МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний педагогічний
університет імені Володимира Гнатюка

Кваліфікаційна наукова праця на правах рукопису

Шимків Назар Ігорович

УДК 378.091.33-027.22:004.056

ДИСЕРТАЦІЯ
МЕТОДИКА ПІДГОТОВКИ ФАХІВЦІВ ЦИФРОВИХ ТЕХНОЛОГІЙ ДО ЗАСТОСУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ДАНИХ

015 Професійна освіта (за спеціалізаціями)
01 Освіта / Педагогіка

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Назар ШИМКІВ Автор цифрового підпису Назар ШИМКІВ
Дата: 2026.07.15 15:33:47 +03'00'
_____ Н.І. Шимків
(підпис, ініціали та прізвище здобувача)

Науковий керівник **Юрій ФРАНКО**, канд. техн. наук, доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Тернопіль, 2026

АНОТАЦІЯ

Шимків Н. І. Методика підготовки фахівців цифрових технологій до застосування програмного забезпечення захисту даних. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії з галузі знань 01 Освіта / Педагогіка за спеціальністю 015 Професійна освіта (заспеціалізаціями). Тернопільський національний педагогічний університет імені Володимира Гнатюка. Тернопіль, 2026.

Роботу присвячено дослідженню теоретичних, методичних та практичних аспектів підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних. У дисертації визначено сутність і структуру готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних, обґрунтовано педагогічні умови, розроблено структурно-функціональну модель та методику підготовки, експериментально підтверджено їх ефективність у процесі професійної підготовки здобувачів освіти за спеціальністю 015 Професійна освіта, спеціалізацією 015.39 Цифрові технології.

На основі аналізу наукової літератури, нормативно-правових документів у сфері інформаційної безпеки, кібербезпеки та захисту персональних даних визначено сучасний стан досліджуваної проблеми, уточнено сутність поняття «готовність майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних» та охарактеризовано її структуру. Встановлено, що готовність до застосування програмного забезпечення захисту даних є інтегративною характеристикою особистості, яка поєднує систему знань, практичних вмінь, професійних цінностей, мотиваційних чинників та рефлексивних здібностей, необхідних для забезпечення безпечної роботи з інформаційними ресурсами та організації освітнього процесу з питань захисту даних.

У процесі дослідження здійснено комплексний аналіз сучасних програмних засобів захисту даних, які використовуються в професійній діяльності фахівців цифрової технологій та можуть бути ефективно інтегровані в освітній процес закладів вищої освіти. Аналіз охоплював програмне забезечення різного функціонального призначення, зокрема засоби моніторингу та аналізу мережевого трафіку, інструменти моделювання комп'ютерних мереж, системи шифрування даних, платформи для тестування безпеки інформаційних систем, а також засоби централізованого збору та аналізу подій інформаційної безпеки.

На основі проведеного аналізу обґрунтовано доцільність використання програмних засобів Wireshark, Cisco Packet Tracer, VeraCrypt, Kali Linux, Splunk та інших спеціалізованих інструментів у професійній підготовці майбутніх фахівців цифрових технологій. Встановлено, що застосування зазначених програмних продуктів забезпечує формування практичних вмінь у сфері кібербезпеки, захисту даних, адміністрування комп'ютерних мереж, виявлення кіберзагроз, аналізу інцидентів інформаційної безпеки та використання сучасних механізмів криптографічного захисту інформації.

У процесі реалізації методики використано сучасне програмне забезпечення захисту даних (Wireshark, Cisco Packet Tracer, VeraCrypt, Kali Linux, Splunk), застосування якого забезпечує формування в майбутніх фахівців цифрових технологій професійних компетентностей щодо аналізу мережевого трафіку, моделювання захищених мережевих середовищ, шифрування даних, оцінювання захищеності інформаційних систем, тестування на проникнення, а також моніторингу й аналізу подій інформаційної безпеки.

У дослідженні визначено особливості інтеграції зазначених програмних засобів в освітній процес підготовки майбутніх фахівців цифрових технологій. Встановлено, що ефективне використання спеціалізованого програмного забезпечення потребує поєднання технічної та педагогічної складових підготовки. З одного боку, здобувачі освіти повинні оволодіти практичними навичками використання інструментів захисту даних, а з іншого – адаптувати

відповідні технології до навчального процесу, розробляти навчальні матеріали, організовувати практичну діяльність здобувачів освіти та формувати в них культуру безпечного використання цифрових технологій.

Обґрунтовано, що інтеграція сучасних програмних засобів захисту даних до змісту професійної підготовки майбутніх фахівців цифрового технологій має здійснюватися на засадах практико-орієнтованого, компетентнісного та міждисциплінарного підходів із використанням віртуальних лабораторій, кіберполігонів, кейсових завдань і проєктної діяльності. Такий підхід забезпечує наближення умов навчання до реального професійного середовища, підвищує рівень сформованості цифрових та професійних компетентностей і сприяє підготовці конкурентоспроможних фахівців, здатних ефективно здійснювати як професійну, так і педагогічну діяльність у сфері цифрових технологій та захисту даних.

Теоретично обґрунтовано педагогічні умови ефективної підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних, а саме: формування позитивної мотивації до використання засобів захисту інформації у професійній діяльності; оновлення змісту професійної підготовки відповідно до сучасних тенденцій розвитку кібербезпеки; забезпечення практико-орієнтованого навчання на основі використання спеціалізованого програмного забезпечення; інтеграція засобів захисту даних у зміст фахових дисциплін та цифрового освітнього середовища; залучення здобувачів освіти до проєктної, дослідницької та рефлексивної діяльності.

Розроблено структурно-функціональну модель підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних, яка охоплює методологічний, змістовий, педагогічний, організаційно-процесуальний та результативний блоки. Модель базується на компетентнісному, системному, діяльнісному, особистісно орієнтованому, практико-орієнтованому та технологічному підходах і спрямована на

формування когнітивного, діяльнісного, мотиваційного та рефлексивного компонентів готовності.

У результаті проведеного дослідження розроблено методику підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних. Методика спрямована на формування у здобувачів освіти системи знань, вмінь і навичок щодо використання сучасних засобів захисту даних у професійній діяльності та передбачає поетапне формування готовності до розв'язання завдань інформаційної безпеки в умовах цифрового середовища.

Особливістю запропонованої методики є комплексне використання сучасних форм і методів навчання, серед яких провідне місце займають, кейс-метод, проєктне навчання, кіберполігони та віртуальні лабораторії. Їх інтеграція дає змогу забезпечити формування практичних навичок налаштування та використання програмного забезпечення захисту даних; сприяє розвитку здатності аналізувати реальні та змодельовані ситуації, пов'язані з кіберзагрозами та порушенням безпеки інформації; проєктне навчання орієнтоване на розроблення власних рішень у сфері захисту даних і розвиток навичок командної роботи. Використання кіберполігонів та віртуальних лабораторій забезпечує моделювання професійних ситуацій, максимально наближених до реальних умов функціонування інформаційних систем, що сприяє формуванню практичного досвіду застосування засобів кіберзахисту.

Для визначення ефективності розробленої методики обґрунтовано критерії, показники та рівні сформованості готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних. Система оцінювання охоплює мотиваційний, когнітивний, діяльнісний та рефлексивний критерії, які характеризують рівень професійної мотивації, обсяг і якість фахових знань, сформованість практичних вмінь використання програмних засобів захисту даних, а також здатність до самоаналізу та професійного вдосконалення. Відповідно до визначених показників виокремлено високий, достатній, середній та низький рівні сформованості готовності, що

забезпечує можливість комплексної діагностики результатів підготовки та моніторингу динаміки професійного розвитку здобувачів освіти.

Експериментально перевірено ефективність розробленої методики. Результати педагогічного експерименту засвідчили статистично значуще підвищення рівня готовності студентів експериментальної групи порівняно з контрольною. Встановлено позитивну динаміку розвитку когнітивного, діяльнісного, мотиваційного та рефлексивного компонентів готовності. Отримані результати підтвердили ефективність запропонованої методики та доцільність її впровадження в систему професійної підготовки майбутніх фахівців цифрових технологій.

Практичне значення одержаних результатів полягає у розробленні та впровадженні методики підготовки майбутніх фахівців спеціальності 015 «Професійна освіта», спеціалізації 015.39 «Цифрові технології» до застосування програмного забезпечення захисту даних. Практичну цінність становлять розроблені структурно-функціональна модель, педагогічні умови, навчально-методичне забезпечення, критерії, показники та діагностичний інструментарій оцінювання готовності здобувачів освіти, а також розроблений та апробований в освітньому процесі електронний навчально-методичний комплекс дисципліни «Кібербезпека та захист даних у професійній освіті», який містить конспекти лекцій, лабораторні роботи, професійно орієнтовані кейси, проєктні й тестові завдання, навчальні матеріали для роботи в кіберполігонах та інші навчально-методичні матеріали, розміщені в системі управління навчанням LMS Moodle. Результати дослідження можуть бути використані для модернізації професійної підготовки майбутніх фахівців цифрових технологій у закладах вищої освіти.

Ключові слова: цифрові технології, цифрова трансформація, підготовка фахівців, освітній процес, цифрова компетентність, практична підготовка, захист даних, кібербезпека, педагогічні методи, навчальні технології, адаптивне навчання, практичні вміння, фахівці цифрових технологій, цифрова безпека, система підготовки.

ABSTRACT

Shymkiv N. I. Methodology for Preparing Digital Technology Specialists to Use Data Protection Software. – Qualification scientific work submitted as a manuscript.

Dissertation submitted for the degree of Doctor of Philosophy in the field of knowledge 01 Education/Pedagogy, specialty 015 Professional Education (by specializations). Ternopil Volodymyr Hnatiuk National Pedagogical University, Ternopil, 2026.

The dissertation is devoted to the theoretical, methodological, and practical aspects of preparing future digital technology specialists to use data protection software. The dissertation defines the essence and structure of the readiness of future digital technology specialists to use data protection software, substantiates the pedagogical conditions, develops a structural-functional model and a training methodology, and experimentally confirms their effectiveness in the process of professional training of students enrolled in specialty 015 Professional Education, specialization 015.39 Digital Technologies.

Based on the analysis of scientific literature and regulatory documents in the fields of information security, cybersecurity, and personal data protection, the current state of the research problem was determined. The essence of the concept of “the readiness of future digital technology specialists to use data protection software” was clarified, and its structure was characterized. It was established that readiness to use data protection software is an integrative personal characteristic that combines a system of knowledge, practical skills, professional values, motivational factors, and reflective abilities necessary to ensure the secure use of information resources and the organization of the educational process related to data protection.

During the research, a comprehensive analysis of modern data protection software used in the professional activities of digital technology specialists and capable of being effectively integrated into the educational process of higher education institutions was conducted. The analysis covered software with various functional

purposes, including network traffic monitoring and analysis tools, computer network simulation tools, data encryption systems, information system security testing platforms, and tools for the centralized collection and analysis of information security events.

Based on the analysis, the feasibility of using Wireshark, Cisco Packet Tracer, VeraCrypt, Kali Linux, Splunk, and other specialized tools for professional training of future digital technology specialists was substantiated. It was established that the use of these software products ensures the development of practical skills in cybersecurity, data protection, computer network administration, cyber threat detection, information security incident analysis, and the application of modern cryptographic mechanisms for information protection.

During the methodology implementation, modern data protection software (Wireshark, Cisco Packet Tracer, VeraCrypt, Kali Linux, and Splunk) was used. Its application ensures the development of professional competencies among future digital technology specialists in network traffic analysis, modeling secure network environments, data encryption, information system security assessment, penetration testing, and the monitoring and analysis of information security events.

The study identifies the specific features of integrating the aforementioned software tools into the educational process of training future digital technology specialists. It was established that the effective use of specialized software requires a combination of both technical and pedagogical components of training. On the one hand, students must acquire practical skills in using data protection tools; on the other hand, they must develop the ability to adapt relevant technologies to the educational process, design instructional materials, organize learners' practical activities, and foster a culture of safe use of digital technologies.

It has been substantiated that integrating modern data protection software into professional training for future digital technology specialists should be based on practice-oriented, competency-based, and interdisciplinary approaches, using laboratory classes, virtual laboratories, cyber ranges, case-based tasks, and project activities. Such an approach brings learning conditions closer to a real professional

environment, enhances the development of digital and professional competencies, and prepares competitive specialists capable of effectively performing both professional and pedagogical activities in the field of digital technologies and data protection.

The pedagogical conditions for the effective preparation of future digital technology specialists to use data protection software have been theoretically substantiated, namely: fostering positive motivation toward the use of information protection tools in professional activities; updating the content of professional training in accordance with current cybersecurity trends; ensuring practice-oriented learning based on the use of specialized software; integrating data protection tools into the content of professional disciplines and the digital educational environment; and engaging students in project-based, research, and reflective activities.

A structural-functional model for preparing future digital technology specialists to use data protection software has been developed. The model encompasses methodological, content, pedagogical, organizational-process, and outcome components. It is based on competency-based, systemic, activity-based, learner-centered, practice-oriented, and technological approaches and is aimed at developing the cognitive, activity, motivational, and reflective components of readiness.

As a result of the research, a methodology for preparing future digital technology specialists to use data protection software was developed. The methodology is based on competency-based, activity-based, and practice-oriented approaches. It aims to develop in students a system of knowledge, skills, and abilities related to the use of modern data protection tools in professional activities and to gradually build readiness to solve information security tasks in a digital environment.

A distinctive feature of the proposed methodology is the integrated use of modern teaching methods and practices, among which laboratory work, the case-study method, project-based learning, cyber ranges, and virtual laboratories play a leading role. Laboratory work ensures the development of practical skills in configuring and using data protection software; the case-study method promotes the ability to analyze real and simulated situations related to cyber threats and information security breaches; and project-based learning focuses on developing original solutions in data protection

and enhancing teamwork skills. The use of cyber ranges and virtual laboratories provides opportunities to simulate professional situations that closely resemble the real operating conditions of information systems, thereby facilitating the acquisition of practical experience in applying cybersecurity tools.

To determine the effectiveness of the developed methodology, criteria, indicators, and levels of readiness of future digital technology specialists to use data protection software were substantiated. The assessment system includes motivational, cognitive, activity-based, and reflective criteria that characterize the level of professional motivation, the scope and quality of professional knowledge, the development of practical skills in using data protection software, and the ability for self-analysis and professional self-improvement. According to the established indicators, four levels of readiness were identified: high, sufficient, medium, and low. This enables a comprehensive assessment of training outcomes and the monitoring of students' professional development.

The effectiveness of the developed methodology was experimentally verified. The results of the pedagogical experiment demonstrated a statistically significant increase in students' readiness in the experimental group compared to the control group. Positive dynamics were observed in the development of the cognitive, activity-based, motivational, and reflective components of readiness. The obtained results confirmed the effectiveness of the proposed methodology and the feasibility of its implementation in the system of professional training of future digital technology specialists.

The practical significance of the obtained results lies in the development and implementation of a methodology for preparing future specialists in specialty 015 "Professional Education", specialization 015.39 "Digital Technologies", to use data protection software. The practical value of the study is reflected in the developed structural-functional model, pedagogical conditions, educational and methodological support, criteria, indicators, and diagnostic tools for assessing the readiness of students, as well as in the electronic educational and methodological complex for the course "Cybersecurity and Data Protection in Professional Education", which was developed

and tested in the educational process. The complex includes lecture notes, laboratory assignments, professionally oriented case studies, project and test tasks, learning materials for work in cyber ranges, and other educational and methodological resources available through the LMS Moodle learning management system. The result of the study can be used to modernize the professional training of future digital technology specialists in higher education institutions.

Keywords: digital technologies, digital transformation, specialist training, educational process, digital competence, practical training, data protection, cybersecurity, pedagogical methods, educational technologies, adaptive learning, practical skills, digital technology specialists, digital security, training system.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, у яких опубліковано основні наукові результати дисертації

1. Шимків, Н. І. (2024). Актуальні проблеми захисту даних у процесі підготовки майбутніх фахівців цифрових технологій в умовах цифрової трансформації професійної освіти. *НАУКОВІ ЗАПИСКИ*, (157), 111–118. https://doi.org/10.31392/nz-udu-157.2024.15
2. Франко, Ю., & Шимків, Н. (2025a). Основні положення практичної підготовки фахівців цифрових технологій у тенденціях сьогодення. *Вісник Національного університету «Чернігівський колегіум» імені Т. Г. Шевченка*, *189*(33), 145–152. https://doi.org/10.58407/visnik.253323
3. Шимків Н., & Кирчей Т (2025b). Вплив штучного інтелекту на специфіку підготовки фахівців в галузі цифрових технологій. *Проблеми інженерно-педагогічної освіти*, (85), 83–92. https://doi.org/10.26565/2074-8922-2025-85-07
4. Шимків, Н. І. (2025c). Застосування спеціалізованого програмного забезпечення захисту даних в освітньому процесі підготовки фахівців цифрових технологій. Наукові записки, 2(164), 159–166. https://doi.org/10.31392/nz-udu-164-2.2025.19

Наукові праці, які засвідчують апробацію матеріалів дисертації

5. Шимків, Н.І. (2025). Вплив війни на професійну освіту в україні: виклики та трансформації. *Моделі міждисциплінарних та міжгалузевих освітніх та освітньо-наукових програм в умовах воєнного стану: виклики та варіанти впровадження.* Матеріали V Міжнар. наук.-практ. конф. (Одеса, **1**0-12 жовтня 2025 р.). (С. 166–168). Одеса–Запоріжжя: АА Тандем.
6. *Шимків, Н. І. (2025). Розвиток компетентності фахівців цифрових технологій в умовах військового стану. У* Матеріали IX Всеукраїнської науково-практичної конференції з міжнародною участю «Теоретико-

методологічні основи розвитку освіти та управлінської діяльності» (с. 357–360). Херсон, Україна.

7. Шимків, Н. І. (2026). Захист даних у сучасній професійній освіті. *Crosspoint: Scientific Almanac*, *2*, 166–168. IV Scientific Conference-Forum *United Perspectives 24/7* within the Ernst Lortikyan International Scientific Project Global Creative Ideas Forum 5.0
8. Шимків, Н. І. (2026). Актуальність вивчення захисту даних у сучасній освіті. *Креативний простір, 41*, 10–12. Матеріали VII Міжнародної науково-практичної конференції «Креативна трансформація та модернізація сучасної освіти» (5-7 червня 2026р.)
9. Шимків, Н. І. (2026). Захист даних у професійній підготовці фахівців цифрових технологій. У Proceedings of the 3rd International Scientific and Practical Conference «The Future of Science: Emerging Research and Technological Innovations» (pp. 335–337). Helsinki, Finland.

Опубліковані праці, які додатково відображають наукові результати дисертації

10. Шимків, Н. І. (б. д.). *Захист даних* [Електронний курс]. Сервер електронного навчання Тернопільського національного педагогічного університету імені Володимира Гнатюка. https://elr.tnpu.edu.ua/course/view.php?id=5517

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 16

ВСТУП 17

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ПІДГОТОВКИ ФАХІВЦІВ ЦИФРОВИХ ТЕХНОЛОГІЙ ДО ЗАСТОСУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ДАНИХ 27

1.1 Сучасний стан проблеми захисту даних у професійній діяльності фахівців цифрових технологій 27

1.2 Теоретичні засади професійної підготовки фахівців цифрових технологій у контексті забезпечення кібербезпеки та захисту даних 42

1.3 Компетентнісний підхід до підготовки фахівців цифрових технологій щодо застосування програмного забезпечення захисту даних 53

1.4 Аналіз програмного забезпечення захисту даних та особливостей його використання у професійній діяльності 61

Висновки до розділу 1 78

РОЗДІЛ 2. РОЗРОБКА МЕТОДИКИ ПІДГОТОВКИ ФАХІВЦІВ ДО ЗАСТОСУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ДАНИХ 80

2.1. Методичні засади формування готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних 80

2.2. Концептуальні положення та принципи розроблення методики підготовки фахівців цифрових технологій 99

2.3. Педагогічні умови формування готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних 106

2.4. Структурно-функціональна модель підготовки фахівців цифрових технологій 121

2.5. Методичне забезпечення підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних 133

Висновки до розділу 2 152

РОЗДІЛ 3 ЕКСПЕРИМЕНТАЛЬНА ПЕРЕВІРКА ЕФЕКТИВНОСТІ МЕТОДИКИ ПІДГОТОВКИ ФАХІВЦІВ 155

3.1. Організація та етапи педагогічного експерименту 155

3.2. Критерії, показники та рівні сформованості готовності до застосування програмного забезпечення захисту даних 161

3.3 Аналіз результатів педагогічного експерименту 168

3.4. Статистична обробка результатів дослідження та інтерпретація даних 172

Висновки до розділу 3……199
ВИСНОВКИ 202
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 208
ДОДАТКИ..... .226

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

LLM – Large Language Model (велика мовна модель)

ШІ – Штучний інтелект

ІТ – інформаційні технології

ОПП – Освітньо-професійна програма

ПЗ – програмне забезпечення

НПА – нормативно-правові акти

ПЗЗД – програмне забезпечення захисту даних

ЕНМК – електронний навчально-методичнй комплекс

ВСТУП

Обґрунтування вибору теми дослідження. Сучасний етап розвитку цифрового суспільства характеризується стрімким поширенням інформаційно-комунікаційних технологій, зростанням обсягів даних, активним впровадженням штучного інтелекту, хмарних обчислень, технологій великих даних (Big Data) та цифрових платформ у всі сфери суспільного життя. Відповідно до концепції Industry 5.0, ключовими чинниками розвитку економіки, виробництва та освіти стають цифровізація, людиноцентричність, безпечність і стійкість інформаційних систем. За таких умов особливого значення набуває проблема забезпечення захисту даних як одного з визначальних чинників стабільного функціонування підприємств, організацій, державних установ та суспільства загалом.

Сучасний розвиток інформаційно-комунікаційних систем супроводжується постійним зростанням кількості, складності та інтенсивності кіберзагроз. Використання зловмисниками технологій штучного інтелекту, автоматизованих систем аналізу даних, інструментів соціальної інженерії та шкідливого програмного забезпечення створює нові виклики для забезпечення інформаційної безпеки. У зв’язку з цим суттєво зростають вимоги до професійної підготовки фахівців цифрових технологій, які повинні не лише володіти сучасними цифровими інструментами, а й бути здатними ефективно застосовувати програмне забезпечення захисту даних у професійній діяльності.

Науково-педагогічна проблема дослідження полягає у необхідності подолання невідповідності між сучасними вимогами цифрового суспільства, ринку праці та системи навчання щодо забезпечення інформаційної безпеки і недостатнім рівнем теоретико-методичного забезпечення підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних у професійній діяльності.

Водночас у системі вищої освіти недостатньо розробленими залишаються теоретичні засади формування готовності майбутніх фахівців цифрових

технологій до використання сучасного програмного забезпечення захисту даних, не визначено цілісної структури такої готовності, педагогічних умов її формування, критеріїв та показників оцінювання, а також ефективних форм, методів і засобів професійної підготовки.

Актуальність проблеми підтверджується положеннями Законів України «Про освіту» (2017), «Про вищу освіту» (2014), «Про професійну освіту» (2025), «Про основні засади забезпечення кібербезпеки України» (2017), Стратегії кібербезпеки України (2021), Концепції розвитку цифрових компетентностей (2021), а також стратегічними документами Європейського Союзу (European Commission, 2020) (European Parliament & Council of the European Union, 2022) щодо цифрової трансформації освіти та розвитку цифрових компетентностей. У зазначених документах наголошується на необхідності формування у майбутніх фахівців компетентностей із безпечного використання цифрових технологій та забезпечення захисту інформаційних ресурсів.

Аналіз наукових джерел засвідчив значний інтерес учених до проблем цифровізації освіти, професійної підготовки майбутніх фахівців цифрових технологій, розвитку цифрової компетентності та формування компетентностей у сфері кібербезпеки. Теоретичні засади цифрової трансформації освіти та розвитку цифрової компетентності розкрито у працях В. Ю. Бикова(2017), О. М. Спіріна(2020), Н. В. Морзе (2019), В. П. Олексюка(2024), С. О. Семерікова(2025) Семеніхіна (2025), Гевко (2025), Потапчук (2025) та Кобися (2022) та інших науковців. Питання цифрової трансформації професійної освіти, розвитку інформаційно-цифрової компетентності та підготовки майбутніх фахівців до професійної діяльності в умовах цифрового суспільства досліджували Р. С. Гуревич, О. М. Трифонова, І. М. Шишенко та інші вчені.

Окремий напрям наукових досліджень присвячений питанням кібербезпеки та захисту інформації. Значний внесок у розвиток теоретичних і прикладних засад інформаційної безпеки зробили В. Л. Бурячок (2018), В. П. Олексюк (2024), В. М. Богуш(2018), О. К. Юдін (2024) та інші науковці. У їхніх працях ґрунтовно досліджено питання кібербезпеки, криптографічного захисту

інформації, проєктування комплексних систем захисту даних, управління інформаційною безпекою та протидії сучасним кіберзагрозам.

Водночас результати аналізу наукових праць свідчать, що переважна більшість досліджень присвячена технічним, технологічним, організаційним і правовим аспектам захисту інформації. Значно меншою мірою розроблено педагогічний аспект підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних. Зокрема, недостатньо обґрунтовано структуру готовності майбутніх фахівців до використання програмних засобів захисту даних, не визначено педагогічні умови її формування, критерії та показники оцінювання, недостатньо розроблено зміст, форми, методи і засоби навчання, спрямовані на формування відповідних професійних компетентностей.

Проведений аналіз наукових джерел і сучасного педагогічного досвіду професійної підготовки майбутніх фахівці цифрових технологій уможливив виявлення низки суперечностей між:

– вимогами цифрового суспільства та ринку праці до рівня компетентності фахівців цифрових технологій у сфері інформаційної безпеки та недостатнім рівнем їхньої готовності до застосування програмного забезпечення захисту даних у професійній діяльності;

– потребою у забезпеченні належного рівня захисту даних в умовах цифровізації всіх сфер діяльності та недостатньою орієнтацією змісту професійної підготовки на формування практичних навичок використання сучасного програмного забезпечення захисту даних;

– стрімким розвитком технологій захисту інформації та повільним оновленням навчально-методичного забезпечення підготовки майбутніх фахівців цифрових технологій;

– необхідністю впровадження компетентнісного підходу до формування здатності майбутніх фахівців цифрових технологій забезпечувати інформаційну безпеку та недостатньою розробленістю методичного інструментарію для реалізації цього завдання в освітньому процесі;

– потребою закладів освіти у цілісній методиці підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних та недостатнім теоретичним обґрунтуванням і практичним впровадженням таких методик.

Виокремлені суперечності та сформульована проблема зумовили актуальність дослідження на тему: «**Методика підготовки фахівців цифрових технологій до застосування програмного забезпечення захисту даних».**

Тему дисертації затверджено вченою радою Тернопільського національного педагогічного університету імені Володимира Гнатюка (протокол № 11 від 27 січня 2026 р.).

Дисертаційне дослідження виконано відповідно до тематичного плану наукової діяльності Тернопільського національного педагогічного університету імені Володимира Гнатюка та є складовою науково-дослідної теми «Теоретико-методологічні засади модернізації освіти і практичні аспекти застосування цифрових технологій у професійній підготовці фахівців» (номер державної реєстрації 0126U001854).

Тема дисертації відповідає напрямам зазначеного наукового дослідження, оскільки спрямована на теоретичне обґрунтування та розроблення методики підготовки фахівців цифрових технологій до застосування програмного забезпечення захисту даних у професійній діяльності. Результати дослідження сприяють удосконаленню професійної підготовки майбутніх фахівців в умовах цифровізації освіти, розвитку інформаційної безпеки та впровадження сучасних цифрових технологій у освітній процес.

Дослідження виконано відповідно до пріоритетних напрямів розвитку цифрової освіти, визначених законодавчими та нормативними документами України у сфері освіти, цифрової трансформації та кібербезпеки.

Результати дослідження спрямовані на вдосконалення професійної підготовки майбутніх фахівців цифрових технологій шляхом розроблення та впровадження методики формування компетентностей із застосування програмного забезпечення захисту даних. Робота відповідає сучасним

тенденціям цифровізації освіти, розвитку кібербезпеки та забезпечення інформаційної безпеки в освітньому й професійному середовищах.

Об’єкт дослідження: підготовка майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних у професійній діяльності.

Предмет дослідження: методика підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних у професійній діяльності.

Мета дослідження: теоретично обґрунтувати і розробити методику підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних у професійній і освітній діяльності.

Для вирішення мети дисертації було поставлено наступні завдання:

1. Дослідити стан проблеми підготовки фахівців цифрових технологій в сфері інформаційної безпеки у науковій літературі, нормативно-правових актах та обґрунтувати доцільність використання програмного забезпечення захисту даних у професійній діяльності майбутніх фахівців цифрових технологій.
2. Обґрунтувати структуру готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних.
3. Виявити й теоретично обґрунтувати педагогічні умови та розробити структурно-функціональну модель методики підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних.
4. Експериментально перевірити ефективність запропонованої методики підготовки фахівців цифрових технологій до застосування програмного забезпечення захисту даних.

Для досягнення мети та розв’язання поставлених завдань дослідження було використано комплекс взаємопов’язаних методів дослідження.

Теоретичні методи: аналіз, синтез, порівняння, систематизація та узагальнення філософської, психолого-педагогічної, методичної та спеціальної літератури з проблем професійної підготовки фахівців цифрових технологій, цифровізації освіти, інформаційної безпеки та застосування програмного

забезпечення захисту даних; термінологічний аналіз – для уточнення сутності ключових понять дослідження; моделювання – для розроблення структурно-функціональної моделі підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних; системний та компетентнісний аналіз – для визначення компонентів, критеріїв, показників і рівнів сформованості готовності здобувачів освіти.

Емпіричні методи: педагогічне спостереження – для вивчення особливостей навчальної діяльності студентів у процесі професійної підготовки; анкетування та опитування – для визначення рівня мотивації, ставлення до використання програмного забезпечення захисту даних і самооцінювання сформованості відповідних компетентностей; бесіда – для уточнення результатів діагностування; тестування – для оцінювання рівня теоретичних знань із питань інформаційної безпеки та програмного забезпечення захисту даних; аналіз результатів виконання лабораторних робіт, практичних завдань, індивідуальних проєктів і навчально-методичних розробок студентів – для визначення рівня сформованості практичних вмінь; педагогічний експеримент (констатувальний, формувальний і контрольний етапи) – для перевірки ефективності запропонованої моделі та педагогічних умов підготовки майбутніх фахівців цифрових технологій.

Методи математичної статистики: кількісний і якісний аналіз результатів експериментальної роботи; обчислення середніх значень, відсоткових показників та показників приросту; перевірка статистичної значущості відмінностей між результатами контрольної та експериментальної груп; графічна та таблична інтерпретація результатів дослідження – для наочного представлення отриманих даних та підтвердження ефективності розробленої моделі підготовки.

Застосування зазначеного комплексу методів забезпечило об’єктивність, наукову достовірність і вірогідність результатів дослідження, а також дало змогу всебічно вивчити процес формування готовності майбутніх фахівців цифрових

технологій до застосування програмного забезпечення захисту даних у професійній діяльності.

Експериментальна перевірка методики, що дозволяє проаналізувати рівень підготовки фахівців професійної освіти в галузі цифрових технологій до вирішення практичних завдання протистояння реальним загрозам та захисту даних.

Експериментальна база дослідження. Експериментальною базою дослідження обрано Тернопільський національний педагогічний університет імені Володимира Гнатюка та Рівненський державний гуманітарний університет. На різних 3 етапах у дослідженні брали участь 122 здобувачів освіти, які навчалися за спеціальністю 015 Професійна освіта, спеціалізацією 015.39 Цифрові технології.

Наукова новизна

вперше:

–*розроблено* структурно-функціональну модель підготовки майбутніх фахівців спеціальності 015 Професійна освіта, спеціалізації 015.39 Цифрові технології до застосування програмного забезпечення захисту даних, яка ґрунтується на взаємозв'язку методологічного, змістового, організаційно-процесуального, результативного блоків та педагогічних умов.

–*обґрунтовано* педагогічні умови підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних, зокрема: формування стійкої мотивації до використання засобів захисту інформації у професійній діяльності; оновлення змісту підготовки відповідно до сучасних тенденцій розвитку кібербезпеки; забезпечення практико-орієнтованого навчання із використанням спеціалізованого програмного забезпечення; інтеграція засобів захисту даних у зміст фахових дисциплін та цифрового освітнього середовища; залучення здобувачів освіти до проєктної, дослідницької та рефлексивної діяльності;

– *розроблено та реалізовано* методику підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних,

яка передбачає комплексне використання лабораторних робіт, кейс-методу, проєктного навчання, кіберполігонів і віртуальних лабораторій з урахуванням педагогічної специфіки спеціальності 015 Професійна освіта, спеціалізації 015.39 Цифрові технології;

- *удосконалено:* зміст професійної підготовки майбутніх фахівців цифрових технологій шляхом інтеграції сучасного програмного забезпечення захисту даних (Wireshark, Cisco Packet Tracer, VeraCrypt, Kali Linux, Splunk та ін.) у фахові дисципліни освітньої програми;

набули подальшого розвитку:

– теоретичні положення щодо професійної підготовки майбутніх фахівців цифрових технологій в умовах цифровізації освіти та зростання ролі інформаційної безпеки;

– наукові уявлення про структуру готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних, її компоненти, критерії, показники та рівні сформованості;

– методичні засади використання цифрових освітніх ресурсів, кіберполігонів, віртуальних лабораторій та спеціалізованого програмного забезпечення в процесі формування професійних компетентностей майбутніх педагогів цифрового профілю.

Практичне значення одержаних результатів полягає у розробленні та впровадженні методики підготовки майбутніх фахівців спеціальності 015 Професійна освіта, спеціалізації 015.39 Цифрові технології до застосування програмного забезпечення захисту даних у професійній та освітній діяльності. Розроблені теоретичні положення, структурно-функціональна модель, педагогічні умови та методичне забезпечення можуть бути використані в закладах вищої освіти під час модернізації змісту професійної підготовки майбутніх фахівців цифрових технологій.

Практичну цінність становлять розроблені навчально-методичні матеріали, зокрема лабораторні роботи із застосуванням програмного забезпечення Wireshark, Cisco Packet Tracer, VeraCrypt, Kali Linux та інших

засобів захисту даних, професійно орієнтовані кейси, проєктні завдання, матеріали для роботи у віртуальних лабораторіях і кіберполігонах, а також рекомендації щодо їх інтеграції у навчальний процес. Запропоновані матеріали можуть використовуватися під час викладання дисциплін «Операційні системи», «Комп'ютерні мережі та захист даних», «Хмарні технології в навчальному процесі», «Інформаційна безпека», а також інших фахових освітніх компонентів.

Практичну цінність становить розроблений та апробований в освітньому процесі електроний навчально-методичний комплекс дисципліни «Кібербезпека та захист даних у професійній освіті», що включає конспекти лекцій, лабораторні роботи, кейс-методи, проєктні та тестові завдання, використання кіберполігонів, діагностичний інструментарій оцінювання результатів навчання та інші навчально-методичні матеріали, розміщені в системі управління навчанням LMS Moodle.

Результати дослідження можуть бути використані під час розроблення та оновлення освітніх програм, навчальних планів, робочих програм дисциплін, навчально-методичних комплексів, курсів підвищення кваліфікації педагогічних працівників, а також у процесі підготовки майбутніх фахівців цифрових технологій у закладах вищої освіти.

Особистий внесок здобувача. Усі представлені в дисертації наукові результати одержані автором самостійно та одноосібно. У працях, опублікованих у співавторстві, особистим внеском здобувача є: у праці (Шимків, & Франко, 2025) – проведено аналіз та виділено основні практичні навички студентів при вивченні захисту систем і мереж.; у праці (Шимків, & Кирчей, 2025) – теоретичне обґрунтування актуальності використання технологій штучного інтелекту та вплив на систему освіти в цілому, а акцент на вплив генеративних моделей на безпеку даних та академічну доброчесність при підготовці фахівців цифрових технологій в умовах трансформаційних процесів.

Апробація результатів дослідження. Основні результати дослідження обговорювалися та отримали позитивну оцінку на науково-практичних конференціях різного рівня, а саме:

– *міжнародних конференціях* – «Моделі міждисциплінарних та міжгалузевих освітніх та освітньо-наукових програм в умовах воєнного стану: виклики та варіанти впровадження» (Одеса; 2025), «The Future of Science: Emerging Research and Technological Innovations» (Хельсінкі, Фінляндія, 2026), «Креативна трансформація та модернізація сучасного суспільства» (м. Харків, Україна – м. Пул, Велика Британія, 2026), «United Perspectives 24/7» (Україна – Німеччина – Велика Британія – США, 2026).

– *всеукраїнських конференціях* – «Теоретико-методологічні основи розвитку освіти та управлінської діяльності» (Херсон, 2025);

Основні положення та результати дослідження обговорювалися й були схвалені на засіданнях кафедри комп'ютерних технологій Тернопільського національного педагогічного університету імені Володимира Гнатюка (2022–2026 рр.).

Публікації. Результати дослідження опубліковано в 10 наукових публікаціях автора (8 – одноосібні), з них 4 відображають основні наукові результати дисертації, 6 – апробаційного характеру та 1 публікація, яка додатково відображає наукові результати дисертації.

Структура та обсяг дисертації. Робота складається зі вступу, трьох розділів, висновків до розділів, загальних висновків, списку використаних джерел (159 найменування, з них 99 – іноземними мовами), додатків (10 на 22 сторінках). Загальний обсяг роботи становить 246 сторінок друкованого тексту, з них 190– основний текст. Роботу ілюстровано 14 таблицями та 19 рисунками.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ПІДГОТОВКИ ФАХІВЦІВ ЦИФРОВИХ ТЕХНОЛОГІЙ ДО ЗАСТОСУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ДАНИХ

1.1 Сучасний стан проблеми захисту даних у професійній діяльності фахівців цифрових технологій

У сучасних умовах цифровізації суспільства проблема захисту даних набуває особливої актуальності для фахівців цифрових технологій, професійна діяльність яких безпосередньо пов’язана зі створенням, обробкою, передаванням та зберіганням інформації. Стрімке зростання обсягів даних, поширення хмарних сервісів, мобільних технологій, інтернету речей та штучного інтелекту сприяють розширенню можливостей для автоматизації процесів, але водночас підвищують ризики несанкціонованого доступу до інформаційних ресурсів. Кібератаки, витоки конфіденційних даних, шкідливе програмне забезпечення та соціальна інженерія стають серйозними викликами для організацій різних сфер діяльності. У зв’язку з цим захист даних розглядається не лише як технічна проблема, а як важливий складник професійної компетентності сучасного фахівця у сфері цифрових технологій.

Аналіз сучасного стану проблеми свідчить про зростання вимог роботодавців до рівня підготовки майбутніх фахівців щодо забезпечення інформаційної безпеки та використання спеціалізованого програмного забезпечення захисту даних. Сучасний ринок праці потребує фахівців, які володіють знаннями про криптографічні методи захисту інформації, системи резервного копіювання, антивірусне програмне забезпечення, мережеву безпеку та засоби контролю доступу. Водночас результати наукових досліджень і практика підготовки здобувачів освіти свідчать про недостатній рівень сформованості відповідних вмінь у частини студентів, що обумовлює необхідність удосконалення змісту професійної підготовки. Особливої уваги

потребує формування практичних навичок використання сучасного програмного забезпечення захисту даних у реальних професійних ситуаціях, що забезпечить готовність майбутніх фахівців цифрових технологій до ефективної діяльності в умовах зростаючих кіберзагроз.

Незважаючи на поступове зниження кількості заяв у 2025 році на спеціальності пов’язані з ІТ-сферою приблизно 10% порівняно з 2024 роком, цифрові технології на даний момент залишаються серед одних із популярних напрямків. Майбутні здобувачі освіти почали дедалі реалістичніше оцінювати конкуренцію на ринку праці.

Найпопулярніші спеціальності за даними офіційного порталу ДП «Інфоресурс» (2025) по кількості заяв.

- -015.39 Цифрові технології
- -014.09 Середня освіта (Інформатика)
- -121 «Інженерія програмного забезпечення»;
- -122 «Комп’ютерні науки»;
- -125 «Кібербезпека та захист інформації» (стабільно зростає через виклики військово стану).

При підготовці сучасного фахівця мають враховуватися не лише виклики воєнного стану та розвитку ІТ-сфери, а й вимоги до сучасних цифрових технологій, які активно впроваджуються в сфері цифрових технологій, штучного інтелекту (ШІ) і введення нових стандартів.

Адже ШІ не вважається забороненим інструментом, а розглядається, як своєрідна допоміжна система, який дозволяє використовувати (LLM) для аналітики, написання коду та тестування. Більшість сучасних освітніх програм зорієнтовані на роботу з вебсервісами та на роботу в браузерному режимі, не використовуючи технічні ресурси користувача та використовують хмарні сервіси. Більшість сучасних освітніх програм акцентують увагу на основних загрозах, які можуть бути викликані застосуванням ШІ та можливий вплив на безпеку даних.

Також відбувається активне оцінювання закладами освіти сертифікатів здобувачів освіти про проходження курсів від провідних ІТ-компаній (Microsoft, Intel, Coursera).

Також одним із найважливіших аспектів у 2025 році є не просто знання програмного забезпечення, а й навички та готовність до безперервної роботи в програмному середовищі. Також важливо виділити вміння працювати в сфері аналітики та використовувати навички аналізу щоб працювати з великими масивами неструктурованих даних.

