Вісник Львівського університету. Серія філос.-політолог. студії. 2024. Випуск 52, с. 11–17
Visnyk of the Lviv University. Series Philos.-Political Studies. Issue 52, p. 11–17

ФІЛОСОФСЬКІ НАУКИ

УДК 316.4:378.016
DOI https://doi.org/10.30970/PPS.2024.52.1

ТРАНСФОРМАЦІЯ, ТРАНСГРЕСІЯ ЧИ ІНТЕНЦІЯ? (СОЦІАЛЬНО-ФІЛОСОФСЬКА РЕФЛЕКСІЯ КІБЕРОСВІТИ)

Валерій Ананьїн
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»,
Інститут спеціального зв'язку та захисту інформації
вул. Верхньоключова, 4, 03056, м. Київ, Україна

Олена Уваркіна
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»,
Інститут спеціального зв'язку та захисту інформації
вул. Верхньоключова, 4, 03056, м. Київ, Україна

Стаття присвячена дослідженню сучасних проблем кіберосвіти в умовах нових викликів та загроз українському суспільству. Визначено, що проблемний горизонт трансформації кіберосвіти в Україні надзвичайно широкий у своєму євроатлантичному інтегральному спрямуванні і потребує системної соціально-філософської рефлексії основних напрямів реконструкції традиційної матриці підготовки кіберфахівців. Стверджується, що трансформаційні траєкторії якісного покращення вітчизняної кіберосвіти мають багаторівневий комплекс системних перетворень, які пов'язані зі змінами когнітивно-аксіологічних пріоритетів суспільного і особистісного розвитку та імплементаційних ознак щодо впровадження кращих світових професійних стандартів підготовки кіберфахівців нового покоління. Проаналізовані етапи розробки та впровадження Національної рамки кваліфікації у сфері кібербезпеки. Зясовано, формування Національної рамки кваліфікацій у сфері кібербезпеки розширює класифікатор професій у сфері кібербезпеки та створює підвалини для сертифікації кіберфахівців у кваліфікаційних центрах та імплементації професійних стандартів до освітніх програм підготовки студентів у закладах вищої освіти. Зазначено, що дослідження трансформації кіберосвіти в епоху світової цифровізації знаходить відображення у всіх стратегіях кібербезпеки провідних держав світу, що поширює міжнародне співробітництво для створення нових сучасних протидійєвих механізмів та технологій запобігання кіберінцидентів на основі обміну досвідом між кіберфахівцями країн-партнерів. Доведено, що трансгресивні кроки трансформації кіберосвіти позитивно відображаються на підвищенні якості підготовки українських фахівців з кібербезпеки та забезпечують високий рівень якості кадрового потенціалу. З'ясовано, що амплітуда коливань трансформаційних процесів у кіберосвіти ранжується від трансгресії до інтенції сучасних кіберінновацій. Рефлексія інтенційних можливостей трансформації кіберосвіти виявила націотворчий потенціал системи підготовки фахівців з кібербезпеки.

Ключові слова: кіберфахівець, професійні стандарти, стратегії кібербезпеки, міжнародне партнерство.

Стратегічна важливість кіберосвіти в епоху світової цифровізації настільки очевидна, що до освітнього простору цієї галузі зусібіч долучаються і держава, і бізнес, і військові. Постановка питання про підвищення рівня компетентнісної парадигми кіберосвіти

знаходить відображення у стратегіях кібербезпеки провідних держав світу, які визнають сучасний кіберпростір «сферою операцій» [1] та в умовах постійного зростання кількості кіберзагроз (хакерські атаки, віруси, фішингові атаки тощо) актуалізують підготовку фахівців з кібербезпеки як одне з пріоритетних завдань освітньої державної політики.

Рефлектуючи з приводу цього аспекту, аналіз сучасних зарубіжних та вітчизняних джерел, показав, що амплітуда концептуальних точок зору на проблемний горизонт трансформації кіберосвіти в Україні надзвичайно широкий у своєму євроатлантичному інтегральному спрямуванні і потребує системної соціально-філософської рефлексії основних напрямів реконструкції системи підготовки кіберфахівців.

Трансформаційні траєкторії якісного покращення вітчизняної кіберосвіти мають багаторівневий комплекс системних перетворень. Зоднобіч, феномен «трансформація системи освіти» сприймають у зв'язку зі змінами когнітивно-аксіологічних пріоритетів суспільного і особистісного розвитку, які мають виключні соціально-формуючі та людинотворчі можливості. Здругобіч, під впливом всесвітніх тенденцій до глобальних змін, трансформація української кіберосвіти протягом останніх років активно набуває очевидних імплементаційних ознак щодо впровадження професійних стандартів підготовки кіберфахівців нового покоління.

