

АНАЛІЗ ВІТЧИЗНЯНОГО Й ІНОЗЕМНОГО ДОСВІДУ МЕТОДИЧНОГО ЗАБЕЗПЕЧЕННЯ З КІБЕРНЕТИЧНОЇ БЕЗПЕКИ У ПРОФЕСІЙНІ ПІДГОТОВЦІ МАЙБУТНІХ ІНЖЕНЕРІВ-ПРОГРАМІСТІВ

Кирило Комарницький, Альона Чорна

Мелітопольський державний педагогічний університет імені Богдана Хмельницького

Анотація:

У статті проаналізовано методичне забезпечення професійної підготовки майбутніх інженерів-програмістів у сфері кібербезпеки, розглянуто вітчизняний та іноземний досвід, зокрема стандарти, навчальні програми, методичні підходи та використання інформаційно-комунікаційних технологій (ІКТ) у навчальному процесі. Методологія дослідження містить кілька основних етапів та методів, що дозволяють всебічно вивчити питання методичного забезпечення кібернетичної безпеки у професійній підготовці майбутніх інженерів-програмістів. Літературний аналіз охоплює дослідження наукових статей, монографій, книг та інших публікацій, присвячених методичному забезпеченню кібербезпеки, що дозволяє зібрати та систематизувати інформацію про поточний стан наукових студій у цій галузі, а також огляд державних стандартів, нормативно-правових актів та рекомендацій, що регулюють професійну підготовку фахівців з кібербезпеки в Україні та за її кордоном. Порівняльний аналіз має у своєму складі порівняння навчальних програм та методичних підходів у провідних українських та закордонних університетах, що допомагає визначити сильні та слабкі сторони вітчизняної системи підготовки фахівців з кібербезпеки. Результати роботи демонструють нові дані щодо відмінностей між вітчизняним і закордонним підходами до методичного забезпечення з кібербезпеки. Встановлено, що українські університети акцентують увагу на базових аспектах кібербезпеки з обмеженням використання інтерактивних методів і сучасних ІКТ через недостатню технічну оснащеність. Закордонні університети, навпаки, широко використовують інтерактивні методи, віртуальні лабораторії, симуляції та проблемно-орієнтоване навчання, що забезпечує більш глибоке засвоєння матеріалу та розвиток практичних навичок студентів. У висновках викладено рекомендації щодо інтеграції міжнародних стандартів у навчальні програми, розширення кількості практичних занять, активного використання сучасних онлайн-ресурсів і підвищення професійного розвитку викладачів. Запропоновано збільшити інвестиції у технічну базу університетів, організовувати курси підвищення кваліфікації для викладачів та налагоджувати співпрацю з міжнародними організаціями та провідними компаніями у сфері кібербезпеки. Інтеграція цих заходів сприятиме підвищенню якості підготовки фахівців з кібербезпеки в Україні та їх конкурентоспроможності на міжнародному ринку праці.

Ключові слова:

аналіз; методичне забезпечення; кібернетична безпека; професійна підготовка; інженери-програмісти; вітчизняний та іноземний досвід.

Resume:

Komarnytsky Kyrylo, Chorna Alona. Analysis of domestic and foreign experience of methodological provision of cybernetic security in the professional training of future software engineers.

The article analyzes the methodological support of professional training of future software engineers in the field of cyber security, considering domestic and foreign experience, including standards, curricula, methodological approaches and the use of information and communication technologies (ICT) in the educational process. The research methodology includes several main stages and methods that allow to comprehensively study the issue of methodical provision of cyber security in the professional training of future software engineers. Literary analysis covers the analysis of scientific articles, monographs, books and other publications devoted to the methodical provision of cyber security, which allows to collect and systematize information about the current state of research in this field, as well as a review of state standards, legal acts and recommendations regulating professional training cyber security specialists in Ukraine and abroad. The comparative analysis includes a comparison of educational programs and methodological approaches in leading Ukrainian and foreign universities, which helps to determine the strengths and weaknesses of the domestic system of training of cyber security specialists. The results of the work include new data on the differences between domestic and foreign approaches to methodological support for cyber security. It is established that Ukrainian universities focus on the basic aspects of cyber security with limited use of interactive methods and modern ICT due to insufficient technical equipment. Foreign universities, on the contrary, widely use interactive methods, virtual laboratories, simulations and problem-oriented learning, which ensures a deeper assimilation of the material and the development of students' practical skills. The conclusions of the study include recommendations for the integration of international standards into educational programs, expansion of the number of practical classes, active use of modern online resources, and improvement of the professional development of teachers. It is proposed to increase investments in the technical base of universities, organize advanced training courses for teachers and establish cooperation with international organizations and leading companies in the field of cyber security. The integration of these measures will contribute to the improvement of the quality of training of cyber security specialists in Ukraine and their competitiveness on the international labor market.

Key words:

analysis; methodological support; cyber security; professional training; software engineers; domestic and foreign experience.

Постановка проблеми. У сучасному світі питання кібернетичної безпеки набувають все більшої актуальності. З розвитком інформаційних технологій і збільшенням кількості кіберзагроз зростає потреба у висококваліфікованих фахівцях з кібербезпеки, зокрема інженерах-програмістах, здатних захищати інформаційні системи від зловмисних дій. Однак, рівень методичного забезпечення з кібербезпеки у вітчизняній освіті ще не досягнув необхідного рівня.

Аналіз вітчизняного та іноземного досвіду у цій сфері є важливим для розробки ефективних

підходів до професійної підготовки майбутніх інженерів-програмістів. Визначення найкращих практик та адаптація їх до умов національної системи освіти сприятиме підвищенню рівня підготовки фахівців, здатних ефективно працювати у сфері кібербезпеки.

