DOI 10.51369/2707-7276-2024-1(37)-6
УДК 004.056.5:378.1(045)

БОГУШ Володимир Михайлович
ХМЕЛЬНИЦЬКИЙ Микола Олександрович

ПРОПОЗИЦІЇ ЩОДО СИСТЕМНОЇ ПІДГОТОВКИ ФАХІВЦІВ ДЛЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ ДО ДІЯЛЬНОСТІ В КІБЕРПРОСТОРІ

Сучасний кіберпростір є важливим елементом інформаційної сфери й економіки України. Він використовується для здійснення широкого спектру діяльності, включаючи комунікацію, торгівлю, фінанси, освіту й управління. У зв'язку з цим зростає значення забезпечення кібербезпеки, що передбачає захист від кіберзагроз, таких як хакерські атаки, розвідувальні операції та поширення дезінформації.

Служба безпеки України є одним із органів державної влади, відповідальних за забезпечення кібербезпеки України. Для виконання цього завдання СБ України потребує висококваліфікованих кадрів, які мають знання та навички роботи у сферах кібербезпеки й інформаційних технологій.

У статті за результатами аналізу стану базової підготовки фахівців СБ України за спеціальностями 251 «Державна безпека», 256 «Національна безпека» галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» зроблено висновок, що на сьогодні традиційних методів навчання недостатньо для того, щоб відповідати сучасним викликам у сфері кібербезпеки, оскільки потрібні спеціалізовані знання та здатність до швидкого реагування, і немає впорядкованого підходу до підготовки спеціалістів для діяльності в кіберпросторі, що призводить до розриву між теоретичними знаннями та їхнім практичним застосуванням. Це пов'язано з низкою факторів, зокрема недостатньою розробленістю теоретичних основ кібербезпеки, відсутністю єдиних стандартів підготовки фахівців у цій сфері, недостатнім фінансуванням системи освіти тощо.

Пропонується концепція системної підготовки фахівців для вказаної сфери, що поєднує декілька дисциплін і безперервне навчання, ураховує розвиток технологій та інфраструктури кіберпростору України, інтеграцію передових технологічних інструментів, а також вирішення актуальних наукових і методологічних проблем у його різних сферах (економічній, соціальній, психологічній, правовій, культурологічній, системотехнічній, безпеки й ін.).

Згідно з цим підходом підготовка фахівців СБ України для діяльності в кіберпросторі повинна здійснюватися за такими напрямами: інфраструктурним, технологічним, науково-дослідним, які відповідно передбачають підготовку фахівців, які будуть відповідати за управління кіберінфраструктурою України, протидію кібератакам і забезпечення кібербезпеки критичної інфраструктури, розробляти та впроваджувати нові технології кібербезпеки, проводити експертизу кіберзагроз, займатися дослідженнями в галузі кібербезпеки, розробкою нових методів і засобів захисту від кіберзагроз.

Пропонується впровадити в систему освіти СБ України нововведення: розширити перелік дисциплін, які вивчаються в межах підготовки фахівців для діяльності в кіберпросторі; запровадити в навчальний процес інтерактивні методи навчання, такі як проєктна робота, командна робота, моделювання, відеолекції та інші, що дасть можливість підвищити ефективність навчання та практичної підготовки фахівців; створити в СБ України центри кібербезпеки за різними напрямами, які будуть забезпечувати практичну підготовку фахівців.

Реалізація таких заходів дасть змогу забезпечити національну безпеку в цифровій сфері й створити надійний кадровий потенціал СБ України, здатний реагувати на динамічні загрози сьогодення.

Ключові слова: *інформаційна сфера, кіберпростір, компетентність, контррозвідувальний захист, національна безпека, результат навчання, спеціальна операція.*

Постановка проблеми. У контексті реформування Служби безпеки України насамперед потрібно вдосконалити систему підготовки кваліфікованих кадрів, необхідних для виконання відповідних завдань. Чинне законодавство України, зокрема Закон «Про національну безпеку України» [1], визначає, що Служба безпеки України є органом спеціального призначення з правоохоронними функціями, що забезпечує державну безпеку з дотриманням прав і свобод громадян. Важливо відзначити, що СБ України виконує низку важливих завдань, таких як протидія розвідувально-підривній діяльності, боротьба з тероризмом, контррозвідувальний захист суверенітету та територіальної цілісності, забезпечення кібербезпеки й ін.

У зв'язку із зростанням значення кіберпростору й інформаційної сфери виконання правоохоронних функцій органами спеціального призначення дедалі більше пов'язується з цими аспектами. Тому надзвичайно важливо забезпечити ефективну підготовку фахівців, які, маючи знання у сфері кібербезпеки й інформаційних технологій, будуть брати активну участь у протидії кіберзагрозам, забезпеченні безпеки в мережі та захисті від несанкціонованого доступу до інформації.

Розроблення якісної системи підготовки фахівців для Служби безпеки України, що спеціалізуються у сфері кібербезпеки й інформаційних технологій, є критично важливим у сучасному ландшафті загроз кібербезпеці та задля успішного виконання завдань як в умовах реформування СБ України, так і після його завершення.

Наказом Міністерства освіти і науки України від 23.12.2021 № 1423 було затверджено і введено в дію Стандарт вищої освіти для другого (магістерського) рівня галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону», спеціальність 256 «Національна безпека». Відповідно до основних завдань Служби безпеки України базова підготовка фахівців здійснюється в галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» з використанням спеціальностей 251 «Державна безпека» та 256 «Національна безпека (за окремими сферами забезпечення та видами діяльності)». Відповідний вид діяльності погоджується СБ України, яка відповідає за виконання завдань у сфері національної безпеки, з узгодженням із Мініс-

терством освіти і науки України [2]. Спеціальність «Національна безпека» в Службі безпеки України була розширена у 2017 році у напрямку 256.04 «Забезпечення державної безпеки в інформаційній сфері» згідно з наказом Центрального управління СБ України від 04.07.2017 № 410. У 2021 році ця спеціальність була конкретизована до 256.04 «Кіберзахист, забезпечення державної безпеки в інформаційній сфері» згідно з наказом Центрального управління СБ України від 19.05.2021 № 169.

Попри велику актуальність цього питання, на сьогодні ще не визначений упорядкований підхід до підготовки фахівців Служби безпеки України для діяльності в кіберпросторі.

Аналіз останніх досліджень і публікацій. Належний науковий аналіз теоретичних аспектів, пов'язаних із створенням освітніх програм для спеціальності 256 «Національна безпека» (за конкретними сферами забезпечення та видами діяльності), до цього часу не проводився, тому є актуальним розгляд цього питання в сучасних наукових джерелах.

Наше дослідження базується на аналізі системних вимог нормативно-правових документів, які регулюють або стосуються підготовки фахівців у галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону», а саме: Стандарту вищої освіти першого (бакалаврського) рівня галузі знань 25 «Воєнні науки, національна безпека, безпека державного кордону» спеціальності 252 «Безпека державного кордону», затвердженого наказом Міністерства освіти і науки України від 12.12.2018 № 1384; Методичних рекомендацій щодо розроблення стандартів вищої освіти, затверджених наказом Міністерства освіти і науки України від 01.06.2017 № 600 (у редакції наказу Міністерства освіти і науки України від 21.12.2017 № 1648); Стандартів і рекомендацій щодо забезпечення якості в Європейському просторі вищої освіти (ESG).

Метою статті є аналіз розвитку кіберпростору з метою розроблення пропозицій щодо системного підходу до підготовки фахівців для Служби безпеки України, зокрема для діяльності у сфері кібербезпеки.

Виклад основного матеріалу. Згідно із законодавством України, яке регулює забезпечення кібербезпеки, поняття «кіберпростір» визначається як віртуальне середовище, що дозволяє взаємодіяти та спілкуватися, а також реалізовувати суспільні відносини. Воно формується завдяки роботі спільних комунікаційних систем та наданню можливостей для електронних комунікацій, що базуються на використанні мережі Інтернет та інших глобальних мереж передачі даних [2; 5; 6].

