DOI:**10.33099/2311-7249/2022-43-1-19-24**

УДК: 351.865

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

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

МІЖНАРОДНІ КІБЕРНАВЧАННЯ LOCKED SHIELDS – 2022. ПРОБЛЕМНІ ПИТАННЯ В ПІДГОТОВЦІ СКЛАДОВИХ СИЛ ОБОРОНИ ТА БЕЗПЕКИ УКРАЇНИ

В сучасних умовах для України забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки. За цих умов вага кіберзагроз зростає і ця тенденція в міру розвитку інформаційних технологій та їх споріднення з технологіями штучного інтелекту в найближче десятиліття посилюватиметься. Збільшення такого впливу на функціонування структур управління як національних, так і транснаціональних вимагає до формування нового безпекового формату. Між світовими центрами сили відбувається поділ сфер впливу у кіберпросторі, посилюється їх прагнення за рахунок такого поділу забезпечити реалізацію власних геополітичних інтересів.

Рівень виклику у національному сегменті кіберпростору країн-світу в цілому з кожним роком зростає як за розміром, так і за рівнем складності. Складовим сил оборони та безпеки України вкрай необхідні досвідчені експерти з хорошими навичками в тестуванні на проникнення, передачі, обміні інформацією та ситуаційною обізнаністю. При цьому важливим є досвід представників, як цивільного сектору, так і сектору оборони держави які залучались до проведення міжнародних кібернавчань у складі команди.

В цій ситуації, в рамках міжнародного співробітництва, українським експертам з кібербезпеки задля досягнення оперативної сумісності є вкрай важливим спрямувати свої практичні навички щодо захисту національних ІТ-систем та критичної інфраструктури від атак у реальному часі.

Так, покращення навичок національних кібергруп швидкого реагування потрібно зосередити на: обміні інформацією про кібератаки та кіберінциденти, проведенні спільних кібероперацій та розслідуваннях міжнародних кіберзлочинів, регулярних спільних кібернавчаннях та тренінгах, обміні досвідом та найкращими практиками із відповідними підрозділами держав – членів НАТО.

Практична спрямованість у тісній співпраці представників експертних груп у сфері кіберзахисту на одній платформі в режимі реального часу – це унікальна можливість для національних кіберзахисників практикувати захист національних ІТ-систем та критичної інфраструктури під тиском серйозної кібератаки.

Ключові слова*: цифрове суспільство, інформаційно-комунікаційні технології, кіберконфлікт, кіберзагрози, кібербезпека, кіберпростір, система підготовки фахівців у сфері кібербезпеки.*

Вступ

Підтримка міжнародно визнаних норм у кіберпросторі має важливе значення для захисту та розвитку обізнаного в цифровому відношенні суспільства. Колективний захист кіберпростору є основою захисту національного сегменту кіберпростору кожної розвинутої держави. Таким чином, однією з головних цілей навчань Locked Shields (LS) є розвиток міжнародного співробітництва у сфері кібербезпеки, шляхом вироблення спільних підходів у протидії кіберзагрозам, недопущення використання кіберпростору в терористичних, воєнних та інших протиправних діях.

Постановка проблеми. Сьогодні незважаючи на досить вагомі фундаментальні напрацювання щодо підготовки фахівців з організації та експлуатації засобів кібербезпеки (кіберрозвідки, кіберзахисту, кібероборони); формування фахових компетентностей та стандартизації процесу підготовки фахівців зі спеціальності 125 “Кібербезпека” складових сил оборони [2]; порядку підготовки органів управління (штабів), військових частин (підрозділів) у взаємодії (під керівництвом) з іноземними тренувальними місіями на території України та країнами-партнерами практична складова українських фахівців все ще потребує підвищеної уваги [6].

Тому, враховуючи те, що метою LS є залучення до навчань досвідчених експертів, з переконливими практичними навичками для української сторони постає доволі суттєва проблема, щодо підбору кваліфікованих

спеціалістів, а наукове супроводження з підготовки фахівців у цій сфері залишаються далекими від завершення.

