DOI https://doi.org/10.30525/978-9934-26-405-4-25

НЕФОРМАЛЬНА КІБЕРОСВІТА: СУЧАСНЕ «ВІКНО МОЖЛИВОСТЕЙ»

Уваркіна О. О., Шевчук О. С., Горнійчук І. В.

ВСТУП

Сучасний світ концептуально визнав, що наріжним каменем освіти є «навчання впродовж життя», яке через формальні, неформальні, інформальні види освіти стане основною передумовою сталого розвитку суспільства майбутнього.

Експоненціальна світова цифровізація кардинально змінює вимоги до сучасної освіти, яка має встигати за соціально-економічним розвитком суспільства та готувати висококваліфікованих фахівців для нових швидкоплинних світових змін у науці і техніці. Звичайно, що під час формальної освіти, закладаються основні фахові підвалини, але необхідність у постійному фаховому зростанні та освоєнні нових технологій надає неформальної освіти більше «вікно можливостей» для становлення власної конкурентоспроможності на ринку праці.

Сучасний глобальний освітній простір надзвичайно актуалізує неформальну освіту через упровадження єдиних кваліфікаційних рівнів та стандартів. Non-formal education стає мотиваційним щабелем якості освіти у світі та активно розвиває нові підходи, отримання компетентностей, завперш, для праксису.

У концептуальному каркасі неформальної української освіти теж спостерігаємо своєрідну активізацію зацікавленості до проблем розвитку системи неформальної освіти. Наприклад, у Законі України «Про освіту» чітко визначено, що «неформальна освіта – це освіта, яка здобувається, як правило, за освітніми програмами та не передбачає присудження визнаних державою освітніх кваліфікацій за рівнями освіти, але може завершуватися присвоєнням професійних та/або присудженням часткових освітніх кваліфікацій»[1].

Наявність величезної кількості різних форм неформальної освіти від очної (курси, тренінги, майстер-класи, семінари, майстерні тощо) до дистанційної (дистанційні курси, вебінари тощо), які організуються неурядовим установами, закладами освіти, приватними особами та платформами дистанційного навчання, надає цієї системі можливості

[1] Закон України «Про освіту». 5 вересня 2017 року № 2145-VIII. URL: https://zakon.rada.gov.ua/laws/show/2145-19

бути більш резильєнтною до вимог сучасності та швидко кумулятувати в умовах конкуретності.

Слід зазначити, що становлення української неформальної освіти відбувається в умовах євроінтеграції та входження у світовий освітній простір і супроводжується повноцінним науковим дискурсом щодо втрати монополії формальної освіти, яка «не може забезпечити гарантовану якість освітніх ресурсів» та актуалізує питання вирішення проблем неформальної освіти «з позиції змісту поняттям, як методології, так практики її організації»[2]. Мабуть тому в останньому десятиріччі більшість праць українських вчених (Барабаш О., Гончарук А., Горук Н., Давидова В., Махиня Н., Огієнко О., Павлик Н., Стрижаковська В., Шапочкіна О.) була присвячена компаративному аналізу найкращого досвіду неформальної освіти у світі та пошуку екзистенційної стратегеми її розвитку.

У цьому контексті спроба «осмислення базових принципів, етичних дилем, ціннісних орієнтацій та практичних підходів»[3] неформальної освіти когерентне доводить необхідність конотації сучасного практичного досвіду молодих українських вчених у системі неформальної кіберосвіти США та Європи. Зрештою, рефлексивна наукова ініціативність визначення основних ланок зарубіжного досвіду організації неформальної кіберосвіти, її інтенцій та праксису, об'єктивно актуалізується протистоянням всього демократичного світу агресії рф та ролі кіберфахівців у досягнення переваг у п'ятивимірній війні сучасності.

