ПЕДАГОГІЧНА АКАДЕМІЯ:
НАУКОВІ ЗАПИСКИ

ТЕОРІЯ І МЕТОДИКА ПРОФЕСІЙНОЇ ОСВІТИ

УДК 004.056.5:621.396.7

DOI https://doi.org/10.5281/zenodo.14723771

Формування професійних компетентностей фахівців для забезпечення інформаційної безпеки в радіотелекомунікаційних системах

Магілевський Владислав Віталійович,
аспірант кафедри професійної підготовки, документознавства та публічного управління Українського державного університету імені Михайла Драгоманова, 01601, м. Київ, вул. Пирогова 9, Україна,
vlad.mahilevskyi@icloud.com
ORCID https://orcid.org/0009-0006-1056-0310

Прийнято: 04.01.2025 | Опубліковано: 23.01.2025

Анотація: *Актуальність дослідження зумовлена необхідністю підвищення ефективності підготовки фахівців для забезпечення інформаційної безпеки в радіотелекомунікаційних системах, що пов'язано зі зростанням кількості та складності сучасних кіберзагроз. Це потребує впровадження освітніх програм, у яких передбачено формування професійних компетентностей для захисту інформаційних ресурсів і забезпечення інформаційної стійкості.* ***Мета*** *роботи полягає у визначенні основних аспектів формування професійних компетентностей фахівців з інформаційної безпеки та розробленні науково обґрунтованих рекомендацій щодо вдосконалення освітніх програм у сфері радіотелекомунікаційних систем. У статті використано* ***методи*** *аналізу наукових джерел, порівняння освітніх програм*

провідних закладів освіти та оцінювання технічних проблем підготовки здобувачів освіти у сфері інформаційної безпеки. У ***результатах*** *дослідження встановлено, що сучасні освітні програми містять фундаментальні дисципліни, проте недостатньо охоплюють практичні модулі з тестування на проникнення, аналізу мережевого трафіку та управління ризиками. Виявлено, що існують обмеження у використанні засобів моніторингу загроз і навчальних платформ для роботи зі складними інформаційними системами. Недостатньо представлено навчальні курси, які охоплюють захист IoT-пристроїв і реагування на багаторівневі атаки. У дослідженні продемонстровано важливість упровадження сучасних освітніх рішень для підготовки фахівців, здатних працювати в критичних інформаційних інфраструктурах. У* ***висновках*** *обґрунтовано необхідність впровадження курсів із застосуванням SIEM-систем та інших інструментів автоматизованого моніторингу загроз, проведення практичних занять у спеціалізованих програмних середовищах та оновлення навчальних планів відповідно до сучасних стандартів інформаційної безпеки. Перспективи подальших досліджень стосуються оцінювання результатів впровадження цих заходів та розробки інтелектуальних систем підтримки освітнього процесу для забезпечення адаптивного підходу до формування професійних компетентностей фахівців у сфері інформаційної безпеки.*

Ключові слова: *інформаційна стійкість, кіберзахист, технічна підготовка, цифрова безпека, мережеві технології.*

ПЕДАГОГІЧНА АКАДЕМІЯ:
НАУКОВІ ЗАПИСКИ

Formation of professional competencies of specialists for ensuring information security in radiotelecommunication systems

Vladyslav Mahilevskyi,
Postgraduate Student of the Department of Professional Training, Document Studies and Public Administration of the Mykhailo Dragomanov Ukrainian State University, 01601, Kyiv, st. Pyrohova 9, Ukraine,
vlad.mahilevskyi@icloud.com
ORCID https://orcid.org/0009-0006-1056-0310

Abstract: *The relevance of the study is determined by the need to increase the effectiveness of training specialists to ensure information security in radiotelecommunication systems due to the growing number and complexity of modern cyber threats. This necessitates the implementation of educational programs aimed at developing professional competencies for the protection of information resources and ensuring information resilience.* ***The purpose*** *of the study is to identify key aspects of forming professional competencies of information security specialists and to develop scientifically grounded recommendations for improving educational programs in the field of radiotelecommunication systems. The study employs* ***methods*** *of scientific literature analysis, generalization of educational programs from leading institutions, and evaluation of challenges related to the technical training of information security learners.* ***The results*** *of the study found that modern educational programs contain fundamental disciplines, but do not sufficiently cover practical modules on penetration testing, network traffic analysis, and risk management. It was revealed that the use of threat monitoring tools and training platforms for working with complex information systems is limited.*

