різного роду "інформаційні революції" різко підвищили як якість, так і кількість інформації що стала доступна в державному секторі.

Висновки і перспективи подальших досліджень. Перш за все, слід зазначити, що основним акцентом при формуванні Cybercom країн-партнерів є належне фінансування, ретельний підбір кадрів, якісна професійна підготовка та забезпечення повної взаємосумісності різнорідних структурних підрозділів суб'єктів забезпечення захисту інформації та кібербезпеки на державному рівні.

По-друге, питома вага кіберзагроз зростає, і ця тенденція буде посилюватися протягом наступного десятиліття, оскільки сфера інтернет-технологій розвивається стрімко, а самі цифрові рішення використовуються компбіновано (напр., штучний інтелект і блокчейн). Наприклад, нинішня росія є однією з головних загроз національній та міжнародній кібербезпеці яка активно реалізує концепцію інформаційного протистояння, що базується на поєднанні деструктивних дій у кіберпросторі.

По-третє, очікується зростання конфліктів між державами та інтенсивність розвідувально-підривної діяльності в кіберпросторі. Зростає коло держав, які прагнуть сформувати власну кібер-розвідку, оволодіти новітніми методами деструктивного впливу в кіберпросторі та посилити державний контроль над державним сегментом Інтернету.

По-четверте, технічний рівень кіберзагроз зростає, а нові інструменти та механізми кібератак постійно вдосконалюються та розробляються. Зростає тенденція до використання кібератак як інструменту для проведення спеціалізованих інформаційних операцій, так і маніпулювання громадською думкою та впливу на виборчі процеси.

По-п'яте, тверезе розуміння того, що вкрай необхідно запровадити та забезпечити об'єднаний підхід до побудови освітнього процесу за спеціальністю 125 "Кібербезпека" для цивільного та військового сектору в подальшому дозволить в повній мірі використовувати єдині системи електронних комунікацій, на основі захищеного інформаційного середовища, одночасно поєднуючи і синхронізуючи застосування сучасних систем управління, обміну інформацією (розвідки), засобів ураження та нелетального впливу (радіоелектронного, інформаційного впливу, дій у кіберпросторі тощо), підвищить спроможності об'єднаних сил під час їх застосування.

Перспективи подальших досліджень пов'язуються з тим, що, як наслідок вище переліченого, це у подальшому дозволить більш ефективно визначити показники оцінювання спроможностей військ зв'язку та кібербезпеки Збройних Сил України із виконання завдань відбиття воєнної агресії в кіберпросторі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Доктрина "Зв'язок та інформаційні системи" Центральне управління зв'язку та інформаційних систем Генерального штабу Збройних Сил України, ВКП 6-00(01).01, червень 2020

2. Дунаєв І. В., Коваленко М. М. Нові траєкторії регулювання інформаційних платформ і платформної економіки заради суспільного блага. *Актуальні проблеми державного управління.* 2022. № 2 (61). С. 6–24. DOI: https://doi.org/10.26565/1684-8489-2022-2-01

3. Живило Є. О., Орлов О. В. Сутність кібербезпеки національного сегменту кіберпростору держави в умовах кризового управління : збірник наукових матеріалів XXII Міжнар. наукового конгресу "Публічне управління XXI століття в умовах гібридних загроз" 27 квітня 2022 р. Харків : ХНУ імені В.Н. Каразіна, 2022. С. 248–254

4. Живило Є. О. Об'єднана підготовка персоналу складових Сил оборони сфери кібербезпеки в умовах тотальної оборони держави. *Теорія та практика державного управління*. № 2 (73). С. 144–153. DOI: https://doi.org/10.34213/tp.21.02.16

5. Живило Є. О., Черноног О. О. Міжнародні кібертренування Locked Shields–2022: проблемні питання в підготовці складових сил оборони та безпеки України. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2022. № 1 (43). С. 19–24. DOI: https://doi.org/10.33099/2311-7249/2022-43-1-19-24

6. Загрози критичній інфраструктурі та їх вплив на стан національної безпеки (моніторинг реалізації Стратегії національної безпеки) : Аналітична записка Національного інституту стратегічних досліджень. Березень 2017 р. URL: http://old.niss.gov.ua/content/articles/files/KI_-Ivanyuta-3a331.pdf

7. Кудь А. А. Децентралізовані інформаційні платформи як інструмент модернізації публічного управління. *Вісник післядипломної освіти: Серія «Управління та адміністрування»*. 2021. № 1. Вип. 15(44). С. 233–274. DOI: https://doi.org/10.32405/2522-9931-2021-15(44)-233-274.