1. Неформальна кіберосвіта в США: сучасний досвід навчання

Українські фахівці з компаративної педагогіки зазначають, що у США існують «два напрямки організації неформального навчання: просвітницький (поширення знань, інформації, компетенцій) і реформістський (зміна соціальних явищ та поліпшення життєвого рівня населення)», які використовують різні форми організації освітньої діяльності. Серед найпоширеніших є навчальні програми і курси, тренінги, літні сесії, освітні семінари, засідання клубів, освітні конференції, кейс-метод, рольові ігри і симуляції, письмові рефлексії та презентації. Дослідники освітньої системи США зазначають, що

[2] Лук'янова Л., Ващенко Л. Неформальна освіта різних категорій дорослого населення: теоретичні аспекти, методичні засади. Освіта для миру: зб. наук. пр. Київ-Переяслав-Хмельницький : Юрка Любченка, Т. 2. 2019. С. 401. https://lib.iitta.gov.ua/734295/1/volume_2_2019-400-417.pdf

[3] Лазоренко О. Філософія освіти дорослих в контексті практичної парадигми пожиттєвого навчання: європейський приклад для України. Філософія освіти. 1-2(10). 2011. С. 255.

держава утримується від втручання у сферу освіти, між формальною і неформальною видами освіти відсутні кордони, а також свідчать про «високий рівень індивідуалізації навчання, врахування потреб та інтересів тих, хто навчається, використання інтерактивних педагогічних методів»[4].

Між іншим, компаративісти-дослідники вважають, що термін «неформальна освіта» був введений у науковий обіг у 1967 році під час Міжнародної конференції у Вільямсбурзі (США). На конференції «було порушено питання щодо світової освітньої кризи через проблеми із швидким застаріванням навчальних програм та низьку здатність формальної освіти адаптуватися до глобальних змін». Тому «на зміну застарілій концепції «освіта на все життя» прийшла інша – «навчання впродовж життя» (lifelong education)»[5]. Цей концепт відомий сьогодні у всьому світі як глобальний підхід до освіти, що дозволяє своєчасно і повно відповідати викликам цифрового суспільства та вимогам сучасності.

Слід врахувати, що підвищення питомої ваги неформальної кіберосвіти в США виявилося результатом збільшення попиту на експертів з безпеки з практичним досвідом реагування на інциденти безпеки. З метою покращення довгострокової позиції у сфері кібербезпеки та створення чіткої стратегії розвитку кадрового потенціалу було створено NICE Flamework (Національна ініціатива з кібербезпекової освіти), яка займається інформуванням, 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».[6]

Нездатність вирішити цю проблему негативно впливає на спроможність сучасного цифрового суспільства у реалізації новітніх розробок. Важливість знань з кібербезпеки зараз широко визнана, але

---

[4] Павлик Н.П. Зарубіжний досвід організації неформальної освіти. *Наукові записки Ніжинського державного університету ім. Миколи Гоголя. Психолого-педагогічні науки*. 2016. № 1. С.268. URL: http://nbuv.gov.ua/UJRN/Nzspp_2016_1_50

[5] Лук'янова Л., Ващенко Л. Неформальна освіта різних категорій дорослого населення: теоретичні аспекти, методичні засади. Освіта для миру: зб. наук. пр. Київ-Переяслав-Хмельницький : Юрка Любченка, Т. 2. 2019. С. 402. https://lib.iitta.gov.ua/734295/1/volume_2_2019-400-417.pdf

[6] Blažič B. J. Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?", *Educ. Inf. Technol.*, 2022. DOI::https://doi.org/10.1007/s10639-021-10704-y.

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. Це свідчить про відставання у підготовці висококваліфікованих кіберфахівців в умовах різкого зростання кіберзлочинності. За прогнозами Cybersecurity Ventures на світовому ринку праці вже 3,5 мільйона незаповнених посад у сфері кібербезпеки і занепокоєння цим фактом виходить далеко за межі звичайної освіти з ІКТ та розвитку навичок[7].

Відомо, що головною подією кіберпростору США у 2023 році стало оприлюднення адміністрацією Президента США Національної стратегії кібербезпеки, у якої започаткована нова довгострокова політика ключового українського міжнародного партнерства у гармонізації безпекових підходів. Російська агресія проти України змінила низку тенденцій в кібербезпековій політиці США та визначила нові пріоритети як глобального, так і національного безпекового середовища. У фокусі уваги Національної стратегії кібербезпеки 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[8].