Moreover, educational courses on IoT device security and response to multi-level attacks are underrepresented. The study highlights the importance of implementing modern educational solutions for training specialists capable of operating in critical information infrastructures. ***The conclusions*** *justify the need to introduce courses involving SIEM systems and other automated threat monitoring tools, conduct practical training in specialized software environments, and update curricula to align with modern information security standards. The prospects for further research include assessing the outcomes of these measures and developing intelligent systems to support the learning process, ensuring an adaptive approach to forming professional competencies in the field of information security.*

Keywords: *information resilience, cybersecurity, technical training, digital security, network technologies.*

Постановка проблеми в загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Формування професійних компетентностей фахівців із забезпечення інформаційної безпеки в радіотелекомунікаційних системах є важливим завданням сфери кіберзахисту. Розвиток цифрових технологій та збільшення обсягів інформаційних потоків підвищують потребу в ефективних заходах протидії кібератакам, несанкціонованому доступу та технічним перешкодам. Це зумовлює необхідність підготовки висококваліфікованих фахівців, здатних використовувати сучасні засоби захисту для забезпечення інформаційної стійкості систем.

Сучасна підготовка фахівців має зосереджуватися на розвитку навичок аналізу загроз, моделювання ризиків та впровадження стратегій протидії інцидентам. Важливим є опанування методів проєктування мереж із

використанням систем шифрування, багаторівневого контролю доступу та аутентифікації. Технічна підготовка також передбачає володіння методами тестування на проникнення, аналізу вразливостей та моніторингу безпеки.

Ефективна реалізація цих завдань потребує дотримання міжнародних стандартів цифрової безпеки та адаптації освітніх програм до сучасних потреб національних мереж. Це сприятиме не лише підвищенню професійної компетентності, а й забезпечить стійкість систем до деструктивного впливу, що є важливою умовою стабільності інформаційного середовища в умовах цифрової трансформації.

Аналіз останніх досліджень і публікацій. Аналіз досліджень підтверджує актуальність проблеми формування професійних компетентностей фахівців для забезпечення інформаційної безпеки в радіотелекомунікаційних системах. Одним з основних питань є здатність спеціалістів ефективно протидіяти багаторівневим атакам. M. Dansarie наголошує на необхідності системного підходу до навчання, що передбачає використання практичних модулів для аналізу мережевого трафіку та тестування на проникнення [1]. Подібну думку висловлюють M. Mukherjee та співавтори, підкреслюючи, що поєднання теоретичної підготовки та практичних занять підвищує здатність здобувачів освіти адаптуватися до сучасних кіберзагроз [2].

На практичну спрямованість навчання звертають увагу J. J. Rugeles Uribe, E. P. Guillen та L. S. Cardoso. Учені показали ефективність програмно визначеного радіо в захисті IoT-пристроїв, що вказує на необхідність формування компетентностей для роботи з інноваційними технологіями [3]. D. Bendler та M. Felderer представили компетентнісну модель для підготовки

фахівців із кіберзахисту, яка охоплює управління ризиками та стратегії реагування на загрози [4].

У дослідженні T. B. L. Tran та співавторів стверджується, що глибоке розуміння архітектури кіберфізичних систем сприяє ефективному впровадженню комплексних методів захисту [5]. Науковці R. Prasad та V. Rohokale акцентують на важливості міждисциплінарного підходу в підготовці фахівців, який дозволяє враховувати особливості сучасних загроз і створювати більш адаптивні навчальні моделі [6].

Інформаційна безпека промислових мереж Industry 4.0 потребує особливої уваги до специфічних аспектів захисту, що підкреслено в дослідженні таких учених, як M. Kiss, G. Breda та L. Muha [7]. На необхідності регулярного оновлення освітніх програм для підвищення здатності фахівців швидко реагувати на динамічні загрози наголошують G. Hatzivasilis та співавтори [8]. P. Cheng та його колеги переконують, що поведінковий аналіз мережевого трафіку є важливим компонентом для забезпечення стійкості радіотелекомунікаційних систем і має бути інтегрований у навчальні курси [9].

Позитивно оцінюють інноваційні методики підготовки майбутніх фахівців Л. А. Карташова, А. О. Квятковська. Науковиці довели ефективність змішаного навчання в формуванні практичних навичок [10]. На значний потенціал імерсивних навчальних середовищ для покращення засвоєння складних алгоритмів захисту та розвитку критичного мислення вказують Л. О. Нікітіна, Н. В. Дженюк [11].

Таким чином, сучасні дослідження підтверджують потребу у впровадженні комплексних навчальних сценаріїв, посиленні практичної складової та розширенні доступу до сертифікаційних програм.