У зв'язку з цим виникає необхідність систематизації та аналізу існуючого досвіду методичного забезпечення з кібербезпеки у професійній підготовці інженерів-програмістів, як в Україні, так і за її кордоном. Це допоможе виявити прогалини в існуючих програмах

підготовки та розробити рекомендації щодо їхнього удосконалення.

Для досягнення мети дослідження використано комплекс різних теоретичних методів, що дають змогу всебічно оцінити існуючий досвід методичного забезпечення кібербезпеки у професійній підготовці майбутніх інженерів-програмістів як в Україні, так і за її кордоном. Основні методи дослідження містять аналіз наукових джерел для систематизації знань про методичне забезпечення кібербезпеки, синтез отриманих даних для формування цілісного уявлення про його стан у різних країнах та порівняльний аналіз методичних підходів вітчизняних та іноземних навчальних закладів для визначення їхньої ефективності та можливостей адаптації до національних умов.

Аналіз останніх досліджень і публікацій. Останні дослідження і публікації з проблеми кібернетичної безпеки свідчать про зростаючий інтерес науковців та освітян до питання забезпечення належного рівня підготовки фахівців у цій сфері. Зокрема, роботи таких вітчизняних дослідників як Л. Арсенович (2022), С. Горліченко (2023), О. Жмурко, (2023) зосереджуються на аналізі поточного стану методичного забезпечення у навчальних закладах України, що готують інженерів-програмістів. Дослідження підкреслюють недостатній рівень теоретичних і практичних знань студентів у галузі кібербезпеки, що викликає занепокоєння з боку роботодавців.

Іноземний досвід, представлений у роботах М. Agbeko (2021), S. Edwards (2021), Н. Барченко, В. Любчак, Т. Лаврик (2022) показує більш розвинені системи підготовки фахівців з кібербезпеки. Наприклад, у Сполучених Штатах Америки та країнах Європейського Союзу широко використовуються комплексні підходи до навчання, що включають як теоретичну підготовку, так і практичні заняття в умовах, наближених до реальних. Ці дослідження наголошують на важливості інтеграції сучасних технологій, таких як віртуальні лабораторії та платформи для симуляцій, у навчальний процес.

Важливим аспектом є також підготовка викладачів, які повинні володіти сучасними знаннями та навичками для ефективного навчання кібербезпеки. У дослідженнях В. Коваленко & Т. Осипчук, (2024) та О. Таволжанського (2018) обговорюються програми підвищення кваліфікації для викладачів, що працюють у сфері інформаційних технологій.

На основі аналізу вітчизняного та іноземного досвіду можна зробити висновок про необхідність удосконалення методичного

забезпечення підготовки майбутніх інженерів-програмістів у сфері кібербезпеки. Це включає адаптацію кращих світових практик до національної системи освіти, розробку нових навчальних програм та матеріалів, а також створення умов для постійного професійного розвитку викладачів.

Таким чином, результати досліджень свідчать про актуальність та необхідність подальших досліджень у цій сфері, що дозволить забезпечити високий рівень підготовки фахівців, здатних ефективно реагувати на сучасні виклики кібербезпеки.

Формулювання цілей статті. Метою даного дослідження є аналіз вітчизняного та іноземного досвіду методичного забезпечення з кібернетичної безпеки у професійній підготовці майбутніх інженерів-програмістів, визначення ефективних методичних підходів та формування рекомендацій щодо їхнього впровадження у національну систему освіти.

Основні завдання статті: 1) вивчення та систематизація наукових досліджень, публікацій і навчальних матеріалів, що стосуються методичного забезпечення з кібернетичної безпеки у професійній підготовці майбутніх інженерів-програмістів як в Україні так і за кордоном; 2) проведення порівняльного аналізу вітчизняного та іноземного досвіду методичного забезпечення з кібернетичної безпеки; 3) запропонування рекомендацій щодо покращення методичного забезпечення кібербезпеки у професійній підготовці майбутніх інженерів-програмістів в Україні на основі отриманих результатів та з урахуванням міжнародного досвіду.

Виклад основного матеріалу дослідження. Кібернетична безпека є критично важливим аспектом професійної підготовки майбутніх інженерів-програмістів. У зв'язку зі зростанням кількості кіберзагроз та складністю інформаційних систем, необхідність якісного методичного забезпечення кібербезпеки стає надзвичайно актуальною (Биков et al., 2020). Розглянемо вітчизняний та іноземний досвід методичного забезпечення кібербезпеки, охоплюючи такі аспекти: стандарти та нормативні документи, що визначають вимоги до навчальних програм та кваліфікаційних характеристик випускників; огляд навчальних програм, що охоплюють як базові, так і спеціалізовані курси з кібербезпеки; методичні підходи до викладання, що варіюються від традиційних лекцій до інтерактивних методів, симуляцій та віртуальних лабораторій; використання інформаційно-комунікаційних технологій (ІКТ) у навчальному процесі, зокрема, платформ для управління навчанням, онлайн-

ресурсів та мультимедійних матеріалів; професійний розвиток викладачів у сфері кібербезпеки, що містить курси підвищення кваліфікації, участь у міжнародних заходах, співпрацю з промисловістю та використання сучасних онлайн-ресурсів.

