УДК 35.088.6:[004:007:351.86](477)
DOI https://doi.org/10.32851/tnv-pub.2022.3.1

ПОДАЛЬШИЙ РОЗВИТОК СИСТЕМИ ПРОФЕСІЙНОГО НАВЧАННЯ ФАХІВЦІВ ІЗ КІБЕРБЕЗПЕКИ В УМОВАХ РОЗВИТКУ ЦИФРОВИХ ТЕХНОЛОГІЙ

Арсенович Л. А. *– доктор філософії з галузі публічне управління та адміністрування, заступник начальника управління – начальник відділу Департаменту кадрової роботи та управління персоналом Адміністрації Держспецзв'язку*
ORCID: 0000-0001-7081-2838

У статті розглянуто нормативно-правове підґрунтя організації професійного навчання в Україні та його форми організації. Конкретизоване сутнісне значення дефініції «віртуально-навчальна лабораторія», під яким вбачається віртуальне середовище навчання, яке дозволяє моделювати поведінку об'єктів реального світу в інформаційно-освітньому середовищі та оволодівати новими знаннями та вміннями. Наведено структурну схему моделі віртуально-навчальної лабораторії для моделювання процесів у кібербезпеці яка підтверджує доцільність та можливість її широкого використання як основного засобу формування системи знань, умінь та навичок при вивченні загальних і професійних цифрових компетенцій, ІТ-технологій та знань у сфері кібербезпеки. Запропоновано функціональну схему моделі віртуально-навчальної лабораторії для моделювання процесів у кібербезпеці, впровадження якої надасть широкі можливості для створення різних навчальних ситуацій у сфері кібербезпеки. Визначено переваги застосування віртуально-навчальної лабораторії для моделювання процесів у кібербезпеці для освітніх потреб державної і приватної кібербезпеки (у загальноосвітньому аспекті: формування фахових компетенцій; підвищення якості самостійної навчально-пізнавальної діяльності; розвиток мотиваційної діяльності; доступність та автоматизація операцій; у організаційно-технічному аспекті: заощадження на придбанні апаратного забезпечення; можливість використання різноманітних операційних систем та потенційно небезпечного програмного забезпечення; можливість створення необхідних апаратних конфігурацій), а також основні недоліки віртуально-навчальної лабораторії та хмарних технологій у цілому (безпека інформації, постійне з'єднання з мережею Інтернет, а також потреба у надійному з'єднанні з нею; можливість втрати даних у «хмарі»).

Ключові слова: *віртуально-навчальна лабораторія, інформаційні технології, кібербезпека, професійне навчання, фахівець із кібербезпеки.*

Arsenovych L. A. Further development of the system of professional training of cyber security specialists in the conditions of the development of digital technologies

The paper considers the regulatory and legal basis of the arrangement of professional training in Ukraine and its organization forms. The essential meaning of the definition "virtual educational laboratory" is particularized, which is understood as a virtual learning environment that makes it possible to simulate the behavior of real world objects in an informational and educational environment and to master new knowledge and skills. The structural diagram of the model of a virtual educational laboratory for modeling processes in cyber security is presented, which confirms the expediency and possibility of its wide use as the main means of forming the system of knowledge, abilities and skills in the study of general and professional digital competencies, IT technologies and knowledge in the field of cyber security. A functional layout of a model of a virtual educational laboratory for modeling processes in cyber security is proposed, the implementation of which will provide ample opportunities for creating various educational situations in the field of cyber security. The advantages of using a virtual educational laboratory for modeling the processes in cyber security for the educational needs of state and private cyber security have been determined (in the general educational aspect: formation of professional competences; improvement of quality of independent educational and cognitive activities; development of motivational activities; accessibility and automation of operations; in the organizational and technical aspect: savings on the purchase of hardware; the possibility of using various operating systems and potentially dangerous software; the possibility of creating the necessary hardware configurations), as well as the main disadvantages of a virtual

educational laboratory and cloud technologies in general (information security, constant connection to the Internet, as well as the need for a reliable connection to it; the possibility of data loss in the "cloud").

Key words: *virtual educational laboratory, information technologies, cyber security, professional training, cyber security specialist.*

Постановка проблеми та її зв'язок із важливими науковими і практичними завданнями. Науково-технічний прогрес докорінно змінив сучасне суспільство: на теперішній день інформаційні технології відіграють чи не найважливішу роль у розвитку країн та визначенні рівня життя населення. За останні десятиліття інформація стала настільки потужним фактором розвитку суспільства, що привела до утворення нового інформаційного укладу, який сприяє внутрішньодержавній і світовій інтеграції та реінтеграції. Україна на теперішній час міцно стала на шлях впровадження нових технологій.