Виділення невирішених раніше частин загальної проблеми. Незважаючи на значний прогрес у дослідженнях інформаційної безпеки в радіотелекомунікаційних системах, залишаються нерозв'язаними питання адаптації захисних рішень до динамічних змін мережевих архітектур, особливо в умовах поширення IoT-пристроїв та 5G. Вимоги до професійних компетентностей фахівців часто мають загальний характер і недостатньо охоплюють навички управління ризиками та роботи зі складними системами моніторингу. Методи навчання потребують глибшого аналізу їхньої ефективності, зокрема в частині використання інтерактивних середовищ для відпрацювання сценаріїв багаторівневих загроз. Наявні освітні програми фрагментарно впроваджують міжнародні стандарти, а доступ до сертифікаційних курсів обмежений. Рекомендації щодо вдосконалення програм здебільшого не охоплюють комплексних сценаріїв для формування системних компетентностей. Пропоноване дослідження сприяє розв'язанню зазначених питань шляхом обґрунтування системного підходу до навчання та розроблення рекомендацій щодо модернізації освітніх програм відповідно до сучасних стандартів інформаційної безпеки.

Формулювання цілей статті (постановка завдання). Мета статті – дослідження процесу формування професійних компетентностей фахівців для забезпечення інформаційної безпеки в радіотелекомунікаційних системах.

Завдання роботи:

1. Проаналізувати сучасний стан та визначити основні тенденції розвитку радіотелекомунікаційних систем у контексті забезпечення цифрової безпеки; з'ясувати основні вимоги до професійних компетентностей фахівців, зокрема в аспектах технічної підготовки та роботи з мережевими технологіями.

2. Дослідити методи та інструменти навчання, які сприяють підготовці фахівців для підвищення рівня кіберзахисту й інформаційної стійкості радіотелекомунікаційних систем, та оцінити наявні програми підготовки фахівців на відповідність міжнародним стандартам у сфері інформаційної безпеки.

3. Розробити рекомендації щодо вдосконалення освітніх програм для формування компетентностей, необхідних для ефективного захисту інформаційних ресурсів.

Виклад основного матеріалу дослідження з повним обґрунтуванням здобутих наукових результатів. Радіотелекомунікаційні системи є важливим елементом сучасної інформаційної інфраструктури, який забезпечує передачу даних у різних сферах діяльності, таких як економіка, оборона, транспорт та комунікації. З розвитком цифрових технологій посилилися вимоги до безпеки цих систем, оскільки збільшення обсягів інформаційних потоків та інтеграція мереж підвищили ризики виникнення кібератак. Забезпечення цифрової безпеки в радіотелекомунікаційних системах передбачає використання сучасних методів захисту, таких як криптографічні алгоритми, системи багаторівневої аутентифікації та засоби моніторингу трафіку. Водночас стрімкий розвиток бездротових технологій, зокрема 5G та IoT-рішень, вимагає вдосконалення не лише технічних засобів кіберзахисту, а й професійної підготовки фахівців (табл. 1).

 ISSN: 2786-9458

Таблиця 1

Тенденції розвитку радіотелекомунікаційних систем у контексті забезпечення цифрової безпеки.

Параметр розвитку	**Стан на попередніх етапах розвитку галузі**	**Сучасний стан**	**Зміни та актуальні тенденції**
Технології передачі даних	Використання технологій мобільного зв'язку поколінь 3G та 4G	Впровадження стандартів 5G і підготовка до впровадження 6G	Збільшення пропускної здатності та зменшення затримок передачі даних
Архітектура систем	Централізовані системи з обмеженими можливостями масштабування	Децентралізовані архітектури на основі MEC (обчислення на краю мережі) та SDN	Розширення застосування обчислень на краю мережі для підвищення швидкості та надійності передачі даних
Кіберзагрози	Основний акцент на запобіганні DDoS-атакам та захисті від несанкціонованого доступу	Збільшення кількості атак на IoT-пристрої та складних багаторівневих загроз	Ускладнення методів атак, поширення атак типу «людина посередині» та експлуатації вразливостей IoT
Методи захисту	Застосування міжмережевих екранів та VPN для створення захищених каналів	Використання систем штучного інтелекту для моніторингу та аналізу трафіку	Автоматизований аналіз поведінки та швидке реагування на інциденти за допомогою технологій штучного інтелекту