[7]. Там же

[8] Уваркіна О., Пучков О. Сталий розвиток системи формальної кіберосвіти: рефлексія сучасних концептів. *Information Technology and Security*. 2023. Vol. 11 Iss.1 (20). P. 61. DOI: https://doi.org/10.20535/2411-1031.2023.11.1.283635

Згідно аналітичної записки Національного Інституту стратегічних досліджень «Національна стратегія кібербезпеки США 2023: критична інфраструктура, координація, проактивність», українська кібербезпекова політика вже бере до уваги ідеї, використані в новій Стратегії США. Зазначається , що «як і більшість країн світу, Україна потребує більше фахівців з кібербезпеки – протягом цього та попереднього років вже було створено шість нових професійних стандартів кібербезпеки, гармонізованих з положеннями NICE Framework, а відтак, впроваджуються найкращі міжнародні практики в освітній процес»[9].

Затверджені у Національної стратегії кібербезпеки США підвалини міжнародного партнерства для обміну інформацією, ресурсами та кращими практиками у галузі кібербезпеки відкрили для українських фахівців «вікно можливостей» для отримання практичного досвіду через неформальну систему освіти.

Як приклад, можна навести навчання українських кіберфахівців (серед яких був один зі співавторів цієї статті, який вже двічі був запрошений протягом року на два різних курса з кібербезпеки), організованого Cybersecurity and Infrastructure Security Agency, *CISA* (Агенство з кібербезпеки і захисту інфраструктури), розташованого на базі Айдахо Нашнл Лабораторії в Айдахо фоллс, США.

У 2023 році на 2-х тижневе неформальне навчання були запрошені українські фахівці з кібербезпеки, які працюють у державних установах. Цей курс був присвячений полюванню на вразливості, вивчення яких передбачають більше практичного і цілеспрямованого характеру освітньої діяльності. Для отримання максимального кумулятивного ефекту, на початку навчання відбувалось обов'язкове знайомство, де обидві сторони представляли учасників (викладачі і так звані студенти). Після чого учасники були розділені на попередньо сформовані команди, таким чином, щоб були між собою не знайомі, по можливості не працювали в одній організації, підрозділі, відділі. Після цього команди всередині були поділені на підгрупи за тим самим принципом. Подальші завдання зазвичай виконувались у складі команди, або підгруп.

Саме навчання складалось з декількох етапів:

1. Лекційні заняття. Фахівці з тієї чи іншої галузі, пов'язаної з темою навчань розповідали матеріали по мережевим аналізаторам, атакам, вразливостям, загрозам, власному досвіді в рамках їх роботи. Під час

[9] Дубов Д. Національна стратегія кібербезпеки США 2023: критичні інфраструктура, координація, проактивність. Аналітична записка / Національний інституту стратегічних досліджень. Київ, 2023. [Рукопис на 4 арк.].

лекцій іноді вони надавали завдання на закріплення матеріалу, яке виконувалось в складі команд.

2. Практична демонстрація. Фахівці, які представляли власно розроблені програмні продукти презентували на практиці їх роботу. Пояснювали принцип роботи з ними та ключові аспекти.

3. Відпрацювання практичних навичок. Для закріплення матеріалу було надано доступ до CTF платформи (платформа по захопленню прапора, пошуку вірної відповіді на поставлене завдання). Доступ кожен отримував індивідуальний та відпрацьовував безпосередньо під власним ім'ям.

4. Короткі лекційно-практичні заняття для кожної команди. В даному виді навчання відбувалось безпосереднє навчання на обладнанні. Підключення обладнання, встановлення програмного забезпечення та його конфігурація.

5. Елемент змагання між командами. Розслідування кіберінциденту. В складі команди на певний час відбувались так звані змагання про розслідуванню інцидентів. Пошук доказів злочину, використання власних навичок та вмінь кібербезпеки та захисту інформації з пошуку додаткових відомостей та завдання на логіку.

6. Останнім етапом були триденні змагання у складі команд у так званому челенджу «Red Team – Blue Team».

