ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ КАДРОВОЇ ПОЛІТИКИ В УКРАЇНІ

Живило Євген Олександрович,
к.держ.упр.,
начальник науково-дослідного управління розвитку військ зв'язку,
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут,
м. Київ
ORCID 0000-0003-4077-7853;

Живило Ірина Олександрівна,
к.м.н.,
молодший науковий співробітник відділу вторинних і легеневих гіпертензій,
Державна установа "Національний науковий центр "Інститут кардіології імені академіка М. Д. Стражеска" НАМН України,
м. Київ
ORCID 0000-0001-8141-363X

УДК 351.86 **doi: 10.34213/tp.21.02.16**

ОБ'ЄДНАНА ПІДГОТОВКА ПЕРСОНАЛУ СКЛАДОВИХ СИЛ ОБОРОНИ СФЕРИ КІБЕРБЕЗПЕКИ В УМОВАХ ТОТАЛЬНОЇ ОБОРОНИ ДЕРЖАВИ

Обґрунтовано актуальність щодо розроблення єдиного сучасного змісту компетентностей з питань кібербезпеки для фахівців вищих військових навчальних закладів та військових навчальних підрозділів закладів вищої освіти складових Сил оборони держави під час об'єднаного багаторівневого навчання персоналу.

Проаналізовано теоретичні аспекти формування та порядку набуття індивідуальних спроможностей фахівцями з кібербезпеки відповідно до розроблених стандартів підготовки, з метою досягнення сумісності в підготовці підрозділів складових Сил оборони та держав – членів НАТО.

Акцентовано увагу на питаннях стандартизації підготовки зі спеціальності 125 "Кібербезпека" та на фахових компетенціях спеціалістів у сфері кібербезпеки для набуття ними об'єднаних спроможностей, які необхідні для швидкого та спільного реагування на загрози воєнній безпеці України, а також загрозам в інших сферах діяльності держави, які забезпечать формування та реалізацію державної політики у сфері цивільного захисту.

Ключові слова: цифрове суспільство; інформаційно-комунікаційні технології; об'єднана підготовка; складові Сил оборони; кібербезпека; кібероборона; система підготовки фахівців у сфері кібербезпеки.

Постановка проблеми. Сьогодні у громадян України немає жодних сумнівів щодо демократичних принципів управління в нашій державі. При цьому переосмислення самого значення держави як головного суб'єкта-виконавця в реалізації інтересів і задоволенні потреб суспільства залишається одним із завдань у теорії сучасного державного управління та практиці публічного адміністрування.

Сучасним етапом у розвитку демократичного суспільства стали інформаційно-комунікаційні технології, які надали змогу за нових умов сформувати діалог держави та суспільства, влади та громадян у новому ракурсі, наближуючи її до ідеальної демократії, при цьому держава набуває сервісних ознак, суспільство перетворюється на smart-спільноту, а влада є якісно новим засобом вирішення публічних справ в інтересах усієї країни шляхом залучення якомога більшої чисельності громадян до цього процесу.

Із розвитком цифрових технологій проблема захисту національного сегмента кіберпростору кожної розвиненої держави стає одним із пріоритетних питань зовнішньої політики, а розвиток обізнаного в цифровому відношенні суспільства є найважливішою галуззю її внутрішньої політики.

Унаслідок надзвичайно широкого використання сучасних інформаційно-комунікативних технологій у всіх сферах свого існування суспільство стало вразливим до кібернетичних впливів, які все частіше стають ефективним інструментом для досягнення мети несилового контролю та управління як об'єктами інфраструктури держави, підприємств, так і окремо взятими громадянами та їхніми об'єднаннями.

Потоки інформації, що передаються, зберігаються й обробляються в кіберпросторі, постійно збільшуються, що вимагає належного захисту їх від несанкціонованого доступу, який має на меті злочинну дію. Тому посилення кібербезпеки є надзвичайно важливим для забезпечення довіри людей до інновацій, взаємозв'язку та автоматизації, отримання переваг від них, а також для захисту основних прав і свобод, зокрема права на приватність та захист персональних даних, а також свободу вираження поглядів та інформації [1].

