КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (23), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.23.171181
УДК 340.113:004ю056

Горліченко Сергій Олександрович
науковий співробітник
Інститут спеціального зв'язку та захисту
інформації Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID 0000-0002-8999-7526
serhii.horlichenko@gmail.com

ОСОБЛИВОСТІ СУЧАСНОГО ПОНЯТІЙНО-ТЕРМІНОЛОГІЧНОГО АПАРАТУ У СФЕРІ ПІДГОТОВКИ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ

Анотація. У статті досліджено актуальність забезпечення сталого розвитку якісної кібербезпеки країни як основної складової сучасного цифрового суспільства. Вивчено ключові напрямки підготовки кадрів органів кібербезпеки України. Проаналізовано основні нормативно-правові акти, які регулюють систему освітньої підготовки фахівців в області кібербезпеки. Загально охарактеризовано систему освіти підготовки кадрів в області кібербезпеки і зіставлено її із головними елементами загальної системи освіти України. Розглянуто теоретичні нюанси процесу створення системи професійної підготовки фахівців із кібербезпеки, встановлено її основні риси, перспективи та функціонування на теперішній час. Запропоновано узагальнене поняття системи підготовки кадрів у сфері кібербезпеки, як комплекс елементів освітньої діяльності, мета яких полягає у реалізації та забезпеченні сталого розвитку цифрового суспільства шляхом підготовки необхідного обсягу кадрів в області кібербезпеки країни. На основі наукових напрацювань вітчизняних та зарубіжних вчених у галузі освіти, окреслено новітні освітні елементи та поняття у процесі сучасної освіти. Розкрито та обумовлено співвідношення таких понять, як «інформаційна безпека» та «кібербезпека», шляхом деталізації їх основних складових. Проаналізовано визначення кібербезпеки у стратегіях кіберберпеки провідних країн світу та співставлено його із визначенням, наведеним у національній стратегії кібербезпеки України. Запропоновано бачення автора дефініції «кібербезпека» на основі дослідженої наукової літератури та офіційних документів, з урахуванням комунікативних, соціологічних та політичних аспектів. Досліджено низку наукових напрацювань сфери кібер- та інформаційної безпеки задля узагальнення сутності визначення «фахівець із кібезбезпеки». Зроблено висновок щодо важливості належного функціонування системи підготовки кваліфікованих кадрів сфери кібербезпеки. Запропоновано зробити детальніше дослідження процесу самої підготовки кадрів та концептуальних основ організації освітньої діяльності на прикладі інших країн світу.

Ключові слова: кібербезпека; інформаційна безпека; цифрове суспільство; кіберосвіта; інформаційні технології.

ВСТУП

Постановка проблеми. Сучасні інформаційні технології та глобальні комп'ютерні мережі роблять інформацію доступною для всіх, включаючи органи влади та звичайних громадян. Зміни в галузі технологій вимагають швидкої адаптації громад до смарт-технологій, а державні структури повинні стати ефективними системами розв'язання проблем, залучаючи активну участь громадян, особливо на шляху до євроінтеграції. Розуміння загроз кіберпростору, зокрема кіберзлочинності, є важливим для розвитку цих тенденцій і сприяє провідним світовим експертам та міжнародним організаціям. Враховуючи це, стає необхідним ефективний захист інформації від незаконних втручань.

Нинішня ситуація в Україні вимагає від державних та приватних структур встановлення високих вимог стандартів підготовки фахівців у сфері захисту інформації. Даний напрямок почав активно розвиватися в нашій країні лише з 2016 року, коли було вперше визнано поняття кібербезпеки на законодавчому рівні, тоді як у всьому цивілізованому світі дана професійна діяльність функціонує вже не перше десятиліття. Варто зазначити, що понятійно-категоріальний апарат сфері підготовки фахівців із кібербезпеки на сьогодні залишається не визначеним остаточно на законодавчому, практичному та науковому рівнях [1, с.187].

Проблема якості кібербезпеки нашої країни полягає, перш за все, у людському ресурсі. Представники органів державної влади, що задіяні у процесі становлення та розвитку кібербезпеки України, наголошують на невідповідності стану забезпечення кваліфікованими кадрами даної спеціалізації. Тож держава має активно долучитися до процесу навчання нових професійних кадрів, особливо під час війни з Російською Федерацією, позаяк важливість цього процесу неможливо перебільшити в нинішній ситуації [2], [24], [25], [29 с. 35].

Отож, підготовка високо кваліфікаційних кадрів у сфері кібербезпеки є ключовими елементами в умовах протистояння нашої держави російській агресії. Проте світовий досвід демонструє нам, що якісна робота системи кібербезпеки будь-якої сучасної країни є актуальним питанням як у випадку надзвичайних ситуацій, так і в мирний час.

