CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

DOI 10.20535/2411-1031.2023.11.1.283635
УДК 371.3

ОЛЕКСАНДР ПУЧКОВ,
ОЛЕНА УВАРКІНА

СТАЛИЙ РОЗВИТОК СИСТЕМИ ФОРМАЛЬНОЇ КІБЕРОСВІТИ: РЕФЛЕКСІЯ СУЧАСНИХ КОНЦЕПТІВ

У статті визначений концептуальний каркас сталого розвитку формальної кіберосвіти. Проведено аналіз сучасних нормативно-правих та наукових джерел з проблем підготовки кіберфахівців для сектору безпеки та оборони. Основними методами дослідження визначено: метод синтезу, порівняльний метод, метод фокусування, причинно-наслідковий метод. Проаналізована нова Стратегія кібербезпеки США щодо питань кіберосвіти, яка визначає нові вимоги до кіберфахівців в умовах трансформації глобального та національного безпекового середовища. Використання даних аналізу освітніх програм з кібербезпеки ЄС, показало характерну мінливість освітнього ландшафту кібербезпеки в ЄС та дало змогу визначити основні прогалини у підготовці майбутніх професіоналів. Доведено, що інтеграція української кіберосвіти в євроатлантичний освітній простір має відбуватися через оновлення навчальних програм з кібербезпеки на основі найкращого міжнародного досвіду, створення єдиної системи акредитації, сертифікації та розвитку кіберплатформ електронного навчання для формальної освіти. Визначено, що компетентнісний підхід у підготовці кіберфахівців є пріоритетним напрямком у дослідженнях науковців з різних галузей знань. З'ясовано, що у тріаді компетентностей «знання-уміння-навички» відбувається гістерезис навичок, набутих під час навчання від вимог передових технологій у професійної діяльності.

Ключові слова: кібербезпека, формальна кіберосвіта, кіберфахівець, сталий розвиток.

Постановка проблеми. Експоненційна цифровізація суспільства прискорює процеси трансформації системи кіберосвіти та відкриває нові перспективи для удосконалення освітнього кіберпростору та вирішення основних цілей сталого розвитку. Складний процес трансформації кіберосвіти у бік євроатлантичної інтеграції характеризується як вибірковою елімінацією старих освітніх догм, так і еволюційними досягненнями світової науки і техніки, які, безсумнівно, впливають на якість підготовки сучасного кіберфахівця. Зрештою, рефлексивна наукова ініціативність визначення основних ланок формальної кіберосвіти, її інтенцій та конотацій, об'єктивно актуалізується протистоянням всього демократичного світу агресії рф та ролі кіберфахівців у досягнення переваг у п'ятивимірній війні сучасності.

Аналіз останніх досліджень і публікацій. На теренах сучасного наукового простору інтерес до проблем кіберосвіти та її трансформації перебуває завперш в епіцентрі дискурсу військових фахівців, серед яких варто зазначити наукові праці В.М. Телелима, Ю.Г. Даника, А.О. Зінченка, О.В. Корнейка, С.І. Мельника та ін. Питома вага досліджень вітчизняних освітян з різних галузей знань науки і техніки присвячена компаративному аналізу підготовки фахівців із кібербезпеки у провідних країнах світу (Б. Бистрова, О.В. Євсюкова, О.К. Юдін, О.В. Матвійчук-Юдіна, О. Овчарук, А. Войцеховський, М. Гаврільцев, Т. Дзюба, Є. Таран та ін.). Основним концептуальним орієнтиром розвитку сучасної кіберосвіти, безсумнівно, є опублікована нова Стратегія кібербезпеки США, яка у сучасній безпековій ситуації стає

своєрідним габітусом світового інформаційного простору та започатковує нову довгострокову політику ключового українського міжнародного партнерства у сфері безпеки та оборони та спрямовує основні парадигми трансформації підготовки кіберфахівців на швидку та якісну підготовку професійних кадрів. З урахуванням затвердження нової Національної стратегії кібербезпеки США, актуалізується питання системного аналізу сучасних концептів сталого розвитку формальної кіберосвіти.