Безперечним є той факт, 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 у сфері кібербезпеки взагалі не піддається ніякому сумніву.

Аналіз останніх досліджень і публікацій. Існує значна кількість досліджень, що стосуються підготовки спеціалістів цивільного сектору за спеціальністю 125 "Кібербезпека". Ідеться про наукові праці Л. Арсеновича (щодо специфіки формування системи підготовки фахівців у сфері кібербезпеки органів публічної влади тощо); Б. Бистрової, Ю. Савчука (щодо формування концептуальних засад професійної підготовки фахівців із кібербезпеки та вдосконалення чинного законодавства, що регулює сферу інформаційної та кібернетичної безпеки, використання найкращих практик із зарубіжного досвіду у вказаному напрямі тощо); І. Діордиці (щодо формування системи забезпечення кібербезпеки, сутнісного визначення кіберзлочинності, правового регулювання кібертероризму тощо); О. Криворучка, І. Костюка (щодо стратегування безпеки інформації); Л. Рудника (щодо інформаційної безпеки та кібербезпеки як складових елементів національної безпеки тощо). При цьому наукова проблематика у сфері кібербезпеки досить ґрунтовно висвітлюється в наукових розробках таких вчених, як В. Богуш, О. Євсюкова, В. Бурячок, С. Воскобойніков, Т. Запорожець, О. Карпенко, І. Кулик, С. Мельник [2].

Розбудова та упровадження системи підготовки фахівців із кібербезпеки для складових сил оборони здійснювалась упродовж останніх п'яти-семи років на державному, галузевому та відомчому рівнях згідно з програмами

фундаментальних і наукових робіт Міністерства оборони України, Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації України та інших суб'єктів сил оборони в рамках науково-дослідних робіт, що виконувались у Національному технічному університеті 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 Служби безпеки України.

Теоретико-методологічне обґрунтування і практичне упровадження системи підготовки фахівців для сектору безпеки і оборони України з кібербезпеки доволі якісно та змістовно дослідили такі досвідчені науковці, як П. Воробієнко, Ю. Даник, О. Корнейко, С. Мамченко, О. Новіков, О. Оксіюк, А. Зінченко, І. Руснак, В. Телелим. Їхні наукові роботи було спрямовано на дослідження сучасних підходів, закономірностей, методів і технологій щодо теорії і практики підготовки до протидії та ведення війни в кібернетичному та інформаційному просторах, протидії кіберзлочинності тощо.

Слід зазначити, що при цьому пріоритетні напрями у проведенні досліджень у зазначеній галузі наук представниками як цивільного сектору, так і сектору оборони держави було пов'язано:

– з порядком імплементації вимог (стандартів підготовки) військових технічних навчальних закладів країн НАТО в навчальний процес підготовки фахівців ступенів вищої освіти "бакалавр", "магістр";

– розвитком систем військової освіти та підготовки військових кадрів, ураховуючи досягнення в галузі освіти та науки, тенденції та перспективи упровадження апаратно-програмних інновацій, їхнє нарощування;

– обґрунтуванням перспективної системи об'єднаної підготовки та підвищення кваліфікації наукових і науково-педагогічних працівників, підготовки наукових кадрів вищої кваліфікації;

– розробленням методичних основ науково обґрунтованої системи підготовки спеціалістів з питань криптографічного та технічного захисту інформації.

Незважаючи на досить вагомі фундаментальні напрацювання зазначених науковців за вказаним напрямом, усе ще залишаються далекими від завершення наукові дослідження 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; порядку підготовки органів управління (штабів), військових частин (підрозділів) у взаємодії (під керівництвом) з іноземними тренувальними місіями на території України та країнами-партнерами з метою переходу на систему підготовки держав – членів НАТО та досягнення взаємосумісності з ними.

Мета статті. З огляду на зазначене головна ідея статті полягає у формуванні єдиного сучасного змісту компетентностей із питань кібербезпеки в межах об'єднаної підготовки складових сил оборони, необхідних для виконання завдань за посадами фахівцями – випускниками військових закладів вищої освіти (*далі – ЗВО*) та військових навчальних підрозділів ЗВО.