Разом з цим доводиться визнати, що зусібіч в національних суспільствах, що перебувають через певні історичні обставини на трансформаційному рівні розвитку, освітні системи відіграють роль основного творця ключових соціально-світоглядних, ціннісних орієнтацій, за якими в подальшому буде таке суспільство розвиватися. Тому усвідомлення принципу первинності освіти щодо інших соціальних процесів і перетворень надзвичайно актуалізує питання про її магістральний вибір спрямування до єдиного європейського освітнього простору. Але принцип європейської спрямованості трансформаційних процесів розвитку освіти України вимагає значних внутрішніх змістовно-структурних трансформацій на всіх рівнях, конкретизації цілей і механізмів їх реалізації, системного аналізу та філософської рефлексії націотворчих процесів у кіберпростору [2, с. 251].

Сьогодні, як ніколи, у суспільстві відчутна зацікавленість абсолютно всіх суб'єктів національного освітнього процесу в досягненні європейських стандартів та цінностей навчально-педагогічного та виховного процесу. Однак в умовах російської агресії проти України, на нашу думку, треба приділити особливу увагу трансформації вітчизняної системи кіберосвіти, яка стає невід'ємною частиною життя кожної людини, кожного фахівця, кожного підприємства, і яка забезпечує всебічний захист та безпеку держав світу у цифровому просторі.

Одними з перших трансформацію української кіберосвіти, щодо впровадження професійних стандартів провідних систем світу, почали співробітники Державної служби спеціального зв'язку та захисту інформації (далі – Держспецзв'язку). На підсумковому у 2022 році засіданні Національного кластера кібербезпеки «Війна в кіберпростору 2022: підсумки, здобутки та прогалини», який є координаційною платформою для об'єднання ресурсів, можливостей, компетенцій РНБО України та Фонду Цивільних досліджень на розвитку США (CRDF GLOBAL), урядових та міжнародних організацій, було зазначено, що перші шість професійних стандартів (розробник систем захисту інформації, адміністратор мереж і систем, фахівець сфери захисту інформації, аналітик з безпеки інформаційно-телекомунікаційних систем, фахівець з питань безпеки (інформаційно-комунікаційні технології), інструктор-методист з інформаційної безпеки та кібербезпеки) були розроблені за підтримки Проєкту USAID Cybersecurity Activity «Кібербезпека критично важливої інфраструктури України», пройшли етапи публічного обговорення та дістали позитивні

висновки експертизи Національного агентства кваліфікацій. Затверджені Держспецзв'язку стандарти стали підвалинами для запровадження нових спеціалізацій та оновлення освітніх програм вищої освіти за напрямками підготовки фахівців з кібербезпеки [3, с. 37; 4].

Виступаючи на Київському міжнародному форумі з кібербезпеки, заступник голови Держспецзв'язку, бригадний генерал Олександр Потій зазначив, що «до 2021 року, в Україні були лише дві професії в галузі кібербезпеки і цього було критично мало для того, щоб відповідати сучасним реаліям інформаційного протиборства у кіберпросторі», тому «розвиток системи підготовки фахівців та професійної сертифікації кадрів в галузі безпеки інформації та кіберзахисту – актуальне завдання для посилення кіберстійкості України» [5] в умовах повномасштабного вторгнення рф та світових тенденцій цифровізації всього суспільства.

До очевидних переваг і здобутків Держспецзв'язку у питанні розробки та впровадження Національної рамки кваліфікації у сфері кібербезпеки слід віднести і створення системи професійних стандартів, яка проводиться у п'ять етапів:

– перший етап (2022–2023 рр.) – до класифікатора професій ДК – 003: 2010 внесені 27 нових професій у сфері кібербезпеки;

– другий етап (січень 2024 р.) – підготовка 21 професійного стандарту у сфері кібербезпеки;

– третій етап – створення кваліфікаційних центрів, які підтверджуватимуть фаховий рівень у відповідності професійній кваліфікації;

– четвертий етап – імплементація професійних стандартів до освітніх програм підготовки студентів у закладах вищої освіти;

– п'ятий етап – формування Національної рамки кваліфікацій у сфері кібербезпеки, а саме: розробка та імплементація в суспільство, безпосередньо самої рамки кваліфікацій з урахуванням сформованих професійних категорій (класифікації організаційної структури, що мають загальні основні професійні функції у сфері кібербезпеки), професійних площин та відповідних їм кваліфікацій, компетентностей тощо [5].