Була представлена червона команда так званих «хакерів», які були спеціально запрошені на навчання, з метою атакувати системи, які синя команда мала захищати. Зрештою, все зводилось до пошуку індикаторів компрометації в реальному часі, пошуку зачіпок, виявлення хронології атаки з елементами форензіки. З практичної точки зору, використовувалось програмне забезпечення, яке було вивчено та встановлено на минулих заняттях. На прикінцевому етапі навчання кожна команда презентувала свої результати і отримала відгук від керівників змагань (білої, жовтої, червоної команд) про правильність виконання завдання та позитивні зрушення.

Тобто, в підсумку можна сказати, що це неформальне навчання відбувалось в змішаному вигляді (рис. 1). З відпрацюванням як теоретичних, так і практичних аспектів, що дозволяє підвищити рівень адаптованості в кризових та нестандартних ситуаціях, оскільки кожен учасник команди має показати свої персональні знання як теоретичні, так і практичні, не покладаючись на свого колегу.

Рис. 1. Модель неформального кібернавчання CISA (приклад 1)

Другий курс, був більш загальний і не суттєво, але все таки відрізнявся від попереднього. Навчання відбувались на базі тієї ж самої Айдахо Нашнл Лабораторії в Айдахо фоллс, США. Однак, курс був проведений для представників державного і приватного сектору не тільки України, а й інших країн світу (Боснії і Герцоговини, Америки, Австрії та Індії).

В перший день учасники також були розділені на команди по 4 учасники. Всі подальші роботи відбувались в складі команд. На початку навчання відбувалось обов'язкове знайомство, де обидві сторони представляли учасників (викладачі і так звані студенти). Після того почалось навчання (рис.2). Так само як і в попередньому навчанні, командам видавались задачі, де кожна мала представити та аргументувати свій варіант рішення. Такі задачі були протягом всіх днів навчання. Всі завдання були інтерактивні, цікаві, більше в ігровій, жвавій формі. Іноді учасники були поділені попарно для виконання менш складних задач (як, наприклад, з пошуку неофіційно підключених клієнтів WF мережі). За кожною групою був закріплений інструктор, який завжди допомагав та відповідав на питання.

Наприкінці навчання було представлене фінальне завдання, яке виконувалось в складі групи і було презентовано учасниками перед викладачами та спеціалістами даної області. Завдання відбувалось у формі гри.

В підсумку можна сказати, що навчання так само відбувалось в змішаному режимі, включаючи теоретичну і практичну складові, що надавало отримати досвід від інших членів команди та проявити себе. Також, під впливом основних положень Національної стратегії

кібербезпеки США, активізація неформальної кіберосвіти, завперш, відбувається у напряму оптимізації реалізації вимог з підвищення практичних навичок в галузі кібербезпеки з використанням інтерактивних платформ. Інтерактивні платформи, такі як віртуальні лабораторії, симулятори тощо, дозволяють практикувати свої навички з кібербезпеки в безпечному середовищі.

Рис. 2. Модель неформального кібернавчання CISA (приклад 2)

Отже , неформальна кіберосвіта в Сполучених Штатах Америки не тільки відображає нові тенденції у навчанні, але і активно реагує на виклики, які ставляться перед сучасними фахівцями кібербезпеки. Зосереджуючись на практичних аспектах, міжнародному та індустріальному партнерствах, система навчання стає більш адаптованою до потреб сьогодення.

2. Досвід неформальної кіберосвіти в Європі (Нідерланди, Іспанія)

Традиційне розуміння неформальної освіти в Європі базується на визначенні, яке було запроваджено фахівцями з Ради Європи та Європейської комісії і змістовно трактує неформальну освіту як «будь-яку організовану поза формальною освітою освітню діяльність, яка доповнює формальну освіту, забезпечуючи освоєння тих умінь і навичок, які необхідні для соціально та економічно активного громадянина країни. При цьому така освітня діяльність має бути структурованою, мати освітню мету, певні часові рамки, інфраструктурну підтримку і повинна відбуватися усвідомлено. Отримані знання, як правило, не сертифікуються, хоча це є можливим»[10].