1. *Стандарти та нормативні документи.* В Україні підготовка фахівців з кібернетичної безпеки регулюється комплексом державних стандартів освіти, які визначають основні вимоги до змісту навчальних програм та кваліфікаційних характеристик випускників. Ці стандарти є обов'язковими для виконання всіма вищими навчальними закладами, які здійснюють підготовку фахівців у цій галузі. Основним нормативним актом є Закон України «Про основні засади забезпечення кібербезпеки України», що встановлює правові та організаційні засади забезпечення кібербезпеки, визначає принципи, завдання та напрями державної політики у цій сфері, а також повноваження органів державної влади. Закон акцентує увагу на необхідності підготовки кваліфікованих кадрів, які відповідають сучасним викликам та загрозам. Державні стандарти вищої освіти містять вимоги до підготовки фахівців з кібербезпеки на рівні бакалаврату, магістратури та докторантури, зокрема зміст навчальних програм, перелік обов'язкових та вибіркових дисциплін, кваліфікаційні характеристики випускників та методичні рекомендації щодо організації навчального процесу. Інші нормативні акти, такі як накази Міністерства освіти і науки України, регулюють питання ліцензування та акредитації освітніх програм, розробки нових навчальних планів та внесення змін до існуючих програм, а стандарти професійної освіти визначають вимоги до кваліфікаційних характеристик та компетенцій фахівців з кібербезпеки на різних рівнях професійної підготовки (Азюковський et al., 2023).

Провідні університети світу дотримуються міжнародних стандартів та нормативних документів у галузі кібербезпеки, що забезпечує високий рівень підготовки фахівців. Серед основних міжнародних стандартів та нормативних документів, що використовуються в освітніх програмах, можна виокремити ISO/IEC 27001 та NIST Cybersecurity Framework. ISO/IEC 27001 є міжнародним стандартом для систем управління інформаційною безпекою (ISMS), що визначає вимоги до встановлення, впровадження, підтримки та постійного покращення системи управління інформаційною безпекою в контексті організаційних ризиків, включаючи оцінку та управління ризиками, розробку політик та процедур, моніторинг та аудит, а також навчання

та підвищення обізнаності співробітників. NIST Cybersecurity Framework, розроблений Національним інститутом стандартів і технологій США (NIST), надає систематичний підхід до управління кібербезпекою та містить компоненти ідентифікації активів, захисту від кіберзагроз, виявлення кіберінцидентів, реагування на них та відновлення систем та послуг після кіберінциденту (Catal et al., 2023).

Отже, порівняльний аналіз вітчизняних та міжнародних стандартів кібербезпеки показує, що вітчизняні стандарти визначають загальні вимоги до змісту навчальних програм та кваліфікаційних характеристик випускників, регулюються державними нормативно-правовими актами та акцентують увагу на базових аспектах кібербезпеки. У той же час міжнародні стандарти забезпечують системний підхід до управління кібербезпекою на основі визнаних моделей та рамок, включають детальні вимоги до оцінки та управління ризиками, розробки політик безпеки, моніторингу та реагування на інциденти, а також встановлюють високі стандарти захисту персональних даних та сертифікації професійних знань. Для підвищення якості підготовки фахівців з кібербезпеки в українських університетах рекомендується інтеграція міжнародних стандартів у навчальні програми, включаючи курси, що охоплюють теоретичні та практичні аспекти міжнародних стандартів ISO/IEC 27001 та NIST Cybersecurity Framework і підготовку студентів до міжнародних сертифікацій у галузі кібербезпеки. Також важливо підвищити рівень співпраці з міжнародними організаціями та університетами з обміну досвідом і найкращими практиками, участь у міжнародних проектах та програмах з кібербезпеки, а також оновлення нормативно-правової бази з урахуванням сучасних вимог та викликів у сфері кібербезпеки. Інтеграція міжнародних стандартів та передових практик до національної системи освіти дозволить підвищити якість підготовки фахівців з кібербезпеки та забезпечити їхню конкурентоспроможність на міжнародному ринку праці.

2. *Огляд навчальних програм.* Більшість українських університетів пропонують курси з кібернетичної безпеки у рамках програм з комп'ютерних наук та інженерії. Ці програми, як правило, містять базові курси, що охоплюють основні аспекти кібербезпеки, такі як введення в кібербезпеку, поняття та визначення, історія розвитку, основні принципи та концепції, типи кіберзагроз та методи їхнього запобігання; мережева безпека, що охоплює основи захисту мережевої інфраструктури, протоколи безпеки мереж (SSL/TLS, IPsec), технології

міжмережевих екранів та систем виявлення вторгнень (IDS); криптографія, включаючи симетричне та асиметричне шифрування, криптографічні алгоритми (AES, RSA, ECC), застосування криптографії (цифрові підписи, сертифікація, керування ключами); безпека програмного забезпечення, що охоплює вразливості програмного забезпечення, методи та інструменти захисту, принципи та практики безпечного програмування. Водночас, спеціалізовані курси, такі як аналіз загроз та реагування на інциденти, зустрічаються рідко. Це обмежує можливості студентів у отриманні поглиблених знань та практичних навичок, необхідних для ефективної роботи у сфері кібербезпеки. Спеціалізовані курси, які іноді пропонуються, включають аналіз загроз, що охоплює методи та інструменти аналізу, ідентифікацію та класифікацію кіберзагроз, розробку стратегій захисту; реагування на інциденти, що охоплює процеси виявлення, аналізу, реагування та відновлення, інструменти та техніки для реагування, розробки та тестування планів реагування; управління ризиками, що охоплює оцінку ризиків, розробку та впровадження програм управління ризиками, моніторинг та аналіз; правові аспекти кібербезпеки, що охоплюють міжнародні та національні нормативно-правові акти, питання конфіденційності та захисту даних, етичні аспекти кібербезпеки (Биков et al., 2020).

