Рекомендації щодо реалізації заходів оборонного планування для набуття й розвитку спроможностей перспективними Кіберсилами Збройних Сил України на основі DOTMLPFI

Володимир Горбатюк
заступник начальника Генерального штабу Збройних Сил України
Генеральний штаб Збройних Сил України
03168, проспект Повітряних Сил, 6, Київ, Україна
e-mail: gorbvol@yahoo.com
ORCID: 0009-0009-9566-3168

Владислав Горгуленко
ад'юнкт науково-організаційного відділу
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: vladyslavhorhulenko@gmail.com
ORCID: 0000-0001-6382-5075

Валерія Горгуленко
молодший науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: horhulenkovaleriia@gmail.com
ORCID: 0009-0009-1394-6325

Юзеф Добровольський
кандидат технічних наук, доцент
заступник начальника кафедри військової підготовки
з навчальної роботи – начальник навчальної частини
Національний авіаційний університет
03048, вулиця Медова 1, Київ, Україна
e-mail: kataza@i.ua
ORCID: 0000-0002-1077-1402

Максим Самсоненко
викладач кафедри військового управління
Інституту державного військового управління
Національного університету оборони України
Національний університет оборони України
03049, проспект Повітряних Сил, 28, м. Київ, Україна
e-mail: samson8115@ukr.net
ORCID: 0009-0001-6264-6582

Анотація. Сьогодні розвиток Міністерства оборони України та її Збройних Сил зокрема здійснюється на основі необхідних для набуття спроможностей, з орієнтуванням на існуючі та потенційні загрози національній і воєнній безпеці держави. Досвід збройного протистояння останнього десятиліття показав, що однією з таких загроз є агресія противника у кіберпросторі. Тому наразі існують достатні підстави для формування Кіберсил як окремого роду військ (сил) Збройних Сил України, завданням якого має стати підготовка та ведення військових заходів з кібероборони. Ефективне виконання покладеного завдання є можливим у разі набуття перспективними Кіберсилами Збройних Сил України визначених у

Стратегічному оборонному бюлетені необхідних спроможностей з ведення протиборства у кіберпросторі.

Під час проведення дослідження було використано методи системного аналізу, узагальнення та систематизації, які за сукупністю дозволили розробити модель реалізації заходів оборонного планування для набуття й розвитку спроможностей перспективними Кіберсилами Збройних Сил України на основі DOTMLPFI.

Метою цієї статті є розроблення моделі впровадження заходів оперативної безпеки для формування та розвитку потенціалу перспективних Кіберсил Збройних Сил України, використовуючи DOTMLPFI – передовий підхід, що застосовується в країнах-членах НАТО.

Розроблена модель являє собою опис спроможностей щодо ведення протиборства у кіберпросторі за кожним із восьми базових компонентів DOTMLPFI у формі: потенціал, якого можна досягнути, реалізувавши набуті спроможності; існуючий стан (проблема) спроможностей; можливі заходи для вирішення проблеми, які дозволять досягнути потенціалу спроможностей. Отже, модель реалізації заходів оборонного планування для набуття й розвитку спроможностей перспективними Кіберсилами Збройних Сил України охоплює такі компоненти спроможностей з ведення протиборства у кіберпросторі як: доктринальна база (D), організація (O), підготовка (T), ресурсне забезпечення (M), управління та лідерство (L), персонал (P), інфраструктура (F), взаємосумісність (I).

Практична значимість результатів дослідження розкривається у потенціалі набуття Збройними Силами України спроможностей з ведення протиборства у кіберпросторі шляхом впровадження запропонованої моделі реалізації заходів оборонного планування на основі DOTMLPFI.

Ключові слова: кібероборона, кіберпростір, кібербезпека, кіберборотьба, Кіберсили, оборонне планування, спроможності, DOTMLPFI.

Вступ (Introduction)

Оборонно-планувальна діяльність відіграє ключову роль у забезпеченні національної безпеки держави [1–3]. Ця діяльність потребує постійного динамічного розвитку, адаптації, модернізації та реформування безпекового сектору загалом та, зокрема, збройних сил для підтримання здатності держави до відбиття збройної агресії. При цьому, складність процесу оборонно-планувальної діяльності полягає в оцінюванні рівня зазначеної здатності, з огляду на невизначеність параметрів майбутньої збройної агресії (масштаб конфлікту, озброєння противника, його мета, цілі та ін.) [4–6]. Відповідно, рівень здатності до відбиття агресії може бути нижчим у разі недостатнього оцінювання загроз, або вищим необхідного та достатнього, що тягне за собою надлишкові витрати державного бюджету на оборонний сектор, які у країнах з ринковою економікою та демократичним устроєм є неприйнятними. В таких умовах розвинулася низка підходів (видів) до оборонного планування (ОП), серед яких: за принципом “зверху-вниз”; на основі ресурсів; на основі технологій; на основі уникнення ризиків; послідовне планування; на основі історичного досвіду; на основі сценаріїв; на основі загроз; на основі спроможностей. В Україні наразі прийнято ОП на основі спроможностей, орієнтоване на загрози. Така модель дає змогу врахувати загрози воєнній безпеці держави та сценарії їхнього розвитку, визначивши на їх основі завдання суб’єктів Сектору безпеки і оборони України та необхідні для виконання цих завдань спроможності, якими мають володіти типові носії спроможностей [7–9].