В умовах збройної агресії проти України, швидкий розвиток та всеохопливе впровадження сучасних інформаційних технологій, формування і розвиток всесвітнього кіберпростору призвело до формування нового спектра ризиків і загроз у сферах національної безпеки і оборони, які розповсюджуються в кіберпросторі та (або) через кіберпростір. Кібернетичні загрози охоплюють усі базові сфери суспільної і громадської діяльності (політичну, безпекову, правову, економічну, інфраструктурну, соціальну тощо), загрозливо впливаючи на складові сектору безпеки і оборони України, основних суб'єктів національної системи кібербезпеки та на органи державної влади України в цілому.

У цьому аспекті передумовою до формування ефективної системи підготовки кадрів у сфері кібербезпеки в умовах розвитку цифрового суспільства України буде повна й відкрита освітня взаємодія держави та приватного сектора, без якого неможливо побудувати ефективну кібернетичну освіту.

Аналіз останніх досліджень, в яких започатковано розв'язання проблеми та визначення невирішених раніше частин загальної проблеми, яким присвячена стаття. Наукові напрацювання вчених і практиків засвідчують, що професійна підготовка фахівців у сфері кібербезпеки є одним із напрямів державної політики у сферах національної безпеки і оборони, без якого є неможливими захищене передавання інформації і відповідно – науково-технічний та соціально-економічний розвиток країни.

Як свідчать останні дослідження і публікації, проблеми професійного розвитку фахівців із кібербезпеки є малодослідженими. Так, І. Діордіца у своїх статтях досліджує питання стандартизації підготовки фахівців із кібербезпеки та здійснює аналіз стану підготовки фахівців у сфері кібернетичної безпеки станом на 2015–2016 роки. С. Мельник у науковій роботі визначає концептуальні основи організації професійної підготовки майбутніх фахівців із кібербезпеки у вищих навчальних закладах. А група науковців у складі В. Бурячка, І. Пархомея, М. Степанова та В. Толубка у своїй статті вивчає проблемні питання та актуальні завдання підготовки фахівців з кібернетичної безпеки галузі знань «Інформаційні технології».

Незважаючи на велику кількість фундаментальних та прикладних робіт, які стосуються актуальних питань підготовки ІТ-фахівців, питанням професійного навчання фахівців із кібербезпеки основних суб'єктів національної системи кібербезпеки приділено мало уваги, що й обумовило актуальність дослідження.

Метою статті є здійснення дослідження системи професійного навчання суб'єктів державної та комерційної кібербезпеки та надання практичних рекомендацій щодо подальшої розбудови системи підготовки кадрів у сфері кібербезпеки.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. З кожним роком ІТ-галузь стрімко розвивається не лише у світі, а й в Україні. Сфера кібербезпеки приваблює українців, особливо молодь, стабільними й хорошими зарплатами, професійним розвитком, кар'єрним ростом та іншими «бонусами», адже надає ІТ-ринку якісний продукт та ефективну співпрацю. На сьогодні, саме сферу кібербезпеки називають «локомотивом» української економіки. І недарма. Адже згідно з даними платіжного балансу України, експорт комп'ютерних послуг упродовж 2019 року зріс на 30,2% порівняно з попереднім роком і склав 4,17 млрд дол., як повідомляє Асоціація ІТ України [1].

Українська ІТ-індустрія як невід'ємна частина глобальної економіки безпосередньо залежить від навичок та знань фахівців, які працюють у галузі, а подальший фінансовий успіх – від кількості та якості кадрів. Тому розвиток кадрового потенціалу в Україні – одне з головних питань для представників вітчизняного ринку кібер-послуг. На теперішній час в галузі кібербезпеки, за різними оцінками, – більш ніж 120 тис. спеціалістів з розробки програмного забезпечення, а приріст спеціалістів, за неофіційними даними, становить близько 19% щороку.

Проте, незважаючи на помітну динаміку приросту кадрів, на сьогодні для українського ринку кібербезпеки дедалі актуальнішим стає питання кадрового голоду. Цей виклик не унікальний для України – перед ним постає і низка інших країн, де активно розвивається кіберіндустрія, і проблема стає глобальною. У рамках опитування, проведеного Асоціацією IT Ukraine, практично кожен з керівників ІТ-компаній, що працюють на території України, акцентував питання розвитку та подальшої модернізації освітньої системи як нагальне та актуальне.