Навчальні програми з кібербезпеки у провідних університетах світу, таких як Массачусетський технологічний інститут (MIT), Стенфордський університет та Університет Карнегі-Меллона, відрізняються своєю глибиною та широтою, включаючи як теоретичні, так і практичні курси, що дозволяють студентам отримати всебічні знання та навички, необхідні для ефективної роботи у сфері кібербезпеки. Програми MIT та Стенфордського університета охоплюють основи кібербезпеки (історія, основні поняття, класифікація кіберзагроз), мережеву безпеку (протоколи та архітектури, методи захисту мереж), криптографію (симетричне та асиметричне шифрування), а також спеціалізовані курси з аналізу загроз та реагування на інциденти, етичного хакерства і правових аспектів кібербезпеки. Університет Карнегі-Меллона включає в свої програми основи кібербезпеки, мережеву безпеку, криптографію, а також спеціалізовані курси щодо аналізу загроз, реагування на інциденти, етичного хакерства та правових аспектів кібербезпеки (Knott et al., 2023).

Порівняльний аналіз навчальних програм з кібербезпеки показує, що вітчизняні програми наголошують на базових аспектах з обмеженою

кількістю спеціалізованих курсів, зосереджуючись на теоретичних знаннях при недостатній кількості практичних занять та обмеженому використанні сучасних методів навчання через брак ресурсів. Закордонні програми є більш різноманітними та глибокими, охоплюючи широкий спектр тем з великою увагою до практичних занять, лабораторних робіт та симуляцій, а також використанням сучасних методів навчання, таких як інтерактивні методи, віртуальні лабораторії та симулятори. Для покращення навчальних програм з кібербезпеки рекомендується розширення навчальних програм шляхом інтеграції нових спеціалізованих курсів, таких як аналіз загроз, реагування на інциденти, моральне хакерство та правові аспекти кібербезпеки, а також використання міжнародних стандартів та професійних сертифікацій; підвищення практичної підготовки шляхом збільшення кількості лабораторних робіт та практичних занять з використанням сучасного обладнання та програмного забезпечення, створення віртуальних лабораторій та симуляторів для моделювання реальних кіберзагроз та інцидентів; використання сучасних методів навчання, включаючи інтерактивні методи, такі як групові обговорення, кейс-стади, рольові ігри та проектна робота, а також онлайн-курси, віртуальні лабораторії та мультимедійні матеріали для підвищення якості навчання. Інтеграція цих рекомендацій сприятиме підвищенню якості підготовки фахівців з кібербезпеки та забезпечить їхню конкурентоспроможність на міжнародному ринку праці.

3. Методичні підходи до викладання. У більшості вітчизняних університетів викладання курсів кібербезпеки базується на традиційному лекційному форматі, де лекції є основним методом передачі теоретичних знань, а студенти пасивно сприймають матеріал. Викладачі проводять лекції, використовуючи попередньо підготовлені конспекти чи презентації, а основним джерелом інформації для студентів є друковані підручники та конспекти лекцій, які часто застарівають через швидкий розвиток технологій. Оцінка знань студентів проводиться через письмові іспити та заліки, які не завжди адекватно оцінюють їхні практичні навички та критичне мислення. Викладання кібербезпеки часто страждає від недостатнього використання інтерактивних методів та інформаційно-комунікаційних технологій (ІКТ) через недостатню технічну оснащеність, обмежений доступ до сучасних онлайн-ресурсів та відсутність інтерактивних занять. Практичні заняття з кібербезпеки обмежені через недостатню кількість годин у навчальних

програмах, обмежені ресурси університетів, включаючи фінансові обмеження та нестачу сучасного обладнання та програмного забезпечення. Основними навчальними матеріалами залишаються друковані підручники та конспекти лекцій, що призводить до застарілої інформації, відсутності інтерактивності та обмеженої доступності для всіх студентів (Єгора & Пономарець, 2023).

У зарубіжних університетах активно використовуються сучасні методичні підходи до викладання кібербезпеки, що сприяє глибшому засвоєнню матеріалу студентами та розвитку їхніх практичних навичок. Ці підходи включають інтерактивні методи навчання, симуляції, віртуальні лабораторії та проблемно-орієнтоване навчання (PBL). Викладачі заохочують студентів до активної участі у групових обговореннях та дискусіях, що допомагає краще розуміти матеріал, розвивати критичне мислення та здатність аргументувати свої точки зору. Рольові ігри та симуляції, де студенти виконують ролі різних фахівців з кібербезпеки, допомагають їм розвивати практичні навички та командну роботу. Використання віртуальних лабораторій дозволяє студентам проводити лабораторні роботи у віртуальному середовищі, що імітує реальні інформаційні системи та мережі, а мультимедійні ресурси, такі як відеолекції, інтерактивні презентації та анімації, роблять навчальний процес більш цікавим та доступним. Проблемно-орієнтоване навчання (PBL) передбачає виконання студентами проектів, що ґрунтуються на реальних проблемах кібербезпеки, та аналіз реальних кейсів, що сприяє розвитку навичок дослідження, планування, реалізації рішень та колективної роботи. Викладачі інтегрують у навчальний процес масові відкриті онлайн-курси (MOOCs) з провідними платформами, такими як Coursera, edX та Udacity, що дозволяє студентам отримувати доступ до якісних навчальних матеріалів від найкращих університетів та експертів у всьому світі. Використання платформ для дистанційного навчання, таких як Moodle, Canvas та Blackboard, дозволяє організувати навчальний процес онлайн, забезпечуючи доступ до навчальних матеріалів, завдань, тестів та інтерактивних занять, що сприяє гнучкості навчання. Переваги сучасних методичних підходів включають практичну орієнтованість, що забезпечує студентам можливість отримати практичні навички, інтерактивність та залученість, що підвищують мотивацію та зацікавленість у вивченні кібербезпеки, а також доступ до сучасних ресурсів, що сприяє поглибленню знань та розширенню кругозору (Северина et al., 2023).