Аналіз останніх досліджень і публікацій. З початком проведення Locked Shields у 2010 році і по теперішній час проведенням досліджень "дилем" які виникали в ході проведення зазначених навчань доволі змістовно та потужно переймались за своїми напрямками дослідники від CCDCOE. Мова йде про таких дослідників, як Майкл Деніел та Джошуа Кенуя (щодо обміну інформацією, розвідувальними даними та порядком реагування на виникаючі кібервпливи між країнами - НАТО та спільнотою зацікавлених сторін, експертами та групами осіб); Шон Абрахам та Саллі Долтрі (щодо національних нормативно-правових протиріч в контексті здійснення обміну інформацією на транснаціональному рівні, при цьому зазначені дослідники пропонують і шляхи вирішення даної проблематики з внесенням ряду пропозицій та змін до відповідних міжнародних організаційних структур та нормативно правових керівних документів); Луїса А. ДаСілви, Джеффрі Х. Ріда, Сачіна Шетті, Джеррі Парка, Думінди Вій Секери та Хайнінг Ванга (щодо реалізації ряду заходів НАТО та її партнерами по безпечному використанню технологій 5G, включаючи форми управління ризиками, стандартизацію та сертифікацію, які максимізуватимуть військові та соціальні переваги цього нового покоління мобільних систем); Симона Р. Соаре та Джо Бартон (щодо вивчення взаємозв'язків між місцевою та наднаціональною безпекою в умовах високих технологій); Якопо Белласіо та Ерік Сільфверстен (по визначенню низки нових технологій, які можуть формувати майбутній ландшафт кіберзагроз, також запропоновано шляхи, за допомогою яких НАТО може підготуватися та адаптуватися до цих загроз); Джеймс Блек і Еліс Лінч (змістовно охарактеризували наслідки мережевих залежностей що стосуються багатодоменних операцій і змоделювали варіанти використання цих залежностей противником, обґрунтовано оцінили корреляцію зовнішніх загроз і внутрішніх вразливостей для боротьби з кіберзагрозами на багатодоменному рівні); Франц-Штефан Гаді та Олександр Стронелл (в проведенні порівняльного аналізу щодо інтеграції кіберспроможностей союзників по НАТО в багатодоменні операції та запропонували порядок набуття цих спроможностей НАТО на тлі майбутніх високоінтенсивних конфліктів в кіберпросторі); Джо Черавіч і Біляна Ліллі (здійснили аналіз розгалуженості інформаційно-телекомунікаційних, інформаційних і телекомунікаційних мереж потенційних противників, дослідили "кіберпропускні" спроможності цих систем, розглянули причини та технологічні обмеження цих систем, запропонували алгоритм використання цих обмежень для власних заходів з кібербезпеки); Мартін К. Лібіцкі та Олеся Ткачова запропонували новий формат ведення кіберконфлікту, проаналізовано можливості горизонтальної ескалації в інші сфери та вертикальну ескалацію всередині домену, а також наслідки на управління ризиками [5].

Визначне теоретико-методологічне обґрунтування з питань кібербезпеки в рамках LS доволі якісно та змістовно дослідили такі досвідчені експерти як: Андреас Хаггманробить, Сінді Вонг, Лорін Б. Вайсінгер. Їх методологічний внесок у дискусію НАТО з питань кібербезпеки був спрямований на інструменти уявлення та передбачення конфліктного майбутнього в їх різноманітних соціальних, політичних і технічних вимірах в цілому, при цьому основну увагу було зосереджено на тому, як слід активізувати режими експертного контролю, щоб задовольнити проблеми кібербезпеки, покращенні розуміння складності мережі, в тому числі шляхом моделювання загроз і атак, щоб забезпечити більш ефективні та індивідуальні рішення щодо кібербезпеки.

Слід зазначити, що в цілому погляди представників, як цивільного сектору, так і сектору оборони держав-партнерів були спрямовані на виклики пов'язані з новими руйнівними технологіями в кіберсфері протягом наступного десятиліття, постійно розглядаються концептуальні та практичні взаємозв'язки між місцевою та наднаціональною безпекою в умовах високих технологій.

Мета статті полягає у формуванні сучасних компетентностей з питань кібербезпеки в межах об'єднаної підготовки складових сил оборони, необхідних для пошуку та засвоєння нових знань, набуття нових вмінь та навичок, а також здатності застосовувати їх на практиці фахівцями-випускниками вищих військових навчальних закладів та навчальних підрозділів закладів вищої освіти.

Виклад основного матеріалу дослідження

Міністерство оборони України підтверджує зацікавленість України у приєднанні до роботи Об'єднаного центру передових технологій з кібероборони НАТО (CCDCOE). Це питання має ключове значення для національної безпеки і оборони України як важлива складова стратегічного курсу набуття повноправного членства України в НАТО [1].