Сучасне суспільство характеризується стрімкими змінами в усіх сферах життя, що особливо впливає на розвиток освітянського простору. Освітня сфера нині зазнає значних трансформаційних процесів та вимагає нових та сучасних освітніх підходів. Тому вимогою сьогодення стає апробація й упровадження інноваційних освітніх технологій у навчальний процес, у тому числі й у сфері кібербезпеки. Концепція розвитку цифрових компетентностей, схвалена розпорядженням Кабінету Міністрів України від 3 березня 2021 року № 167-р [2], визначає у тому числі здобуття особою цифрової освіти з використанням інформаційних ресурсів, нових освітніх технологій та цифрових освітніх ресурсів, спрямованих на підвищення рівня цифрових навичок та цифрових компетентностей.

В умовах інформаційного суспільства деякі аспекти традиційного навчання поступово втрачають свій сенс. Тому дієвим інструментом поліпшення якості освіти визначають застосування компетентнісного підходу до неї, який на перше місце ставить не поінформованість особи, а вміння на основі знань розв'язувати проблеми, які виникають у різних ситуаціях. Тому, з метою створення ефективної системи професійного (корпоративного) навчання фахівців із кібербезпеки, потрібно змінювати технологію навчального процесу та підходи до його організації.

На теперішній час нормативно-правовим підґрунтям організації професійного навчання є Закон України від 12 січня 2012 року № 4312-VI «Про професійний розвиток працівників» [3], який визначає правові, організаційні та фінансові засади функціонування системи професійного розвитку працівників. Так, відповідно до статті 6 зазначеного Закону, роботодавці можуть здійснювати формальне і неформальне професійне навчання працівників. Враховуючи, що формальне професійне навчання працівників – це набуття працівниками професійних знань, умінь і навичок безпосередньо у роботодавця відповідно до вимог державних стандартів освіти, а неформальне професійне навчання працівників – це набуття

працівниками професійних знань, умінь і навичок, яке не регламентоване місцем набуття, строком та формою навчання, можна вважати, що основні суб'єкти національної системи кібербезпеки (Держспецзв'язку, Нацполіція, СБ України, Міноборони, Генштаб ЗС України, розвідувальні органи України), які відносяться до державної кібербезпеки, надають формальну професійну освіту, а ІТ-компанії, які відносяться до комерційної кібербезпеки, організовують неформальну професійну освіту, або так зване корпоративне навчання.

Науковці розрізняють дві основні форми професійного навчання в трудових колективах: навчання безпосередньо на робочому місці та навчання поза робочим місцем. Вибір форми професійного навчання здійснюється роботодавцем і залежить від мети навчання й можливостей підприємства.

Навчання на робочому місці організовується безпосередньо для органу (підрозділу) або компанії та її працівників. Співробітник навчаючись на робочому місці підтримує на належному рівні набуті знання та удосконалює практичні навички для якісного та ефективного виконання службових обов'язків. Перевагами такого навчання є своєчасність навчання та використання вивченого на робочому місці, а недоліками – вузько спрямованість та обмеженість ситуацією, що не позволяє вийти за рамки традиційної поведінки й не дає можливостей для розкриття потенціалу працівника. Навчання поза робочим місцем може здійснюватись будь де: в конференц-залі, кафетерії або на свіжому повітрі. При цьому такі заняття можуть проходити у виді лекції, конференції, тематичної дискусії, семінару, он-лайн курсу, вебінару, воркшопу, корпоративного блогу тощо.

Необхідно зазначити, що в науковій літературі розрізняють також закрите або відкрите професійне навчання. Закрите навчання організовується персоналом підприємства, без запрошення інших фахівців, а відкрите навчання здійснюється зовнішніми викладачами (тренерами). Може бути й комбінована форма навчання, яка передбачає залучення внутрішніх і зовнішніх інструкторів [4].

Деяким прикладом організації внутрішньої системи навчання фахівців із кібербезпеки є досвід підрозділів комерційної кібербезпеки, де система корпоративного навчання є важливим інструментом для розвитку кадрового потенціалу, та є поєднанням навчання безпосередньо на робочому місці та поза ним.