Методи дослідження. Для визначення функціонально-інструментальних особливостей дослідження сучасних концептів сталого розвитку системи формальної кіберосвіти варто зазначити, що «метод – це взаємопотенціююче поєднання принципів та вимог, що орієнтують суб'єкта в його пізнавальній і предметно-практичні діяльності» [1]. Тому для з'ясування основних характеристик, функцій та взаємодії кіберосвіти в освітньому просторі використовується системний науковий метод, а причинно-наслідковий метод визначає основні тенденції та динаміку трансформаційних процесів в системі підготовки фахівців. Шляхи оптимізації кіберосвіти досягаються використанням праксеологічного методу, а для цілісності та об'єднання всіх складових системи кіберосвіти застосовується метод синтезу. У дослідженні активно використовується порівняльний метод для виявлення специфіки та структуризації сучасних концептів, а також метод фокусування для акцентування уваги на окремих (здебільшого найважливіших на даному етапі дослідження) аспектах сталого розвитку кіберосвіти.

Метою статті є вивчення основних концептів розвитку кіберосвіти, яка в останньому цифровому десятилітті стає пріоритетним вектором безпеки у кіберпросторі.

Виклад основного матеріалу дослідження. Рефлексійно намагаючись визначити концептуальний каркас сталого розвитку формальної кіберосвіти у сучасному цифровому десятилітті, апріорно, завперш, звертаємо увагу на оприлюднену 1 березня 2023 року Національну стратегію кібербезпеки США (Стратегія США), у якої започаткована нова довгострокова політика ключового українського міжнародного партнерства у гармонізації безпекових підходів. Безсумнівно, що російська агресія проти України спричинила зміни у пріоритетах як глобального, так і національного безпекового середовища. Тому у фокусі уваги Стратегії США (Ціль 4.6) зазначена національна інтенція комплексного та скоординованого підходу державної політики у напрямку розширення доступу до кіберосвіти. Розробку та впровадження Національної стратегії кібертрудових ресурсів та освіти доручено ONCD (Office of the National Cyber Director), який має задовольнити потребу в експертних знаннях з кібербезпеки в усіх секторах економіки для продовження впровадження інновацій в безпечні та стійки технології наступного покоління. Серед завдань політики кібербезпеки є залучення стратегічних державних інвестицій в інновації, науково-дослідні й дослідно-конструкторські роботи (НДДКР) через використання регіональної програми інноваційного розвитку Національного наукового фонду (NSF), довгострокових програм безпечного та надійного кіберпростору, нових грантових програм, включаючи Національну ініціативу з кіберосвіти (NICE), програму CyberCorps: стипендія для служби, програму Національних центрів академічної майстерності в галузі кібербезпеки, програму навчання та допомоги з питань кібербезпеки [2].

Між іншим, з метою покращення довгострокової позиції у сфері кібербезпеки та створення чіткої стратегії розвитку кадрового потенціалу і було створено NICE Flamework (Національна ініціатива з кібербезпекової освіти), яка займається інформуванням, формальною освітою, професійною підготовкою та структурою кіберфахівців у США. NICE Flamework, відповідаючи нещодавно на інформаційний запит відповідної великої корпорації, вказувало, що «теперішнє освітнє середовище не забезпечує загального базового набору навичок, на основі яких можна побудувати конкретні знання, необхідні для задоволення вимог роботодавців до робочої сили». Нездатність вирішити цю проблему негативно впливає на

спроможність сучасного цифрового суспільства у реалізації новітніх розробок. Важливість знань з кібербезпеки зараз широко визнана, але потреба в їх широкому застосуванні залежить від навичок кібербезпеки. У цьому контексті навички розуміються як поєднання здібностей, знань і досвіду, які дозволяють людині добре виконувати професійні завдання. Дослідження навичок у сфері інформаційно-комунікаційних технологій, яке щорічно проводить Enterprise Strategy Group, показало, що розрив у навичках у сфері кібербезпеки продовжує збільшуватися та подвоївся за останні п'ять років. Відсоток відповідей, у яких організації повідомляли про брак навичок, зріс з 23 до 51% лише за два роки. Ця проблема виникає в багатьох галузях промисловості та організаціях, і занепокоєння виходить далеко за межі звичайної освіти з ІКТ та розвитку навичок. За прогнозами Cybersecurity Ventures на 2021 рік на світовому ринку праці буде 3,5 мільйона незаповнених посад у сфері кібербезпеки, що свідчить про відставання у підготовці висококваліфікованих кіберфахівців в умовах різкого зростання кіберзлочинності [3].