Виклад основного матеріалу. Кіберпростір України є невід'ємною частиною глобального (світового) кіберпростору, який взаємопов'язує критичну

інформаційну інфраструктуру всіх складових сектору безпеки та оборони України, органів державної влади та об'єкти критичної інфраструктури державної та приватної форм власності.

Україна підтверджує оборонний мандат і визнає кіберпростір сферою операцій, у якій має захищати себе так само ефективно, як вона це робить у повітрі, на землі та на морі. Підготовка до виконання цього завдання силами оборони держави здійснюється під час проведення об'єднаного багаторівневого навчання персоналу та його злагодження. Метою об'єднаної підготовки персоналу складових сил оборони сфери кібербезпеки є набуття ними об'єднаних спроможностей, необхідних для швидкого та спільного реагування на загрози воєнній безпеці України, а також загрози в інших сферах.

Набуття об'єднаних спроможностей та навчальних об'єднаних спроможностей Збройних Сил України та сил оборони щодо захисту національного сегмента кіберпростору, проведення операцій у кіберпросторі в будь-яких умовах щодо стримування, відмови від агресії в кіберпросторі або через кіберпростір є першочерговим завданням в умовах тотальної оборони держави.

Аналізуючи нормативно-правові документи щодо упровадження та нарощування системи кадрового менеджменту за напрямом кібероборони держави, слід зауважити, що на загальнодержавному рівні було прийнято низку концептуальних документів довгострокового планування.

Зокрема, у березні 2016 р. було затверджено Стратегію кібербезпеки України, у жовтні 2017 р. набрав чинності Закон України "Про основні засади забезпечення кібербезпеки України", а в березні 2021 р. Указом Президента України № 121/2021 затверджено рішення Ради національної безпеки і оборони України "Про Стратегію воєнної безпеки України".

Вказаними законодавчими актами визначено завдання щодо здійснення заходів з підготовки держави до відбиття воєнної агресії в кіберпросторі (кібероборони), військової співпраці з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз, а також упровадження заходів із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного станів [3].

Відтак, із затвердженням Стратегічного оборонного бюлетеня України, розпочнеться розроблення відповідних програмних документів, спрямованих на зміцнення обороноздатності держави, порядку та циклічності набуття необхідних оборонних спроможностей силами оборони, усебічного забезпечення їхнього застосування, зокрема й організації кадрового забезпечення розвитку систем кібербезпеки складових сил оборони.

За цих умов є необхідним розробити єдиний сучасний зміст компетентностей із питань кібербезпеки для фахівців військових навчальних закладів та військових навчальних підрозділів ЗВО складових сил оборони держави під час об'єднаного багаторівневого навчання персоналу.

При цьому військовим навчальним підрозділам ЗВО для підготовки військових фахівців тактичного рівня є вкрай важливим скорегувати свою систему підготовки персоналу у сфері захисту інформації та кібербезпеки, стандартизувати методику професійної підготовки зі спеціальності 125 "Кібербезпека задля досягнення відповідних фахових компетенцій спеціалістів у сфері кібербезпеки та кібероборони держави.

У цілому це дозволить забезпечити:

– сталу та єдину організацію освітнього процесу під час виконання заходів об'єднаної підготовки персоналу складових сил оборони у сфері кібербезпеки та кібероборони держави;

– досягти сумісності у підготовці підрозділів складових сил оборони, забезпечити формування та реалізацію державної політики у сфері цивільного захисту держави,

– здійснити активне освоєння та використання кіберпростору в інтересах реалізації своїх національних інтересів на основі поєднання наявних інформаційних технологій та управління ними в умовах, які швидко змінюються.

Ураховуючи зазначене вище, можна дійти висновку, що різноманіття можливостей такого поєднання спричиняє появу відповідних форм практичної діяльності сил оборони держави в кіберпросторі, які стали реальністю та стрімко трансформуються. Стрімкість розвитку цих форм створює умови для появи операцій у кіберпросторі.

Основними чинниками, що впливають на розвиток операцій у кібепросторі, є спроможності сил оборони держави, зокрема Збройних Сил України, адекватно реагувати на актуальні загрози в кібер- та інформаційному просторах [4].