Підвищення кваліфікації персоналу будь-якої ІТ-компанії сьогодні обумовлено вимогами ринкової конкуренції, потребою в оптимізації роботи колективу та необхідністю змін. Корпоративне навчання надає компанії новий імпульс, забезпечує її конкурентоспроможність і виводить персонал на якісно інший рівень. Корпоративне навчання покликане створити управлінську команду на дуже високому рівні, а його завдання – об'єднати керівників-професіоналів в різних сферах діяльності. Як і партнерство з вищими навчальними закладами, цей тип навчання є характерним як для великих міжнародних компаній, так і для менших представників ІТ-індустрії. Внутрішні освітні ініціативи компаній мають кілька напрямків: це навчальні довгострокові програми, окремі лекції та воркшопи тощо, які мають у переважній більшості звичний для кіберосвіти дистанційний режим навчання. Тематика охоплює важливі сегменти знань та навичок, що необхідні для подальшого гармонійного розвитку співробітників та акумулювання експертизи всередині компанії: комунікаційні навички та робота в команді, управління проєктами, вивчення іноземних мов та ініціативи технічного спрямування. «По-перше, за допомогою програм у сфері корпоративної освіти ми можемо виконувати складні завдання для задоволення потреб замовника. По-друге, спеціалісти обирають собі місце роботи не тільки за параметром заробітної платні, але здебільшого йдуть

туди, де бачать перспективи для розвитку себе як професіонала. По-третє, компанія залучає найкращі кадри з ринку, і проведення навчань дозволяє нам накопичувати експертизу, яка робить нас привабливішими в очах майбутніх замовників. Нарешті, завдяки навчанням ми можемо розв'язати різні проблеми, з якими стикаємось в роботі як спеціалісти», – розповідають в Intellias, що є провідною компанією в IT-галузі [5].

Підтверджує цю тезу і Тетяна Хряпіна, керівник відділу навчання компанії GlobalLogic: «Одне з головних завдань, які ставить для себе компанія, запускаючи освітні ініціативи, – це пожвавлення обміну досвідом та підвищення кваліфікації наших спеціалістів. Наші інженери ведуть велику кількість різноманітних проєктів, і за допомогою освітньої платформи GlobalLogic Education вони знаходять потрібну експертизу, знання та підтримку, необхідну для розвитку. Також ми стаємо більш конкурентними на ринку та можемо надавати якісніші послуги нашим партнерам та замовникам» [5].

Слід зазначити, що корпоративне навчання є відкритим не лише для працівників IT-бізнесу, а й для зовнішніх користувачів. Крім цього, в деяких компаніях корпоративна освіта виокремлюється у спеціалізовані департаменти, академії та навіть університети, що мають стратегічне значення для подальшого розвитку сфери кібербезпеки. Яскравим прикладом такого виокремлення освітнього напрямку є корпоративний університет корпорації SoftServe, заснований у 2008 році. Нині це потужний навчальний підрозділ, що здійснює діяльність за декількома векторами роботи, спрямованих на розвиток як спеціалістів компанії, так і на тих, хто хоче опанувати спеціальність у сфері кібертехнологій. В університеті на постійній основі функціонують декілька проєктів: IT Academy – підрозділ, що проводить технологічні курси для кіберзахисників; Training and Development Group – підрозділ, що організовує та проводить внутрішні навчання та тренінги працівників; Language School – корпоративна мовна школа, що проводить індивідуальні навчання з іноземних мов; E-learning team – підрозділ, що здійснює розробку внутрішніх онлайн-курсів; Сертифікаційний центр, який надає можливість проходити внутрішні та міжнародні технологічні сертифікації. Зазначені підрозділи, на кшталт SoftServe, покривають по суті всі потреби спеціалістів у сфері професійної освіти, створюючи необхідні умови для розвитку талантів всередині компанії.

При цьому, більшість освітніх ініціатив IT-компаній для слухачів безкоштовні – комерційна кібербезпека не розглядає корпоративні програми як джерела прибутку. Навпаки, внутрішнє навчання – це суттєвий пункт видатків. Загалом же корпоративні програми реалізовують IT-компанії в містах, де розташовані їхні офіси, і фактично доступні в усіх великих населених пунктах країни, формуючи один з головних елементів інфраструктури української кіберіндустрії.

Таким чином, до переваг корпоративного навчання комерційної кібербезпеки слід віднести максимальну участь фахівців компанії в навчальному процесі, повну адаптованість навчальних програм до цілей і завдань компанії, консалтингову допомогу викладачів та можливість проведення занять на будь якій території.