Законом України [10] завдання з підготовки та ведення кібероборони покладено на Міністерство оборони України (МО України) та Генеральний штаб Збройних Сил України (ЗС України), а Стратегічним оборонним бюлетенем [11] визначено перелік необхідних для набуття спроможностей складових Сектору безпеки і оборони України, серед яких ЗС України є носієм усіх без винятку зазначених спроможностей. Водночас, Стратегією кібербезпеки України [12] встановлено формування у системі МО України кібервійськ. На виконання цього положення у Верховній Раді України зареєстровано законопроєкт [13], яким пропонується

утворення Кіберсил як окремого роду військ (сил) ЗС України, основним завданням якого має стати виконання саме військових заходів з кібероборони держави. Доцільність та нагальність формування Кіберсил як окремого роду військ (сил) у складі ЗС України додатково підтверджується результатами аналізу та узагальнення передового досвіду ведення кіберборотьби у воєнних конфліктах сучасності [14], які свідчать про загрозу національній та воєнній безпеці України у вигляді військових кібероперацій російської федерації (рф) та підкреслюють домінування в кіберпросторі держав, у складі оборонних відомств яких наявні кібервійська. В умовах війни рф активно використовує власні кіберсили, які впливають на перебіг війни в Україні в інформаційному та когнітивному вимірах. На відміну від США, рф формально не оголошувала про наявність кіберсил, але фактично вони існують у вигляді кількох структур, основними з яких є: в головному управлінні генерального штабу збройних сил рф – APT "Sandworm", у федеральній службі безпеки рф – APT "Turla", у службі зовнішньої розвідки рф – APT "Nobelium" [14].

Цілком логічним і раціональним було б агрегування перспективними Кіберсилами усіх необхідних спроможностей з ведення протиборства у кіберпросторі, що визначені для ЗС України, набуття яких дозволило б забезпечити інтегральну спроможність до виконання військових заходів з кібероборони держави. При цьому, використання під час оборонно-планувальної діяльності новітніх методів, моделей, підходів та методик ОП може якісно покращити модель реалізації заходів для набуття спроможностей Кіберсилами [15–18].

Метою статті є розроблення моделі реалізації заходів ОП для набуття і розвитку спроможностей перспективними Кіберсилами ЗС України на основі DOTMLPFI – одного з передових методів (методик, підходів), що використовується в країнах НАТО.

Методологічна основа (Methodological Framework)

Методологічну основу дослідження становить втілення принципів DOTMLPFI до процесу набуття та розвитку спроможностей перспективними Кіберсилами ЗС України шляхом розроблення моделі реалізації заходів оборонного планування на основі спроможностей.

Основу DOTMLPFI складають вісім базових компонентів, за якими здійснюється декомпозиція спроможності, а саме:

1. Doctrine (D) – доктринальна база.
2. Organization (O) – організація.
3. Training (T) – підготовка.
4. Materiel (M) – ресурсне забезпечення.
5. Leadership (L) – управління та лідерство.
6. Personnel (P) – персонал.
7. Facility (F) – військова інфраструктура.
8. Interoperability (I) – взаємосумісність.

Приклади застосування методу DOTMLPFI в оборонних відомствах провідних держав світу дають змогу ширше осягнути стратегію м'якого впровадження Кіберсил в систему МО України.

Система DOTMLPFI базується на оборонних спроможностях НАТО. Альянс НАТО є світовим лідером у сфері кібероборони завдяки продуманій стратегії захисту цифрового простору, ефективній координації між союзниками та розвиненій інфраструктурі кібербезпеки. Ще у 2008 році Північноатлантичний альянс визнав кіберпростір окремим театром бойових дій, а з 2016 року прирівняв його до традиційних сфер війни – суші, моря, повітря і космосу. Це свідчить про те, що НАТО розглядає кібератаки не просто як загрозу, а як серйозний виклик, що може мати критичні наслідки для національної безпеки. Війна рф проти України наочно продемонструвала наслідки кібератак на кіберпростір та інформаційне поле України в цілому. Необхідність набуття ЗС України спроможностей щодо кібероборони держави є обґрунтованою.

Розробити модель реалізації заходів ОП для набуття та розвитку спроможностей перспективними Кіберсилами ЗС України пропонується за допомогою використання методології оцінювання спроможностей, яка складається із чотирьох етапів [19]:

1. Підготовчий етап.
2. Аналіз вимог.
3. Аналіз недоліків.
4. Аналіз рішення.

За цією методологією підготовчий етап передбачає створення робочої групи відповідно до предмета оцінювання. Зміст етапу аналізу вимог зводиться до визначення вимог до спроможностей із врахуванням особливостей завдання, умов, показників оцінювання, стандартів тощо. Вважатимемо ці два етапи виконаними, результатом чому є сформована множина необхідних спроможностей ЗС України з ведення протиборства у кіберпросторі [12]. А, відповідно, на основі імплементації у дослідженні третього та четвертого етапів зазначеної методології буде розроблено модель реалізації заходів ОП для набуття і розвитку спроможностей перспективними Кіберсилами ЗС України на основі DOTMLPFI.