Аналіз останніх досліджень і публікацій. Проблеми та шляхи покращення підготовки кваліфікованих кадрів в області кібербезпеки виступають об’єктом дослідження вітчизняних науковців, таких як Мельник С. В. [1], Кормич Б. А. [5], Баранов О. А. [7] та ін.

Такі відомі вчені як Баранов О. А. та Скрипник Л. В. звертають увагу на те, що завдання кібербезпеки полягають у забезпеченні конфіденційності та цілісності інформації, тобто її захистом у кіберпросторі [7], [8].

Діордіца І. В. [3] досліджував системи забезпечення кібербезпеки та вніс своє авторське уявлення про це поняття, визначивши суб’єктів і об’єкти системи, основну сутність та призначення.

У своїй роботі Даник Ю. та Зінченко А. [14] проаналізували стан формування та розвитку кіберосвіти як в Україні, так і в світі. Вони довели, що в сучасних умовах знання з кібербезпеки повинні входити до базових курсів усіх навчальних закладів, а не обмежуватися лише спеціалізованими напрямками в ІТ та кібербезпеці.

В [26] проведено комплексне наукове дослідження адміністративно-правових засад кібербезпеки в умовах гібридної війни. Це дослідження ґрунтувалося на аналізі чинного національного та міжнародного законодавства, а також практики його застосування та реалізації.

Мета статті — це здійснення аналізу наявного понятійно-термінологічного апарату у сфері підготовки фахівців із кібербезпеки.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

В сучасних умовах феномен кібербезпеки носить бінарний характер, тобто з однієї сторони її розглядають як елемент національної безпеки, а з іншої — як транснаціональний, позаяк інформаційний простір не має чітко визначених кордонів. В свою чергу це означає, що питання підготовки кваліфікованих кадрів даної галузі носить глобальний характер, актуальний не лише для України, а й для всього світу [3].

На сьогодні науковці і досі мають досить суперечливі погляди відносно термінів з приставкою «кібер-» (cyber-). Одним із перших хто використав термін «кібернетика», щоб позначити мистецтво управління був давньогрецький філософ Платон. Надалі, у 1834 р., цей термін вжив французький науковець Андре Марі Ампер, щоб дати визначення науці управління суспільством, яка в той час ще не існувала. Офіційно кібернетика бере свої витоки із наукової праці Норберта Вінера «Кібернетика», написаною 1947 р., в якій зазначається що кібернетика — це наука про управління та взаємозв'язок тварин та машин. У сучасному розумінні кібернетика — це наука про процес переробки інформації [1, с. 191].

Об'єктом дослідження кібернетики виступають так звані кібернетичні системи. Дані системи розглядають як сукупність об'єднаних елементів системи, що мають здатність до запам'ятовування, обробки та обміну інформацією між собою та зовнішнім світом. Головною функціональною кібернетичною системою, відомою на сьогоднішній день, є комп'ютер [4, с. 165].

Франсело Д. вказує на те, що термін «кібербезпека» набуває все більшого поширення в останні часи, проте водночас багато керівників служб безпеки і експертів з інформаційної безпеки мають певні непорозуміння щодо правильного використання цього терміну та визначення його контексту [21].

Слід зазначити, що поняття «кібербезпека» тісно взаємопов'язане із поняттям «безпеки інформації» зі сторони законодавчого, технологічного та правоохоронного сенсу. Поняття інформаційної безпеки має безліч трактувань, що обумовлюється різноманітністю підходів його розуміння.

Один із провідних представників німецького екзистенціалізму, Карл Ясперс, вніс концептуальні підходи до вивчення проблеми інформаційної безпеки. Екзистенційна філософія Ясперса у цьому контексті базується на розумінні безпеки людини, яке прямо пов'язане з інформацією про світ [26].

Кормич Б. А надає наступне визначення інформаційної безпеки — це захист правил, що встановлені законом, завдяки яким відбуваються всебічні інформаційні процеси держави, що забезпечують відповідні умови існування та розвитку суспільства і держави в цілому, гарантом чого виступає Конституція [5, с. 42].

Максименко Ю. Є, в свою чергу, характеризує інформаційну безпеку як кінцевий результат управління потенційними та реальними загрозами, задля забезпечення відповідності інтересів країни та суспільства в інформаційному просторі [6, с.186].

Отож, проаналізувавши вищевказані визначення, можна конкретизувати термін інформаційної безпеки як «захищеність країни та суспільства від імовірних та реальних небезпек в інформаційному просторі».

Термін «кібербезпека» вперше почали використовувати у 1990-х роках у США, коли дане питання почало гостро поставати у теренах країни [19].