В умовах загроз воєнного характеру для України, коли використовуються гібридні підходи до ведення війни (воєнних дій), особливо загострюється інформаційне протиборство, при цьому головна роль відводиться операціям у кіберпросторі, однією з форм яких є кібероперація.

Тому упровадження політики щодо ведення кібероборони, проведення кібероперацій та нарощування спроможностей в об'єднаній підготовці відповідних фахівців за напрямом забезпечення кіберзахисту своїх інформаційно-телекомунікаційних систем та здійснення активного кібервпливу на інформаційно-телекомунікаційні системи противника з використанням засобів кіберзахисту, апаратно-програмних комплексів із кібербезпеки, кіберозброєнь, які побудовано з урахуванням передових технологій, є вкрай важливим фактором.

Отже, на думку авторів, вимоги до компетентностей військового фахівця з організації та експлуатації засобів кібербезпеки (кіберрозвідки, кіберзахисту, кібероборони), що слугують основою для формування професійних кваліфікацій зі спеціальності 125 "Кібербезпека", повинні складатися:

– *зі знань щодо*:

основних вимог керівних документів із кібербезпеки, кіберзахисту, кіберрозвідки, кібероборони та дій (операцій) у кіберпросторі;

основних вимог нормативних документів у сфері електронних комунікацій, інформаційно-комунікаційних технологій, технічного та криптографічного захисту інформації, забезпечення безпеки інформації та кібербезпеки, міжнародних і національних стандартів (ISO/IEC, NIST), стандартів ЄС і НАТО у сферах безпеки інформації та кібербезпеки [5];

основних інформаційно-комунікаційних технологій (включаючи технології онлайн-доступу), організації функціонування ІСД-інтернет та АСУ "Дніпро";

складу та порядку (алгоритмів) дій основних кіберугруповань у кіберпросторі (військові, терористичні, хакерські та ін.);

технологій кіберзахисту, зокрема із забезпечення апаратної, контентної безпеки, безпеки додатків та сервісів зв'язку;

порядку своєчасного виявлення, запобігання та нейтралізації кіберзагроз, дій у разі надзвичайних ситуацій та інцидентів у кіберпросторі;

порядку оперативного реагування на кібератаки та кіберінциденти, усунення їхніх наслідків, особливостей кіберзахисту критичної інфраструктури;

порядку аудиту інформаційної безпеки в мережах, контролю за станом захисту інформації, кібербезпеки та кіберзахисту, експертного оцінювання стану кібербезпеки;

складу, оснащення, можливості та порядку функціонування команд реагування на комп'ютерні надзвичайні події (CERT);

складу та можливостей організаційно-технічної моделі національної системи кібербезпеки, системи захисту інформації та кібербезпеки в інформаційно-телекомунікаційних системах Міністерства оборони та Збройних Сил України, повноваження та порядку взаємодії суб'єктів забезпечення кібербезпеки;

порядку проведення навчань (ззокрема і в рамках заходів колективної оборони) щодо реагування на кібератаки та кіберінциденти;

основних можливостей сил, засобів та інструментів можливої відповіді на агресію у кіберпросторі (активного кіберзахисту);

вимог нормативно-правової бази щодо адміністративної та кримінальної відповідальності за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

основних методів виявлення та боротьби з кіберзлочинами та шахрайством у кіберпросторі, зокрема: збирання доказів в електронній формі, ідентифікації та фіксації кіберзлочинів, проведення експертних досліджень;

порядку зняття інформації з каналів телекомунікацій у разі розслідування інцидентів кібероборони;

базової еталонної моделі взаємодії відкритих систем OSI та розподілу основних протоколів за рівнями моделі OSI, архітектури мереж Ethernet;

стеку протоколів TCP/IP, структури пакета IP, порядку планування IP адресного простору, використання маски IP-адреси, розподілу IP-мереж на підмережі;

принципів побудови Інтернет та організації світової і державної структури IP- та DNS-адресації, системи адресації v4/v6 та принципів маршрутизації AS;