Процес професійного навчання фахівців із кібербезпеки основних суб'єктів національної системи кібербезпеки має свої особливості. Він проводиться в умовах постійної службової та бойової готовності та характеризується різко вираженою практичною спрямованістю. Підготовка протікає в умовах високого рівня інтелектуального, морального, психологічного та фізичного напруження, а процес навчання знаходиться в безпосередній залежності від технічних можливостей того чи іншого органу або підрозділу.

Професійне навчання фахівців із кібербезпеки основних суб'єктів національної системи кібербезпеки – організована та цілеспрямована система навчання, що передбачає:

– задоволення потреб основних суб'єктів національної системи кібербезпеки кваліфікованим особовим складом;

– набуття нових та/або вдосконалення раніше набутих знань, практичного досвіду виконання завдань та обов'язків у службовій діяльності;

– оновлення, розширення і формування нових професійних знань за напрямами діяльності;

– вивчення сучасних методів управління, ознайомлення з досягненнями науки і техніки та перспективами їх розвитку;

– створення умов щодо професійного та особистісного розвитку.

Враховуючи зазначене, можна зробити висновок, що професійне навчання фахівців основних суб'єктів національної системи кібербезпеки повинне стати відповіддю на виклики, які постають перед сучасною освітою. У зв'язку з цим управління розвитком персоналу повинно сконцентрувати свої зусилля на вирішенні таких проблем, як розробка стратегії з питань формування кваліфікованого персоналу; визначення потреб у навчанні працівників; вибір форм і методів професійного розвитку персоналу; вибір програмно-методичного та матеріально-технічного забезпечення процесу навчання; фінансове забезпечення всіх видів навчання в потрібній кількості.

У цьому аспекті пройти навчання загальним і професійним цифровим компетенціям, ІТ-технологіям та знанням у сфері кібербезпеки, набути фахові компетенції і попрактикуватися в умовах, максимально наближених до реальних кіберзагроз, працівникам державних і недержавних суб'єктів кібербезпеки можуть допомогти, наприклад, віртуально-навчальні лабораторії для моделювання процесів у кібербезпеці, впровадження яких у практичну площину кіберосвіти стане дієвою розбудовою системи підготовки кадрів у сфері кібербезпеки.

З'ясуємо сутність поняття «віртуально-навчальна лабораторія», визначивши при цьому значення слів «віртуальна реальність» та «навчальна лабораторія». Віртуальна реальність – це комп'ютерні системи, які забезпечують візуальні й звукові ефекти, що занурюють глядача в уявний світ за екраном. За іншим трактуванням – це нова технологія безконтактної інформаційної взаємодії, яка створює за допомогою комплексних мультимедіа операційних середовищ ілюзію безпосереднього входження й присутності в реальному часі в стереоскопічно представленому «екранному світі». Більш абстрактно – це світ, створений в уяві користувача [6, с. 6]. Навчальна лабораторія – навчально-допоміжна установа, призначена для проведення практичних занять. Оснащена спеціальним обладнанням, апаратурою та матеріалами для проведення демонстрацій дослідів і виконання самостійних робіт [7, с. 185]. Поєднавши ці два поняття, під віртуально-навчальною лабораторією слід розуміти віртуальне середовище навчання, яке дозволяє моделювати поведінку об'єктів реального світу в інформаційно-освітньому середовищі та оволодівати новими знаннями та вміннями.

Чинниками створення та впровадження віртуальних лабораторій у деяких сферах діяльності з одного боку став швидкий розвиток інформаційних технологій, а з іншого – велика ціна апаратного обладнання для проведення тих чи інших практичних занять. Віртуальна лабораторія для вивчення різноманітних технологій насправді не існує у вигляді окремого приміщення, проте її функціональні можливості реалізуються із застосуванням реальних апаратно-програмних засобів та комп'ютерних мереж [8, с. 130]. Така лабораторія розробляється під певну предметну галузь, яка надає необхідний інструментарій для розв'язування задач

та проведення віртуальних експериментів у даній предметній галузі. Основним завданням віртуальної лабораторії інформаційних технологій є моделювання процесів обробки даних у сучасних інформаційних системах та мережах.

Програмною основою спроєктованої віртуальної лабораторії є технології хмарних обчислень, які доступні, у тому числі, у режимі віддаленого доступу через канали глобального зв'язку, наприклад Інтернету. Нагадаємо, що хмарними називають такі технології, які забезпечують доступ до обчислювальних ресурсів засобами протоколу передавання гіпертексту (HTTP, HTTPS). Тобто хмарними є технології, які забезпечують можливість роботи з її ресурсами (апаратним, системним, прикладним програмним забезпеченням) засобами веббраузера [8, с. 131]. Наприклад, співробітник, перебуваючи вдома, в Інтернет-кафе або навіть у закордонному відрядженні для доступу до віртуально-навчальної лабораторії може використовувати ноутбук, планшетний комп'ютер або смартфон.