Стратегія Франції, присвячена питанням кібербезпеки країни, пропонує нам наступне визначення даного терміну: кібербезпека — це такий стан інформаційної системи, який характеризують як задовільний за умови всебічного протистояння всім можливим загрозам доступності та цілісності конфіденційних даних [16].

Німецька стратегія кібербезпеки трактує її як сукупність певних заходів, спрямованих на мінімізацію ризиків. Більше того, в стратегії уточнюється, що базис кібербезпеки має становити комплексний підхід [17].

У стратегії кібербезпеки Канади термін «кібербезпека» не має чіткого визначення, хоча очевидно, що це охоплює захист кіберсистем від неправомірного використання та інших деструктивних атак. Стратегія визначає поняття кібератак і стверджує, що

кібербезпека служить засобом захисту від таких загроз. Також вона наголошує на необхідності протидії кіберзагрозам для ефективного та стратегічного використання кіберпростору, який вважається стратегічним активом [15].

Стратегія Канади [15] фокусується на захисті критичних систем, підтримці всієї країни, бізнесу та окремих громадян. Вона передбачає три основні напрями реалізації: перше — забезпечення захисту урядових систем через визначення повноважень та відповідальності, посилення безпеки інформаційних систем на федеральному рівні та підвищення рівня обізнаності уряду у сфері кібербезпеки; друге — співпраця з нефедеральними кіберсистемами через розвиток партнерських відносин з приватним сектором та суб'єктами критичної інфраструктури; третє — забезпечення безпеки громадян в кіберпросторі, що включає боротьбу з кіберзлочинністю та захист особистих даних.

У стратегії кібербезпеки Нідерландів наведено наступне визначення; кібербезпека — це об'єднані зусилля, направленні на протидію шкоді, що може бути завдана в результаті збою роботи інформаційних технологій чи їх невідповідного використання [18].

Стратегія [18] визначає, що до збоїв належать ситуації, коли надійність інформаційно-комунікаційних технологій знижується, обмежується доступність або порушується конфіденційність та/або цілісність збереженої в системах інформаційно-комунікаційних технологій інформації.

Незважаючи на ускладнення визначення критеріїв кібербезпеки, нідерландська стратегія вносить ключовий методологічний висновок: досягнення кібербезпеки можливе лише у системній взаємодії з розв'язанням завдань щодо захисту та забезпечення основних прав, цінностей і соціально-економічних вигод членів суспільства [21].

Національна стратегія кібербезпеки України закріплює визначення не самої кібербезпеки, а забезпечення кібербезпеки як стану протекції найважливіших суспільних та державних інтересів у сфері кіберпростору, що в свою чергу може бути досягнуто шляхом використання, комплексу організаційних, правових та інформаційних заходів [9].

В загальному, спираючись на визначення у науковій літературі, можна визначити, що кібербезпека — це заходи, спрямовані на захист даних від несанкціонованого доступу.

Аналіз взаємозв'язку між поняттями «інформаційна безпека» та «кібербезпека» показує, що з технологічної точки зору та зважаючи на забезпечення національної безпеки, кібербезпека, безумовно, є складовою інформаційної безпеки. Водночас, ті ж самі технічні характеристики є підставою розглядати кібербезпеку як самостійну категорію, що полягає у заходах із забезпечення громадської та міжнародної безпеки.

Наукові праці дослідників проблеми освіти фахівців кіберзахисту свідчать, що державна політика сфери національної безпеки наразі спрямована на підготовку висококваліфікованих кадрів кібербезпеки. За відсутності цього аспекту стає неможливим безпечна передача інформації та стрімкий науково-технічний розвиток країни в цілому.

Наразі процес профпідготовки кадрів кібербезпеки нашої країни стоїть на шляху становлення та має потребу у детальному дослідженні та стандартизації. Охарактеризувати наявну систему підготовки фахівців сфери кібербезпеки та надати найбільш вдале визначення узагальнене поняттю «система підготовки кадрів у сфері кібербезпеки» допоможе аналіз чинних нормативно-правових актів, що в подальшому дасть змогу окреслити головні шляхи щодо удосконалення процесу підготовки професіоналів зазначеного профілю.

На наступний день після прийняття концепції розвитку сектору безпеки і оборони України було затверджено першу редакцію Стратегії кібербезпеки України (Указ Президента України від 15 березня 2016 року № 96/2016), вважається базовим документом у сфері кібербезпеки [9]. Його мета полягала у створенні відповідних умов, задля забезпечення надійного функціонування кібернетичного простору.