Девід Кларк запропонував модель, у якій визначаються чотири рівні кіберпростору [7]:

1. **Фізичний рівень** містить усі апаратні пристрої, які включаються: маршрутизатори, комутатори, носії та супутники, датчики й інші технічні з'єднувачі, як проводові, так і безпроводові. Фізична інфраструктура географічно розташовується в «реальному просторі», отже, є предметом різних національних юрисдикцій.

2. **Логічний рівень** у цілому належить до коду, який включає в

себе як програмне забезпечення, так і протоколи, які в ньому реалізуються.

3. **Рівень контенту** описує всю інформацію, яка створюється, береться, зберігається й обробляється в кіберпросторі. Інформація визначається як знання, що стосуються об'єктів, наприклад, факти, події, речі, процеси або ідеї.

4. **Соціальний рівень** складається з усіх людей, які використовують і визначають характер кіберпростору. Це фактичний інтернет людей та їхні потенційні відносини. Він не стосується інтернету апаратних засобів і програмного забезпечення. За суттю соціальний прошарок включає уряд, приватний сектор, громадянське суспільство й суб'єкти технічного співтовариства.

Основні напрями підготовки фахівців за спеціальністю 256.04 «Кіберзахист, забезпечення державної безпеки в інформаційній сфері» відповідно до моделі Д. Кларка та їхній зв'язок з основними галузями знань представлено на рис. 1.

Беручи до уваги запропоновану Д. Кларком концепцію, ми вирішили її доповнити ще деякими значущими елементами, ураховуючи мінливість світових засад розвитку кіберпростору. На нашу думку, кіберпростір можна концептуалізувати та класифікувати за різними рівнями, кожен з яких представляє певний шар або вимір цифрового середовища. Ці рівні допомагають зрозуміти й організувати різні аспекти кіберпростору:

1. **Рівень фізичної інфраструктури**. Цей рівень охоплює матеріальне обладнання та фізичні компоненти, які складають кіберпростір, такі як сервери, центри обробки даних, мережеві кабелі та комунікаційна інфраструктура.

2. **Мережевий рівень.** Мережевий рівень зосереджується на підключенні та комунікаційних протоколах, які забезпечують передачу даних між пристроями. Він включає в себе інтернет, інтрамережі та різні мережеві технології.

3. **Рівень даних**. На рівні даних основна увага приділяється інформації та цифровому контенту, яким обмінюються в кіберпросторі. Сюди входять бази даних, файли, документи та всі форми цифрової інформації.

4. **Рівень додатків.** Цей рівень включає в себе програмне забезпечення та програми, які працюють у кіберпросторі. Сюди входять веббраузери, поштові клієнти [Email client], платформи соціальних мереж та інші програми, які полегшують взаємодію з користувачем.

5. **Рівень ідентичності.** Рівень ідентичності охоплює цифрові ідентичності осіб, організацій і пристроїв у кіберпросторі. Він включає облікові записи користувачів, механізми автентифікації та цифрові сертифікати.

6. **Поведінковий рівень.** На поведінковому рівні основна увага приділяється діям, взаємодії та поведінці користувачів і організацій у кіберпросторі. Сюди входять діяльність в інтернеті, моделі спілкування та цифрові транзакції.

7. **Рівень безпеки.** Рівень безпеки стосується заходів і протоколів, що застосовуються для захисту кіберпростору від кіберзагроз. Сюди вхо-

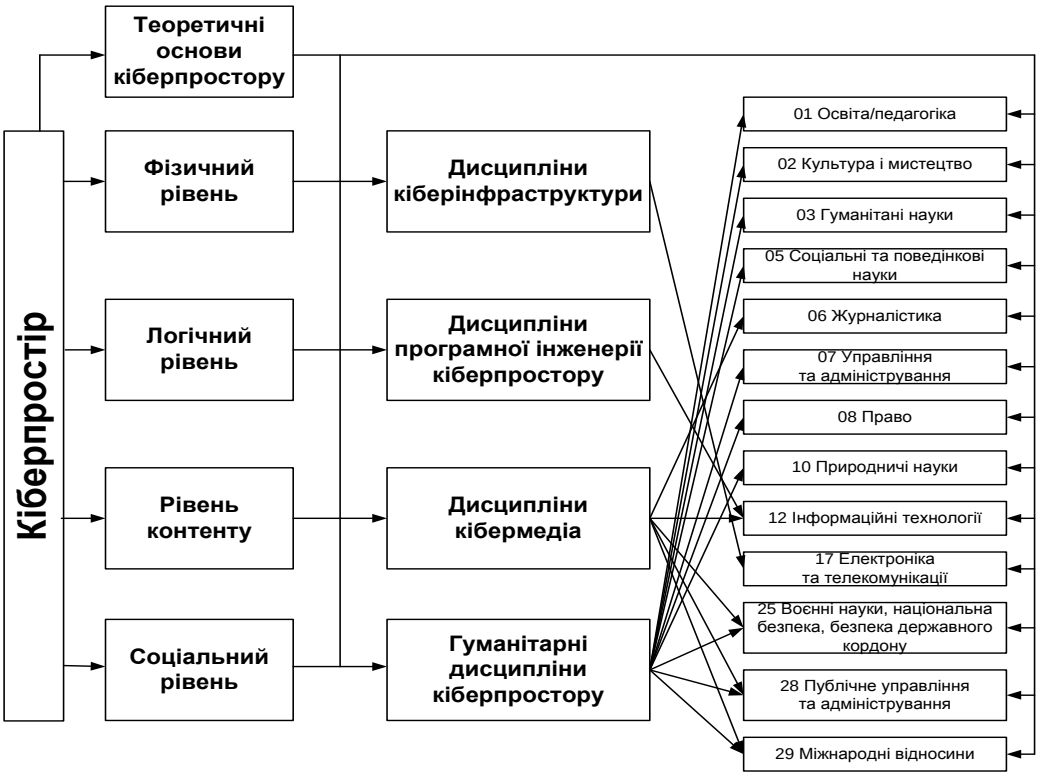

Рисунок 1 – Основні напрями підготовки фахівців до діяльності в кіберпросторі відповідно до моделі Д. Кларка (узагальнено авторами)

дять брандмауери, шифрування, антивірусне програмне забезпечення й інші інструменти кібербезпеки.

8. **Правовий рівень**. Це правові та політичні рамки врегулювання діяльності в кіберпросторі. Він включає міжнародні договори, національні закони й організаційну політику, пов'язану з кібербезпекою та цифровим урядуванням. До цього можна віднести як приклад NIST Cybersecurity Framework, Anti-Spam Act, Personal Information Protection and Electronic Documents Act тощо [9].

9. **Економічний рівень.** На економічному рівні кіберпростір розглядається з погляду його впливу на економічну діяльність. Сюди входять електронна комерція, цифрові валюти, онлайн-транзакції та ширша цифрова економіка.

10. **Соціальний рівень**. Соціальний рівень включає взаємодії та відносини, що формуються в кіберпросторі. Сюди входять платформи соціальних мереж, онлайн-спільноти та вплив цифрових технологій на суспільство.

11. **Політичний рівень**. Політичний рівень стосується впливу кіберпростору на політичну діяльність та управління. Сюди входять кібервійни, державна кібердіяльність і роль кіберпростору в геополітичних стратегіях.

12. **Глобальний рівень**. На глобальному рівні кіберпростір розглядається як безмежне та взаємопов'язане середовище, що виходить за межі національних кордонів. Він включає в себе міжнародне співробітництво, кібернетичні норми та глобальні виклики кібербезпеці.