Сучасний напрямок підготовки фахівців цифрових технологій формується на основі глобальних цифрових трансформацій, що викликає потребу в актуальних вміннях та навичках.

Виділимо сучасні вимоги на які акцентується увага при розробці сучасних освітніх програм:

- Гнучкість та адаптивність сучасних програм адже актуальна програма не може бути сталою, а повинна розвиватися та удосконалюватися під сучасні тенденції розвитку технологій. Частково можна розглядати впровадження в освітній процес сучасних сертифікованих курсів від популярних ІТ-компаній, що дозволяє реалізувати практичну складову ОПП.
- Практикоорієнтованість та проєктне навчання – подача теоретичного матеріалу у процесі навчання без проведення лабораторно-практичних занять – це даремно витрачений час, що не дає конкретних результатів. Також варто розглядати поєднання навчання із практичними завданнями на основі реальних задач.
- Впровадження штучного інтелекту – одне із спірних питань у сучасній освіті загалом адже використання ШІ як інструменту, що дозволяє спростити освітній процес, як і викладачам так і здобувачам несе за собою наслідки для захисту даних. Основа використання генеративних моделей має полягати у вмінні їх використовувати, а також поєднує в собі етичні аспекти їх застосування при виконанні завдань.

- Командна роботи та розвиток навичок – вміння працювати над складними завданнями у команді, делегування завдань, робота над спільними проектами, що також дозволяє правильно виконувати свій спектр робіт.

- Сучасна дисципліна в сфері підготовки фахівців цифрових технологій це не лише перелік дисциплін, а й поєднання фундаментальних знань та прикладного програмного забезпечення, що дозволяє логічно вибудувати структуру підготовки професійної підготовки цифрових технологій (рис. 1.1).

Рис. 1.1 Основні компоненти професійної підготовки фахівців цифрових технологій

Відповідно до стандарту вищої освіти України першого (бакалаврського) рівень, галузі знань 01 – «Освіта / Педагогіка», спеціальності 015 – «Професійна освіта (за спеціалізаціями)» (Міністерство освіти і науки України, 2019) підготовка здобувачів освіти спрямована на формування компетентностей, необхідних для здійснення як професійно-педагогічної діяльності, так і діяльності у сфері цифрових технологій. Такий підхід забезпечує поєднання педагогічної та фахової підготовки, орієнтуючи майбутніх фахівців не лише на викладання спеціальних дисциплін, а й на ефективне застосування сучасних

цифрових технологій у професійній діяльності. Освітні програми передбачають формування загальних і спеціальних (фахових) компетентностей, пов’язаних із використанням комп’ютерних систем і мереж, програмування, розроблення цифрових продуктів, адміністрування інформаційних ресурсів та забезпечення захисту інформації.

Особливого значення набувають програмні результати навчання, які орієнтують здобувачів освіти на здатність застосовувати сучасні програмні та апаратні засоби для розв’язання професійних завдань, використовувати технології адміністрування мереж і баз даних, здійснювати моніторинг інформаційних систем та забезпечувати їхній захист від зовнішніх і внутрішніх загроз. Крім того, випускник повинен уміти аналізувати стан інформаційної безпеки, застосовувати нормативно-правові вимоги щодо захисту інформації та використовувати спеціалізоване програмне забезпечення для забезпечення конфіденційності, цілісності та доступності даних. Вказані результати навчання відображають сучасні вимоги до професійної підготовки фахівців цифрових технологій в умовах цифрової трансформації суспільства та постійного зростання кіберзагроз.

Водночас аналіз змісту освітніх програм і практики підготовки здобувачів освіти показує, що формування зазначених компетентностей потребує посилення практичної складової навчання. Незважаючи на наявність дисциплін, пов’язаних із комп’ютерними мережами, інформаційними системами та кібербезпекою, студенти часто отримують переважно теоретичні знання, які не завжди забезпечують готовність до використання сучасного програмного забезпечення захисту даних у реальних професійних ситуаціях. Це обумовлює необхідність удосконалення методики професійної підготовки майбутніх фахівців цифрових технологій шляхом цілеспрямованого формування практичних навичок використання антивірусних систем, засобів резервного копіювання, криптографічного захисту інформації, систем контролю доступу та інших інструментів кібербезпеки.

Аналіз стандарту вищої освіти України першого (бакалаврського) рівень, галузі знань 01 – «Освіта / Педагогіка», спеціальності 015 – «Професійна освіта (за спеціалізаціями)» (Міністерство освіти і науки України, 2019) та освітньо-професійних програм спеціальності 015 Професійна освіт», спеціалізації 015.39 Цифрові технології свідчить про наявність низки компетентностей і програмних результатів навчання, безпосередньо пов’язаних із кібербезпекою, захистом даних, комп’ютерними мережами та інформаційними системами. Зокрема, серед фахових компетентностей важливе місце займають здатність використовувати сучасні інформаційно-комунікаційні технології у професійній діяльності, проєктувати та адмініструвати комп’ютерні системи і мережі, здійснювати налаштування програмного забезпечення, забезпечувати надійність функціонування інформаційних ресурсів та дотримуватися вимог інформаційної безпеки. Такі компетентності формують основу для професійної діяльності майбутніх фахівців цифрових технологій, оскільки передбачають не лише технічне володіння цифровими інструментами, а й усвідомлення ризиків, пов’язаних із зберіганням, обробкою та передаванням даних.

Крім того, випускник повинен уміти аналізувати стан інформаційної безпеки, застосовувати нормативно-правові вимоги щодо захисту інформації та використовувати спеціалізоване програмне забезпечення для дотримання конфіденційності, цілісності та доступності даних. Вказані програмні результати навчання відображають сучасні вимоги до професійної підготовки фахівців цифрових технологій в умовах цифрової трансформації суспільства та постійного зростання кіберзагроз.

Отже, аналіз компетентностей і програмних результатів навчання спеціальності 015 Професійна освіта, спеціалізації 015.39 Цифрові технології підтверджує необхідність підготовки майбутніх фахівців до професійного використання програмного забезпечення захисту даних. Саме це визначає актуальність дослідження методичних засад формування відповідних знань, вмінь і навичок у процесі професійної підготовки здобувачів освіти, що є

важливою передумовою забезпечення їхньої конкурентоспроможності та готовності до діяльності в умовах сучасного цифрового середовища.

Сильною стороною стандарту є його практична спрямованість. Значна увага приділяється виробничій практиці, дуальній формі навчання та розвитку практичних навичок. Також стандарт враховує цифрову трансформацію освіти і вимагає від майбутніх педагогів володіння сучасними цифровими інструментами.

Водночас аналіз показує суттєві недоліки в частині підготовки з питань кібербезпеки та захисту даних. Теми захисту інформації присутні в стандарті, але носять переважно загальний характер і не мають достатнього обсягу. У результаті випускники отримують поверхневі знання з кібергігієни, але часто недостатньо підготовлені до реальних загроз, роботи з професійними інструментами захисту даних та формування культури безпеки в майбутніх фахівців.

Крім того, стандарт недостатньо чітко визначає вимоги до цифрової компетентності самих викладачів, які мають навчати студентів. Відсутність обов’язкових обсягів годин на практичну роботу з інструментами аналізу трафіку, криптографії та виявлення вразливостей не дозволяє забезпечити належний рівень готовності майбутніх педагогів до роботи в умовах сучасних кіберзагроз.

Таким чином, чинний стандарт вищої освіти спеціальності 015 Професійна освіта, спеціалізації 015.39 Цифрові технології є досить сучасним за загальною концепцією, проте потребує суттєвого посилення блоку кібербезпеки та захисту даних, а також чіткішої інтеграції практичної підготовки з використанням сучасних інструментів і технологій.

Стандарт вищої освіти зі спеціальності 015 Професійна освіта, спеціалізації 015.39 Цифрові технології висуває високі вимоги до викладача, зумовлені дуальним характером підготовки. Викладач повинен одночасно виступати як педагог і як висококваліфікований фахівець у сфері цифрових технологій. Це передбачає наявність глибоких знань як у галузі педагогіки та

психології професійної освіти, так і в технічних дисциплінах – комп'ютерних мережах, програмуванні, базах даних та захисту інформації.

Особливе місце в стандарті посідає вимога щодо цифрової компетентності викладача. Він має не лише володіти сучасними цифровими інструментами, а й уміти ефективно інтегрувати їх у навчальний процес, організовувати практичну підготовку студентів і формувати у них професійні компетентності. Важливим є також розвиток у викладача здатності працювати з хмарними технологіями, віртуальними лабораторіями та елементами штучного інтелекту.

Щодо компетентностей у сфері кібербезпеки та захисту даних, стандарт містить загальні вимоги, але не визначає їх достатньо чітко та конкретно. У результаті викладач повинен розуміти основи захисту інформації, загрози кібербезпеки та методи їх протидії, однак рівень цих знань не регламентований. Це призводить до ситуації, коли багато викладачів мають лише поверхневе уявлення про актуальні інструменти та загрози, що негативно впливає на якість підготовки майбутніх педагогів.

Крім того, стандарт акцентує необхідність постійного професійного розвитку викладача, оскільки швидкі зміни в IT-сфері вимагають регулярного оновлення знань і навичок. Однак механізми забезпечення цього розвитку на рівні стандарту залишаються недостатньо прописаними.

Таким чином, вимоги до викладача спеціальності 015 Професійна освіта, спеціалізація 015.39 Цифрові технології є прогресивними за своєю суттю, оскільки передбачають подвійну компетентність і високий рівень цифрової підготовки. Водночас вони потребують суттєвого уточнення та посилення, особливо в частині кібербезпеки, захисту персональних даних та практичних навичок роботи з сучасними інструментами інформаційної безпеки.

Стандарт вищої освіти зі спеціальності 015 Професійна освіта, спеціалізації 015.39 Цифрові технології (Міністерство освіти і науки України, 2021) містить вимоги до підготовки з питань кібербезпеки, проте вони мають переважно загальний характер і не відрізняються високою конкретизацією.

У даному стандарті кібербезпека розглядається як складова цифрової компетентності педагога. Передбачається, що випускник повинен мати уявлення про основні загрози інформаційній безпеці, розуміти принципи захисту персональних даних, а також володіти базовими навичками забезпечення безпеки в комп'ютерних мережах. Зокрема, стандарт вимагає формування вміння використовувати основні засоби захисту інформації, дотримуватися правил кібергігієни та навчати цьому здобувачів.

Однак детальний аналіз нормативного документа показує, що вимоги до кібербезпеки залишаються поверховими. У стандарті відсутні чіткі обсяги кредитів на вивчення цієї тематики, не визначено обов'язковий перелік інструментів (наприклад, Wireshark, VeraCrypt, Nmap), не встановлено мінімальний рівень практичних навичок з тестування на проникнення чи аналізу трафіку. Більшість компетентностей сформульовані у вигляді загальних формулювань («розуміє», «знає основи», «має уявлення»), що ускладнює їх об'єктивну оцінку.

Особливо слабко представлена педагогічна складова кібербезпеки. Стандарт не вимагає від випускника вміння розробляти навчальні матеріали з кібергігієни, проводити уроки з захисту даних для здобувачів або формувати в них культуру інформаційної безпеки. Це є суттєвим недоліком, оскільки майбутній педагог повинен не лише сам володіти навичками захисту даних, а й ефективно передавати ці знання здобувачам освіти.

Таким чином, вимоги стандарту до кібербезпеки є недостатньо розвиненими і не відповідають реальним викликам цифрової трансформації професійної освіти. Вони потребують суттєвого уточнення, збільшення обсягу практичної підготовки та обов'язкового включення педагогічної складової, що дозволить підготувати випускників, здатних якісно формувати культуру кібербезпеки в закладах професійної освіти.

Сучасний міжнародний досвід свідчить про активне впровадження технологій штучного інтелекту в систему професійної освіти. У Великій Британії платформа Century Tech успішно застосовується в технічних коледжах для

створення індивідуальних навчальних траєкторій, постійного аналізу прогресу студентів і адаптації навчального матеріалу. У Німеччині та Нідерландах у рамках дуальної освіти використовуються інтелектуальні симулятори та віртуальні лабораторії, які дозволяють студентам набувати практичних навичок у безпечному середовищі. У Сінгапурі та Південній Кореї ШІ широко застосовується для підготовки ІТ-фахівців, зокрема для симуляції виробничих процесів і автоматизованої оцінки компетентностей.

В Україні використання ШІ-технологій у професійній освіті має переважно фрагментарний характер. Окремі заклади освіти застосовують інструменти Google Gemini, ChatGPT та Microsoft Copilot для генерації презентацій, тестів і практичних завдань. Національна платформа Prometheus (ГО «Прометеус», 2026) використовує елементи машинного навчання для рекомендації курсів і аналізу успішності. Однак системного впровадження ШІ у професійну підготовку здобувачів на державному рівні ще не відбулося.

Порівняльний аналіз показує, що найефективніші моделі використання ШІ в професійній освіті ґрунтуються на гібридному підході, де штучний інтелект виступає не заміною викладача, а потужним інтелектуальним помічником. Найкращі результати досягаються при поєднанні технологій з практичною підготовкою, персоналізацією навчання та збереженням ролі викладача як наставника і фасилітатора.

Водночас український досвід вирізняється низьким рівнем системності, недостатнім технічним оснащенням закладів і обмеженою цифровою компетентністю викладачів. Це зумовлює необхідність розробки власної національної моделі інтеграції ШІ-технологій у професійну освіту, яка враховувала б специфіку фахових коледжів і вимоги сучасного ринку праці.

Використання технологій штучного інтелекту в процесі професійної підготовки студентів фахових коледжів породжує комплекс серйозних етичних проблем, які тісно переплітаються з питаннями захисту даних і кібербезпеки.

Однією з ключових етичних загроз є збір і використання персональних даних студентів генеративними моделями. ШІ-системи постійно аналізують

навчальну діяльність, поведінку, темп засвоєння матеріалу та емоційний стан. У контексті спеціальності 015 «Професійна освіта», спеціалізації 015.39 «Цифрові технології» це створює парадокс: студенти вивчають принципи захисту даних і кібербезпеки, але самі стають об’єктами інтенсивного цифрового моніторингу (Шимків & Кирчей, 2025). Відсутність прозорої згоди, чітких правил зберігання та захисту такої інформації може призвести до витоків даних або їх неправомірного використання.

Друга важлива проблема – упередженість алгоритмів і ризик дискримінації. Моделі ШІ, навчені на історичних даних, часто відтворюють соціальні, гендерні чи професійні стереотипи (Шимків & Кирчей, 2025). У професійній освіті це може проявлятися в упередженому оцінюванні здобутків здобувачів, рекомендаціях щодо кар’єрного розвитку або генерованих навчальних матеріалах, що порушує принципи рівності та справедливості.

Третя суттєва загроза стосується кібербезпеки навчального середовища. Використання генеративних моделей (ChatGPT, Gemini, Claude) створює нові вектори атак: витік конфіденційної інформації через промпти, інференційні атаки, отруєння даних для навчання моделей та зловживання ШІ для створення шкідливого контенту. Викладачі та здобувачів, які активно працюють з ШІ, часто не усвідомлюють цих ризиків, що підвищує вразливість як їх самих, так і закладів освіти.

Не менш важливим є ризик втрати критичного мислення та академічної доброчесності (Шимків & Кирчей, 2025). Легкість генерації контенту штучним інтелектом може призвести до того, що студенти перестануть самостійно аналізувати інформацію, розробляти рішення та нести відповідальність за результати своєї роботи. У майбутньому це загрожує формуванням фахівців, які не готові до реальних викликів кібербезпеки.

Крім того, виникає проблема відповідальності за якість організації освітнього процесу. Якщо навчальний матеріал, створений ШІ, містить помилки, рекомендації, що порушують захист даних, або сприяє кіберзагрозам, хто несе відповідальність - розробник моделі, викладач чи заклад освіти?

Таким чином, етичні аспекти використання штучного інтелекту в професійній освіті тісно пов’язані з питаннями захисту персональних даних і кібербезпеки. Формування етичної культури роботи з ШІ, розвміння ризиків витоку інформації та відповідального ставлення до кібербезпеки повинно стати невід’ємною частиною підготовки майбутніх педагогів спеціальності 015 «Професійна освіта», спеціалізація 015.39 «Цифрові технології».

Сучасний етап розвитку інформаційного суспільства характеризується стрімким поширенням цифрових технологій у всіх сферах життєдіяльності людини. Цифровізація економіки, державного управління, освіти, науки та виробництва зумовлює зростання потреби у висококваліфікованих фахівцях, здатних ефективно використовувати цифрові інструменти, розробляти програмні продукти, адмініструвати інформаційні системи, забезпечувати кібербезпеку та захист даних. У зв’язку з цим особливої актуальності набуває проблема професійної підготовки фахівців цифрових технологій у закладах освіти.

Розвиток цифрової економіки сприяє трансформації вимог до професійної компетентності майбутніх фахівців. Сучасний ринок праці потребує не лише ґрунтовних знань із програмування, комп’ютерних мереж чи баз даних, а й сформованих навичок роботи з хмарними сервісами, технологіями штучного інтелекту, засобами аналізу великих масивів даних, цифровими платформами та програмним забезпеченням для забезпечення інформаційної безпеки. Тому система вищої освіти повинна оперативно реагувати на виклики цифрової трансформації та забезпечувати підготовку конкурентоспроможних фахівців відповідно до сучасних вимог роботодавців (Work.ua, 2026).

В Україні підготовка фахівців цифрового профілю здійснюється за низкою спеціальностей галузі знань 12 «Інформаційні технології», зокрема за спеціальностями 121 «Інженерія програмного забезпечення», 122 «Комп’ютерні науки», 123 «Комп’ютерна інженерія», 126 «Кібербезпека та захист інформації», 126 «Інформаційні системи та технології», а також за спеціальністю 015 Професійна освіта, спеціалізацією 015.39 Цифрові технології. Особливістю підготовки майбутніх педагогів професійного навчання цифрового профілю є

поєднання інженерно-технічної та психолого-педагогічної складових, що забезпечує формування як фахових, так і методичних компетентностей.

Аналіз освітньо-професійних програм закладів вищої освіти свідчить, що підготовка фахівців цифрових технологій орієнтована на формування інтегральної, загальних та спеціальних компетентностей, визначених стандартами вищої освіти. Значна увага приділяється вивченню дисциплін, пов'язаних із програмуванням, комп'ютерними мережами, вебтехнологіями, інформаційними системами, цифровим дизайном, базами даних та технологіями розробки програмного забезпечення. Водночас питання захисту даних та практичного використання спеціалізованого програмного забезпечення інформаційної безпеки часто розглядаються фрагментарно або в межах окремих навчальних модулів.

Суттєвий вплив на розвиток професійної підготовки фахівців цифрових технологій мають міжнародні рамки цифрових компетентностей. Зокрема, європейська рамка цифрових компетентностей громадян DigComp (European Commission, Joint Research Centre, n.d.) абовизначає ключові напрями формування цифрової грамотності, серед яких окреме місце посідає безпека у цифровому середовищі. Для педагогічних працівників важливим орієнтиром виступає рамка DigCompEdu (Redecker, 2017), яка акцентує увагу на ефективному використанні цифрових технологій у професійній діяльності та освітньому процесі.

Аналіз наукових досліджень свідчить, що проблема професійної підготовки фахівців цифрового профілю перебуває у центрі уваги вітчизняних та зарубіжних вчених. У працях дослідників розглядаються питання цифрової трансформації освіти, формування цифрової компетентності, розвитку професійних компетентностей майбутніх фахівців інформаційної галузі, впровадження хмарних технологій, дистанційного навчання та інноваційних педагогічних технологій. Водночас питання методичної підготовки здобувачів освіти до застосування програмного забезпечення захисту даних потребує подальшого наукового обґрунтування.

Роботи Д. В. Дубова (2018) присвячені цифровій трансформації освіти та ролі кібербезпеки в підготовці педагогічних кадрів. Автор акцентує увагу на необхідності посилення практичної складової підготовки, проте основний фокус зроблено на загальних аспектах інформаційної безпеки.

Т. О. Коваль (2025) досліджує ризик-орієнтований підхід до захисту даних в освітньому середовищі, обґрунтовуючи важливість його впровадження в професійну підготовку фахівців. Однак у роботі недостатньо розкрито педагогічну складову формування готовності майбутніх викладачів.

О. М. Литвиненко (2003) розглядає питання захисту персональних даних у системах дистанційного навчання. його дослідження підкреслюють необхідність інтеграції кібергігієни в освітній процес, але здебільшого мають загальнотеоретичний характер і потребують конкретизації для спеціальності 015 Професійна освіта, спеціалізації 015.39 Цифрові технології.

Л. В. Барановська (2023) та О. В. Шаповал (2023) приділяють увагу формуванню цифрової компетентності педагогів, зокрема культурі кібергігієни. Автори наголошують на важливості підготовки викладачів до роботи з персональними даними студентів, проте їхні напрацювання стосуються переважно загальної середньої освіти й потребують адаптації до умов фахової передвищої освіти.

Я. Б. Сікора (2025) досліджує використання сучасних інструментів захисту даних у професійній підготовці педагогів. У її роботах розглядаються технічні аспекти застосування програмного забезпечення, однак педагогічна складова (розробка уроків, інструкцій, чек-листів) висвітлена недостатньо.

Сучасна підготовка фахівців цифрових технологій здійснюється із широким використанням цифрових освітніх ресурсів та платформ. У навчальному процесі активно застосовуються системи управління навчанням, хмарні сервіси, віртуальні лабораторії, симулятори комп’ютерних мереж, середовища програмування та спеціалізовані програмні комплекси. Це сприяє підвищенню практичної спрямованості навчання та наближенню освітнього процесу до реальних умов професійної діяльності.

Важливою тенденцією розвитку професійної освіти є посилення практикоорієнтованого підходу до навчання. Роботодавці висувають вимоги щодо наявності у випускників не лише теоретичних знань, а й сформованих практичних навичок використання сучасних цифрових технологій. У зв'язку з цим заклади вищої освіти розширюють співпрацю з ІТ-компаніями, впроваджують дуальні форми освіти, залучають студентів до виконання проєктних завдань та проходження виробничих практик.

Разом із позитивними тенденціями аналіз сучасного стану підготовки фахівців цифрових технологій дозволяє виокремити низку проблем. Серед них: недостатня інтеграція питань кібербезпеки та захисту даних у зміст фахових дисциплін; обмежене використання спеціалізованого програмного забезпечення захисту інформації під час практичної підготовки; недостатній рівень методичного забезпечення формування відповідних професійних компетентностей; швидке моральне старіння навчального контенту внаслідок динамічного розвитку цифрових технологій; недостатня кількість навчальних матеріалів, орієнтованих на формування практичних навичок використання сучасних засобів захисту даних.

Особливої актуальності зазначені проблеми набувають в умовах зростання кількості кіберзагроз, активного використання хмарних технологій та цифрових сервісів. Сучасний фахівець цифрових технологій повинен володіти знаннями щодо забезпечення конфіденційності, цілісності та доступності інформації, вміти використовувати програмне забезпечення для резервного копіювання даних, шифрування інформації, захисту комп'ютерних систем від шкідливого програмного забезпечення, контролю доступу та моніторингу інформаційної безпеки.

Таким чином, аналіз сучасного стану підготовки фахівців цифрових технологій у закладах вищої освіти свідчить про наявність позитивних тенденцій, пов'язаних із цифровізацією освітнього процесу, оновленням змісту освіти та впровадженням практикоорієнтованих форм навчання. Водночас виявлено недостатню увагу до формування готовності майбутніх фахівців до

застосування програмного забезпечення захисту даних у професійній діяльності. Це зумовлює необхідність розроблення та наукового обґрунтування методики підготовки фахівців цифрових технологій до використання сучасних програмних засобів захисту даних, що сприятиме підвищенню якості їхньої професійної підготовки та відповідності вимогам цифрового суспільства.

1.2 Теоретичні засади професійної підготовки фахівців цифрових технологій у контексті забезпечення кібербезпеки та захисту даних

Контроль за методами і системами захисту персональних даних завжди регулюється нормативно-правовими актами та законами, що спрямовані на конфіденційність, доступність інформації та цілісності. Основними законодавчими документами в нашій державі є Закон України «Про захист персональних даних» №2297-VI (2010), який було укладено 1 червня 2010 року (з подальшими змінами та доповненнями). Саме цей документ описує основні принципи обробки персональних даних, право на доступ, виправлення та видалення даних, а також можливості і функції структур, які займаються збором і зберіганням даних. Його основою є відповідні документи Міжнародного права такі, як: Директива ЄС 2016/679 (Європейський Парламент & Рада ЄС, 2016) та Протоколом CETS № 223 (Рада Європи, 2018)про захист персональних даних осіб.

Також можна виділити додаткові закони та законодавчі акти які регулюються захист інформації та даних: Конституція України (1996), Цивільний кодекс України (2003), Закон про кібербезпеку (2017), Закон про хмарні послуги (2022).

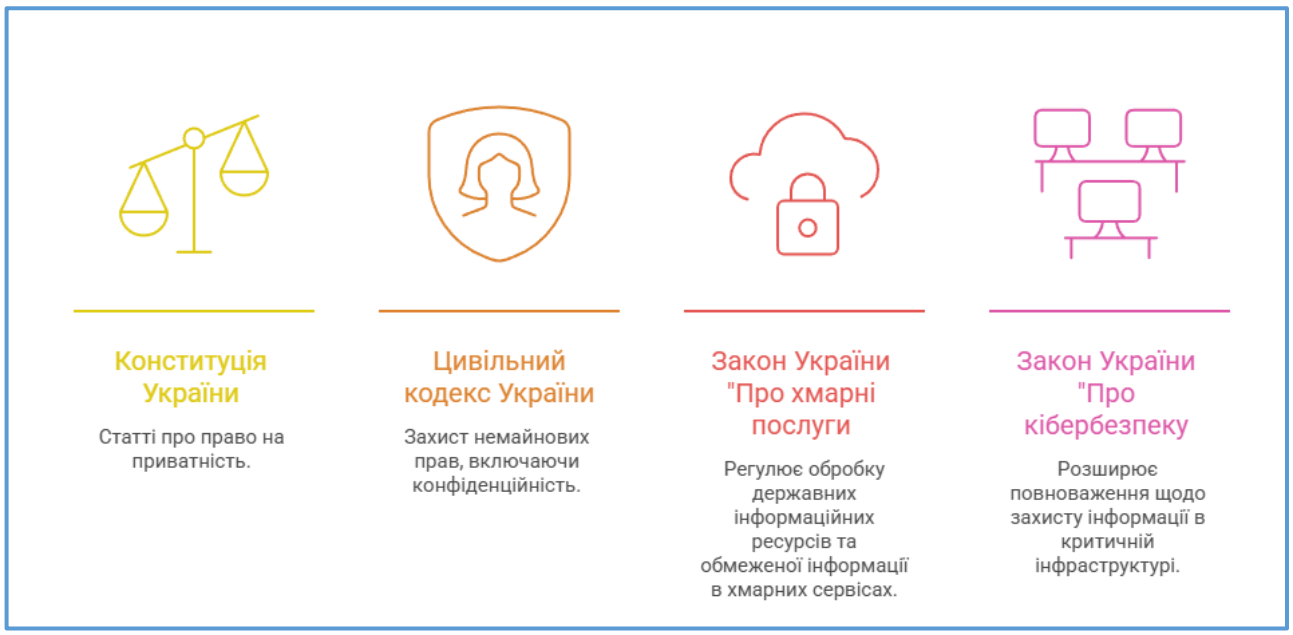

Рис. 1.2 Законодавчі акти України щодо захисту інформації

Однією із ключових ланок контролю за конфіденційністю та захистом інформації є Державна служба спеціального зв'язку та захисту інформації України, саме ця структура є основним органом у сфері захисту інформації та кібербезпеки. До її обов'язків входить:

– регулювання роботи хмарних сервісів та дата-центрів;

– сертифікація програмного забезпечення (для систем, що працюють з конфіденційною інформацією;

– захист державної інфраструктури від кібератак і різних видів ризику пов'язаних із комп'ютерними системами та мережами;

– контроль та протидія технічній розвідці, забезпечення спецзв'язку для державних структур.

На даний час відбувається оновлення законодавства згідно чинним нормативно-правових актів ЄС, зокрема закону про захист персональних даних

На світовому рівні кібербезпека та захист даних впорядковується великою кількістю міжнародних законів та стандартів, що можуть бути, як і регіонального, так і глобального характеру, як, наприклад, Протокол CETS № 223 (Рада Європи, 2018), який буи ратифікований Україною.

З точки зору підготовки фахівців в сфері цифрових технологій (методики навчання, формування компетентностей майбутніх викладачів професійної освіти за спеціальністю 015 Професійна освіта, спеціалізації 015.39 Цифрові технології нормативно-правові акти (НПА) та закони у сфері захисту даних та кібербезпеки безпеки досліджуються не лише як набір документів, які потрібно запам’ятати, а саме, як основа для формування основних правових та цифрових компетентностей фахівця в сфері професійної підготовки (рис. 1.3).

Їх впровадження в навчальну дисципліну «Кібербезпека та захист даних в професійній освіті» дозволяє формувати такі вміння:

- пояснювати здобувачам професійної освіти юридичні наслідки розголошення або втрати даних у своїй діяльності;
- розробляти інструкції, правила та заняття з кібергігієни;
- забезпечити безпечну обробку даних усіх учасників освітнього процесу включаючи журнали (фото/відео та електронні платформи);
- формувати культуру безпечної поведінки в інформаційному просторі.

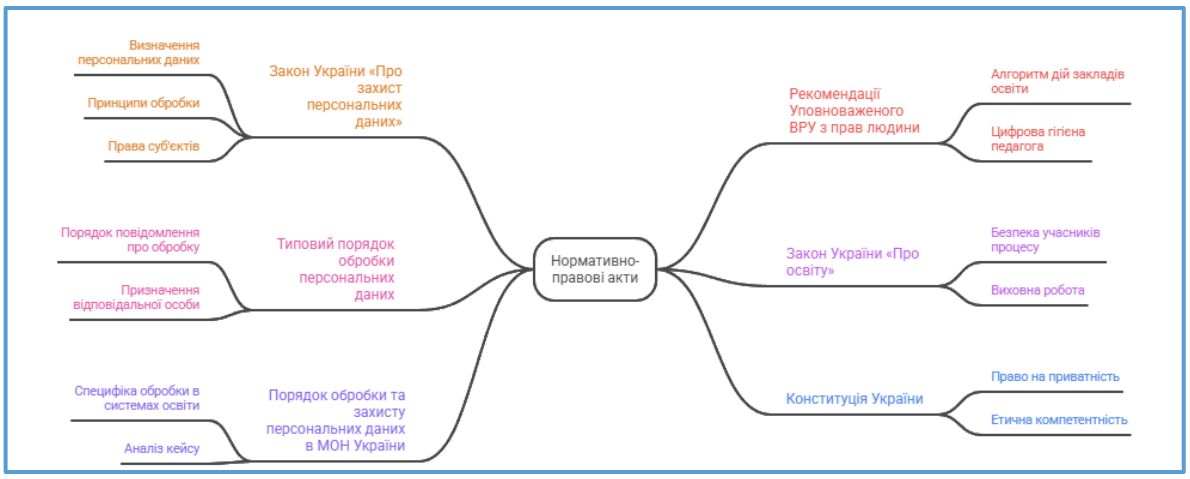

Рис. 1.3 Нормативно-правові акти та їх вплив на компетентності

Педагогічна складова підготовки майбутніх фахівців має базуватися на таких основних принципах:

– компетентності (результати навчання);

– інтеграції (включення в методологію професійної освіти);

– активності (практичні завдання);

– андрагогіки (для дорослих здобувачів).

Компетентності випускника – згідно Стандарту вищої освіти України першого (бакалаврського) рівня, галузі знань 01 – «Освіта / Педагогіка», спеціальності 015 – «Професійна освіта (за спеціалізаціями)» (Міністерство освіти і науки України., 2021):

- К 20. Здатність здійснювати професійну діяльність з дотриманням вимог законодавства, стандартів освіти та внутрішніх нормативних документів закладу освіти.
- К16 Здатність використовувати сучасні інформаційні технології та спеціалізоване програмне забезпечення та інтегрувати їх в освітнє середовище.
- К18 Здатність аналізувати ефективність проєктних рішень, пов’язаних з підбором, експлуатацією, удосконаленням, модернізацією технологічного обладнання та устаткування галузі/сфери відповідно до спеціалізації.
- К19 Здатність використовувати відповідне програмне забезпечення для вирішення професійних завдань, відповідно до спеціалізації.

Та згідно Стандарту фахової передвищої освіти освітньо-професійного ступеня (фаховий молодший бакалавр), галузі знань 01 – «Освіта / Педагогіка», спеціальності 015 – «Професійна освіта (за спеціалізаціями)» (Міністерство освіти і науки України, 2022).

- СК5 Здатність застосовувати інноваційні педагогічні та цифрові технології, інформаційне та програмне забезпечення для вирішення професійних завдань відповідно до спеціалізації
- СК9 Здатність розв’язувати типові спеціалізовані задачі, пов’язані із виконанням необхідних розрахунків, конструюванням технічних об’єктів у своїй предметній галузі відповідно до спеціалізації.
- СК8 Здатність експлуатувати виробниче устаткування та здійснювати технологічний процес відповідно до спеціалізації.

На основі проведення аналізу згаданих вище стандартів рекомендується використовувати не лише завдання на запам’ятовування НПА, а також проводити практичні заняття (інструкції, плани уроків, чек-листи, міні-тренінги).

Підводячи підсумки можна сказати, що нормативно-правові акти – це не просто документи, а засіб формування відповідального цифрового педагога, який навчає здобувачів освіти жити та працювати в безпечному цифровому середовищі.

Сучасний розвиток цифрового суспільства, активне впровадження інформаційно-комунікаційних технологій у всі сфери людської діяльності та постійне зростання кількості кіберзагроз, актуалізують проблему підготовки фахівців цифрових технологій, здатних забезпечувати безпечне функціонування інформаційних систем і ефективно використовувати програмне забезпечення для захисту даних. У цих умовах професійна підготовка майбутніх фахівців цифрового профілю повинна ґрунтуватися на сучасних теоретико-методологічних засадах, які враховують тенденції цифрової трансформації суспільства, вимоги ринку праці та особливості розвитку кібербезпекового середовища.

Професійна підготовка фахівців цифрових технологій є складним педагогічним процесом, спрямованим на формування системи знань, вмінь, навичок, професійно важливих якостей і компетентностей, необхідних для виконання професійної діяльності в умовах цифрового середовища. У сучасній педагогічній науці професійна підготовка розглядається як цілеспрямований процес формування готовності майбутнього фахівця до професійної діяльності, що передбачає засвоєння професійних знань, набуття практичного досвіду та розвиток цифрової компетентності (Шимків, 2025).

У контексті цифрових технологій професійна підготовка набуває нових характеристик, пов’язаних із необхідністю постійного оновлення знань, адаптації до швидких технологічних змін та безперервного професійного розвитку. Особливого значення набуває формування здатності працювати в

умовах інформаційних ризиків, забезпечувати безпеку цифрових ресурсів і застосовувати сучасні програмні засоби захисту інформації.

Теоретичним підґрунтям професійної підготовки фахівців цифрових технологій виступає компетентнісний підхід (Кремень, 2008; Овчарук, 2023; Сущенко, 2022), який нині є провідною методологічною основою розвитку вищої освіти. Відповідно до цього підходу результатом навчання є не лише засвоєння певного обсягу знань, а й формування професійних компетентностей, що забезпечують готовність особистості до успішної професійної діяльності.

У межах компетентнісного підходу (Мозгальов & Кізім, 2026) підготовка майбутніх фахівців цифрових технологій повинна забезпечувати формування таких груп компетентностей:

- цифрової компетентності;
- інформаційно-комунікаційної компетентності;
- компетентності у сфері кібербезпеки;
- професійно-технічної компетентності;
- проєктувальної компетентності;
- дослідницької компетентності;
- комунікативної компетентності;
- здатності до самоосвіти та професійного саморозвитку.

Ієрархія компетентностей у підготовці здобувачів спеціальності 015 Професійна освіта, спеціалізації 015.39 Цифрові технології (табл. 1.1) включає ключові компетентності, загальнопрофесійні (міжпредметні) компетентності, спеціальні (предметні, професійні) компетентності, особистісно-професійні компетентності та соціально-комунікативні компетентності

Ключові компетентності становлять універсальну основу професійної діяльності та забезпечують здатність особистості успішно функціонувати в сучасному інформаційному суспільстві. Вони формуються впродовж усього періоду навчання та інтегрують знання, вміння, навички, цінності й особистісні якості, необхідні для самореалізації, професійного розвитку та громадянської активності.

Таблиця 1.1

Ієрархічна структура компетентностей майбутніх фахівців цифрових технологій

Рівень компетентностей	**Група компетентностей**	**Зміст (характеристика)**	**Приклади для спеціальності 015.39 «Цифрові технології»**
I рівень (базовий, надпредметний)	Ключові компетентності	Універсальні компетентності, що забезпечують життєдіяльність, навчання впродовж життя та соціальну адаптацію	Інформаційно-цифрова грамотність, комунікативна компетентність, вміння вчитися, критичне мислення, громадянська компетентність
II рівень (інтегративний)	Загальнопрофесійні (міжпредметні) компетентності	Формуються на основі кількох дисциплін і забезпечують здатність розв’язувати типові професійні завдання	Проєктно-технологічна компетентність, алгоритмічна компетентність, компетентність у сфері ІКТ, базова кіберграмотність, цифрова педагогічна компетентність
III рівень (фаховий)	Спеціальні (предметні, професійні) компетентності	Безпосередньо пов’язані з професійною діяльністю у сфері цифрових технологій	Розробка цифрових освітніх ресурсів, адміністрування комп’ютерних мереж, використання хмарних сервісів, застосування програмного забезпечення захисту даних, робота з LMS/IDE
IV рівень (індивідуально-особистісний, інтегративний)	Особистісно-професійні компетентності	Забезпечують професійний розвиток, саморегуляцію та ефективність діяльності фахівця	Самоосвіта, цифрова адаптивність, відповідальність у роботі з даними, стресостійкість, професійна рефлексія
V рівень (соціально-професійний)	Соціально-комунікативні компетентності	Визначають ефективність взаємодії в професійному середовищі	Командна робота в IT-проєктах, педагогічна комунікація, управління цифровими командами, етика використання даних

До складу ключових компетентностей належать цифрова, інформаційна, комунікативна, громадянська, підприємницька, навчально-пізнавальна та

соціальна компетентності. Їх сформованість забезпечує готовність майбутнього фахівця до безперервного навчання, адаптації до технологічних змін та ефективного використання сучасних цифрових технологій у професійній діяльності.

Загальнопрофесійні (міжпредметні) компетентності відображають здатність майбутнього фахівця використовувати знання та вміння, набуті під час вивчення різних навчальних дисциплін, для вирішення професійних завдань. Вони забезпечують міждисциплінарну інтеграцію змісту навчання та сприяють формуванню системного бачення професійної діяльності. До цієї групи належать вміння здійснювати аналіз і синтез інформації, використовувати методи наукового пізнання, застосовувати сучасні інформаційно-комунікаційні технології, здійснювати проєктування та планування професійної діяльності, працювати з нормативно-правовою документацією та приймати обґрунтовані рішення в умовах професійної практики.

Спеціальні (предметні, професійні) компетентності характеризують рівень готовності здобувача освіти до виконання професійних функцій у конкретній галузі діяльності. Для майбутніх фахівців цифрових технологій вони охоплюють здатність використовувати сучасне програмне забезпечення, проєктувати та адмініструвати інформаційні системи, здійснювати розроблення програмних продуктів, застосовувати мережеві технології, аналізувати інформаційні процеси, забезпечувати кібербезпеку та захист даних. Особливе значення мають компетентності, пов’язані з використанням спеціалізованого програмного забезпечення захисту даних, виявленням потенційних загроз інформаційній безпеці та впровадженням заходів щодо їх попередження й усунення.

Особистісно-професійні компетентності відображають індивідуальні характеристики майбутнього фахівця, які забезпечують ефективність професійної діяльності та здатність до професійного саморозвитку. До них належать відповідальність, дисциплінованість, самостійність, критичне мислення, здатність до рефлексії, професійна мобільність, готовність до

інноваційної діяльності та безперервної освіти. Важливою складовою цих компетентностей є здатність до самооцінювання власної професійної діяльності, визначення шляхів удосконалення професійних знань і навичок та адаптації до нових технологічних викликів.

Соціально-комунікативні компетентності забезпечують ефективну взаємодію майбутнього фахівця з іншими учасниками освітнього та професійного процесу. Вони охоплюють вміння працювати в команді, здійснювати професійну комунікацію, організовувати спільну діяльність, вирішувати конфліктні ситуації, дотримуватися етичних норм професійної поведінки та принципів академічної доброчесності. В умовах цифрового суспільства особливого значення набуває здатність використовувати сучасні цифрові засоби комунікації, організовувати співпрацю в мережевому середовищі та забезпечувати безпечну взаємодію учасників освітнього процесу.

Особливе місце серед зазначених компетентностей посідає компетентність у сфері кібербезпеки, яка передбачає здатність виявляти потенційні загрози інформаційній безпеці, застосовувати методи захисту даних, використовувати програмні засоби кіберзахисту та забезпечувати безпечну роботу цифрових систем.

Однією з ключових теоретичних засад професійної підготовки є системний підхід, відповідно до якого процес формування професійної компетентності розглядається як цілісна система взаємопов’язаних компонентів. Такими компонентами є мета, зміст, методи, форми, засоби навчання, педагогічні умови та результати підготовки.