Опираючись на положення Стратегії, розвиток подальшого потенціалу сфери кібербезпеки України мав здійснюватися відповідно до установленого порядку, включаючи розвиток галузі підготовки фахівців задля потреб органів сектору безпеки і оборони України та розвиток науково-виробничого потенціалу такої системи

Отже, згідно з положеннями Стратегії розвитку потенціалу сектору безпеки і оборони України у сфері забезпечення кібербезпеки, було заплановано здійснення різноманітних заходів, у тому числі спрямованих на підвищення ефективності підготовки кадрів для вимог органів управління сектору безпеки та оборони України. Також планувався розвиток науково-виробничого потенціалу цієї підготовчої системи [9].

У другій редакції Стратегії кібербезпеки України, а саме в Указі Президента України від 26 серпня 2021 року № 447/2021, були окреслені пріоритетні напрямки державних інтересів сфери кібербезпеки нашої країни [10]. В Стратегії зазначається, що діяльність, пов'язана із суб'єктами національної системи кібербезпеки, характеризується як недостатньо скоординована та, в основному, спрямовується на вирішення лише поточних завдань.

Як зазначають експерти даної галузі, першу стратегію було реалізовано не більш як на 40%. Нагальними залишилися питання швидкого обміну інформації щодо кіберзагроз, сталої ефективної моделі державно-приватного партнерства та результативної системи підготовки фахівців. Зважаючи на це, одним із пріоритетних завдань вказаної стратегії є проведення кардинального реформування системи підготовки кадрів у сфері кібербезпеки шляхом проведення наукових досліджень, перебудови системи підготовки фахівців та розгорненням ряду навчальних програм, курсів та тренінгів кібернавчання для всього населення [10].

Третім, проте не менш важливим, є Закон України «Про основні засади забезпечення кібербезпеки України», підписаний у травні 2017 року. Відповідно до цьому Закону було встановлено організаційно-правові базиси, мета яких полягає у забезпеченні захисту ключових інтересів суспільства та країни, національних стратегій держави у сфері кіберпростору, а також головні цілі та принципи політики держави у галузі кібербезпеки, компетенції державних установ, підприємств, органів та організацій, фізичних осіб та громадян у даній галузі, головні принципи регулювання узгодження їхньої діяльності задля забезпечення кібернетичної безпеки [11].

Статтею 10 [11] встановлено, що створення системи підготовки кадрів та підвищення компетентності фахівців у сферах кібербезпеки в Україні реалізується через взаємодію державних та приватних структур. Це є ключовим елементом національної системи кібербезпеки, який враховується у рамках стратегічного планування держави і сприяє прискоренню розробки відповідних механізмів для підготовки фахівців в області кібербезпеки для органів влади України.

Постанова Кабінету Міністрів України від 11 липня 2018 року № 481-р «Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України» стала першим розпорядженням, що стосується систем навчання з кібербезпеки, згідно з яким протягом 2-го півріччя 2018 року Адміністрація Держспецзв'язку, Міноборони та штаб ЗС України мусили розвивати таку систему, зокрема у:

- підготовці тактичних та оперативно-тактичних професіоналів у напрямі «кібербезпека»;
- підготовці, атестації та переатестації, підвищення кваліфікації фахівців в області кіберзахисту для закриття потреб державних органів, військових формувань і правоохоронних органів [12].

Важливо зазначити і про План реалізації Стратегії кібербезпеки України [23], що набув чинності із Указом Президента України від 1 лютого 2022 року № 37/2022, він спрямований на виконання комплексу заходів для збереження вже існуючого компетентного особового потенціалу в галузі кібербезпеки. Основна мета полягає в стимулюванні наукових досліджень і новітніх розробок в області кібербезпеки, що враховує зростаючі кіберзагрози і виклики. Крім цього, створюються національні інформаційні системи, платформи та продукти для забезпечення кібербезпеки. Заплановано впровадити ці заходи шляхом вдосконалення системи підготовки та покращення компетентності фахівців у галузі кібербезпеки. Ця ініціатива передбачає розроблення та реалізацію відповідної концепції впродовж періоду з 2022 по 2025 роки. Проведення цих заходів передбачає активну участь Кабінету Міністрів України, Міністерства освіти і науки України, Національного агентства України з питань державної служби та головних гарантів національної системи кібербезпеки.

Стаття 1 Закону України «Про освіту» описує систему освіти як комплексну систему, що включає різноманітні складові, рівні та ступені освіти, кваліфікації, програми навчання, освітні стандарти, ліцензійних умов, учбові заклади та інші елементи освітньої діяльності, учасників освітнього процесу, управлінські органи у галузі освіти, а також відповідні нормативно-правові акти, що регулюють їх взаємовідносини [13].