Як відомо, системні вимоги щодо розгортання хмарної інфраструктури передбачають використання двох комп'ютерів, один з яких виконуватиме функції сервера управління та первинного сховища, а інший відповідатиме за роботу віртуальних машин (гіпервізор) та міститиме вторинне сховище (рис. 1).

Зазвичай у віртуальній лабораторії відомості з предметної галузі базуються на окремих фактах, а тому обмежені набором заздалегідь передбачених експериментів. Інший підхід передбачає можливість проводити будь-які експерименти, не обмежуючись заздалегідь підготовленим набором результатів. Широкий спектр можливостей спеціального програмного забезпечення для віртуалізації надає унікальні можливості при організації навчального процесу, що і підтверджує доцільність та можливість його широкого використання як основного засобу формування системи знань, умінь та навичок при вивченні загальних і професійних цифрових компетенцій, ІТ-технологій та знань у сфері кібербезпеки, а також при формуванні системи умінь у галузі інформаційних технологій.

Основними характеристиками наведеної моделі віртуально-навчальної лабораторії є:

– можливість здійснення обслуговування за потреби (користувач може негайно отримати системні ресурси (увімкнути, перезавантажити віртуальний комп'ютер) без попереднього запиту;

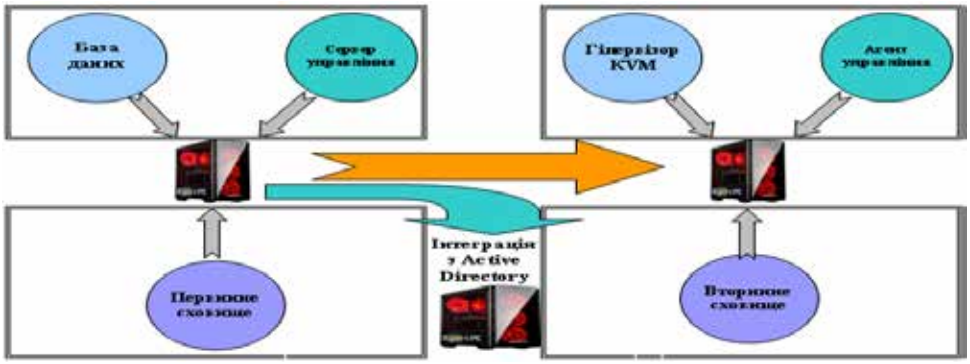

Рис. 1. Структурна схема моделі віртуально-навчальної лабораторії для моделювання процесів у кібербезпеці

Розробив автор

– повсюдний доступ не залежно від географічного розташування;

– еластичність масштабування, яка передбачає можливість зміни обсягу обчислюваних ресурсів без суттєвих змін у роботі операційних систем [8, с. 134].

Проєкт віртуально-навчальної лабораторії надасть широкі можливості для створення різних навчальних ситуацій у сфері кібербезпеки, в яких користувачі зможуть освоювати і відпрацьовувати необхідні навички в службовій діяльності. Серед них: інформаційна грамотність (тобто вміння шукати інформацію, порівнювати її з різних джерел, розпізнавати та вибирати найнеобхідніше); мультимедійна грамотність – здатність розпізнавати і використовувати різні типи медіаресурсів як у роботі, так і в навчанні; організаційна грамотність (здатність планувати свій час так, щоб встигнути все, що заплановано); розуміння взаємозв'язків, які існують між різними людьми, групами та організаціями; комунікативна грамотність (це навички ефективного спілкування та співробітництва); продуктивна грамотність – здатність до створення якісних продуктів, можливість використання засобів планування тощо.