CCDCOE – це акредитований НАТО центр кіберзахисту, діяльність якого зосереджується на проведенні досліджень, навчанні та навчаннях. Він представляє спільноту країн НАТО та партнерів Альянсу, які надають 360-градусний погляд на кіберзахист, з досвідом у сферах технологій, стратегії, операцій та права [7].

Наразі, доволі гостро постає питання щодо залучення спеціалістів із кіберзахисту від української сторони до найбільших і найскладніших міжнародних навчань з

кіберзахисту LS які будуть проведені в 2022 році.

За цих умов організатори навчань наполегливо пропонують країнам сформувати навіть у більшій кількості спільні команди для навчання, щоб максимізувати зусилля в навчанні. Оскільки однією з основних цілей навчань є підтримка та розвиток подальших зусиль НАТО щодо колективної оборони, то організатори наполегливо працюють над тим, щоб створити більше технічних залежностей та проблем між умовними противниками (командами).

Для української сторони ще невідомі концепція, склад та порядок (алгоритми) дій основних кібер угрупувань в кіберпросторі (військові, терористичні, хакерські та інші). Точна концепція та цілі LS22 будуть визначені в процесі планування.

Однак відомо, що основні елементи та складові будуть схожими на попередні навчання Locked Shields, противенство Blue/Red Team CDX з компонентом вправ на рівні стратегії. У "технічних Blue Teams" використовується ігровий підхід. Це означає, що учасники не будуть виконувати свої реальні життєві ролі, а представлятимуть умовні ролі. Дії навчаємих відбуваються у кіберпросторі. Виробничі мережі не використовуються. Місія захисників полягає в тому, щоб зрозуміти та оцінити ситуацію, підтримувати доступність, конфіденційність та цілісність послуг у попередньо створеній мережі, яка підпала під кібератаки. Сині команди матимуть короткий час на ознайомлення, але загалом вони відпрацьовують свої завдання у невідомому їм середовищі.

При цьому, щоб забезпечити зворотній зв'язок з командами та оцінити успіх різних запроваджених стратегій і тактик, технічним Blue Teams будуть виставлятись оцінки в автоматичному та ручному режимі.

Щоб підвищити рівень обізнаності та компетенції на всіх рівнях, до навчань буде включено юридичні аспекти, медіа та стратегічні проблеми, а також вправу з прийняття стратегічних рішень.

Locked Shields – це практична робота "червоної команди проти синьої команди", де остання формуються країнами-членами та партнерами CCDCOE, Представники синьої команди, відіграють роль національних груп швидкого реагування в кіберпросторі, які розгорнуті для допомоги умовній країні в боротьбі з великомасштабними кіберінцидентами та всіма їх різноманітними наслідками. Вперше проведення цих навчань було започатковано в 2010році.

Аналізуючи формат проведення Locked Shields 2021, можливо припустити, що увагу навчаємих буде зосереджено на відпрацюванні практичних заходах пов'язаних з захистом складних ІТ-мереж у разі масштабної кібератаки. Організатори об'єднували як технічні, так і стратегічні ігри, дозволяючи країнам-учасникам відпрацювати весь ланцюг управління у разі серйозного кіберінциденту. Це включає прийняття рішень на стратегічному та оперативному рівні, а також захист цивільної та військової інфраструктури та потенціалу.

В LS 2021 команди ефективно та своєчасно виявляли та реагували на кіберінциденти, приймали стратегічні рішення та вирішували криміналістичні, юридичні та медійні проблеми.

Новизною навчань LS 2021 було те, що модератори вперше залучили нові кіберфізичні системи та інтегровані технічні та стратегічні елементи, що дозволили країнам-учасникам відпрацювати весь цикл управління з планування та реагування на великомасштабний кіберінцидент. Навчання розглядали захист життєво важливих послуг та критичної інфраструктури, які є основоположними для функціонування сучасного суспільства. Сюди входила критична інформаційна інфраструктура, енерго- та водопостачання, а також системи національної оборони, які представляли кілька нових систем із розширеними можливостями. Наприклад, уперше до навчання залучали супутникову систему управління місією, необхідну для забезпечення ситуаційної поінформованості в режимі реального часу для сприяння прийняттю військових рішень [4].