Опираючись на детально описану систему підготовки фахівців галузі кібербезпеки і термінологічну базу, яка закріплена в актах законодавства щодо забезпечення належного рівня кібербезпеки України, пропонуємо наступне узагальнювальне визначення вказаної системи: система підготовки кадрів сфери кібербезпеки — це комплекс принципів, положень та складових освітнього процесу, мета яких полягає у реалізації та забезпеченні стабільного розвитку цифрового суспільства та інформаційного простору, за допомогою підготовки професійних кадрів в обсязі, потрібному задля задоволення потреб сектора економіки держави та покращення обізнаності громадян України і фахівців різних областей з питань кібербезпеки.

До того ж, суб’єктами державної політики сфери кібербезпеки в рамках їхньої компетенції можуть розроблятися та реалізовуватися різноманітні заходи, зокрема освітні, у галузі кібербезпеки і проводитися різні інструктажі щодо дій у випадках непередбачуваних випадків та казусів у кіберпросторі.

Враховуючи вищеперераховане, можна узагальнити основні особливості, притаманні кіберосвіті сучасного рівня:

- безперервний ріст можливостей впливу на складові систем кібернетики;
- стрімка зміна кібернетичних, електронних та інфокомунікаційних технологій;
- величезна кількість характерних компонентів кібербезпеки;
- потреба у постійному оновлені відповідних знань у питаннях кібербезпеки;
- поділ на рівні навчання, відповідно до здатності та готовності учнів [14].

В [27] наголошено на тому, що висококваліфікований знавець своєї справи має бути прикладом особи, що забезпечує безпечну інформаційну діяльність і розуміється в усіх аспектам та нюансах інформаційної безпеки, а саме: юридичних, соціально-історичних, програмно-технічних, психологічних та педагогічних, позаяк інформаційні

ресурси та їх інфраструктура являється базисом, з яким майбутнім фахівцям доведеться працювати в наш час.

За висновками відомого дослідника та впливової постаті в сфері безпеки, професора Джованні Баттіста Карія, фахівець із кібербезпеки в компанії «Сентурія Інтел» повинен мати потенціал, який не тільки гарантує ефективне виконання своїх професійних обов'язків, але й сприяє професійному самовдосконаленню [28].

Арсенович Л. А. визначає, що фахівець із кібербезпеки — це спеціаліст галузі інформаційних технологій, який досконало володіє технологією побудови комп'ютерних систем та мереж, теорією проєктування, моделювання та конструювання систем управління доступом, комп'ютерних та інформаційних систем, а також підходами, засобами та технологіями адміністрування систем та мереж [29].

Аналіз наукових напрацювань і досліджень допомагає уточнити основне значення терміна «фахівець із кібербезпеки». Фахівець із кібербезпеки — це кваліфікований спеціаліст, який не лише забезпечує безпечну інформаційну діяльність, а й глибоко розуміє всі аспекти інформаційної безпеки, включаючи юридичні, соціальні, програмно-технічні, психологічні. Робота фахівця базується на інформаційних ресурсах та їх інфраструктурі, а його потенціал дозволяє ефективно виконувати професійні обов'язки та сприяти власному професійному розвитку.

Після початку повномасштабного вторгнення кібербезпека стала одним із найважливіших сфер, що потребують нагального та прискореного розвитку. Різноманітні освітні ініціативи щодо підготовки відповідних кадрів даної сфери існували і раніше, але за останні півтора року ми спостерігаємо тенденцію до появи можливостей та навчальних проєктів, які створюються не лише виключно для молодого населення країни, а й для громадян, що виявили бажання до зміни професійної діяльності.

Наприклад, Міністерством цифрової трансформації України у березні 2023 року було започатковано освітній проєкт під назвою «Restart in cyber» [22]. Дана програма має два етапи, а саме: онлайн курс по вивченню основ кібербезпеки на базі Toronto Metropolitan University (набуття теоретичної та бази) та підготовка до подальшого працевлаштування за допомогою компанії BazaIT, де учасники отримують необхідну інформацію щодо правил складання професійного резюме та проведення співбесіди. Вимоги для участі у даній програмі наступні:

– наявність досвіду роботи не менш як півтора року (галузь неважлива, проте це має бути не сфера кібербезпеки);
– знання англійської мови починаючи з рівня B2.

Результатом завершення курсу є всесвітньо визнаний сертифікат GIAC Foundational Cybersecurity Technologies (GFACT).