Спроможності висвітлюють та є показниками здатності носіїв спроможностей досягнути бажаного результату (ефекту) в операції (бойових діях) військ (сил) [1]. Такими здатностями типових носіїв спроможностей ЗС України щодо ведення протиборства у кіберпросторі (кібероборони) є [11]:

здатність до проведення інформаційних заходів оборони держави;

створення системи кібероборони для ведення протиборства в інформаційному просторі (включаючи кіберпростір);

здатність до забезпечення ефективного кіберзахисту власної інформаційної інфраструктури (критичної інформаційної інфраструктури), проведення превентивних дій щодо виявлення, реагування на кібератаки та інциденти кібербезпеки, усунення їх наслідків в умовах ведення противником кіберрозвідки та інтенсивного кібервпливу (кібератак);

здатність до ведення кіберрозвідки та кібердорозвідки в інформаційно-телекомунікаційних мережах та системах державного, приватного і військового призначення (об'єктів критичної інфраструктури) противника для здобуття інформації про кіберінфраструктуру противника, її призначення, місцезнаходження, технологічні процеси, уразливість, встановлення прихованого контролю, перехоплення та дешифрування керуючих і ресурсних даних та інформації;

здатність до підготовки та проведення скоординованих демонстраційних кібердій (кібервпливу) у кіберпросторі щодо запобігання виникненню воєнних конфліктів, стримування та відсічі воєнній агресії в кіберпросторі;

здатність організовувати підготовку та проводити кібердії (кібервпливи, кібератаки) із застосуванням усіх видів кіберзброї або захоплення (виведення з ладу, отримання контролю), заподіяння шкоди (каскадний ефект), порушення функціонування об'єктів критичної та інформаційної інфраструктури противника з одночасним приховування слідів своєї діяльності в кіберпросторі;

застосування апаратно-програмних комплексів кібербезпеки, засобів з кіберзахисту, кіберзброї для вирішення завдань кіберборотьби.

Процес набуття та розвитку перелічених спроможностей перспективних Кіберсил ЗС України потенційно може спричинити додаткові видатки з державного бюджету. Тому при обґрунтуванні раціональності реалізації тих чи інших заходів ОП за цим напрямом пропонуємо використовувати показник повернення інвестицій, в англомовній літературі – *return of investment* (ROI). Показник повернення інвестицій P_{ROI} оперує величиною можливого фінансового збитку внаслідок дій противника у кіберпросторі та витраченими коштами на кібероборону:

$$P_{ROI} = \frac{P_{loss} - P_{cost}}{P_{loss}}, \quad (1)$$

де, P_{loss} – можливий фінансовий збиток, грн;

P_{cost} – витрачені кошти на кібероборону, грн;

$0 < P_{cost} < P_{loss}$;

$0 \leq P_{ROI} \leq 1$.

Тобто витрата мільйону гривень на кібероборону, завдяки якій було захищено кіберінфраструктуру від деструктивних дій противника, що потенційно могли призвести до фінансового збитку у десять мільйонів гривень, дасть змогу отримати значення $P_{ROI} = 0{,}9$ (90%). За числовим значенням показника P_{ROI}, знаючи критерій раціональності реалізації заходів з кібероборони, можливо судити про доцільність таких заходів. Утім, обґрунтування зазначеного критерія раціональності є окремим напрямом дослідження.

Результати та обговорення (Results and Discussions)

Описаний вище стан справ доводить необхідність та підтверджує задекларований в Стратегії кібербезпеки України курс на створення Кіберсил як окремого роду військ (сил) ЗС України, завдяки чому останні зможуть набути спроможностей до виконання поставленого їм завдання на підготовку та ведення кібероборони України. З метою ефективного виконання покладеного завдання Кіберсилам ЗС України після (у разі) формування необхідно набути попередньо наведених спроможностей з ведення протиборства у кіберпросторі.

Беручи до уваги те, що перші два пункти обраної за основу методології оцінювання спроможностей [19] реалізовані безпосередньо у вигляді переліку спроможностей, модель реалізації заходів ОП для набуття й розвитку спроможностей перспективними Кіберсилами ЗС України буде розроблено як результат виконання етапів аналізу недоліків спроможностей та аналізу рішення. Імплементацію цих етапів методології оцінювання спроможностей пропонується здійснювати за кожним із восьми базових компонентів DOTMLPFI. Для цього кожен із восьми базових компонентів спроможностей ЗС України із ведення протиборства у кіберпросторі буде описано за формою:

потенціал, якого можна досягнути, реалізувавши набуті спроможності;

існуючий стан (проблема) спроможностей;

заходи для рішення проблеми, які дозволять досягнути потенціалу спроможностей.

Умовно структуру моделі реалізації заходів ОП для набуття та розвитку спроможностей перспективних Кіберсил ЗС України можна представити у вигляді рис. 1 (для кожного базового компонента спроможностей DOTMLPFI).

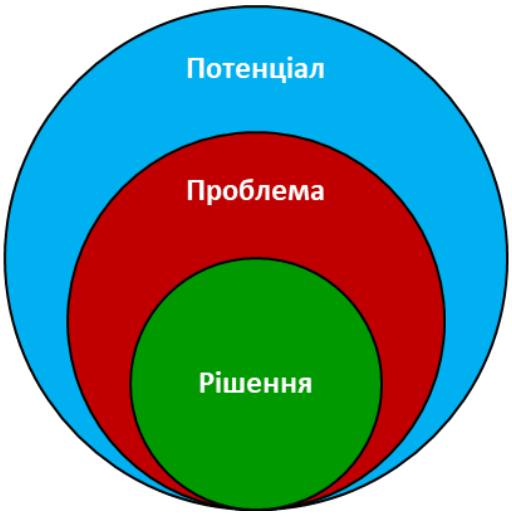


Рисунок 1. Структура моделі реалізації заходів ОП для кожного базового компонента спроможностей DOTMLPFI

Переходячи до безпосереднього викладу основного змісту моделі реалізації заходів ОП для набуття та розвитку спроможностей перспективними Кіберсилами ЗС України з ведення протиборства у кіберпросторі, необхідно зазначити, що вона не є догмою, постулатом чи керівництвом до дії. Метою розроблення цієї моделі є означення проблемних напрямів, які потрібно розвивати, та орієнтовних заходів за цими напрямами, котрі можуть бути корисними для досягнення потенціалу від набуття зазначених спроможностей.