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

9. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про Стратегічний оборонний бюлетень України : Указ Президента України № 473/2021 від 17 вересня 2021 року. URI: https://www.president.gov.ua/documents/4732021-40121

10. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" : Указ Президента України № 96/2016р. (у ред. від 28 серпня 2021 року). URL: https://www.rnbo.gov.ua/ua/Ukazy/417.html

11. Craig A., Johnson R., Gallop M. Building cybersecurity capacity: a framework of analysis for national cybersecurity strategies. *Journal of Cyber Policy*. 2022. № 7/3. С. 375–398. DOI: https://doi.org/10.1080/23738871.2023.2178318

12. Creese S., Dutton W., Esteve-González P., Shillair R. Cybersecurity capacity-building: cross-national benefits and international divides. *Journal of Cyber Policy*. 2021. № 6/2. С. 214–235. DOI: https://doi.org/10.1080/23738871.2021.1979617

13. D'Elia D. Industrial policy: the holy grail of French cybersecurity strategy? *Journal of Cyber Policy*. 2018. № 3/3. С. 385–406. DOI: https://doi.org/10.1080/23738871.2018.1553988

14. Koval M., Sova O., Orlov O., Zhyvylo Y., Zhyvylo I. Improvement of complex resource management of special-purpose communication systems. *Eastern-European Journal of Enterprise Technologies*. 2022. № 5 (9-119). P. 34–44.

15. NATO OSINT Reader. Oslo, 2002. URL: https://cyberwar.nl/d/NATO%20OSINT%20Reader%20FINAL%20Oct2002.pdf

16. 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. Vol. 5 (13 (125). P. 65–76. URL: https://journals.uran.ua/eejet/article/view/288175/283817 DOI: https://doi.org/10.15587/1729-4061.2023.288175

17. Siudak R. (2022) Cybersecurity discourses and their policy implications. *Journal of Cyber Policy*. 2022. №7/3. С. 318–335, DOI: https://doi.org/10.1080/23738871.2023.2167607

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

19. Tijerina W. (2022) Industrial policy and governments' cybersecurity capacity: a tale of two developments? *Journal of Cyber Policy*. 2022. № 7/2. С. 194–212. DOI: https://doi.org/10.1080/23738871.2022.2071747

20. Timmers P. (2018) The European Union's cybersecurity industrial policy. *Journal of Cyber Policy*. 2018. № 3/3. С. 363–384. DOI: https://doi.org/10.1080/23738871.2018.1562560

21. 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). С. 144–153. DOI: https://doi.org/10.34213/tp.21.02.16

Стаття надійшла до редакції 10.09.2023 р.

Стаття рекомендована до друку 22.10.2023 р.

Zhyvylo Y. O.,
Doctor of Sciences in Public Administrfnion,
Full Professor of the Department of Public Policy,
Education and Research Institute of Public Administration, V. N. Karazin Kharkiv National University,
4, Svobody Sq., Kharkiv, 61022, Ukraine
e-mail: zhivilka@i.ua https://orcid.org/0000-0003-4077-7853

EXPLORING AND ACQUIRING MODERN HUMAN RESOURCE COMPETENCIES IN CYBERSECURITY AMIDST STATE DIGITAL TRANSFORMATION

Annotation. This paper validates the relevance of contemporary electronic communication systems, networks, and hardware and software suites and tools being particularly susceptible to cyber influences. The goal of the article is to concisely summarize international experience in modern human resource competencies within the cybersecurity domain and to identify their components according to specific directions.

The paper examines current international trends regarding the formation of a minimal necessary package for creating, implementing, technical support, and enhancing an information security and cyber defense management system. This necessitates the development of a digitally aware society by the state, a crucial area of its internal policy. It emphasizes the undeniable fact that the demand for cybersecurity professionals will continually grow as high-technology society advances. In the context of the state's total defense, the role of unified training for defense force personnel and the civilian sector in cybersecurity is beyond doubt.

It is concluded that the main focus in forming Cybercom of partner countries is adequate funding, careful selection of personnel, quality professional training, and ensuring full interoperability of diverse structural units of subjects ensuring information protection and cybersecurity at the state level. The share of cyber threats is increasing, and this trend will intensify over the next decade as the internet technology sphere is developing rapidly, and digital solutions are being used in combination (e.g., artificial intelligence and blockchain). For instance, current Russia is one of the main threats to national and international cybersecurity, actively implementing the concept of information confrontation based on a combination of destructive actions in cyberspace. An increase in conflicts between states and the intensity of intelligence and subversive activities in cyberspace is expected. The number of states seeking to form their own cyber-intelligence, master the latest methods of destructive influence in cyberspace, and strengthen state control over the state segment of the Internet is growing. The technical level of cyber threats is increasing, and new tools and mechanisms for cyber attacks are constantly being improved and developed.

Keywords: digital technologies, information protection system, cybersecurity, information technologies, information security, national security, cyber influence.

REFERENCES

1. Doctrine "Communication and Information Systems" Central Management of Communication and Information Systems of the General Staff of the Armed Forces of Ukraine, VKP 6-00(01).01, June 2020 [in Ukrainian].