Отож, після проведеного аналізу можна підсумувати, що першочергові завдання сфери кіберосвіти такі: формування сталої національної політики кіберосвіти як однієї із пріоритетних складових процесу реформи освіти; підготовка, адаптація, організація доступності учнів до мультимедійних технологій та широкосмугового Інтернету у закладах освіти; створення онлайн-платформ, завдання яких полягає у допомозі та полегшенні освітнього процесу.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Конкретизована та правильно сформульована термінологія є основою на професійному шляху фахівців із кібербезбеки у їх головному робочому завданні —

забезпеченні кібербезпеки інформаційно-комунікаційної інфраструктури. Саме тому, починаючи з підготовчого етапу до майбутньої кар'єри спеціалістів, важливим є акцентування уваги суб'єктами учбового процесу на єдиному тезаурусі кібербезпеки. На сьогоднішній день такі визначення як «кібербезпека» та «інформаційна безпека» найчастіше застосовуються в практиці інформаційного захисту, дослідженнях пов'язаних із даною областю науки та в процесі освітньої діяльності. Галузево-понятійний апарат, за умов розвитку національної системи кібербезпеки, знаходиться на етапі формування.

Можливостями для подальшого розвитку даного напряму досліджень є усвідомлення проблеми соціальної потреби у якісній та кількісній підготовці майбутніх професіоналів сфери кібербезпеки з наукової сторони, більш детальне дослідження процесу власне підготовки кадрів та концептуальних основ організації учбової діяльності на прикладі інших країн.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Melnyk, S. (2016). Conceptual-categorical apparatus in the system of professional training of future experts of information and cyber security. *Information Technologies and Learning Tools, 55(5),* 187–197. https://doi.org/10.33407/itlt.v55i5.1497
2. *Кібербезпека як важлива складова всієї системи захисту держави*. (2018). Міністерство оборони України. https://www.mil.gov.ua/ukbs/kiberbezpeka-yak-vazhliva-skladova-vsiei-sistemi-zahistu-derzhavi.html
3. Діордіца, І. (2017). Система забезпечення кібербезпеки: Сутність та призначення. *Підприємництво, господарство і право, (7),* 109–116.
4. Мельник, С., Тихомиров, О., & Лєсков, О. (2011). До проблеми формування понятійно-термінологічного апарату кібербезпеки. *Збірник наукових праць Київського національного університету імені Тараса Шевченка, (30),* 165–172.
5. Кормич, Б. (2004). *Організаційно-правові основи політики інформаційної безпеки України*. [Автореф. Дис. докт. юрид. наук: 12.00.07].
6. Максименко, Ю. (2007). *Теоретико-правові засади забезпечення інформаційної безпеки України*. [Дис. канд. юрид. наук: 12.00.01].
7. Баранов, О. (2014). Про тлумачення та визначення поняття «кібербезпека». *Правова інформатика, (2),* 54–62.
8. Скрипник, Л. (2013). Щодо кібербезпеки. *СТСЗІ, (2),* 126–130.
9. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», Указ Президента України № 96/2016 (2016) (Україна).
10. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України», Указ Президента України № 447/2021 (2021) (Україна).
11. Про основні засади забезпечення кібербезпеки України, Закон України № 2163-VIII (2017) (Україна).
12. Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України, рішення Ради національної безпеки і оборони України № 481-р (2018) (Україна).
13. Про освіту, Закон України № 2145-VIII (2017) (Україна).
14. Даник, Ю., & Зінченко, А. (2018). Кіберосвіта та її особливості. *Військова освіта, (2),* 67–84. https://doi.org/10.33099/2617-1783/2018-2/67-84
15. *Canada's cyber security strategy: For a stronger and more prosperous canada*. (2010). Government of Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-cbr-scrt-strtgy/archive-index-en.aspx
16. *Information systems defence and security: France's strategy*. (2013). French Network and Information Security Agency. https://www.vie-publique.fr/rapport/33131-livre-blanc-sur-la-defense-et-la-securite-nationale-2013
17. *Cybersicherheitsstrategie für Deutschland 2021*. (2021). Bundesministerium des Innern und für Heimat. https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.html