Було підкреслено кіберзалежність сектору фінансових послуг. У навчаннях було досліджено, як розвиваються технології, такі як дипфейки, їх вплив на майбутні конфлікти. Сценарій також вивчав нові реалії, запроваджені пандемією COVID-19, такі як більша вразливість у безпеці, яку запроваджують дистанційна робота та автоматизація. Загалом, навчання з прийняття стратегічних рішень дозволили керівникам вищого рівня відпрацювати процес координації та прийняття рішень, необхідний для вирішення великої кіберподії як всередині країни, так і за допомогою міжнародних партнерів.

Передбачається Locked Shields 2022 провести на реалістичних сценаріях і передових технологіях, відповідних мережах і методах атаки. Додатково заплановано розгорнути понад 5000 віртуалізованих систем, включаючи реалістичні копії критичної національної інфраструктури.

Враховуючи такий формат проведення навчань українським фахівцям було б варто оволодіти певними практичними здібностями, щодо нейтралізації кіберзагроз в паливно-енергетичній та енергетичній сферах України [9].

LS 2022 планується провести у співпраці з Агентством зв'язку та інформації НАТО, Міністерством оборони Естонії, Силами оборони Естонії, Siemens, Ericsson, TalTech, Foundation CR14, Bittium, Clarified Security, Arctic Security, Cisco, Stamus Networks, SpaceIT , Sentinel, Центром обміну та аналізу інформації фінансових служб (FS-ISAC), підрозділами оборонних інновацій США, Microsoft, Atech, Avibras, SUTD iTrust Singapore, Європейським центром передового досвіду протидії гібридним загрозам,

Центром передового досвіду стратегічних комунікацій НАТО, Європейським Агентством оборони, Space ISAC, Федеральним бюром розслідувань США, STM, VTT Technical Research Center of Finland Ltd, мережами НАТО M&S COE та PaloAlto [4].

З кожним роком в CCDCOE рівень вимог до фахівців країн-учасників залучаємих до навчань зростає (як за розміром, так і за рівнем складності), і лише досвідчені експерти з навичками нападу, тестуванні на проникнення обираються для приєднання до спільних команд.

Основною проблемою, що стосується української команди в контексті LS, полягає в тому щоб зібрати велику кваліфіковану команду, при цьому мати відповідні спроможності справлятися з виникаючими раптовими змінами у обстановці під час виконання спільних процедур реагування.

Отже, на думку авторів військові фахівці (фахівців у сфері кібербезпеки цивільного сектору), з організації та експлуатації засобів кібербезпеки (кіберрозвідки, кіберзахисту, кібероборони) повинні мати знання та практичний досвід у таких областях:

Адміністрування системи та мережі:

архітектура мережі TCP/IP:

- призначення мережевих протоколів, послуг і технологій, таких як DNS, NTP, DHCP, HTTP, HTTPS, SMTP, POP3, IMAP, SSH, FTP, VoIP;

- базові знання про IPv6;

порядок адміністрування та захист систем на базі Windows і Linux (як приклад: домен Windows і Active Directory; робочі станції та сервери на базі різних версій Windows; сервери Linux, що працюють на дистрибутивах Ubuntu, Debian та Centos; брандмауери на основі Netfilter або PF, проксі-сервери; платформа віртуалізації VMWare vSphere);

адміністрування мережевих пристроїв (Cisco IOS, протокол маршрутизації BGP);

навички програмування мовою високого рівня, наприклад Python для автоматизації;

знання кластерних систем високої доступності, таких як patroni, zookeeper, etcd, glusterfs.

Технології веб-додатків, їх розробка:

HTML, сценарії на стороні клієнта та сервера, мови програмування такі як JavaScript, PHP, Python, Go, SQL тощо, системи керування реляційними базами даних, такі як MySQL;

пакет інструментів Devops, на зразок - Docker, Kubernetes, Jenkins тощо.

Захист комп'ютерних мереж:

моніторинг, виявлення, аналіз, звітність, вирішення інцидентів безпеки;

аналіз файлів журналів і захоплень пакетів для виявлення інцидентів.

Мережева криміналістика:

хост криміналістичної експертизи - Windows/Linux/iOS зображення та аналіз пам'яті;

мережева експертиза – мережеві пристрої, мікропрограмне забезпечення, пам'ять і мережевий трафік;

аналіз шкідливих програм - зворотний інжиніринг;

криміналістична експертиза смартфонів та IoT.