Усі ці рівні взаємопов'язані, і зміни або події на одному рівні можуть спричиняти наслідки для інших. Розуміння цих рівнів має вирішальне значення для розроблення комплексних стратегій кібербезпеки, цифрового врядування та навігації в складному ландшафті кіберпростору, що являє собою взаємозалежність між цим і якісною та послідовною моделлю створення практичних і сучасних за своєю суттю освітньо-професійних програм, робочих навчальних програм, навчально-методичного забезпечення тощо.

Для вивчення фізичного рівня моделі Д. Кларка можна сформувати цикли навчальних дисциплін кіберінфраструктури або відповідні освітні програми для галузі знань 17 «Електроніка та телекомунікації». Для вивчення логічного рівня моделі Д. Кларка можна сформувати цикли навчальних дисциплін програмної інженерії кіберпростору або відповідні освітні програми для галузі знань 12 «Інформаційні технології».

Для вивчення рівня контенту моделі Д. Кларка можна сформувати цілу низку циклів навчальних дисциплін кібермедіа або відповідні освітні програми для таких галузей знань: 06 «Журналістика»; 28 «Публічне управління та адміністрування», 25 «Воєнні науки, національна безпека, безпека державного кордону»; 12 «Інформаційні технології»; 29 «Міжнародні відносини».

Для вивчення соціального рівня моделі Д. Кларка можна сформувати цілий спектр циклів гуманітарних навчальних дисциплін кіберпростору, а також освітніх програм великої кількості галузей знань: 01 «Освіта»; 02 «Культура та мистецтво»; 03 «Гуманітарні науки»; 05 «Соціальні і поведінкові науки»; 06 «Журналістика»; 07 «Управління та адміністрування»; 08 «Право»; 10 «Природничі науки»; 25 «Воєнні науки, безпека державного кордону, національна безпека»; 28 «Публічне управління та адміністрування»; 29 «Міжнародні відносини» тощо.

Ключовою наукою для формування базових навчальних дисциплін вивчення кіберпростору є кібергеографія [3]. Великого поширення набувають гуманітарні навчальні дисципліни кіберпростору.

Кібергеографія являє собою наукову галузь, яка досліджує організаційну та просторову структуру кіберпростору. Зазвичай кібергеографія розглядається як галузь географії, що спрямована на аналіз внутрішньої структури віртуальних просторів комп'ютерних мереж та їхнього впливу на інші соціально-економічні системи.

Термін «кібергеографія» стосується вивчення географічних аспектів і наслідків кіберпростору. Передбачає вивчення того, як цифрові технології, інформаційні мережі та віртуальні простори перетинаються з фізичною географією, соціальними структурами й політичними кордонами. Кібергеографія охоплює широкий спектр тем, включаючи розподіл інтернет-інфра-

структури, географію кіберзагроз, вплив кіберпростору на геополітику та просторові виміри цифрової діяльності. Можна визначити деякі ключові аспекти кібергеографії:

1. **Інфраструктура інтернету.** Аналіз фізичного розподілу інтернет-інфраструктури, такої як центри обробки даних, сервери та мережеві кабелі, у різних географічних регіонах.

2. **Цифрові розриви.** Дослідження відмінностей у доступі до інтернету та цифрових ресурсів між різними географічними регіонами, ураховуючи такі фактори як, наприклад, розбіжності між містом і селом та глобальну нерівність.

3. **Геополітика кіберпростору.** Вивчення того, як геополітичні міркування впливають на управління та регулювання кіберпростору, включаючи питання, пов'язані з кібервійною, державною кібердіяльністю та міжнародним співробітництвом.

4. **Кібербезпека та ландшафти загроз.** Картографування географічного розподілу кіберзагроз, атак та уразливостей. Розуміння того, як кіберзагрози відрізняються в різних регіонах, та визначення потенційних «гарячих точок».

5. **Цифрові економіки.** Вивчення просторових вимірів цифрової економіки, включаючи концентрацію технологічних галузей, інноваційних центрів та економічний вплив кіберпростору на різні географічні регіони.

6. **Культурні та мовні аспекти.** Дослідження того, як кіберпростір відображає і впливає на культурне та мовне розмаїття в різних регіонах. Аналіз того, як онлайн-спільноти та контент формуються під впливом географічних і культурних факторів.

7. **Кіберзлочинність і право.** Дослідження викликів, пов'язаних з юрисдикцією в кіберпросторі, особливо в боротьбі з кіберзлочинністю. Розуміння того, як правові рамки узгоджуються з географічними кордонами або виходять за їхні межі.

8. **Віртуальні простори та соціальні взаємодії.** Вивчення того, як віртуальні простори, такі як платформи соціальних мереж та онлайн-спільноти, впливають на соціальну взаємодію та відносини в різних географічних регіонах.

9. **Суверенітет даних.** Розгляд концепції суверенітету даних, що передбачає розуміння того, як різні країни регулюють і контролюють зберігання та обробку даних у межах своїх кордонів.

10. **Національна та регіональна політика.** Аналіз впливу національної та регіональної політики на кіберпростір, включаючи регулювання, цензуру та цифрові права. Розгляд того, як ці політики формують досвід користування інтернетом для користувачів у різних місцях.

11. **Вразливості інфраструктури.** Виявлення вразливостей у критично важливій інтернет-інфраструктурі та розуміння того, як ці вразливості можуть відрізнятися в різних географічних регіонах.

12. **Управління інтернетом.** Вивчення ролі міжнародних організацій, урядів і приватних структур в управлінні інтернетом, включаючи обговорення таких питань як мережевий нейтралітет і відкритий характер кіберпростору.

13. **Цифровий активізм і протести.** Вивчення географічних аспектів цифрового активізму й онлайн-протестів, зокрема того, як соціальні та політичні рухи використовують кіберпростір для транскордонної мобілізації.

14. **Просторовий аналіз кіберінцидентів.** Використання географічних інформаційних систем і просторового аналізу для розуміння просторових моделей і впливу кіберінцидентів.

15. **Нові технології і просторові наслідки.** Вивчення того, як нові технології, такі як інтернет речей (IoT), штучний інтелект і блокчейн, мають просторові наслідки і впливають на географію кіберпростору.

Тобто кібергеографія – це міждисциплінарна галузь, яка спирається на географію, інформатику, політологію, соціологію та інші навчальні дисципліни, щоб забезпечити розуміння складних і мінливих відносин між кіберпростором і фізичним світом. Дослідники в цій галузі прагнуть зрозуміти просторові виміри цифрової сфери та її вплив на суспільство, економіку і геополітику.

У ширшому розумінні до кібергеографії можна віднести щонайменше п’ять взаємопов’язаних між собою напрямів досліджень:

• загальна теорія і основи кібергеографії, вивчення організаційної структури віртуальних просторів, співвідношення кібер- і реального просторів (власне кібергеографія);

• картографування комп’ютерних і комунікаційних мереж; візуалізація віртуального простору (кіберкартографування);

• вивчення впливу кіберпростору на територіальну організацію суспільства;

• вивчення економіки, соціуму, політики;

• вивчення територіальної організації комп’ютерних і комунікаційних мереж.

Такий поділ є умовним, тому що явища в кіберпросторі не можна розглядати без урахування їхнього взаємозв’язку в реальному просторі.

Кібергеографія виходить за межі традиційної географії і може бути розглянута як науковий напрям, що знаходиться на перетині соціально-економічної географії та кібернетики.

Проаналізувавши аспекти географічного пізнання кіберпростору, доходимо висновку, що на сьогодні виразно сформувалися, принаймні, три області знань, які входять в ієрархічну структуру кібергеографії і будуть розвиватися в найближчому майбутньому. Це: кібергеополітика, кібердемографія і кіберкартографія.

Окремого розгляду потребує поняття «кіберекономіка».