[10] Савельєв Є.В. Неформальна освіта як інструмент розвитку додаткових можливостей молоді. *Вчені записки Університету «КРОК»* . №1 (61), 2021. С. 231.DOI: 10.31732/2663-2209-2021-61-228-232

Аналіз досліджень вітчизняних педагогів-компаративістів показав, що європейська неформальна освіта характеризуються як складна, нелінійна, відкрита, здатна до самоорганізації соціально-педагогічна система, яка спрямована на задоволення соціальних, професійних та особистісних освітніх потреб. Основними завданнями сучасної неформальної освіти в Європі, на думку дослідників, є: вирівнювання кваліфікації через модернізацію навчання; надання додаткових можливостей особам, що не одержали належного освітнього рівня або кваліфікації; зменшення кількості некваліфікованих осіб; соціальна інтеграція мігрантів; підвищення віку для кар'єрного зростання[11]. Зрозуміло, що пошук нових та відмова від застарілих компетентностей, формування індивідуальної освітньої траєкторії та моделі саморозвитку для удосконалення фахової майстерності стає невід'ємною складовою високопрофесійного спеціаліста при виборі неформальної освіти.

Завдяки затвердженої Стратегії розвитку вищої освіти в Україні на 2022–2032 роки для українських фахівців відкрилось «вікно можливостей» для забезпечення якісної освітньо-наукової діяльності через збільшення кількості проектів наукової співпраці, інтеграції науковців та освітян до світового наукового простору, а також впровадження кращого іноземного освітнього досвіду в Україні[12].

Відповідно поставленим завданням, неформальна освіта реалізується через європейські заходи і програми, які спрямовані на підвищення рівня професійних навичок для оволодіння новими технологіями, зокрема у кіберпросторі. Важливим аспектом є обмін досвідом між суб'єктами кібербезпеки, в тому числі із залученням найкращих практик кібербезпеки та кіберосвіти країн Європи.

Проаналізувавши отриманий досвід кіберосвіти в Королівстві Нідерланди та Королівстві Іспанія, варто також відмітити, що розвиток та покращення освіти в цілому та кіберосвіти зокрема, передбачається в національних стратегіях кібербезпеки цих країн. Наприклад, Національною стратегією кібербезпеки Королівства Іспанії та Національною стратегією Королівства Нідерланди, які визначають основні напрямки розвитку кіберосвіти у таких напрямках: навчальні програми та курси; центри експертизи і навчання; співпраця з

[11] Павлик Н.П. Зарубіжний досвід організації неформальної освіти. *Наукові записки Ніжинського державного університету ім. Миколи Гоголя. Психолого-педагогічні науки*. 2016. № 1. С.267. URL: http://nbuv.gov.ua/UJRN/Nzspp_2016_1_50

[12]Стратегія розвитку вищої освіти в Україні на 2022-2032 роки. URL: https://zakon.rada.gov.ua/laws/show/286-2022-%D1%80#Text

університетами та приватним сектором; підтримка наукових досліджень; свідомість громадськості[13].

Проте, окрім кіберосвіти в межах формальних освітніх установ можна з впевненістю зауважити велику роль європейської неформальної освіти та сучасних методів навчання у формуванні фахівців із кібербезпеки. Дуже часто неформальна освіта переплітається із освітою формальною, що в свою чергу лише підсилює рівень знань та практичних навичок фахівців. Так для успішного отримання магістерського ступеню необхідно пройти практичне стажування та навчальні курси за напрямом освіти. Часто-густо навчальні курси в межах неформальної освіти із кібербезпеки організовуються із залученням державних організацій та приватних компаній, що зацікавлені в отриманні висококваліфікованих фахівців. Спеціалісти із таких організацій залучаються до проведення занять, а вибудований протягом проходження курсів нетворкінг дозволяє з легкістю знаходити місце для подальшого практичного стажування, і навіть подальшого працевлаштування здобувачів освіти.