ISSN: 2786-9458

Регулятивна база	Вибіркове застосування міжнародних стандартів безпеки даних	Уніфікація нормативної бази відповідно до стандартів ISO 27001, NIST, GDPR	Підвищення вимог до контролю безпеки даних і забезпечення відповідності міжнародним стандартам

Джерело: сформовано автором на підставі [1, с. 91102; 5, с. 68–70; 7, с. 899; 9, с. 14–17; 12; 13]

Сучасна практика демонструє, що впровадження нових технологій, таких як 5G, значно підвищило пропускну здатність мереж, але також збільшило обсяг потенційних векторів атак. Наприклад, поширення IoT-рішень створює додаткові загрози через можливість компрометації кінцевих пристроїв, що раніше не були частиною критичної інфраструктури. Водночас розвиток децентралізованих архітектур на основі обчислень на краю мережі сприяє зниженню затримок передачі даних, але вимагає інтеграції складних систем моніторингу та прогнозування кіберзагроз. На практиці це реалізується шляхом впровадження рішень на базі штучного інтелекту, що дозволяють здійснювати автоматичне виявлення аномалій у поведінці мережевих пристроїв.

Іншою важливою зміною стало вдосконалення регулятивної бази з метою забезпечення інформаційної стійкості. Наприклад, міжнародні стандарти ISO 27001 [12] та NIST [13] стали основою для розробки національних протоколів безпеки даних, що дозволяє уніфікувати заходи захисту та забезпечити відповідність міжнародним вимогам. В Україні також активізовано впровадження рекомендацій ЄС щодо регулювання цифрової

безпеки, що сприяє інтеграції національних систем у глобальні інформаційні мережі.

Формування професійних компетентностей фахівців у сфері інформаційної безпеки в радіотелекомунікаційних системах вимагає глибоких знань сучасних методів захисту, навичок роботи з мережевими технологіями та високого рівня технічної підготовки. Професіонали повинні не лише мати знання про основи криптографії, захист мереж і управління доступом, а й бути готовими до швидкого реагування на складні кіберзагрози. Особливого значення набувають такі компетентності, як розуміння архітектури децентралізованих систем, досвід роботи з автоматизованими платформами кіберзахисту та вміння інтегрувати рішення штучного інтелекту для аналізу загроз (табл. 2).

Таблиця 2

Основні вимоги до професійних компетентностей фахівців з інформаційної безпеки в радіотелекомунікаційних системах

Напрям компетентності	**Основні вимоги до знань і навичок**	**Практичне значення для забезпечення безпеки**
Технічна підготовка	Глибоке знання протоколів безпеки, методів шифрування, роботи з міжмережевими екранами та системами виявлення вторгнень	Забезпечення безперервного функціонування систем в умовах зовнішніх загроз та зменшення ризику несанкціонованого доступу
Робота з мережевими технологіями у	Володіння технологіями маршрутизації, сегментації мереж, побудови VPN та налаштування захищених каналів зв’язку	Зниження вразливості систем до атак типу «людина посередині» та підтримка стабільності мережевих з’єднань

Робота з автоматизованими системами захисту	Уміння використовувати SIEM-системи, IDS/IPS та інші рішення для моніторингу безпеки в режимі реального часу	Підвищення ефективності моніторингу та виявлення аномалій завдяки швидкій обробці великого обсягу даних
Упровадження стандартів безпеки	Знання міжнародних стандартів ISO 27001, NIST, регламентів GDPR та відповідних національних норм	Підвищення рівня довіри до системи через відповідність міжнародним нормам та єдність процедур захисту даних
Оперативне реагування	Навички швидкого виявлення, класифікації та усунення загроз, документування та аналізу інцидентів	Зменшення часу на ліквідацію наслідків атак і підвищення стійкості систем до повторних атак

Джерело: сформовано автором на підставі [2, с. 11–13; 4, с. 6–7; 5 с. 75–76; 6; 10, с. 60–61; 12; 13]

У сучасних умовах професійні компетентності фахівців інформаційної безпеки визначають здатність забезпечити надійний захист інформаційних потоків у радіотелекомунікаційних системах. На практиці це реалізується через уміння ефективно реагувати на нові типи загроз, такі як багаторівневі атаки на IoT-пристрої та комбіновані DDoS-атаки. Фахівці повинні не лише обслуговувати базові засоби захисту, як-от VPN і міжмережеві екрани, а й активно використовувати автоматизовані системи моніторингу для аналізу аномалій. Це набуло особливої актуальності у зв’язку з поширенням SIEM-рішень, які дозволяють аналізувати великий обсяг трафіку та виявляти кіберінциденти на ранніх етапах. Застосування міжнародних стандартів безпеки забезпечує уніфікацію процедур захисту, що дозволяє оптимізувати

процеси контролю доступу та реагування на інциденти. Нові тренди також передбачають інтеграцію освітніх програм із симуляціями реальних кібератак, що дозволяє фахівцям ефективно відпрацьовувати навички протидії загрозам у контрольованих умовах та бути готовими до непередбачуваних ситуацій.