Спеціальні системи кіберзахисту автоматизованих систем об'єктів критичної інфраструктури [8]:

фахівці з ICS повинні мати принаймні базові знання та досвід з кіберзахисту, адміністрування, тестування, оцінки та сертифікації промислових об'єктів (промислового контролю), володіти знаннями програмних та апаратних елементів системи SCADA та її компонентами PLCs та HMIs;

рекомендується досвід роботи з мережами мобільного зв'язку. Базове розуміння функціональності компонентів мережі мобільного зв'язку, таких як MME, SGW, PGW, HSS, eNodeB тощо.

Зв'язки з громадськістю:

проходження навчання на курсах ЗМІ (відвідування тренінгів, заздалегідь).

Нормативно-правові аспекти:

юрисконсульт зобов'язаний вирішувати питання, пов'язані з застосуванням спеціального програмного забезпечення для тестування на проникнення і проведення аудиту безпеки. Йому слід пам'ятати, що під час виконання вправи їхні колеги-члени, ймовірно, будуть сильно вражені кібератаками на системи, і тому матимуть обмежений час для спілкування з юридичними радниками. Таким чином, юрисконсульт повинен мати принаймні базові знання про інформаційні технології, оскільки в іншому випадку він ризикує тим, що інформація, яка надходить від технічних експертів, буде незрозумілою, а юрисконсульт не буде відповідати цілям навчання.

Крім зазначених базових знань експерти повинні мати відповідні навички, щодо здійснення етапів планування, розуміти ієрархію побудови технічного середовища, вміти настроїти та налагодити роботу віртуальної машини з власними інструментами, протестувати канали та засоби зв'язку, підключитись до кібер-діапазону (CCDCOE надає облікові записи cr14, програмне забезпечення VPN, RocketChat та програмне забезпечення для веб-конференцій тощо) і запустити тестові атаки та відпрацювати цикл звітності.

Також у разі потреби експерти-практики повинні вміти спроектувати та створити такі системи [3]:

сервер Microsoft Exchange;

різні військові системи, які можна легко інтегрувати в мережу навчань;

будь-які масштабні цивільні програми, такі як SAP, Dynamics тощо;

різні web-додатки: Інтранет, системи документообігу тощо;

вбудовані пристрої, пристрої "Інтернету речей (IoT)", смартфони, планшети тощо.

Висновки й перспективи подальших досліджень

Отже, як висновок слід зазначити, що Locked Shields 2022 це перший крок українських фахівців складових Сил оборони та фахівців вищих навчальних закладів із кібербезпеки щодо практичної перевірки набутих ними компетентностей з питань кібербезпеки в ході об'єднаної багаторівневої системи навчання.

Експерти з кібербезпеки покращать свої навички захисту національних ІТ-систем та критичної інфраструктури від атак у реальному часі, перевірять свої технічні та управлінські навички для захисту сфери електронних комунікацій від повношвидкісних кібератак.

При цьому набутий практичний досвід та наукове супроводження Locked Shields 2022 дозволить скорегувати концептуальні засади професійної підготовки фахівців із кібербезпеки за спеціальністю 125 "Кібербезпека" та удосконалити чинне законодавство, що регулює сферу інформаційної та кібернетичної безпеки.

В майбутньому застосувати на практиці в закладах вищої освіти складових Сил оборони держави та цивільного сектору отриманий зарубіжний досвід навчання у вказаному напрямі тощо.