Доктринальна база (D). Законодавство України та доктринальна база ЗС України у сфері кібербезпеки, кібероборони, а також ведення військових операцій у кіберпросторі вимагають розвитку (удосконалення) у напрямі уніфікації, систематизації та ієрархізації термінологічного апарату, утвореного низкою нормативно-правових актів та галузевих керівних документів. Сьогодні не виділені межі застосування кіберпростору у воєнних цілях.

Надане в Законі України [10] визначення кіберпростору характеризує його у цивільному сенсі, не даючи законних підстав вважати кіберпростір середовищем ведення операцій. Кібероборона, відповідальність за підготовку та ведення якої несе МО України та Генеральний штаб ЗС України, передбачає не лише військові, а й економічні, політичні, правові, соціальні та інші заходи. При цьому не зрозумілими є механізми та алгоритми реалізації останніх. У доктринальній базі не надано зв'язок між кібероборoною та кіберборотьбою, попри те, що останні дослідження термінологічного апарату за означеним напрямом [20] обґрунтовують необхідність запровадження чіткого взаємозв'язку цих двох понять. Окрім цього, у термінологічному апараті на одному рівні існують такі терміни, як "кібердії" та "дії у кіберпросторі", які де-факто позначають одне і те саме поняття. Тобто наявний певний дубляж та підміна понять у доктринальній базі.

Потенціалом удосконалення та врегулювання доктринальної бази є можливість однозначно трактувати, описувати та класифікувати дії у кіберпросторі, та, як наслідок, оцінювати їх ефективність. Відповідно, ефективність виконання завдань перспективними Кіберсилами ЗС України у разі їх формування стане одним із головних критеріїв оцінювання доцільності існування цього роду військ (сил). Без уніфікації термінологічного апарату у галузі кібероборони, кібербезпеки та кіберборотьби більш ніж ймовірним є складність у чіткому визначенні завдань, повноважень та сфери відповідальності Кіберсил ЗС України.

Можливим рішенням проблеми доктринальної бази для реалізації потенціалу набуття спроможностей з ведення протиборства у кіберпросторі перспективними Кіберсилами ЗС України є проведення спільного комплексного дослідження із залученням представників за військовою, технічною та правничою галузями у межах, принаймні, науково-дослідної роботи. Таке дослідження має переформатувати доктринальну базу України у частині, що стосується ведення протиборства у кіберпросторі, забезпечити чіткість та однозначність у розподілі повноважень складових Сектору безпеки і оборони України щодо забезпечення кібербезпеки держави.

Організація (O). Наразі в структурі МО України функціонують органи військового управління та військові формування, які виконують визначені їм завдання щодо кібероборони України. А саме, це Головне управління радіоелектронної та кіберборотьби Генерального штабу ЗС України, Головне управління зв'язку та кібербезпеки Генерального штабу ЗС України та Війська зв'язку та кібербезпеки ЗС України. Проблема полягає в тому, що наразі немає чітко вираженого розподілу завдань та повноважень між цими суб'єктами забезпечення кібероборони держави, що породжує невизначеність у відповідальності за вказаний напрям діяльності ЗС України.

Потенціалом формування Кіберсил ЗС України як окремого роду військ (сил), завданням якого буде виконання військових заходів з підготовки та ведення кібероборони держави, є усунення дублювання повноважень між організаційними структурами МО України за вказаним напрямом, побудова ієрархічної системи управління кібероборoною та можливість масштабування.

Рішення організаційної проблеми спроможностей ЗС України з ведення протиборства у кіберпросторі є однозначним – формування Кіберсил як окремого роду військ (сил) ЗС України з покладанням на нього повноважень щодо виконання військових заходів з підготовки та ведення кібероборони України.

Підготовка (Т). Підготовка є невіддільною частиною системи забезпечення кібероборони держави. Сьогодні цикл підготовки військових фахівців з кібербезпеки та їх цільового застосування у системі МО України та ЗС України є незамкнутим. Провідним військовим закладом вищої освіти, який готує офіцерів тактичної рівня за напрямом інформаційних технологій та, зокрема, кібербезпеки, є Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут. Втім, повсюдним явищем є призначення випускників, після закінчення навчання та здобуття відповідного фаху, на посади за спорідненими військово-обліковими спеціальностями, наприклад – командир взводу зв'язку механізованого (танкового) батальйону, офіцер штабу батальйону тощо. Підготовка військового персоналу з кібербезпеки сержантської ланки існує лише в дуже узагальненому вигляді, так як переважна більшість профільних посад є офіцерськими.

Водночас, незважаючи на досвід НАТО зі створення кіберполігонів для симуляції та моделювання воєнних дій у кіберпросторі та значну кількість досліджень у сфері кібербезпеки, які обґрунтовують доцільність впровадження такого досвіду в систему підготовки ЗС України, наразі підготовка військових фахівців з кібербезпеки не здійснюється з використанням кіберполігонів. Доцільність впровадження кіберполігонів в систему підготовки спеціалістів ЗС України з кібербезпеки підсилюється стрімким зростанням кількості інформаційно-комунікаційних систем в органах військового управління ЗС України та складністю їхньої технічної організації.