Порівняльний аналіз методичних підходів у сфері кібербезпеки показує, що в Україні основний акцент робиться на традиційних лекціях з обмеженим використанням інтерактивних та інноваційних методів, недостатньою кількістю практичних занять та лабораторних робіт, а також обмеженим використанням ІКТ через недостатню технічну оснащеність. Закордонні університети активно використовують інтерактивні методи, такі як групові обговорення, рольові ігри та симуляції, приділяють велику увагу практичним заняттям, віртуальним лабораторіям та мультимедійним ресурсам, впроваджують проблемно-орієнтоване навчання (PBL) з акцентом на проектну роботу та аналіз реальних кейсів, а також широко використовують сучасні онлайн-ресурси та платформи для дистанційного навчання. Для покращення методичних підходів до викладання кібербезпеки в українських університетах рекомендується розширити використання інтерактивних методів навчання, включивши групові обговорення, кейс-стаді, рольові ігри та проектну роботу, залучати студентів до активної участі у навчальному процесі для розвитку критичного мислення та комунікативних навичок, збільшити кількість практичних занять, забезпечити університети сучасним обладнанням та програмним забезпеченням для проведення лабораторних робіт, використовувати віртуальні лабораторії та симулятори для моделювання реальних кіберзагроз та інцидентів, інтегрувати сучасні онлайн-ресурси, використовуючи масові відкриті онлайн-курси (MOOCs) для доповнення навчальних програм та забезпечення доступу до якісних навчальних матеріалів, використовувати платформи для дистанційного навчання для організації онлайн-курсів, вебінарів та інтерактивних занять, підвищити рівень професійного розвитку викладачів через організацію курсів підвищення кваліфікації, стажування та програми обміну, залучати викладачів до міжнародних конференцій, семінарів та тренінгів для ознайомлення з найновішими методами навчання та технологіями у сфері кібербезпеки. Інтеграція цих рекомендацій сприятиме підвищенню якості підготовки фахівців з кібербезпеки та забезпечить їхню конкурентоспроможність на міжнародному ринку праці.

4. Використання інформаційно-комунікаційних технологій (ІКТ) у навчальному процесі. Використання інформаційно-комунікаційних технологій (ІКТ) у навчальному процесі є важливою складовою сучасної освіти, особливо у сфері кібербезпеки, проте в українських університетах це часто обмежується через недостатню технічну оснащеність. Основні

проблеми включають застаріле обладнання, брак ресурсів, недостатню кількість комп'ютерних класів та лабораторій, що ускладнює проведення практичних занять та лабораторних робіт. Деякі університети використовують платформи для управління навчанням (LMS), такі як Moodle, Canvas, Blackboard, що допомагають організувати навчальний процес, забезпечують дистанційне навчання та моніторинг успішності студентів, але загальний рівень впровадження LMS залишається низьким через відсутність технічної підтримки, недостатні навички викладачів та студентів, а також відсутність інтеграції з іншими інформаційними системами університетів. Використання онлайн-ресурсів, таких як відкриті освітні ресурси (OER) та масові відкриті онлайн-курси (MOOCs), також обмежене через відсутність доступу до якісних ресурсів, низьку якість Інтернет-з'єднання та недостатню мотивацію і підтримку викладачів та студентів. Для покращення використання ІКТ у навчальному процесі необхідно оновити технічну базу університетів, забезпечити тренінги для викладачів та студентів, інтегрувати ІКТ у навчальні програми та забезпечити підтримку з боку керівництва університетів для впровадження ІКТ у навчальний процес (Лузан et al., 2018).

У провідних університетах світу інформаційно-комунікаційні та інноваційні технології широко використовуються для покращення якості навчального процесу та підвищення підготовки студентів. Ці університети впроваджують різні технологічні рішення, що сприяють інтерактивному навчанню, доступу до сучасних навчальних ресурсів та розвитку практичних навичок. Використання спеціалізованих програмних платформ, таких як Moodle, Canvas та Blackboard допомагає організувати навчальний процес, провести тестування, організувати дискусії та моніторити прогрес студентів. Віртуальні лабораторії та симулятори, такі як NetLab, Packet Tracer та Cyber Range дозволяють студентам виконувати лабораторні роботи у віртуальному середовищі, моделюючи реальні мережеві сценарії та виявлення вразливостей. Онлайн-платформи, такі як Coursera, edX, Udacity та Khan Academy, пропонують масові відкриті онлайн-курси (MOOCs) від провідних університетів та організацій, що дозволяє студентам проходити курси з кібербезпеки, отримувати сертифікати та доступ до матеріалів світового рівня. Мультимедійні ресурси, включаючи YouTube, подкасти та вебінари, використовуються для наочного пояснення складних концепцій та демонстрації практичних завдань. Використання передових технологій, таких як віртуальна

реальність (VR) та доповнена реальність (AR), створює інтерактивні навчальні середовища, де студенти можуть моделювати реальні ситуації та тренувати свої навички в умовах максимально наближених до реальних. Переваги використання ІКТ та інноваційних технологій включають підвищення доступності навчання, розвиток практичних навичок, інтерактивність і залученість студентів, а також забезпечення актуальності знань. Завдяки використанню онлайн-платформ та ресурсів, студенти мають можливість навчатися у будь-який час та з будь-якого місця, що підвищує гнучкість навчального процесу та сприяє самоосвіті. Віртуальні лабораторії та симулятори дозволяють студентам відпрацьовувати практичні завдання та сценарії у безпечному середовищі, що сприяє кращому засвоєнню матеріалу та підготовці до реальних викликів, а використання VR, AR та інших передових технологій робить навчальний процес більш інтерактивним та цікавим, підвищуючи залучення студентів та їхню мотивацію до навчання (Knott et al., 2023).