Застосування системного підходу до підготовки фахівців цифрових технологій дозволяє забезпечити взаємозв’язок між теоретичним навчанням і практичною діяльністю, інтеграцію знань із різних галузей інформаційних технологій та формування комплексного бачення проблем інформаційної безпеки.

Важливого значення набуває діяльнісний підхід (Манойленко, 2017), відповідно до якого професійна підготовка здійснюється через активну

діяльність здобувачів освіти. Формування компетентностей у сфері захисту даних неможливе лише шляхом засвоєння теоретичного матеріалу. Майбутні фахівці повинні набувати практичного досвіду роботи із засобами захисту інформації, виконувати лабораторно-практичні та проєктні завдання, моделювати реальні ситуації кіберзагроз та відпрацьовувати алгоритми реагування на них.

У межах діяльнісного підходу особливу роль відіграють:

- практичні заняття;
- лабораторні роботи;
- кейс-методи;
- проєктне навчання;
- симуляційні вправи;
- навчальні кіберполігони;
- віртуальні лабораторії;
- технологічна практика.

Сучасна професійна освіта також спирається на особистісно орієнтований підхід (Поліщук, 2022), який передбачає врахування індивідуальних особливостей здобувачів освіти, їхніх професійних інтересів, рівня підготовленості та освітніх потреб. Реалізація цього підходу сприяє розвитку мотивації до вивчення засобів кібербезпеки, формуванню відповідального ставлення до захисту інформації та готовності до професійного самовдосконалення.[посилання]

У контексті цифровізації освіти важливого значення набуває технологічний підхід (Княжева І.А.), який передбачає проєктування освітнього процесу на основі сучасних педагогічних та цифрових технологій. Використання систем управління навчанням, хмарних сервісів, віртуальних лабораторій, засобів моделювання кіберзагроз та цифрових платформ забезпечує підвищення ефективності професійної підготовки та створює умови для набуття практичного досвіду роботи з програмним забезпеченням захисту даних.

Теоретичні засади підготовки фахівців цифрових технологій у сфері кібербезпеки значною мірою базуються на міжнародних стандартах та рамках цифрових компетентностей. Важливими орієнтирами виступають:

– Європейська рамка цифрових компетентностей громадян DigComp; (Vuorikari et al., 2022).

– Європейська рамка цифрових компетентностей педагогів DigCompEdu; (Redecker, 2017).

– рамка кібербезпекових компетентностей Європейського агентства з кібербезпеки (ENISA); (European Union Agency for Cybersecurity ENISA, 2022).

– рекомендації міжнародної асоціації обчислювальної техніки ACM; (Association for Computing Machinery & IEEE Computer Society, 2020).

– рекомендації Інституту інженерів з електротехніки та електроніки IEEE; (IEEE, 2023).

– рамка кібербезпекової освіти NIST NICE Cybersecurity Workforce Framework. (National Institute of Standards and Technology NIST, 2024).

Зазначені документи визначають перелік знань, вмінь і компетентностей, необхідних для ефективної діяльності у сфері цифрових технологій та кібербезпеки.

У сучасних умовах важливим теоретичним поняттям виступає готовність майбутнього фахівця до застосування програмного забезпечення захисту даних. Готовність доцільно розглядати як інтегративну характеристику особистості, що включає когнітивний, діяльнісний, мотиваційний, рефлексивний компоненти.

Мотиваційний компонент відображає усвідомлення значущості захисту даних у професійній діяльності та прагнення до оволодіння відповідними технологіями. Когнітивний компонент охоплює систему знань щодо принципів інформаційної безпеки, сучасних кіберзагроз, методів захисту інформації та функціональних можливостей спеціалізованого програмного забезпечення. Діяльнісний компонент характеризує практичні вміння використовувати програмні засоби захисту даних у різних професійних ситуаціях. Рефлексивний

компонент забезпечує здатність до самооцінювання власної діяльності, аналізу результатів та подальшого професійного розвитку.

Аналіз сучасних досліджень свідчить, що ефективність підготовки фахівців цифрових технологій значною мірою залежить від реалізації принципів інтеграції освіти, науки та практики. У процесі навчання необхідно забезпечувати поєднання фундаментальної підготовки з реальними потребами ІТ-галузі та сфери кібербезпеки. Це сприяє формуванню у здобувачів освіти практичних навичок використання сучасних програмних засобів захисту даних і готовності до професійної діяльності в умовах цифрової трансформації.

Таким чином, теоретичні засади професійної підготовки фахівців цифрових технологій у контексті забезпечення кібербезпеки та захисту даних базуються на компетентнісному, системному, діяльнісному, особистісно орієнтованому та технологічному підходах. Їх реалізація забезпечує формування готовності майбутніх фахівців до ефективного застосування програмного забезпечення захисту даних, розвитку професійних компетентностей у сфері кібербезпеки та успішної діяльності в умовах сучасного цифрового середовища. Отримані теоретичні положення становлять методологічну основу для розроблення моделі та методики підготовки фахівців цифрових технологій до застосування програмного забезпечення захисту даних.

1.3 Компетентнісний підхід до підготовки фахівців цифрових технологій щодо застосування програмного забезпечення захисту даних

Сучасний розвиток цифрових технологій у закладах вищої освіти потребує підготовки фахівців, які не лише володіють базовими знаннями з інформаційних технологій, але й уміють практично застосовувати цифрові інструменти для забезпечення безпеки даних. Зростання кількості кіберзагроз, вірусних атак, витоків інформації та порушень конфіденційності обумовлює необхідність формування у студентів практичної готовності до використання програмного забезпечення захисту даних у професійній діяльності.

У цих умовах провідним методологічним підходом виступає *компетентнісний підхід,* який орієнтує освітній процес не лише на засвоєння теоретичних знань (Близнюк, М., & Радько, Я. 2025), а насамперед на формування здатності студента діяти у реальних або наближених до реальних професійних ситуаціях. Для студентів фахової передвищої освіти це означає вміння налаштовувати, використовувати та обслуговувати програмні засоби захисту інформації у комп'ютерних системах і мережах.

Компетентнісний підхід у підготовці майбутніх фахівців цифрових технологій передбачає формування цілісної системи компетентностей, які забезпечують готовність до професійної діяльності у сфері захисту даних. У ЗФПО особливий акцент робиться на практичній складовій, оскільки саме вона визначає рівень професійної підготовленості випускника.

У процесі підготовки фахівців цифрових технологій до застосування програмного забезпечення захисту даних доцільно виокремити такі основні групи компетентностей.

Базова цифрова компетентність

Вона передбачає впевнене користування комп'ютерною технікою, операційними системами, офісним програмним забезпеченням та мережевими сервісами. У контексті захисту даних ця компетентність включає:

- дотримання правил безпечної роботи в Інтернеті;
- використання базових засобів захисту інформації;
- розвміння ризиків цифрового середовища;
- відповідальне поводження з персональними даними.

Компетентність у сфері інформаційної безпеки

Ця компетентність є ключовою для тематики дослідження і включає:

- розвміння основ кібербезпеки;
- знання типів кіберзагроз (віруси, фішинг, шпигунські програми);
- розвміння принципів захисту інформації;
- базові навички використання програмного забезпечення захисту даних.

Практична (операційна) компетентність

Вона відображає здатність студента виконувати конкретні дії з використанням програмного забезпечення захисту даних, зокрема:

- встановлення та налаштування антивірусних програм;
- використання засобів резервного копіювання;
- базове шифрування файлів і папок;
- налаштування паролів та прав доступу;
- використання VPN та мережевих засобів безпеки.

Аналітична компетентність

Передбачає вміння аналізувати ситуації, пов’язані з інформаційною безпекою, зокрема:

- виявлення потенційних загроз;
- оцінювання рівня ризику для даних;
- вибір відповідних засобів захисту;
- аналіз наслідків порушення безпеки.

Самоосвітня компетентність

Оскільки цифрові технології швидко змінюються, важливо сформувати у студентів готовність до постійного навчання:

- самостійне вивчення нового програмного забезпечення;
- використання онлайн-курсів і інструкцій;
- оновлення знань про кіберзагрози;
- розвиток професійних навичок у сфері ІТ-безпеки.

Методи оцінювання компетенцій у підготовці фахівців цифрових технологій повинні відповідати компетентнісному підходу і враховувати чотири основні компоненти готовності: когнітивний, діяльнісний, мотиваційний та рефлексивний. У сучасній професійній освіті найефективнішими є комплексні методи, які дозволяють оцінити не лише теоретичні знання, а й практичні вміння, мотивацію та здатність до самоаналізу.

Серед основних методів оцінювання використовуються спостереження за виконанням практичних завдань у віртуальних середовищах і лабораторних роботах, аналіз продуктів діяльності студентів (створені інструкції, чек-листи,

проєкти з налаштування захисту даних), портфоліо, яке включає результати лабораторних робіт, проєктів і рефлексивні звіти. Важливим інструментом є матриця компетентностей, яка дозволяє кількісно оцінити рівень сформованості кожної компетенції за бальною шкалою. Також застосовуються ситуативні завдання та кейси, де студентам пропонується проаналізувати реальну ситуацію витоку даних і запропонувати заходи захисту. Для оцінки мотиваційного та рефлексивного компонентів ефективними є методи самооцінки, рефлексивні есе та структуровані інтерв'ю.

Таке різноманіття методів забезпечує об'єктивність оцінювання, дозволяє відстежувати динаміку розвитку компетенцій протягом навчання і дає змогу коригувати індивідуальні освітні траєкторії студентів.

У межах компетентнісного підходу результатом навчання є сформована готовність студента до практичного використання програмного забезпечення захисту даних. Ця готовність має комплексний характер і включає мотиваційний компонент, який передбачає усвідомлення важливості захисту інформації та зацікавленість у вивченні засобів кібербезпеки; когнітивний компонент, що охоплює базові знання про кіберзагрози та програмні засоби їх нейтралізації; діяльнісний компонент, який проявляється у вмінні використовувати антивірусні програми, засоби резервного копіювання та шифрування даних; а також рефлексивний компонент, що виражається в здатності оцінювати власні дії та дотримуватися правил інформаційної безпеки.

Реалізація компетентнісного підходу в закладах вищої освіти має свою специфіку. Вона характеризується переважанням практико-орієнтованого навчання, активним використанням лабораторних робіт і тренажерів, моделюванням реальних ситуацій кіберзагроз, виконанням навчальних проєктів із захисту даних, широким застосуванням сучасного програмного забезпечення, такого як антивіруси, VPN та системи резервного копіювання, а також тісною інтеграцією навчального процесу з потребами майбутньої професійної діяльності студентів.

Особливу роль відіграє використання практичних кейсів, у яких студенти навчаються реагувати на типові ситуації: зараження комп’ютера вірусом, втрата даних, витік паролів або несанкціонований доступ до інформації.

Психологічний аспект реалізації даної педагогічної умови полягає у забезпеченні поступового переходу здобувачів освіти від пасивного засвоєння знань до їх практичного застосування під час використання програмного забезпечення захисту даних. Такий перехід здійснюється відповідно до діалектико-матеріалістичної концепції розвитку (Вілков, 2021) та передбачає поетапне ускладнення навчальних завдань: від виконання базових операцій із налаштування механізмів автентифікації та захисту облікових записів до моделювання складних сценаріїв порушення інформаційної безпеки та ліквідації наслідків витоку даних у віртуальному середовищі. Зазначений підхід сприяє формуванню впевненості у власних професійних можливостях, розвитку критичного мислення та здатності приймати обґрунтовані рішення в умовах потенційних кіберзагроз.

Педагогічний аспект ґрунтується на організації освітнього процесу через активну практичну підготовку здобувачів освіти, що передбачає безпосередню взаємодію з програмними засобами захисту даних, моделювання професійних ситуацій та розв’язання практико-орієнтованих завдань. Реалізація даного підходу забезпечує інтеграцію теоретичних знань із практичними навичками та створює умови для наближення навчальної діяльності до реальних умов практичної підготовки фахівців цифрових технологій.

Організація практико-орієнтованого навчання майбутніх фахівців цифрових технологій шляхом використання спеціалізованого програмного забезпечення захисту даних та моделювання професійних ситуацій у сфері інформаційної безпеки.

Організація практико-орієнтованого навчання майбутніх фахівців цифрових технологій шляхом виконання лабораторних робіт, проєктних завдань і технологічної практики. Зокрема, під час лабораторних занять здобувачі освіти виконують налаштування захищених комп’ютерних мереж у середовищі Cisco

Packet Tracer, здійснюють моніторинг та аналіз мережевого трафіку за допомогою Wireshark, а також проводять оцінювання вразливостей вебресурсів із використанням спеціалізованих інструментів Burp Suite (PortSwigger, n.d.) та OWASP ZAP (Aikido Security, n.d.). Така діяльність сприяє формуванню професійних вмінь щодо виявлення потенційних загроз інформаційній безпеці та застосування сучасних засобів їх нейтралізації.

Важливим складником практичної підготовки здобувачів цифрових технологій є виконання проєктних завдань, спрямованих на розроблення комплексних рішень у сфері захисту даних. Одним із прикладів може бути створення захищеної платформи дистанційного навчання на основі системи LMS Moodle (рис. 1.4) із впровадженням механізмів шифрування та контролю доступу.

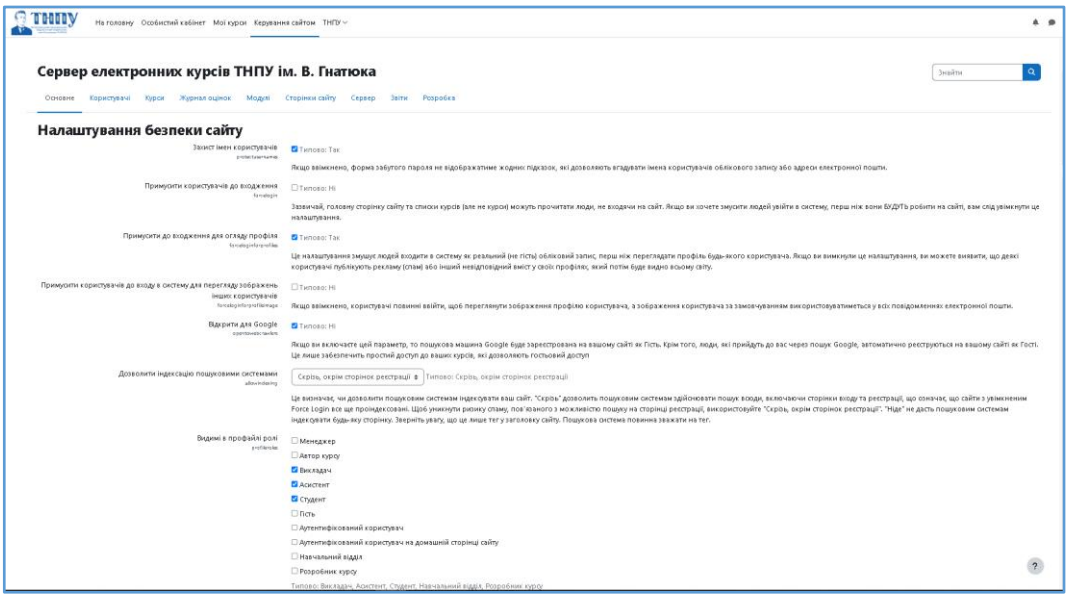

Рис.1.4. Налаштування захищеної платформи дистанційного навчання LMS Moodle

Закріплення набутих знань і навичок здійснюється під час технологічної практики, де здобувачі освіти мають можливість застосовувати програмне забезпечення захисту даних у реальних умовах функціонування підприємств та організацій. Результатом такої діяльності є не лише виконання практичних завдань із забезпечення інформаційної безпеки, але й розроблення методичних

рекомендацій щодо використання засобів захисту даних, які можуть бути використані в подальшій професійній та освітній діяльності.

Особистісно-орієнтований та гуманістичний підхід у підготовці майбутніх фахівців цифрових технологій акцентує увагу на розвитку внутрішньої мотивації, етичної чутливості та особистісного ставлення до питань захисту даних. Психологічний аспект цього підходу передбачає формування в студентів усвідомлення реальних наслідків витоку інформації для конкретної людини, її прав і психологічного благополуччя. Це допомагає долати типові бар'єри, такі як «мені це не потрібно», «це не стосується моєї професії» чи «це надто складно». Педагогічний аспект реалізується через створення індивідуальних освітніх траєкторій, систематичну рефлексію та врахування емоційного стану студентів, зокрема страху помилок під час налаштування засобів захисту. Ефективними інструментами є рефлексивні завдання («Як я захистив свої дані цього тижня?», «Які мої типові помилки в кіберпросторі?») та етичні дискусії, наприклад, щодо балансу між зручністю використання Zoom і безпекою персональних даних студентів.

Андрагогічний підхід, який особливо важливий при роботі з дорослими здобувачами освіти, ґрунтується на врахуванні життєвого досвіду, професійних потреб і мотивації дорослих. Психологічний аспект полягає в опорі на реальний досвід дорослих, їхні попередні помилки в кіберпросторі та мотивацію через практичну користь («як це допоможе мені на роботі»). Педагогічний аспект передбачає проблемно-орієнтоване навчання, модульну структуру матеріалів, активне використання кейсів з реального виробництва та симуляцію професійних ситуацій. Здобувачі краще сприймають матеріал, коли бачать його безпосередній зв'язок із їхньою професійною діяльністю, тому акцент робиться на розробці практичних інструкцій, чек-листів і планів реагування на інциденти, які вони можуть відразу застосовувати на робочому місці.

Психологічний аспект підготовки ґрунтується на опорі на власний досвід дорослих студентів, зокрема на їхніх реальних помилках у кіберпросторі. Це дозволяє підвищити мотивацію через усвідомлення практичної користі від

вивчення захисту даних, адже студенти чітко бачать, як ці знання можуть убезпечити їх на майбутній роботі. Педагогічний аспект реалізується через проблемно-орієнтоване навчання та модульну організацію матеріалу, що сприяє розвитку самоосвіти. Ефективним методом є використання реальних кейсів витоків даних на виробництві та в ІТ-сфері, на основі яких студенти розробляють інструкції та рекомендації для дорослих здобувачів. Особливе місце займають тренінги з симуляцією фішингових атак для здобувачів з подальшим аналізом реакції учасників.

Ризик-орієнтований та проблемно-орієнтований підходи дозволяють формувати в студентів адаптивну тривожність – усвідомлення реальних ризиків без зайвої паніки, а також розвивати стресостійкість під час моделювання кіберінцидентів. Педагогічно це реалізується через оцінку ризиків як основу вибору засобів захисту даних. Студенти працюють з матрицями ризиків для освітнього процесу, зокрема щодо можливих витоків даних в електронних журналах, і виконують проєкти зі створення плану реагування на витік інформації при проведені лабораторних робіт.

Гейміфікаційний та симуляційний підхід суттєво підвищує мотивацію студентів. Завдяки елементу азарту та безпечному середовищу для помилок вони охочіше залучаються до навчання. Використання CTF-завдань (Capture The Flag) та симуляторів кібератак дозволяє не лише закріпити практичні навички, а й розвивати стратегічне мислення та командну взаємодію в умовах, максимально наближених до реальних.

Гейміфіковані лабораторні: «Захисти мережу від атаки» (TryHackMe).

Розробка ігрових занять з кібербезпеки для здобувачів освіти.

Ключові психолого-педагогічні умови ефективності (специфічні для спеціальності 015 Професійна освіта, спеціалізації 015.39 Цифрові технології)

Подвійна спрямованість: студент вчиться захищати дані сам – вчить цьому інших – подвійна практика (технічна + педагогічна).

Інтеграція в методику професійного навчання: теми захисту даних обов’язково при проведенні занять дисциплін професійної підготовки (програмування, адміністрування, веб).

Психологічна підтримка: робота з бар'єрами (страх помилок, низька самооцінка в ІТ) через рефлексію та успіхи в лабораторних.

Етичний та правовий компонент: формування усвідомлення Закону про персональні дані, GDPR-принципів, відповідальності педагога за дані студентів.

У підсумку, для спеціальності 015 Професійна освіта, спеціалізації 015.39 Цифрові технології, готовність до використання програмного забезпечення (Кулакова, Л., & Онокало, О. 2025) захисту даних – це не технічна навичка, а професійно-педагогічна компетентність, де фахівець одночасно є користувачем, фахівцем і вчителем кібербезпеки. Підходи поєднують психологічну мотивацію, діяльнісну практику та педагогічну спрямованість на передачу знань здобувачам.

Таким чином, компетентнісний підхід у підготовці студентів закладів фахової передвищої освіти до застосування програмного забезпечення захисту даних забезпечує формування базових цифрових, інформаційно-безпекових, практичних, аналітичних та самоосвітніх компетентностей. Його реалізація дозволяє підготувати конкурентоспроможних фахівців, здатних ефективно використовувати програмні засоби захисту інформації у професійній діяльності та адаптуватися до сучасних викликів цифрового середовища.

1.4 Аналіз програмного забезпечення захисту даних та особливостей його використання у професійній діяльності

Стрімкий розвиток цифрових технологій, поширення хмарних сервісів, мобільних платформ та мережевих інформаційних систем супроводжується постійним зростанням обсягів даних, що обробляються, передаються та зберігаються в електронному вигляді. За таких умов забезпечення належного рівня захисту інформації стає одним із ключових завдань професійної діяльності фахівців цифрових технологій. Ефективне вирішення цього завдання значною

мірою залежить від використання спеціалізованого програмного забезпечення захисту даних, яке забезпечує конфіденційність, цілісність та доступність інформаційних ресурсів.

У сучасній науковій літературі поняття програмного забезпечення захисту даних трактується як сукупність програмних засобів, призначених для виявлення, попередження, нейтралізації та усунення загроз інформаційній безпеці, а також для забезпечення захисту даних від несанкціонованого доступу, модифікації, знищення або витоку (Лубко, Д. В., & Мірошниченко, М. Ю. 2024). Таке програмне забезпечення є важливою складовою комплексної системи інформаційної безпеки та використовується в державному управлінні, бізнесі, освіті, науковій діяльності та інших сферах.

Основною метою застосування програмного забезпечення захисту даних є реалізація базових принципів інформаційної безпеки, які забезпечують надійне функціонування інформаційних систем, захист інформаційних ресурсів від несанкціонованого доступу та мінімізацію ризиків, пов’язаних із кіберзагрозами. До таких принципів належать:

– *конфіденційність інформації* – забезпечення доступу до інформації виключно авторизованим користувачам;

– *цілісність даних* – захист інформації від несанкціонованого модифікування, пошкодження або знищення;

– *доступність інформаційних ресурсів* – гарантування своєчасного доступу користувачів до необхідних даних і сервісів;

– *автентичність інформації* – підтвердження достовірності даних та справжності користувачів, які здійснюють доступ до інформаційної системи;

– *контроль доступу* – регулювання прав користувачів щодо використання інформаційних ресурсів відповідно до їхніх функціональних обов’язків;

– *підзвітність та аудит дій користувачів* – забезпечення можливості реєстрації, моніторингу та аналізу дій користувачів для виявлення порушень політик безпеки та розслідування інцидентів.

Реалізація зазначених принципів здійснюється за допомогою різноманітних програмних засобів, які забезпечують захист даних на різних рівнях інформаційної інфраструктури: від окремих робочих станцій до корпоративних мереж і хмарних середовищ. Вибір конкретного програмного забезпечення залежить від характеру інформаційних ресурсів, рівня потенційних загроз, вимог нормативно-правових документів та особливостей функціонування інформаційної системи.

У сучасних інформаційних системах використовується широкий спектр програмних засобів захисту даних, які можуть виконувати функції запобігання, виявлення та реагування на кіберінциденти. До них належать антивірусні програми, міжмережеві екрани, системи виявлення та запобігання вторгненням, засоби криптографічного захисту інформації, програмне забезпечення резервного копіювання та відновлення даних, системи контролю доступу, засоби моніторингу подій інформаційної безпеки та інші спеціалізовані програмні продукти.

З метою систематизації існуючих програмних рішень доцільно здійснити їх класифікацію за функціональним призначенням. Такий підхід дозволяє визначити роль кожного класу програмного забезпечення в забезпеченні комплексного захисту інформації та окреслити напрями їх практичного застосування в професійній діяльності фахівців цифрових технологій. Класифікацію програмного забезпечення захисту даних за функціональним призначенням наведено на рисунку 1.5.

Рис. 1.5 Класифікація програмного забезпечення захисту даних за функціональним призначенням

Мережеві засоби захисту інформації

Для захисту даних під час передачі мережею використовуються спеціалізовані програмні комплекси, які забезпечують фільтрацію трафіку, моніторинг мережевої активності та виявлення потенційних загроз.

До таких засобів належать:

– міжмережеві екрани (Firewall);

– системи виявлення вторгнень (IDS);

– системи запобігання вторгненням (IPS);

– VPN-системи;

– засоби моніторингу мережевого трафіку.

Серед популярних рішень можна виділити:

– pfSense;

– OpenVPN;

– Snort;

– Suricata.

Програмне забезпечення резервного копіювання та відновлення даних

Втрата інформації внаслідок технічних несправностей, помилок користувачів або кібератак може спричинити значні матеріальні та репутаційні збитки. Для мінімізації таких ризиків застосовуються системи резервного копіювання даних.

Серед найбільш поширених рішень можна виділити:

– Acronis Cyber Protect;

– Veeam Backup & Replication;

– Cobian Backup;

– Backup Exec.

Застосування таких систем дозволяє забезпечити швидке відновлення інформації після збоїв та підтримувати безперервність роботи інформаційних систем.

Антивірусне програмне забезпечення

Однією з найбільш поширених категорій програмного забезпечення захисту даних є антивірусні системи. Вони призначені для виявлення, блокування та видалення шкідливого програмного забезпечення, зокрема вірусів, троянських програм, програм-вимагачів, шпигунського програмного забезпечення та інших видів кіберзагроз.

До найбільш відомих антивірусних рішень належать:

– Microsoft Defender;

– ESET NOD32 Antivirus;

– Kaspersky Standard;

– Bitdefender Total Security;

– Avast Premium Security.

Антивірусне програмне забезпечення широко використовується системними адміністраторами, розробниками програмного забезпечення, фахівцями з кібербезпеки та працівниками організацій для забезпечення безпечного функціонування комп’ютерних систем.

Програмне забезпечення для шифрування даних

Важливу роль у забезпеченні конфіденційності інформації відіграють засоби криптографічного захисту даних. Вони дозволяють перетворювати інформацію у зашифрований вигляд та забезпечують доступ до неї лише авторизованим користувачам.

До програмних засобів шифрування належать:

– VeraCrypt;

– BitLocker;

– GNU Privacy Guard;

– AxCrypt.

У професійній діяльності фахівців цифрових технологій криптографічні засоби використовуються для захисту конфіденційної інформації, корпоративних документів, баз даних та персональних даних користувачів.

Програмне забезпечення для захисту хмарних даних

Сучасні організації активно використовують хмарні технології для зберігання та оброблення інформації. Це обумовлює необхідність застосування спеціалізованих засобів захисту хмарних ресурсів.

Основними функціями таких систем є:

– контроль доступу до хмарних сервісів;

– моніторинг активності користувачів;

– шифрування даних;

– виявлення аномальної поведінки;

– захист від витоку інформації.

До цієї категорії належать:

– Microsoft Defender for Cloud;

– AWS Security Hub;

– Google Security Command Center.

Засоби контролю доступу та автентифікації

Одним із ключових напрямів захисту даних є обмеження доступу до інформаційних ресурсів. Для цього використовуються програмні засоби управління доступом та автентифікації користувачів.

До них належать:

– системи багатофакторної автентифікації;

– менеджери паролів;

– системи єдиного входу (SSO);

– програмні комплекси керування обліковими записами;

– засоби біометричної автентифікації.

Особливої актуальності набуває використання багатофакторної автентифікації, яка значно знижує ризики несанкціонованого доступу до інформаційних систем.

Аналіз сучасної практики використання програмного забезпечення захисту даних свідчить про його інтеграцію практично в усі напрями діяльності фахівців цифрових технологій. Незалежно від спеціалізації – програмування, адміністрування мереж, розроблення вебсистем, аналізу даних чи цифрового дизайну – майбутні фахівці повинні володіти навичками забезпечення інформаційної безпеки.

У професійній діяльності використання програмного забезпечення захисту даних характеризується такими особливостями (рис. 1.6):

– комплексний характер захисту, що передбачає одночасне використання декількох програмних засобів;

– постійне оновлення програмного забезпечення відповідно до нових видів кіберзагроз;

– автоматизація процесів моніторингу та реагування на інциденти безпеки;

– інтеграція засобів захисту з корпоративними інформаційними системами;

– використання хмарних технологій та віддаленого адміністрування;

– необхідність дотримання вимог нормативно-правових документів у сфері захисту інформації та персональних даних.

Рис. 1.6 Особливості використання програмного забезпечення захисту даних

Сучасний фахівець цифрових технологій повинен володіти не лише теоретичними знаннями про принципи інформаційної безпеки, а й практичними навичками налаштування, адміністрування та використання програмних засобів захисту даних у різних професійних ситуаціях.

Таким чином, проведений аналіз показав, що програмне забезпечення захисту даних є важливою складовою сучасної цифрової інфраструктури та невід'ємним інструментом професійної діяльності фахівців цифрових технологій. Сучасні програмні засоби забезпечують антивірусний захист, шифрування інформації, резервне копіювання даних, контроль доступу, захист мережевих ресурсів та хмарних сервісів. Водночас ефективне використання такого програмного забезпечення потребує спеціальної професійної підготовки, що зумовлює необхідність розроблення методики формування у майбутніх фахівців цифрових технологій готовності до застосування засобів захисту даних у професійній діяльності.

Спеціалізоване програмне забезпечення захисту даних (ПЗЗД) є ключовим інструментом у професійній діяльності фахівців з кібербезпеки, мережевих адміністраторів, ІТ-педагогів та аналітиків. Воно допомагає виявляти загрози, аналізувати трафік, моделювати мережі та тестувати вразливості.

Серед популярних рішень для закладів освіти часто використовують pfSense як універсальний відкритий міжмережевий екран, OpenVPN для організації безпечних віддалених з'єднань, а також Snort і Suricata – потужні open-source системи виявлення та запобігання вторгнень, які добре підходять для навчального процесу завдяки своїй гнучкості та безкоштовності.

Сучасні засоби шифрування даних (VeraCrypt, BitLocker, GNU Privacy Guard та AxCrypt) можуть бути використані в освітньому процесі. VeraCrypt є одним з найпопулярніших кросплатформенних інструментів, який дозволяє створювати зашифровані контейнери та томи з високим рівнем захисту. BitLocker – вбудоване рішення Microsoft для повного шифрування дисків у Windows, зручне для корпоративного та навчального використання. GNU Privacy Guard (GnuPG) – потужний open-source інструмент для шифрування файлів і електронної пошти, що відповідає стандарту OpenPGP. AxCrypt – проста та зручна програма для швидкого шифрування окремих файлів і папок, яка має інтуїтивний інтерфейс і добре підходить для початківців.

Актуальність використання сучасних рішень для резервного копіювання даних у професійній освіті зумовлена необхідністю забезпечення надійного захисту інформації в умовах цифрової трансформації та зростання кіберзагроз. Серед ефективних інструментів, що застосовуються в освітньому процесі та професійній діяльності, варто виділити Acronis Cyber Protect, Veeam Backup & Replication, Cobian Backup та Backup Exec. Acronis Cyber Protect поєднує надійне резервне копіювання з активними функціями кіберзахисту, включаючи захист від ransomware та швидке відновлення даних. Veeam Backup & Replication є одним з лідерів ринку для захисту віртуальних середовищ і хмарних інфраструктур, характеризується високою швидкістю відновлення та гнучкістю налаштувань. Cobian Backup – це легке, безкоштовне та просте у використанні

рішення, яке добре підходить для закладів освіти і невеликих організацій. Backup Exec – класичне корпоративне рішення від Veritas, орієнтоване на централізоване управління резервним копіюванням у великих IT-інфраструктурах.

У контексті підготовки здобувачів освіти за спеціальністю 015 Професійна освіта, спеціалізацією 015.39 Цифрові технології особливого значення набуває формування компетентностей у сфері інформаційної безпеки та застосування програмного забезпечення захисту даних. Майбутні фахівці цифрових технологій повинні володіти не лише теоретичними знаннями щодо сучасних загроз інформаційній безпеці, але й практичними навичками використання спеціалізованих програмних засобів для моніторингу, аналізу, виявлення та попередження кіберінцидентів.

Вивчення програмного забезпечення захисту даних у процесі професійної підготовки спрямоване на формування здатності забезпечувати базовий рівень кібербезпеки, реалізовувати заходи кібергігієни, здійснювати моніторинг інформаційних систем та захищати цифрові ресурси освітнього середовища. Набуті компетентності є важливими як для майбутньої професійної діяльності випускників, так і для безпечного використання цифрових технологій у процесі організації та здійснення освітньої діяльності. Зокрема, фахівці цифрових технологій повинні вміти забезпечувати захист освітніх платформ, електронних освітніх ресурсів, персональних даних користувачів, мережевої інфраструктури закладів освіти та інших інформаційних ресурсів.

З огляду на це, до змісту професійної підготовки доцільно включати вивчення сучасних програмних засобів, які широко використовуються у сфері кібербезпеки та захисту даних. Серед них особливу увагу привертають Wireshark, Splunk Enterprise, Kali Linux та Cisco Packet Tracer (Wireshark Foundation, n.d.; Splunk Inc., n.d.; Offensive Security, n.d.; Cisco Systems, Inc., n.d.)., які забезпечують реалізацію різних аспектів інформаційної безпеки та дозволяють формувати практичні навички роботи з інструментами професійного рівня.

Для визначення дидактичного потенціалу зазначених програмних засобів у дослідженні здійснено їх порівняльний аналіз за такими критеріями, як функціональне призначення, можливості використання в освітньому процесі, практична цінність для майбутньої професійної діяльності, переваги та обмеження застосування. Аналіз базується на актуальних характеристиках програмних продуктів і сучасних тенденціях розвитку інформаційної безпеки станом на 2026 рік. Результати проведеного аналізу дозволяють обґрунтувати доцільність інтеграції зазначених програмних засобів у процес підготовки майбутніх фахівців цифрових технологій та визначити їх місце в реалізації методики формування готовності до застосування програмного забезпечення захисту даних.

Wireshark – це безкоштовний відкритий аналізатор мережевого трафіку (packet sniffer), який у реальному часі захоплює та аналізує мережеві пакети. Версія Wireshark 4.6.6 (Wireshark Foundation) (станом на травень 2026 року) підтримує сучасні мережеві протоколи, зокрема QUIC, HTTP/3, TLS 1.3, DNS-over-HTTPS (DoH), інструмент не має власного вбудованого ШІ, але підтримує інтеграцію з моделями (ChatGPT, Claude, Gemini) через Model Context Protocol. Завдяки розвинутим засобам фільтрації, сортування та візуалізації даних програмне забезпечення надає можливість здійснювати глибокий аналіз мережевих з’єднань, виявляти аномалії в роботі мережі, досліджувати причини збоїв та оцінювати рівень захищеності інформаційного середовища (Олексюк, 2024).

В процесі підготовки фахівців цифрових технологій, Wireshark є одним з основних інструментів для навчання аналізу мережевого трафіку, основ кібергігієни та розвміння принципів захисту даних. У професійній діяльності ПЗ використовують мережеві адміністратори та фахівці з інформаційної безпеки для діагностики проблем, виявлення витоків даних та оптимізації захисту.

Серед головних переваг – повна безкоштовність, кросплатформенність, висока деталізація аналізу та можливість інтеграції з іншими інструментами (Kali Linux, Splunk). Водночас Wireshark вимагає ґрунтовних знань мереж, є

складним для початківців і виконує лише функцію аналізу, не забезпечуючи блокування загроз у реальному часі. Крім того, його використання пов’язане з етичними та правовими аспектами, оскільки несанкціоноване захоплення трафіку може порушувати законодавство про захист персональних даних.

Splunk Enterprise – це комерційна SIEM-платформа (Security Information and Event Management), призначена для централізованого збору, аналізу, кореляції та візуалізації даних подій і логів з різних джерел. Версія Splunk Enterprise 10.4 (Splunk) (станом на травень 2026 року) значно розширена завдяки інтеграції штучного інтелекту та машинного навчання, що дозволяє автоматизовано виявляти складні загрози, включаючи Shadow AI та аномальну активність у хмарних середовищах і контейнерах (Kubernetes).

Платформа забезпечує збір логів з тисяч джерел – серверів, мереж, хмарних сервісів, додатків та кінцевих пристроїв. Важливою перевагою Splunk Enterprise є використання спеціалізованої мови запитів та обробки даних – SPL (Search Processing Language), яка забезпечує можливість виконання складного аналізу великих обсягів машинно-генерованих даних. Застосування спеціалізованої мови запитів (SPL) дозволяє здійснювати пошук, фільтрацію, аналізу та візуалізації великих обсягів машинно-генерованих даних і логів, подій із різних джерел інформації, що сприяє своєчасному виявленню потенційних загроз інформаційній безпеці та аномалій у функціонуванні інформаційних систем.

Основним призначенням ПЗ є аналіз подій у режимі реального часу, що дає змогу ефективно виявляти підозрілу активність, оцінювати стан інформаційної інфраструктури та приймати обґрунтовані рішення щодо реагування на інциденти безпеки. Завдяки механізмам кореляції подій Splunk Enterprise дозволяє встановлювати взаємозв’язки між різними подіями та джерелами даних, що є особливо важливим для розслідування кіберінцидентів (Cyber incident investigation) і моніторингу складних інформаційних систем.

Серед ключових переваг платформи – висока масштабованість, потужні аналітичні можливості з використанням ШІ, а також широка інтеграція з іншими

інструментами (Wireshark, мережеве обладнання Cisco, AzureWM, Amazon Web Services) (Wireshark Foundation, n.d.; Cisco Systems, Inc., n.d.; Microsoft, n.d.; Amazon Web Services, n.d.). Однак Splunk має суттєві недоліки. Платформа є комерційною і досить дорогою, особливо для невеликих організацій. Вона вимагає спеціальної підготовки для ефективної роботи з пошуковою мовою SPL, а також не є безкоштовною на відміну від open source альтернатив, таких як ELK Stack (Elasticsearch, Logstash, Kibana).

Одним із найбільш поширених спеціалізованих програмних засобів для навчання та практичної підготовки фахівців цифрових технологій у сфері кібербезпеки є дистрибутив *Kali Linux* (Offensive Security, n.d.). Він являє собою спеціалізовану операційну систему на базі Linux, розроблену для проведення тестування на проникнення, аналізу вразливостей та аудиту інформаційної безпеки. Завдяки широкому набору інтегрованих інструментів Kali Linux використовується як у професійній діяльності фахівців з кібербезпеки, так і в освітньому процесі підготовки майбутніх фахівців цифрових технологій.

Функціональні можливості Kali Linux охоплюють широкий спектр завдань із забезпечення інформаційної безпеки. До складу дистрибутива входить понад 600 спеціалізованих програмних інструментів, призначених для аналізу мережевої інфраструктури, виявлення вразливостей, тестування захищеності інформаційних систем та дослідження кіберінцидентів. Серед найбільш поширених інструментів слід виокремити Nmap, який використовується для сканування мереж і виявлення активних вузлів та сервісів; Metasploit Framework, що забезпечує можливість аналізу та моделювання експлуатації вразливостей; Burp Suite для оцінювання рівня захищеності вебзастосунків; Wireshark для захоплення й аналізу мережевого трафіку; Aircrack-ng для дослідження безпеки бездротових мереж стандарту Wi-Fi.

Важливим компонентом Kali Linux є наявність інструментів цифрового аналізу, зокрема Autopsy (Basis Technology, n.d.) та Volatility (Volatility Foundation, n.d.), які дозволяють здійснювати аналіз цифрових слідів, дослідження файлових систем і виявлення несанкціонованої діяльності в

інформаційних системах. Крім того, дистрибутив містить спеціалізовані засоби дешифрування (John the Ripper та Hashcat) призначені для аналізу стійкості паролів і дослідження криптографічних механізмів захисту інформації.

Суттєвою перевагою платформи є підтримка віртуалізації та можливість створення спеціалізованих образів для середовищ VMware, VirtualBox і KVM (VMware, n.d.; Oracle, n.d.; Linux Foundation, n.d.). Це забезпечує безпечне використання інструментів кібербезпеки в ізольованому навчальному середовищі та сприяє моделюванню реальних сценаріїв професійної діяльності без ризику для освітніх інформаційних систем.

У професійній діяльності Kali Linux широко застосовується для проведення тестування на проникнення, виявлення вразливостей інформаційних систем, оцінювання рівня захищеності мережевої інфраструктури та моделювання можливих кіберзагроз. Використання цього програмного забезпечення дозволяє фахівцям здійснювати комплексний аналіз безпеки інформаційних систем і розробляти рекомендації щодо підвищення їхньої захищеності.

У контексті освітнього процесу підготовки майбутніх фахівців цифрових технологій Kali Linux має значний дидактичний потенціал. Використання зазначеного дистрибутива сприяє формуванню практичних навичок роботи з інструментами етичного хакінгу, аналізу кіберзагроз, оцінювання вразливостей та цифрової криміналістики. Це дозволяє наблизити навчальну діяльність до реальних умов професійної практики та забезпечує розвиток компетентностей у сфері цифрових технологій.