Ефективне навчання фахівців інформаційної безпеки є важливим для забезпечення високого рівня кіберзахисту та інформаційної стійкості радіотелекомунікаційних систем. З огляду на зростання складності загроз і поширення децентралізованих мережевих архітектур, методи навчання повинні бути адаптовані до сучасних потреб. Вони мають охоплювати практичні симуляції реальних інцидентів, навчальні платформи на основі штучного інтелекту та спеціалізовані курси, що дозволяють засвоювати новітні методи аналізу загроз і реагування на атаки. Зокрема, популярним стало використання систем кіберполігонів, які дозволяють моделювати складні сценарії загроз у контрольованих умовах. Важливо також застосовувати інструменти тестування на проникнення та навчальні тренажери для підвищення навичок у виявленні вразливостей (табл. 3).

Таблиця 3

Методи та інструменти навчання, які сприяють підготовці фахівців для підвищення рівня кіберзахисту й інформаційної стійкості радіотелекомунікаційних систем

Метод чи інструмент навчання	**Характеристики та особливості**	**Практичне значення для підвищення рівня кіберзахисту**
Симуляції та кіберполігони	Платформи, що імітують реальні інциденти та атаки на мережеві інфраструктури	Відпрацювання навичок реагування на кіберінциденти та усунення їхніх наслідків

Навчальні тренажери	Програми, що дозволяють моделювати дії фахівця у відповідь на виявлені загрози	Підвищення оперативності та точності прийняття рішень у критичних ситуаціях
Системи на основі штучного інтелекту	Платформи, що аналізують навчальні дані та пропонують персоналізовані сценарії	Автоматизація процесу навчання та виявлення індивідуальних прогалин у знаннях
Курси з тестування на проникнення	Навчальні програми, що охоплюють методи виявлення вразливостей систем	Зниження ризику експлуатації вразливостей шляхом поглиблення практичних навичок
Спеціалізовані онлайн-курси	Вебресурси, що надають доступ до навчальних матеріалів і тренувань у реальному часі	Забезпечення безперервного професійного розвитку та доступу до актуальних знань

Джерело: сформовано автором на підставі [2, с. 12–16; 8; 9, с. 16; 10, с. 62–63]

На практиці навчальні кіберполігони широко використовуються у великих організаціях та закладах вищої освіти (далі – ЗВО) для моделювання складних кібератак і аналізу відповідей фахівців у режимі реального часу. Наприклад, українські ІТ-університети активно інтегрують в освітній процес симуляційні платформи, що дозволяють здобувачам освіти відпрацьовувати дії у випадку DDoS-атак або вторгнень на сервери. Це дає змогу сформувати навички роботи в умовах високого навантаження на системи та швидкого прийняття рішень. Системи на основі штучного інтелекту дозволяють не лише здійснювати аналіз успішності навчання, а й формувати персоналізовані рекомендації для вдосконалення навичок. Курси з тестування на проникнення дають можливість фахівцям відпрацьовувати техніки етичного хакінгу, що

дозволяє своєчасно виявляти вразливості в системах і попереджати потенційні атаки. Інтеграція таких методів сприяє не лише підвищенню інформаційної стійкості, а й створенню культури постійного вдосконалення у сфері кіберзахисту.

Для оцінювання програм підготовки фахівців з інформаційної безпеки було проаналізовано освітні програми п'яти провідних ЗВО України: Українського державного університету імені Михайла Драгоманова, Київського національного університету імені Тараса Шевченка, Національного університету «Львівська політехніка», Харківського національного університету радіоелектроніки та Національного університету «Одеська політехніка».