Для підвищення якості використання ІКТ у навчальному процесі рекомендується підвищити технічну оснащеність навчальних закладів шляхом забезпечення сучасним обладнанням та швидкісним інтернетом, а також інвестувати в оновлення технічної бази університетів, включаючи комп'ютери, мультимедійні засоби та програмне забезпечення; організувати курси підвищення кваліфікації для викладачів з використання ІКТ у навчальному процесі та заохочувати їх до участі у міжнародних конференціях, семінарах та вебінарах для ознайомлення з новітніми технологіями і методиками; використовувати масові відкриті онлайн-курси (MOOCs) для доповнення навчальних програм та забезпечення доступу до якісних навчальних матеріалів, а також платформи для дистанційного навчання для організації онлайн-курсів, вебінарів та інтерактивних занять; створювати та впроваджувати віртуальні лабораторії й симулятори для моделювання реальних кіберзагроз та інцидентів, використовуючи VR та AR технології для створення інтерактивних середовищ і наочного пояснення складних концепцій. Інтеграція цих рекомендацій сприятиме підвищенню якості навчання, розвитку практичних навичок у студентів та забезпечить їхню конкурентоспроможність на міжнародному ринку праці.

5. Професійний розвиток викладачів у сфері кібербезпеки. Професійний розвиток викладачів є ключовим фактором забезпечення високої якості освіти у сфері кібербезпеки. В українських університетах цей процес часто обмежується

внутрішніми тренінгами та семінарами, що має переваги й недоліки. Переваги внутрішніх тренінгів та семінарів включають доступність і контекстуальну релевантність, адже такі заходи легко організувати і вони розробляються з урахуванням специфіки конкретного навчального закладу. Недоліками є обмежений доступ до нових знань та мінімальна взаємодія із зовнішніми фахівцями. Співпраця з промисловістю, що допомагає викладачам залишатися в курсі новітніх розробок, технологій та практик, має переваги у вигляді актуалізації знань й отримання реального практичного досвіду. Однак організаційні складнощі та ризик комерційного впливу можуть бути значними недоліками. Інші методи професійного розвитку містять участь у міжнародних конференціях та семінарах, що дозволяє викладачам дізнатися про найновіші досягнення у сфері кібербезпеки, але потребує значних фінансових витрат та часу на поїздки; онлайн-курси та вебінари, що дають можливість навчатися у зручний час, але можуть мати варіативну якість та глибину; а також стажування за програмами обміну, які забезпечують практичний досвід і нові знання, але організація таких програм може бути складною та потребувати значних ресурсів (Азюковський et al., 2023).

У провідних університетах світу професійний розвиток викладачів – один із ключових елементів забезпечення високої якості освіти. Викладачі регулярно проходять курси підвищення кваліфікації, беруть участь у міжнародних конференціях, семінарах та тренінгах, а також активно співпрацюють із провідними компаніями у сфері кібербезпеки, що дозволяє їм залишатися в курсі новітніх розробок і технологій. Курси підвищення кваліфікації включають спеціалізовані курси та сертифікаційні програми, такі як Certified Information Systems Security Professional (CISSP) та Certified Information Security Manager (CISM), а також внутрішні тренінги та семінари, де розглядаються новітні методики викладання та сучасні технології в галузі кібербезпеки. Участь у міжнародних заходах, таких як конференції Black Hat, DEF CON, RSA Conference, семінари та воркшопи, дозволяє викладачам ознайомлюватися з передовими практиками, налагоджувати міжнародні контакти та обмінюватися досвідом із колегами з усього світу (Edwards, 2021). Співпраця з провідними компаніями включає індустріальні стажування, які допомагають отримати практичний досвід, та спільні дослідницькі проекти, що сприяють обміну знаннями між академічним та індустріальним співтовариствами. Використання сучасних онлайн-ресурсів, таких як масові

відкриті онлайн-курси (MOOCs) на платформах Coursera, edX, Udacity, а також участь у вебінарах та онлайн-семінарах дозволяє викладачам отримувати доступ до якісних навчальних матеріалів, залишатися в курсі останніх тенденцій та інтегрувати новітні знання у навчальному процесі (Agbeko, 2021).

Для підвищення професійного розвитку викладачів кібербезпеки в Україні рекомендується організовувати регулярні курси підвищення кваліфікації з акцентом на сучасні технології та методики викладання кібербезпеки; налагоджувати співпрацю з промисловістю для розвитку партнерських відносин із провідними компаніями у сфері кібербезпеки для організації спільних проектів, стажувань та тренінгів для викладачів; забезпечувати фінансову підтримку для участі викладачів у міжнародних конференціях, семінарах та тренінгах для ознайомлення з новітніми досягненнями та найкращими практиками; заохочувати викладачів до використання масових відкритих онлайн-курсів (MOOCs) та інших онлайн-ресурсів для підвищення кваліфікації та оновлення знань; організовувати програми міжнародного обміну та стажувань для викладачів у провідних університетах та за кордоном. Інтеграція цих рекомендацій сприятиме підвищенню рівня професійного розвитку викладачів та забезпеченню високої якості освіти у сфері кібербезпеки в Україні.