Потенціалом побудови замкненої системи підготовки військових фахівців з кібербезпеки та їх цільового застосування у відповідних підрозділах ЗС України, наприклад, у перспективних Кіберсилах ЗС України, є сталий рівень навченості та злагодженості підрозділів, призначених для ведення протиборства у кіберпросторі, їх спроможність до виконання поставлених завдань із підготовки та ведення кібероборони держави.

З огляду на стійку невизначеність кіберпростору та процесів, що відбуваються у ньому, військових фахівців з кібербезпеки мають готувати на засадах творчого підходу до виконання поставлених завдань, гнучкості та здатності пристосовуватися та змінювати характер дій залежно від обстановки, що склалася. Кіберспеціалісти ЗС України мають вільно володіти стеком прикладних інформаційних технологій та вміти їх застосувати на практиці без суттєвого звернення до технічної літератури. У військових закладах вищої освіти програми спеціальностей за напрямом кібербезпеки мають регулярно оновлюватися, з урахуванням появи нових форм та способів ведення кіберборотьби, розвитком інформаційних технологій. Співпраця з НАТО у процесі підготовки також є важливою, необхідно брати участь у спільних навчаннях з кібероборони, таких як Locked Shields та ін.

Ресурсне забезпечення (М). Набуття та розвиток спроможностей з ведення протиборства у кіберпросторі напряму залежать від достатності та якості ресурсного забезпечення.

Сьогодні в існуючих підрозділах в системі МО України та ЗС України, відповідальних за підготовку та ведення кібероборони, наявні певні зразки антивірусного програмного забезпечення для боротьби з шкідливим програмним кодом, програмно-апаратні комплекси сканування комп'ютерних мереж для виявлення та нейтралізації проникнення з боку противника в інформаційно-комунікаційні системи. Водночас, процес оснащення ЗС України кіберзброєю перебуває на етапі визначення тактико-технічних вимог до неї.

Потенціалом створення достатнього, якісного та передового у технологічному відношенні ресурсного забезпечення набуття й розвитку спроможностей з ведення протиборства у кіберпросторі перспективними Кіберсилами ЗС України є можливість

розроблення власних технологій та програмних рішень з кіберзахисту та кібервпливу, взаємодія у сфері кібероборони з державами-партнерами, використання технологій штучного інтелекту для аналізу атак та кіберрозвідки.

У разі ухвалення рішення на формування в системі МО України Кіберсил, необхідним є озброєння цього роду військ (сил) найсучаснішим обладнанням, що є на ринку. Окрім цього, зважаючи на часті випадки проникнення противника в кіберінфраструктуру об'єктів критичної інформаційної інфраструктури України, спричиненого використанням програмного забезпечення, виробленого компаніями-нерезидентами, необхідним є нарощування власних розробок України у галузі кібербезпеки. Створення власних, внутрішніх програмних (програмно-апаратних) засобів з кіберзахисту та кібервпливу дадуть можливість незалежно проводити дії або операції у кіберпросторі. У цьому ключі та з метою отримання переваги над противником у кіберпросторі при розробленні власного та закупівлі кіберозброєння необхідно звернути увагу на ті зразки, які оснащені алгоритмами (технологіями) штучного інтелекту для автоматизованого виявлення кіберрозвідки (кібератак) противника, а також вразливостей власної кіберінфраструктури. Сьогодні використання штучного інтелекту в кібербезпеці є однією із найактуальніших тенденцій.

Не менш важливим питанням ресурсного забезпечення є фінансове забезпечення. Оскільки військові фахівці з кібербезпеки мають вільно володіти усім спектром прикладних інформаційних технологій, це робить їх конкурентноздатними на ринку праці в той час, коли їх грошове забезпечення в ЗС України не надто відрізняється від забезпечення військовослужбовців інших видів (родів) військ (сил).

Управління та лідерство (L). Управління та лідерство є рушійним базовим компонентом будь-якої спроможності. В умовах прямо пропорційної залежності результатів ведення протиборства у кіберпросторі від знання та володіння прикладних інформаційних технологій та здатності до їх імплементації, забезпечення принципів єдиноначальства та лідерства є складним. Це підсилюється тим, що військових фахівців з кібербезпеки у військових закладах вищої освіти готують з явною технічною направленістю, звертаючи недостатню увагу на методичні та лідерські якості як керівника.

Потенціалом удосконалення компоненти управління та лідерства спроможностей з ведення протиборства у кіберпросторі перспективних Кіберсил ЗС України є підвищення рівня злагодженості відповідних підрозділів, здорова конкуренція серед особового складу за кар'єрне просування та побудова ефективної системи управління воєнними діями у кіберпросторі.

Водночас, операції у кіберпросторі, як і звичайні операції військ (сил), вимагають чіткої ієрархічної системи управління. Тому лідер у перспективних Кіберсилах ЗС України має володіти як знаннями та навичками прикладного застосування інформаційних технологій в питаннях кібероборони, так і лідерськими здібностями – показувати приклад, вести за собою колектив, заохочувати найкращих. Лідерський підхід передбачає кар'єрне зростання найкращих та найвмотивованіших.

Персонал (P). Особливості підготовки та цільового застосування військових фахівців з кібербезпеки було розглянуто під час аналізу базового компонента спроможності "Підготовка (T)". Проте, є певні проблемні питання, пов'язані з патріотичною налаштованістю та мотивацією особового складу, який є носієм спроможностей з ведення протиборства у кіберпросторі. Мотивація та патріотична налаштованість персоналу часто є взаємопов'язаними аспектами. Водночас, такі проблеми існують не тільки у підрозділів кібероборони системи МО України, а й в інших організаційних структурах.