З цих міркувань, Європейська організація з кібербезпеки (ECSO) для вирішення проблеми дефіциту кіберфахівців пропонує розглядати кібербезпеку як нову метадисципліну, яка ліквідує гістерезис кіберосвіти від вимог сучасності не тільки через залучення вчених зі знаннями, практичним досвідом, дослідницьким досвідом та академічними прагненнями, але і через оновлення навчального плану освітніх програм з кібербезпеки з чітким розумінням різноманітних потреб у цій галузі. Дослідники кіберосвіти в ЄС вважають необхідним вирішення наступних проблем: методологічне оновлення навчальних програм у вишах з орієнтацією на актуальні запити суспільства у сфері кібербезпеки для різних галузей та підприємств та створення єдиної для ЄС системи акредитації та сертифікації. Перед формальною кіберосвітою ЄС стоїть завдання підготувати фахівців, які будуть навчені ефективно вирішувати промислові, наукові, суспільні і політичні питання у сфері кібербезпеки [4].

Різноманітність навичок кібербезпеки визнає і корпорація CISCO, яка вже для української формальної кіберосвіти пропонує цілий спектр різноманітних по тематиці курсів, таких як Switching&Routing, CiberSecuritateOperation, CCNA Securitate, які забезпечують можливість систематизувати знання, отримані при вивченні дисциплін навчального плану, отримувати відомості про найсучасніші цифрові технології, вдосконалювати практичні навички налаштування мережевого обладнання, а також за результатами навчання отримати сертифікат про її закінчення міжнародного зразку.

Широкий спектр розвитку кібернавичок пропонує і компанія IBM, яка об'єднала провідних експертів з кібербезпеки, архітекторів із сертифікації для створення програм швидкого розвитку кіберосвіти на різних освітніх рівнях. Через канал SkillsBuild компанія IBM надає персоналізований коучинг та навчання, через канал IBM Skilis Academy забезпечує IT-навчання мережі вищих навчальних закладів, а також проводить навчальну академію з кібербезпеки через забезпечення безкоштовним технічним навчанням продуктам IBM Security [5].

Нагальна потреба світового суспільства у фахівцях з кібербезпеки сприяє розвитку багатьох кіберплатформ електронного навчання (Coursera; Udacity; edX), але прикладом формальної кіберосвіти може служити магістерська програма Simplilearn Cyber Security Expert, яка передбачає отримання провідних у галузі кібербезпеки сертифікатів, таких як CompTIA Security+, CEH, CISM, CISSP і CCSP [6], а також унікальна база даних ENISA, яка містить перелік програм кібербезпеки в ЄС (Освітня карта ЄС з кібербезпеки). Перелік освітніх програм на карті не закритий, оскільки доступний протокол для подальших доповнень. Будь-який вищий навчальний заклад може подати визнану (державою-членом ЄС) програму, надавши інформацію про ступінь (бакалавр, магістр) за допомогою спеціального шаблону ENISA де для отримання для ступеня бакалавра 25% модулів, що викладаються,

мають бути темами з кібербезпеки; а для отримання ступеня магістра принаймні 40% модулів, що викладаються, мають бути темами кібербезпеки. [4]. Зрештою, в наш час цифрових технологій це дозволяє талановитим молодим людям приймати обґрунтовані рішення щодо різноманітних можливостей, які пропонує вища освіта ЄС у сфері кібербезпеки, і допомагає університетам залучати висококваліфікованих студентів, мотивованих підтримувати кібербезпеку Європи.

Проблема забезпечення суспільства фахівцями з кібербезпеки на вимогу глобального цифрового світу розширює можливості доступу до найкращих кіберосвітніх програм сучасності та залишається пріоритетним напрямом та стратегічним імперативом всіх країн-партнерів НАТО. Для України це стало основною траєкторією реформування української системи кіберосвіти протягом останнього цифрового десятиліття, як нагальна потреба своєчасного та ефективного «виявлення, запобігання і нейтралізації реальних загроз національній безпеці України у кіберпросторі» [7].