З огляду на зазначену обставину, слід зазначити, що формування власної Національної рамки кваліфікації України у сфері кібербезпеки відбувається на основі використання світового передового досвіду національної рамки кваліфікації у кібербезпеки США (Cybersecurity Workforce Framework / NICE NIST 800–801) та Європейської рамки навичок з кібербезпеки (European Cybersecurity Skills Framework / ECSF ENISA), які мають забезпечити процес якісної трансформації української кіберосвіті для подолання відчутного дефіциту кваліфікованих кадрів у сфері кібербезпеки та формування «армії кіберфахівців» для протидії ворожим атакам у кіберпросторі.

Відомо, що під час трансформаційних процесів відбувається базисний розрив між соціально-економічними змінами та запізнілим створенням соціальних інститутів, встановленням формальних і неформальних обмежень, що спрямовують процеси активізації в певному напрямку. Тому до трансформації вітчизняної кіберосвіти мають бути залучені всі ланки виконавчої влади та весь націотворчий потенціал українського суспільства.

Бурхливий розвиток глобалізаційних процесів зафіксував не тільки активність світових трансформацій у кіберпростору, але і виявив трансгресивні тенденції, які набуваючи спеціальних ознак і значущості для сьогодення унеможливлюють спроби агресора у майбутньому похитнути незалежність української держави.

Рефлектуючи до появи перших трансгресивних кроків у трансформації кіберосвіти, варто зазначити про рішення щодо стратегічного курсу України на набуття повноправного членства в Європейському Союзі та НАТО, яке було закріплено в преамбулі, трьох статтях

та перехідних положеннях Основного Закону і підтвердило «європейську ідентичність Українського народу і незворотність європейського та євроатлантичного курсу України» [6; 7, с. 52].

Такий трансгресивний прорив українського суспільства, як феномен переходу межі між можливим і неможливим, безсумнівно вплинув на вітчизняне кіберосвітнє середовище, яке отримало можливість трансгресивного переходу до нового рівня подальшого розвитку галузі, пошуку сучасних форм, методів, стандартів, враховуючи кращі досягнення освітніх систем країн-партерів НАТО [7, с. 52].

Слід зазначити, що під впливом євроатлантичної інтеграції динамічні освітні трансгресії відбулися і у діючому вітчизняному нормативно-правовому полі. Завперш, це стосується змін до деяких законів України щодо військової освіти та науки, які чітко встановлюють особливі вимоги як щодо управління відповідними вищими військовими навчальними закладами, закладами вищої освіти із специфічними умовами навчання та військовими навчальними підрозділами закладів вищої освіти, так і науковими установами, в яких організована наукова та науково-технічна діяльність у військової галузі [8].

Зміни у діючих нормативно-правових актах евентуально підготували систему національної кіберосвіти до випробувань у воєнному стані, а трансформаційні процеси продовжуються відповідно стратегічного курсу держави та затверджених імплементаційних етапів у практику підготовки кіберфахівців.

Сутнісним моментом трансгресивного переходу вітчизняної кіберосвіти є активне залучення українських кіберфахівців до міжнародних програм навчання у Європі та США. Наприклад, тільки протягом 2022–2023 року співробітники Держспецзв'язку та інших державних установ України, як мінімум, двічі були запрошені на курси з кібербезпеки, які були організовані Cybersecurity and Infrastructure Security Agency, CISA (Агенство з кібербезпеки і захисту інфраструктури), розташованого на базі Айдахо Нашнл Лабораторії в Айдахо фоллс, США. Під час навчання відбувалось відпрацювання як теоретичних, так і практичних аспектів, що дозволяло учасникам навчань підвищити рівень адаптованості в кризових та нестандартних ситуаціях.

Відповідне «вікно можливостей» для українських фахівців з кібербезпеки відкрила і Європа. Останнім часом магістри, які навчаються за спеціальністю «кібербезпека та захист інформації» систематично отримають можливість за різними програмами пройти кіберкурси у прибалтійських країнах та отримати відповідні кваліфікаційні сертифікати.