Кіберекономіка [cyber-economy] – це складна система, яка забезпечує оптимальні зв’язки та взаємодію суб’єктів і об’єктів економічних відносин при виробництві, обміні та розподілі матеріальних благ. Кіберекономіка складається із системних ресурсів, які підвищують ефективність економічних процесів шляхом оптимального управління зв’язком і взаємодією між підсистемами суб’єктів і об’єктів економічних відносин. Вона описує економічну діяльність, спрямовану на створення інформаційних продуктів і

послуг в інтернеті та глобальних комерційних мережах, включаючи електронну торгівлю, маркетинг, рекламу, видавничу справу, інвестування тощо. За своєю суттю термін «кіберекономіка» означає економічну діяльність і транзакції, що здійснюються за допомогою цифрових технологій, інтернету та кіберпростору. Він охоплює широкий спектр цифрових взаємодій, транзакцій і бізнесу, які сприяють економічному зростанню та розвитку. Кіберекономіка є частиною ширшої цифрової економіки і включає різні сектори та види діяльності, які використовують інформаційно-комунікаційні технології. Виділяємо такі ключові аспекти кіберекономіки:

1. **Електронна комерція.** Купівля та продаж товарів і послуг в інтернеті, включаючи роздрібну електронну комерцію, транзакції між бізнесом і бізнесом (B2B) та електронні ринки.

2. **Цифрові послуги.** Надання різних послуг через інтернет, таких як програмне забезпечення як послуга (SaaS), хмарні обчислення, онлайн-трансляції та цифрова реклама [10].

3. **Цифрові платежі та фінансові технології.** Фінансові операції, що здійснюються в електронному вигляді, включаючи онлайн-банкінг, мобільні платежі, криптовалюти й інновації у сфері ФТ (FinTech) [11].

4. **Індустрія кібербезпеки.** Підприємства та послуги, що займаються захистом цифрових систем, мереж і даних від кіберзагроз. Сюди входять програмне забезпечення для кібербезпеки, консалтинг і керовані послуги безпеки.

5. **Економіка даних.** Генерація, збирання та монетизація даних, включаючи аналітику даних, великі дані та бізнеси, які використовують дані для прийняття рішень та інновацій.

6. **Цифрові платформи.** Онлайн-платформи, які об'єднують користувачів і сприяють різним видам діяльності, наприклад, платформи соціальних мереж, онлайн-маркети та платформи економіки спільного використання.

7. **Телекомунікаційні та інтернет-провайдери.** Це компанії, які забезпечують підключення до інтернету, телекомунікаційні послуги й інфраструктуру, необхідну для діяльності в інтернеті.

8. **Розробка технологій і програмного забезпечення.** Компанії, що займаються розробкою програмного забезпечення, додатків і технологічних рішень, які забезпечують роботу цифрової економіки.

9. **Електронне урядування та цифрове управління.** Використання цифрових технологій для покращання державних послуг, оптимізації адміністративних процесів і підвищення рівня залучення громадян. Як вітчизняний приклад можемо навести Постанову КМ України від 20.09.2017 № 649-р «Про схвалення Концепції розвитку електронного урядування в Україні» [8].

10. **Цифрова інфраструктура.** Інвестиції в цифрову інфраструктуру, включаючи широкосмугові мережі, центри обробки даних та інші компоненти, які підтримують функціонування цифрової економіки.

11. **Онлайн-освіта та електронне навчання.** Платформи та послуги, які надають освітній контент і сприяють навчанню за допомогою

онлайн-курсів, віртуальних класів та освітніх технологій.

12. **Цифрова охорона здоров'я.** Використання цифрових технологій в охороні здоров'я, включаючи телемедицину, медичні інформаційні системи та додатки, пов'язані з охороною здоров'я.

13. **Розумні міста та інтернет речей.** Впровадження ініціатив «розумного міста» [Smart city] та інтернету речей (IoT) для покращання життя в містах, підвищення ефективності й оптимізації використання ресурсів.

14. **Цифрові розваги.** Створення та споживання цифрового контенту в розважальних цілях, включно з онлайн-трансляціями, іграми та виробництвом цифрових медіа.

15. **Кіберспорт та ігрова індустрія.** Конкурентні ігри та пов'язані з ними індустрії, включаючи турніри з кіберспорту, розробку ігор і продаж віртуальних товарів.

16. **Цифровий маркетинг і реклама.** Рекламні заходи, що проводяться через цифрові канали, включно з рекламою в інтернеті, маркетингом у соціальних мережах і маркетингом впливових осіб.

17. **Дистанційна робота та телекомунікації.** Використання цифрових технологій для полегшення віддаленої роботи, дистанційної роботи та віртуальної співпраці, що особливо актуально в контексті мінливого робочого ландшафту.

18. **Кіберстрахування.** Страхові продукти, призначені для захисту бізнесу та фізичних осіб від фінансових втрат, спричинених кіберзагрозами та витоком даних.

19. **Блокчейн і криптовалюти.** Технології та фінансові інструменти, пов'язані з блокчейном, криптовалютами та децентралізованими фінансами (DeFi).

20. **Штучний інтелект та автоматизація.** Інтеграція технологій штучного інтелекту та автоматизації в різних галузях, що сприяє підвищенню ефективності й інноваціям у різних секторах економіки.

21. **Кіберланцюги поставок.** Взаємопов'язана мережа постачальників і продавців, які беруть участь у виробництві та розповсюдженні цифрових товарів і послуг.

Тобто, як бачимо, кіберекономіка є динамічною та постійно розвивається, оскільки технологічний прогрес, цифрові інновації та зміни в поведінці споживачів формують відповідний сучасний ландшафт. Вона відіграє вирішальну роль у сучасній економіці, сприяючи створенню робочих місць, інноваціям і глобальному взаємозв'язку. Політики, бізнес, громадяни повинні адаптуватися до можливостей і викликів, які несе кіберекономіка.

Електронний бізнес [e-business] описує підприємницьку діяльність, яка використовує можливості інформаційних технологій і глобальних інформаційних мереж для досягнення прибутковості. У цьому контексті головним активом є інформація, і тому часом електронний бізнес називають інформаційним бізнесом. Важливу частину електронного бізнесу становить електронна комерція. Електронна комерція [e-commerce] охоплює не лише транзакції купівлі-продажу, але й усі аспекти створення попиту на товари

та послуги, онлайн-замовлення, а також обмін інформацією між партнерами. Електронна комерція є важливим відділом електронного бізнесу, де взаємодія між суб'єктами торгівлі товарами та послугами реалізується через глобальну мережу Інтернет.

Гуманітарні навчальні дисципліни кіберпростору – це сфера наукової діяльності на стику комп'ютерних (або цифрових) технологій і гуманітарних навчальних дисциплін. Вона включає в себе систематичне використання цифрових ресурсів у гуманітарних науках, а також аналіз їх застосування. Надає цифрові інструменти та методи для вивчення гуманітарних наук з усвідомленням того, що друковане слово більше не є основним інструментарієм виробництва та поширення знань.

Створюючи та використовуючи нові застосунки й методи, гуманітарні навчальні дисципліни кіберпростору роблять можливими нові види навчання і досліджень, одночасно вивчаючи та критикуючи їхній вплив на культурну спадщину й цифрову культуру (кіберкультуру). Відмінною рисою гуманітарних навчальних дисциплін кіберпростору є культивування двосторонніх відносин між гуманітарними науками та цифровими технологіями: у цій галузі технології використовуються як для проведення гуманітарних досліджень, так і для гуманістичних питань, часто одночасно.

Кіберсоціологія – це субдисципліна соціології, яка фокусується на розумінні використання кібермедіа в повсякденному житті й того, як ці різні технології сприяють формуванню моделей людської поведінки, соціальних відносин і уявлень про себе.