У корпоративному середовищі Kali Linux застосовується під час проведення аудитів інформаційної безпеки, організації навчань типу Red Team та Blue Team, а також для оцінювання стійкості інформаційної інфраструктури до зовнішніх і внутрішніх кіберзагроз. Завдяки цьому програмний продукт став одним із найбільш популярних інструментів серед фахівців із кібербезпеки.

До основних переваг Kali Linux належать безкоштовне розповсюдження та відкритий вихідний код, наявність великої кількості попередньо налаштованих

інструментів інформаційної безпеки, підтримка портативного режиму роботи з використанням Live USB(не потребує встановлення). Крім того, дистрибутив регулярно оновлюється міжнародною спільнотою розробників (GitHub, n.d.), що забезпечує своєчасне впровадження нових функціональних можливостей, актуалізацію інструментів кібербезпеки та усунення виявлених вразливостей.

Водночас застосування Kali Linux має певні обмеження. Насамперед дистрибутив орієнтований переважно на виконання завдань аналізу захищеності та тестування інформаційних систем, що знижує його доцільність для повсякденного використання як універсальної операційної системи. Крім того, ефективне використання більшості інструментів потребує ґрунтовних знань операційних систем сімейства Linux, мережевих технологій та основ кібербезпеки, що може ускладнювати його опанування здобувачами освіти початкового рівня підготовки. Окремої уваги потребує питання етичного використання інструментів дистрибутива, оскільки за відсутності належної професійної підготовки та контролю окремі засоби можуть бути використані не за призначенням. Тому застосування Kali Linux в освітньому процесі повинно супроводжуватися формуванням у здобувачів освіти культури кібербезпеки, відповідальності та дотримання етичних норм професійної діяльності.

Cisco Packet Tracer – це безкоштовний мережевий симулятор, розроблений компанією Cisco (Cisco Systems), який широко застосовується у навчальному процесі для моделювання комп’ютерних мереж та вивчення основ кібербезпеки. На платформі https://www.netacad.com доступні усі актуальні версії програми, які отримують постійне оновлення, зокрема розширені елементи інтеграції штучного інтелекту.

Cisco Packet Tracer надає можливість симулювати повноцінні мережеві середовища, включаючи роутери, комутатори, firewall та кінцеві пристрої. Важливою перевагою для вивчення захисту даних є можливість налаштування списків контролю доступу (ACL), створення VPN-тунелів, базових механізмів автентифікації та фільтрації трафіку. Програма також дозволяє моделювати

типові мережеві атаки (DoS, IP-spoofing, MAC-flooding) та відпрацьовувати заходи захисту від них.

У професійній діяльності Cisco Packet Tracer використовується у кількох напрямах. У сфері кібербезпеки він застосовується для навчання моделюванню захищених мереж, тестування конфігурацій безпеки та аналізу потенційних вразливостей. В освітньому процесі програма є ефективним інструментом для проведення інтерактивних занять із здобувачами, дозволяючи формувати практичні навички роботи з мережами та базовим захистом даних. У бізнес-середовищі Packet Tracer використовується для моделювання мереж перед їх реальним розгортанням.

Серед основних переваг симулятора варто виділити його повну безкоштовність для студентів і викладачів у рамках Cisco Networking Academy (Cisco Systems, Inc., n.d.), інтуїтивний інтерфейс, можливість роботи без реального обладнання, а також хорошу інтеграцію з Wireshark для глибокого аналізу мережевого трафіку.

Водночас Packet Tracer має певні обмеження. Як симулятор він не повністю відтворює поведінку реального мережевого обладнання, має певну обмежену реалістичність. Крім того, програма орієнтована переважно на мережеве обладнання Cisco, що знижує її універсальність. Також вона не призначена для проведення глибокого пентестингу та складних сценаріїв оцінювання захищеності інформаційних систем.

Відбір програмного забезпечення захисту даних для підготовки майбутніх фахівців цифрових технологій здійснювався з урахуванням сукупності педагогічних, методичних і технічних критеріїв, що забезпечують ефективність його використання в освітньому процесі. До основних критеріїв віднесено: професійну релевантність, яка передбачає відповідність функціональних можливостей програмного забезпечення сучасним вимогам інформаційної безпеки та майбутньої професійної діяльності фахівців цифрових технологій; дидактичну доцільність, що забезпечує можливість реалізації цілей, змісту, методів і форм навчання; практичну спрямованість, яка полягає у створенні умов

для формування практичних навичок аналізу мережевого трафіку, шифрування даних, моделювання захищених мереж, моніторингу подій інформаційної безпеки та тестування захищеності інформаційних систем; доступність і відкритість, що передбачає використання безкоштовного або навчального програмного забезпечення, доступного для встановлення та використання в закладах вищої освіти; сумісність із цифровим освітнім середовищем, яка забезпечує інтеграцію програмних засобів із системами управління навчанням, віртуальними лабораторіями та кіберполігонами; актуальність і підтримку розробником, що гарантує регулярне оновлення програмного забезпечення відповідно до сучасних викликів кібербезпеки; безпечність використання, яка передбачає можливість виконання навчальних завдань у контрольованому віртуальному середовищі без ризику для реальної інформаційної інфраструктури.

Відповідно до визначених критеріїв для реалізації розробленої методики було обрано програмні засоби Wireshark, Cisco Packet Tracer, VeraCrypt, Kali Linux та Splunk, які забезпечують комплексне формування професійних компетентностей майбутніх фахівців цифрових технологій у сфері застосування програмного забезпечення захисту даних, поєднуючи теоретичну підготовку з практичною діяльністю у змодельованих умовах професійного середовища.

Висновки до розділу 1

Аналіз сучасного стану проблеми захисту даних у професійній діяльності фахівців цифрових технологій свідчить про її високу актуальність і недостатню вирішеність. Стрімка цифровізація освітнього процесу, поширення хмарних технологій та зростання кількості кіберзагроз зумовили необхідність якісно нового рівня підготовки педагогів у сфері кібербезпеки. Водночас у більшості закладів вищої освіти питання захисту даних залишаються фрагментарними, а підготовка майбутніх фахівців часто має декларативний характер.

Теоретичні засади професійної підготовки фахівців цифрових технологій у контексті кібербезпеки ґрунтуються на компетентнісному, ризик-орієнтованому, діяльнісному та андрагогічному підходах. Вони дозволяють розглядати захист даних не як суто технічну задачу, а як комплексну професійну і педагогічну компетентність, що включає технічні навички, правову обізнаність, етичну чутливість та вміння передавати ці знання здобувачам.

Сучасні освітні стандарти передбачають певну підготовку здобувачів у сфері інформаційної безпеки, проте вона носить переважно загальний або технічний характер. У більшості програм відсутня окрема обов’язкова дисципліна з кібербезпеки та захисту персональних даних. Теми захисту даних найчастіше інтегровані в дисципліни «Комп’ютерні мережі», «Інформаційна безпека» або «Цифрові технології в освіті», що не дозволяє сформувати цілісну компетентність. Крім того, у стандартах недостатньо відображена педагогічна складова – вміння майбутніх викладачів передавати знання з кібергігієни та захисту даних студентам закладів професійної (професійно-технічної) освіти.

Позитивним аспектом є поступове посилення цифрової складової стандартів, зокрема впровадження компетентностей, пов’язаних з інформаційною безпекою. Однак глибина підготовки залишається недостатньою для реальних викликів сучасності – зростання кіберзагроз, масового використання хмарних сервісів, обробки великих обсягів персональних даних та активної цифровізації освіти.

У контексті компетентнісного підходу до підготовки фахівців цифрових технологій важливого значення набуває використання спеціалізованого програмного забезпечення захисту даних як інструменту формування професійних компетентностей у сфері інформаційної безпеки та кібербезпеки. Застосування таких програмних засобів, як Wireshark, Cisco Packet Tracer, VeraCrypt, Nmap та Splunk, забезпечує формування системи знань і практичних навичок, необхідних для аналізу мережевого трафіку, виявлення потенційних загроз інформаційним системам, проєктування та налаштування захищених комп'ютерних мереж, використання криптографічних механізмів захисту даних, проведення аудиту безпеки мережевої інфраструктури та моніторингу подій інформаційної безпеки.

Комплексне використання зазначеного програмного забезпечення в освітньому процесі створює умови для поєднання теоретичної підготовки з практичною діяльністю, забезпечує формування когнітивного, діяльнісного, мотиваційного та рефлексивного компонентів готовності до застосування засобів захисту даних. Водночас інтеграція цих інструментів у зміст фахових дисциплін дозволяє моделювати реальні професійні ситуації, наближені до умов сучасного цифрового середовища, що сприяє розвитку навичок аналізу ризиків, прийняття обґрунтованих рішень та ефективного використання програмних засобів інформаційної безпеки. Отже, використання Wireshark, Cisco Packet Tracer, VeraCrypt, Nmap та Splunk є доцільним і методично виправданим засобом підготовки майбутніх фахівців цифрових технологій до професійної діяльності в умовах зростання вимог до захисту інформаційних ресурсів та забезпечення кібербезпеки.

Таким чином, у першому розділі теоретично обґрунтовано необхідність удосконалення підготовки фахівців цифрових технологій шляхом посилення практичної, педагогічної та правової складових захисту даних, що створює підґрунтя для розробки відповідної методики в наступних розділах дослідження.

РОЗДІЛ 2
РОЗРОБКА МЕТОДИКИ ПІДГОТОВКИ ФАХІВЦІВ ДО ЗАСТОСУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ДАНИХ

2.1. Методичні засади формування готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних

Розроблення та впровадження методики підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних потребує визначення структури їхньої готовності до здійснення відповідної професійної діяльності. Визначення компонентів, критеріїв і показників готовності є необхідною умовою проведення педагогічного експерименту та подальшого оцінювання ефективності запропонованої методики.

У науковій літературі готовність до професійної діяльності (Кулакова, Л., & Онокало, О. 2025). розглядається як інтегративне особистісне утворення, що поєднує систему знань, вмінь, навичок, професійно значущих якостей, мотиваційних установок та здатність до ефективного виконання професійних функцій. З урахуванням специфіки дослідження готовність майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних визначається як інтегративна характеристика особистості, яка відображає рівень сформованості мотивації, професійних знань, практичних вмінь та здатності до самостійного використання сучасних програмних засобів захисту інформації в умовах професійної діяльності.

Сучасні тенденції розвитку цифрових технологій, стрімке зростання обсягів інформаційних ресурсів та поширення кіберзагроз зумовлюють необхідність удосконалення професійної підготовки майбутніх фахівців цифрових технологій у сфері захисту даних. Особливого значення набуває формування готовності здобувачів освіти до ефективного використання програмного забезпечення захисту даних у професійній діяльності, що

передбачає не лише оволодіння відповідними технічними знаннями та практичними навичками, а й розвиток здатності аналізувати ризики інформаційної безпеки, приймати обґрунтовані рішення щодо захисту інформаційних ресурсів та адаптуватися до динамічних змін цифрового середовища.

Методичні засади формування готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних ґрунтуються на положеннях компетентнісного, системного, діяльнісного, особистісно орієнтованого, практико-орієнтованого та технологічного підходів. Їх комплексне використання забезпечує цілісність освітнього процесу та спрямовує його на формування професійної готовності як інтегративної характеристики особистості, що поєднує знання, вміння, ціннісні орієнтації, мотивацію та здатність до професійного саморозвитку.

З метою систематизації методологічних засад дослідження в табл. 2.1 представлено характеристику основних наукових підходів та їх роль у формуванні готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних. Аналіз наведених підходів свідчить, що кожен із них виконує окрему функцію в структурі професійної підготовки, проте лише їх інтеграція забезпечує досягнення цілісного освітнього результату.

Таблиця 2.1

Характеристика методологічних підходів до формування готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних

Методологічний підхід	Сутність підходу	Роль у формуванні готовності до застосування ПЗ захисту даних
Компетентнісний	Орієнтує освітній процес на формування професійних компетентностей, необхідних для ефективної діяльності в умовах цифрового суспільства.	Забезпечує формування знань, вмінь, навичок та досвіду застосування програмного забезпечення захисту даних у професійній діяльності фахівців цифрових технологій.
Системний	Розглядає професійну підготовку як цілісну педагогічну систему, елементи якої перебувають у взаємозв’язку та взаємозалежності.	Забезпечує узгодженість мети, змісту, методів, форм, засобів навчання та результатів підготовки до застосування програмного забезпечення захисту даних.

Продовження таблиці 2.1

Методологічний підхід	Сутність підходу	Роль у формуванні готовності до застосування ПЗ захисту даних
Особистісно орієнтований	Враховує індивідуальні особливості, потреби, інтереси та професійні можливості здобувачів освіти.	Забезпечує розвиток професійної мотивації, відповідальності за безпечне використання цифрових технологій та готовності до саморозвитку у сфері захисту даних.
Практико-орієнтований	Спрямований на наближення освітнього процесу до реальних умов професійної діяльності.	Формує досвід використання програмного забезпечення захисту даних у типових і проблемних ситуаціях шляхом виконання проєктів, кейсів, лабораторних робіт та роботи у віртуальних лабораторіях.
Технологічний	Передбачає використання сучасних цифрових технологій, спеціалізованого програмного забезпечення та інноваційних засобів навчання.	Забезпечує інтеграцію програмних засобів захисту даних, хмарних сервісів, кіберполігонів і віртуальних середовищ у процес професійної підготовки майбутніх фахівців цифрових технологій.
Діяльнісний	Орієнтує освітній процес на засвоєння знань через активну навчально-пізнавальну та професійну діяльність, виконання практичних завдань і розв'язання професійних проблем.	Сприяє формуванню практичних умінь і навичок застосування програмного забезпечення захисту даних, розвитку здатності приймати обґрунтовані рішення щодо забезпечення інформаційної безпеки в реальних і змодельованих професійних ситуаціях.

Взаємозв’язок зазначених підходів та їх місце у структурно-функціональній моделі підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних відображено на рис. 2.1.

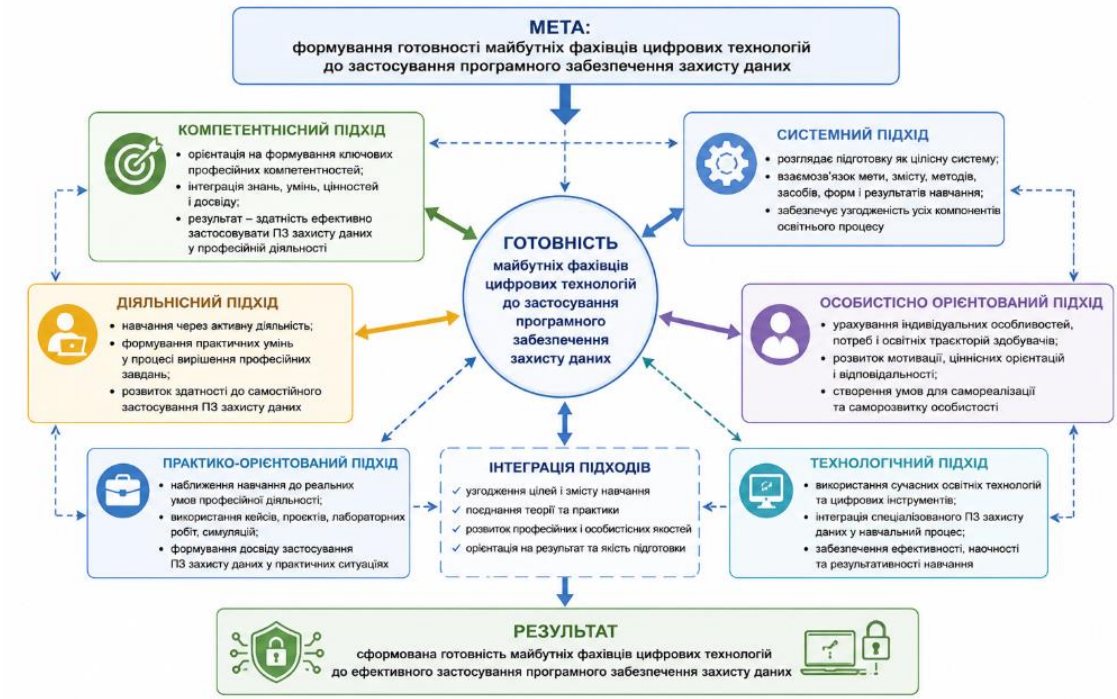

Рис. 2.1. Взаємозв'язок методологічних підходів у системі формування готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних

Визначальним у межах дослідження є компетентнісний підхід, який орієнтує освітній процес на формування здатності майбутніх фахівців ефективно використовувати програмне забезпечення захисту даних для розв'язання професійних завдань. Реалізація цього підходу передбачає набуття здобувачами освіти знань щодо сучасних технологій інформаційної безпеки, принципів функціонування засобів захисту інформації, нормативно-правових основ обробки та захисту персональних даних.

Системний підхід забезпечує розгляд процесу підготовки майбутніх фахівців цифрових технологій як цілісної педагогічної системи, структурними компонентами якої є мета, зміст, форми, методи, засоби навчання та результати підготовки. У межах цього підходу готовність до застосування програмного забезпечення захисту даних розглядається як багатокомпонентне утворення, що включає когнітивний, діяльнісний, мотиваційний та рефлексивний компоненти.

Діяльнісний підхід передбачає формування готовності через активне залучення здобувачів освіти до практичної діяльності з використанням сучасного

програмного забезпечення захисту даних. Його реалізація забезпечується виконанням лабораторних робіт, практичних завдань, навчальних проєктів, кейсів, а також роботою у віртуальних лабораторіях і кіберполігонах. Така організація навчання створює умови для набуття досвіду застосування засобів інформаційної безпеки в ситуаціях, наближених до реальної професійної діяльності.

Особистісно орієнтований підхід спрямований на врахування індивідуальних освітніх потреб, професійних інтересів та рівня підготовленості здобувачів освіти. Його реалізація забезпечує формування внутрішньої мотивації до опанування сучасних технологій захисту даних, розвитку професійної відповідальності та усвідомлення значущості інформаційної безпеки в умовах цифрового суспільства.

Практико-орієнтований підхід передбачає наближення змісту підготовки до реальних умов професійної діяльності фахівців цифрових технологій. У межах дослідження це реалізується шляхом використання сучасного програмного забезпечення захисту даних, зокрема Wireshark, Cisco Packet Tracer, VeraCrypt, Nmap, Kali Linux, Splunk (Wireshark Foundation, n.d.; Cisco Systems, Inc., n.d.; IDRIX, n.d.; Nmap Project, n.d.; Offensive Security, n.d.; Splunk Inc., n.d.) та інших інструментів, що широко застосовуються в галузі інформаційної безпеки.

Технологічний підхід забезпечує використання сучасних цифрових освітніх технологій, електронних навчальних ресурсів, систем управління навчанням, віртуальних лабораторій та кіберполігонів для організації освітнього процесу. Застосування таких засобів дозволяє моделювати різноманітні сценарії кіберзагроз, відпрацьовувати алгоритми реагування на інциденти інформаційної безпеки та здійснювати контроль сформованості професійних компетентностей майбутніх фахівців.

Відповідно до визначених методологічних підходів формування готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних доцільно розглядати як

цілеспрямований і поетапний процес, результатом якого є сформованість системи знань, вмінь, цінностей і професійно значущих якостей, необхідних для ефективного використання сучасних засобів захисту інформації в умовах професійної діяльності.

Проведений аналіз теоретичних засад підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних дозволив обґрунтувати методичні основи розроблюваної методики та визначити її структурні компоненти. Встановлено, що ефективне формування готовності до використання програмних засобів захисту інформації забезпечується завдяки комплексному поєднанню компетентнісного, системного, діяльнісного, практико-орієнтованого та особистісно орієнтованого підходів, які створюють методологічне підґрунтя професійної підготовки майбутніх фахівців цифрових технологій.

Реалізація запропонованої методики передбачає інтеграцію змісту інформаційної безпеки у фахові дисципліни, використання сучасного програмного забезпечення захисту даних, залучення здобувачів освіти до виконання лабораторних робіт, кейсів, проєктних завдань, роботи у віртуальних лабораторіях та кіберполігонах.

У результаті дослідження визначено структуру готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних, яка охоплює когнітивний, діяльнісний, мотиваційний та рефлексивний компоненти. Особливістю запропонованого підходу є подвійна спрямованість підготовки, що передбачає формування не лише здатності використовувати програмне забезпечення захисту даних у власній професійній діяльності, а й готовності здійснювати освітню діяльність щодо формування культури кібербезпеки та захисту інформації у здобувачів освіти.

Для забезпечення об’єктивного оцінювання результативності розробленої методики визначено критерії, показники та рівні сформованості готовності до застосування програмного забезпечення захисту даних, які відображають ступінь розвитку кожного з її структурних компонентів. Запропонований

діагностичний інструментарій створює підґрунтя для проведення педагогічного експерименту та подальшої перевірки ефективності розробленої методики підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних.

У межах розроблюваної методики підготовки фахівців цифрових технологій важливим є визначення методичних засад формування їхньої готовності до застосування програмного забезпечення захисту даних. Реалізація зазначеної готовності забезпечується через поетапну організацію освітнього процесу, інтеграцію змісту інформаційної безпеки в професійно-орієнтовані дисципліни та використання спеціалізованого програмного забезпечення у навчальній діяльності.

Методика ґрунтується на поєднанні традиційних та інноваційних підходів до навчання, зокрема компетентнісного, діяльнісного та практико-орієнтованого, що забезпечує формування не лише теоретичних знань, а й практичних вмінь застосування засобів захисту даних у реальних та імітаційних умовах.

Основними методами реалізації методики визначено: проблемне навчання, проєктні технології, кейс-метод, лабораторні роботи з використанням програмного забезпечення захисту даних, а також симуляційні завдання, що моделюють реальні кіберзагрози.

Організаційними формами навчання виступають лекції, практичні та лабораторні заняття, самостійна робота студентів, а також індивідуальні та групові проєкти, спрямовані на застосування програмних засобів захисту інформації.

Впровадження запропонованої методики підготовки фахівців цифрових технологій до застосування програмного забезпечення захисту даних в освітній процес здійснюється як цілісна, поетапно організована педагогічна система, що охоплює всі складові професійної підготовки здобувачів освіти. Її реалізація передбачає інтеграцію змісту інформаційної безпеки та відповідного програмного забезпечення у структуру професійно орієнтованих навчальних

дисциплін, зокрема таких, що пов’язані з комп’ютерними мережами, системним адмініструванням, кібербезпекою та технологіями захисту інформації.

Методика реалізується через поєднання аудиторної, практичної та самостійної діяльності здобувачів освіти, що забезпечує поступове формування всіх компонентів готовності до застосування програмного забезпечення захисту даних. На лекційних заняттях забезпечується формування теоретичної бази знань щодо принципів функціонування засобів захисту інформації, архітектури сучасних систем безпеки, а також основних загроз інформаційним ресурсам. Лабораторні заняття спрямовуються на опанування студентами нормативно-правової бази та конкретних інструментів програмного забезпечення захисту даних, зокрема засобів криптографічного захисту та моніторингу безпеки.

Особливе значення у реалізації методики відводиться практико-орієнтованому навчанню, яке передбачає виконання навчально-професійних завдань, максимально наближених до реальних умов функціонування інформаційних систем. З цією метою застосовуються кейс-методи, моделювання ситуацій кіберзагроз, проєктна діяльність, а також виконання індивідуальних і групових завдань із розгортання та налаштування програмного забезпечення захисту даних.

Важливою складовою реалізації методики є використання хмарних сервісів (TryHackMe), віртуальних лабораторій (CyberRanges) та спеціалізованих програмних середовищ (WireShark, Cisco Packet Tracer, Kali Linux), що дозволяє створювати безпечні навчальні умови для відпрацювання навичок без ризику для реальних інформаційних систем. Це забезпечує можливість багаторазового виконання практичних операцій, аналізу помилок та корекції дій здобувачів освіти.

Окрему роль у впровадженні методики відіграє організація самостійної роботи студентів, спрямованої на поглиблення знань, дослідження сучасних програмних засобів захисту даних, аналіз актуальних кіберзагроз та підготовку власних проєктних рішень у сфері інформаційної безпеки. Такий підхід

забезпечує розвиток аналітичного мислення, професійної автономності та здатності до самонавчання.

Готовність до застосування програмного забезпечення захисту даних у випускника цієї спеціальності – це інтегративна характеристика, яка поєднує технічну спроможність педагога та його методичну здатність формувати відповідні компетентності в здобувачів. Вона має чітко виражену подвійну спрямованість:

– особиста готовність (як педагога, який працює з даними здобувачів, електронними журналами, платформами дистанційного навчання);

– педагогічна готовність (як педагога, який навчає здобувачів застосовувати захист даних у майбутній професії).

У структурі готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних доцільно виокремити чотири взаємопов’язані компоненти: когнітивний, діяльнісний, мотиваційний та рефлексивний.

Когнітивний компонент характеризує систему знань, необхідних для ефективного використання програмного забезпечення захисту даних у професійній та педагогічній діяльності. Він охоплює знання основ кібербезпеки, принципів захисту інформації та персональних даних, сучасних кіберзагроз і способів протидії їм. Важливою складовою є розвміння можливостей спеціалізованого програмного забезпечення захисту даних, принципів його функціонування, а також знання нормативно-правової бази у сфері інформаційної безпеки та захисту персональних даних. Крім того, цей компонент передбачає усвідомлення педагогічних аспектів формування цифрової безпеки та кібергігієни у здобувачів освіти.

Діяльнісний (операційний) компонент відображає здатність майбутнього фахівця застосовувати набуті знання на практиці. Він включає вміння використовувати програмне забезпечення захисту даних для забезпечення конфіденційності, цілісності та доступності інформації, здійснювати налаштування базових засобів захисту, аналізувати мережевий трафік, виявляти

потенційні загрози та запобігати їм. Водночас цей компонент охоплює методичні вміння, необхідні для навчання здобувачів професійної освіти основам кібербезпеки, розроблення навчальних матеріалів, проведення практичних занять та використання цифрових інструментів для формування навичок захисту даних.

Мотиваційний компонент визначає ставлення майбутнього фахівця до проблеми захисту даних та його готовність до відповідальної професійної діяльності. Він характеризується усвідомленням значущості інформаційної безпеки в сучасному цифровому суспільстві, прагненням до постійного вдосконалення власних компетентностей, зацікавленістю у використанні сучасних засобів захисту інформації та готовністю формувати відповідальне ставлення до захисту даних у здобувачів освіти. До цього компонента також належать етичні та правові орієнтири, що забезпечують дотримання принципів конфіденційності, академічної доброчесності та професійної відповідальності.

Рефлексивний компонент характеризує здатність майбутнього фахівця до самоаналізу, самоконтролю та професійного самовдосконалення. Він передбачає вміння оцінювати власний рівень підготовленості до застосування програмного забезпечення захисту даних, виявляти прогалини у знаннях і навичках, аналізувати результати власної діяльності та визначати напрями подальшого професійного розвитку. Важливою ознакою цього компонента є готовність до безперервної освіти, самостійного опанування нових технологій і засобів захисту даних, а також здатність адаптуватися до постійних змін у сфері цифрових технологій та кібербезпеки.

Сукупність зазначених компонентів забезпечує цілісну готовність майбутнього фахівця цифрових технологій до ефективного застосування програмного забезпечення захисту даних у професійній та педагогічній діяльності.

Рівні сформованості готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних

Для оцінювання результативності підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних доцільно виокремити чотири рівні сформованості готовності: *низький, середній, достатній та високий.* Кожен рівень відображає ступінь сформованості когнітивного, діяльнісного, мотиваційного та рефлексивного компонентів готовності й характеризує здатність здобувача освіти ефективно використовувати програмні засоби захисту даних у професійній діяльності.

Низький рівень характеризується фрагментарністю знань щодо основ інформаційної безпеки, нормативно-правових засад захисту даних та принципів функціонування програмного забезпечення захисту інформації. Здобувач освіти має лише загальне уявлення про окремі засоби захисту даних, не розуміє особливостей їх практичного використання та не здатний самостійно обирати інструменти для розв'язання професійних завдань.

Практичні вміння застосування програмного забезпечення захисту даних сформовані недостатньо або відсутні. Виконання лабораторних завдань можливе лише за детальними інструкціями викладача, а під час виникнення нестандартних ситуацій студент не може самостійно приймати рішення та виправляти помилки. Здобувач освіти не володіє навичками аналізу мережевого трафіку, налаштування базових механізмів захисту чи використання засобів шифрування даних.

Мотивація до вивчення засобів захисту інформації має ситуативний характер. Усвідомлення значущості захисту даних для професійної діяльності виражене недостатньо, а питання кібербезпеки сприймаються як другорядний елемент професійної підготовки. Самоаналіз власної діяльності здійснюється епізодично або відсутній, що негативно впливає на професійне самовдосконалення.

Такий рівень готовності не забезпечує ефективного виконання професійних завдань, пов'язаних із використанням програмного забезпечення захисту даних, і потребує суттєвої корекції підготовки.

Середній рівень характеризується наявністю базових знань щодо інформаційної безпеки, кіберзагроз, принципів захисту персональних даних та функціональних можливостей окремих програмних засобів захисту інформації. Здобувач освіти орієнтується в основних поняттях кібербезпеки та розуміє призначення найпоширеніших інструментів захисту даних.

Практична діяльність здійснюється переважно за типовими алгоритмами. Студент може виконувати стандартні операції у програмних середовищах Wireshark, Cisco Packet Tracer або VeraCrypt, проте відчуває труднощі під час розв’язання складніших професійних завдань. Аналіз ризиків та оцінювання рівня захищеності інформаційних ресурсів виконуються на елементарному рівні.

Мотиваційний компонент характеризується позитивним ставленням до питань захисту даних і розвмінням необхідності дотримання правил кібергігієни. Водночас потреба у професійному саморозвитку ще не набула стійкого характеру. Самоаналіз результатів власної діяльності здійснюється нерегулярно та переважно після зовнішнього стимулювання з боку викладача.

Цей рівень забезпечує виконання типових професійних завдань, однак не гарантує достатньої автономності та ефективності діяльності в умовах виникнення нових кіберзагроз або нестандартних ситуацій.

Достатній рівень характеризується сформованою системою знань щодо нормативно-правових, організаційних та технологічних аспектів захисту даних. Здобувач освіти розуміє принципи функціонування сучасних програмних засобів захисту інформації, орієнтується у видах кіберзагроз та здатний обґрунтовано добирати інструменти для забезпечення інформаційної безпеки.

Практичні вміння дозволяють самостійно використовувати програмне забезпечення захисту даних під час виконання навчально-професійних завдань. Студент упевнено працює з мережевими аналізаторами, засобами шифрування даних, системами моделювання мережевої інфраструктури та іншими програмними продуктами. Він здатний здійснювати аналіз мережевого трафіку, налаштовувати базові механізми захисту, виявляти потенційні загрози та пропонувати шляхи їх усунення.

Мотиваційний компонент характеризується стійким усвідомленням важливості захисту даних у професійній діяльності. Здобувач освіти демонструє відповідальне ставлення до питань інформаційної безпеки, дотримується принципів кібергігієни та прагне до постійного професійного вдосконалення.

Рефлексивний компонент виявляється у здатності до систематичного самоаналізу результатів діяльності, оцінювання власного рівня підготовки та планування подальшого професійного розвитку. Студент бере участь у додаткових освітніх заходах, опановує нові програмні засоби та самостійно розширює власні компетентності.

Достатній рівень є оптимальним для випускника спеціальності 015.39 «Професійна освіта (Цифрові технології)», оскільки забезпечує готовність до ефективного використання програмного забезпечення захисту даних у професійній діяльності.

Високий рівень характеризується системним і глибоким володінням знаннями у сфері інформаційної безпеки, захисту персональних даних та сучасних технологій кібербезпеки. Здобувач освіти демонструє цілісне розвміння принципів функціонування програмного забезпечення захисту даних, сучасних моделей загроз та міжнародних стандартів інформаційної безпеки.

Практична підготовка забезпечує здатність самостійно розв’язувати складні професійні завдання, здійснювати комплексний аналіз кіберзагроз, впроваджувати програмні засоби захисту даних та оцінювати ефективність їх використання. Студент упевнено працює з різними категоріями програмного забезпечення захисту інформації, інтегрує декілька інструментів у межах одного проєкту та демонструє високий рівень автономності під час виконання професійних завдань.

Мотиваційний компонент характеризується високим рівнем професійної відповідальності, внутрішньою потребою до постійного саморозвитку та активною позицією щодо поширення культури кібербезпеки. Майбутній фахівець усвідомлює власну роль у забезпеченні інформаційної безпеки організації та готовий виступати провідником сучасних практик захисту даних.

Рефлексивний компонент виявляється у здатності критично оцінювати результати власної діяльності, прогнозувати напрями професійного розвитку та самостійно формувати індивідуальну траєкторію навчання. Студент активно бере участь у професійних спільнотах, проходить спеціалізовані курси та сертифікаційні програми, здійснює пошук нових рішень у сфері кібербезпеки та готовий до впровадження інновацій у професійній діяльності.

Високий рівень готовності свідчить про сформованість професійної компетентності щодо застосування програмного забезпечення захисту даних і забезпечує готовність до ефективної діяльності в умовах сучасного цифрового середовища та постійної еволюції кіберзагроз.

Готовність до застосування ПЗ захисту даних у випускника спеціальності 015 Професійна освіта, спеціалізації 015.39 Цифрові технології – це не вузькотехнічна навичка, а професійно-педагогічна компетентність подвійної спрямованості (Сисоєва, С. О. 2015), яка оцінюється за чотирма компонентами та відповідними критеріями/показниками.

Критерії оцінювання рівня сформованості готовності до застосування програмного забезпечення захисту даних представлена чотирибальною шкалою (0–3), де 0 відповідає низькому рівню, 1 – середньому, 2 – достатньому, 3 – високому. Загальна максимальна сума балів становить 24.

Таким чином, визначені рівні сформованості готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних відображають послідовну динаміку розвитку когнітивного, діяльнісного, мотиваційного та рефлексивного компонентів готовності – від фрагментарного засвоєння знань і недостатньої практичної підготовленості до системного володіння сучасними засобами захисту даних, сформованої професійної мотивації, здатності до самостійного розв’язання професійних завдань і безперервного професійного саморозвитку. Анкета оцінювання готовності до застосування ПЗ захисту даних наведена у таблиці 2.2.

.

Таблиця 2.2

Анкета оцінювання готовності до застосування ПЗ захисту даних

Компонент	Показник (індикатор)	0 балів (низький рівень)	1 бал (середній рівень)	2 бали (достатній рівень)	3 бали (високий рівень)	Макс. бали
Когнітивний	Знання нормативно-правової бази та принципів захисту даних	Відсутні або фрагментарні знання про нормативні акти та принципи ІБ	Має загальні уявлення про окремі нормативні документи	Знає основні положення Закону України «Про захист персональних даних», CIA-тріаду, базові принципи ІБ	Глибоко володіє нормативною базою (GDPR, ISO/IEC 27001/27002), принципами кібербезпеки та моделями загроз	/3
Когнітивний	Знання інструментів програмного забезпечення захисту даних	Не орієнтується в інструментах	Має фрагментарні уявлення про окремі інструменти	Знає призначення Wireshark, Packet Tracer та аналогічних засобів	Вільно орієнтується в Kali Linux, VeraCrypt, Splunk та інших засобах захисту інформації	/3
Діяльнісний	Вміння застосовувати інструменти захисту даних	Не володіє практичними навичками роботи з інструментами	Виконує прості операції під керівництвом викладача	Самостійно виконує базові операції (захоплення трафіку, моделювання мереж)	Аналізує трафік, застосовує фільтри, налаштовує базові засоби захисту	/3
Діяльнісний	Розробка навчально-методичних матеріалів	Не здатний до створення навчальних матеріалів	Розробляє прості інструкції або пам’ятки	Створює структуровані навчальні матеріали (конспекти, чек-листи)	Розробляє повноцінні навчальні заняття/уроки для ЗФПО	/3
Мотиваційний	Усвідомлення значущості інформаційної безпеки	Не визнає важливість захисту даних	Частково усвідомлює значущість ІБ	Усвідомлює важливість і періодично застосовує знання	Системно дотримується принципів ІБ як професійної норми	/3
Мотиваційни	Мотивація до професійного розвитку та навчання інших	Відсутня мотивація	Ситуативна мотивація	Стійка позитивна мотивація до розвитку	Висока внутрішня мотивація до навчання інших та саморозвитку	/3
Рефлексивний	Здатність до самоаналізу професійної діяльності	Відсутній самоаналіз	Епізодично аналізує власні дії	Регулярно здійснює самооцінювання після практичних робіт	Системно аналізує діяльність, коригує власні дії	/3
Рефлексивний	Готовність до самоосвіти	Не займається самоосвітою	Планує окремі освітні заходи	Має план підвищення кваліфікації	Реалізує системну самоосвіту (курси, сертифікації, дослідження)	/3
Загальна сума						/24

Інструментарій діагностики (додаток Б)

У структурі готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних виокремлено чотири взаємопов'язані компоненти: когнітивний, діяльнісний, мотиваційний та рефлексивний. Кожен компонент характеризується відповідними показниками, які дозволяють оцінити рівень сформованості готовності здобувачів освіти до професійної діяльності у сфері захисту даних.

Когнітивний компонент характеризує рівень теоретичної підготовки майбутніх фахівців та відображає сформованість системи знань щодо нормативно-правових, організаційних і технологічних засад захисту даних. Першим показником цього компонента є знання нормативної бази та принципів захисту даних. На низькому рівні здобувач освіти володіє лише фрагментарними знаннями окремих нормативних документів і може назвати один-два законодавчі акти, що стосуються захисту інформації. Середній рівень передбачає знання основних положень Закону України «Про захист персональних даних» та розвміння базових принципів інформаційної безпеки, зокрема моделі конфіденційності, цілісності та доступності інформації (CIA-тріади). Достатній рівень характеризується впевненим знанням національної нормативно-правової бази у сфері захисту даних, розвмінням призначення міжнародних стандартів ISO/IEC 27001 (2022) та ISO/IEC 27002 (2022), основних положень GDPR (2016) і здатністю застосовувати ці знання під час аналізу типових професійних ситуацій. Високий рівень характеризується ґрунтовним знанням національних і міжнародних нормативних документів, розвмінням принципів GDPR, стандартів ISO/IEC 27001 (2022) та ISO/IEC 27002 (2022), а також усвідомленням сучасних загроз інформаційній безпеці.

Другим показником когнітивного компонента є знання інструментів програмного забезпечення захисту даних. Низький рівень характеризується поверхневим ознайомленням із програмними засобами та знанням лише окремих назв програм. Середній рівень передбачає розвміння призначення таких інструментів, як Wireshark та Cisco Packet Tracer, а також знання основних

напрямів їх використання. Достатній рівень характеризується знанням функціональних можливостей сучасних програмних засобів захисту даних, вмінням пояснити особливості їх використання та обґрунтовано обирати відповідний програмний засіб для виконання типових завдань із захисту інформації. Високий рівень виявляється у знанні функціональних можливостей спеціалізованих програмних засобів захисту даних, зокрема Wireshark, Packet Tracer, Kali Linux, VeraCrypt, Splunk та інших сучасних систем кібербезпеки.

Діяльнісний компонент відображає практичну готовність здобувачів освіти до використання програмного забезпечення захисту даних у професійній діяльності. Одним із його показників є самостійне застосування інструментів захисту даних. Низький рівень характеризується нездатністю самостійно працювати з базовими програмними засобами аналізу та захисту інформації. На середньому рівні здобувач освіти здатний виконувати типові завдання: захоплювати мережевий трафік у Wireshark або моделювати прості мережі в Packet Tracer. Достатній рівень передбачає самостійне виконання практичних завдань із використанням програмного забезпечення захисту даних, аналіз мережевого трафіку, моделювання мережевих процесів, застосування базових засобів шифрування та виявлення типових кіберзагроз із незначною консультативною підтримкою викладача. Високий рівень передбачає вміння аналізувати результати моніторингу мережі, використовувати фільтрацію трафіку, виявляти загрози та здійснювати базове налаштування засобів захисту.

Іншим показником діяльнісного компонента є здатність до розроблення навчальних матеріалів з питань захисту даних. Низький рівень характеризується труднощами під час підготовки навіть найпростіших інструктивних матеріалів. Середній рівень передбачає здатність створювати пам'ятки, алгоритми дій або чек-листи щодо безпечної роботи з даними. Достатній рівень характеризується здатністю самостійно розробляти лабораторні завдання, практичні вправи, навчальні презентації та методичні матеріали з питань захисту даних, адаптуючи їх до рівня підготовки здобувачів освіти. Високий рівень виявляється у здатності

розробляти конспекти занять, навчальні презентації, методичні рекомендації та інші освітні матеріали для підготовки здобувачів освіти.

Мотиваційний компонент відображає систему професійних цінностей, ставлення до інформаційної безпеки та внутрішню мотивацію до використання програмного забезпечення захисту даних. Показником цього компонента є усвідомлення відповідальності та етичне ставлення до захисту інформації. На низькому рівні здобувач освіти не усвідомлює значущості захисту даних і розглядає питання інформаційної безпеки як другорядні. Середній рівень характеризується розвмінням важливості дотримання вимог інформаційної безпеки, хоча відповідні правила застосовуються не завжди систематично. Достатній рівень передбачає сформоване відповідальне ставлення до захисту інформації, свідоме дотримання норм інформаційної безпеки та прагнення використовувати сучасні засоби захисту даних у навчальній і професійній діяльності. Високий рівень передбачає стійке переконання щодо необхідності захисту інформації та усвідомлення відповідальності за безпечне використання цифрових ресурсів у професійній діяльності.