Український державний університет імені Михайла Драгоманова пропонує освітню програму (далі – ОП) за спеціальністю 121 «Інженерія програмного забезпечення» [14]. У межах цієї програми викладається дисципліна «Безпека програм та даних», яка охоплює сучасні методи забезпечення захисту інформації, зокрема апаратно-програмні засоби захисту, криптографічні методи та системи контролю доступу. Особливістю ОП є міждисциплінарний підхід, який поєднує технічні та правові аспекти інформаційної безпеки, що сприяє формуванню компетенцій у сфері захисту програмних систем. Проте певним недоліком є обмежена кількість практичних занять на базі кіберполігонів та відсутність модулів, присвячених управлінню ризиками та міжнародним стандартам кіберзахисту. Водночас університет пропонує курси підвищення кваліфікації для державних службовців та представників місцевого самоврядування з питань інформаційної безпеки, що підвищує практичну орієнтацію освітньої діяльності. Для подальшого вдосконалення підготовки фахівців доцільним є впровадження симуляційних

платформ для моделювання сценаріїв реагування на кіберзагрози та сертифікаційних модулів за міжнародними стандартами, що дозволить випускникам підвищити конкурентоспроможність на ринку праці.

Освітня програма «Кібербезпека» бакалаврського рівня Київського національного університету імені Тараса Шевченка [15] охоплює фундаментальні дисципліни, пов'язані з аналізом мережевих загроз, криптографічними методами та моніторингом безпеки. Основною перевагою ОП є наявність модулів із реагування на інциденти відповідно до стандартів ISO 27001 [12]. Проте обмежений практичний компонент є недоліком, адже більшість занять присвячена теоретичному вивченню методів захисту. Здобувачі освіти також мають недостатній доступ до симуляційних платформ та поведінкового аналізу загроз, що знижує готовність до роботи в реальних умовах.

У Національному університеті «Львівська політехніка» освітня програма «Адміністрування систем кібербезпеки» [16] магістерського рівня орієнтована на підготовку фахівців із поглибленими знаннями про SIEM-системи та міжмережеві екрани. Проте, незважаючи на наявність курсів з етичного хакінгу та тестування на проникнення, відсутність модулів з управління інформаційними ризиками й аудиту безпеки є слабким місцем програми. Це обмежує можливість здобувачів працювати у сфері управління ризиками та розробляти стратегії відповідно до рекомендацій NIST [13].

У Харківському національному університеті радіоелектроніки освітня програма «Управління інформаційною безпекою» [17] акцентує на захисті IoT-пристроїв та роботі з кіберполігонами для моделювання атак. Майбутні фахівці відпрацьовують сценарії багаторівневих атак і реагування на інциденти в реальному часі. Проте обмежена кількість курсів із глобального

регулювання у сфері кібербезпеки та інтеграції знань щодо захисту критичної інфраструктури.

Освітня програма «Національна безпека» [18] в Національному університеті «Одеська політехніка» містить дисципліни з багаторівневої аутентифікації та управління інформаційними потоками. Водночас програма не передбачає навчання із застосування автоматизованих систем поведінкового аналізу та реагування на кіберзагрози, що обмежує можливість ефективного прогнозування загроз.

Альтернативою університетським програмам є професійні курси, такі як Certified Information Systems Security Professional (CISSP) від ISC2 [19], що забезпечує знання у сферах управління ризиками, криптографії та розробки політик безпеки. Курси CEH від EC-Council [20] та CompTIA Security+ [21] пропонують поглиблене навчання методів етичного хакінгу, оцінки загроз і тестування на проникнення. Вони надають слухачам сертифікати міжнародного зразка, що підвищує конкурентоспроможність на ринку праці. Проте такі курси можуть бути недоступними через високу вартість і обмежену кількість програм фінансування.

Удосконалення освітніх програм для формування компетентностей, необхідних для ефективного захисту інформаційних ресурсів, має враховувати сучасні вимоги та міжнародний досвід у сфері кібербезпеки. Одним із напрямів модернізації є збільшення кількості практичних занять на основі симуляційних тренінгів і кіберполігонів для формування навичок реагування на реальні загрози. Використання автоматизованих систем для аналізу аномалій і моніторингу мережевого трафіку дозволить забезпечити якісну підготовку здобувачів освіти до роботи з великими обсягами даних та виявлення складних загроз у реальному часі.

 ISSN: 2786-9458

Окрім цього, важливо розширити співпрацю з міжнародними сертифікаційними організаціями для підвищення рівня доступності програм сертифікації, таких як CISSP [19], CEH [20] і CompTIA Security+ [21]. Це не означає простого дублювання вже наявних курсів, а передбачає інтеграцію сертифікованих модулів у навчальні плани ЗВО. Такий підхід дозволить здобувачам освіти отримувати як академічну освіту, так і сертифікати міжнародного зразка, що підвищує їх конкурентоспроможність на ринку праці без додаткових витрат на стороннє навчання.