Хоча термін «кіберсоціологія» ще не повністю ввійшов у культурний лексикон, соціологи займаються дослідженнями, пов'язаними з інтернетом, із моменту його появи. Вони розглянули безліч соціальних проблем, пов'язаних з онлайн-спільнотами, кіберпростором і кіберідентифікацією. У таких дослідженнях розглянуто багато різних понять: «кіберсоціологія», «соціологія інтернету», «соціологія онлайн-спільнот», «соціологія соціальних мереж», «соціологія кіберкультури» тощо.

Кіберпсихологія є галуззю психології, що зосереджується на методології, теорії та практиці вивчення різних аспектів використання соціальних сервісів інтернету людьми. Соціальні сервіси охоплюють не лише соціальні мережі, але й будь-які засоби взаємодії в інтернеті – від інтернет-форумів та чатів до месенджерів (як частина кіберкультури). Кіберпсихологія тісно переплітається з медіапсихологією, теорією медіа, інформаційними технологіями, комунікативістикою та іншими відомими науковими галузями. У контексті психології вона наближається до медіапсихології.

Кіберпсихологія – це галузь психології, яка досліджує взаємодію між людьми та цифровими технологіями, онлайн-середовищами та віртуальними просторами. Вона вивчає, як на поведінку, пізнання та емоції людини впливає використання цифрових пристроїв, інтернету, соціальних мереж, онлайн-ігор та інших віртуальних платформ. Кіберпсихологія охоплює ши-

рокий спектр тем, пов'язаних із психологічними аспектами поведінки в інтернеті та впливом цифрових технологій на психічне благополуччя. Слід виділити такі ключові аспекти кіберпсихології:

1. Онлайн-ідентичність і самопрезентація. Вивчення того, як люди конструюють і представляють свою ідентичність в онлайн-просторі, включаючи профілі в соціальних мережах, аватари й онлайн-персони.

2. Соціальна взаємодія в інтернеті. Дослідження динаміки соціальних відносин, що формуються та підтримуються у віртуальних середовищах, таких як соціальні мережі, онлайн-форуми й програми для обміну повідомленнями.

3. Цифрова комунікація та відносини. Вивчення впливу цифрової комунікації на міжособистісні стосунки, включаючи «онлайн-дружбу», знайомства та вплив технологій на моделі спілкування.

4. Інтернет-залежність і компульсивна поведінка. Аналіз проблемного використання інтернету та поведінки, пов'язаної з надмірною активністю в мережі, включаючи ігрову залежність, залежність від соціальних мереж та інші види компульсивної поведінки.

5. Кібербулінг та онлайн-переслідування. Дослідження психологічного впливу кібербулінгу, онлайн-переслідувань і негативного досвіду в цифровому просторі на психічне здоров'я людей.

6. Цифрове благополуччя та психічне здоров'я. Вивчення взаємозв'язку між цифровими технологіями та результатами психічного здоров'я, зокрема й потенціалу технологій для покращання добробуту або сприяння вирішенню проблем психічного здоров'я.

7. Ігрова психологія. Розуміння психологічних аспектів відеоігор, включаючи мотивацію до гри, вплив ігрового досвіду на емоції та потенціал ігрової залежності.

8. Онлайн-навчання та когнітивні процеси. Дослідження того, як середовище онлайн-навчання впливає на когнітивні процеси, пам'ять, увагу й освітні результати.

9. Конфіденційність і безпека. Вивчення сприйняття людьми конфіденційності в інтернеті, обізнаності щодо кібербезпеки та психологічного впливу витоків даних і онлайн-загроз.

10. Цифрове громадянство й етика. Вивчення розвитку навичок цифрового громадянства, етичних аспектів поведінки в інтернеті та психологічних аспектів відповідальної цифрової взаємодії.

11. Віртуальна реальність та імерсивні технології. Вивчення психологічного впливу віртуальної реальності (VR) та імерсивних технологій на сприйняття, пізнання та емоційні переживання.

12. Онлайн-терапія та інтервенції у сфері психічного здоров'я. Оцінка ефективності онлайн-терапевтичних втручань, телемедицини та цифрових платформ психічного здоров'я у вирішенні проблем психічного здоров'я.

13. Технології та когнітивні функції. Дослідження того, як широке використання цифрових технологій, таких як смартфони та соціальні мережі, може впливати на когнітивні

функції, концентрацію уваги й обробку інформації.

14. Поведінка та обізнаність у сфері кібербезпеки. Розуміння поведінки людей у сфері кібербезпеки, сприйняття ризиків та обізнаність щодо онлайн-загроз.

15. Цифровий слід і репутація в інтернеті. Аналіз психологічних наслідків цифрового сліду людини, включаючи управління онлайн-репутацією та її вплив на офлайн-життя.

16. Емоційне вираження та використання емодзі. Вивчення того, як люди виражають емоції онлайн, включаючи використання емодзі, смайликів та інших невербальних сигналів у цифровій комунікації.

17. Культурні та крос-культурні перспективи. Розгляд культурних впливів на поведінку в інтернеті, норм цифрової комунікації та відмінностей у психологічному впливі цифрових технологій у різних культурах.

18. Батьківство в цифрову епоху. Вивчення викликів і стратегій, пов'язаних із батьківством в епоху всепроникних цифрових технологій, включаючи управління екранним часом і цифрову грамотність для дітей.

19. Технології та сон. Вивчення впливу часу, проведеного перед екраном, і використання цифрових пристроїв на режим сну та загальну якість сну.

20. Взаємодія людини та комп'ютера. Вивчення психологічних аспектів користувацького досвіду, дизайну інтерфейсу та впливу юзабіліті технологій на людину.

Тобто можна прямо констатувати, що кіберпсихологія – це міждисциплінарна галузь, яка спирається на знання з психології, соціології, комунікаційних досліджень, взаємодії людини з комп'ютером та інших дисциплін, щоб зрозуміти складну взаємодію між людиною та цифровими технологіями. Дослідники кіберпсихології прагнуть надати цінну інформацію про психологічні наслідки нашого життя, що стає все більше цифровим.

Основною навчальною дисципліною (циклом дисциплін), на нашу думку, для системної підготовки фахівців до діяльності в кіберпросторі може бути теорія кіберпростору, призначена для надання систематизованих знань і формування вмінь щодо діяльності фахівців у кіберпросторі. Виходячи з того, що кіберпростір є надзвичайно уразливою субстанцією, необхідним є осмислення таких напрямів теорії кіберпростору як безпека кіберпростору та захист кіберпростору [3]. Такий підхід дасть можливість швидко адаптувати підготовку фахівців для Служби безпеки України до діяльності в інформаційній сфері та кіберпросторі.

Теорія кіберпростору дає цілісне уявлення про цифровий ландшафт, охоплюючи його технічні, соціальні, політичні й економічні виміри. Таке всебічне розуміння має вирішальне значення для фахівців, які займаються захистом і роботою в цій сфері. Теорія розглядає такі фундаментальні поняття як кібергеографія, архітектура мереж, поведінка цифрових акторів і динаміка кіберконфліктів. Маючи знання з цієї проблематики, фахівці можуть краще зрозуміти взаємозв'язок і взаємозалежність у кіберпросторі, що

дасть змогу приймати правильні ефективні рішення.

Стратегічне мислення має важливе значення у протистоянні складним викликам, що постають перед кіберпростором. Теорія кіберпростору озброює фахівців інтелектуальними інструментами для аналізу й інтерпретації ширших наслідків кібердіяльності. Ця дисципліна заохочує критичне мислення щодо стратегічного використання кіберпростору в інтересах національної безпеки, захисту критичної інфраструктури та захисту від кіберзагроз. Фахівці, підготовлені з теорії кіберпростору, можуть передбачати дії супротивників, розробляти надійні механізми захисту та сприяти виробленню національних та організаційних стратегій кібербезпеки. Ця стратегічна перспектива є безцінною для підтримання проактивної і стійкої позиції в кіберпросторі.