Серед переваг застосування віртуально-навчальної лабораторії для моделювання процесів у кібербезпеці для освітніх потреб державної і приватної кібербезпеки слід виділити:

у загальноосвітньому аспекті:

– формування фахових компетенцій, які можуть бути безпосередньо перенесені в реальність;

– підвищення якості самостійної навчально-пізнавальної діяльності;

– зацікавленість у вивченні матеріалу, розвиток мотиваційної діяльності;

– доступність та автоматизацію операцій;

– постійне удосконалення програмних систем та технологій тощо [9, с. 100];

у організаційно-технічному аспекті:

– заощадження на придбанні апаратного забезпечення;

– доступ до комп'ютерів віртуально-навчальної лабораторії можна забезпечити із традиційних та мобільних платформ, використовуючи стандартні протоколи (RDP, SSH, VNC);

– можливість використання різноманітних операційних систем;

Рис. 2. Функціональна схема моделі віртуально-навчальної лабораторії для моделювання процесів у кібербезпеці

Розробив автор

– можливість використання потенційно небезпечного програмного забезпечення без загрози ушкодження реальних комп'ютерів;

– можливість створення необхідних апаратних конфігурацій;

– можливість об'єднання віртуальних машин у локальну мережу та доступ до них засобами поширених протоколів;

– високу мобільність працівників та кібертренерів (викладачів), що вирішує питання «прив'язаності» до певного місця, а також створює можливості для самостійної роботи фахівців у сфері кібербезпеки.

Основними недоліками віртуально-навчальної лабораторії та хмарних технологій у цілому є:

– безпека інформації (не кожному користувачу зберігання особистих даних на віддаленому сервері видається надійним);

– постійне з'єднання з мережею Інтернет, а також потреба у надійному з'єднанні з нею;

– можливість втрати даних у «хмарі» (якщо дані втрачаються – вони втрачаються назавжди).

Сучасний освітній процес спирається все більше і більше на інформаційні технології. Віртуальні освітні технології в світі тільки розпочали конкурувати з традиційними формами навчання, та в умовах сьогодення є безсумнівною підтримкою та стимулом до плідного навчання, цікавої наукової діяльності та законодавчої ініціативи.

Використання та подальше впровадження віртуально-навчальної лабораторії для моделювання процесів у кібербезпеці для потреб державної і приватної кібербезпеки стане ефективним інструментом навчання, який дозволить рухатися власною освітньою траєкторією та розширить коло навчальних задач і збагатить їх сучасним змістом. Практика засвідчує, що ніяка теорія не буде реалізована в освітній діяльності, якщо для її впровадження не буде розроблений відповідний алгоритм. Тому надалі вектор досліджень у сфері кіберосвіти необхідно спрямовувати на створення освітньої медіатехнології як цілісної системи підготовки кадрів у сфері кібербезпеки в умовах розвитку цифрового суспільства України.

Висновки. Експертні дослідження свідчать, що в сучасному світі підготовка кадрів із кібербезпеки не може обмежуватися лише отриманням вищої освіти у закладах освіти за відповідною спеціальністю. Для збереження належної конкурентоспроможності та професійного рівня цим фахівцям необхідно перманентно підвищувати свою кваліфікацію на засадах так званої концепції безперервної освіти (або «освіти протягом життя»), множинність форм та методів якої відкриває ще один широкий та перспективний напрям для галузевого кібербезпекового державно-приватного партнерства. Можливі декілька варіантів роботи в цьому напрямі, серед яких перепідготовка в рамках післядипломної освіти фахівців у споріднених з кібернетичною безпекою спеціальностях, застосування нелінійної схеми підготовки фахівців, використання потенційних можливостей неформальної освіти для підвищення кваліфікації фахівців-практиків через проведення кібертренінгів, семінарів, міжнародних стажувань тощо [10, с. 62].

Критично важливим є також забезпечення належного рівня обізнаності персоналу компаній та установ у питаннях кібернетичної безпеки, – знову ж таки спільними зусиллями приватних та державних суб'єктів. Форми кібербезпекового державно-приватного партнерства тут можуть бути різноманітними: спільні семінари, тренінги, онлайн курси, залучення науково-аналітичних та консалтингових компаній усіх форм власності і багато іншого. Крім того, необхідними є регулярні

тестування (навчання) на проникнення, моделювання загроз, грамотність поведінки працівників/користувачів у мережі (дотримання елементарних правил онлайн безпеки, стійкість до спроб фішингу тощо).

Навчання протягом життя виходить на чільні позиції у світових освітніх процесах – це диктується базовими тенденціями сучасного розвитку людства. Такий підхід, на наш погляд, дозволить кардинально змінити систему підготовки кадрів у сфері кібербезпеки. Адже до цього часу, на жаль, у переважній більшості вона зорієнтована на запити минулого. Сучасна ж економіка потребує кадрів, готових працювати в умовах конкуренції, тобто в інноваційній економіці.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Як карантин вплинув на українських програмістів. *Українське інтернет-видання «День»*. URL: https://m.day.kyiv.ua/uk/article/ekonomika/it-v-onlayn

2. Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації : розпорядження Кабінету Міністрів України № 167-р від 03.03.2021 р. URL: https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80#Text

3. Про професійний розвиток працівників : Закон України № 4312-VI від 12.01.2012 р. URL: https://zakon.rada.gov.ua/laws/show/4312-17#Text

4. Литовченко І. М. Форми й методи корпоративного навчання у контексті навчання дорослих. *Освіта дорослих: теорія, досвід, перспективи.* 2015. Вип. 2. С. 45–50.