Другим показником мотиваційного компонента є мотивація до навчання інших основам захисту даних і кібергігієни. Низький рівень характеризується відсутністю інтересу до поширення знань у сфері інформаційної безпеки. Середній рівень відображає позитивне ставлення до такої діяльності. Достатній рівень характеризується стійким інтересом до проведення інформаційно-просвітницької роботи, готовністю брати участь у навчанні інших основам кібергігієни та популяризації безпечної поведінки в цифровому середовищі. Високий рівень характеризується наявністю стійкої внутрішньої мотивації до популяризації безпечної поведінки в цифровому середовищі та готовністю навчати інших основам кібербезпеки.

Рефлексивний компонент характеризує здатність здобувача освіти до самоаналізу, саморозвитку та професійного вдосконалення. Одним із його показників є здатність до самоаналізу та рефлексії. Низький рівень характеризується відсутністю аналізу власної діяльності та причин допущених

помилок. Середній рівень передбачає здійснення елементарної рефлексії після виконання лабораторних робіт або практичних завдань. Достатній рівень характеризується регулярним аналізом власних результатів навчання, визначенням причин успіхів і помилок, формулюванням висновків та плануванням шляхів удосконалення професійної діяльності. Високий рівень виявляється у систематичному аналізі власних результатів навчання, веденні рефлексивних записів та здатності самостійно визначати напрями подальшого професійного розвитку.

Другим показником рефлексивного компонента є готовність до самоосвіти. Низький рівень характеризується відсутністю прагнення до подальшого професійного розвитку. Середній рівень передбачає планування окремих заходів щодо підвищення кваліфікації, зокрема проходження короткострокових онлайн-курсів. Достатній рівень характеризується систематичним самостійним опрацюванням сучасних джерел із кібербезпеки, регулярним проходженням професійних онлайн-курсів, прагненням до оновлення власних знань та вдосконалення цифрових компетентностей. Високий рівень характеризується наявністю чіткої індивідуальної траєкторії професійного розвитку, що включає систематичне проходження курсів, отримання сертифікатів, вивчення нових технологій та постійний моніторинг сучасних тенденцій у сфері кібербезпеки.

Для комплексного оцінювання рівня сформованості готовності використовується система діагностичних засобів, яка включає анкету самооцінки, оцінювання лабораторних і проєктних робіт та аналіз електронного портфоліо здобувача освіти. Анкета самооцінки містить вісім запитань, що дозволяють визначити рівень сформованості кожного компонента готовності за шкалою від 0 до 3 балів. Рубрика оцінювання лабораторних і проєктних робіт спрямована на оцінку технічного виконання завдань, розвміння ризиків інформаційної безпеки, здатності розробляти навчальні матеріали та здійснювати рефлексію результатів власної діяльності. Портфоліо включає звіти

лабораторних робіт, розроблені методичні матеріали, результати самооцінювання та рефлексивні записи.

Інтерпретація результатів здійснюється за сумарною кількістю балів. Сума балів від 0 до 7 відповідає низькому рівню готовності. Результат від 8 до 12 балів свідчить про середній рівень готовності та необхідність корекції професійної підготовки. Показник від 13 до 18 балів характеризує достатній рівень сформованості готовності, який забезпечує виконання типових професійних завдань, проте потребує подальшого вдосконалення. Результат від 19 до 24 балів відповідає високому рівню готовності та свідчить про сформованість професійних компетентностей, необхідних для ефективного застосування програмного забезпечення захисту даних у професійній діяльності.

2.2. Концептуальні положення та принципи розроблення методики підготовки фахівців цифрових технологій

Сучасні тенденції цифровізації суспільства, стрімкий розвиток інформаційно-комунікаційних технологій, зростання кількості кіберзагроз та поширення хмарних сервісів актуалізують проблему якісної підготовки фахівців цифрових технологій до забезпечення захисту даних у професійній діяльності. У зв’язку з цим особливого значення набуває розроблення ефективної методики підготовки майбутніх фахівців до застосування програмного забезпечення захисту даних, що забезпечує формування відповідних професійних компетентностей та готовності до виконання завдань із кібербезпеки.

Концепція розробленої методики ґрунтується на положенні про те, що підготовка фахівців цифрових технологій до застосування програмного забезпечення захисту даних є цілеспрямованим педагогічним процесом формування системи знань, вмінь, практичних навичок і професійно значущих якостей, необхідних для забезпечення конфіденційності, цілісності та доступності інформації в умовах цифрового середовища.

Теоретико-методологічною основою методики виступає сукупність взаємопов’язаних наукових підходів: компетентнісного, діяльнісного, системного, особистісно орієнтованого, практико-орієнтованого та технологічного.

Компетентнісний підхід забезпечує спрямованість освітнього процесу на формування інтегральної, загальних і професійних компетентностей, пов’язаних із застосуванням програмних засобів захисту даних. Результатом підготовки виступає не лише засвоєння теоретичних знань, а й здатність ефективно використовувати їх у професійній діяльності.

Діяльнісний підхід передбачає залучення здобувачів освіти до виконання практичних завдань, наближених до реальних виробничих ситуацій, що виникають під час забезпечення інформаційної безпеки комп’ютерних систем і мереж.

Системний підхід дозволяє розглядати процес підготовки як цілісну педагогічну систему, компонентами якої є мета, зміст, форми, методи, засоби навчання та результати підготовки.

Особистісно орієнтований підхід спрямований на врахування індивідуальних особливостей здобувачів освіти, їхніх професійних інтересів, рівня цифрової підготовки та освітніх потреб.

Практико-орієнтований підхід забезпечує інтеграцію теоретичної підготовки з практичною діяльністю шляхом використання кейсів, лабораторних робіт, проєктних завдань та моделювання професійних ситуацій у сфері захисту даних.

Технологічний підхід передбачає проєктування освітнього процесу на основі чітко визначених цілей, очікуваних результатів, критеріїв оцінювання та використання сучасних цифрових технологій навчання.

Концепція методики базується на таких положеннях:

– підготовка до застосування програмного забезпечення захисту даних повинна бути невід’ємною складовою професійної підготовки фахівців цифрових технологій;

– зміст навчання має відповідати сучасним тенденціям розвитку інформаційної безпеки, кібербезпеки та цифрових технологій;

– освітній процес повинен забезпечувати поєднання фундаментальної теоретичної підготовки з інтенсивною практичною діяльністю;

– формування готовності до використання програмного забезпечення захисту даних має здійснюватися на міждисциплінарній основі із залученням знань із комп'ютерних мереж, операційних систем, інформаційної безпеки, хмарних технологій та адміністрування інформаційних систем;

– ефективність підготовки забезпечується використанням сучасних цифрових освітніх технологій, віртуальних лабораторій, симуляторів кіберзагроз і професійного програмного забезпечення.

Розроблення методики здійснювалося на основі системи дидактичних принципів, серед яких провідними є:

Принцип професійної спрямованості передбачає орієнтацію змісту навчання на реальні завдання професійної діяльності фахівців цифрових технологій щодо забезпечення захисту даних.

Принцип практичної спрямованості навчання **р**еалізується через виконання лабораторних робіт, практичних кейсів, навчальних проєктів та завдань із використанням сучасного програмного забезпечення захисту даних.

Принцип інтеграції теорії та практики забезпечує взаємозв'язок теоретичних знань про механізми захисту інформації з практичним застосуванням відповідних програмних засобів.

Принцип актуальності змісту навчання передбачає постійне оновлення навчального матеріалу відповідно до розвитку цифрових технологій та появи нових кіберзагроз.

Принцип міждисциплінарної інтеграції полягає у взаємозв'язку змісту дисциплін комп'ютерного циклу та дисциплін, пов'язаних із кібербезпекою і захистом даних.

Принцип безперервності професійного розвитку спрямований на формування готовності майбутніх фахівців до постійного оновлення знань і вдосконалення навичок у сфері захисту інформації.

Принцип моделювання професійної діяльності передбачає створення навчальних ситуацій, максимально наближених до умов майбутньої професійної діяльності.

Принцип цифровізації освітнього процесу реалізується через використання хмарних сервісів, систем дистанційного навчання, цифрових платформ та спеціалізованого програмного забезпечення.

Принцип кібербезпекової спрямованості орієнтує навчальний процес на формування відповідального ставлення до захисту інформаційних ресурсів, дотримання вимог інформаційної безпеки та культури кібербезпеки.

Спираючись на результати теоретичного аналізу проблеми професійної підготовки фахівців цифрових технологій у сфері захисту даних, було визначено концептуальні положення, які відображають основні напрями розроблення методики дослідження. Їх реалізація здійснюється на основі комплексу взаємопов’язаних наукових підходів та дидактичних принципів, що забезпечують формування відповідних професійних компетентностей здобувачів освіти. Узагальнення зазначених положень та особливостей їх упровадження в методику підготовки фахівців цифрових технологій до застосування програмного забезпечення захисту даних наведено в таблиці 2.3.

Таблиця 2.3

Концептуальні засади розробки методики підготовки фахівців цифрових технологій

Концептуальні положення	**Наукові підходи**	**Принципи**	**Реалізація в методиці**
Підготовка до застосування програмного забезпечення захисту даних є невід’ємною складовою професійної підготовки фахівців цифрових технологій	Компетентнісний, системний	Професійної спрямованості, кібербезпекової спрямованості	Визначення цілей навчання через систему професійних компетентностей; інтеграція питань захисту даних у фахові дисципліни

Продовження таблиці 2.3

Концептуальні положення	**Наукові підходи**	**Принципи**	**Реалізація в методиці**
Підготовка майбутніх фахівців повинна забезпечувати єдність теоретичної та практичної складових навчання	Діяльнісний, практико-орієнтований	Інтеграції теорії та практики, практичної спрямованості навчання	Виконання лабораторних робіт, практичних завдань, кейсів із використанням програмного забезпечення захисту даних
Формування професійних компетентностей має здійснюватися через активну навчально-пізнавальну діяльність здобувачів освіти	Діяльнісний, особистісно орієнтований	Активності та самостійності навчання, моделювання професійної діяльності	Проєктна діяльність, розв’язування проблемних ситуацій, виконання індивідуальних і групових завдань
Підготовка повинна враховувати індивідуальні особливості та професійні потреби здобувачів освіти	Особистісно орієнтований	Індивідуалізації та диференціації навчання	Варіативність навчальних завдань, індивідуальні освітні траєкторії, диференційований контроль результатів навчання
Формування готовності до захисту даних потребує міждисциплінарної інтеграції знань	Системний, компетентнісний	Міждисциплінарної інтеграції	Поєднання змісту дисциплін «Операційні системи», «Комп’ютерні мережі та захист даних», «Хмарні технології в навчальному процесі» та «Інформаційна безпека»
Освітній процес має відображати реальні умови професійної діяльності фахівців цифрових технологій	Діяльнісний, практико-орієнтований	Моделювання професійної діяльності, професійної спрямованості	Створення навчальних ситуацій, що відтворюють типові загрози інформаційній безпеці та шляхи їх усунення
Ефективність підготовки забезпечується використанням сучасних цифрових технологій навчання	Технологічний, системний	Цифровізації освітнього процесу, наочності	Використання LMS-платформ, хмарних сервісів, віртуальних лабораторій, симуляторів кіберзагроз і програмних засобів захисту даних
Підготовка повинна формувати готовність до постійного професійного самовдосконалення у сфері захисту даних	Компетентнісний, особистісно орієнтований	Безперервності професійного розвитку	Організація самостійної роботи, дослідницьких завдань, вивчення нових програмних продуктів і технологій захисту даних

Продовження таблиці 2.3

Формування культури кібербезпеки є необхідною умовою професійної діяльності фахівців цифрових технологій	Компетентнісний, аксіологічний	Кібербезпекової спрямованості, відповідальності та безпечної поведінки в цифровому середовищі	Формування навичок безпечної роботи з даними, дотримання політик безпеки, етичних та правових норм використання інформаційних ресурсів

Концептуальну основу підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних представлено у вигляді концептуальної моделі методики підготовки фахівців цифрових технологій до застосування програмного забезпечення захисту даних (рис. 2.1). Модель відображає взаємозв'язок між метою, методологічними засадами, змістовим наповненням, організацією освітнього процесу та очікуваними результатами підготовки.

Як показано на рисунку 2.1, метою підготовки є формування готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних у професійній діяльності. Досягнення поставленої мети забезпечується на основі сукупності наукових підходів, серед яких компетентнісний, системний, діяльнісний, особистісний, технологічний та практико-орієнтований. Їх реалізація сприяє формуванню професійних компетентностей, необхідних для ефективного використання сучасних засобів захисту інформації.

Відповідно до моделі, концептуальні положення підготовки передбачають інтеграцію питань захисту даних у зміст професійної підготовки, міждисциплінарний характер навчання, поєднання теоретичних знань із практичною діяльністю та забезпечення актуальності навчального контенту відповідно до сучасних тенденцій розвитку цифрових технологій.

Важливу роль у реалізації моделі відіграють принципи професійної спрямованості, практичної орієнтації, інтеграції теорії та практики, цифровізації

освітнього процесу та врахування вимог кібербезпеки. Саме вони визначають логіку відбору змісту навчання та організації освітньої діяльності.

Змістовий компонент моделі охоплює вивчення комп'ютерних мереж, основ кібербезпеки, програмного забезпечення захисту даних і сучасних технологій забезпечення інформаційної безпеки. Реалізація змістового компонента здійснюється через різні форми та методи організації навчання, зокрема лекції, практичні та лабораторні заняття, кейс-метод, проєктне навчання й моделювання кіберзагроз.

Результатом реалізації запропонованої моделі є сформована готовність майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних, що виявляється у набутті професійних компетентностей, необхідних для забезпечення захисту інформаційних ресурсів у сучасному цифровому середовищі (рис. 2.2).

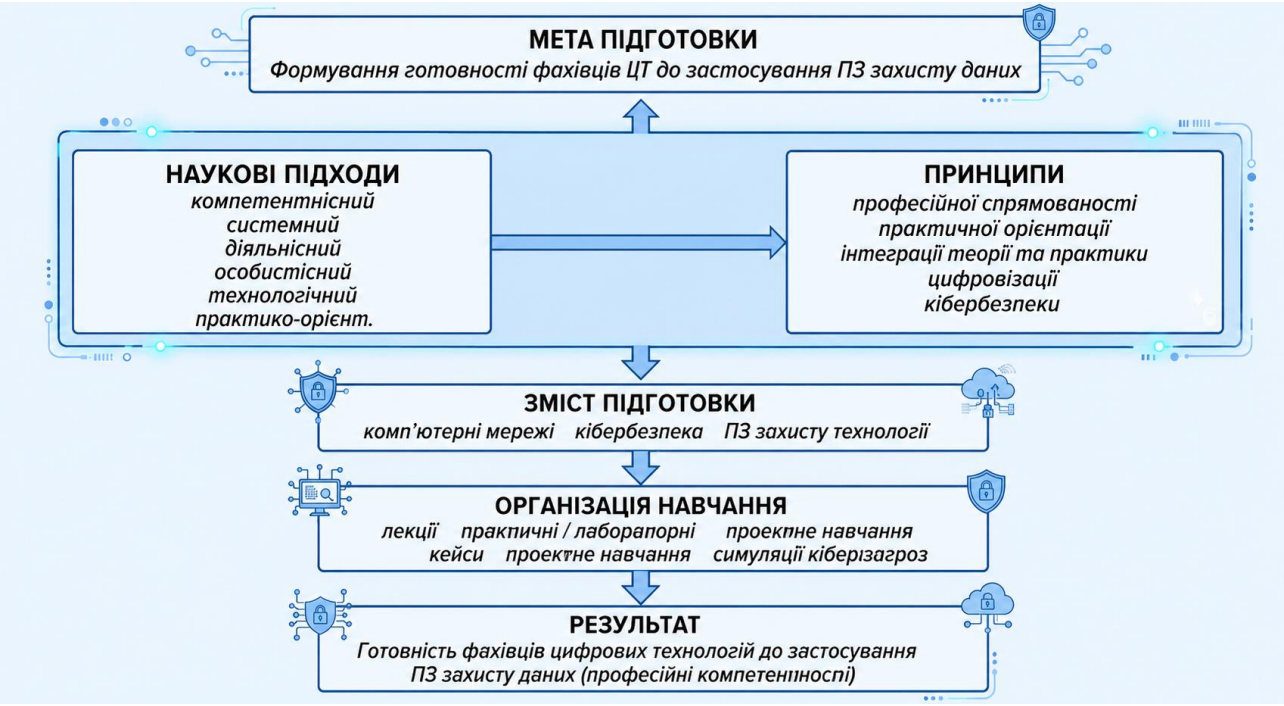

Рис. 2.2. Модель методики підготовки фахівців цифрових технологій до застосування програмного забезпечення захисту даних

Таким чином, концептуальні положення та визначені принципи створюють методологічне підґрунтя для розроблення та впровадження методики підготовки

фахівців цифрових технологій до застосування програмного забезпечення захисту даних. Їх реалізація забезпечує формування професійної готовності майбутніх фахівців до ефективного використання сучасних засобів захисту інформації у професійній діяльності та створює передумови для побудови структурно-функціональної моделі досліджуваної методики.

2.3. Педагогічні умови формування готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних

В дисертаційному дослідженні педагогічні умови доцільно сформулювати як сукупність спеціально створених організаційно-педагогічних обставин, що забезпечують ефективне формування готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних.

На основі здійсненого аналізу науково-педагогічної літератури припускаємо, що ефективність підготовки фахівців цифрових технологій до застосування програмного забезпечення захисту даних забезпечується створенням низки педагогічних умов, зокрема:

1) інтеграція змісту підготовки із сучасними технологіями захисту даних та вимогами кібербезпеки;

2) забезпечення практико-орієнтованого навчання шляхом використання професійного програмного забезпечення захисту даних;

3) використання цифрового освітнього середовища та засобів моделювання кіберзагроз;

4) реалізація міждисциплінарної інтеграції у процесі підготовки до застосування програмного забезпечення захисту даних;

5) мотивація навчально-пізнавальної діяльності здобувачів освіти через проєктні та дослідницькі методи навчання.

На основі визначених концептуальних положень, наукових підходів і принципів розробленої методики виокремлено такі педагогічні умови:

*1) Інтеграція змісту підготовки із сучасними технологіями захисту даних та вимогами кібербезпеки***.**

Однією з визначальних педагогічних умов формування готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних є інтеграція змісту професійної підготовки із сучасними технологіями захисту інформації та актуальними вимогами кібербезпеки. Необхідність реалізації цієї умови обумовлена стрімким розвитком цифрових технологій, постійним оновленням програмних засобів захисту інформації та зростанням кількості кіберзагроз, які потребують від майбутніх фахівців не лише ґрунтовних теоретичних знань, а й здатності оперативно застосовувати сучасні інструменти захисту даних у професійній діяльності.

Сутність зазначеної педагогічної умови полягає в забезпеченні системного включення питань інформаційної безпеки та використання програмного забезпечення захисту даних до змісту професійної підготовки майбутніх фахівців цифрових технологій. При цьому підготовка не повинна обмежуватися вивченням окремої дисципліни з кібербезпеки, а має реалізовуватися через міждисциплінарну інтеграцію знань з комп'ютерних мереж, операційних систем, інформаційних систем, хмарних технологій, адміністрування серверів та мережевої інфраструктури.

Реалізація цієї умови передбачає актуалізацію змісту навчальних дисциплін відповідно до сучасних тенденцій розвитку інформаційної безпеки. Зокрема, у процесі підготовки доцільно включати питання використання антивірусного програмного забезпечення, систем виявлення та запобігання вторгненням, засобів шифрування даних, технологій резервного копіювання та відновлення інформації, систем контролю доступу, DLP-систем, багатофакторної автентифікації, хмарних механізмів захисту інформації та засобів моніторингу кіберзагроз.

Особливого значення набуває орієнтація змісту підготовки на актуальні стандарти та нормативно-правові вимоги у сфері інформаційної безпеки.

Ознайомлення здобувачів освіти з міжнародними стандартами управління інформаційною безпекою, політиками захисту даних, вимогами щодо конфіденційності інформації та кібергігієни сприяє формуванню відповідального ставлення до професійної діяльності та розумінню важливості дотримання вимог безпеки під час роботи з інформаційними ресурсами.

Важливим аспектом реалізації педагогічної умови є забезпечення динамічного оновлення змісту навчання. Оскільки технології захисту даних постійно вдосконалюються, освітній процес має оперативно реагувати на появу нових кіберзагроз, програмних рішень та технологічних підходів до забезпечення інформаційної безпеки. Це досягається шляхом використання сучасних професійних джерел інформації, галузевих стандартів, рекомендацій міжнародних організацій у сфері кібербезпеки та аналізу реальних інцидентів інформаційної безпеки.

Реалізація зазначеної умови забезпечує формування у майбутніх фахівців системи актуальних знань про сучасні програмні засоби захисту даних, розвміння принципів їх функціонування та сфер застосування, а також готовності до вирішення професійних завдань щодо забезпечення конфіденційності, цілісності та доступності інформації в умовах сучасного цифрового середовища. Водночас інтеграція змісту підготовки із сучасними технологіями захисту даних сприяє розвитку професійного мислення, формуванню культури кібербезпеки та здатності до безперервного професійного самовдосконалення у сфері інформаційної безпеки.

Таким чином, інтеграція змісту професійної підготовки із сучасними технологіями захисту даних та вимогами кібербезпеки виступає базовою педагогічною умовою формування готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних, оскільки забезпечує актуальність змісту навчання, його практичну спрямованість та відповідність сучасним потребам цифрового суспільства і ринку праці.

2) Забезпечення практико-орієнтованого навчання шляхом використання професійного програмного забезпечення захисту даних

Важливою педагогічною умовою формування готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних є забезпечення практико-орієнтованого навчання шляхом систематичного використання професійних програмних засобів захисту інформації в освітньому процесі. Необхідність реалізації цієї умови зумовлена тим, що сучасна професійна діяльність фахівців цифрових технологій потребує не лише знання теоретичних засад інформаційної безпеки, а й сформованих вмінь застосовувати спеціалізоване програмне забезпечення для виявлення, попередження та нейтралізації кіберзагроз.

Практико-орієнтоване навчання розглядається як організація освітнього процесу, за якої засвоєння теоретичних знань відбувається через виконання практичних завдань, максимально наближених до реальних умов професійної діяльності. Такий підхід забезпечує перенесення знань у практичну площину та сприяє формуванню професійних компетентностей, необхідних для ефективного використання програмного забезпечення захисту даних у майбутній професійній діяльності.

Сутність зазначеної педагогічної умови полягає в організації освітнього процесу таким чином, щоб кожний теоретичний компонент супроводжувався практичною діяльністю із застосуванням сучасних програмних засобів захисту інформації. У процесі навчання здобувачі освіти повинні не лише ознайомлюватися з функціональними можливостями програмного забезпечення, а й виконувати комплекс практичних дій щодо його встановлення, налаштування, адміністрування та оцінювання ефективності використання.

Реалізація педагогічної умови передбачає використання під час лабораторних і практичних занять різних категорій програмного забезпечення захисту даних, серед яких антивірусні системи, засоби шифрування інформації, системи резервного копіювання та відновлення даних, засоби моніторингу мережевої безпеки, програмні комплекси контролю доступу, міжмережеві екрани, VPN-технології, DLP-системи та інші програмні рішення, що застосовуються у професійній діяльності фахівців цифрових технологій.

Особливе значення має використання кейс-технологій, що дозволяють моделювати реальні ситуації, пов’язані із захистом інформації. Під час виконання кейсів здобувачі освіти аналізують типові проблеми інформаційної безпеки, визначають можливі загрози, добирають відповідні програмні засоби захисту та обґрунтовують доцільність їх використання. Такий підхід сприяє розвитку професійного мислення, здатності аналізувати ризики та приймати обґрунтовані рішення щодо забезпечення безпеки інформаційних ресурсів.

Важливим елементом реалізації педагогічної умови є проєктна діяльність. У процесі виконання навчальних проєктів здобувачі освіти розробляють комплексні рішення із забезпечення захисту даних для змодельованих або реальних інформаційних систем. Проєктна діяльність сприяє формуванню навичок інтегрованого використання різних програмних засобів захисту інформації, розвитку самостійності, відповідальності та готовності до виконання професійних завдань у команді.

Ефективність практико-орієнтованого навчання значною мірою забезпечується використанням технології моделювання професійної діяльності. Створення навчальних ситуацій, що відтворюють реальні кіберінциденти, дає можливість здобувачам освіти відпрацьовувати алгоритми реагування на загрози інформаційній безпеці, здійснювати пошук уразливостей, налаштовувати засоби захисту та оцінювати результати їх функціонування. Завдяки цьому формується досвід професійної діяльності ще на етапі навчання.

Важливим результатом реалізації цієї педагогічної умови є розвиток у здобувачів освіти здатності працювати з різними програмними продуктами незалежно від їх виробника чи функціонального призначення. Майбутні фахівці набувають вмінь аналізувати можливості програмних засобів захисту даних, адаптувати їх до конкретних умов функціонування інформаційних систем та здійснювати вибір оптимального програмного рішення залежно від характеру кіберзагроз.

Крім того, практико-орієнтоване навчання сприяє формуванню стійкої мотивації до професійної діяльності, оскільки здобувачі освіти усвідомлюють

практичну значущість отриманих знань і бачать можливості їх використання у майбутній професії. Безпосередня робота з професійним програмним забезпеченням підвищує рівень зацікавленості навчанням, розвиває впевненість у власних професійних можливостях та стимулює подальше самовдосконалення у сфері захисту даних.

Отже, забезпечення практико-орієнтованого навчання шляхом використання професійного програмного забезпечення захисту даних є важливою педагогічною умовою формування готовності майбутніх фахівців цифрових технологій до професійної діяльності. Її реалізація забезпечує поєднання теоретичної підготовки з практичним досвідом застосування засобів захисту інформації, розвиток професійних компетентностей та формування здатності ефективно вирішувати завдання забезпечення інформаційної безпеки в сучасному цифровому середовищі.

3) Використання цифрового освітнього середовища та засобів моделювання кіберзагроз.

Важливою педагогічною умовою формування готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних є використання цифрового освітнього середовища та засобів моделювання кіберзагроз. Актуальність цієї умови зумовлена трансформацією сучасної освіти в умовах цифровізації суспільства, зростанням ролі інформаційно-комунікаційних технологій у професійній діяльності та необхідністю підготовки фахівців, здатних ефективно діяти в умовах постійної зміни кіберзагроз і технологій захисту інформації.

У контексті дослідження цифрове освітнє середовище розглядається як сукупність цифрових ресурсів, програмних платформ, інформаційних сервісів, електронних освітніх матеріалів і технологічних засобів, які забезпечують організацію, підтримку та управління процесом професійної підготовки майбутніх фахівців цифрових технологій. Таке середовище створює умови для інтеграції теоретичного навчання, практичної діяльності та самостійної роботи здобувачів освіти в єдиний освітній простір.

Сутність даної педагогічної умови полягає у створенні та використанні цифрового освітнього середовища, що забезпечує можливість систематичного застосування програмного забезпечення захисту даних, проведення практичних досліджень, виконання лабораторних робіт, моделювання кіберзагроз та відпрацювання алгоритмів реагування на інциденти інформаційної безпеки. Такий підхід дозволяє максимально наблизити процес навчання до реальних умов професійної діяльності фахівців цифрових технологій.

Реалізація цієї умови передбачає використання систем управління навчанням (LMS), хмарних сервісів, віртуальних лабораторій, платформ дистанційного навчання, цифрових освітніх ресурсів та спеціалізованого програмного забезпечення у сфері інформаційної безпеки. Використання цифрового середовища забезпечує постійний доступ здобувачів освіти до навчальних матеріалів, практичних завдань, інструкцій щодо роботи з програмними засобами захисту даних, а також засобів комунікації та співпраці.

Особливого значення набуває застосування віртуальних лабораторій, які дають можливість здійснювати налаштування та тестування програмного забезпечення захисту даних без ризику пошкодження реальних інформаційних систем. У таких лабораторіях студенти можуть відпрацьовувати навички налаштування антивірусних систем, міжмережевих екранів, систем резервного копіювання, засобів контролю доступу, криптографічного захисту інформації та інших програмних продуктів, що використовуються в професійній діяльності.

Важливим складником цифрового освітнього середовища є використання засобів моделювання кіберзагроз. Моделювання дозволяє створювати навчальні сценарії, які відображають реальні або потенційні загрози інформаційній безпеці. У процесі виконання таких завдань здобувачі освіти аналізують джерела загроз, визначають можливі вразливості інформаційних систем, обирають відповідні засоби захисту та оцінюють ефективність їх використання.

Моделювання кіберзагроз створює умови для формування практичного досвіду реагування на інциденти інформаційної безпеки. Здобувачі освіти мають можливість працювати в умовах, максимально наближених до професійної

діяльності, виконуючи завдання з виявлення атак, локалізації загроз, аналізу журналів подій, відновлення інформації після інцидентів та забезпечення безперервності функціонування інформаційних систем. У результаті формується здатність оперативно приймати рішення в умовах невизначеності та підвищується готовність до виконання професійних обов'язків.

Використання цифрового освітнього середовища також сприяє розвитку самостійної пізнавальної діяльності здобувачів освіти. Завдяки доступу до електронних ресурсів, навчальних платформ та професійного програмного забезпечення студенти можуть самостійно поглиблювати знання, виконувати додаткові дослідницькі завдання, вивчати нові програмні продукти та технології захисту даних. Це відповідає сучасним вимогам безперервного професійного розвитку у сфері цифрових технологій та кібербезпеки.

Суттєвою перевагою цифрового освітнього середовища є можливість організації колективної діяльності. Використання хмарних сервісів, засобів відеоконференцій та платформ спільної роботи дозволяє виконувати групові проєкти, проводити аналіз кіберінцидентів у командах, розробляти комплексні рішення із захисту інформаційних ресурсів та формувати навички професійної взаємодії, які є важливими для майбутньої професійної діяльності.

Крім того, цифрове освітнє середовище забезпечує можливість здійснення поточного моніторингу та оцінювання результатів навчання. Викладачі можуть відстежувати активність здобувачів освіти, результати виконання практичних завдань, рівень сформованості професійних компетентностей та своєчасно коригувати освітній процес. Це сприяє підвищенню ефективності підготовки та забезпечує індивідуалізацію навчання.

Результатом реалізації зазначеної педагогічної умови є формування у майбутніх фахівців цифрових технологій практичних навичок роботи в цифровому середовищі, готовності до використання сучасних програмних засобів захисту даних, здатності аналізувати та прогнозувати кіберзагрози, приймати обґрунтовані рішення щодо забезпечення інформаційної безпеки та адаптуватися до швидких змін у сфері цифрових технологій.

Отже, використання цифрового освітнього середовища та засобів моделювання кіберзагроз є важливою педагогічною умовою формування готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних, оскільки забезпечує практичну спрямованість підготовки, створює умови для набуття професійного досвіду та сприяє формуванню професійних компетентностей, необхідних для ефективної діяльності в умовах сучасного цифрового середовища.

4) Реалізація міждисциплінарної інтеграції у процесі підготовки до застосування програмного забезпечення захисту даних.

Однією з ключових педагогічних умов формування готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних є реалізація міждисциплінарної інтеграції у процесі професійної підготовки. Необхідність упровадження цієї умови обумовлена комплексним характером сучасних інформаційних систем, у яких питання захисту даних тісно пов'язані з функціонуванням операційних систем, комп’ютерних мереж, хмарних сервісів та механізмів інформаційної безпеки. Ефективне використання програмного забезпечення захисту даних потребує від майбутнього фахівця не лише знань окремих програмних продуктів, а й розвміння взаємозв’язків між усіма компонентами цифрового середовища.

Сутність цієї педагогічної умови полягає в цілеспрямованому поєднанні змісту навчальних дисциплін «Операційні системи», «Комп’ютерні мережі та захист даних», «Хмарні технології в навчальному процесі» та «Інформаційна безпека» з метою формування цілісної системи знань і практичних вмінь щодо застосування програмного забезпечення захисту даних. Міждисциплінарна інтеграція забезпечує усвідомлення здобувачами освіти взаємозалежності процесів обробки, передавання, зберігання та захисту інформації, що є необхідною передумовою формування професійної компетентності у сфері кібербезпеки.

Особливе значення у реалізації зазначеної педагогічної умови має дисципліна *«Операційні системи»,* яка формує базові знання про архітектуру

операційних систем, механізми управління ресурсами, файлові системи, облікові записи користувачів та політики безпеки. Саме в межах цієї дисципліни здобувачі освіти отримують уявлення про принципи розмежування доступу до ресурсів, механізми автентифікації та авторизації користувачів, засоби аудиту подій безпеки та інструменти адміністрування операційних систем.

Під час вивчення програмного забезпечення захисту даних знання, отримані в межах дисципліни «Операційні системи», стають основою для практичного налаштування політик безпеки, конфігурування міжмережевих екранів, керування правами доступу до файлів і каталогів, використання засобів резервного копіювання та відновлення інформації. Таким чином, питання захисту даних розглядаються не ізольовано, а як складова функціонування операційної системи.

Важливе місце в міждисциплінарній інтеграції посідає дисципліна *«Комп'ютерні мережі та захист даних»,* зміст якої безпосередньо пов'язаний із забезпеченням безпеки передавання інформації в мережевому середовищі. У процесі її вивчення здобувачі освіти опановують принципи функціонування мережевих протоколів, засоби мережевої взаємодії, технології маршрутизації та комутації, а також механізми виявлення та протидії мережевим атакам.

Міждисциплінарна інтеграція реалізується через поєднання знань про мережеву інфраструктуру із практичним використанням програмних засобів захисту даних. Наприклад, під час налаштування VPN-з'єднань, міжмережевих екранів, систем моніторингу мережевого трафіку або систем виявлення вторгнень здобувачі освіти використовують знання як з мережевих технологій, так і з інформаційної безпеки. Це дозволяє сформувати комплексне бачення процесу захисту даних на рівні мережевої взаємодії.

Значний потенціал для реалізації досліджуваної педагогічної умови має дисципліна *«Хмарні технології в навчальному процесі»,* оскільки сучасні інформаційні системи дедалі частіше функціонують на базі хмарної інфраструктури. У межах цієї дисципліни здобувачі освіти ознайомлюються з

моделями надання хмарних послуг, принципами організації хмарних середовищ, технологіями зберігання та обробки даних у хмарі.

Інтеграція змісту даної дисципліни з підготовкою до застосування програмного забезпечення захисту даних передбачає вивчення механізмів забезпечення безпеки хмарних ресурсів, використання технологій шифрування даних у хмарному середовищі, налаштування політик доступу до хмарних сервісів, організацію резервного копіювання інформації та моніторинг безпеки хмарної інфраструктури. Завдяки цьому здобувачі освіти усвідомлюють специфіку захисту даних в умовах використання сучасних цифрових сервісів і набувають навичок роботи з відповідними програмними інструментами.

Системоутворюючу роль у реалізації міждисциплінарної інтеграції виконує дисципліна *«Інформаційна безпека»,* яка забезпечує теоретичне підґрунтя для розвміння загальних принципів захисту інформації. У межах цієї дисципліни формуються знання про загрози інформаційній безпеці, методи та засоби захисту інформації, криптографічні технології, системи управління інформаційною безпекою та сучасні підходи до забезпечення кіберстійкості інформаційних систем.

Саме дисципліна «Інформаційна безпека» забезпечує інтеграцію знань, отриманих під час вивчення інших навчальних компонентів, у єдину систему професійної підготовки. Вона дозволяє майбутнім фахівцям розглядати програмне забезпечення захисту даних як комплексний інструмент забезпечення конфіденційності, цілісності та доступності інформації незалежно від середовища її обробки чи зберігання.

Практична реалізація міждисциплінарної інтеграції здійснюється через виконання комплексних лабораторних робіт, міждисциплінарних проєктів та кейсових завдань. Наприклад, здобувачам освіти може пропонуватися завдання зі створення корпоративної інформаційної системи, у межах якого необхідно налаштувати операційну систему, організувати мережеву взаємодію, забезпечити безпечне зберігання даних у хмарному середовищі та впровадити комплекс програмних засобів захисту інформації. Виконання таких завдань

сприяє інтеграції знань із різних дисциплін та формує здатність застосовувати їх для розв’язання реальних професійних проблем.

Результатом реалізації зазначеної педагогічної умови є формування у майбутніх фахівців цифрових технологій цілісного бачення процесів захисту даних у сучасному цифровому середовищі, здатності комплексно використовувати знання з операційних систем, комп’ютерних мереж, хмарних технологій та інформаційної безпеки під час вибору, налаштування й застосування програмного забезпечення захисту даних. Це сприяє підвищенню рівня професійної компетентності, розвитку системного мислення та готовності до виконання професійних завдань у сфері забезпечення інформаційної безпеки.

Отже, реалізація міждисциплінарної інтеграції на основі взаємопов’язаного вивчення дисциплін «Операційні системи», «Комп’ютерні мережі та захист даних», «Хмарні технології в навчальному процесі» та «Інформаційна безпека» створює необхідні передумови для формування готовності майбутніх фахівців цифрових технологій до ефективного застосування програмного забезпечення захисту даних у професійній діяльності та забезпечує комплексний характер їхньої професійної підготовки.

5) Мотивація навчально-пізнавальної діяльності здобувачів освіти через проєктні та дослідницькі методи навчання.

Важливою педагогічною умовою формування готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних є мотивація навчально-пізнавальної діяльності здобувачів освіти через використання проєктних та дослідницьких методів навчання. Актуальність цієї умови обумовлена тим, що сучасний фахівець у сфері цифрових технологій повинен не лише володіти певним обсягом знань і практичних навичок, а й бути здатним самостійно аналізувати інформацію, досліджувати нові технології, приймати обґрунтовані рішення та ефективно діяти в умовах постійної зміни кіберзагроз і програмних засобів захисту інформації.

У сучасних умовах розвитку цифрового суспільства знання швидко оновлюються, а програмне забезпечення захисту даних постійно

вдосконалюється. Тому професійна підготовка майбутніх фахівців повинна бути спрямована не лише на засвоєння готових знань, а й на розвиток здатності до самостійного пошуку, аналізу та використання нової інформації. Саме проєктні та дослідницькі методи навчання створюють сприятливі умови для формування таких вмінь і забезпечують активну позицію здобувачів освіти в освітньому процесі.

Сутність зазначеної педагогічної умови полягає в організації навчальної діяльності, за якої здобувачі освіти виступають активними учасниками процесу пізнання, самостійно або в складі групи розв’язують професійно орієнтовані завдання, досліджують можливості сучасного програмного забезпечення захисту даних, аналізують кіберзагрози та розробляють способи їх попередження або усунення. Така діяльність сприяє переходу від репродуктивного засвоєння знань до творчого застосування отриманого досвіду в нових професійних ситуаціях.

Одним із найбільш ефективних способів реалізації цієї педагогічної умови є використання проєктного навчання. У процесі виконання проєктів здобувачі освіти здійснюють комплексну діяльність, спрямовану на вирішення практичних завдань із використанням програмного забезпечення захисту даних. Наприклад, вони можуть розробляти проєкти організації системи захисту даних для навчального закладу, малого підприємства або корпоративної мережі, обирати необхідні програмні засоби, здійснювати їх налаштування та оцінювати ефективність запропонованих рішень.

Проєктна діяльність забезпечує інтеграцію знань, отриманих під час вивчення дисциплін «Операційні системи», «Комп’ютерні мережі та захист даних», «Хмарні технології в навчальному процесі» та «Інформаційна безпека». У процесі виконання проєктів здобувачі освіти застосовують знання щодо налаштування операційних систем, організації мережевої безпеки, захисту хмарних ресурсів та використання сучасних засобів забезпечення інформаційної безпеки. Це сприяє формуванню системного бачення процесів захисту інформації та розвитку здатності вирішувати комплексні професійні завдання.

Не менш важливим напрямом реалізації даної педагогічної умови є використання дослідницьких методів навчання. Дослідницька діяльність передбачає самостійне вивчення здобувачами освіти нових програмних продуктів, аналіз їх функціональних можливостей, порівняння ефективності різних засобів захисту даних, виявлення переваг і недоліків окремих технологічних рішень. У процесі досліджень майбутні фахівці набувають досвіду роботи з професійною інформацією та розвивають навички критичного мислення.

Особливу роль відіграє проведення навчальних досліджень, пов’язаних із моделюванням кіберзагроз та оцінюванням ефективності різних програмних засобів захисту даних. Наприклад, здобувачі освіти можуть здійснювати аналіз вразливостей інформаційної системи, досліджувати механізми функціонування шкідливого програмного забезпечення в контрольованому середовищі, оцінювати рівень захищеності мережевої інфраструктури або порівнювати можливості різних антивірусних систем. Така діяльність сприяє глибокому розумінню принципів забезпечення інформаційної безпеки та формуванню навичок професійного аналізу.

Мотивація навчально-пізнавальної діяльності також реалізується через застосування проблемного навчання. Викладач створює проблемні ситуації, пов’язані з порушенням безпеки інформаційних ресурсів, витоком даних, несанкціонованим доступом або мережевими атаками, а здобувачі освіти самостійно знаходять шляхи їх вирішення. Робота над проблемними завданнями сприяє розвитку аналітичного мислення, вміння приймати рішення в умовах невизначеності та здатності прогнозувати наслідки різних кіберзагроз.

Важливим компонентом реалізації цієї педагогічної умови є організація групової дослідницької діяльності. Під час виконання колективних проєктів студенти навчаються працювати в команді, розподіляти обов’язки, координувати власну діяльність із діяльністю інших учасників та спільно приймати рішення щодо вибору програмних засобів захисту даних. Це дозволяє формувати не лише

професійні компетентності, а й навички командної роботи, які є важливою складовою професійної діяльності сучасного фахівця цифрових технологій.