Потенціалом від забезпечення перспективних Кіберсил ЗС України кваліфікованим, патріотично налаштованим та мотивованим особовим складом (персоналом), який відповідає визначеним вимогам до спроможностей з ведення протиборства у кіберпросторі, є

недопущення кадрового голоду у підрозділах цього роду військ (сил) та здатність підрозділів до виконання завдань за призначенням завдяки ретельному відбору кандидатів.

Для реалізації зазначеного потенціалу необхідно здійснювати відбір кандидатів на проходження служби в перспективних Кіберсилах ЗС України на основі фахових здібностей, проводити постійне мотивування персоналу та підвищувати рівень патріотизму підрозділів шляхом створення привабливих умов служби та справедливості в управлінських рішеннях.

Окремим напрямом удосконалення забезпечення кваліфікованим персоналом є залучення цивільних фахівців з кібербезпеки, яких в Україні є чимало, під час особливого періоду або воєнного стану до виконання завдань з кібероборони України як альтернатива їх мобілізації на загальних засадах до загальновійськових з'єднань. Прикладом цьому є програма CyberGuard у США, яка дозволяє ІТ-експертам із приватного сектору працювати з військовими підрозділами.

Військова інфраструктура (F). Рівень військової інфраструктури за напрямом ведення протиборства у кіберпросторі можливо оцінити за наявністю та станом об'єктів, окремих споруд і пов'язаних з ними комунікацій, а також землі, призначені для забезпечення підготовки і ведення кібероборони держави, їх розміщення, пристосованість до забезпечення життєдіяльності та підготовки.

Потенціал забезпечення військовою інфраструктурою розкривається у можливості належної підготовки підрозділів та військових частин до виконання заходів з кібероборони держави та підвищенні ефективності застосування кіберзброї, якою їх буде оснащено.

Наразі в ЗС України відсутня мережа кіберполігонів, що ускладнює процес підготовки фахівців з кібербезпеки. Окрім цього, для набуття й розвитку спроможностей перспективними Кіберсилами ЗС України необхідне нарощення військової інфраструктури для базування та виконання заходів за призначенням, яка буде відповідати всім технічним потребам цього роду військ. Такі об'єкти мають бути сумісними з озброєнням Кіберсил.

Україна вже розширює державні дата-центри для захисту інформації, створені проєкти резервних серверів для захисту державних даних, проте проблемою є критична залежність від цивільної інфраструктури (комерційних хмарних сервісів).

Взаємосумісність (I). Наразі проблема взаємосумісності полягає у децентралізації відповідальності за кібероборону України серед органів військового управління. Різні завдання та повноваження щодо ведення протиборства у кіберпросторі визначені для різних організаційних структур, між якими немає підпорядкованості. Більше того, низькою є взаємосумісність між суб'єктами Національної системи кібербезпеки України, до якої, окрім МО України, входить Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, та деякі інші органи. Окремим питання є набуття перспективними Кіберсилами ЗС України взаємосумісності з підрозділами кібероборони держав НАТО, враховуючи курс України на вступ до альянсу.

Потенціалом підвищення взаємосумісності щодо ведення протиборства у кіберпросторі є набуття здатності ЗС України до ведення спільних, узгоджених, ефективних та результативних дій з метою досягнення тактичних, оперативних та стратегічних цілей кібероборони.

Для вирішення проблеми взаємосумісності Україна має масштабувати вже розпочату інтеграцію у кібермережу НАТО, визначити для перспективних Кіберсил ЗС України чіткі завдання та межі повноважень на ведення протиборства у кіберпросторі, а також організувати дієві механізми взаємодії цього роду військ (сил) із іншими організаційними структурами МО України, до сфери діяльності яких входить кібербезпека, кіберзахист та кібероборона.

Для повноти розкриття цього питання та його узагальнення варто відобразити основні тези моделі реалізації заходів з ОП для набуття та розвитку спроможностей перспективних Кіберсил ЗС України у вигляді табл. 1.