18. *The Netherlands cybersecurity strategy 2022-2028.* (2022). National Coordinator for Counterterrorism and Security. https://english.nctv.nl/documents/publications/2022/12/06/the-netherlands-cybersecurity-strategy-2022-2028
19. Stubley, D. (2013). *What is cyber security?* 7elements. https://www.7elements.co.uk/resources/blog%20/what-is-cyber-security/
20. Franscella, J. (2013). *Cybersecurity vs. cyber security: When, why and how to use the term.* SecurityWeek. http://www.infosecisland.com/blogview/23287-Cybersecurity-vsCyber-Security-When-Why-and-How-to-Use-the-Term.html
21. Довгань, О., & Доронін, І. (2017). *Ескалація кіберзагроз національним інтересам україни та правові аспекти кіберзахисту*. Видавничий дім «АртЕк».
22. *За підтримки Мінцифри стартує програма безоплатного навчання спеціалістів з кібербезпеки*. (2023). Урядовий портал. https://www.kmu.gov.ua/news/za-pidtrymky-mintsyfry-startuie-prohrama-bezoplatnoho-navchannia-spetsialistiv-z-kiberbezpeky
23. Про План реалізації Стратегії кібербезпеки України, рішення Ради національної безпеки і оборони України (2021) (Україна).
24. Барановський, О. (2021). *Кіберпрофесіонали для держави в XXI столітті*. Національний кластер кібербезпеки. https://cybersecuritycluster.org.ua/blog/kiberprofesionaly-dlya-derzhavy-v-hhi-stolitti/
25. Жора, В. (2023). *Кібербезпека потребує кадрів: Чому держава та бізнес повинні співпрацювати*. ЕКОНОМІЧНА ПРАВДА. https://www.epravda.com.ua/columns/2023/02/27/697467/
26. Веселова, Л. (2021). *Адміністративно-правові основи кібербезпеки в умовах гібридної війни* [Дис. докт. юрид. наук: 12.00.07] Одеський державний університет внутрішніх справ.
27. Джалладова, І. (2015). Політика інформаційної безпеки: Науково-прикладні аспекти і проблеми підготовки фахівців. *Моделювання та інформаційні системи в економіці, (91),* 57–75.
28. Бистрова, Б. (2018). *Професійна підготовка бакалаврів з кібербезпеки у вищих навчальних закладах США* [Дис. канд. пед. наук: 13.00.04]. Інститут педагогічної освіти і освіти дорослих НАПН України.
29. Арсенович, Л. (2022). Понятійно-категоріальний апарат у сфері підготовки фахівців із кібербезпеки органів державної влади України. *Наукові перспективи, (2),* 33–53.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (23), 2024
ISSN 2663 - 4023

Horlichenko Serhii
Researcher
Institute of Special Communication and Information Protection
National Technical University of Ukraine "Ihor Sikorsky Kyiv Polytechnic Institute"
ORCID 0000-0002-8999-7526
serhii.horlichenko@gmail.com

FEATURES OF MODERN CONCEPTUAL AND TERMINOLOGICAL APPARATUS IN THE FIELD OF TRAINING OF CYBER SECURITY SPECIALISTS

Abstract. The article examines the relevance of ensuring the sustainable development of high-quality cyber security of the state, as the main component of a modern digital society. Guidelines for the training of personnel of cyber security agencies of Ukraine were studied. The main normative legal acts regulating the system of educational training of experts in the domain of cyber security have been analyzed. The education system of personnel education in the cyber security niche is generally characterized and compared with the main elements of the general education system of Ukraine. The theoretical aspects of the formation of the system of training professionals specializing in cyber security are considered, the peculiarities and prospects of its functioning in today's conditions are determined. A generalized concept of "system of personnel training in the field of cyber security" is proposed as a set of elements of educational activity, the purpose of which is to implement and ensure the enduring development of the digital society by training the necessary amount of personnel in the cyber security niche of the country. Fixed on the scientific achievements of domestic and foreign scientists in the field of education, the newest educational elements are outlined and concepts in the process of modern education. The definition of "cyber security" in the cyber security strategies of the world's leading countries was analyzed and compared with the definition given in the national strategy for cybersecurity of Ukraine. The author's vision of the term "cyber security" is proposed on the basis of researched scientific literature and official documents, taking into account communicative, sociological, and political aspects. A number of scientific developments in the field of cyber and information security were studied in order to generalize the essence of the definition of "cyber security specialist". A conclusion was made regarding the importance of the proper functioning of the system of training qualified personnel in the field of cyber security. It is proposed to conduct a more detailed study of the process of personnel training itself and the conceptual foundations of the organization of educational activities on the example of other countries of the world.

Keywords: cyber security; digital society; informational security; cyber education; information technologies.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Melnyk, S. (2016). Conceptual-categorical apparatus in the system of professional training of future experts of information and cyber security. *Information Technologies and Learning Tools, 55(5),* 187–197. https://doi.org/10.33407/itlt.v55i5.1497
2. *Cyber security as an important component of the entire system of state protection*. (2018). Ministry of Defence Ukraine. https://www.mil.gov.ua/ukbs/kiberbezpeka-yak-vazhliva-skladova-vsiei-sistemi-zahistu-derzhavi.html
3. Diorditsa, I. (2017). The cyber security system: Essence and purpose. *Pidpryiemnytstvo, hospodarstvo i pravo, (7),* 109–116.
4. Melnyk, S., Tikhomirov, O., & Leskov, O. (2011). To the problem of formation of the conceptual and terminological apparatus of cyber security. *Collection of scientific works of Taras Shevchenko Kyiv national University, (30),* 165–172.
5. Kormych, B., (2004) *Legal and organizational basis of the policy of information security of Ukraine*. [The studies for the degree of doctor of legal Sciences spec.: 12.00.07].
6. Maksymenko, Y., (2007). *Theoretical-legal bases of ensuring of information security of Ukraine*. [Thesis of the Candidate of Legal Sciences: 12.00.01].
7. Baranov O., (2014). On the interpretation and definition of "cybersecurity". *Legal Informatics, (2),* 54–62.