Для досягнення цілей в європейській неформальній кіберосвіті використовується безліч підходів та методик навчання та викладання. Наприклад, під час проходження навчальних курсів з кібербезпеки для підвищення рівня оволодіння теоретичними знаннями та практичними навичками застосовується елемент змагань. Слухачів розбивають на команди, що змагаються впродовж всього курсу, або ж певного навчального модуля. Самі ж змагання можуть нести різний характер, наприклад, для підсилення практичних навичок організовують змагання в форматі хакатону, «під час якого спеціалісти переважно одного профілю вирішують конкретне завдання або розробляють дієве рішення за обмежений час»[14]. Або в форматі змагань CTF (Capture The Flag), мета яких є захоплення прапора – необхідної інформації або даних в симульованому середовищі[15]. Також можливе відпрацювання сценаріїв на інтерактивних кіберплатформах. Часто-густо завдання формуються організаціями-спонсорами та вендорами кібербезпеки.

---

[13] Estrategia Nacional de Ciberseguridad 2019 | DSN [Electronic resource] // DSN | Sitio oficial del Departamento de Seguridad Nacional. – Mode of access: https://www.dsn.gob.es/en/documento/estrategia-nacional-ciberseguridad-2019; The Netherlands Cybersecurity Strategy 2022-2028 [Electronic resource] // Home | National Coordinator for Security and Counterterrorism. – Mode of access: https://english.nctv.nl/topics/netherlands-cybersecurity-strategy-2022-2028/documents/publications/2022/12/06/the-netherlands-cybersecurity-strategy-2022-2028

[14] Хакатони що завгодно: що таке хакатон і навіщо брати в ньому участь. Happy Monday. URL: https://happymonday.ua/shho-take-hakaton-i-navishho-braty-v-nomu-uchast

[15] USAID CYBERSECURITY ACTIVITY. Змагання CTF – ключ до успішної кар'єри у сфері кібербезпеки. DOU.UA. URL: https://dou.ua/forums/topic/43810/

Власний досвід неформальної освіти в Міжнародній літній школі з кібербезпеки (International Cyber Security Summer School), яка проходила в місті Гаага, Королівство Нідерланди в кінці серпня 2022 року показав, що «вікно можливостей» для отримання нідерландського досвіду кіберосвіти для співавтора цієї статті відкрилось завдяки перемозі в Першому національному хакатоні з кіберзахисту в Україні. Організатором курсів стала некомерційна організація Haague Security Delta (HSD), що є своєрідним кластером безпеки в Європі (наприклад, з 2013 року понад 275 компаній, урядових організацій і інституцій працюють разом, щоб вплинути на захист цифрового суспільства). Партнерами виступали Лейденський університет, Нідерландський банк, Європол, Агентство з питань обслуговування систем інформації та зв'язку НАТО, а також спонсори з приватного сектору Accenture, deloitte, Booz Allen Hamilton, EclecticIQ, та багато інших. Спікери з цих організацій були долучені до проведення занять, а також було чимало занять в офісах цих організацій, наприклад Європол, Агенція НАТО та Accenture.

У навчальному курсі брало участь 63 учасників із 18 країн Європи та світу, більшість з яких здобувачі магістерського ступеню вищої освіти, здобувачі ступеню доктора філософії та просто молоді спеціалісти, що шукали своє місце в сфері кібербезпеки. Значний акцент протягом курсів приділявся саме розвитку нетворкінгу між слухачами курсу та партнерами із подальшим стажуванням та навіть працевлаштуванням.

Протягом курсу була проведена командна робота над проектами у вигляді невеличкого змагання. За методикою курсу усіх слухачів поділили на групи, що протягом всього періоду навчання мали працювати над вирішенням одного із 7 завдань, які були надані партнерами та спонсорами. Зокрема: Leiden University, SecuredNow, Booz Allen Hamilton, DNB, Europol, NATO CIA, Deloitte. Також щодня виділявся час для роботи над проектом, який передбачав вивчення нормативних документів, ринку програмного забезпечення тощо. В останній день відбулось заслуховування результатів та визначення переможців.

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.

Другим досвідом неформальної освіти стали у 2023 році навчання з тематики «Infrastructure Control Systems», організованими в рамках Меморандуму про взаєморозуміння у сфері кіберзахисту між

Держспецзв'язку та Іспанським національним інститутом кібербезпеки (INCIBE). Навчання проходили в місті Леон, Королівство Іспанія та були організовані спеціально для співробітників Державної служби спеціального зв'язку та захисту інформації України Іспанським національним інститутом кібербезпеки (INCIBE) – некомерційною організацією для розвитку кібербезпеки та цифрової довіри громадян, іспанської академічної та дослідницької мережі (RedIRIS) і компаній.