Таблиця 1. Основні положення моделі реалізації заходів оборонного планування

	Потенціал	Проблема	Рішення
D	– однозначність в трактуванні, описі, класифікації та оцінюванні ефективності дій у кіберпросторі; – уніфікований термінологічний апарат у галузі кібероборони, кібербезпеки та кіберборотьби; – чіткість визначення завдань, повноважень та сфери відповідальності перспективних Кіберсил	– неоднозначність термінологічного апарату; – дублювання термінів і підміна понять у системі нормативно-правових актів та керівних документів; – відсутність чіткого розподілу завдань щодо підготовки і ведення кібероборони держави; – відсутність єдиної військової доктрини кібероборони; – низький рівень інтеграції кіберстратегії у загальну концепцію ведення війни	– переформатування доктринальної бази у частині, що стосується ведення протиборства у кіберпросторі, забезпечити чіткість та однозначність у розподілі повноважень складових Сектору безпеки і оборони України щодо забезпечення кібербезпеки держави
O	– усунення дублювання повноважень між організаційними структурами МО України за напрямом кібероборони; – побудова ієрархічної системи управління кібероборoною та можливість її масштабування	– відсутність чітко вираженого розподілу завдань та повноважень між суб'єктами забезпечення кібероборони держави; – невизначеність у відповідальності за кібероборону держави	– формування Кіберсил ЗС України як окремого роду військ (сил); – агрегування Кіберсилами усіх визначених спроможностей з ведення протиборства у кіберпросторі
T	– сталий рівень навченості та злагодженості підрозділів, призначених для ведення протиборства у кіберпросторі; – спроможність до виконання поставлених завдань з підготовки та ведення кібероборони держави	– незамкнутість циклу підготовки військових фахівців з кібербезпеки та їх цільового застосування у системі військової освіти	– якісна підготовка військових фахівців з кібербезпеки на засадах творчого підходу та гнучкості; – регулярне оновлення з урахуванням програм спеціальностей за напрямом кібербезпеки у військових закладах вищої освіти; – співпраця з НАТО у процесі підготовки та спільних навчань
M	– можливість розроблення власних технологій та програмних рішень з кіберзахисту та кібервпливу; – взаємодія у сфері кібероборони з державами – партнерами НАТО; – використання технологій штучного інтелекту для аналізу атак та кіберрозвідки	– процес оснащення ЗС України кіберзброєю перебуває на етапі визначення тактико-технічних вимог до неї	– озброєння перспективних Кіберсил ЗС України найсучаснішим обладнанням; – нарощування власних розробок України у галузі кібербезпеки; – використання алгоритмів (технологій) штучного інтелекту для автоматизованого виявлення кіберрозвідки (кібератак) противника, вразливостей кіберінфраструктури; – гідне фінансове забезпечення військових фахівців з кібербезпеки
L	– підвищення рівня злагодженості підрозділів кібероборони; – здорова конкуренція серед особового складу за кар'єрне просування у сфері кібероборони; – побудова ефективної системи управління воєнними діями у кіберпросторі	– складність у забезпеченні принципів єдиноначальства та лідерства у предметній області протиборства у кіберпросторі; – переважна технічна направленість підготовки військових фахівців з кібербезпеки; – низький рівень методичних та лідерських якостей	– підвищення лідерських здібностей військових фахівців з кібербезпеки; – кар'єрне зростання найкращих та найвмотивованіших у підрозділах кібероборони; – перейняття досвіду НАТО з лідерства у підрозділах кібероборони

Продовження таблиці 1. Основні положення моделі реалізації заходів оборонного планування

P	– недопущення кадрового голоду у підрозділах перспективних Кіберсил ЗС України; – здатність підрозділів до виконання завдань за призначенням завдяки детальному відбору кандидатів	– недостатній рівень підготовленості персоналу з кібербезпеки та кібероборони за фахом; – проблемні питання, пов'язані з патріотичною налаштованістю та мотивацією особового складу	– відбір кандидатів на проходження служби в перспективних Кіберсилах ЗС України на основі фахових здібностей; – постійне мотивування персоналу та підвищення рівня патріотизму підрозділів шляхом створення привабливих умов служби та справедливості в управлінських рішеннях
F	– можливість належної підготовки підрозділів та військових частин до виконання заходів з кібероборони держави; – підвищення ефективності застосування кіберзброї	– відсутність системи кіберполігонів для симуляції та моделювання ведення протиборства у кіберпросторі	– нарощення військової інфраструктури для базування та виконання заходів з кібероборони; – відповідність військової інфраструктури потребам перспективних Кіберсил ЗС України; – сумісність об'єктів військової інфраструктури з озброєнням Кіберсил
I	– набуття здатності ЗС України до ведення спільних, узгоджених, ефективних та результативних дій з метою досягнення тактичних, оперативних та стратегічних цілей кібероборони	– децентралізація відповідальності за кібероборону України серед органів військового управління; – низька взаємосумісність між суб'єктами Національної системи кібербезпеки України	– масштабування розпочатої інтеграції у кібермережу НАТО; – визначення чітких завдань та повноважень на ведення протиборства у кіберпросторі; – організація дієвих механізмів взаємодії із іншими структурами МО України, до сфери діяльності яких входить кібербезпека, кіберзахист та кібероборона; – взаємосумісність з підрозділами кібероборони держав НАТО

Висновок (Conclusion)

Отже, у статі було запропоновано рекомендації щодо реалізації заходів з оборонного планування для набуття й розвитку спроможностей перспективними Кіберсилами ЗС України на основі DOTMLPFI. Розроблена модель являє собою опис кожного з восьми базових компонентів спроможностей ЗС України з ведення протиборства у кіберпросторі за формою: потенціал, якого можна досягнути, реалізувавши набуті спроможності; існуючий стан (проблема) спроможностей; заходи для вирішення проблеми, які дозволять досягнути потенціалу спроможностей. Реалізація та впровадження цієї моделі стануть суттєвим кроком до зміцнення національної безпеки України, дадуть змогу ефективно здійснювати підготовку та ведення кібероборони, протидіяти агресії у цифровій сфері.

Рекомендації (Recommendations)

Матеріали статті можуть бути корисними для організаційних структур МО України та Генерального штабу ЗС України, які у разі ухвалення остаточного рішення на формування Кіберсил будуть забезпечувати реалізацію заходів оборонного планування для набуття і розвитку ними відповідних спроможностей. Окрім цього, праця може становити інтерес для науковців, науково-педагогічних працівників та здобувачів вищої освіти за напрямом тематики статті або суміжними напрямами.