8. Skrypnyk, L., (2013) Regarding of cybersecurity. *STSZI, (2),* 126–130.
9. On the decision of the National Security and Defense Council of Ukraine dated January 27, 2016 "On the Cybersecurity Strategy of Ukraine", Decree of the President of Ukraine № 96/2016 (2016) (Ukraine).
10. On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine", Decree of the President of Ukraine № 447/2021 (2021) (Ukraine).
11. On the main principles of ensuring cyber security of Ukraine, Law of Ukraine № 2163-VIII (2017) (Ukraine).
12. On approval of the 2018 action plan for the implementation of the Cybersecurity Strategy of Ukraine, order of the Cabinet of Ministers of Ukraine № 481-p (2018) (Ukraine).
13. On education, Law of Ukraine № 2145-VIII (2017) (Ukraine).
14. Danyk, Yu., & Zinchenko, A. (2018). Cyber education and its features. *Military Education, (2),* 67–84. https://doi.org/10.33099/2617-1783/2018-2/67-84
15. *Canada's cyber security strategy: For a stronger and more prosperous canada*. (2010). Government of Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-cbr-scrt-strtgy/archive-index-en.aspx
16. *Information systems defence and security: France's strategy*. (2013). French Network and Information Security Agency. https://www.vie-publique.fr/rapport/33131-livre-blanc-sur-la-defense-et-la-securite-nationale-2013
17. *Cybersicherheitsstrategie für Deutschland 2021*. (2021). Bundesministerium des Innern und für Heimat. https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.html
18. *The Netherlands cybersecurity strategy 2022-2028.* (2022). National Coordinator for Counterterrorism and Security. https://english.nctv.nl/documents/publications/2022/12/06/the-netherlands-cybersecurity-strategy-2022-2028
19. Stubley, D. (2013). *What is cyber security?* 7elements. https://www.7elements.co.uk/resources/blog%20/what-is-cyber-security/
20. Franscella, J. (2013). *Cybersecurity vs. cyber security: When, why and how to use the term.* SecurityWeek. http://www.infosecisland.com/blogview/23287-Cybersecurity-vsCyber-Security-When-Why-and-How-to-Use-the-Term.html
21. Dovgan, O., & Doronin, I. (2017). *Escalation of cyber threats to the national interests of Ukraine and legal aspects of cyber protection*. Publishing house «ArtEk».
22. *With the support of the Ministry of Digital Affairs, a free training program for cyber security specialists will be launched*. (2023). Government portal. https://www.kmu.gov.ua/news/za-pidtrymky-mintsyfry-startuie-prohrama-bezoplatnoho-navchannia-spetsialistiv-z-kiberbezpeky
23. About the Implementation Plan of the Cybersecurity Strategy of Ukraine, the decision of the National Security and Defense Council of Ukraine (2021).
24. Baranovskyi, O. (2021). *Cyber professionals for the state in the 21st century*. National cyber security cluster. https://cybersecuritycluster.org.ua/blog/kiberprofesionaly-dlya-derzhavy-v-hhi-stolitti/
25. Zhora, V. (2023). *Cybersecurity needs staff: Why government and business should work together*. ECONOMIC TRUTH. https://www.epravda.com.ua/columns/2023/02/27/697467/
26. Veselova, L. (2021). *Administrative and legal foundations of cyber security in conditions of hybrid warfare* [Thesis of the degree of doctor of Legal Sciences: 12.00.07] Odessa State University of Internal Affairs.
27. Jalladova, I. A. (2015). Information security policy: Scientific and applied aspects and problems of training specialists. *Modeling and information systems in the economy*, (91), 57–75.
28. Bystrova, B. (2018). *Professional training of bachelors in cyber security in higher educational institutions of the USA* [Thesis of the Candidate of Pedagogical Sciences: 13.00.04] Institute of Pedagogical Education and Adult Education of the National Academy of Pedagogical Sciences of Ukraine.
29. Arsenovych, L. (2022). Conceptual and categorical apparatus in the field of training specialists in cyber security of state authorities of Ukraine. *Scientific perspectives, (2),* 33–53.