Висновки. Аналіз вітчизняного та іноземного досвіду методичного забезпечення кібернетичної безпеки у професійній підготовці майбутніх інженерів-програмістів дозволяє зробити кілька ключових висновків. По-перше, вітчизняні стандарти та нормативні документи потребують оновлення та адаптації до сучасних міжнародних вимог, щоб забезпечити належний рівень підготовки фахівців. По-друге, навчальні програми в українських університетах часто обмежуються базовими аспектами кібербезпеки та мають недостатню кількість спеціалізованих курсів та практичних занять. По-третє, методичні підходи до викладання в Україні переважно традиційні з обмеженим використанням інтерактивних методів та ІКТ, що знижує ефективність навчального процесу. Порівняння із закордонним досвідом показує, що провідні університети світу активно використовують інноваційні методи навчання, віртуальні лабораторії, симуляції та проблемно-орієнтоване навчання (PBL), що сприяє глибшому засвоєнню матеріалу та розвитку практичних навичок. Викладачі у зарубіжних університетах проходять регулярне підвищення кваліфікації, беруть участь у міжнародних заходах та співпрацюють із промисловістю, що забезпечує актуалізацію

знань та практичних навичок. Рекомендується інтегрувати ці підходи в українську систему освіти, оновити технічну базу навчальних закладів, запровадити сучасні методи навчання та

забезпечити професійний розвиток викладачів для підвищення якості підготовки фахівців із кібербезпеки.

Список використаних джерел

- Азюковський, О., Павличенко, А., Пашенко, О., & Медведовська, Т. (2023). Щодо питання кваліфікаційних центрів для фахівців кібербезпеки: виклики часу, роль та значення. *Collection of Scientific Papers «ΛΟΓΟΣ»*, (June 23, 2023; Oxford, UK), 225–230. URL: <https://doi.org/10.36074/logos-23.06.2023.62>
- Арсенович, Л.А. (2022). Подальший розвиток системи професійного навчання фахівців із кібербезпеки в умовах розвитку цифрових технологій. *Таврійський науковий вісник. Серія: Публічне управління та адміністрування*, 3, 3–13. URL: <https://doi.org/10.32782/pma2663-5240-2023.33.6>
- Барченко, Н.Л., Любчак, В.О., & Лаврик, Т.В. (2022). Модель індикаторів оцінки національного рівня цифровізації та кібербезпеки держав світу. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2 (18), 73–85. URL: <https://doi.org/10.28925/2663-4023.2022.18.7385>
- Биков, В.Ю., Романовський, А.А., & Романовська, Ю.Ю. (2020). Навчання кібербезпеки і кіберзахисту фахівців з управління фінансами, економікою і бізнесом. *Інформаційні технології і засоби навчання*, 80 (6), 386–413. URL: <https://doi.org/10.33407/itlt.v80i6.4101>
- Горліченко, С. (2023). Міжнародний підхід до підготовки фахівців у сфері кібербезпеки. *Scientific Collection «InterConf»*, 170, 42–46.
- Єгорова, Ю., Пономарець, Г. (2023). Критичне мислення вчителів та здобувачів Нової української школи. *Науковий вісник Мелітопольського державного педагогічного університету. Серія: Педагогіка*, 1 (30), 111–115. URL: <https://doi.org/10.33842/22195203-2023-30-111-115>
- Жмурко, О.В. (2023). Формування культури безпеки майбутніх фахівців з цифрових технологій як наукова проблема. *Педагогіка безпеки*, 8 (1–2), 51–56. URL: <https://doi.org/10.31649/2524-1079-2023-8-1-051-056>
- Коваленко, В., & Осипчук, Т. (2024). Проблема розвитку цифрової компетентності з кібербезпеки вчителів закладів загальної середньої освіти. *Фізико-математична освіта*, 39 (2), 35–41. URL: <https://doi.org/10.31110/fmo2024.v39i2-05>
- Лузан, П.Г., Пашенко, Т.М., Ваніна, Н.М., & Колісник, Н.В. (2018). Стандартизація професійної освіти на основі компетентнісного підходу. *ScienceRise*, 5 (25), 32–35.
- Северина, Л., Здорівець, О., & Беляєва, О. (2023). Трансформація освіти. *Педагогічні науки та освіта*, 76–83.
- Таволжанський, О.В. (2018). Особливості забезпечення кібербезпеки у сучасному світі: огляд суб'єктів запобігання кіберзлочинності. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія: Право*, (6), 154–163.
- Agbeko, M. (2021). Understanding cyber safety behavior among teenagers in Ghana. *International Journal of Computer Science and Information Security (IJCSIS)*, 19 (6). <https://doi.org/10.5281/zenodo.5111963> [in English]
- Edwards, S. (2021). Cyber-safety and COVID-19 in the early years: A research agenda. *Journal of Early Childhood Research*, 19 (3), 396–410. <https://doi.org/10.1177/1476718X211014908> [in English]
- Catal, C., Ozcan, A., Donmez, E., & Kasif, A. (2023). Analysis of cyber security knowledge gaps based on cyber security body of knowledge. *Education and Information Technologies*, 28 (2), 1809–1831. <https://doi.org/10.1007/s10639-022-11261-8> [in English]