Література

1. Указ Президента України Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" https://zakon.rada.gov.ua/laws/show/447/2021#Text.
2. Євсюкова О. В. Особливості підготовки фахівців у сфері кібербезпеки: сучасні виклики та перспективи: URL: http://www.dy.nayka.com.ua/pdf/2_2021/4.pdf, DOI: 10.32702/2307-2156-2021.2.2. **3. Живило Є.О**. Об'єднана підготовка персоналу складових Сил оборони сфери кібербезпеки в умовах тотальної оборони держави: URL: https://tp.kh.ua/index.php/tpdu/article/view/295/273, DOI: 10.34213/tp.21.02.16. **4.** Locked Shields is a unique international cyber defence exercise offering the most complex technical live-fire challenge in the world: URL://https://ccdcoe.org/exercises/locked-shields/.
5. A. Ertan (Eds.) Cyber Threats and NATO 2030: Horizon Scanning and Analysis: URL://https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf.
6. Доктрина "Зв'язок та інформаційні системи" Центральне управління звязку та інформаційних систем Генерального штабу Збройних Сил України, ВКП 6-00(01).01, червень 2020. **7. Ілмар Тамм** Центр експертизи з питань кооперативної кібер-оборони (CCDCOE), NATO unclassified rel to EU/PFP: URL: https://www.nato.int/docu/other/ukr/pdf/CCD%20COE%20presentation%20ukr.pdf. **8.** "Загрози критичній інфраструктурі та їх вплив на стан національної безпеки (моніторинг реалізації Стратегії національної безпеки)". Аналітична записка Національного інституту стратегічних досліджень. Березень 2017 р.: http://old.niss.gov.ua/content/articles/files/KI_-Ivanyuta-3a331.pdf. **9.** Рішення Ради національної безпеки і оборони України від 16 лютого 2017 року «Про невідкладні заходи з нейтралізації загроз енергетичній безпеці України та посилення захисту критичної інфраструктури», Введене в дію Указом Президента України від 16 лютого 2017 року № 37/2017//https://zakon.rada.gov.ua/laws/show/n0001525-17#Text.

МЕЖДУНАРОДНЫЕ КИБЕРУЧЕНИЯ LOCKED SHIELDS – 2022. ПРОБЛЕМНЫЕ ВОПРОСЫ В ПОДГОТОВКЕ СОСТАВНЫХ СИЛ ОБОРОНЫ И БЕЗОПАСНОСТИ УКРАИНЫ

***Евгений Александрович Живило** (кандидат наук по государственному управлению)[1]*
***Александр Александрович Черноног**[2]*

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

В современных условиях для Украины обеспечение кибербезопасности является одним из приоритетов в системе национальной безопасности. В этих условиях вес киберугроз растет и эта тенденция по мере развития информационных технологий и их родства с технологиями искусственного интеллекта в ближайшее десятилетие будет усиливаться. Увеличение такого влияния на функционирование структур управления как национальных, так и транснациональных требует формирования нового формата безопасности. Между мировыми центрами силы происходит разделение сфер влияния в киберпространстве, усиливается их стремление за счет такого разделения обеспечить реализацию собственных геополитических интересов [1].

Уровень вызова в национальном сегменте киберпространства стран мира в целом с каждым годом растет как по размеру, так и по уровню сложности. Составляющим сил обороны и безопасности Украины крайне необходимы опытные эксперты с хорошими навыками в тестировании на проникновение, передачу, обмен информацией и ситуационной осведомленностью. При этом важен опыт представителей как гражданского сектора, так и сектора обороны государства, которые привлекались к проведению международных киберучений в составе команды.

В этой ситуации, в рамках международного сотрудничества, украинским экспертам по кибербезопасности для достижения оперативной совместимости крайне важно направить свои практические навыки по защите национальных ИТ-систем и критической инфраструктуры от атак в реальном времени.Так, улучшение навыков национальных кибергрупп быстрого реагирования следует сосредоточить на: обмене информацией о кибератаках и киберинцидентах, проведении совместных

кибероперацій и расследованиях международных киберпреступлений, регулярных совместных киберобучениях и тренингах, обмене опытом и наилучшими подразделениями – лучшими практиками.

Практическая направленность в тесном сотрудничестве представителей экспертных групп в сфере киберзащиты на одной платформе в режиме реального времени – это уникальная возможность национальных киберзащитников практиковать защиту национальных ИТ-систем и критической инфраструктуры под давлением серьезной кибератаки.

Ключевые слова: *цифровое общество, информационно-коммуникационные технологии, киберконфликт, киберугрозы, кибербезопасность, киберпространство, система подготовки специалистов в области кибербезопасности.*

INTERNATIONAL CYBER TESTS LOCKED SHIELDS – 2022. PROBLEM ISSUES IN TRAINING THE COMPOSITE DEFENSE AND SECURITY FORCES OF UKRAINE

Yevgen Zhyvylo *(**Candidate of Science in Public Administration**)* [1]
Olexandr Chernonog [2]

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

In modern conditions for Ukraine, ensuring cybersecurity is one of the priorities in the national security system. Under these conditions, the weight of cyber threats is growing, and this trend, as information technologies develop and their relationship with artificial intelligence technologies, will increase in the next decade. An increase in such influence on the functioning of governance structures, both national and transnational, requires the formation of a new security format. Between the world centers of power, there is a division of spheres of influence in cyberspace, their desire to ensure the implementation of their own geopolitical interests through such division is increasing [1].