Кіберпростір – це сфера, що швидко розвивається та характеризується безперервним технологічним прогресом і новими загрозами. Теорія кіберпростору розвиває адаптивне мислення, що дає змогу фахівцям передбачати майбутні тенденції та виклики й реагувати на них. Вивчаючи історичний розвиток кіберпростору, теоретичні засади та нові технології, фахівці можуть виявити закономірності та спрогнозувати майбутній розвиток подій. Такий далекоглядний підхід має вирішальне значення для того, щоб випереджати супротивників, зменшувати ризики та використовувати нові можливості. За навчальними програмами з акцентом на теорію кіберпростору фахівці готуються до навігації в умовах невизначеності та складнощів цифрового майбутнього.

Теорія кіберпростору за своєю суттю є міждисциплінарною, спираючись на такі галузі як комп'ютерні науки, інформаційні технології, соціологія, політологія, право й економіка. Цей міждисциплінарний характер є значною перевагою для підготовки фахівців, оскільки він сприяє формуванню всебічних та універсальних навичок. Фахівці, які розуміють технічні аспекти кіберпростору, а також його соціальні та політичні наслідки, можуть розглядати кібервиклики з різних точок зору. Така інтеграція знань підвищує їхню здатність розробляти комплексні рішення з безпеки, брати участь у політичних дискусіях та ефективно співпрацювати з різними зацікавленими сторонами.

Хоча практичні навички й практичний досвід мають вирішальне значення для фахівців із кіберпростору, вони повинні ґрунтуватися на міцних теоретичних знаннях. Теорія кіберпростору слугує фундаментом, на якому базуються практичні застосування. Вона лежить в основі розробки й упровадження заходів кібербезпеки, розробки тактики кіберзахисту та проведення наступальних кібероперацій. Навчальні програми, у яких акцентується на теорії кіберпростору, гарантують, що фахівці зможуть застосовувати свої практичні навички в межах узгодженої та обґрунтованої системи. Така теоретична підготовка також сприяє безперервному навчанню й адаптації, оскільки фахівці можуть краще розуміти та інтегрувати нові методи і технології.

Теорія кіберпростору також охоплює етичні та політичні аспекти кібердіяльності. Фахівці повинні орієнтуватися в складних правових рамках, етичних дилемах і політичних міркуваннях. Теорія забезпечує структурований підхід до розуміння цих питань, гарантуючи, що фахівці можуть діяти в межах правових та етичних норм, ефективно досягаючи при цьому своїх цілей. Включаючи питання політики й етики в навчальну програму, теорія кіберпростору сприяє вихованню відповідальних і підзвітних кадрів у сфері кібербезпеки.

Також уважаємо, що кібергеографія та теорія кіберпростору – це дві взаємопов'язані галузі, які досліджують просторові та теоретичні виміри цифрової сфери. У той час як кібергеографія зосереджується на просторових аспектах інтернету та цифрових технологій, теорія кіберпростору заглиблюється в концептуальні та соціальні наслідки застосування цих технологій. Розуміння того, як ці дві галузі співвідносяться одна з одною, має вирішальне значення для розуміння складнощів цифрової епохи.

Кібергеографія вивчає просторові та географічні аспекти кіберпростору. Вона включає в себе картографування цифрового рельєфу, аналіз розподілу цифрових інфраструктур та розуміння просторової динаміки онлайн-активності. Ключові сфери інтересу кібергеографії включають фізичне розташування центрів обробки даних, просторовий розподіл інтернет-користувачів і географічні патерни кібератак.

Перевагою кібергеографії є її здатність візуалізувати й кількісно оцінювати просторові виміри цифрового світу. За допомогою таких методів як цифрове картографування і просторовий аналіз, кібергеографи здатні виявити закономірності й тенденції, які можуть бути невидимими для традиційного аналізу. Наприклад, картографування фізичного розташування інтернет-інфраструктури може виявити регіональні відмінності в цифровому доступі та підключенні, проливаючи світло на цифровий розрив.

Теорія кіберпростору, з іншого боку, займається концептуальними та соціальними вимірами інтернету та цифрових технологій. Вона вивчає, як окремі особи та суспільства створюють, сприймають і розуміють цифрові простори. Ключові поняття теорії кіберпростору включають віртуальну реальність, онлайн-ідентичність, цифрові спільноти та природу цифрової взаємодії.

Теорія кіберпростору забезпечує основу для розуміння глибоких змін, які цифрові технології вносять у людський досвід. Вона досліджує, як кіберпростір трансформує поняття простору й часу, змінює соціальну взаємодію і створює нові форми спільнот та ідентичності. Досліджуючи ці зміни, теорія кіберпростору пропонує розуміння ширших наслідків застосування цифрових технологій для суспільства.

Незважаючи на різні фокуси, кібергеографія і теорія кіберпростору глибоко взаємопов'язані. Обидві галузі досліджують різні аспекти одного й того ж явища – цифрового світу. Вивчаючи їхні перетини, можна отримати повніше розуміння кіберпростору (див. табл. 1).

Таблиця 1 – Взаємопов'язаність кібергеографії і теорія кіберпростору (складено авторами)

Кібергеографія	Теорія кіберпростору	Перетин
Аналізує фізичний розподіл і зв'язок цифрових спільнот, виявляючи географічні закономірності та диспропорції	Вивчає формування та динаміку цифрових спільнот, досліджуючи, як вони створюють і підтримують соціальні зв'язки та ідентичності	Розуміння просторового розподілу цифрових спільнот може дати уявлення про соціальну динаміку та взаємодію всередині цих спільнот
Складає карти географічного розподілу доступу до інтернету та визначає регіони з обмеженим підключенням	Досліджує соціальні та економічні наслідки цифрового розриву, включаючи питання нерівності та ізоляції	Поєднання просторового аналізу із соціальною теорією може допомогти визначити стратегії подолання цифрового розриву та сприяння цифровій інклюзії
Вивчає географічні закономірності кібератак і розташування вразливих об'єктів інфраструктури	Досліджує соціальні та організаційні фактори, що сприяють ризикам кібербезпеки, а також наслідки кіберзагроз для суспільства	Інтегрований підхід може покращити наше розуміння того, як просторові та соціальні фактори взаємодіють для формування вразливості та стійкості кібербезпеки
Відображає на картах розташування й розподіл додатків і користувачів віртуальної та доповненої реальностей	Досліджує емпіричні та концептуальні наслідки віртуальної та доповненої реальностей для людського сприйняття та взаємодії	Розуміння просторового розподілу цих технологій може допомогти в аналізі їхнього соціального та емпіричного впливу

Розробка нових методологій, що поєднують просторовий аналіз із соціальною теорією, може забезпечити глибше розуміння кіберпростору. Наприклад, методи просторово-часового аналізу можна використовувати для вивчення еволюції цифрових спільнот у часі, тоді як якісні методи можуть досліджувати життєвий досвід людей у цифровому просторі. Інтегрований підхід може також сприяти формуванню політики в таких сферах як цифрова інклюзія, кібербезпека та міське планування. Розуміючи просторові та соціальні виміри кіберпростору, політики можуть розробляти ефективніші заходи для вирішення проблем і використання можливостей цифрової епохи.

Підготовка фахівців для Служби безпеки України з урахуванням їхньої діяльності в кіберпросторі базується на таких аспектах: забезпечення запобігання, виявлення, припинення та розкриття кримінальних порушень проти миру та безпеки людства, що

вчиняються в онлайн-середовищі; проведення контррозвідувальних та оперативно-розшукових операцій, спрямованих на боротьбу з кібертероризмом і кібершпигунством; конфіденційна перевірка на готовність об'єктів критичної інфраструктури до можливих кібератак та інцидентів у кіберпросторі; протидія кіберзлочинності, яка може негативно вплинути на життєво важливі інтереси держави; розслідування кіберінцидентів та кібератак, спрямованих на державні електронні інформаційні ресурси, а також на інформацію, захист якої передбачений законом, включаючи критичну інформаційну інфраструктуру; забезпечення ефективного реагування на кіберінциденти, що можуть загрожувати державній безпеці [2].