Розробка міждисциплінарних курсів, що поєднують аспекти управління ризиками, аналізу великих даних та захисту критичної інфраструктури, дозволить сформувати всебічно підготовлених фахівців для подолання комплексних загроз [8]. Навчальні модулі з використанням технологій штучного інтелекту для поведінкового аналізу та прогнозування кіберінцидентів сприятимуть адаптації здобувачів освіти до сучасних методів забезпечення кіберстійкості [9, с. 14]. Особливу увагу варто приділити тематиці кризового управління та координації дій під час масштабних атак для підтримки стабільної роботи систем. Також необхідно впровадити курси з кібергігієни та захисту персональних даних для мінімізації ризиків, пов’язаних із людським фактором. Підвищення технічної оснащеності закладів освіти через використання тренажерів і симуляційних платформ дозволить значно підвищити ефективність навчання. Крім того, модернізація навчальних планів шляхом використання сучасних SIEM-рішень забезпечить ефективну підготовку до управління інформаційною безпекою в умовах зростання кількості кіберзагроз. Розвиток міжнародної співпраці між університетами та участь у міжнародних навчальних конкурсах із кібербезпеки дадуть змогу

здобувачам освіти долучитися до світової спільноти та підвищити їхню конкурентоспроможність на глобальному ринку праці.

Висновки. Отже, розвиток технологій передачі даних та впровадження архітектур на основі обчислень на краю мережі вимагають підготовки фахівців із високим рівнем технічних навичок, здатних ефективно застосовувати засоби моніторингу та прогнозування загроз. Аналіз освітніх програм українських ЗВО засвідчив наявність теоретичної бази, проте практична підготовка потребує значного розширення через запровадження симуляційних платформ та інтеграцію модулів із сертифікацією міжнародного рівня.

Основними проблемами є недостатнє використання автоматизованих систем для поведінкового аналізу та моніторингу трафіку, обмежений доступ до міжнародних курсів і сертифікаційних програм, а також відсутність міждисциплінарних навчальних модулів, які поєднують управління ризиками й роботу з критичною інфраструктурою. Важливо зазначити, що окремі освітні програми недостатньо охоплюють тематику управління інформаційною безпекою IoT-пристроїв та реагування на багаторівневі загрози, що є актуальним у сучасних умовах.

Рекомендовано впроваджувати кіберполігони для моделювання складних інцидентів, розширити доступ до міжнародних сертифікацій через партнерські програми та використовувати інструменти штучного інтелекту для підвищення ефективності навчання. Перспективи подальших досліджень полягають в аналізі довгострокових результатів впровадження симуляційного навчання та розробці персоналізованих курсів із використанням інтелектуальних систем, здатних адаптувати освітній процес відповідно до потреб здобувачів освіти.

 ISSN: 2786-9458

Список використаних джерел

1. Dansarie M. Security Issues in Special-Purpose Digital Radio Communication Systems: A Systematic Review. *IEEE Access.* 2024. Vol. 12. P. 91101–91126. URL: https://doi.org/10.1109/ACCESS.2024.3420091 (date of access: 14.10.2024).

2. Mukherjee M., Le N. T., Chow Y.-W., Susilo W. Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes. *Information.* 2024. Vol. 15. № 2. URL: https://doi.org/10.3390/info15020117 (date of access: 14.10.2024).

3. Uribe J. J. R., Guillen E. P., Cardoso L. S. A Technical Review of Wireless Security for the Internet of Things: Software Defined Radio Perspective. *Journal of King Saud University-Computer and Information Sciences.* 2022. Vol. 34. № 7. P. 4122–4134. URL: https://doi.org/10.1016/j.jksuci.2021.04.003 (date of access: 14.10.2024).

4. Bendler D., Felderer M. Competency Models for Information Security and Cybersecurity Professionals: Analysis of Existing Work and a New Model. *ACM Transactions on Computing Education.* 2023. Vol. 23. № 2. P. 1–33. URL: https://dl.acm.org/doi/full/10.1145/3573205 (date of access: 14.10.2024).

5. Tran T. B. L., Törngren M., Nguyen H. D., Paulen R., Gleason N. W., Duong T. H. Trends in Preparing Cyber-Physical Systems Engineers. *Cyber-Physical Systems.* 2019. Vol. 5. № 2. P. 65–91. URL: https://doi.org/10.1080/23335777.2019.1600034 (date of access: 14.10.2024).

6. Prasad R., Rohokale V. Cyber Security: The Lifeline of Information and Communication Technology. Cham: Springer International Publishing, 2020. URL: https://link.springer.com/book/10.1007/978-3-030-31703-4 (date of access: 14.10.2024).