Суттєве значення має також залучення здобувачів освіти до участі в науково-дослідній роботі, конференціях, конкурсах студентських проєктів, хакатонах та змаганнях із кібербезпеки. Такі форми діяльності сприяють розвитку професійної мотивації, підвищують інтерес до вивчення сучасних технологій захисту інформації та стимулюють прагнення до самостійного професійного розвитку.

У результаті реалізації зазначеної педагогічної умови формуються такі важливі складові готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних, як здатність до самостійного навчання, дослідницькі вміння, критичне мислення, навички аналізу кіберзагроз, вміння обирати та обґрунтовувати використання програмних засобів захисту інформації, а також готовність до розв’язання нестандартних професійних завдань.

Отже, мотивація навчально-пізнавальної діяльності здобувачів освіти через проєктні та дослідницькі методи навчання є важливою педагогічною умовою формування готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних. Її реалізація забезпечує розвиток професійного мислення, дослідницької культури, самостійності та творчої активності здобувачів освіти, що є необхідною передумовою успішної професійної діяльності в умовах сучасного цифрового та кібербезпекового середовища.

Отже, ефективність формування готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних забезпечується реалізацією комплексу взаємопов’язаних педагогічних умов: інтеграцією актуального змісту захисту даних у професійну підготовку; організацією практико-орієнтованого навчання із використанням професійного програмного забезпечення; застосуванням цифрового освітнього середовища та засобів моделювання кіберзагроз; міждисциплінарною інтеграцією змісту

навчання; мотивацією до проєктної та дослідницької діяльності здобувачів освіти. Реалізація зазначених умов створює підґрунтя для формування професійних компетентностей і готовності майбутніх фахівців до ефективного забезпечення захисту даних у сучасному цифровому середовищі.

2.4. Структурно-функціональна модель підготовки фахівців цифрових технологій

На основі проведеного теоретичного аналізу наукової літератури, визначених концептуальних положень, наукових підходів, принципів підготовки та обґрунтованих педагогічних умов було розроблено структурно-функціональну модель підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних. Необхідність побудови такої моделі зумовлена потребою системного відображення процесу формування готовності здобувачів освіти до використання сучасних програмних засобів захисту інформації в умовах цифровізації суспільства та зростання кіберзагроз.

Структурно-функціональна модель виступає теоретичною основою реалізації розробленої методики та відображає взаємозв’язок між метою, методологічними засадами, змістом підготовки, педагогічними умовами, організацією освітнього процесу та результатами навчання. Її побудова ґрунтується на компетентнісному, системному, діяльнісному, особистісно орієнтованому, практико-орієнтованому та технологічному підходах, що забезпечують цілісність і послідовність професійної підготовки майбутніх фахівців цифрових технологій.

Запропонована модель охоплює методологічний, змістовий, організаційно-процесуальний та результативний компоненти, які функціонують у взаємозв’язку та забезпечують досягнення поставленої мети. Особливе місце в структурі моделі посідають педагогічні умови, реалізація яких спрямована на підвищення ефективності формування професійних компетентностей у сфері застосування програмного забезпечення захисту даних.

Структурно-функціональну модель підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних представлено на рисунку 2.3.

Рис. 2.3. Структурно-функціональна модель підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних

Структурно-функціональна модель підготовки майбутніх фахівців цифрових технологій (рис. 2.3) до застосування програмного забезпечення захисту даних складається з взаємопов'язаних методологічного, змістового, організаційно-процесуального та результативного блоків, які забезпечують цілісність процесу професійної підготовки та спрямовані на формування готовності здобувачів освіти до ефективного використання засобів захисту інформації у професійній діяльності.

Методологічний блок визначає теоретичні засади функціонування моделі та виступає концептуальною основою підготовки майбутніх фахівців цифрових технологій. Центральне місце в ньому займає мета підготовки, яка полягає у

формуванні готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних у професійній діяльності. Саме мета визначає спрямованість усіх інших компонентів моделі та забезпечує їх узгоджене функціонування.

Важливою складовою методологічного блоку є наукові підходи, які визначають логіку організації освітнього процесу. Компетентнісний підхід забезпечує орієнтацію навчання на формування професійних компетентностей у сфері захисту даних. Системний підхід дозволяє розглядати підготовку як цілісну педагогічну систему, у якій усі елементи взаємопов’язані між собою. Діяльнісний підхід спрямовує навчальний процес на активну практичну діяльність здобувачів освіти. Особистісно орієнтований підхід забезпечує врахування індивідуальних особливостей, освітніх потреб і професійних інтересів студентів. Практико-орієнтований підхід створює умови для наближення навчання до реальних умов професійної діяльності, а технологічний підхід забезпечує проєктування освітнього процесу відповідно до визначених результатів навчання.

Концептуальні положення моделі визначають основні напрями підготовки майбутніх фахівців цифрових технологій. Вони передбачають інтеграцію питань захисту даних у зміст професійної підготовки, міждисциплінарний характер навчання, поєднання теоретичної та практичної складових освітнього процесу, а також постійне оновлення змісту навчання відповідно до сучасних тенденцій розвитку цифрових технологій та кібербезпеки. Реалізація зазначених положень забезпечує відповідність підготовки сучасним вимогам ринку праці та професійної діяльності.

Функціонування моделі ґрунтується на системі дидактичних принципів, які визначають вимоги до організації навчання. До них належать принцип професійної спрямованості, принцип практичної спрямованості навчання, принцип інтеграції теорії та практики, принцип актуальності змісту навчання, принцип міждисциплінарної інтеграції, принцип безперервності професійного розвитку, принцип моделювання професійної діяльності, принцип цифровізації

освітнього процесу та принцип кібербезпекової спрямованості. Зазначені принципи забезпечують цілісність та ефективність підготовки майбутніх фахівців цифрових технологій.

Змістовий блок моделі відображає систему професійних знань, вмінь і навичок, необхідних для застосування програмного забезпечення захисту даних. Його основу становить міждисциплінарна інтеграція навчальних дисциплін «Операційні системи», «Комп'ютерні мережі та захист даних», «Хмарні технології в навчальному процесі» та «Інформаційна безпека». Дисципліна «Операційні системи» забезпечує формування знань про механізми захисту операційних систем, управління доступом до ресурсів, адміністрування облікових записів користувачів, аудит подій безпеки та резервне копіювання даних. Дисципліна «Комп'ютерні мережі та захист даних» спрямована на формування знань щодо організації мережевої взаємодії, використання мережевих протоколів, технологій VPN, засобів моніторингу мережевого трафіку та протидії мережевим атакам. У межах дисципліни «Хмарні технології в навчальному процесі» здобувачі освіти опановують моделі надання хмарних послуг, механізми захисту даних у хмарному середовищі, технології резервного копіювання та управління доступом до хмарних ресурсів. Дисципліна «Інформаційна безпека» формує теоретичні засади забезпечення інформаційної безпеки, знання про кіберзагрози, криптографічні методи захисту, політики безпеки та механізми реагування на інциденти.

Особливе місце у структурі моделі займає блок педагогічних умов, який забезпечує ефективність формування готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних. Перша педагогічна умова передбачає інтеграцію змісту професійної підготовки із сучасними технологіями захисту даних та вимогами кібербезпеки, що забезпечує актуальність навчального контенту та його відповідність сучасним викликам цифрового середовища. Друга педагогічна умова полягає у забезпеченні практико-орієнтованого навчання шляхом використання професійного програмного забезпечення захисту даних, що сприяє формуванню практичних

вмінь і навичок майбутніх фахівців. Третя педагогічна умова передбачає використання цифрового освітнього середовища та засобів моделювання кіберзагроз, які створюють можливості для відпрацювання професійних дій у ситуаціях, наближених до реальної діяльності. Четверта педагогічна умова полягає у реалізації міждисциплінарної інтеграції змісту дисциплін, що забезпечує формування цілісного уявлення про процеси захисту інформації в сучасних інформаційних системах. П’ята педагогічна умова спрямована на активізацію навчально-пізнавальної діяльності здобувачів освіти через використання проєктних і дослідницьких методів навчання, які сприяють розвитку професійного мислення, самостійності та творчої активності.

Організаційно-процесуальний блок визначає механізми реалізації змісту підготовки. Він охоплює форми навчання, серед яких лекції, практичні та лабораторні заняття, проєктна діяльність, самостійна робота та онлайн-консультації. Реалізація змісту підготовки здійснюється із застосуванням проблемного, проєктного, дослідницького та інтерактивного методів навчання, кейс-технологій і методів моделювання професійних ситуацій. Засобами навчання виступають LMS-платформи, хмарні сервіси, віртуальні лабораторії, симулятори кіберзагроз, програмне забезпечення захисту даних та електронні освітні ресурси. Важливим елементом організаційно-процесуального блоку є система контролю та оцінювання результатів навчання, яка включає поточний контроль, модульне оцінювання, захист лабораторних робіт і проєктів, підсумкову атестацію, самооцінювання та взаємооцінювання. Ефективність функціонування цього компонента забезпечується відповідним нормативно-методичним, кадровим, матеріально-технічним та інформаційно-освітнім забезпеченням.

Результативний блок відображає підсумкові результати реалізації моделі. Його змістом є сформованість професійних компетентностей, необхідних для забезпечення конфіденційності, цілісності та доступності даних, виявлення й аналізу кіберзагроз, використання сучасних програмних засобів захисту інформації, забезпечення безпеки локальних і хмарних середовищ, дотримання

правових та етичних норм у сфері інформаційної безпеки. Кінцевим результатом функціонування моделі є сформована готовність майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних у професійній діяльності в умовах цифрового середовища, що виявляється у здатності ефективно виконувати професійні завдання із забезпечення інформаційної безпеки та захисту даних.

Таблиця 2.4

Характеристика структурно-функціональної моделі підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних

Блок	Складові	Характеристика
Методологічний	Мета, наукові підходи, концептуальні положення, принципи підготовки	Визначає теоретико-методологічні засади підготовки, цілі, підходи та принципи формування готовності до застосування програмного забезпечення захисту даних.
Змістовий	«Операційні системи», «Комп'ютерні мережі та захист даних», «Хмарні технології в навчальному процесі», «Інформаційна безпека»	Забезпечує формування системи знань, вмінь і навичок щодо використання програмних засобів захисту даних на основі міждисциплінарної інтеграції.
Педагогічні умови	Інтеграція змісту підготовки із сучасними технологіями захисту даних; практико-орієнтоване навчання; використання цифрового освітнього середовища; міждисциплінарна інтеграція; проєктно-дослідницька діяльність	Забезпечують ефективність освітнього процесу та створюють умови для формування професійних компетентностей у сфері захисту даних.
Організаційно-процесуальний	Форми, методи, засоби навчання, контроль та оцінювання, умови реалізації	Визначає механізми реалізації підготовки через лекції, лабораторні роботи, проєкти, цифрові платформи, віртуальні лабораторії та систему оцінювання результатів навчання.
Результативний	Професійні компетентності та готовність до застосування програмного забезпечення захисту даних	Відображає кінцевий результат підготовки – сформовану готовність майбутніх фахівців цифрових технологій до забезпечення захисту даних у професійній діяльності.

На основі аналізу українських досліджень (Биков, В., Спірін, О., & Пінчук, О. 2020; Спірін, О., Олексюк, В., Василенко, Я., & Сіренко, О. 2024)., а також специфіки ОПП у педагогічних ЗВО.

Таким чином, запропонована система підготовки забезпечує формування висококваліфікованого, мобільного та відповідального фахівця цифрових технологій, здатного ефективно працювати в сучасному освітньому середовищі та сприяти цифровій трансформації професійної освіти.

Структурними компонентами методики підготовки фахівців цифрових технологій до застосування програмного забезпечення захисту даних є взаємопов’язані блоки, які забезпечують цілісність та результативність освітнього процесу.

Ефективність реалізації методики забезпечується сукупністю педагогічних умов. До них належать: формування позитивної мотивації студентів до використання програмного забезпечення захисту даних у професійній діяльності; інтеграція змісту дисциплін цифрових технологій, кібербезпеки та професійної педагогіки; використання практико-орієнтованого навчання на основі реальних кейсів і проєктних завдань; створення цифрового освітнього середовища для моделювання професійних ситуацій із захисту даних; залучення студентів до розроблення власних освітніх продуктів і методичних матеріалів із питань кібербезпеки; забезпечення взаємодії закладів вищої освіти з IT-компаніями та закладами професійної освіти для організації практичної підготовки.

Взаємодія структурних компонентів методики та реалізація визначених педагогічних умов забезпечують формування готовності майбутніх фахівців цифрових технологій до ефективного застосування програмного забезпечення захисту даних і використання його в професійній та педагогічній діяльності.4. Переваги структурно-функціональної моделі

Запропонована структурно-функціональна модель підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних має *низку переваг*.

По-перше, модель характеризується цілісністю та системністю, оскільки об'єднує мету, методологічні засади, зміст підготовки, педагогічні умови, організацію освітнього процесу та результати навчання в єдину взаємопов'язану систему.

По-друге, важливою перевагою є компетентнісна спрямованість, що забезпечує орієнтацію підготовки не лише на засвоєння знань, а й на формування професійних компетентностей, необхідних для практичного використання програмного забезпечення захисту даних.

По-третє, модель забезпечує міждисциплінарну інтеграцію змісту навчання шляхом поєднання дисциплін «Операційні системи», «Комп’ютерні мережі та захист даних», «Хмарні технології в навчальному процесі» та «Інформаційна безпека», що сприяє формуванню комплексного бачення процесів захисту інформації.

Наступною перевагою є практико-орієнтований характер підготовки, який реалізується через використання лабораторних робіт, кейсів, проєктної діяльності, віртуальних лабораторій та засобів моделювання кіберзагроз.

Важливою особливістю моделі є її відповідність сучасним тенденціям цифровізації та кібербезпеки, що забезпечується інтеграцією актуального програмного забезпечення, хмарних сервісів та цифрових освітніх технологій.

Модель також характеризується гнучкістю та адаптивністю, оскільки дозволяє оновлювати зміст навчання відповідно до появи нових кіберзагроз, програмних продуктів та технологій захисту даних.

Додатковою перевагою є можливість використання в умовах змішаного та дистанційного навчання завдяки широкому застосуванню цифрового освітнього середовища та LMS-платформ.

Крім того, модель сприяє формуванню навичок самоосвіти та безперервного професійного розвитку, що є особливо важливим у сфері цифрових технологій, де знання швидко оновлюються.

Недоліки структурно-функціональної моделі

Разом із перевагами запропонована модель має певні обмеження, які необхідно враховувати під час її впровадження.

Одним із основних недоліків є залежність від матеріально-технічного забезпечення закладу освіти. Ефективна реалізація моделі потребує сучасної комп'ютерної техніки, мережевої інфраструктури, ліцензійного програмного забезпечення та доступу до хмарних сервісів.

Іншим обмеженням є необхідність високого рівня цифрової та професійної компетентності викладачів, які повинні володіти сучасними технологіями захисту даних, методиками цифрового навчання та навичками роботи зі спеціалізованим програмним забезпеченням.

Певні труднощі можуть виникати через швидке оновлення програмних засобів захисту даних і появу нових кіберзагроз, що потребує постійного коригування змісту навчальних дисциплін та методичного забезпечення.

Обмеженням також є значні часові витрати на організацію практичної та проєктної діяльності, особливо під час виконання комплексних міждисциплінарних завдань і моделювання професійних ситуацій.

Впровадження моделі може ускладнюватися через нерівномірний рівень початкової підготовки здобувачів освіти, що потребує додаткової диференціації навчального процесу.

Крім того, реалізація окремих компонентів моделі, зокрема віртуальних лабораторій та симуляторів кіберзагроз, може вимагати додаткових фінансових ресурсів на придбання або підтримку спеціалізованого програмного забезпечення.

Структурно-функціональна модель підготовки фахівців цифрових технологій до застосування програмного забезпечення захисту даних за спеціальністю 015 Професійна освіта, за спеціалізацією 015.39 Цифрові технології – це *педагогічно-орієнтована система подвійної компетентності*, яка забезпечує баланс між технічними навичками (програмування, мережі, захист даних) та професійною педагогічною майстерністю (методика викладання, розробка занять для здобувачів).

Модель ефективно працює, коли методика підготовки фахівців цифрових технологій до застосування програмного забезпечення захисту даних базується на діяльнісному, компетентнісному та ризик-орієнтованому підходах. Вона передбачає використання сучасних інструментів захисту даних, зокрема Wireshark і Cisco Packet Tracer, у поєднанні з методичною підготовкою майбутніх педагогів. Важливе місце в методиці займає формування знань щодо етичних і правових аспектів захисту інформації відповідно до національного законодавства та міжнародних стандартів. Практична спрямованість підготовки забезпечується завдяки застосуванню проєктного методу та елементів дуальної освіти.У підсумку випускник отримує не просто «технічні знання», а готовність бути наставником у сфері цифрової безпеки у системі професійної освіти України - готувати робітників і техніків, які свідомо захищають дані в умовах цифрової трансформації економіки та суспільства.

У контексті захисту даних спеціальність 015.39 Професійна освіта, спеціалізації 015.39 Цифрові технології має особливе значення, оскільки спрямована на підготовку педагогів, які поєднують цифрові та педагогічні компетентності. На відміну від спеціальностей, орієнтованих на підготовку фахівців з кібербезпеки, підготовка майбутніх педагогів цифрових технологій передбачає формування знань і практичних навичок із захисту даних, необхідних для безпечної професійної діяльності в цифровому освітньому середовищі.

Водночас майбутні фахівці повинні бути готовими передавати ці знання студентам закладів професійної освіти, формуючи в них основи кібергігієни, навички безпечної роботи з інформацією та відповідальне ставлення до захисту даних. Тому підготовка з питань захисту даних має подвійне спрямування: як складова професійної компетентності майбутнього педагога та як важливий елемент його методичної підготовки до навчання здобувачів освіти основам цифрової безпеки.

Підготовка здобувачів освіти за спеціальністю 015 Професійна освіта, спеціалізації 015.39 Цифрові технології забезпечує формування достатнього рівня компетентностей із захисту даних для виконання професійної та

педагогічної діяльності. Освітні програми, як правило, передбачають вивчення дисциплін або окремих модулів, присвячених комп'ютерним мережам, захисту даних, криптології та інформаційній безпеці. Важливою перевагою є поєднання теоретичної підготовки з практичною діяльністю, що реалізується через виконання лабораторних робіт із використанням сучасних програмних засобів та мережевих симуляторів. Значна увага приділяється нормативно-правовим аспектам захисту інформації, зокрема питанням захисту персональних даних, конфіденційності та безпечної роботи в цифровому освітньому середовищі.

Особливістю підготовки є її педагогічна спрямованість, яка передбачає формування здатності не лише використовувати засоби захисту даних у професійній діяльності, а й навчати цьому здобувачів закладів професійної освіти. Майбутні фахівці опановують методику розроблення навчальних матеріалів, інструктажів, рекомендацій та цифрових освітніх ресурсів з питань кібербезпеки. Водночас важливе місце посідає формування навичок кібергігієни, безпечного використання цифрових сервісів, захисту облікових записів та протидії поширеним кіберзагрозам.

Разом із тим підготовка за спеціальністю має певні обмеження. Насамперед вона орієнтована на формування базового або середнього рівня компетентностей у сфері захисту даних і не передбачає поглибленого вивчення спеціалізованих напрямів кібербезпеки, таких як тестування на проникнення, цифрова криміналістика, управління інцидентами безпеки чи аналіз шкідливого програмного забезпечення. Основний акцент робиться на освітньому та професійно орієнтованому застосуванні засобів захисту даних, а не на підготовці вузькопрофільних спеціалістів для корпоративного сектору або об'єктів критичної інфраструктури. Крім того, ефективність підготовки значною мірою залежить від рівня матеріально-технічного забезпечення закладу вищої освіти та доступності сучасного програмного забезпечення для навчання.

У процесі підготовки майбутніх фахівців за спеціальністю 015 Професійна освіта, спеціалізації 015.39 Цифрові технології важливе місце посідає формування компетентностей у сфері захисту даних. Насамперед випускник

повинен володіти навичками особистої цифрової безпеки, які забезпечують його безпечну професійну діяльність у цифровому освітньому середовищі. Це передбачає вміння захищати власні облікові записи за допомогою надійних паролів, багатофакторної автентифікації та засобів керування паролями, безпечно використовувати системи дистанційного навчання, працювати з хмарними сервісами, контролювати доступ до інформаційних ресурсів і забезпечувати захист персональних даних здобувачів освіти відповідно до вимог чинного законодавства.

Водночас майбутній фахівець цифрових технологій повинен бути готовим до навчання здобувачів закладів професійної освіти основам захисту даних та кібергігієни. Для цього він має володіти методикою розроблення навчальних матеріалів, уроків, практичних занять та інструктажів з питань цифрової безпеки для здобувачів різних професій. Важливим є вміння використовувати сучасні цифрові інструменти та навчальні симулятори для демонстрації типових загроз і способів їх попередження, а також інтегрувати питання захисту даних у зміст професійно орієнтованих ІТ-дисциплін, таких як програмування, комп’ютерні мережі та вебтехнології. Особливу увагу необхідно приділяти формуванню в студентів усвідомлення відповідальності за збереження даних клієнтів, роботодавців та організацій.

Важливою складовою підготовки є також етичний і правовий аспекти захисту даних. Майбутній педагог повинен усвідомлювати власну відповідальність за збереження та належне використання персональних даних студентів, знати основні положення законодавства у сфері захисту персональних даних, нормативні вимоги щодо обробки інформації в освітньому середовищі та принципи конфіденційності під час створення й використання цифрових освітніх ресурсів. Це сприяє формуванню відповідального ставлення до роботи з інформацією та дотримання професійної етики.

Таким чином, захист даних у підготовці фахівців за спеціальністю 015.39 Професійна освіта (Цифрові технології) розглядається не як окрема спеціалізація, а як невід’ємна складова цифрової компетентності педагога. Його

значення полягає у забезпеченні безпечної професійної діяльності майбутнього викладача та формуванні в здобувачів освіти культури відповідального і безпечного поводження з інформацією в умовах цифрового суспільства.

2.5. Методичне забезпечення підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних

Методичне забезпечення підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних розроблено відповідно до визначених педагогічних умов, структурно-функціональної моделі та сучасних вимог до професійної діяльності фахівців у сфері цифрових технологій і кібербезпеки.

Основою методичного забезпечення виступає змістове наповнення навчальних дисциплін «Операційні системи», «Комп’ютерні мережі та захист даних», «Хмарні технології в навчальному процесі» та «Інформаційна безпека». До змісту навчання включено тематичні модулі, присвячені сучасним технологіям захисту даних, програмному забезпеченню інформаційної безпеки, системам резервного копіювання, криптографічному захисту інформації, технологіям контролю доступу, мережевій безпеці та захисту хмарних ресурсів.

Практична складова методики реалізується через систему лабораторних робіт, практичних занять, кейсових завдань і навчальних проєктів. Лабораторні роботи передбачають встановлення та налаштування програмних засобів захисту даних, аналіз мережевої безпеки, налаштування міжмережевих екранів, систем резервного копіювання та засобів контролю доступу. Кейс-завдання орієнтовані на розв'язання професійних ситуацій, пов'язаних із виявленням та усуненням загроз інформаційній безпеці. Проєктна діяльність передбачає розроблення комплексних рішень щодо захисту даних в інформаційних системах різного призначення.

Реалізація методики здійснюється з використанням сучасних форм і методів навчання, серед яких лекції, практичні та лабораторні заняття, проєктне

навчання, кейс-метод, проблемне навчання, дослідницькі методи, групова робота та самостійна діяльність здобувачів освіти. Особлива увага приділяється використанню кіберполігонів, віртуальних лабораторій та цифрових симуляторів кіберзагроз, що дозволяють моделювати реальні умови професійної діяльності.

Важливим напрямом реалізації методики є інтеграція спеціалізованого програмного забезпечення захисту даних у навчальний процес. Для цього використовуються антивірусні системи, програмні засоби резервного копіювання, криптографічні системи, мережеві сканери безпеки, міжмережеві екрани, засоби моніторингу мережевого трафіку та програмне забезпечення для захисту хмарних сервісів. Їх застосування забезпечує формування практичного досвіду використання сучасних засобів інформаційної безпеки.

Розгляд методичного забезпечення та цифрових освітніх ресурсів у контексті підготовки майбутніх інженерно-педагогічних працівників за спеціальністю 015 Професійна освіта, спеціалізацією 015.39 Цифрові технології вимагає зміщення акцентів із суто інструментальних характеристик програм на їхній розвивальний та дидактичний потенціал. У цій системі технологічні засоби захисту даних перестають бути лише об’єктом вивчення та конфігурування, а перетворюються на потужний засіб формування інноваційного мислення майбутнього викладача. Весь комплекс методичних матеріалів та цифрових платформ проектується як відкрите середовище, що спонукає студента пройти шлях від технічного виконавця до архітектора безпечного освітнього простору та розробника авторського навчального контенту.

Важливим кроком у реалізації цієї концепції є трансформація середовищ віртуалізації із суто інженерних лабораторій на специфічні дидактичні тренажери професійної діяльності. Створюючи моделі гетерогенних мереж у віртуальних машинах чи хмарних сервісах, майбутній педагог вчиться проєктувати не просто захищений контур, а безпосередньо безпечне цифрове середовище закладу освіти. Студент отримує можливість імітувати в одній частині ізольованої системи типову недбалу поведінку підлітка, наприклад,

підключення до скомпрометованих точок доступу чи ігнорування сертифікатів безпеки, а в іншій – налаштовувати засоби моніторингу та блокування таких дій. Такий підхід забезпечує формування у майбутніх фахівців цифрових технологій здатності аналізувати сценарії реалізації кібератак, розвиває їхню професійну й методичну компетентність та сприяє ефективному поясненню здобувачам освіти причинно-наслідкових зв'язків у сфері кібергігієни.

Електронні освітні ресурси, на базі яких розгортається підготовка самих студентів, виконують функцію еталонного дидактичного зразка для моделювання їхньої майбутньої поведінки. Коли навчальний курс у системі управління навчанням побудований на засадах мікронавчання, містить інтерактивні відеотренажери, динамічні чек-лісти та гейміфіковані модулі з миттєвим зворотним зв'язком, студенти засвоюють цю викладацьку культуру через механізм наслідування. Вони на власному досвіді бачать, як правильно дозувати складний технічний матеріал, як утримувати увагу аудиторії в умовах дистанційного чи змішаного навчання і як автоматизувати контроль знань без створення зайвого когнітивного навантаження. Це закладає міцний фундамент для відмови від застарілих репродуктивних форм викладання на користь гнучких цифрових технологій.

Центральне місце у методичному забезпеченні посідають інструменти формування навичок методичної редукції, де студенти вчаться перекладати складну термінологію та інженерні логи захисного програмного забезпечення доступною мовою дидактики. Навчальні завдання формулюються таким чином, щоб спонукати здобувачів вищої освіти до створення власного цифрового продукту за допомогою інтерактивних конструкторів, платформ візуалізації та ментальних карт. Замість традиційних текстових звітів про перехоплення пакетів чи створення криптоконтейнерів, майбутні фахівці фахівці цифрових технологій розробляють наочну інфографіку, квізи, симуляційні ігри та адаптовані інструкції, орієнтовані на студентську аудиторію з кліповим сприйняттям інформації. Це дозволяє органічно поєднати глибокі технічні знання з креативною педагогічною майстерністю, перетворюючи методичне

забезпечення на цілісну екосистему, яка готує мобільного, технологічно грамотного викладача, здатного ефективно формувати культуру безпеки у майбутніх кваліфікованих робітників.

Поглиблення дидактичного потенціалу методики вимагає детального аналізу конкретних типів цифрових освітніх ресурсів, які трансформують інженерну практику в інноваційне педагогічне поле. У межах підготовки майбутніх викладачів цифрових технологій ці ресурси розподіляються на кілька функціональних рівнів, кожен з яких вирішує специфічні завдання з розвитку подвійної компетентності студентів – від налаштування захисту до візуалізації та трансляції цього досвіду студентам.

Перший рівень утворюють спеціалізовані хмарно-орієнтовані кіберполігони та віртуальні лабораторії штучного моделювання інфраструктури. На відміну від стандартних локальних програм віртуалізації, сучасні хмарні сервіси дозволяють розгортати масштабовані шаблони гетерогенних мереж, де студенти можуть експериментувати із промисловим програмним забезпеченням безпеки без ризику пошкодження фізичного обладнання закладу освіти. Методична цінність таких ресурсів полягає в можливості створення сценаріїв керованих кібератак. Студенти використовують ці інструменти як дидактичні тренажери, де вони спочатку самостійно ліквідують витоки даних або конфігурують дзеркалювання трафіку, а потім розробляють на основі цих віртуальних стендів завдання для самостійної роботи своїх майбутніх студентів, враховуючи необхідний рівень складності.

Другим важливим рівнем є інтерактивні платформи аналізу та візуалізації прихованих інформаційних процесів. Програми мережевого моніторингу та утиліти графічного відображення логів безпеки виконують у навчанні роль засобів макроскопічного унаочнення абстрактних явищ. Коли студент працює з аналізатором пакетів, програма виступає не просто технічною утилітою, а цифровим мікроскопом, який робить видимим рух даних, структуру протоколів та моменти несанкціонованого перехоплення інформації. Педагогічна складова тут реалізується через те, що майбутній викладач вчиться створювати цифрові

демонстраційні кейси. Він записує файли мережевого дампа із зафіксованою атакою, щоб згодом на заняттях у коледжі показати студентам явні ознаки компрометації системи, перетворюючи невидиму загрозу на очевидний навчальний факт.

Третій рівень охоплює конструктори інтерактивного контенту та цифрові платформи гейміфікації навчання. Саме ці ресурси є головним інструментом методичної редукції, коли складні алгоритми криптографії чи правила налаштування DLP-систем необхідно упакувати у доступну для підлітків форму. Студенти опановують сервіси створення ментальних карт, онлайн-дошки для командної роботи та платформи розробки квізів і симуляційних ігор. У процесі підготовки вони створюють мультимедійні навчальні продукти: квести з пошуку вразливостей, інтерактивні схеми побудови захищених з'єднань та візуальні чек-листи з персональної кібергігієни. Такий досвід учить майбутніх педагогів адаптувати контент під особливості сприйняття сучасних здобувачів освіти, комбінувати різні типи медіа та відходити від монотонного викладання теорії.

Завершальним рівнем є цифрові системи управління навчанням та інструменти автоматизованого моніторингу освітніх досягнень. Сучасні оболонки навчання інтегруються із зовнішніми лабораторними стендами за допомогою спеціальних програмних інтерфейсів, що дозволяє створювати наскрізні траєкторії підготовки. Для майбутнього фахівця така система стає простором для проектування власного цифрового кабінету. Вони вчаться налаштовувати автоматичний зворотний зв’язок, створювати бази компетентнісних тестів, де оцінюється не запам'ятовування термінів, а правильність вибору програмного рішення в імітаційній ситуації, та керувати груповою динамікою під час командних змагань із кібербезпеки. У результаті взаємодія з усім спектром цих цифрових ресурсів формує у студентів системне бачення того, як технології можуть підсилювати педагогічний процес, роблячи навчання безпеці даних динамічним, наочним та максимально наближеним до вимог реального життя.

З метою забезпечення системності та практичної спрямованості розроблюваної методики особливого значення набуває визначення її змістового наповнення, яке конкретизується через структуру навчальної дисципліни, зокрема через модулі, теми, практичні роботи та кейси.

Структура дисципліни «Кібербезпека та захист даних у професійній освіті» наведена в додатку Г.

Змістове наповнення навчальної дисципліни свідчать про необхідність подальшого обґрунтування дидактичних умов її реалізації в освітньому процесі підготовки майбутніх фахівців за спеціальністю 015 Професійна освіта, спеціалізації 015.39 Цифрові технології. Зокрема, актуалізується питання вибору найбільш ефективних форм, методів та засобів навчання, які забезпечують формування професійних компетентностей здобувачів освіти у сфері захисту даних, кібербезпеки та цифрової грамотності, а також сприяють практико-орієнтованій підготовці до застосування програмного забезпечення захисту інформації у майбутній професійній діяльності.

Структурувати матеріал за основними формами та методами, які важливо використовувати у контексті нашої спеціальності.

У системі підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних особливе місце посідає метод *проєктного навчання,* який розглядається як один із найбільш ефективних та комплексних, оскільки інтегрує технічну, аналітичну та педагогічну складові професійної діяльності. Його використання забезпечує не лише формування практичних навичок у сфері кібербезпеки, але й розвиток педагогічної компетентності здобувачів освіти, що є особливо важливим у межах спеціальності 015 Професійна освіта, спеціалізації 015.39 Цифрові технології.

Проєктне навчання передбачає виконання здобувачами освіти тривалих навчально-професійних проєктів, тривалість яких варіюється від 2 до 8 тижнів залежно від рівня складності. Такі проєкти мають подвійний цільовий характер: з одного боку, вони спрямовані на розроблення реального технічного рішення у

сфері захисту даних або кібербезпеки, а з іншого – на створення повноцінного навчально-методичного пакета для використання у закладах вищої освіти.

Зміст проєктної діяльності включає обов'язкову технічну та педагогічну складові. Технічна складова охоплює розробку політик інформаційної безпеки, налаштування програмних засобів захисту даних (зокрема VeraCrypt, BitLocker), конфігурацію мережевих середовищ із використанням систем керування доступом (ACL) у симульованих середовищах, таких як Cisco Packet Tracer, а також проведення базового аналізу вразливостей інформаційних систем.

Педагогічна складова передбачає розроблення методичних матеріалів для навчання здобувачів освіти, зокрема конспектів занять, презентацій, інструкцій, чек-листів, тестових завдань і навчальних кейсів. Особлива увага приділяється здатності студентів трансформувати складний технічний матеріал у доступні навчальні ресурси, що забезпечує формування їхньої методичної компетентності.

Прикладами проєктів є, зокрема: розробка комплексної програми захисту персональних даних для закладів освіти, створення захищеної онлайн-платформи для освітнього середовища, а також аудит безпеки Wi-Fi мережі навчальних майстерень. У кожному з цих випадків реалізується поєднання технічного аналізу та педагогічного моделювання навчального процесу.

Оцінювання результатів проєктної діяльності здійснюється за критеріальною системою, що забезпечує комплексний підхід до визначення рівня сформованості компетентностей. Зокрема, 40 % загальної оцінки становить технічна якість розробленого рішення, 40 % – якість педагогічної складової (методична обґрунтованість, структурованість навчальних матеріалів), і 20 % – рівень рефлексії, аргументованість та якість презентації результатів.

Таким чином, проєктне навчання виступає інтегрованим дидактичним інструментом, що забезпечує поєднання технічної підготовки у сфері кібербезпеки з формуванням педагогічної компетентності, сприяючи цілісному розвитку професійної готовності майбутніх фахівців цифрових технологій.

Кейс-метод

Дуже ефективний для формування критичного мислення та правової свідомості.

В дослідженні запропоновано використання таких кейс-методів у процесі підготовки фахівців цифрових технологій на лабораторних заняттях дисципліни «Захист даних у професійній діяльності»:

1. Реальні витоки даних в освіті та бізнесі (2023-2025 рр.). – приклад: витік даних здобувачів через відкритий Google Drive викладача. Завдання: визначити порушені статті Закону Про захист персональних даних (Верховна Рада України. 2010), відповідальних осіб, наслідки, заходи запобігання.

2. Професійно-орієнтовані кейси Приклад: здобувач надіслав файл з даними одногрупників через незахищений месенджер → витік. Завдання: розробити інструкцію «Безпечна передача даних клієнтів у логістиці».

3. Етичні дилеми Приклад: викладач хоче записати заняття для YouTube, але на відео видно обличчя здобувачів. Завдання: аргументувати рішення (згода / анонімізація / відмова від публікації).

Під час проведення лабораторного заняття на тему: «Оцінка ризиків витоку персональних даних у повсякденних та професійних ситуаціях» з дисципліни «Захист даних у професійній діяльності» здобувачам освіти пропонується кейс «Реальні витоки даних в освіті та бізнесі», побудований на основі реальної ситуації витоку персональних даних через помилкове налаштування прав доступу до хмарного сховища Google Drive. За умовами кейсу викладач закладу освіти розмістив у спільній папці документи, що містили персональні дані здобувачів освіти, однак через некоректні налаштування доступу інформація стала доступною стороннім особам.

На рисунку 2.4 представлено інтерфейс керування доступом до файлу в хмарному сервісі Google Drive. Вікно налаштування спільного доступу демонструє механізм надання прав користувачам для перегляду або редагування електронних документів, що зберігаються у хмарному середовищі. Зокрема, відображено процес додавання нового користувача до переліку осіб, які можуть отримати доступ до файлу, а також вибір рівня його повноважень.

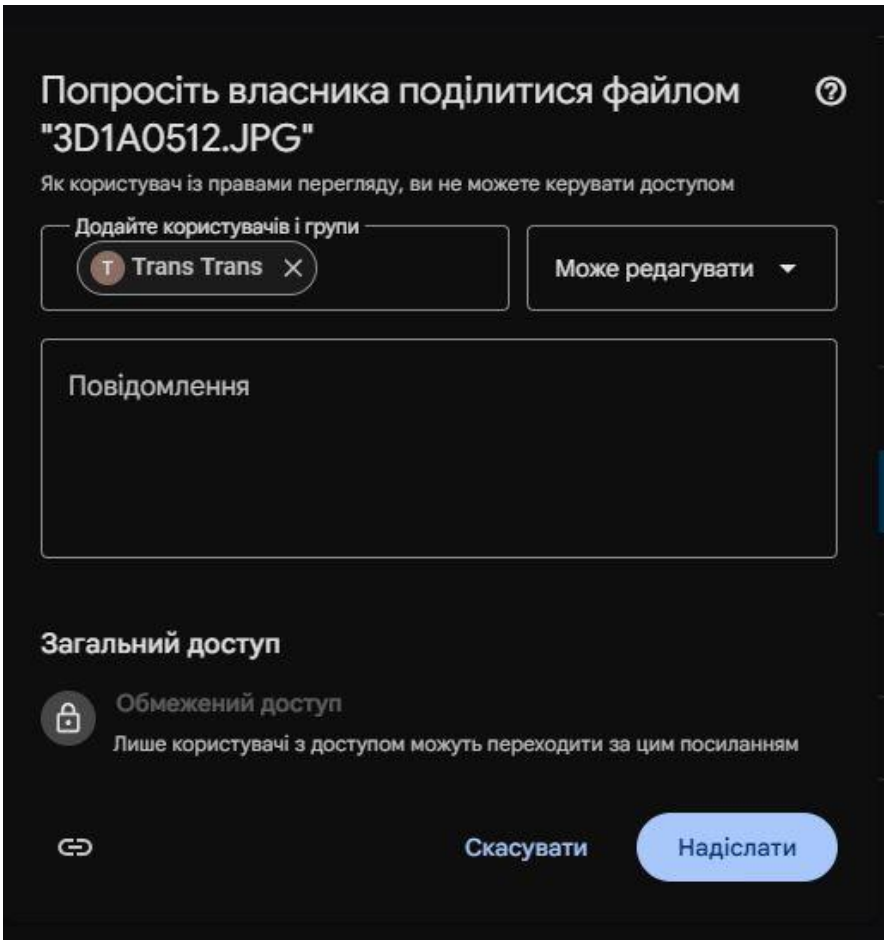

Рис. 2.4. Приклад помилкового налаштування прав доступу до файлу в Google Drive як джерела ризику витоку персональних даних

Представлена ситуація ілюструє один із типових ризиків інформаційної безпеки, пов’язаних із неправильним налаштуванням прав доступу до інформаційних ресурсів. Помилки під час надання дозволів, недостатній контроль за колом користувачів або випадкове надання розширених привілеїв можуть призвести до несанкціонованого доступу до конфіденційної інформації та витоку персональних даних. Особливої актуальності такі ризики набувають в освітньому середовищі, де в хмарних сховищах можуть зберігатися відомості про здобувачів освіти, результати навчання, персональні документи та інші інформаційні ресурси з обмеженим доступом.

Робота з кейсом організовується протягом 60-80 хвилин і передбачає кілька послідовних етапів. На першому етапі (10 хвилин) студенти ознайомлюються з описом ситуації, вивчають вихідні дані та визначають

ключову проблему інформаційної безпеки. Особлива увага приділяється аналізу обставин виникнення інциденту та характеристиці інформації, яка зазнала витоку.

Другий етап передбачає роботу в малих групах (40-60 хвилин). У процесі обговорення студенти аналізують причини виникнення інциденту, визначають порушені вимоги законодавства України щодо захисту персональних даних, встановлюють коло відповідальних осіб та оцінюють можливі наслідки для закладу освіти і суб'єктів персональних даних. Окремим завданням є розроблення комплексу організаційних та технічних заходів щодо запобігання подібним ситуаціям у майбутньому. Результати аналізу оформлюються у вигляді рекомендацій або плану реагування на інцидент.

На третьому етапі (близько 20 хвилин) представники кожної групи презентують результати своєї роботи. Під час обговорення здійснюється порівняння запропонованих рішень, оцінювання їх ефективності та визначення найбільш доцільних заходів захисту даних. Викладач координує дискусію та акцентує увагу на правильності застосування нормативно-правових положень і сучасних підходів до забезпечення інформаційної безпеки.