основних протоколів та інтерфейсів (FTP, TTP, TCP, UDP, BigTorrent, SMTP, POP3, IP ICMP, ARP, HTTP, HTTPS, SMTP, IRC, SSM ICQ, AOL, NAT, SPX/IPX, NetBIOS/NetBEUI, NetBEUI, SPX/IPX, SQL, SSL, TLS та ін.), призначення основних портів операційних систем;

принципів організації процесів аудиту, віртуалізації, гіпервізорів та центрів оброблення даних;

порядку організації та засобів реалізації віддаленого доступу, резервування, зберігання та відновлення інформації;

основ адміністрування й підтримки серверних систем на основі Microsoft Windows Server, Unix (FreeBSD, CentOS, Debian), включаючи сервери мережевих служб (DHCP, DNS та ін.);

основ адміністрування Apache, PHP, MySQL, Mail, FTP, squid, ін.;

основ застосування систем віртуалізації (VmWare, Proxmox, ін.);

основних принципів побудови та протоколів IP-телефонії, SIP-серверів;

принципів розгортання, маршрутизації та адміністрування мережевого обладнання Cisco, побудови LAN/WAN мереж на обладнанні Cisco;

різноманітних класифікацій та описів кібератак (CISCO, OWASP, CAPEC, ін.);

основних методів реалізації кібератак та кіберзахисту від них, за напрямами: Ethical Hacking, Footprinting and Reconnaissance, Scanning Networks, Enumeration, System Hacking, Malware Threats, Sniffing, Social Engineering, Denial-of-Service, Session Hijacking, Hacking Webservers, Hacking Web Applications, SQL Injection, Hacking Wireless Networks, Hacking Mobile Platforms, Evading IDS, Firewalls, and Honeypots, Cloud Computing, Buffer Overflows, Cryptography, Penetration Testing;

структури, основних характеристик сервісів безпеки (зокрема, локальної та групової політики безпеки (Active Directory, ін.) операційних систем сімейств Windows, Linux та ін.;

складу та порядку розгортання сервісів безпеки систем керування базами даних та систем SCADA;

порядку налаштування та дистанційного керування міжмережевими екранами, зокрема з IPS;

порядку використання програмного забезпечення контролю (моніторингу) дій користувача, знищення (затирання) даних, контролю USB-носіїв інформації;

порядку та механізмів захисту Web-ресурсів, електронної пошти;

порядку організації та забезпечення мережної безпеки, зокрема і конфігурування мережних пристроїв та сервісів безпеки, застосування аналізаторів пакетів, IOS, VPN, Packet Tracer та ін.;

порядку організації моніторингу мережного трафіку і забезпечення його безпеки;

необхідних мов програмування (не менше трьох) в обсязі, достатньому для практичного розроблення спеціального програмного забезпечення кібербезпеки;

основ криптографії та криптографічних алгоритмів: TEA, Two fish, cast256, DES, AES, Triple24bit, RC2, RC4, RC5 та інші;

основ автентифікації, ідентифікації, розмежування доступу до інформаційних ресурсів, перехоплення та розкриття автентифікаційних даних користувачів;

технологій SSL, TLS, VLAN, HTTPS, антивірусного захисту, сертифікатів, шифрування даних засобами операційної системи, PKI, порядку використання електронно-цифрового підпису, технології VPN (DMVPN, IPSec, GRE), ін.;

основних механізмів захисту безпроводових мереж (WEP, WPA, WPA-2 шифрування та вразливості WPS);

порядку визначення маршрутів проходження пакетів та джерел кібератак;

підходів до ведення боротьби в соціальних мережах;

методів анонімного доступу, ведення кіберрозвідки, порядку використання прихованих мереж (TOR, I2P, P2P та ін.);

порядку організації сканування та моніторингу мереж із застосуванням засобів типу Zabbix, Warchark, Iris, Nmap, ZENMAP та ін.;

порядку упровадження та виявлення різноманітних вразливостей вебсайтів;

вимог та порядку оцінювання стійкості паролів (операційних систем, електронних поштових скриньок, архівів, ін.) із використанням програмних засобів;

порядку організації різноманітних кібератак (Brute force, ін.) та дій (операцій) у кіберпросторі;

порядку виявлення в мережі хостів з інформаційними ресурсами, які знаходяться у відкритому доступі, отримання доступу до віддаленого хоста;