2. Dunayev, I.V., & Kovalenko, M.M. (2022). New traces of regulating information platforms and platform economy for the public good. *Actual Problems of State Administration, no. 2 (61), 6–24*. DOI: https://doi.org/10.26565/1684-8489-2022-2-01 [in Ukrainian].

3. Zhyvylo, Ye.O., & Orlov, O.V. (2022). The essence of cybersecurity of the national segment of the state's cyberspace in crisis management conditions. Proceedings of the XXII International Scientific Congress "Public Administration of the XXI Century in the Conditions of Hybrid Threats" on April 27, 2022. Kyiv: KhNU named after V.N. Karazin, 248–254 [in Ukrainian].

4. Zhyvylo, Ye.O. (2021). Joint training of personnel of the components of the defense forces in the field of cybersecurity in the conditions of total defense of the state. *Theory and Practice of Public Administration, no.2 (73), 144–153.* DOI: https://doi.org/10.34213/tp.21.02.16 [in Ukrainian].

5. Zhyvylo, Ye.O., & Chernonog, O.O. (2022). International cyber exercises Locked Shields–2022: problematic issues in the preparation of the components of the defense and security forces of Ukraine. *Modern Information Technologies in the Sphere of Security and Defense, no. 1 (43), 19–24*. DOI: https://doi.org/10.33099/2311-7249/2022-43-1-19-24 [in Ukrainian].

6. Threats to critical infrastructure and their impact on the state of national security (monitoring the implementation of the National Security Strategy): Analytical note of the National Institute for

Strategic Studies. March 2017: URL: http://old.niss.gov.ua/content/articles/files/KI_-Ivanyuta-3a331.pdf [in Ukrainian].

7. Kud, A.A. (2021). Decentralized information platforms as a tool for modernizing public administration. *Herald of Postgraduate Education: Series "Management and Administration", no. 1, vol. 15(44), 233–274*. DOI: https://doi.org/10.32405/2522-9931-2021-15(44)-233-274 [in Ukrainian].

8. On approval of the Procedure for conducting an overview of the state of cyber protection of critical information infrastructure, state information resources and information, the requirement for the protection of which is established by law: Resolution of the Cabinet of Ministers of Ukraine of November 11, 2020. No. 1176. URL: https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#Text [in Ukrainian].

9. On the decision of the National Security and Defense Council of Ukraine of August 20, 2021 "On the Strategic Defense Bulletin of Ukraine": Decree of the President of Ukraine No.473/2021 of September 17, 2021. URL: https://www.president.gov.ua/documents/4732021-40121 [in Ukrainian].

10. On the decision of the National Security and Defense Council of Ukraine of January 27, 2016 "On the Cybersecurity Strategy of Ukraine": Decree of the President of Ukraine No. 96/2016r. (as amended on August 28, 2021). URL: https://www.rnbo.gov.ua/ua/Ukazy/417.html [in Ukrainian].

11. Craig, A., Johnson, R., & Gallop, M. (2022). Building cybersecurity capacity: a framework of analysis for national cybersecurity strategies. *Journal of Cyber Policy, 7(3), 375–398*. DOI: https://doi.org/10.1080/23738871.2023.2178318

12. Creese, S., Dutton, W., Esteve-González, P., & Shillair, R. (2021). Cybersecurity capacity-building: cross-national benefits and international divides. *Journal of Cyber Policy, 6 (2), 214–235*. DOI: https://doi.org/10.1080/23738871.2021.1979617

13. D'Elia, D. (2018). Industrial policy: the holy grail of French cybersecurity strategy? *Journal of Cyber Policy, 3(3), 385–406.* DOI: https://doi.org/10.1080/23738871.2018.1553988

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

15. NATO OSINT Reader. Oslo, 2002. URL: https://cyberwar.nl/d/NATO%20OSINT%20Reader%20FINAL%20Oct2002.pdf

16. 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.* URL: https://journals.uran.ua/eejet/article/view/288175/283817 DOI: https://doi.org/10.15587/1729-4061.2023.288175

17. Siudak, R. (2022). Cybersecurity discourses and their policy implications. *Journal of Cyber Policy, 7(3), 318–335.* DOI: https://doi.org/10.1080/23738871.2023.2167607

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

19. Tijerina, W. (2022). Industrial policy and governments' cybersecurity capacity: a tale of two developments?. *Journal of Cyber Policy, 7(2), 194–212*. DOI: https://doi.org/10.1080/23738871.2022.2071747

20. Timmers, P. (2018). The European Union's cybersecurity industrial policy. *Journal of Cyber Policy, 3(3), 363–384.* DOI: https://doi.org/10.1080/23738871.2018.1562560

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

The article was received by the editors 10.09.2023.
The article is recommended for printing 22.10.2023.