Між іншим, завдяки перемозі в Першому національному хакатоні з кіберзахисту в Україні, група кіберфахівців (магістри, здобувачі ступеню доктора філософії та просто молоді спеціалісти) разом з 63 представниками з 18 країн Європи та світу за підтримки некомерційної організації Haague Security Delta (HSD), Лейденського університету, Нідерландському банку, Європолу, Агентству з питань обслуговування систем інформації та зв'язку НАТО, а також спонсорам з приватного сектору Accenture, deloitte, Booz Allen Hamilton, EclecticIQ отримала запрошення до Міжнародної літньої школі з кібербезпеки (International Cyber Security Summer School), яка проходила в місті Гаага, Королівство Нідерланди в кінці серпня 2022 року. Особливістю цього навчання став організований в межах курсу захід типу Capture the flag, де команда слухачів курсу змагалась проти фахівців із Connected2trust та у результаті якого, українська команда показала достатньо високий фаховий рівень безпекових навичок у професійної боротьбі з колегами-фахівцями.

У 2023 році трансгресивний горизонт можливостей для української кіберосвіти розширився завдяки навчанню, організованому в рамках Меморандуму про взаєморозуміння у сфері кіберзахисту між Держспецзв'язку та Іспанським національним інститутом

кібербезпеки (INCIBE) з тематики «Infrastructure Control Systems». Основними підходами до навчання на цих курсах стала командна робота з елементами змагань, хакатони, Capture The Flag (CTF), Red Team – Blue Team training, а також відпрацювання сценаріїв на інтерактивних кіберплатформах.

Однак, розуміючи позитивні сторони трансгресивних спрямувань трансформації сучасної кіберосвіти, слід зазначити що відповідне ранжування відбувається завдяки інтенційним основам трансформації.

Конотація інтенції кіберосвіти, її план дій, її стратегія передбачається в національних стратегіях кібербезпеки провідних країн світу. Наприклад, Національною стратегією кібербезпеки Королівства Іспанії та Національною стратегією Королівства Нідерланди визначаються основні напрямки розвитку кіберосвіти у таких напрямках: навчальні програми та курси; центри експертизи і навчання; співпраця з університетами та приватним сектором; підтримка наукових досліджень; свідомість громадськості [9; 10].

Інтенція довгострокової політики ключового українського міжнародного партнерства у гармонізації безпекових підходів була започаткована у Національної стратегії кібербезпеки США, яку 1 березня 2023 року оприлюднила адміністрація Президента США. Серед пріоритетів зазначається національна стратегія комплексного та скоординованого підходу державної політики у напрямку розширення доступу до кіберосвіти. 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 [3, с. 36; 11].

Зрештою, інтенційно 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 і дослідницьким досвідом та академічними прагненнями, але і через оновлення навчального плану освітніх програм з кібербезпеки з чітким розумінням різноманітних проблем у цій галузі, а саме: 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 [12, с. 62; 13].

Отже, соціально-філософська рефлексія процесів трансформації кіберосвіти показала поліаспектність підготовки сучасних кіберфахівців, що аргументаційно актуалізує проблемний горизонт цього дослідження. Сучасний праксис реалізації інтенційного євроатлантичного інтегрального спрямування кіберосвіти був забезпечений в умовах радикальної зміни безпекової ситуації оновленими українськими та міжнародними нормативно-правовими документами через розроблення професійних стандартів для нових професій з кібербезпеки на основі найкращого міжнародного досвіду, подолання гістерезису компетентностей та створення єдиної системи акредитації та сертифікації. Система кіберосвіти отримала динамічні можливості трансгресивного переходу до стандартів НАТО та оновлення курикулуму за кращими зразками світового освітнього простору. Проведене дослідження показало, що українська кіберосвіта має величезні перспективи успішно завершити трансформацію, покращити кадровий потенціал кіберфахівців та стати повноцінним міжнародним партнером у гармонізації безпекових підходів у світовому кіберпростору з урахуванням появи нових кіберзагроз і викликів.