Вважаємо, що такий підхід потребує введення до освітньої програми «Контррозвідувальна діяльність у сфері забезпечення державної безпеки» зі спеціальності 251 «Державна безпека» [4] додаткової профільної дисципліни (циклу дисциплін) «Контррозвідувальний захист кібербезпеки держави та об'єктів критичної інфраструктури».

Під час вивчення цієї дисципліни мають формуватися компетентності щодо здатності обґрунтовування, впровадження та застосування заходів, методів і засобів контррозвідувального захисту в інформаційній сфері та кіберпросторі.

Зміст циклу додаткових навчальних дисциплін можуть становити такі змістові модулі (теми):

1. Концептуальні засади контррозвідувального захисту кібербезпеки держави.

2. Тактика добування та використання оперативної інформації про кіберрозвідку іноземних держав.

3. Виявлення, попередження і припинення розвідувально-підривних акцій кіберрозвідки іноземних держав, що проводяться з використанням портативної розвідувальної апаратури, автоматичних і закладних пристроїв.

4. Виявлення, попередження та припинення кібератак комп'ютерної розвідки іноземних держав.

5. Попередження кіберзагроз на об'єктах критичної інфраструктури.

6. Тактика негласного контролю стану готовності об'єктів критичної інфраструктури до кібератак і кіберінцидентів тощо.

Ураховуючи сучасні умови, за яких потрібна негайна реакція з боку суспільства, пропонуємо також розглянути такі вектори щодо змістового наповнення навчальних дисциплін:

1. Оцінка ефективності заходів кіберконтррозвідки в захисті національної критичної інфраструктури – це оцінювання ефективності поточних стратегій контррозвідки в запобіганні кіберзагрозам для критичної інфраструктури, ураховуючи як технологічні, так і людиноцентричні підходи.

2. Поведінковий аналіз інсайдерських загроз для об'єктів критичної інфраструктури як контррозвідувальна перспектива. Це може бути, наприклад, дослідження психологічних і поведінкових аспектів внутрішніх загроз у секторах критичної інфраструктури, вивчення контррозвідувальних заходів для виявлення та пом'якшення потенційних ризиків.

3. Роль міжнародного співробітництва в кіберконтррозвідці для

національної безпеки. Тут цілком можливо розглянути, як країни можуть співпрацювати у сфері кіберконтррозвідки для захисту критичної інфраструктури, ураховуючи обмін інформацією, спільну оцінку загроз та скоординоване реагування.

4. Механізми обміну розвідувальною інформацією про кіберзагрози для посилення захисту критичної інфраструктури. Оцінка існуючих і запропонованих механізмів обміну розвідданими про кіберзагрози між державними установами, суб'єктами приватного сектору та міжнародними партнерами з метою посилення загального захисту критичної інфраструктури.

5. Застосування машинного навчання та штучного інтелекту в кіберконтррозвідці для покращання предиктивного аналізу з метою захисту критичної інфраструктури. Вивчення застосування машинного навчання та штучного інтелекту в кіберконтррозвідці з акцентом на прогностичному аналізі для завчасного виявлення потенційних кіберзагроз критичній інфраструктурі.

6. Оцінка впливу геополітичних чинників на стратегії кіберконтррозвідки для критичної інфраструктури. Вивчення того, як геополітичні міркування впливають на розроблення та реалізацію стратегій кіберконтррозвідки, особливо щодо захисту критичної інфраструктури, та підготовка пропозицій щодо застосування адаптивних підходів.

Ці практичні за своєю суттю вектори для наповнення змісту, наприклад, робочих програм навчальних дисциплін або лекційних курсів, охоплюють низку важливих сфер, що стосуються контррозвідувального забезпечення кібербезпеки з урахуванням важливості технологій, людського фактору, міжнародного співробітництва, прогнозного аналізу та геополітичних міркувань у захисті державних активів та об'єктів критичної інфраструктури від кіберзагроз.

Якщо вважати, що до освітньої програми «Контррозвідувальна діяльність у сфері забезпечення державної безпеки» зі спеціальності 251 «Державна безпека» вже включена навчальна дисципліна «Інформаційні технології», то доопрацювання вже діючої освітньої програми не буде становити великих труднощів.

Крім того, пропонується впровадити в систему освіти СБ України такі нововведення:

– розширити перелік дисциплін, які вивчаються в межах підготовки фахівців для діяльності в кіберпросторі, додавши до них такі: «Основи кібербезпеки», «Кібербезпека критичної інфраструктури», «Кібербезпека інформаційних систем», «Кібербезпека телекомунікацій», «Кібербезпека мережі Інтернет», «Кібербезпека штучного інтелекту», «Кібербезпека великих даних», «Кібербезпека кіберпростору» тощо;

– запровадити в навчальний процес інтерактивні методи навчання, такі як проєктна робота, командна робота, моделювання, відеолекції тощо, що дасть змогу підвищити ефективність навчання та практичної підготовки фахівців;

– створити в СБ України центри кібербезпеки за різними напрямами, які будуть забезпечувати практичну

підготовку фахівців у сфері кібербезпеки.

Висновки. Підготовка фахівців для роботи в кіберпросторі є не лише технічним завданням, але й стратегічним імперативом. Розроблення цілісної національної стратегії кібербезпеки, узгодженої з міжнародними стандартами та найкращими практиками, є життєво важливим. Політика повинна сприяти співпраці між державними установами, суб'єктами приватного сектору та міжнародними партнерами, а нормативно-правова база – впровадженню заходів із кібербезпеки та переслідування кіберзлочинів. СБ України має брати участь у реалізації політики з підвищення кіберстійкості та впровадження найкращих практик безпеки в усіх секторах суспільства.

Людський фактор часто є найслабшою ланкою кібербезпеки. Тому в навчальній програмі слід передбачити розвиток «м'яких» навичок, таких як критичне мислення, вирішення проблем і прийняття рішень під тиском. Не менш важливими є психологічна готовність і стійкість. Навчання має включати модулі з вивчення питань управління стресом, когнітивних упереджень і психології кіберпротивників. Регулярне психологічне оцінювання та застосування механізмів підтримки сприятимуть забезпеченню ефективної діяльності фахівців СБ України в умовах високого рівня стресу.

Кіберпростір – це динамічна сфера, що швидко розвивається. Безперервне навчання та адаптація необхідні для продуктивної праці в умовах виникнення нових загроз і технологій. У співробітників СБ України мають бути безперервний професійний розвиток і регулярне оновлення навичок. Партнерство з науковими установами, промисловістю та міжнародними організаціями може полегшити доступ до новітніх досліджень, тенденцій і передового досвіду. Крім того, створення централізованого сховища знань і регулярні тренінги можуть гарантувати, що фахівці СБ України залишатимуться на передовій у сфері кібербезпеки.

Забезпечення кібербезпеки потребує спільного підходу. СБ України має тісно співпрацювати з іншими органами національної безпеки, правоохоронними органами та приватним сектором. Міжвідомча координація може покращити обмін інформацією, підвищити обізнаність про ситуацію та оптимізувати зусилля з реагування. Спільні навчання та симуляційні тренування можуть сприяти формуванню мислення співпраці та підготувати фахівців СБ України до скоординованого реагування на кіберінциденти. Міжнародна співпраця також має вирішальне значення, ураховуючи глобальний характер кіберзагроз. СБ України має брати активну участь у міжнародних форумах, ділитися розвідданими з партнерами та долучатися до глобальних ініціатив із кібербезпеки.