У методики стажування молодих співробітників INCIBE застосовується багатоступеневе навчання з відпрацюванням практичних завдань, яке складається з наступних етапів: іспит на базові знання з кібербезпеки; прийом на стажування; самостійне, поглиблене вивчення матеріалу наданого INCIBE (1-2 місяці); іспит на поглиблені знання з кібербезпеки.

Зрештою, само стажування в INCIBE CERT поділяється по-перше, на роботу з інцидентами першого рівня критичності (1,5–2 місяці), яка включає: отримання досвіду від старших колег, щодо опрацювання інцидентів першого рівня критичності (1–2 тижні); опрацювання інцидентів першого рівня критичності під наглядом досвідчених колег (2–3 тижні); самостійне опрацювання інцидентів першого рівня критичності (2–3 тижні). По-друге, роботу з інцидентами другого рівня критичності (1,5–2 місяці), яка передбачає: отримання досвіду від старших колег, щодо опрацювання інцидентів другого рівня критичності (1–2 тижні); опрацювання інцидентів другого рівня критичності під наглядом досвідчених колег (2–3 тижні); самостійне опрацювання інцидентів другого рівня критичності (2–3 тижні).

По завершенню стажування отримується відгук співробітників INCIBE CERT та відбувається вибір подальшого напряму діяльності в INCIBE.

Отже, аналізуючи неформальну кіберосвіту Нідерландів та Іспанії, вимога науково-педагогічної сумлінності потребує визнання, що забезпечення якісної кіберосвіти – завдання, що вимагає комплексного підходу від усіх суб'єктів кібербезпеки, їх постійної взаємодії, обміну досвідом та організації на рівні законодавства (рис. 3).

Рис. 3. Ефективна кіберосвіта

ВИСНОВКИ

Загалом окреслена проблематика неформальної освіти, зокрема кіберосвіти є кроком до багатоманітного і поліаспектного дослідження найактуальнішої парадигми сучасності. Дослідження визначило, що основними підходами до неформального навчання є командна робота з елементами змагань, хакатони, Capture The Flag (CTF), Red Team – Blue Team training, а також відпрацювання сценаріїв на інтерактивних кіберплатформах. Власний досвід участі у неформальної освіті США та Європи засвідчив відсутність кордонів між формальною і неформальною видами освіти, поєднання когнітивних кодів яких надає континуум lifelong education при ефективній взаємодії з інформальною освітою та стейкхолдерами із державного та приватного сектору. Визначено, що неформальна кіберосвіта – це процес набуття цифрових навичок, знань і компетентностей без формальної участі в традиційних освітніх установах. Цей підхід дозволяє самостійно вивчати та розвивати свої навички в області кібербезпеки, програмування, веб-розробки, аналізу даних та інших сфер інформаційних технологій. Разом з тим кіберосвіта – це галузь освіти, яка спеціалізується на навчанні та розвитку компетенцій у сфері кібербезпеки. У дослідженні доведено, що неформальна кіберосвіта не тільки відображає нові тенденції у навчанні, але і активно реагує на виклики, які ставляться перед сучасними фахівцями кібербезпеки в умовах збільшення агресивних дій в кіберпросторі проти цивілізаційних та демократичних цінностей світової спільноти.

АНОТАЦІЯ

У статті проаналізовані нові актуальні форми неформальної кіберосвіти. Визначено, що міжнародне партнерство України та США у секторі безпеки та оборони має значні досягнення для неформальної