порядку роботи з наборами програм типу BackTrack та Kali Linux;

порядку використання основних систем виявлення атак та запобігання їм, захисту від вторгнень, виявлення вразливостей, витоку інформації та юридичної фіксації кібернетичних інцидентів типу: SIEM, DLP, IDS, IPS, DDiOD, FSIGHT, FirePower;

порядку реалізації, виявлення та нейтралізації DDoS-атак;

порядку розгортання, виявлення та нейтралізації бот-мереж, проксисерверів, анонімайзерів;

порядку адміністрування безпеки комп'ютерних мереж;

- умінь щодо:

опрацьовування фізичної та логічної топологій комп'ютерних мереж, налаштування локальної та групової політики безпеки операційних систем;

розроблення програмного забезпечення кібербезпеки;

встановлення та здійснення конфігурації комутаторів і маршрутизаторів у багатопротокольних мережах, які об'єднують локальні та територіально розділені мережі (LAN і WAN);

розгортання, конфігурування локальних і супроводження територіально розподілених мереж і сервісів віддаленого доступу відносно мереж, які мають 100 і більше вузлів та в яких використовуються такі протоколи й технології, як TCP/IP, OSPF, EIGRP, BGP, ISDN, STP і VTP;

навичок із проєктування побудови мереж зв'язку з використанням різних технологій із застосуванням сучасного обладнання типу Cisco, Dlink та ін.;

розгортання та адміністрування системи телефонії Cisco Unified Communication, Asterisk, телефонних апаратів;

здійснення налаштування основних сервісів безпеки на основі Microsoft Windows Server, Unix (FreeBSD, CentOS, Debian), включаючи сервери мережевих служб (DHCP, DNS та ін.);

створення VPN-каналів для необхідних напрямів комунікацій, практичного оцінювання стійкості паролів різноманітними програмними засобами;

здійснення розгортання та дистанційного керування міжмережевими екранами, зокрема з IPS;

адміністрування, налаштування та порядку експлуатації системи моніторингу мережі, здійснення контролю технічних параметрів і параметрів якості сервісів;

реалізації захисту та оцінювання ефективності захищеності безпроводових мереж;

визначення маршрутів проходження пакетів та джерела кібератак;

використання методів анонімного доступу;

користування прихованими мережами (TOR, I2P, P2P та ін.);

упровадження та виявлення різноманітних вразливостей (SQL, XSS та ін.) на тестових вебсайтах, практичного оцінення захищеності вебсайтів із використанням програмного забезпечення (Acunetix Web Vulnerability Scanner, ін.);

виконання практичних заходів із наборами програм типу BackTrack та Kali Linux;

проведення розгортання, виявлення та нейтралізації бот-мереж, проксисерверів, анонімайзерів;

проведення розгортання основних систем виявлення атак та запобігання їм, захисту від вторгнень, виявлення вразливостей, витоку інформації та юридичної фіксації кібернетичних інцидентів типу: SIEM, DLP, IDS, IPS, DDiOD, FSIGHT, FirePower.

Висновки з цього дослідження і перспективи подальших розвідок у цьому напрямі. Сьогодні вищим військовим закладам (військовим навчальним підрозділам ЗВО) та ЗВО, 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 відповідно до сучасних умов динамічного розвитку світової цифрової обізнаності.

Об'єднану підготовку складових сил оборони зі спеціальності 125 "Кібербезпека" повинно бути сформовано на основі єдиного сучасного змісту компетентностей з питань кібербезпеки, якість рівня кваліфікації здобувачів вищої освіти повинна мати практичну спрямованість із питань організації та експлуатації засобів кібербезпеки (кіберрозвідки, кіберзахисту, кібероборони).

Цей напрям діяльності повинен мати динамічний розвиток та корегування і потребує подальших досліджень.

Список використаних джерел

1. Воробієнко П. П. Теоретико-методологічне обґрунтування і практичне впровадження системи підготовки фахівців для сектору безпеки і оборони України з кібербезпеки. URL: https://itgip.org/wp-content/uploads/2019/06/%D0%A0%D0%B5%D1%84%D0%B5%D1%80%D0%B0%D1%82.pdf.