Завершальним етапом є рефлексія, під час якої здобувачі освіти відповідають на запитання: «Як би я діяв на місці відповідальної особи?». Така форма підсумкового обговорення сприяє усвідомленню особистої відповідальності за забезпечення захисту даних, розвитку критичного мислення та формуванню професійної готовності до прийняття рішень у реальних ситуаціях, пов'язаних із порушенням інформаційної безпеки.

Застосування даного кейсу забезпечує формування когнітивного компонента готовності через засвоєння нормативно-правових основ захисту персональних даних, діяльнісного компонента через аналіз інцидентів і розроблення заходів реагування, мотиваційно-ціннісного компонента через усвідомлення значущості захисту інформації, а також рефлексивного компонента через самооцінювання власних професійних дій у запропонованій ситуації.

Лабораторні роботи

У межах розробленої методики підготовки майбутніх фахівців цифрових технологій лабораторні заняття розглядаються як цілісна педагогічна система, спрямована на поетапне формування професійних компетентностей. Їх організація ґрунтується на структурно-логічній послідовності навчальної діяльності, що забезпечує поступовий перехід від мотиваційного залучення здобувачів освіти до самостійного виконання практичних завдань, їх аналітичного опрацювання та рефлексивного осмислення отриманих результатів.

На початковому етапі лабораторного заняття здійснюється організація навчальної діяльності, актуалізація опорних знань та формування навчальної мотивації. У цей період викладач створює проблемну ситуацію професійного характеру, яка сприяє усвідомленню здобувачами освіти практичної значущості навчального матеріалу та активізує їх пізнавальну діяльність. Такий підхід забезпечує формування внутрішньої готовності до виконання подальших навчальних завдань і сприяє розвитку інтересу до професійно орієнтованої діяльності.

Наступний етап передбачає теоретичне забезпечення навчальної діяльності, у межах якого відбувається систематизація та актуалізація базових знань, необхідних для виконання практичних завдань. Здобувачі освіти опановують ключові поняття, принципи та алгоритми дій, що формують когнітивну основу для подальшої практичної роботи. Викладач виконує функцію координатора та фасилітатора навчального процесу, забезпечуючи зрозуміле подання навчального матеріалу та його зв’язок із майбутньою професійною діяльністю.

Основний етап лабораторного заняття має практично-діяльнісний характер і передбачає безпосереднє виконання навчально-практичних завдань. На цьому етапі здобувачі освіти застосовують набуті знання для розв’язання типових і проблемних ситуацій, здійснюють моделювання професійної діяльності, а також фіксують і систематизують отримані результати. Саме на цьому рівні

відбувається формування операційно-технологічних вмінь, розвиток самостійності та здатності до практичного застосування теоретичних знань.

Подальший етап передбачає аналітичне опрацювання результатів виконаної роботи. Здобувачі освіти здійснюють їх інтерпретацію, виявляють закономірності, помилки та труднощі, що виникали в процесі виконання завдань, а також формулюють обґрунтовані висновки. Така діяльність сприяє розвитку критичного мислення, аналітичних вмінь і здатності до узагальнення навчального матеріалу.

Важливим компонентом лабораторного заняття є рефлексивний етап, у межах якого здобувачі освіти здійснюють самооцінювання власної діяльності, визначають рівень досягнутих результатів, аналізують труднощі та окреслюють шляхи їх подолання. Рефлексія сприяє формуванню здатності до саморегуляції навчальної діяльності та розвитку професійного самовдосконалення.

Завершальним етапом є підсумково-оцінювальний, який передбачає представлення та захист результатів виконаної роботи, їх обговорення та оцінювання. Оцінювання здійснюється з урахуванням правильності виконання завдань, рівня самостійності, якості аналітичних висновків та здатності здобувачів освіти до узагальнення і презентації результатів діяльності. Таким чином, запропонована структура лабораторного заняття забезпечує цілісність навчального процесу та сприяє ефективному формуванню професійних компетентностей майбутніх фахівців цифрових технологій.

Тематика лабораторних робіт охоплює основні напрями використання сучасних засобів захисту даних (табл. 2.5). Виконання лабораторних завдань передбачає використання спеціалізованого програмного забезпечення, аналіз реальних і змодельованих ситуацій у сфері кібербезпеки, а також розроблення практичних рішень щодо забезпечення конфіденційності, цілісності та доступності даних. Зазначені інструкції наведено в додатку В.

Таблиця 2.5

Теми лабораторних занять

№ з/п	Назва лабораторної роботи	Кількість годин (денна форма)
1	Лабораторна робота №1. Оцінка ризиків витоку персональних даних (ідентифікація загроз, класифікація ризиків, визначення рівнів критичності). Результат: таблиця ризиків та пам'ятка з мінімізації ризиків	4
2	Лабораторна робота №2. Аналіз реальних порушень законодавства у сфері захисту персональних даних (розгляд кейсів інцидентів, визначення правових наслідків). Результат: аналітична таблиця та рекомендації щодо запобігання порушенням	4
3	Лабораторна робота №3. Шифрування даних за допомогою VeraCrypt (створення зашифрованих контейнерів, налаштування доступу). Результат: пам'ятка «Правила створення надійних паролів та використання шифрування»	4
4	Лабораторна робота №4. Аналіз мережевого трафіку з використанням Wireshark (захоплення пакетів, виявлення потенційно небезпечної активності). Результат: пам'ятка «Як перевірити безпеку веб-ресурсів за мережевою активністю»	4
5	Лабораторна робота №5. Моделювання захищеної локальної мережі у Cisco Packet Tracer (налаштування сегментації та базового контролю доступу). Результат: інструкція «Правила безпеки локальної обчислювальної мережі»	4
6	Лабораторна робота №6. Сканування мережевих портів у контрольованому середовищі (Nmap) та аналіз відкритих сервісів. Результат: інструкція «Чому необхідно обмежувати відкриті порти та сервіси»	4
7	Лабораторна робота №7. Аналіз ризиків платформ дистанційного навчання (Zoom, Google Classroom, Moodle) з точки зору захисту персональних даних. Результат: чек-лист «Безпечне використання платформ дистанційного навчання»	4
8	Лабораторна робота №8. Розробка політики інформаційної безпеки для малого підприємства або закладу освіти (визначення політик доступу, зберігання та захисту даних). Результат: готова політика інформаційної безпеки та методичні рекомендації	4

Кіберполігони та віртуальні лабораторії

У дослідженні запропоновано використання кіберполігонів та віртуальних лабораторій у процесі підготовки майбутніх фахівців цифрових технологій на

лабораторних заняттях дисципліни «Захист даних у професійній діяльності». Застосування спеціалізованих платформ дає можливість моделювати реальні сценарії забезпечення інформаційної безпеки, здійснювати аналіз кіберзагроз, досліджувати вразливості інформаційних систем та відпрацьовувати практичні навички використання програмного забезпечення захисту даних у безпечному навчальному середовищі. Особливістю такого підходу є поєднання теоретичної підготовки з практичною діяльністю, максимально наближеною до умов майбутньої професійної діяльності фахівців цифрових технологій.

Однією з найбільш доступних і педагогічно доцільних платформ для організації такого навчання є TryHackMe, яка містить значну кількість інтерактивних навчальних кімнат (Rooms), присвячених основам кібербезпеки, мережевим технологіям, захисту інформації та аналізу кіберзагроз.

У межах виконання лабораторного заняття на тему: «Захоплення та аналіз власного мережевого трафіку» доцільним є використання навчальних кімнат Pre Security, Intro to Defensive Security, Network Fundamentals та Web Scanning. (рис. 2.5).Зазначені модулі дозволяють здобувачам освіти ознайомитися з базовими принципами захисту інформації, механізмами функціонування комп'ютерних мереж, методами виявлення вразливостей вебресурсів та способами протидії кіберзагрозам.

Рисунок 2.5 Послідовність формування компетентностей з кібербезпеки на платформі TryHackMe

Під час лабораторного заняття студентам пропонується пройти визначену кімнату на платформі TryHackMe та виконати передбачені практичні завдання. Наприклад, у межах кімнати Intro to Defensive Security здобувачі освіти досліджують основні типи кіберзагроз, знайомляться з принципами моніторингу подій безпеки та аналізують способи реагування на інциденти інформаційної безпеки. У кімнаті Network Fundamentals студенти виконують завдання з аналізу мережевої взаємодії, досліджують принципи адресації та маршрутизації даних, а також визначають потенційні ризики для мережевої інфраструктури.

Робота у віртуальній лабораторії організовується за такою схемою: на першому етапі здобувачі освіти ознайомлюються з теоретичними відомостями та інструкцією до виконання завдання; на другому етапі проходять інтерактивний сценарій платформи TryHackMe, виконуючи запропоновані практичні вправи; на третьому етапі аналізують отримані результати та формулюють висновки щодо виявлених загроз і способів їх усунення.

Особливістю використання даної платформи в підготовці майбутніх педагогів професійного навчання є поєднання технічної та методичної складових підготовки. Після завершення роботи у віртуальній лабораторії студенти розробляють короткий конспект-урок або навчальну інструкцію для здобувачів освіти за тематикою виконаного завдання. Такий підхід сприяє формуванню не лише професійних компетентностей у сфері кібербезпеки, а й педагогічних вмінь щодо організації навчання з питань захисту даних та цифрової безпеки.

Використання кіберполігону TryHackMe забезпечує можливість навчання в умовах, максимально наближених до реальної професійної діяльності, сприяє розвитку навичок аналізу кіберзагроз, прийняття рішень у нестандартних ситуаціях та формуванню готовності до застосування сучасного програмного забезпечення захисту даних. Додатковими перевагами платформи є наявність безкоштовних навчальних модулів, готових сценаріїв практичної роботи, системи контролю результатів та можливість отримання сертифікатів про проходження окремих курсів.

Проведений аналіз форм, методів і засобів навчання дозволяє стверджувати, що найбільш ефективною для підготовки майбутніх фахівців спеціальності 015 «Професійна освіта» (спеціалізація 015.39 «Цифрові технології») до застосування програмного забезпечення захисту даних є комплексна реалізація проєктного навчання, лабораторних робіт, кейс-методу, кіберполігонів і віртуальних лабораторій (рис. 2.6). Поєднання зазначених методів забезпечує формування всіх компонентів готовності майбутніх фахівців до професійної діяльності у сфері захисту даних та інформаційної безпеки.

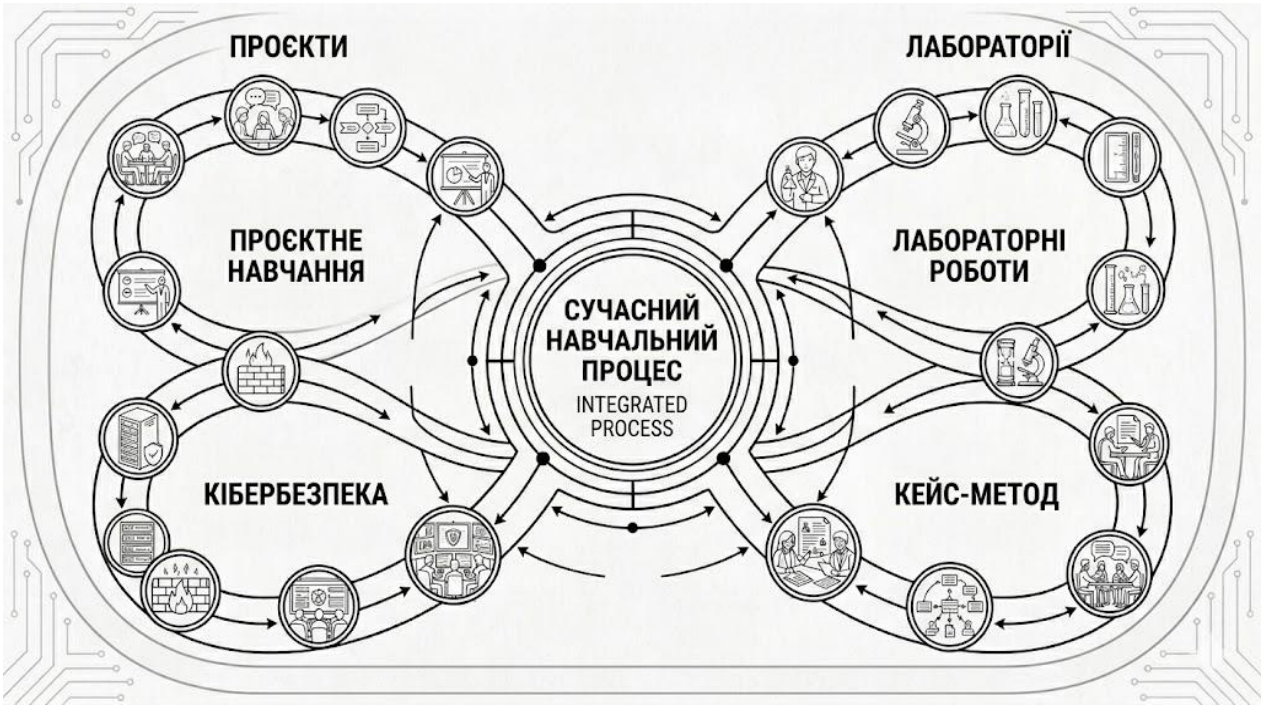

Рис.2.6 Модель інтеграції методів підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних

Визначальну роль у системі підготовки відіграє проєктне навчання, яке виступає завершальним етапом формування професійних компетентностей та забезпечує інтеграцію знань, вмінь і практичного досвіду, отриманих у процесі навчання. Реалізація комплексних проєктів, пов’язаних із розробленням та впровадженням систем захисту даних, дозволяє здобувачам освіти застосовувати набуті компетентності для розв’язання професійних завдань у наближених до реальної практики умовах.

Основою формування практичних навичок виступають лабораторні роботи, які забезпечують безпосереднє опанування сучасного програмного забезпечення захисту даних, відпрацювання технологій моніторингу мережевого трафіку, налаштування засобів захисту інформації, аналізу вразливостей та реагування на інциденти інформаційної безпеки. Саме лабораторні заняття створюють необхідні умови для переходу від теоретичного засвоєння матеріалу до практичного застосування отриманих знань.

Важливим засобом формування правової та етичної компетентності майбутніх фахівців є кейс-метод, який передбачає аналіз реальних або змодельованих ситуацій порушення інформаційної безпеки. Робота з кейсами сприяє розвитку здатності оцінювати ризики, приймати обґрунтовані рішення щодо захисту даних, застосовувати нормативно-правові акти у сфері інформаційної безпеки та усвідомлювати професійну відповідальність за збереження інформаційних ресурсів.

Особливе значення у підготовці майбутніх фахівців цифрових технологій мають кіберполігони та віртуальні лабораторії, використання яких доцільне переважно на старших курсах навчання. Такі засоби забезпечують моделювання реальних кіберзагроз, відпрацювання навичок виявлення та нейтралізації атак, дослідження вразливостей інформаційних систем і формування практичного досвіду роботи в умовах, максимально наближених до професійної діяльності. Використання платформ типу TryHackMe дозволяє поєднати технічну підготовку з розвитком педагогічних компетентностей через розроблення студентами навчально-методичних матеріалів за результатами виконаних завдань.

Таким чином, найбільшу ефективність забезпечує комплексне використання проєктного навчання, лабораторних робіт, кейс-методу та кіберполігонів, оскільки саме така інтеграція створює умови для формування когнітивного, діяльнісного, мотиваційного та рефлексивного компонентів готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних у професійній діяльності.

Важливим складником підготовки майбутніх фахівців спеціальності 015 Професійна освіта, спеціалізації 015.39 Цифрові технології є інтеграція спеціалізованого програмного забезпечення захисту даних у освітньо професійну програму. Актуальність такого підходу зумовлена необхідністю формування в майбутніх фахівців цифрових технологій не лише технічних компетентностей у сфері інформаційної безпеки, але й здатності здійснювати освітню діяльність, спрямовану на формування цифрової грамотності, кібергігієни та навичок захисту даних у здобувачів професійної освіти.

На відміну від технічних спеціальностей галузі інформаційних технологій, де вивчення програмного забезпечення захисту даних орієнтоване переважно на підготовку фахівців із розроблення та адміністрування інформаційних систем, у межах спеціальності 015 Професійна освіта, спеціалізації 015.39 Цифрові технології інтеграція таких програмних засобів має подвійне спрямування. По-перше, вона забезпечує формування власної професійної компетентності майбутнього фахівця цифрових технологій щодо використання сучасних засобів захисту інформації у професійній діяльності. По-друге, сприяє розвитку його здатності організовувати та проводити навчальні заняття з питань інформаційної безпеки, адаптуючи складні технічні поняття до рівня підготовки фахівців цифрових технологій.

У процесі дисертаційного дослідження запропоновано інтегрувати в освітній процес такі програмні засоби, як Wireshark, Cisco Packet Tracer, VeraCrypt, Nmap у складі дистрибутива Kali Linux, а також платформу Splunk Enterprise для демонстрації сучасних підходів до моніторингу подій інформаційної безпеки. Використання зазначених інструментів дозволяє забезпечити формування практичних навичок аналізу мережевого трафіку, моделювання комп’ютерних мереж, шифрування даних, виявлення вразливостей інформаційних систем та моніторингу подій безпеки.

Особливістю запропонованої методики є педагогічно орієнтований підхід до використання спеціалізованого програмного забезпечення. У цьому випадку програмні засоби розглядаються не лише як об’єкти професійного навчання, а й

як дидактичні засоби навчання, навколо яких організовується освітня діяльність. Кожен інструмент стає основою для розроблення навчальних занять, практичних завдань, проєктів, інструктажів використання програмного забезпечення захисту даних (додаток А) та тренінгів, що забезпечує одночасне формування технічних і фахових компетентностей майбутніх фахівців цифрових технологій.

Реалізація інтеграції спеціалізованого програмного забезпечення здійснюється відповідно до принципу подвійної спрямованості навчання. Під час виконання лабораторних робіт, здобувачі освіти не лише опановують функціональні можливості програмних продуктів та набувають практичних навичок роботи з ними, але й можуть розробляти навчально-методичні матеріали для майбутньої педагогічної діяльності. Зокрема, результатом виконання завдань можуть бути чек-листи, тестові завдання, презентації або фрагменти навчальних занять, присвячених питанням захисту даних і кібербезпеки. Такий підхід сприяє інтеграції професійної та педагогічної підготовки та забезпечує формування готовності до викладання відповідних дисциплін у закладах вищої освіти.

Інтеграція спеціалізованого програмного забезпечення здійснюється за принципом поступового ускладнення змісту навчання. На початкових етапах підготовки (1-2 курси) доцільним є використання програмних засобів Cisco Packet Tracer та VeraCrypt. Cisco Packet Tracer забезпечує формування базових уявлень про побудову комп’ютерних мереж, принципи маршрутизації та засоби мережевого захисту, тоді як VeraCrypt дозволяє опанувати основи шифрування інформації та захисту даних від несанкціонованого доступу.

На третьому курсі навчання до змісту підготовки вводяться складніші інструменти, зокрема Wireshark, який використовується для моніторингу та аналізу мережевого трафіку, дослідження мережевих протоколів і виявлення потенційних загроз інформаційній безпеці. Одночасно здобувачі освіти опановують базові механізми контролю доступу та захисту мережевої інфраструктури.

На завершальному етапі підготовки (4 курс) доцільним є використання спеціалізованих інструментів аналізу захищеності інформаційних систем,

зокрема Nmap у середовищі Kali Linux, а також ознайомлення з можливостями платформи Splunk Enterprise. Робота з такими інструментами здійснюється виключно в ізольованих навчальних середовищах, кіберполігонах або віртуальних лабораторіях із дотриманням вимог безпечного та етичного використання засобів кібербезпеки. На цьому етапі особливого значення набуває проєктна діяльність, у межах якої здобувачі освіти розробляють комплексні рішення щодо захисту даних та створюють методичні матеріали для їх подальшого використання в освітньому процесі.

Таким чином, інтеграція спеціалізованого програмного забезпечення захисту даних у підготовку майбутніх фахівців спеціальності 015 Професійна освіта, спеціалізації 015.39 Цифрові технології забезпечує формування цілісної системи професійних і педагогічних компетентностей, необхідних для ефективного використання сучасних засобів інформаційної безпеки та організації навчання з питань захисту даних у закладах професійної освіти.

Висновки до розділу 2

У другому розділі дисертаційного дослідження розроблено та теоретично обґрунтовано методику підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних. Встановлено, що необхідність удосконалення такої підготовки зумовлена процесами цифровізації суспільства, зростанням кількості кіберзагроз та підвищенням вимог до забезпечення інформаційної безпеки в професійній діяльності фахівців цифрової галузі.

Визначено концептуальні засади методики, основу яких становлять компетентнісний, системний, діяльнісний, особистісно орієнтований, практико-орієнтований і технологічний наукові підходи. Їх інтеграція забезпечує цілісність освітнього процесу та спрямованість підготовки на формування готовності здобувачів освіти до ефективного використання програмного забезпечення захисту даних у професійній діяльності.

Обґрунтовано структурно-функціональну модель підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних, яка включає методологічний, змістовий, організаційно-процесуальний та результативний компоненти. Модель відображає взаємозв'язок мети, змісту, педагогічних умов, форм, методів і засобів навчання та орієнтована на формування професійних компетентностей у сфері захисту інформації.

Визначено та охарактеризовано педагогічні умови ефективного формування готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних, а саме: актуалізацію змісту професійної підготовки відповідно до сучасних тенденцій розвитку цифрових технологій і кібербезпеки; забезпечення практико-орієнтованого навчання із застосуванням спеціалізованого програмного забезпечення; використання цифрового освітнього середовища та віртуальних лабораторій; реалізацію міждисциплінарної інтеграції фахових дисциплін; активізацію навчально-пізнавальної діяльності здобувачів освіти через проєктну та дослідницьку діяльність.

Розроблено методичне забезпечення дисципліни «Кібербезпека та захист даних у професійній освіті» (ЕНМК), яке охоплює вивчення сучасних програмних засобів захисту даних, зокрема Wireshark, Cisco Packet Tracer, VeraCrypt, Kali Linux та Splunk. Запропоновано механізми інтеграції зазначених програмних продуктів у професійну підготовку майбутніх педагогів цифрових технологій на засадах поєднання технічної та педагогічної складових професійної діяльності.

Обґрунтовано доцільність використання комплексу сучасних методів навчання, серед яких лабораторні роботи, кейс-метод, проєктне навчання, кіберполігони та віртуальні лабораторії. Встановлено, що їх комплексне застосування забезпечує формування когнітивного, діяльнісного, мотиваційного та рефлексивного компонентів готовності до застосування програмного забезпечення захисту даних, сприяє розвитку професійного мислення, навичок

аналізу кіберзагроз та здатності приймати обґрунтовані рішення щодо забезпечення інформаційної безпеки.

Отримані результати стали підґрунтям для проведення педагогічного експерименту, спрямованого на перевірку ефективності розробленої методики підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних, результати якого наведено у третьому розділі дисертаційного дослідження.

РОЗДІЛ 3
ЕКСПЕРИМЕНТАЛЬНА ПЕРЕВІРКА ЕФЕКТИВНОСТІ МЕТОДИКИ ПІДГОТОВКИ ФАХІВЦІВ

3.1. Організація та етапи педагогічного експерименту

Експериментальна перевірка ефективності розробленої методики підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних здійснювалася відповідно до мети, завдань та логіки педагогічного дослідження. Необхідність проведення педагогічного експерименту була зумовлена потребою перевірки результативності запропонованої структурно-функціональної моделі, педагогічних умов та методичного забезпечення підготовки здобувачів освіти до використання сучасного програмного забезпечення захисту даних у професійній діяльності.

Експериментальна робота проводилася на базі закладів вищої освіти, які здійснюють підготовку фахівців за спеціальностями галузі інформаційних технологій та цифрових технологій. У дослідженні брали участь здобувачі освіти, які вивчали дисципліни «Операційні системи», «Комп'ютерні мережі та захист даних», «Хмарні технології в навчальному процесі» та «Інформаційна безпека». Для забезпечення об'єктивності результатів було сформовано контрольну та експериментальну групи, приблизно рівні за кількістю учасників і рівнем попередньої підготовки.

Педагогічний експеримент проводився протягом трьох взаємопов'язаних етапів: діагностичного, формувального та контрольного.

Метою педагогічного експерименту (Співаковський, О. В., Осипова, Н. В., & Сніжко, М. В. 2010) була перевірка ефективності розробленої методики підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних, яка ґрунтується на комплексному поєднанні демонстрації мережевого трафіку із використанням спеціалізованого

програмного забезпечення, аналізу реальних кейсів із практики захисту персональних даних, виконання практичних завдань та організації рефлексивної діяльності здобувачів освіти. Запропонована методика була спрямована на підвищення рівня усвідомлення ризиків витоку персональних даних, формування практичних навичок кібергігієни та розвиток мотивації до безпечної поведінки в цифровому середовищі.

Відповідно до поставленої мети дослідження було визначено такі завдання педагогічного експерименту: здійснити діагностику початкового рівня готовності студентів до застосування програмного забезпечення захисту даних; реалізувати комплекс навчальних занять із використанням спеціалізованого програмного забезпечення та інтерактивних методів навчання; провести підсумкове оцінювання рівня сформованості знань, вмінь, навичок і мотиваційних установок здобувачів освіти; здійснити статистичний та якісний аналіз отриманих результатів для визначення ефективності розробленої методики.

У педагогічному експерименті, спрямованому на перевірку ефективності розробленої методики підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних, взяли участь 122 здобувачі вищої освіти спеціальності 015 Професійна освіта, спеціалізації 015.39 Цифрові технології. У вибірці брали участь сформовані академічні групи, які навчаються за ОПП «Професійна освіта (Цифрові технології)». Експериментальне дослідження проводилося на базі Тернопільського національного педагогічного університету імені Володимира Гнатюка та Рівненського державного гуманітарного університету, що дало змогу забезпечити показовість вибірки та підвищити об’єктивність отриманих результатів.

Відповідно до завдань педагогічного експерименту учасників було розподілено на контрольну та експериментальну групи (табл. 3.1). До складу експериментальної групи увійшли 64 студенти, професійна підготовка яких здійснювалася із застосуванням розробленої методики, що передбачала

впровадження спеціального навчального модуля з питань захисту даних та кібербезпеки, використання спеціалізованого програмного забезпечення захисту даних, виконання лабораторних робіт, кейс-завдань, проєктної діяльності та рефлексивного аналізу результатів навчання. Освітній процес у цій групі був спрямований на комплексне формування когнітивного, діяльнісного, мотиваційного та рефлексивного компонентів готовності до професійної діяльності у сфері захисту даних.

Таблиця 3.1

Розподіл учасників педагогічного експерименту за контрольними та експериментальними групами

Група	Кількість студентів	Особливості організації підготовки
Експериментальна група (ЕГ)	64	Підготовка здійснювалася за розробленою методикою формування готовності до застосування програмного забезпечення захисту даних
Контрольна група (КГ)	58	Підготовка здійснювалася відповідно до чинної освітньо-професійної програми та традиційної методики навчання
Разом	**122**	**–**

Контрольну групу становили 58 студентів, підготовка яких здійснювалася відповідно до чинних освітніх програм і традиційної методики навчання без цілеспрямованого впровадження спеціально розробленого навчального модуля. Здобувачі освіти контрольної групи опановували зміст навчальних дисциплін у межах передбачених освітньо-професійною програмою компонентів, що дозволило використовувати результати їхньої підготовки як базу для порівняльного аналізу ефективності запропонованої методики.

Формування експериментальної та контрольної груп здійснювалося з урахуванням принципу порівнюваності за основними характеристиками: рівнем попередньої підготовки, академічною успішністю, віком та змістом професійного навчання. Це забезпечило можливість об’єктивного порівняння результатів констатувального та формувального етапів експерименту й

підвищило достовірність висновків щодо впливу запропонованої методики на рівень сформованості готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних.

Педагогічний експеримент проводився у три етапи: діагностичний, формувальний та контрольний. Тривалість експерименту становила від чотирьох до шести тижнів та охоплювала вісім-десять навчальних занять тривалістю 80 хвилин кожне.

На діагностичному етапі здійснювалося визначення вихідного рівня готовності студентів до застосування програмного забезпечення захисту даних. Для збору емпіричних даних використовувалися анкети самооцінювання (додаток А) та тестові завдання (додаток Д). Анкетування було спрямоване на виявлення особливостей цифрової поведінки студентів, рівня використання засобів захисту інформації, обізнаності щодо загроз інформаційній безпеці та ставлення до проблем захисту персональних даних. Тестові завдання дозволяли оцінити рівень знань з основ кібербезпеки, принципів захисту інформації, використання захищених протоколів передавання даних та розпізнавання типових кіберзагроз. Результати початкового діагностування засвідчили переважання низького та середнього рівнів готовності, що підтвердило необхідність цілеспрямованого формування відповідних компетентностей.

Формувальний етап передбачав реалізацію авторської методики підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних. Заняття будувалися на поєднанні теоретичної підготовки, практичної діяльності та рефлексивного аналізу результатів навчання.

На початковому етапі студенти ознайомлювалися з нормативно-правовими засадами захисту персональних даних, аналізували законодавчі вимоги та розглядали реальні випадки витоку інформації в освітній і професійній сферах. Використання кейс-методу забезпечувало формування навичок аналізу проблемних ситуацій та прийняття обґрунтованих рішень щодо запобігання інформаційним ризикам.

Наступним етапом формувального експерименту стало проведення лабораторного заняття, спрямованого на опанування можливостей програмного забезпечення Wireshark для моніторингу, аналізу та інтерпретації мережевого трафіку. У процесі виконання лабораторних завдань здобувачі освіти здійснювали захоплення та дослідження мережевих пакетів, аналізували DNS-запити, файли cookie, HTTP-заголовки та інші елементи мережевої взаємодії. Практична робота дозволила наочно продемонструвати механізми передавання даних у комп'ютерних мережах, виявити потенційні ризики несанкціонованого доступу до інформації та усвідомити загрози, пов'язані з використанням незахищених каналів зв'язку.

Важливе місце у структурі формувального експерименту посідало вивчення засобів криптографічного захисту даних із використанням програмного забезпечення VeraCrypt. Під час виконання лабораторних робіт студенти створювали зашифровані контейнери, аналізували надійність паролів та розробляли рекомендації щодо захисту конфіденційної інформації в освітньому та професійному середовищі.

Для формування навичок захисту комп'ютерних мереж використовувалося програмне середовище Cisco Packet Tracer. Студенти моделювали локальні мережі, налаштовували механізми автентифікації та контролю доступу, створювали правила фільтрації трафіку та розробляли інструкції щодо забезпечення безпеки мережевої інфраструктури закладів освіти.

Завершальний етап формувальної роботи передбачав інтеграцію отриманих знань і навичок у професійний контекст діяльності майбутнього педагога цифрових технологій. Студенти виконували групові проєкти, пов'язані з розробленням політики інформаційної безпеки закладу освіти, створенням інструкцій з кібергігієни та рекомендацій щодо захисту персональних даних учасників освітнього процесу.

На контрольному етапі було проведено повторне тестування та анкетування студентів із використанням тих самих діагностичних інструментів, що застосовувалися на початку дослідження. Крім того, здобувачам освіти

пропонувалося виконати практичне завдання щодо розроблення рекомендацій з кібергігієни для майбутньої професійної діяльності.

Аналіз результатів експерименту здійснювався шляхом порівняння показників контрольної та експериментальної груп до і після впровадження методики. Оцінювалися зміни рівня знань, практичних вмінь, мотивації та готовності до застосування програмного забезпечення захисту даних. Додатково проводився якісний аналіз рефлексивних матеріалів студентів, створених інструкцій, рекомендацій та навчальних розробок.

Передбачалося, що впровадження розробленої методики забезпечить суттєве зростання рівня сформованості когнітивного, діяльнісного, мотиваційного та рефлексивного компонентів готовності студентів до застосування програмного забезпечення захисту даних, сприятиме розвитку навичок кібергігієни та формуванню відповідального ставлення до забезпечення інформаційної безпеки в професійній діяльності.

Для забезпечення об’єктивності та достовірності результатів дослідження використовувалися методи математичної статистики, які дозволили здійснити кількісний аналіз отриманих даних і перевірити статистичну значущість виявлених змін. Результати педагогічного експерименту стали підставою для висновків щодо ефективності розробленої методики підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних.

Організація педагогічного експерименту забезпечила комплексну перевірку всіх компонентів запропонованої методики та дозволила отримати об’єктивні дані щодо результативності впровадження розроблених педагогічних умов у процес професійної підготовки майбутніх фахівців цифрових технологій.

3.2. Критерії, показники та рівні сформованості готовності до застосування програмного забезпечення захисту даних

Метою аналізу результатів педагогічного експерименту було визначення ефективності розробленої методики підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних та перевірка впливу запропонованих педагогічних умов на рівень сформованості їхньої готовності до професійної діяльності у сфері інформаційної безпеки.

Оцінювання результатів експериментальної роботи здійснювалося відповідно до визначених у дослідженні критеріїв і показників готовності (додаток Б), що охоплювали мотиваційний, когнітивний, діяльнісний та рефлексивний компоненти. Для визначення рівня сформованості готовності використовувалися результати анкетування, тестування, виконання лабораторних і практичних робіт, аналізу проєктних завдань та електронного портфоліо здобувачів освіти.

На констатувальному етапі експерименту було встановлено, що рівні сформованості готовності здобувачів освіти контрольної та експериментальної груп суттєво не відрізнялися. Більшість учасників дослідження продемонстрували середній та низький рівні готовності до застосування програмного забезпечення захисту даних. Отримані результати підтвердили необхідність удосконалення професійної підготовки майбутніх фахівців цифрових технологій шляхом упровадження спеціально розробленої методики.

Після завершення формувального етапу було проведено повторну діагностику рівня сформованості готовності здобувачів освіти контрольної та експериментальної груп. Порівняльний аналіз результатів показав позитивну динаміку в обох групах, однак зміни в експериментальній групі виявилися значно більш вираженими.

Результати дослідження засвідчили, що в експериментальній групі суттєво зросла кількість здобувачів освіти з високим та достатнім рівнями готовності до застосування програмного забезпечення захисту даних. Одночасно

спостерігалося значне зменшення кількості студентів із низьким рівнем сформованості відповідних компетентностей. У контрольній групі також відбулося певне покращення результатів, однак воно було зумовлене переважно природним впливом освітнього процесу та не досягло показників експериментальної групи.

Динаміка змін рівнів сформованості готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних наведено в таблиці 3.2.

Таблиця 3.2

Динаміка рівнів сформованості готовності здобувачів освіти до застосування програмного забезпечення захисту даних

Рівень	Контрольна група (до)	Контрольна група (після)	Експериментальна група (до)	Експериментальна група (після)
Високий	6	9	7	20
Достатній	14	18	16	27
Середній	27	24	29	14
Низький	11	7	12	3
Разом	**58**	**58**	**64**	**64**

Для наочного представлення змін у рівнях сформованості готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних результати експериментальної групи подано у вигляді діаграми (рис. 3.1).

Як видно з рис. 3.1, результати формувального етапу педагогічного експерименту засвідчили позитивну динаміку змін рівнів готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних. Після впровадження розробленої методики спостерігається суттєве збільшення кількості здобувачів освіти, які досягли високого та достатнього рівнів готовності. Зокрема, кількість студентів експериментальної групи з високим рівнем готовності зросла з 7 до 20 осіб, що свідчить про ефективне формування в них системи професійних знань, практичних вмінь і

навичок використання сучасних засобів захисту даних. Кількість здобувачів освіти з достатнім рівнем готовності також збільшилася – з 16 до 27 осіб, що підтверджує позитивний вплив запропонованої методики на розвиток професійних компетентностей у сфері інформаційної безпеки.

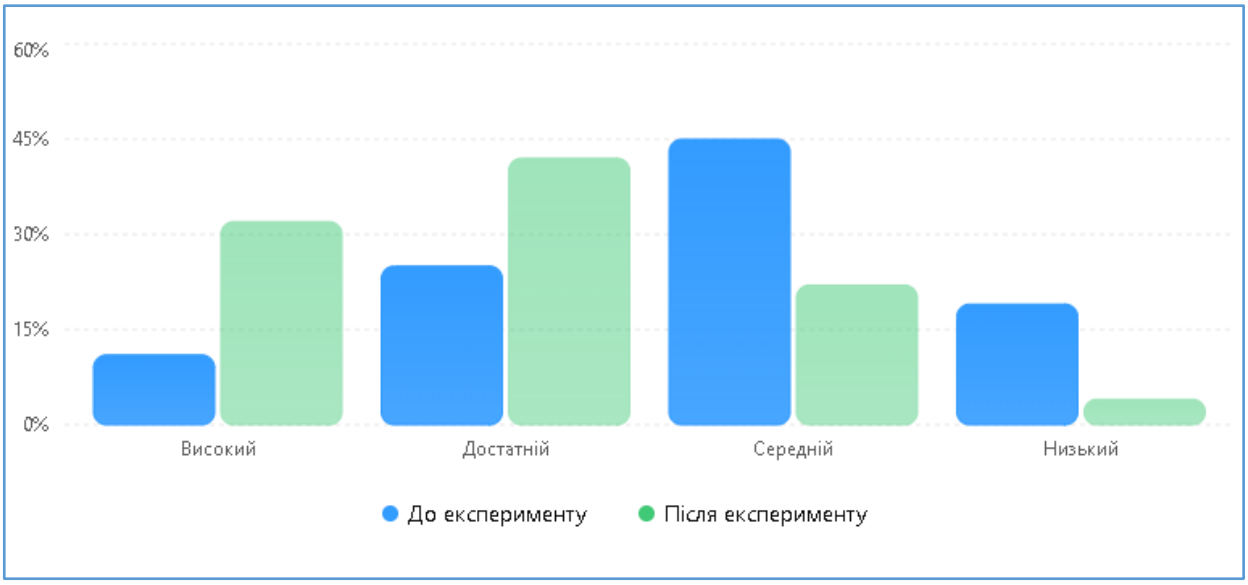

Рис. 3.1 Динаміка рівнів готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних в експериментальній групі до та після експерименту

Водночас зафіксовано зменшення кількості студентів, які перебували на середньому та низькому рівнях готовності. Так, чисельність здобувачів освіти із середнім рівнем знизилася з 29 до 14 осіб, а з низьким рівнем – з 12 до 3 осіб. Отримані результати свідчать про поступовий перехід значної частини студентів до вищих рівнів сформованості готовності, що характеризуються здатністю не лише володіти теоретичними знаннями щодо захисту даних, але й ефективно застосовувати відповідне програмне забезпечення у практичній діяльності, аналізувати кіберзагрози та приймати обґрунтовані рішення щодо забезпечення інформаційної безпеки.

Для порівняння, у контрольній групі зміни були менш вираженими: кількість студентів із високим рівнем готовності збільшилася з 6 до 9 осіб, із достатнім рівнем – з 14 до 18 осіб, тоді як чисельність здобувачів освіти із

середнім рівнем зменшилася з 27 до 24 осіб, а з низьким рівнем – з 11 до 7 осіб. Це свідчить про наявність певних позитивних змін унаслідок традиційного освітнього процесу, однак їх інтенсивність є значно нижчою порівняно з результатами, отриманими в експериментальній групі, де було реалізовано авторську методику формування готовності до застосування програмного забезпечення захисту даних

Як свідчать наведені дані, в експериментальній групі частка здобувачів освіти з високим рівнем готовності зросла майже втричі, а кількість студентів із низьким рівнем зменшилася більш ніж у чотири рази. Такі результати підтверджують позитивний вплив розробленої методики на формування готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних.

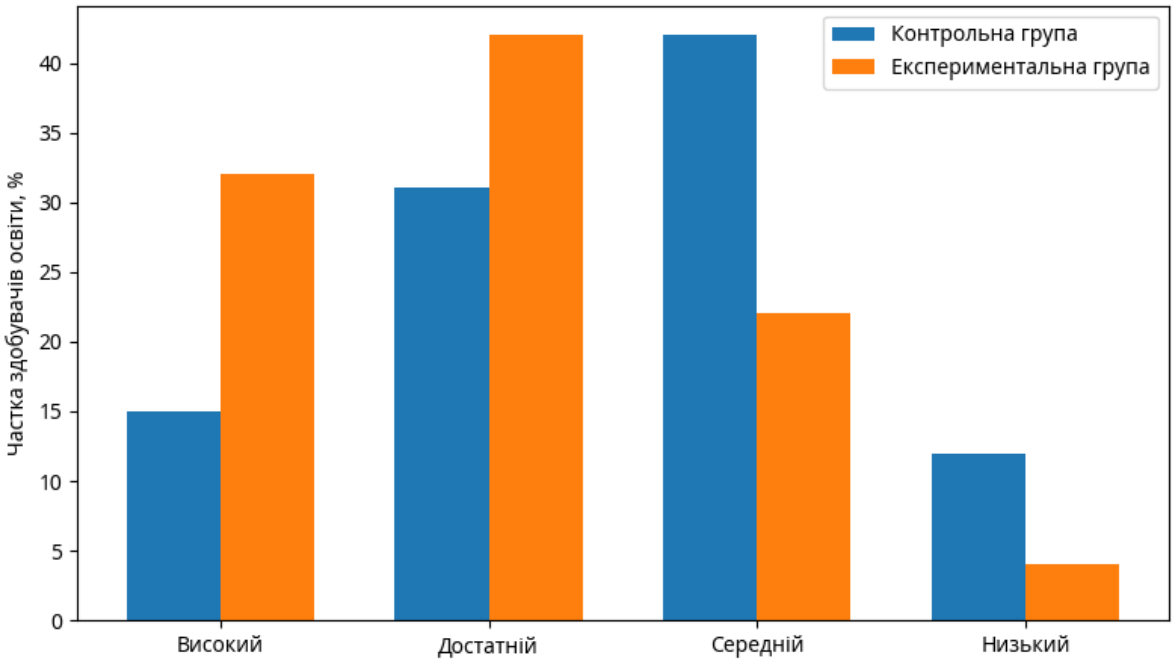

Рис. 3.2 Порівняння рівнів готовності контрольної та експериментальної груп після завершення педагогічного експерименту

Аналіз результатів, наведених на рисунку 3.2, свідчить про вищу ефективність запропонованої методики підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних порівняно

з традиційною організацією навчання. Після завершення педагогічного експерименту в експериментальній групі спостерігається суттєве переважання здобувачів освіти з високим та достатнім рівнями готовності. Зокрема, частка студентів із високим рівнем готовності становить 32 %, що більш ніж удвічі перевищує відповідний показник контрольної групи (15 %). Аналогічна тенденція спостерігається і щодо достатнього рівня готовності, який в експериментальній групі досяг 42 %, тоді як у контрольній групі – 31 %.