На виконання завдань євроатлантичної інтеграції кіберосвіти, Державна служба спеціального зв'язку та захисту інформації України (далі – Держспецзв'язку), як один з основних суб'єктів національної системи кібербезпеки у кіберпросторі, пропонує реформувати систему кіберосвіти через запровадження нових професійних стандартів на основі досвіду Європейської рамки кваліфікацій та американської Стратегічної освітньої ініціативи у сфері кібербезпеки. Перші шість професійних стандартів, які були розроблені за підтримки Проєкту USAID Cybersecurity Activity «Кібербезпека критично важливої інфраструктури України», вже пройшли етапи публічного обговорення, дістали позитивні висновки експертизи Національного агентства кваліфікацій та були затверджені головою Держспецзв'язку Юрієм Щиголем. Затверджені стандарти відтепер є основою для запровадження нових спеціалізацій та оновлення освітніх програм вищої освіти за напрямками підготовки фахівців з кібербезпеки. Враховуючи, що в умовах війни п'ятого виміру виникає гостра потреба у висококваліфікованих кіберфахівцях, у 2023 році Держспецзв'язку планує розробити професійні стандарти для 14 нових професій з кібербезпеки, гармонізованих з положеннями NICE Flamework на основі найкращого міжнародного досвіду [8].

Як беззастережний факт слід визнати, що ідеї, які використані в новій Стратегії США, вже впроваджуються у вітчизняну кібербезпекову політику: визначено Уповноважений орган у сфері захисту критичної інфраструктури України (Держспецзв'язку), впроваджуються міжнародні стандарти кібербезпеки КІ – зокрема, NIST Cybersecuriti Flamework, на базі Держспецзв'язку створений Центр активної протидії агресії у кіберпросторі [9]. Зрештою, скоординовані спільні дії міжнародних партнерів у сфері інновацій, науково-дослідних розробок та освіти, посилюють сталий розвиток кіберосвіти, як основи безпечних технологій наступних поколінь та захисту цифрової екосистеми.

Аналіз сучасних зарубіжних та вітчизняних джерел, показав, що проблемний горизонт концептуального каркасу сталого розвитку формальної кіберосвіти в Україні і надзвичайно широкий у своєму євроатлантичному інтегральному спрямуванні, і симптоматично нечіткий та невиразний у питаннях реконструкції традиційної освітньої матриці.

Разом з тим, впровадження освітніх стандартів НАТО у підготовку військових кіберфахівців були визначені у законодавстві в сфері освіти через зміни до деяких законів. Наприклад, до Закону України «Про вищу освіту» (2014) у Розділі I, статтю 1 додано нову редакцію визначення термінів «вищий військовий заклад освіти» та «заклад вищої освіти із специфічними умовами навчання», а у Законі України «Про наукову і науково-технічну діяльність» (2016) статтю 13 було також доповнено положеннями про встановлення особливих вимог у сфері управління відповідних наукових установ, вищих військових навчальних закладів, закладів вищої освіти із специфічними умовами навчання, військових навчальних підрозділів закладів вищої освіти [10].

Крім того, затверджена у 2021 році Політика Міністерства оборони у сфері військової освіти зазначає, що основні проблеми у сфері освіти треба розв'язати через «оновлення, застосування нових підходів до формування її структури та змісту» на основі застосування нових форм і методів кращих вітчизняних та закордонних практик [11].

Слід зазначити, що основні напрями реформування системи підготовки фахівців у сфері кібербезпеки регулюються Планом реалізації Стратегії кібербезпеки України (2022) [12], який в умовах агресивних дій рф проти України ще більше актуалізує трансформаційні процеси у системі кіберосвіти для якісної підготовці фахівців так званої «нелетальної зброї».

Водночас розширення горизонтів трансформації української безпекової доктрини у напряму європейської і євроатлантичної інтеграції спрямовує фахівців з кібербезпеки на вирішення головного завдання розвитку системи кібербезпеки – «гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури» [13] та врахування того, що «можливості комунікативного впливу на ворога зрівнялися й перевищили можливості збройного впливу» [14].

В умовах воєнного стану, наприклад, проблема ransonware менш помітна в Україні, ніж у західних країнах. Тому значна увага до трансформації системи кіберосвіти приділяється сфері сектору безпеки та оборони України (СБОУ).