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.

3. Указ Президента України "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України"". URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text.

4. Доктрина підготовки сил оборони держави / затв. наказом Генерального штабу Збройних Сил України від 21.01.2020 № 18. ВКП 7-00(01).01.

5. Факультет інформаційно-комп'ютерних технологій, спеціальність 125 "кібербезпека". Інформація про спеціальність. URL: https://vstup.ztu.edu.ua/bakalavr/125-kiberbezpeka/.

Zhyvylo Ye. O.,
PhD in Public Administration, Head of the Research of Communications Troops Development Department, Military Institute of Telecommunications and Information Technologies named after Heroiv Krut, Kyiv
ORCID 0000-0003-4077-7853;
Zhyvylo I. O.,
PhD in Medicine, junior researcher of Secondary and Pulmonary Hypertension Department, NSC "Institute of Cardiology named after M. D. Strazhesko" of AMS of Ukraine, Kyiv
ORCID 0000-0001-8141-363X

JOINT TRAINING OF THE CYBER SECURITY DEFENSE FORCES PERSONNEL IN THE CONDITIONS OF TOTAL STATE DEFENSE

Nowadays, the process of Defense Forces training allows to agree the strategic requirements for training objectives, its tasks, and selected priorities for generating trained and ready to perform tasks of personnel, military units (units), and military authorities.

The relevance of developing a single modern content of competencies on cybersecurity for specialists of higher military educational institutions and military educational units of higher education institutions of the State Defense Forces during the joint multilevel training of personnel is substantiated in the article.

Theoretical aspects of the formation and acquisition of individual capabilities by cybersecurity specialists, in accordance with the developed training standards, to achieve compatibility in the training of units of the Defense Forces and NATO member states were analyzed.

Emphasis is placed on the issues of standardization of training in the speciality 125 "Cybersecurity" and the professional competencies of specialists in the field of cybersecurity to acquire independent programs that require a rapid and joint response to the threat of military security agencies of Ukraine, as well as threats in other areas of state activity. formation and implementation of state policy in the field of civil protection

The result of the study is the development of a single modern list of requirements for specialists of higher education institutions of the Defense Forces in the area of cybersecurity, which is consistent with the Military Security Strategy of Ukraine, takes into account the requirements of the Basic Joint Operational Concept "Defense Forces - 2030" and ensures readiness states to comprehensive (total) defense by conducting joint (interservice, interstate departmental, multinational) operations.

Keywords: digital society; information and communication technologies; joint training; components of the Defense Forces; cybersecurity; cyber defense; training system in the field of cybersecurity.

References

1. Vorobiyenko, P.P. Teoretyko-metodologichne obgruntuvannya i praktychne vprovadzhennya systemy pidgotovky faxivciv dlya sektoru bezpeky` i oborony Ukrayiny z kiberbezpeky. URL: https://itgip.org/wp-content/uploads/2019/06/%D0%A0%D0%B5%D1%84%D0%B5%D1%80%D0%B0%D1%82.pdf [in Ukrainian].

2. Yevsyukova, O.V. Osoblyvosti pidgotovky faxivciv u sferi kiberbezpeky: suchasni vyklyky ta perspektyvy: http://www.dy.nayka.com.ua/pdf/2_2021/4.pdf [in Ukrainian].

3. Ukaz Prezydenta Ukrayiny "Pro rishennya Rady nacionalnoyi bezpeky i oborony Ukrayiny vid 27 sichnya 2016 roku "Pro Strategiyu kiberbezpeky Ukrayiny"". URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text;

4. Doktryna pidgotovky Syl oborony derzhavy, zatverdzhena nakazom Generalnogo shtabu Zbrojnyx Syl Ukrayiny vid 21.01.2020 No. 18, VKP 7-00(01).01 [in Ukrainian].

5. Fakultet informacijno-kompyuternyx texnologij, specialnist: 125 "kiberbezpeka". Informaciya pro specialnist. URL:https://vstup.ztu.edu.ua/bakalavr/125-kiberbezpeka/ [in Ukrainian].

Надійшла до редколегії 15.05.2021 р.