Використані джерела

1. Deniezhkin, M. M., Nalyvaiko, A. D., & Polyayev, A. I. (2017). Features of Defense Planning in NATO Member States Based on Capabilities. *Collection of Scientific Papers of the Center for Military-Strategic Studies, National Defense University of Ukraine, 2* (60), 34–38. https://doi.org/10.33099/2304-2745/2017-2-60/34-38.
2. Nalyvaiko, A. D., Polyayev, A. I., & Nalyvaiko, L. P. (2019). Theoretical Foundations of Building a Functional Model of the Defense Planning Process for Defense Forces. *Collection of Scientific Papers of the Center for Military-Strategic Studies, National Defense University of Ukraine, 2* (66), 35–41. https://doi.org/10.33099/2304-2745/2019-2-66/35-41.
3. Nalyvaiko, A. D., & Polyayev, A. I. (2021). Approaches to Developing a Functional Defense Management Model. *Social Development and Security*, *11* (3), 20–29. https://doi.org/10.33445/sds.2021.11.3.2.
4. Pavlikovsky, A., Frolov, V., & Saghanyuk, F. (2020). *Defense Reform: A Systematic Approach to Defense Management*. (Edited by A. Syrotenko). National University of Defense of Ukraine.
5. Valtonen, I., Rautio, S., & Salmi, M. (2022). Capability Development in Hybrid Organizations: Enhancing Military Logistics with Additive Manufacturing. *Progress in Additive Manufacturing. 7*, 1037–1052. https://doi.org/10.1007/s40964-022-00280-z.
6. Korendovych, V. S., & Chirikalov, O. S. (2020). The Problem of Decentralization of Command and Control in Hybrid Warfare. *Development of Theory and Methodology, 3* (12), 32–40. https://doi.org/10.33099/2618-1614-2020-12-3-32-40.
7. Shchipansky, P. V., Saghanyuk, F. V., & Mudrak Y. M. (2021). Defense Management: Approaches to Managing the Defense Planning Process. *Collection of Scientific Papers of the Center for Military-Strategic Studies, National Defense University of Ukraine*, *1* (71), 52–58. https://doi.org/10.33099/2304-2745/2021-1-71/52-58.
8. Nalyvaiko, A. D. (2024). Justification of Directions for Improving Strategic Planning in the Defense Sector. *Collection of Scientific Papers of the Center for Military-Strategic Studies, National Defense University of Ukraine*, *1* (80), 27–33. https://doi.org/10.33099/2304-2745/2024-1-80/27-33.
9. Lutsyk, Y. O., Parkhomenko P. P., Demeniev O. M., & Alimov D. I. (2023). Analysis of the Defense Planning System Based on Capabilities, Considering the Leading Experience of NATO Member States. *Modern Economics*, *41*, 73–78. https://doi.org/10.31521/modecon.V41(2023)-11.
10. Law of Ukraine *"On the Basic Principles of Cybersecurity Provision in Ukraine"* No. 2163-VIII (2017, 05 Aug. 10): as of June 28, 2024. https://zakon.rada.gov.ua/laws/show/2163-19
11. President of Ukraine. (2021). *On the Decision of the National Security and Defense Council of Ukraine of August 20, 2021 "On the Strategic Defense Bulletin of Ukraine"* (473/2021). https://zakon.rada.gov.ua/laws/show/473/2021#Text
12. President of Ukraine. (2021). *On the Decision of the National Security and Defense Council of Ukraine of May 14, 2021, "On the Cybersecurity Strategy of Ukraine"* (447/2021). https://zakon.rada.gov.ua/laws/show/447/2021#Text
13. *Draft Law on Cyber Forces of the Armed Forces of Ukraine.* https://itd.rada.gov.ua/billinfo/Bills/Card/45453
14. Horhulenko, V. A. (2024). Cyber Warfare in Modern Conflicts: Advanced Experience, Trends, and Development Patterns. *Modern Information Technologies in Security and Defense*, *2* (50), 11–28. https://doi.org/10.33099/2311-7249/2024-50-2-11-28.
15. Krykun, P., Pavlenko, V., Korendovych, V., Yasenko, S., & Tkach, M. (2024). Development of the National Defense Planning System of Ukraine Based on Euro-Atlantic Principles: Military-Historical Analysis. *Social Development and Security*, *14* (3), 14–32. https://doi.org/10.33445/sds.2024.14.3.2.
16. Fediienko, O. P. (2024). Modern Trends in Normative Support for Institutional Formation of Cyber Forces (Cyber Troops): The Experience of Some NATO Countries. *Information and Law, 1* (48), 150–161. https://doi.org/10.37750/2616-6798.2024.1(48).300800.

17. Nagy, J., Foltin, P., & Ondryhal, V. (2022). Use of Big Data Analysis to Identify Possible Sources of Supply Chain Disruption through the DOTMLPFI Method. *LogForum*, *18* (3), 309–319. http://doi.org/10.17270/J.LOG.2021.731.
18. Llopis Sanchez, S., Sandoval Rodriguez-Bermejo, D., Daton Medenou, R., Pasqual de Riquelme, R., Torelli, F., & Maestre Vidal, J. (2022). Tackling Verification and Validation Techniques to Evaluate Cyber Situational Awareness Capabilities. *Mathematics, 10*, 2617. https://doi.org/10.3390/math10152617.
19. Tkach, M. Y., & Korendovych, S. A. (2024). *Basics of Defense Management*. National University of Defense of Ukraine.
20. Horhulenko, V. A. (2024). Military-Theoretical Justification of Recommendations for the Development of Terminological Apparatus in the Field of Cyber Warfare. *Modern Information Technologies in Security and Defense*, *3* (51). https://doi.org/10.33099/2311-7249/2024-51-3-41-50.