Навчальна програма повинна закласти міцний етичний фундамент у професіоналів СБ України. Кібероперації часто пов'язані із складними правовими й етичними дилемами. Фахівці мають бути добре обізнані з правовою базою, що регулює кібердіяльність як на національному, так і міжнародному рівнях. Навчання повинно включати тематичні дослідження та сценарії, які допомагають фахів-

цям орієнтуватися в етичних питаннях і приймати обґрунтовані рішення. Дотримання етичних стандартів має важливе значення для збереження суспільної довіри й забезпечення того, щоб кібероперації проводилися в межах закону.

Системна підготовка фахівців для Служби безпеки України до діяльності в кіберпросторі є критично важливою складовою національної безпеки. За результатами дослідження зроблено висновок щодо важливості комплексного й інтегрованого підходу до навчання, який поєднує технологічну підготовку, теоретичні знання та практичні навички. Ураховуючи багатогранну природу кібербезпеки, включаючи технологічні, освітні, політичні, людські й етичні аспекти, СБ України може підготувати висококваліфікований і стійкий кіберперсонал. Оскільки кіберзагрози продовжують розвиватися, СБ України повинна залишатися гнучкою, адаптивною та проактивною у своїх навчальних та оперативних цілях, забезпечуючи безпеку та стійкість цифрової інфраструктури країни.

Теорія кіберпростору має стати основною навчальною дисципліною або циклом дисциплін для систематичної підготовки фахівців до діяльності в кіберпросторі. Її комплексний підхід забезпечує глибоке розуміння цифрового ландшафту, розвиває стратегічне мислення, прогнозує майбутні тенденції, інтегрує міждисциплінарні знання та покращує практичне застосування. В епоху, коли кіберпростір відіграє ключову роль у національній безпеці та функціонуванні суспільства, підготовка фахівців із теорії кіберпростору має важливе значення для розвитку кваліфікованих, адаптивних і далекоглядних кадрів із кібербезпеки. Ця теоретична база не лише озброює фахівців знаннями та навичками, необхідними для вирішення поточних завдань, але й готує їх до орієнтації в складних умовах цифрового майбутнього, що постійно змінюються.

Пропозиції щодо системної підготовки фахівців для Служби безпеки України до діяльності в кіберпросторі засновані на результатах практичної реалізації деяких освітніх програм зі спеціальності 256.04 «Національна безпека (кіберзахист, забезпечення державної безпеки в інформаційній сфері)» і доповнюють освітню програму «Контррозвідувальна діяльність у сфері забезпечення державної безпеки» за спеціальністю 251 «Державна безпека».

Подальші дослідження можуть бути спрямовані на вивчення тематики розвитку кіберпростору та комплексного використання методів і засобів контррозвідувальної діяльності й кіберконтррозвідувального захисту. Висновки дослідження можуть бути використані при розробці стандартів вищої освіти та навчальних планів для інших спеціальностей і рівнів підготовки здобувачів, включаючи програми перепідготовки та підвищення кваліфікації.

Список використаних джерел

1. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. *База даних «Законодавство України»* / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2469-19 (дата звернення: 16.01.2024).

2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *База даних «Законодавство України»* / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2163-19 (дата звернення: 13.01.2024).

3. Богуш В. М., Богуш В. В., Бровко В. Д., Настрадін В. П. Основи кіберпростору, кібербезпеки та кіберзахисту : навчальний посібник / під ред. В. М. Богуша. Київ : Ліра-К, 2020. 552 с.

4. Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти : Постанова Кабінету Міністрів України від 29.04.2015 № 266. *База даних «Законодавство України»* / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/266-2015-%D0%BF (дата звернення: 03.03.2024).

5. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. *База даних «Законодавство України»* / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/447/2021 (дата звернення: 03.03.2024).

6. Про План реалізації Стратегії кібербезпеки України : Рішення РНБО від 30.12.2021. *База даних «Законодавство України»* / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/n0087525-2 (дата звернення: 13.02.2024).

7. Clark D. Characterizing cyberspace: past, present and future, MIT/CSAIL Working Paper. 12 March 2010. P. 1–18.

8. Про схвалення Концепції розвитку електронного урядування в Україні : розпорядження Кабінету Міністрів України від 20.09.2017 № 649-р. *База даних «Законодавство України»* / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/649-2017-%D1%80 (дата звернення: 13.02.2024).

9. Personal Information Protection and Electronic Documents Act. Justice Laws Website – Site Web de la lÃgislation (Justice). URL: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-1.html (дата звернення: 05.03.2024).

10. IaaS, PaaS and SaaS. OVHcloud. URL: https://www.ovhcloud.com/en/public-cloud/cloud-computing/iaas-paas-saas/#:~:text=IaaS%20stands%20for%20’Infrastructure%20as,of%20services%20over%20the%20internet (дата звернення: 05.03.2024).

11. Fintech: Definition, services and sectors. Alter Finance. URL: https://www.alterfinancegroup.com/en/blog/dictionary/what-is-a-fintech (дата звернення: 05.03.2024).

Стаття надійшла до редакції 24.03.2024

UDC 004.056.5:378.1(045)

Bohush V. M., Khmelnytskyi M. O.

SUGGESTIONS FOR SYSTEM TRAINING OF SPECIALISTS FOR THE SECURITY SERVICE OF UKRAINE FOR ACTIVITIES IN CYBERSPACE

Modern cyberspace is an important element of information sphere and the economy of Ukraine. It is used to carry out a wide range of activities, including communication, trade, finance, education and management. In this regard, the importance of ensuring cybersecurity, which involves protection against cyber threats, such as hacker attacks, intelligence operations and the spread of disinformation, is growing.

The Security Service of Ukraine is one of the public authorities responsible for ensuring cybersecurity of Ukraine. To fulfill this task, the Security Service of Ukraine needs highly qualified personnel who have knowledge and skills in the fields of cybersecurity and information technology.

In the article, based on the results of the analysis of the state of basic training of specialists of the Security Service of Ukraine in specialties 251 "State Security", 256 "National Security" of the field of knowledge 25 "Military Sciences, National Security, Security of the State Border", it is concluded that today traditional teaching methods are not enough to meet modern challenges in the field of cybersecurity, since specialized knowledge and abilities to respond quickly are required, and there is no orderly approach to the training of specialists for activities in cyberspace, which leads to a gap between theoretical knowledge and its practical application. This is due to a number of factors, in particular, insufficient development of the theoretical foundations of cybersecurity, lack of uniform standards for training specialists in this field, insufficient funding of the education system, etc.

The concept of systematic training of specialists for this field is proposed, which combines several disciplines and continuous training, takes into account the development of technologies and facilities of cyberspace of Ukraine, the integration of advanced technological tools, as well as the solution of current scientific and methodological problems in its various fields (economic, social, psychological, legal, cultural, systemic, security, etc.).

According to this approach, the training of specialists of the Security Service of Ukraine for activities in cyberspace should be carried out in the following directions: infrastructure, technological, research, which, respectively, provide for the training of specialists who will be responsible for managing cyber facilities of Ukraine, countering cyberattacks and ensuring cybersecurity of critical infrastructure, developing and implementing new cybersecurity technologies, conducting cyberthreat expertise, conducting research in the field of cybersecurity, developing new methods and means of protection against cyberthreats.

It is proposed to introduce innovations into the education system of the Security Service of Ukraine: to expand the list of disciplines that are learned within the framework of training specialists for activities in cyberspace; to introduce interactive teaching methods into the educational process, such as project work, teamwork, modeling, video lectures and others, which will increase the effectiveness of theoretical and practical training of specialists; to create cybersecurity centers in the Security Service of Ukraine in various areas that will provide practical training of specialists.

The implementation of such measures will ensure national security in the digital sphere and create a reliable human resources potential of the Security Service of Ukraine, capable of responding to the dynamic current threats.

Key words: *information sphere, cyberspace, competence, counterintelligence protection, national security, training result, special operation.*