З огляду на зазначену обставину, крім цивільних вищих навчальних закладів, підготовка фахівців у сфері кібербезпеки з вищою освітою для державних органів і формувань СБОУ ведеться також у вищих військових навчальних закладах, що підпорядковані або знаходяться в сфері управління Міністерства Оборони України, Генерального штабу Збройних Сил України, Міністерства внутрішніх справ України, Адміністрації Держспецзв'язку, Служби безпеки України, Державної служби України з надзвичайних ситуацій, Державної прикордонної служби України, розвідувальних органів України тощо. Щоправда, вітчизняні дослідники звертають увагу, що, на відміну від певною мірою налагодженої системи підготовки кіберфахівців у цивільних вишах, актуальною проблемою в системі підготовки фахівців з питань кібербезпеки та загальної кіберосвіти для всіх фахівців СБОУ залишається відсутність єдиної методології до змістовного осучаснення всіх аспектів галузі знань «Інформаційна безпека», враховуючи загострення протиборства у кібернетичному просторі та експоненціальну цифровізацію суспільства [15].

У подібному контексті проблему реформування кіберосвіти на основі компетентнісного підходу, який потенційно має озброїти майбутніх кіберфахівців необхідними для забезпечення професійного виконання завдань компетентностями, бачать і дослідники, і освітяни. Після завершення процесу відпрацювання стандартів освіти на основі компетентнісного підходу, освітні програми для підготовки здобувачів вищої освіти на першому (бакалаврському) та другому (магістерському) рівні мають містити перелік компетентностей випускника, якими він повинен оволодіти за різними формами організації навчання для успішної майбутньої професійної діяльності на первинних посадах в частинах та підрозділах. Однак, цей концепт також пропонує і розробку інноваційних заходів в організації освітнього процесу кожного навчального закладу з урахуванням специфічних особливостей підготовки спеціальностей, які готуються у ВВНЗ та військових навчальних підрозділах вищих навчальних закладів [16]. Дійсно запропоновані авторами методики навчання на платформі Moodle спрямовані на підвищення якості освіти і, на нашу думку, можливі при використанні позитивних механізмів оптимізації освітнього процесу у підготовці військових кіберфахівців.

Очевидно, що компетентнісна парадигма у концептуальному каркасі формальної кіберосвіти відчутно домінує у науковому дискурсі, дихотомічно впливаючи на розвиток інших концептів трансформації підготовки кіберфахівців у вишах. Наприклад, проблемний горизонт актуального питання гістерезису тріади «знання-уміння-навички» при навчанні від вимог поточної реальності, для якої характерні швидкі та приголомшливі зміни у галузях

передових технологій цифрового світу, парадигмально розглядається переважно у зарубіжних дискурсах. Слід зазначити, що опитування Cybersecurity 4Europe вивчало контент, який надається на рівні вищої освіти та в рамках присуджених ступенів магістра. Вивчення даних із зібраних 104 освітніх програм у більшості країн-члені ЄС, показало, що у 92% навчальних програм більшість обов'язкових тем присвячено питанням безпеки даних (криптографія, цифрова криміналістика, цілісність даних та автентифікація), а у 84% програм наявні теми, що стосуються безпеки підключення (архітектура обладнання, розподілені системи). Дослідники звернули увагу на недостатню кількість (60%) тем у програмах, присвячених організаційним, кадровим, соціальним, експлуатаційним та технічним дисциплінам, а саме: управління ризиками, політика та адміністрування, людський і соціальний захист (кіберзлочинність, конфіденційність та соціальна інженерія). Наприклад, як стверджують дослідники, тема у сфері конфіденційності була знайдена лише у 30% обов'язкових дисциплін, а тема документації, яка пов'язана з кібербезпекою була присутня лише у 15% курсів. Але незбалансований розподіл тем у навчальних програмах не є показовим для Іспанії, Франції, Німеччини та Італії. У цих країнах освітні програми охоплюють 75% розділів знань у своїх обов'язкових курсах [4].

Занепокоєність ЄС недостатнім вивченням організаційних або людських аспектів кібербезпеки у вишах ЄС є позитивно потенціальним напрямом роботи над осучасненням 137 (за даними сайту osvita.ua) українських освітніх програм за спеціальністю 125 Кібербезпека для заповнення цієї змістовної прогалини. Тому, на нашу думку, у питанні створення нових підходів до підготовки кіберфахівців не варто поспішати погоджуватися з концепцією поглибленого технічного оволодіння студентами сучасними інформаційними технологіями (за рахунок гуманітарної складової) та збільшення використання цифрових засобів навчання, як це зазначається у публікації європейських військових викладачів [17].