5. Розвиток української ІТ-індустрії. Аналітичний звіт. URL: https://ko.com.ua/files/u125/Ukrainian_IT_Industry_Report_UKR.pdf

6. Крупський Я. В. Тлумачний словник з інформаційно-педагогічних технологій : словник / Я. В. Крупський, В. М. Михалевич. Вінниця : ВНТУ, 2010. 72 с.

7. Гончаренко С. У. Український педагогічний словник / Семен Гончаренко ; гол. ред. С. Головко. Київ: Либідь, 1997. 373 с.

8. Олексюк В. П. Досвід організації віртуальних лабораторій на основі технологій хмарних обчислень. *Інформаційні технології в освіті*. 2014. Вип. 20. С. 128–138.

9. Бурячок В. Л. Віртуальна лабораторія для моделювання процесів в інформаційній та кібербезпеці як засіб формування практичних навичок студентів / В. Л. Бурячок, С. М. Шевченко, П. М. Складанний. *Кібербезпека: освіта, наука, техніка*. 2018. № 2. С. 98–104.

10. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України : аналіт. доп. / за заг. ред. Д. Дубова. К. : НІСД, 2018. 84 с.

REFERENCES:

1. Yak karantyn vplynuv na ukrainskykh prohramistiv. Ukrainske internet-vydannia “Den” [How the quarantine affected Ukrainian programmers. Ukrainian online publication "Den"]. URL: https://m.day.kyiv.ua/uk/article/ekonomika/it-v-onlayn

2. The Cabinet of Ministers of Ukraine (2021). Pro skhvalennia Kontseptsii rozvytku tsyfrovykh kompetentnostei ta zatverdzhennia planu zakhodiv z yii realizatsii [On the approval of the Concept of the development of digital competences and the approval of the plan of measures for its implementation]. URL: https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80#Text

3. The Verkhovna Rada of Ukraine (2012). Pro profesiinyi rozvytok pratsivnykiv [About the professional development of employees]. URL: https://zakon.rada.gov.ua/laws/show/4312-17#Text

4. Lytovchenko I. M. (2015) Formy y metody korporatyvnoho navchannia u konteksti navchannia doroslykh [Forms and methods of corporate training in the context of adult education]. *Osvita doroslykh: teoriia, dosvid, perspektyvy*. Vup. 2. 45–50.

5. Rozvytok ukrainskoi IT-industrii. Analitychnyi zvit [Development of the Ukrainian IT industry. Analytical report]. URL: https://ko.com.ua/files/u125/Ukrainian_IT_Industry_Report_UKR.pdf

6. Krupskyi Ya. V. (2010) Tlumachnyi slovnyk z informatsiino-pedahohichnykh tekhnolohii : slovnyk [Explanatory dictionary of information and pedagogical technologies: dictionary]. Vinnytsia : VNTU, 72 s.

7. Honcharenko S. U. (1997) Ukrainskyi pedahohichnyi slovnyk [Ukrainian pedagogical dictionary]. Kyiv : Lybid, 373 s.

8. Oleksiuk V. P. (2014) Dosvid orhanizatsii virtualnykh laboratorii na osnovi tekhnolohii khmarnykh obchyslen [Experience in organizing virtual laboratories based on cloud computing technologies]. *Informatsiini tekhnolohii v osviti*. Vyp. 20. 128–138.

9. Buriachok V. L. (2018) Virtualna laboratoriia dlia modeliuvannia protsesiv v informatsiinii ta kiberbezpetsi yak zasib formuvannia praktychnykh navychok studentiv [Virtual laboratory for modeling processes in information and cyber security as a means of forming students' practical skills]. *Kiberbezpeka: osvita, nauka, tekhnika*. № 2. 98–104.

10. Derzhavno-pryvatne partnerstvo u sferi kiberbezpeky: mizhnarodnyi dosvid ta mozhlyvosti dlia Ukrainy : analit. dop. [Public-private partnership in the field of cyber security: international experience and opportunities for Ukraine]. NISD, 2018, 84 s.