7. Kiss M., Breda G., Muha L. Information Security Aspects of Industry 4.0. *Procedia Manufacturing*. 2019. Vol. 32. P. 848–855. URL: https://doi.org/10.1016/j.promfg.2019.02.293 (date of access: 14.10.2024).

8. Hatzivasilis G., Ioannidis S., Smyrlis M., Spanoudakis G., Frati F., Goeke L., Hildebrandt T., Tsakirakis G., Oikonomou F., Leftheriotis G., Koshutanski H. Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees. *Applied Sciences.* 2020. Vol. 10. № 16. Art. 5702. URL: https://www.academia.edu/73709685/Modern_Aspects_of_Cyber_Security_Training_and_Continuous_Adaptation_of_Programmes_to_Trainees (date of access: 14.10.2024).

9. Cheng P., Chen Z., Ding M., Li Y., Vucetic B., Niyato D. Spectrum Intelligent Radio: Technology, Development, and Future Trends. *IEEE Communications Magazine.* 2020. Vol. 58. № 1. P. 12–18. URL: https://doi.org/10.1109/MCOM.001.1900200 (date of access: 14.10.2024).

10. Карташова Л. А., Квятковська А. О. Змішане навчання: методика підготовки майбутніх фахівців з телекомунікацій. *Вісник післядипломної освіти. Серія «Педагогічні науки».* 2024. Вип. 27 (56). С. 55–69. URL: https://ojs.uem.edu.ua/index.php/vpo/article/view/685 (дата звернення: 12.10.2024).

11. Нікітіна Л. О., Дженюк Н. В. Імерсивне навчання студентів у галузі телекомунікацій. *Системи управління, навігації та зв'язку.* 2023. № 4 (74). С. 160–166. URL: https://journals.nupp.edu.ua/sunz/article/view/3176/2582 (date of access: 14.10.2024).

12. ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems Requirements.

International Organization for Standardization: official website. 2022. URL: https://www.iso.org/standard/82875.html (date of access: 14.10.2024).

13. National Institute of Standards and Technology (NIST). Cybersecurity Framework. *NIST: official website.* 2023. URL: https://www.nist.gov/cyberframework (date of access: 14.10.2024).

14. Освітня програма зі спеціальності 121 «Інженерія програмного забезпечення» (бакалаврський рівень). *Український державний університет імені Михайла Драгоманова: офіційний сайт.* 2024. URL: https://fi.npu.edu.ua/abituriientu/napriam-pidhotovky/121-inzheneriia-prohramnoho-zabezpechennia (дата звернення: 14.10.2024).

15. Освітня програма зі спеціальності 125 «Кібербезпека» (бакалаврський рівень). *Київський національний університет імені Тараса Шевченка: офіційний сайт.* 2024. URL: https://infopacket.knu.ua/CourseInfo?courseId=35502 (дата звернення: 01.10.2024).

16. Освітня програма «Адміністрування систем кібербезпеки» (магістерський рівень). *Національний університет «Львівська політехніка»: офіційний сайт.* 2024. URL: https://directory.lpnu.ua/majors/ikta/8.125.00.04/19/2023/ua/full (дата звернення: 14.10.2024).

17. Освітня програма «Управління інформаційною безпекою» (бакалаврський рівень). *Харківський національний університет радіоелектроніки: офіційний сайт.* 2024. URL: https://nure.ua/abituriyentam/spetsialnosti-ta-spetsializatsiyi/spetsialnist-125-kiberbezpeka-ta-zakhyst-informatsii/bakalavr-125-kiberbezpeka-ta-zakhyst-

informatsii/osvitnja-programa-upravlinnja-informacijnoju-bezpekoju (дата звернення: 14.10.2024).

18. Освітня програма зі спеціальності 256 «Національна безпека» (магістерський рівень). *Національний університет «Одеська політехніка»: офіційний сайт.* 2024. URL: https://op.edu.ua/education/programs/mag-256-0 (дата звернення: 14.10.2024).

19. Certified Information Systems Security Professional (CISSP). *ISC2: website.* 2024. URL: https://www.isc2.org/Certifications/CISSP (date of access: 14.10.2024).

20. Certified Ethical Hacker (CEH). *EC-Council: website.* 2024. URL: https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ (дата date of access: 14.10.2024).

21. CompTIA Security+. *CompTIA: website.* 2024. URL: https://www.comptia.org/certifications/security (date of access: 14.10.2024).