Висновки. Рефлексія основних парадигм підготовки кіберфахівців показала, що амплітуда концептуальних точок зору на проблемний горизонт трансформаційних процесів в системі формальної кіберосвіти коливається в надзвичайно широких межах. Концептуальний каркас формальної кіберосвіти сталого розвитку має багаторівневий комплекс пропозицій до її покращення на основі оновлення освітніх програм у вишах на вимогу реального часу, євроатлантичної інтеграції, збалансованості навчальних програм з відповідних спеціальностей між ВВНЗ зоднобіч та, здругобіч, дотримання та урахування певних специфічних особливостей підготовки кіберфахівців для різних галузей, поглиблення технічного оволодіння сучасними інформаційними технологіями, обов'язкового включення в навчальні програми людських аспектів кібербезпеки, розроблення професійних стандартів для нових професій з кібербезпеки на основі найкращого міжнародного досвіду, розвиток кіберплатформ електронного навчання для формальної освіти, подолання гістерезису компетентностей та створення єдиної системи акредитації та сертифікації.

Трансформації глобального та національного безпекового середовища вкотре нагадали світу про необхідність захисту кіберпростору та виявили відчутний дефіцит у кіберфахівцях, підготовка яких залишається у фокусі міжнародного партнерства у заходах щодо гармонізації безпекових підходів.

У перспективі для подальших досліджень у цій сфері необхідна філософська рефлексія особливостей війни у кіберпросторі для захисту критичної інфраструктури та посилення безпеки IoT-пристроїв.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] З. Ф. Самчук, *Світоглядні основи соціально-філософського дослідження ідеології: Проблема критеріїв та пріоритетів вибору, т. 1*. Дніпропетровськ, Україна: АРТ-ПРЕС, 2009.

[2] *Strategy, National Cybersecurity Strategy*. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf. Accessed on: Mar. 01, 2023.

[3] B. J. Blažič, "Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?", *Educ. Inf. Technol.*, 2021, doi: https://doi.org/10.1007/s10639-021-10704-y. Accessed on: May 03, 2023.

[4] Higher Education in Europe: Understanding the Cybersecurity Skills Gap in the EU, 2021. [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/higher-education-in-europe-understanding-the-cybersecurity-skills-gap-in-the-eu. Accessed on: Feb. 12, 2023.

[5] D. Leaser, Future of Work / The demand for cybersecurity professionals is outstripping the supply of skilled workers. [Online]. Available: https://www.ibm.com/blogs/ibm-training/new-cybersecurity-threat-not-enough-talent-to-fill-open-security-jobs. Accessed on: Apr. 22, 2023.

[6] Cyber security expert / master's program. [Online]. Available: https://www.simplilearn.com/cyber-security-expert-master-program-training-course. Accessed on: May 06, 2023.

[7] Верховна Рада України. 7 сесія (2017, Жовт. 5). *Закон № 2163-VIII, Про основні засади забезпечення кібербезпеки України*. [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/2163-19#Text. Дата звернення: Груд. 18, 2022.

[8] *Cyber Digest. Огляд подій в сфері кібербезпеки, грудень 2022*. Київ, Україна: Національний координаційний центр кібербезпеки, 2022. [Електронний ресурс]. Доступно: https://www.rnbo.gov.ua/files/НКЦК/НКЦК-1/Cyber%20digest_December_2022.pdf. Дата звернення: Січ. 18, 2023.

[9] Д. Дубов, *Національна стратегія кібербезпеки США 2023: критична інфраструктура, координація, проактивність. Аналітична записка*. Київ, Україна: Національний інституту стратегічних досліджень, 2023.

[10] Верховна Рада України. 6 сесія. (2021, Груд. 17). *Закон України № 1986-IX, Про внесення змін до деяких законів України щодо військової освіти та науки*. [Електронний ресурс]. Доступно: https://https://zakon.rada.gov.ua/laws/show/1986-20#Text. Дата звернення: Квіт. 19, 2023.