освіти висококваліфікованих українських фахівців з кібербезпеки. Методика навчання передбачає участь українських спеціалістів у курсах, тренінгах, літніх сесіях, освітніх конференціях і семінарах, під час яких використовується кейс-метод, рольові ігри і симуляції, письмові рефлексії та презентації. Зазначається, що під впливом основних положень Національної стратегії кібербезпеки США, активізація неформальної кіберосвіти відбувається у напряму оптимізації реалізації вимог з підвищення практичних навичок в галузі кібербезпеки. Неформальне навчання організовується в безпечному середовищі, з відпрацюванням як теоретичних, так і практичних аспектів, що дозволяє підвищити рівень адаптованості в кризових та нестандартних ситуаціях. Зазначено, що передбачена у національної стратегії кібербезпеки країн Європи неформальна кіберосвіта також активно розвивається. Доведено, що основними підходами до неформального навчання є командна робота з елементами змагань, хакатони, Capture The Flag (CTF), Red Team – Blue Team training, а також відпрацювання сценаріїв на інтерактивних кіберплатформах.

Література

1. Blažič B. J. Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?", *Educ. Inf. Technol.*, 2022. DOI::https://doi.org/10.1007/s10639-021-10704-y.

2. Estrategia Nacional de Ciberseguridad 2019 | DSN [Electronic resource] // DSN | Sitio oficial del Departamento de Seguridad Nacional. – Mode of access: https://www.dsn.gob.es/en/documento/estrategia-nacional-ciberseguridad-2019

3. The Netherlands Cybersecurity Strategy 2022-2028 [Electronic resource] // Home | National Coordinator for Security and Counterterrorism. – Mode of access: https://english.nctv.nl/topics/netherlands-cybersecurity-strategy-2022-2028/documents/publications/2022/12/06/the-netherlands-cybersecurity-strategy-2022-2028

4. Дубов Д. Національна стратегія кібербезпеки США 2023: критичні інфраструктура, координація, проактивність. Аналітична записка / Національний інституту стратегічних досліджень. Київ, 2023. [Рукопис на 4 арк.].

5. Закон України «Про освіту». 5 вересня 2017 року № 2145-VIII. URL: https://zakon.rada.gov.ua/laws/show/2145-19

6. Лазоренко О. Філософія освіти дорослих в контексті практичної парадигми пожиттєвого навчання: європейський приклад для України. *Філософія освіти*. 1-2(10). 2011. С. 255-265.

7. Лук'янова Л., Ващенко Л. Неформальна освіта різних категорій дорослого населення: теоретичні аспекти, методичні засади. *Освіта для миру: зб. наук. пр.* Київ-Переяслав-Хмельницький : Юрка Любченка, Т. 2. 2019. С.400-417. URL: https://lib.iitta.gov.ua/734295/1/volume_2_2019-400-417.pdf

8. Павлик Н.П. Зарубіжний досвід організації неформальної освіти. Наукові записки Ніжинського державного університету ім. Миколи Гоголя. Психолого-педагогічні науки. 2016. № 1. С. 264-273. URL: http://nbuv.gov.ua/UJRN/Nzspp_2016_1_50

9.Савельєв Є.В. Неформальна освіта як інструмент розвитку додаткових можливостей молоді. *Вчені записки Університету «КРОК»*. № 1 (61), 2021. С.228-232. DOI: 10.31732/2663-2209-2021-61-228-232

10. Стратегія розвитку вищої освіти в Україні на 2022-2032 роки. URL: https://zakon.rada.gov.ua/laws/show/286-2022-%D1%80#Text

11. Уваркіна О., Пучков О. 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

12. Хакатони що завгодно: що таке хакатон і навіщо брати в ньому участь. Happy Monday. URL: https://happymonday.ua/shho-take-hakaton-i-navishho-braty-v-nomu-uchast

13. USAID CYBERSECURITY ACTIVITY. Змагання CTF – ключ до успішної кар'єри у сфері кібербезпеки. DOU.UA. URL: https://dou.ua/forums/topic/43810/

Information about the authors:

Uvarkina Olena Vasylivna,
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"
4, Verkhneklyuchova str., Kyiv, 03056, Ukraine

Shevchuk Olga Sergiivna,
Teacher at the Special Department № 5
Institute of Special Communication and Information Protection
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"
4, Verkhneklyuchova str., Kyiv, 03056, Ukraine

Horniichur Ivan Viktorovich,
teacher of special department № 5
Institute of Special Communication and Information Protection
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"
4, Verkhneklyuchova str., Kyiv, 03056, Ukraine