References

- Agbeko, M. (2021). Understanding cyber safety behavior among teenagers in Ghana. *International Journal of Computer Science and Information Security (IJCSIS)*, 19 (6). <https://doi.org/10.5281/zenodo.5111963> [in English]
- Arsenovych, L.A. (2022). Further development of the system of professional training of cyber security specialists in the conditions of the development of digital technologies. *Taurian Scientific Herald. Series: Public management and administration*, 3, 3–13. <https://doi.org/10.32782/pma2663-5240-2023.33.6> [in Ukrainian]
- Aziukovsky, O., Pavlychenko, A., Pashchenko, O., & Medvedovska, T. (2023). Regarding the issue of qualification centers for cyber security specialists: challenges of time, role and importance. *Collection of Scientific Papers «ΛΟΓΟΣ»*, (June 23, 2023; Oxford, UK), 225–230. <https://doi.org/10.36074/logos-23.06.2023.62> [in Ukrainian]
- Barchenko, N.L., Liubchak, V.O., Lavryk, T.V. (2022). A model of indicators for assessing the national level of digitalization and cyber security of the countries of the world. *Electronic professional scientific publication "Cybersecurity: education, science, technology"*, 2 (18), 73–85. <https://doi.org/10.28925/2663-4023.2022.18.7385> [in Ukrainian]
- Bykov, V.Yu., Romanovsky, A.A., & Romanovska, Yu. Yu. (2020). Cyber security and cyber protection training for financial, economic and business management specialists. *Information technologies and teaching aids*, 80 (6), 386–413. <https://doi.org/10.33407/itlt.v80i6.4101> [in Ukrainian]
- Catal, C., Ozcan, A., Donmez, E., & Kasif, A. (2023). Analysis of cyber security knowledge gaps based on cyber security body of knowledge. *Education and Information Technologies*, 28 (2), 1809–1831. <https://doi.org/10.1007/s10639-022-11261-8> [in English]
- Edwards, S. (2021). Cyber-safety and COVID-19 in the early years: A research agenda. *Journal of Early Childhood Research*, 19 (3), 396–410. <https://doi.org/10.1177/1476718X211014908> [in English]
- Horlichenko, S. (2023). An international approach to the training of specialists in the field of cyber security. *Scientific Collection "InterConf"*, 170, 42–46. [in Ukrainian]
- Knott, J., Yuan, H., Boakes, M., & Li, S. (2023, March). Cyber Security and Online Safety Education for Schools in the UK: Looking through the Lens of Twitter Data. In *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing* (pp. 1603–1606). ACM, New York, USA <https://doi.org/10.1145/3555776.3577805> [in English]
- Kovalenko, V., & Osypchuk, T. (2024). The problem of developing digital competence in cyber security of teachers of general secondary education institutions. *Physical and mathematical education*, 39 (2), 35–41. <https://doi.org/10.31110/fmo2024.v39i2-05> [in Ukrainian]
- Luzan, P.G., Pashchenko, T.M., Vanina, N.M., & Kolisnyk, N.V. (2018). Standardization of professional education based on the competence approach. *ScienceRise*, 5 (25), 32–35. [in Ukrainian]
- Severina, L., Zdorovets, O., & Beliaeva, O. (2023). Digital transformation of education. *Pedagogical sciences and education*, 76–83. [in Ukrainian]

Technologies, 28 (2), 1809-1831.
<https://doi.org/10.1007/s10639-022-11261-8>
 Knott, J., Yuan, H., Boakes, M., & Li, S. (2023, March). Cyber Security and Online Safety Education for Schools in the UK: Looking through the Lens of Twitter Data. In *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing* (pp. 1603-1606). ACM, New York, USA
<https://doi.org/10.1145/3555776.3577805>

Tavolzhansky, O.V. (2018). Peculiarities of ensuring cyber security in the modern world: an overview of cybercrime prevention subjects. *Scientific and information bulletin of the Ivano-Frankivsk University of Law named after King Danylo Halytskyi. Series: Law*, 6, 154-163. [in Ukrainian]
 Yehorova, Yu., Ponomarets, G. (2023). Critical thinking of teachers and students of the New Ukrainian School. *Scientific Bulletin of Melitopol State Pedagogical University. Series: Pedagogy*, 1 (30), 111-115.
<https://doi.org/10.33842/22195203-2023-30-111-115> [in Ukrainian]
 Zhmurko, O.V. (2023). Formation of security culture of future specialists in digital technologies as a scientific problem. *Safety Pedagogy*, 8 (1-2), 51-56.
<https://doi.org/10.31649/2524-1079-2023-8-1-051-056> [in Ukrainian]

Відомості про авторів:

Комарницький Кирило Сергійович

kyrylo_komarnytskyi@mdpu.org.ua

Мелітопольський державний педагогічний
 університет імені Богдана Хмельницького
 Наукове Містечко, вулиця, 59, Запоріжжя,
 Запорізька обл., 69000, Україна

Чорна Альона Віталіївна

chornaa@mdpu.org.ua

Мелітопольський державний педагогічний
 університет імені Богдана Хмельницького
 Наукове Містечко, вулиця, 59, Запоріжжя,
 Запорізька обл., 69000, Україна

doi: 10.33842/22195203-2024-2-33-52-60

*Матеріал надійшов до редакції 05. 09. 2024 р.
 Прийнято до друку 25. 09. 2024 р.*

Information about the authors:

Komarnytsky Kyrylo Serhiiovych

kyrylo_komarnytskyi@mdpu.org.ua

Bohdan Khmelnytsky Melitopol
 State Pedagogical University
 Scientific Town, Street 59, Zaporizhzhia,
 Zaporizhzhia region, 69000, Ukraine

Chorna Alona Vitaliivna

chornaa@mdpu.org.ua

Bohdan Khmelnytsky Melitopol
 State Pedagogical University
 Scientific Town, Street 59, Zaporizhzhia,
 Zaporizhzhia region, 69000, Ukraine

doi: 10.33842/22195203-2024-2-33-52-60

*Received at the editorial office 05. 09. 2024.
 Accepted for publishing 25. 09. 2024.*