The call level in the national segment of the cyberspace of the countries of the world as a whole is growing every year both in size and in complexity. The components of the Ukrainian Defense and Security Forces are in dire need of experienced experts with good skills in penetration testing, transmission, information sharing and situational awareness. At the same time, the experience of representatives of both the civilian sector and the state defense sector, who were involved in conducting international cyber exercises as part of a team, is important.

In this situation, within the framework of international cooperation, it is extremely important for Ukrainian cybersecurity experts to achieve interoperability by directing their practical skills to protect national IT systems and critical infrastructure from real-time attacks. Thus, improving the skills of national cyber rapid response teams should be focused on: exchanging information about cyber attacks and cyber incidents, conducting joint cyber operations and investigating international cyber crimes, regular joint cyber education and training, sharing experience and best units - best practices.

The practical focus of closely collaborating between representatives of cyber defense expert groups on a single platform in real time is a unique opportunity for national cyber defenders to practice protecting national IT systems and critical infrastructure under the pressure of a serious cyber attack.

Key words: *digital society; information and communication technologies; cyber conflict; cyber threats; cybersecurity; Cyberspace; a system for training specialists in the field of cybersecurity.*

References

1. Ukaz Prezy`denta Ukrayiny` Pro rishennya Rady` nacional`noyi bezpeky` i oborony` Ukrayiny` vid 14 travnya 2021 roku "Pro Strategiyu kiberbezpeky` Ukrayiny`" https://zakon.rada.gov.ua/laws/show/447/2021#Text. **2. Yevsyukova O. V.** Osobly`vosti pidgotovky` faxivciv u sferi kiberbezpeky`: suchasni vy`kly`ky` ta perspekty`vy`: URL: http://www.dy.nayka.com.ua/pdf/2_2021/4.pdf, DOI: 10.32702/2307-2156-2021.2.2. **3. Zhy`vy`lo Ye.O.** Ob'yednana pidgotovka personalu skladovy`x Cy`l oborony` sfery` kiberbezpeky` v umovax total`noyi oborony` derzhavy`: URL: https://tp.kh.ua/index.php/tpdu/article/view/295/273, DOI: 10.34213/tp.21.02.16. **4.** Locked Shields is a unique international cyber defence exercise offering the most complex technical live-fire challenge in the world: URL://https://ccdcoe.org/exercises/locked-shields/. **5. A. Ertan** (Eds.) Cyber Threats and NATO 2030: Horizon Scanning and Analysis: URL://https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf. **6. Doktry`na** "Zv'yazok ta informacijni sy`stemy`" Central`ne upravlinnya zvyazku ta informacijny`x sy`stem General`nogo shtabu Zbrojny`x Sy`l Ukrayiny`, VKP 6-00(01).01, cherven` 2020. **7. Ilmar Tamm** Centr eksperty`zy` z py`tan` kooperaty`vnoyi kiber-oborony` (CCDCOE), NATO unclassified rel to EU/PFP: URL: https://www.nato.int/docu/other/ukr/pdf/CCD%20COE%20presentation%20ukr.pdf. **8.** "Zagrozy` kry`ty`chnij infrastrukturi ta yix vply`v na stan nacional`noyi bezpeky` (monitory`ng realizaciyi Strategiyi nacional`noyi bezpeky`)". Anality`chna zapy`ska Nacional`nogo insty`tutu strategichny`x doslidzhen`. Berezen` 2017 r.: http://old.niss.gov.ua/content/articles/files/KI_-Ivanyuta-3a331.pdf. **9.** Rishennya Rady` nacional`noyi bezpeky` i oborony` Ukrayiny` vid 16 lyutogo 2017 roku «Pro nevidkladni zaxody` z nejtralizaciyi zagroz energety`chnij bezpeci Ukrayiny` ta posy`lennya zaxy`stu kry`ty`chnoyi infrastruktury`», Vvedene v diyu Ukazom Prezy`denta Ukrayiny` vid 16 lyutogo 2017 roku # 37/2017//https://zakon.rada.gov.ua/laws/show/n0001525-17#Text.