Список використаної літератури

1. CCDCOE – The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise. [Electronic resource]. https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/
2. Уваркіна О.В. Освітній потенціал нації: монографія. Київ: Вид-во НПУ імені М. П. Драгоманова, 2011. 383 с.
3. Ананьїн В.О.,Уваркіна О.В. Політичні візії кіберосвіти. *Вісник Національного технічного університету України «Київський політехнічний інститут». Політологія. Соціологія. Право* : зб. наук. праць. Київ, 2023. Випуск 1(57). С. 35–39. DOI https://doi.org/10.20535/2308-5053.2023.1(57).280780
4. Cyber Digest. Огляд подій в сфері кібербезпеки. Київ, грудень 2022. URL: https://www.rnbo.gov.ua/files/%D0%9D%D0%9A%D0%A6%D0%9A/%D0%9D%D0%9A%D0%A6%D0%9A-1/Cyber%20 digest_December_2022.pdf
5. Ставка на освіту: Україна посилює стійкість у кіберпростору через професійну підготовку. https://cip.gov.ua/ua/news/stavka-na-osvitu-ukrayina-posilyuye-stiikist-u-kiberprostori-cherez-profesiinu-pidgotovku)
6. Конституція України [Електронний ресурс]: Закон України від 28.06.1996 № 254к/96-ВР // Верховна Рада України. URL: http://zakon2.rada.gov.uaЛaws/show/254к/96-вр
7. Пучков О.О., Уваркіна О.В. Сучасна військова освіта: трансгресивний прорив в умовах трансформації. *Актуальні проблеми філософії та соціології.* 2022. Вип. 39. С. 51–55. DOI https://doi.org/10.32782/apfs.v039.2022.9
8. Закон України «Про внесення змін до деяких законів України щодо військової освіти та науки». 17 грудня 2021 року № 1986-IX. URL: https://zakon.rada.gov.ua/laws/show/1986-20#Text
9. Estrategia Nacional de Ciberseguridad 2019. DSN [Electronic resource] // DSN: Sitio oficial del Departamento de Seguridad Nacional. https://www.dsn.gob.es/en/documento/estrategia-nacional-ciberseguridad-2019
10. The Netherlands Cybersecurity Strategy 2022–2028 [Electronic resource] // National Coordinator for Security and Counterterrorism. https://english.nctv.nl/topics/netherlands-cybersecurity-strategy-2022-2028/documents/publications/2022/12/06/the-netherlands-cybersecurity-strategy-2022-2028
11. The White House: National Cybersecurity Strategy. Washington. March 1, 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
12. Пучков О.О., Уваркіна О.В. Сталий розвиток системи формальної кіберосвіти: рефлексія сучасних концептів. *Information Technology and Security*. 2023. Vol. 11 Iss. 1 (20). P. 60–68. DOI: https://doi.org/10.20535/2411-1031.2023.11.1.283635
13. Higher Education in Europe: Understanding the Cybersecurity Skills Gap in the EU, 2021. https://www.enisa.europa.eu/news/enisa-news/higher-education-in-europe-understanding-the-cybersecurity-skills-gap-in-the-eu

TRANSFORMATION, TRANSGRESSION OR INTENT? (SOCIAL-PHILOSOPHICAL REFLECTION OF CYBER EDUCATION)

Valerii Ananin
National Technical Unversity of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute",
Institute of Specialized Communication and Information Security
Verkhneklyuchova str., 4, 03056, Kyiv, Ukraine

Olena Uvarkina
National Technical Unversity of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute",
Institute of Specialized Communication and Information Security
Verkhneklyuchova str., 4, 03056, Kyiv, Ukraine

The article is devoted to the study of modern problems of cyber education in the context of new challenges and threats to Ukrainian society. It is determined that the problematic horizon of the transformation of cyber education in Ukraine is extremely broad in its Euro-Atlantic integral direction and requires a systematic socio-philosophical reflection on the main directions of reconstruction of the traditional matrix of cyber specialists training. It is argued that the transformational trajectories of qualitative improvement of domestic cyber education have a multilevel complex of systemic transformations associated with changes in the cognitive and axiological priorities of social and personal development and implementation features for the introduction of the best world professional standards for the training of new generation cyber specialists. The stages of development and implementation of the National Cybersecurity Qualifications Framework are analyzed. It is clarified that the formation of the National Cybersecurity Qualifications Framework expands the classifier of professions in the field of cybersecurity and creates the basis for the certification of cyber specialists in qualification centers and the implementation of professional standards in educational programs for students in higher education institutions. It is noted that the study of the transformation of cyber education in the era of global digitalization is reflected in all cybersecurity strategies of the world's leading countries, which promotes international cooperation to create new modern countermeasures and technologies to prevent cyber incidents based on the exchange of experience between cyber professionals.

It has been proven that the transgressive steps in the transformation of cyber education are positively reflected in the improvement of the quality of training of Ukrainian cyber security specialists and ensure a high level of quality of personnel potential. It was found that the amplitude of fluctuations of transformational processes in cyber education ranges from transgression to the intention of modern cyber innovations. Reflection on the intentional possibilities of transformation of cyber education revealed the nation-building potential of the system of training cyber security specialists.

Key words: cyber specialist, professional standards, cyber security strategies, international partnership.