[11] Міністерство оборони України. (2021, Груд. 15). *Політика Міністерства оборони України у сфері військової освіти*, 2021. [Електронний ресурс]. Доступно: https://www.mil.gov.ua/content/education/politika_mou_osvita.pdf. Дата звернення: Квіт. 19, 2023.

[12] Рада національної безпеки і оборони України. (2021, Груд. 30). *Рішення Ради національної безпеки і оборони України "Про План реалізації Стратегії кібербезпеки України"*. [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text. Дата звернення: Квіт. 23, 2023.

[13] Рада національної безпеки і оборони України. (2020, Верес. 14). *Рішення Ради національної безпеки і оборони України "Про Стратегію національної безпеки України"*. [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/n0005525-20#Text. Дата звернення: Квіт. 27, 2023.

[14] Д. Кулеба, *Війна за реальність. Як перемагати у світі фейків, правд і спільнот*. Київ, Україна: Книголав, 2022.

[15] Y. Danyk, and O. Korneiko, "Fundamentals methodology of formation cyber competences at security sector experts and Ukraine defense", *Information Technology and Security*, vol. 6, no. 2, pp. 105-123, 2018, doi: https://doi.org/10.20535/2411-1031.2018.6.2.153495.

[16] Ю. Щавінський, О. Левчук, В. Левчук, та О. Сирський, "Організаційно-технічні і правові аспекти формування компетентностей військових фахівців", *Військ. освіта*, № 2 (46), с. 311-324, 2022, doi: https://doi.org/10.33099/2617-1783/2022-46/311-324.

[17] T. Holth, and O. Boe, “Lost in transition: The dissemination of digitization and the challenges of leading in the military educational organization”, *Frontiers Psychol.*, vol. 10, 2019, doi: https://doi.org/10.3389/fpsyg.2019.02049.

Стаття надійшла до редакції 18.05.2023.

REFERENCE

[1] Z. F. Samchuk, *Ideological foundations of socio-philosophical research of ideology: The problem of criteria and priorities of choice, v. 1*. Dnipropetrovsk, Ukraine: ART-PRESS, 2009.

[2] *Strategy, National Cybersecurity Strategy*. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf. Accessed on: Mar. 01, 2023.

[3] B. J. Blažič, “Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?”, *Educ. Inf. Technol.*, 2021, doi: https://doi.org/10.1007/s10639-021-10704-y. Accessed on: May 03, 2023.

[4] Higher Education in Europe: Understanding the Cybersecurity Skills Gap in the EU, 2021. [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/higher-education-in-europe-understanding-the-cybersecurity-skills-gap-in-the-eu. Accessed on: Feb. 12, 2023.

[5] D. Leaser, Future of Work / The demand for cybersecurity professionals is outstripping the supply of skilled workers. [Online]. Available: https://www.ibm.com/blogs/ibm-training/new-cybersecurity-threat-not-enough-talent-to-fill-open-security-jobs. Accessed on: Apr 22, 2023.

[6] Cyber security expert / master's program. [Online]. Available: https://www.simplilearn.com/cyber-security-expert-master-program-training-course. Accessed on: May 06, 2023.

[7] Verkhovna Rada of Ukraine. 7th Session. (2017, Oct. 5). *Law of Ukraine No. 2163-VIII, On Basic Principles of Cybersecurity of Ukraine*. [Online]. Available: https://zakon.rada.gov.ua/laws/show/2163-19#Text. Accessed on: Dec. 18, 2022.

[8] *Cyber Digest. Cybersecurity Events Review, Dec. 2022*. Kyiv, Ukraine: National Cybersecurity Coordination Center. [Online]. Available: https://www.rnbo.gov.ua/files/НКЦК/НКЦК-1/Cyber%20digest_December_2022.pdf. Accessed on: Jan. 18, 2023.

[9] D. Dubov, *U.S. National Cybersecurity Strategy 2023: Critical Infrastructure, Coordination, Proactivity. Policy Brief*. Kyiv, Ukraine: National Institute for Strategic Studies, 2023.

[10] Verkhovna Rada of Ukraine. 6th Session. (2021, Dec. 17). *Law of Ukraine No. 1986-IX, On Amendments to Certain Laws of Ukraine on Military Education and Science*. [Online]. Available: https://https://zakon.rada.gov.ua/laws/show/1986-20#Text. Accessed on: Apr. 19, 2023.

[11] Ministry of Defense of Ukraine. (2021, Dec. 15). *Policy of the Ministry of Defense of Ukraine in the field of military education.* [Online]. Available: https://www.mil.gov.ua/content/education/politika_mou_osvita.pdf. Accessed on: Apr. 19, 2023.

[12] National Security and Defense Council of Ukraine. (2021, Dec. 30). *Decision of the National Security and Defense Council of Ukraine “On the Implementation Plan of the Cybersecurity Strategy of Ukraine”*. [Online]. Available: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text. Accessed Apr. 23, 2023.

[13] [National Security and Defense Council of Ukraine. (2020, Sep 14). *Decision of the National Security and Defense Council of Ukraine “On the National Security Strategy of Ukraine”*. [Online]. Available: https://zakon.rada.gov.ua/laws/show/n0005525-20#Text. Accessed Apr. 27, 2023.

[14] D. Kuleba, *The War for Reality. How to win in the world of fakes, truths and communities*. Kyiv, Ukraine: Knyholav, 2022.

[15] Y. Danyk, and O. Korneiko, “Fundamentals methodology of formation cyber competences at security sector experts and Ukraine defense”, *Information Technology and Security*, vol. 6, no. 2, pp. 105-123, 2018, doi: https://doi.org/10.20535/2411-1031.2018.6.2.153495.
[16] Y. Shchavinsky, O. Levchuk, V. Levchuk, and O. Syrsky, “Organizational, technical and legal aspects of the formation of competencies of military specialists”, *Military Education*, no. 2 (46), pp. 311-324, 2022, doi: https://doi.org/10.33099/2617-1783/2022-46/311-324.
[17] T. Holth, and O. Boe, “Lost in transition: The dissemination of digitization and the challenges of leading in the military educational organization”, *Frontiers Psychol.*, vol. 10, 2019, doi: https://doi.org/10.3389/fpsyg.2019.02049.

OLEKSANDR PUCHKOV,
OLENA UVARKINA

SUSTAINABLE DEVELOPMENT OF THE SYSTEM OF FORMAL CYBER EDUCATION: REFLECTION OF MODERN CONCEPTS

The article defines the conceptual framework for sustainable development of the formal cyberworld system. An analysis of contemporary regulatory, legal, and scientific sources on the preparation of cyber specialists for the security and defense sector has been conducted. The main research methods identified are synthesis, comparative analysis, focusing method, and cause-and-effect method. The new U.S. Cybersecurity Strategy addressing cyber education issues has been analyzed, which sets new requirements for cyber professionals in the context of the transformation of the global and national security environment. The use of analysis data from EU cybersecurity educational programs revealed the characteristic variability of the cybersecurity educational landscape in the EU and helped identify key gaps in the preparation of future professionals. It has been demonstrated that the integration of Ukrainian cyber education into the Euro-Atlantic educational space should occur through the updating of cybersecurity curricula based on the best international practices, the establishment of a unified system for accreditation, certification, and the development of cyber e-learning platforms for formal education. The competency-based approach in the preparation of cyber specialists is identified as a priority direction in research across various fields of knowledge. It has been revealed that there is a hysteresis of skills within the knowledge-ability-skill triad, acquired during education, in relation to the demands of advanced technologies in professional activities.

Keywords: cybersecurity, formal cybereducation, cyber specialist, sustainable development.

Пучков Олександр Олександрович, кандидат філософських наук, професор, начальник, Інститут спеціального зв’язку та захисту інформації Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського”, Київ, Україна, ORCID 0000-0002-8585-1044, iszzi@iszzi.kpi.ua.

Уваркіна Олена Василівна, доктор філософських наук, професор, завідувач Спеціальної кафедри № 4, Інститут спеціального зв’язку та захисту інформації Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського”, Київ, Україна, ORCID 0000-0001-9053-2016, uvarkinaev@ukr.net.

Puchkov Oleksandr, candidate of philosophy science, professor, head of Institute of special communications and information protection, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, Ukraine.

Uvarkina Olena, doctor of philosophy science, professor, head of special department № 4, Institute of special communication and information protection National technical university of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, Ukraine.