Водночас кількість здобувачів освіти із середнім та низьким рівнями готовності в експериментальній групі є значно меншою порівняно з контрольною. Частка студентів із середнім рівнем становить 22 % проти 42 % у контрольній групі, а з низьким рівнем – лише 4 % проти 12 %. Отримані результати підтверджують позитивний вплив упроваджених педагогічних умов, сучасних форм і методів навчання, використання спеціалізованого програмного забезпечення захисту даних, віртуальних лабораторій та проєктної діяльності на формування готовності майбутніх фахівців цифрових технологій до професійної діяльності у сфері захисту інформації.

Аналіз результатів за окремими компонентами готовності також підтвердив ефективність запропонованих педагогічних умов. Найбільші позитивні зміни були зафіксовані за діяльнісним і когнітивним компонентами, що пояснюється широким використанням спеціалізованого програмного забезпечення, віртуальних лабораторій, проєктної діяльності та кейс-методу під час реалізації методики.

Зростання показників когнітивного компонента свідчить про покращення рівня знань здобувачів освіти щодо нормативно-правових засад захисту даних, сучасних кіберзагроз, принципів інформаційної безпеки та функціональних можливостей програмного забезпечення захисту даних. Водночас суттєве підвищення показників діяльнісного компонента підтверджує ефективність практико-орієнтованого підходу, який забезпечив формування навичок використання сучасних інструментів кібербезпеки, аналізу мережевого трафіку, налаштування засобів захисту та розроблення навчальних матеріалів.

Позитивна динаміка спостерігалася також за мотиваційним компонентом. Після завершення формувального етапу більшість здобувачів освіти експериментальної групи продемонстрували підвищення інтересу до проблем захисту даних, усвідомлення професійної відповідальності за забезпечення інформаційної безпеки та готовність до поширення знань із кібергігієни серед інших користувачів цифрових технологій.

Значні зміни були зафіксовані й за рефлексивним компонентом. Здобувачі освіти експериментальної групи виявили вищий рівень здатності до самоаналізу, оцінювання результатів власної діяльності та планування подальшого професійного розвитку у сфері кібербезпеки. Це підтверджує доцільність використання рефлексивних завдань, електронного портфоліо та елементів самооцінювання в процесі професійної підготовки.

Таким чином, результати педагогічного експерименту підтвердили ефективність розробленої методики та доцільність реалізації визначених педагогічних умов у процесі професійної підготовки майбутніх фахівців цифрових технологій. Впровадження структурно-функціональної моделі, спеціально розробленого методичного забезпечення, сучасного програмного забезпечення захисту даних, цифрового освітнього середовища та проєктно-дослідницьких технологій навчання забезпечило суттєве підвищення рівня готовності здобувачів освіти до професійної діяльності у сфері захисту інформації та кібербезпеки (додаток Е).

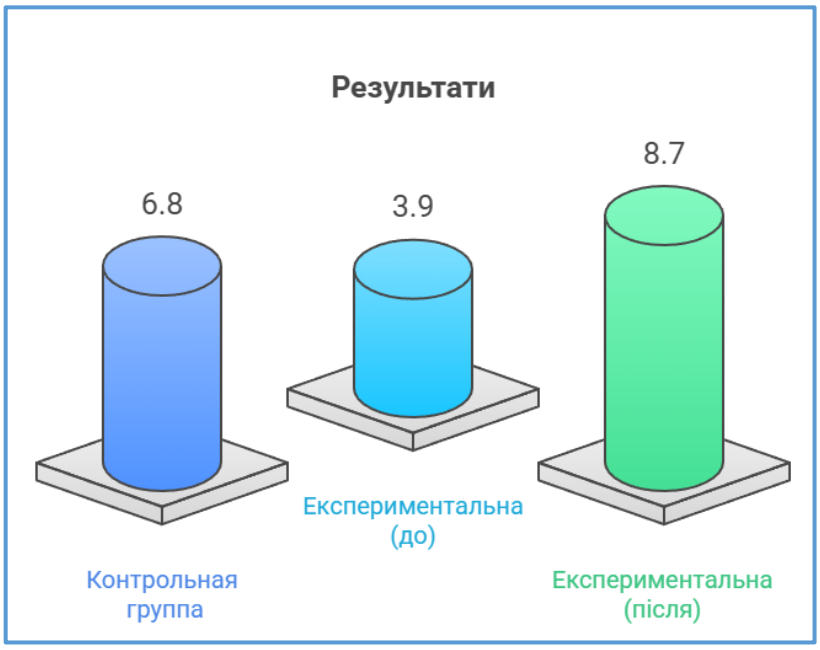

Рис.3.3 Рівні готовності майбутніх педагогів цифрових технологій до застосування програмного забезпечення захисту даних до і після експерименту.

Висновки та рекомендації щодо впровадження методики.

Діагностика рівнів сформованості готовності майбутніх педагогів цифрових технологій до застосування програмного забезпечення захисту даних є ключовим інструментом оцінювання ефективності освітнього процесу. Цей процес спрямований на об'єктивне вимірювання динаміки розвитку професійно-особистісного новоутворення і вимагає чіткого розмежування якісних та кількісних характеристик на кожному етапі підготовки. Відповідно до визначеної структури феномену готовності, оцінювання здійснюється за чотирма базовими рівнями, які відображають ступінь автономності, усвідомленості та професійної майстерності майбутнього викладача.

Інструментарій та процедура діагностики

Для точного визначення приналежності студента до того чи іншого рівня використовується комплексний діагностичний інструментарій, а саме анкета самооцінювання готовності до застосування програмного забезпечення захисту даних та тестові завдання інтегровані у розроблений курс. Оцінювання когнітивного складника здійснюється не через класичне репродуктивне

тестування, а шляхом розв’язання проблемних ситуаційних завдань та аналізу технічних кейсів реальних підприємств. Діяльнісний компонент вимірюється безпосередньо в консолі програмного забезпечення під час виконання комплексних лабораторних робіт у віртуальному середовищі, де критеріями успішності виступають швидкість реагування на інцидент, точність конфігурування фільтрів та обґрунтованість вибору захисних засобів.

Педагогічна та методична складові готовності діагностуються через захист індивідуальних проєктів, які містять розроблені студентами навчально-методичні комплекси, плани-конспекти уроків та інструкції до практичних занять для студентів освітніх закладів. Додатковим інструментом виступає експертне оцінювання під час проходження педагогічної та технологічної практики, де перевіряється здатність майбутнього викладача ефективно взаємодіяти з аудиторією та управляти когнітивним навантаженням здобувачів під час пояснення складних тем. Рефлексивний компонент фіксується через ведення щоденників самооцінювання та участь у фінальних дебатах, що дозволяє відстежити якісні трансформації у професійній самосвідомості майбутнього педагога цифрових технологій.

3.3 Аналіз результатів педагогічного експерименту

Важливим етапом дослідження є аналіз результатів педагогічного експерименту, спрямованого на перевірку ефективності розробленої методики підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних. Оцінювання результативності методики здійснювалося шляхом порівняння показників контрольної та експериментальної груп до та після завершення формувального етапу експерименту.

Особлива увага приділялася визначенню динаміки сформованості готовності студентів за когнітивним, діяльнісним, мотиваційним та рефлексивним компонентами. Для цього використовувалися результати

комплексного оцінювання, отримані за авторською матрицею діагностики готовності до застосування програмного забезпечення захисту даних. Аналіз проводився як за загальним сумарним балом, так і за рівнями готовності, що дозволило встановити характер змін, які відбулися під впливом запропонованої методики.

Особливе значення становлять результати студентів, які після завершення навчання досягли високого або близького до високого рівня готовності. До цієї категорії належать здобувачі освіти, які набрали від 21 до 24 балів із максимально можливих 24 балів, приклад інших результатів здобувачів наведено в таблиці 3.3 та в додатку Е. Саме зазначений показник відображає сформованість системних знань у сфері захисту даних, здатність застосовувати спеціалізоване програмне забезпечення в практичній діяльності, усвідомлення важливості дотримання вимог інформаційної безпеки та готовність до подальшого професійного саморозвитку.

Порівняння результатів контрольної та експериментальної груп дозволяє оцінити ефективність впровадження запропонованої методики та визначити її вплив на підвищення рівня готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних. Виявлені відмінності між групами характеризують особливості формування професійних компетентностей та відображають результативність використання лабораторних робіт, кейс-методу, проєктного навчання, кіберполігонів і віртуальних лабораторій у процесі професійної підготовки.

Емпіричні дані, отримані в ході педагогічного експерименту, дозволяють сформулювати узагальнену інтерпретацію результатів упровадження розробленої методичної системи підготовки майбутніх фахівців цифрових технологій. Фінальний зріз продемонстрував переконливу позитивну динаміку за всіма досліджуваними показниками, підтвердивши високу ефективність синергетичного поєднання інженерно-технічної та дидактичної складових навчання.

Таблиця 3.3

Приклад прогресу студента до і після проведення педагогічного експерименту

№	Компонент	Показник	До експерименту	Після експерименту	Приріст
1	Когнітивний	Знання нормативної бази та принципів захисту даних	2	3	+1
2	Когнітивний	Знання інструментів ПЗЗД	1	3	+2
3	Діяльнісний	Самостійне застосування інструментів	1	3	+2
4	Діяльнісний	Розробка навчальних матеріалів з теми	2	3	+1
5	Мотиваційний	Усвідомлення відповідальності та етичне ставлення	2	3	+1
6	Мотиваційний	Мотивація навчати інших	2	3	+1
7	Рефлексивний	Здатність до самоаналізу та рефлексії	2	3	+1
8	Рефлексивний	Готовність до самоосвіти	2	2	0
Загальна сума			**14**	**23**	**+9**

Головним кількісним індикатором успішності методики став той факт, що абсолютно всі студенти експериментальної групи за результатами підсумкового оцінювання досягли показників, які відповідають рівням вище середнього та творчо-прогностичного з набором від двадцяти однієї до двадцяти чотирьох можливих балів. Такий однорідний високий результат свідчить про універсальність інклюзивного освітнього середовища, створеного в межах експерименту, де кожен здобувач отримав достатній простір для індивідуального розвитку професійних навичок. При цьому середній індивідуальний приріст

зафіксовано в діапазоні від семи до дев'яти балів, що є надзвичайно вагомим показником, враховуючи відносно стислий часовий проміжок формувального етапу, який тривав від шести до восьми тижнів інтенсивних занять.

Якісний аналіз структурних змін у профілі готовності студентів виявив нерівномірність розвитку окремих її компонентів, що має глибоке психолого-педагогічне обґрунтування. Найбільш стрімкий і виражений прогрес було зафіксовано в межах діяльнісного та мотиваційного складників підготовки. Саме в цих зонах інтерактивний інструментарій навчання, що включав наскрізні лабораторні роботи у віртуальних лабораторіях, вирішення реальних кейсів та самостійне проєктування дидактичних матеріалів, дав найшвидший кумулятивний ефект. Безпосереднє занурення в інженерну практику та моделювання професійних ситуацій дозволили студентам оперативно подолати когнітивний бар'єр перед складним захисним софтом, що одночасно викликало сильний внутрішній відгук і різко підвищило мотивацію до майбутньої педагогічної діяльності.

На противагу цьому, показники рефлексивного компонента, який відповідає за самоаналіз та довгострокову готовність до безперервної самоосвіти, демонстрували значно повільніші темпи зростання. Така тенденція є цілком закономірною для освітнього процесу, оскільки рефлексивна позиція та навички прогностичного мислення належать до глибинних особистісних новоутворень. Вони формуються не стільки через інтенсивне освоєння технологічних алгоритмів, скільки через тривалу зміну когнітивних звичок та накопичення різнопланового досвіду, включаючи досвід подолання помилок. Повільний приріст у цій площині вказує на те, що рефлексивний компонент вимагає тривалого педагогічного супроводу, систематичної підтримки та регулярного інтегрування елементів самооцінювання у структуру всіх наступних дисциплін професійного циклу, виходячи за межі короткострокових експериментальних модулів.

3.4. Статистична обробка результатів дослідження та інтерпретація даних

Для перевірки ефективності розробленої методики підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних було здійснено педагогічний експеримент за схемою «до–після» з використанням контрольної та експериментальної груп. Такий дизайн дослідження дозволив визначити динаміку змін рівня готовності здобувачів освіти та оцінити вплив запропонованої методики на формування відповідних професійних компетентностей.

У педагогічному експерименті взяли участь 122 студентів спеціальності 015 Професійна освіта, спеціалізації 015.39 Цифрові технології, які були розподілені на дві групи. До експериментальної групи увійшли 64 студентів, які навчалися за розробленою методикою із застосуванням спеціально створеного навчального модуля з питань захисту даних та кібербезпеки. Контрольну групу становили 58 студентів, підготовка яких здійснювалася відповідно до чинної освітньої програми без використання додаткових методичних компонентів.

Для визначення рівня готовності студентів до застосування програмного забезпечення захисту даних було використано комплексний діагностичний інструментарій, основу якого становила анкета самооцінювання готовності до застосування програмного забезпечення захисту даних.

Критерії оцінювання готовності до застосування ПЗ захисту даних охоплюють чотири структурні компоненти готовності: когнітивний, діяльнісний, мотиваційний та рефлексивний. Кожен компонент характеризувався двома ключовими показниками, які оцінювалися за чотирирівневою шкалою. Максимально можливий результат становив 24 бали.

Когнітивний компонент передбачав оцінювання рівня знань студентів щодо нормативно-правових засад захисту даних, принципів інформаційної безпеки та функціональних можливостей програмного забезпечення захисту даних. Діяльнісний компонент характеризував сформованість практичних вмінь

щодо використання спеціалізованих програмних засобів, аналізу мережевого трафіку, налаштування механізмів захисту та розроблення навчально-методичних матеріалів. Мотиваційний компонент відображав ставлення студентів до питань інформаційної безпеки, усвідомлення професійної відповідальності та готовність до поширення знань із кібергігієни. Рефлексивний компонент характеризував здатність до самоаналізу, оцінювання власного рівня підготовки та готовність до безперервного професійного розвитку.

Діагностування рівня готовності здійснювалося двічі: на початку експерименту (вхідне тестування) та після завершення формувального етапу (підсумкове тестування). Такий підхід забезпечив можливість порівняння початкових і кінцевих результатів, а також визначення індивідуальної та групової динаміки розвитку професійних компетентностей.

Отримані результати було переведено в кількісні показники шляхом підрахунку сумарного балу за всіма критеріями оцінювання. Для інтерпретації результатів використовувалася така шкала рівнів готовності: низький рівень – від 0 до 7 балів, середній рівень – від 8 до 12 балів, достатній рівень від 13 до 18 та високий рівень – від 19 до 24 балів. Запропонована шкала дозволила не лише визначити загальний рівень готовності студентів, але й простежити зміни в структурі сформованості окремих компонентів готовності.

Оскільки результати оцінювання були представлені у вигляді порядкових даних, отриманих за чотирирівневою шкалою, а також сумарних балів, для їх статистичної обробки використовувалися непараметричні методи аналізу (табл. 3.4). Такий підхід забезпечив коректність інтерпретації результатів педагогічного експерименту та дозволив об’єктивно оцінити ефективність запропонованої методики підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних.

Таким чином, обраний інструментарій дослідження забезпечив комплексне оцінювання рівня готовності студентів за всіма структурними компонентами та створив підґрунтя для подальшого статистичного аналізу результатів педагогічного експерименту.

Таблиця 3.4

Методи обробки результатів експерименту

Етап обробки	Метод / статистичний критерій	Мета обробки
Описова статистика	Середнє арифметичне (M), медіана (Me), мода, стандартне відхилення (SD), розмах, квартилі	Показати центральну тенденцію та розкид
Порівняння «до–після» в експериментальній групі	критерій знаків Уілкінсона (парний непараметричний) або парний t-критерій	Перевірити значущість змін усередині групи
Порівняння приросту між групами	U-критерій Манна–Уітні для різниць (після – до)	Перевірити, чи більший приріст в експериментальній групі
Розмір ефекту	Вілсон /Манн_Уітні	Показати практичну значущість змін

З метою статистичної перевірки ефективності розробленої методики (табл. 3.5) підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних було проведено аналіз результатів педагогічного експерименту із застосуванням методів математичної статистики описаних в таблиці 3.4. Обробка отриманих даних здійснювалася за допомогою пакета статистичного аналізу з використанням критеріїв, адекватних характеру розподілу досліджуваних показників.

Таблиця 3.5

Статистична перевірки ефективності розробленої методики

Група	Етап	n	M (середнє)	SD	Медіана	Мінімум	Максимум
Експериментальна	До	64	14.8	2.9	15	9	20
Експериментальна	Після	64	22.1	1.8	22.5	18	24
Контрольна	До	58	15.1	3.1	15	8	21
Контрольна	Після	58	16.4	3.0	16	10	22

На першому етапі було перевірено відповідність емпіричних даних нормальному закону розподілу за допомогою критерію Шапіро–Вілка.

$$W = \frac{(sum_{i=1}^{n} a_i x_i)^2}{sum_{i=1}^{n} (x_i - \bar{x})^2} \quad (3.1)$$

Результати аналізу засвідчили, що розподіл сумарного показника готовності як на констатувальному, так і на формувальному етапах експерименту статистично відрізняється від нормального ($p<0,05$). Отримані результати обумовили доцільність використання непараметричних статистичних критеріїв для подальшого аналізу експериментальних даних.

Для визначення однорідності контрольної та експериментальної груп на початку педагогічного експерименту було застосовано U-критерій Манна–Уітні.

$$U = n_1 n_2 + \frac{n_1(n_1+1)}{2} - R_1 \quad (3.2)$$

За результатами аналізу отримано значення U = 1856 при рівні статистичної значущості $p > 0,05$. Оскільки отримане значення p перевищує критичний рівень статистичної значущості 0,05, статистично значущих відмінностей між контрольною та експериментальною групами на констатувальному етапі не виявлено. Це свідчить про їхню початкову однорідність і підтверджує коректність формування контрольної та експериментальної вибірок для проведення педагогічного експерименту. Для оцінювання змін рівня готовності студентів у межах кожної групи до та після впровадження розробленої методики було використано критерій знаків Вілкоксона.

$$W = sum_{i=1}^{n} R_i * sgn(d_i) \quad (3.3)$$

З метою безпосереднього порівняння ефективності підготовки в контрольній та експериментальній групах було проаналізовано показники приросту рівня готовності, які визначалися як різниця між підсумковими та початковими результатами. Середній приріст у експериментальній групі становив +7,3 бала, тоді як у контрольній групі лише +1,3 бала. Для перевірки статистичної значущості відмінностей між контрольною та експериментальною групами після формувального етапу експерименту застосовано U-критерій Манна–Уітні для незалежних вибірок. Обчислення виконувалися у програмному середовищі IBM SPSS Statistics на основі рангового розподілу результатів досліджуваних груп. Отримане значення статистики U та відповідний рівень

статистичної значущості ($p < 0{,}001$) засвідчили наявність статистично значущих відмінностей між групами. Величина ефекту ($r = 0{,}68$) свідчить про практичний вплив запропонованої методики на формування готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних.

Таким чином, результати статистичного аналізу підтверджують ефективність розробленої методики підготовки. Значно вищі показники приросту рівня готовності в експериментальній групі, а також наявність великого ефекту впливу свідчать про доцільність використання запропонованих педагогічних умов, форм, методів і засобів навчання в процесі підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних.

Експериментальна перевірка ефективності розробленої методики підготовки майбутніх педагогів цифрових технологій здійснювалася із залученням вибірки, що охоплювала 122 студентів, розподілених на експериментальну групу в кількості 64 осіб та контрольну групу, яка налічувала 58 здобувачів.

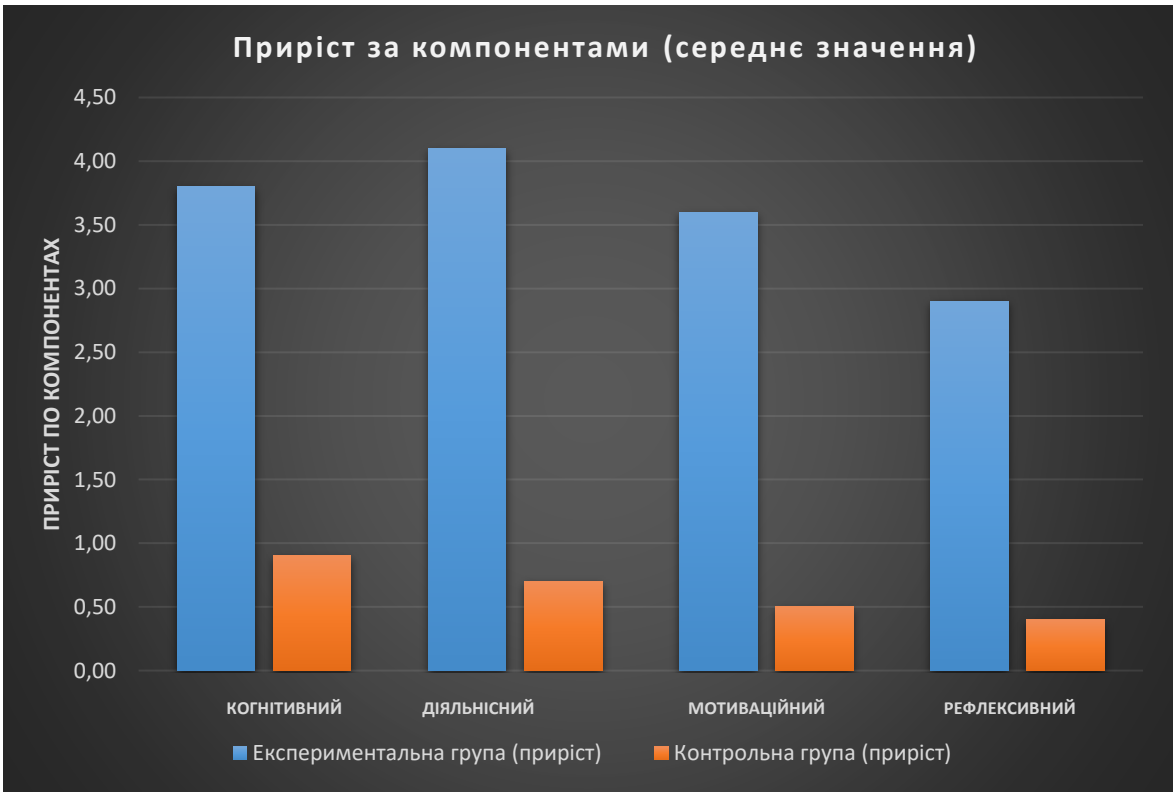

Рис.3.4 Статистичний аналіз розробленої методики

Об'єктивність висновків вимагала попереднього тестування характеру розподілу отриманих первинних даних (табл. 3.6.)

Таблиця 3.6

Приріст за компонентами (середнє значення)

Компонент	**Експериментальна група (приріст)**	**Контрольна група (приріст)**	**Різниця між групами**
Когнітивний	+3.8	+0.9	$p < 0.001$
Діяльнісний	+4.1	+0.7	$p < 0.001$
Мотиваційний	+3.6	+0.5	$p < 0.001$
Рефлексивний	+2.9	+0.4	$p = 0.002$

Оскільки розраховане значення показника виявилося статистично значущим з імовірністю помилки менше п'яти сотих, це чітко вказало на відхилення розподілу від закону нормальності. У поєднанні з порядковою природою шкалювання оцінювання за розробленою матрицею, яка базувалася на восьми критеріях із максимальним сумарним результатом у двадцять чотири бали, зазначений факт зумовив вибір непараметричних методів математичної статистики. Конкретно, для встановлення внутрішніх зв’язків та динаміки змін було застосовано коефіцієнт рангової кореляції Спірмена, що дозволило забезпечити високу точність та математичну коректність інтерпретації емпіричних даних.

Аналіз кількісних показників після завершення формувального етапу експерименту продемонстрував високий рівень статистичної значущості зрушень в експериментальній групі, де ймовірність помилки є надзвичайно низькою і становить менше однієї сотої. Одночасно зафіксовано значний розмір ефекту, який коливається в межах від нуля цілих шести десятих до нуля цілих семи десятих, що свідчить про стабільну та невипадкову дію проведеного педагогічного експерименту. На противагу цьому, у контрольній групі, де навчання відбувалося за традиційною репродуктивною схемою, будь які вагомі

позитивні зміни виявилися мінімальними або статистично не підтвердженими. У практичному вимірі ефективність методики виявилася в переконливому зростанні середнього балу студентів експериментальної групи на 7,3 бали, що зафіксувало якісний стрибок із початкових 14,8 балів до підсумкових 22,1 балів. З погляду педагогічної діагностики це означає повноцінний перехід майбутніх фахівців від базового середнього до стійкого високого рівня готовності до професійної діяльності. Розрахунки доводять, що найбільш виражений прогрес відбувся в межах діяльнісного компонента, де приріст склав 4,1 бали. Такі цифри безпосередньо відображають трансформацію пасивних знань у впевнені практичні навички роботи зі складним програмним забезпеченням, зокрема мережевими аналізаторами WireShark, емуляторами Cisco Packet Tracer, засобами криптографічного захисту інформації VeraCrypt, а також вміння самостійно створювати дидактичні матеріали.

Поряд із кількісними показниками, методика спричинила позитивні зміни у структурі освітньої діяльності та професійної поведінки майбутніх викладачів професійної освіти. Підтвердженням цього є кардинальна зміна ставлення до особистої та корпоративної кібергігієни. Якщо до початку експерименту лише 15% студентів використовували технології двофакторної автентифікації (2FA), то після завершення навчання цей показник зріс до 78% відсотків (рис. 3.5), що вказує на формування стійкої звички захисту облікових записів. Аналогічно, 92% відсотки майбутніх фахівців цифрових технологій зазначили, що перевірка захищених протоколів з’єднання під час взаємодії в інтернет-просторі стала для них автоматичною дією, тоді як на констатувальному етапі це робили лише 28% здобувачів. Важливим досягненням розробленої методики є зсув в аксіологічній сфері здобувачів вищої освіти, адже 85% респондентів експериментальної групи почали усвідомлено сприймати захист даних як невіддільний і критично важливий елемент своєї майбутньої інженерно-педагогічної професії, порівняно з 42% відсотками на початковому етапі. Це свідчить про успішне подолання вузькоспрямованого сприйняття безпеки та формування цілісного розвміння

ролі викладача, як ретранслятора культури безпеки для майбутніх поколінь фахівців цифрових технологій.

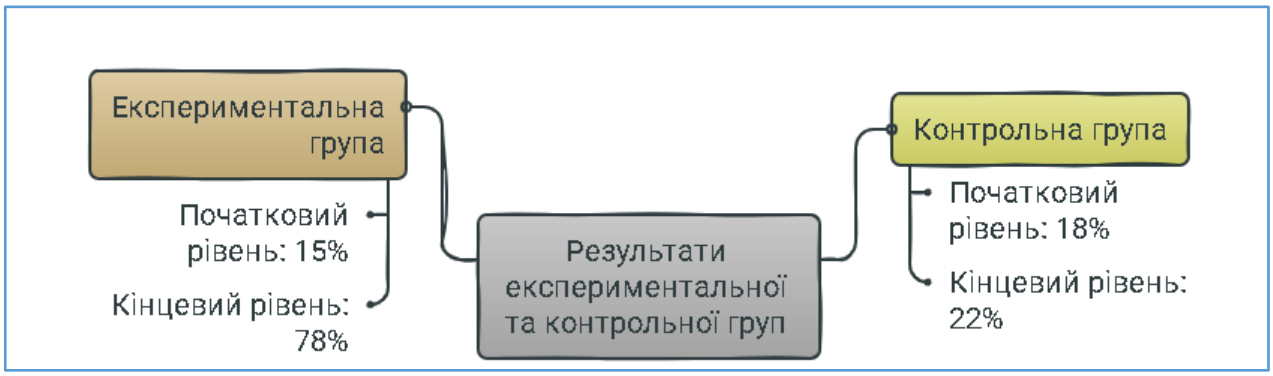

Рис.3.5 Порівняння результатів експериментальної та контрольної групи

Отримані емпіричні результати дають змогу сформулювати концептуальні висновки щодо специфіки підготовки кадрів за спеціальністю 015 Професійна освіта 015.39 Цифрові технології. Доведено, що запропонована методика гармонійно поєднує дослідження, аналіз реальних професійних кейсів, постійну рефлексію та наскрізну проєктну діяльність, що є оптимальною для формування подвійної компетентності здобувача. Особлива цінність методики полягає в тому, що найбільший розвивальний ефект досягається не за рахунок ізольованого вивчення програмного забезпечення захисту даних, а завдяки його поєднанню з педагогічною складовою. Студенти не просто вчилися конфігурувати параметри безпеки для себе, а паралельно розробляли дидактичні матеріали, адаптовані інструкції, наочні презентації та навчальні чек-листи, призначені для здобувачів освіти. Таким чином, процес формування технічних вмінь щодо використання програмного забезпечення захисту даних супроводжувався їх подальшою педагогічною та методичною трансформацією. Кожне практичне завдання, виконане здобувачами освіти із застосуванням спеціалізованих програмних засобів, доповнювалося розробленням відповідних дидактичних матеріалів, методичних рекомендацій, інструкцій або фрагментів навчальних занять. Такий підхід забезпечував не лише набуття професійних компетентностей у сфері захисту даних, але й формування здатності ефективно передавати відповідні знання та практичний досвід іншим.

З огляду на результати проведеного педагогічного експерименту та підтверджену ефективність розробленої методики підготовки майбутніх фахівців спеціальності 015 Професійна освіта, спеціалізації 015.39 Цифрові технології до застосування програмного забезпечення захисту даних, доцільним є формулювання практичних рекомендацій щодо подальшого вдосконалення освітнього процесу в закладах вищої освіти. Реалізація таких рекомендацій сприятиме підвищенню якості професійної підготовки здобувачів освіти відповідно до сучасних вимог цифрової трансформації суспільства та зростання потреб у забезпеченні інформаційної безпеки.

Одним із пріоритетних напрямів удосконалення професійної підготовки є системне впровадження в освітні програми практико-орієнтованого навчання з використанням спеціалізованого програмного забезпечення захисту даних. З цією метою доцільно передбачити в робочих програмах дисциплін «Операційні системи», «Комп’ютерні мережі та захист даних», «Хмарні технології в навчальному процесі» та «Інформаційна безпека» окремий навчальний блок, який охоплюватиме шість-вісім взаємопов’язаних практичних занять. Зміст такого блоку має бути спрямований на формування практичних навичок використання програмних засобів захисту даних шляхом виконання лабораторних робіт, аналізу професійно орієнтованих кейсів, роботи у віртуальних лабораторіях та реалізації наскрізних навчальних проєктів. Особливу увагу доцільно приділяти інтеграції технічної та педагогічної складових підготовки, що забезпечить розвиток не лише професійних вмінь у сфері кібербезпеки, а й здатності майбутніх педагогів здійснювати навчання інших основам захисту інформації та безпечної роботи в цифровому середовищі.

Важливим напрямом подальшого розвитку освітнього процесу є удосконалення системи оцінювання результатів навчання. У ході дослідження була розроблена та апробована *анкета самооцінювання готовності до застосування програмного забезпечення захисту даних*, яка охоплює когнітивний, діяльнісний, мотиваційний та рефлексивний компоненти. Отримані результати свідчать про доцільність її використання не лише як інструменту

наукового дослідження, а й як засобу поточного та підсумкового контролю навчальних досягнень здобувачів освіти. Використання такої матриці дозволяє забезпечити комплексність оцінювання, підвищити об’єктивність визначення рівня сформованості професійних компетентностей та здійснювати систематичний моніторинг індивідуальної освітньої траєкторії здобувачів.

Перспективним напрямом удосконалення професійної підготовки є також розширення використання цифрових освітніх ресурсів, кіберполігонів, симуляторів кіберзагроз та платформ для практичного навчання у сфері кібербезпеки.

Перспективи проведеного дослідження полягають у необхідності подальшої перевірки ефективності запропонованої методики в різних освітніх умовах. Доцільним є проведення аналогічних педагогічних експериментів у закладах вищої освіти різних регіонів України з метою розширення вибірки дослідження та підвищення актуальності отриманих результатів. Це дозволить здійснити додаткову верифікацію розробленої методики, підтвердити її універсальність для підготовки майбутніх фахівців цифрових технологій, а також виявити нові фактори, що впливають на формування готовності до застосування програмного забезпечення захисту даних. Подальші наукові пошуки можуть бути спрямовані на розроблення адаптивних моделей навчання, удосконалення цифрових засобів оцінювання результатів підготовки та дослідження можливостей використання технологій штучного інтелекту в системі професійної підготовки фахівців цифрових технологій.

Перед проведенням статистичної перевірки ефективності розробленої методики доцільно проаналізувати взаємозв’язки між окремими показниками готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних. З цією метою було використано коефіцієнт рангової кореляції Спірмена, який дає змогу визначити силу та напрям зв’язків між когнітивними, діяльнісними, мотиваційними та рефлексивними показниками готовності до застосування програмного

забезпечення захисту даних. Результати проведеного кореляційного аналізу подано в таблиці 3.7.

Позначення рівня значущості:

$$p < 0.05 ** p < 0.01 *** p < 0.001 \quad (3.5)$$

Результати кореляційного аналізу, проведеного за допомогою коефіцієнта рангової кореляції Спірмена, дозволили виявити внутрішні закономірності, взаємозв'язки та структурну динаміку процесу формування готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних. Отримані емпіричні дані підтверджують високу щільність взаємодії між різними компонентами досліджуваної методики та дають змогу з’ясувати причиново-наслідкові механізми функціонування розробленої методики підготовки.

Таблиця 3.7

Кореляційна матриця (Спірмена, ρ)

Компонент / Показник	Когнітивний 1 (нормативна база)	Когнітивний 2 (інструменти)	Діяльнісний 1 (застосування)	Діяльнісний 2 (матеріали)	Мотиваційно-ціннісний 1 (відповідальність)	Мотиваційно-ціннісний 2 (мотивація навчати)	Рефлексивний 1 (самоаналіз)	Рефлексивний 2 (самоосвіта)
Когнітивний	–	0.68*	0.52**	0.47**	0.61***	0.55**	0.42**	0.38*
Когнітивний	0.68**	–	0.81*	0.73***	0.59**	0.64***	0.51**	0.46**
Діяльнісний	0.52**	0.81***	–	0.79*	0.66***	0.71***	0.58**	0.49**
Діяльнісний	0.47**	0.73***	0.79***	–	0.72***	0.84*	0.67***	0.61***
Мотиваційний	0.61***	0.59**	0.66***	0.72***	–	0.78***	0.69***	0.64***
Мотиваційний	0.55**	0.64***	0.71***	0.84***	0.78***	–	0.75*	0.70***
Рефлексивний	0.42**	0.51**	0.58**	0.67***	0.69***	0.75***	–	0.82*
Рефлексивний	0.38*	0.46**	0.49**	0.61***	0.64***	0.70***	0.82***	–

Найбільш виражені, сильні кореляційні зв’язки зафіксовані між кількома ключовими парами показників, де значення коефіцієнта перевищує позначку у 0,8. Зокрема, тісна взаємодія виявлена між першим діяльнісним та другим когнітивним показниками, що становить 0,81 і наочно демонструє, як фундаментальні знання технічних інструментів безпеки безпосередньо конвертуються у стійкі практичні навички їх адміністрування. Ще сильніший зв'язок, що досягає 0,84, спостерігається між другим діяльнісним та другим мотиваційним показниками. Цей факт свідчить про те, що рівень володіння технологіями розробки авторських навчальних матеріалів прямо пропорційно посилює внутрішню мотивацію майбутнього викладача до трансляції цих знань іншим. Також високий ступінь взаємозалежності, що дорівнює 0,82, виявлено між першим та другим рефлексивними показниками, підтверджуючи логічну тезу про те, що розвинена здатність до самоаналізу є основою до безперервної самоосвіти впродовж усього життя.

Групу середньо-сильних зв’язків у діапазоні від 0,07 до 0,79 формують показники, які відображають взаємодію педагогічних та особистісних характеристик здобувачів. Так, зв'язок між другим мотиваційним та першим рефлексивним показниками становить 0,75, вказуючи на те, що прагнення навчати майбутніх фахівців цифрових технологій суттєво залежить від вміння критично оцінювати та аналізувати власні професійні дії. У цьому ж контексті коефіцієнт кореляції між другим діяльнісним та першим рефлексивним показниками, що дорівнює 0,67, підтверджує, що процес самостійного конструювання дидактичних засобів та методичних систем є дієвим чинником розвитку загальної професійної рефлексії студента.

Водночас у ході дослідження було зафіксовано слабші, проте статистично значущі взаємозв’язки у межах від 0,38 до 0,52. Характерним прикладом є кореляція між першим когнітивним та другим рефлексивним показниками, яка становить лише 0,38. Це свідчить про те, що знання нормативно-правової бази та теоретичних аспектів захисту інформації досить слабко корелює з внутрішньою готовністю до самоосвіти, яка більшою мірою визначається стійкими

індивідуально-особистісними рисами студента. Подібну тенденцію демонструє і зв’язок між першим когнітивним та другим діяльнісним показниками, який дорівнює 0,47, підтверджуючи, що сухе знання законодавчих актів чи стандартів безпеки автоматично не трансформується у методичне вміння розробляти якісні навчальні матеріали для здобувачів.

Узагальнення результатів кореляційного аналізу дає підстави для формулювання низки важливих висновків щодо структури та закономірностей формування готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних. Встановлено, що когнітивний і діяльнісний компоненти утворюють основу для дослідження готовності, оскільки характеризуються найбільшою кількістю сильних взаємозв’язків з іншими компонентами. Це свідчить про визначальну роль ґрунтовних теоретичних знань і сформованих практичних вмінь у забезпеченні професійної підготовки майбутнього фахівця цифрових технологій. Отримані результати також підтверджують, що вирішальної умовою професійного розвитку здобувачів освіти є їхня безпосередня практична взаємодія зі спеціалізованими програмними засобами захисту даних, зокрема мережевими аналізаторами, середовищами моделювання комп’ютерних мереж та засобами криптографічного захисту інформації. Саме практико-орієнтована діяльність забезпечує інтеграцію знань, вмінь, ціннісних орієнтацій і рефлексивного досвіду в цілісну систему професійної готовності до майбутньої педагогічної та цифрової діяльності.

Педагогічна складова, виражена у діяльності з розробки навчального контенту, виконує роль своєрідного інтеграційного мосту між практичними навичками та особистісно-мотиваційною сферою здобувача. Чим успішніше майбутній фахівець структурує дидактичні матеріали, тим вищою стає його мотивація до викладання і тим глибшим є процес усвідомлення власної ролі.

Важливе місце у структурі готовності посідає мотиваційний компонент, зокрема прагнення до передачі знань і формування в інших культури безпечної роботи з даними. Високі показники кореляції цього параметра з рефлексивними

характеристиками та професійно-етичними установками свідчать про його системоутворювальну роль у процесі професійного становлення майбутнього педагога цифрових технологій. Водночас встановлено, що готовність до самоосвіти характеризується відносно слабшими зв’язками з теоретичними знаннями, проте демонструє тісну залежність від практичного досвіду застосування програмного забезпечення захисту даних. Це дає підстави стверджувати, що розвиток здатності до безперервного професійного самовдосконалення значною мірою зумовлюється не лише засвоєнням теоретичного матеріалу, а насамперед активним залученням здобувачів освіти до практичної діяльності, розв’язання професійно орієнтованих завдань та осмисленням власного досвіду у сфері захисту інформації.

Практичне впровадження отриманих кореляційних закономірностей у реальний освітній процес вимагає врахування кількох стратегічних орієнтирів. Пріоритетну увагу в робочих програмах необхідно зміщувати у бік виконання практичних завдань, оскільки саме діяльнісний компонент забезпечує максимальний ефект для розвитку всієї особистості майбутнього викладача. Освітні завдання мають обов’язково включати етап створення дидактичних матеріалів, що дозволить ефективно поєднати сформованість професійних технічних компетентностей із внутрішньою мотивацією. Після виконання лабораторного завдання доцільно впроваджувати цілеспрямовану короткочасну рефлексію, що суттєво прискорить розвиток рефлексивного складника підготовки.

Змістовні блоки, присвячені нормативній базі, стандартизації та професійній етиці, не повинні викладатися відірвано від контексту. Їх варто повністю інтегрувати у структуру практичних занять через метод вирішення прикладних кейсів та моделювання загроз, оскільки ізольовані теоретичні знання мають низький рівень конвертації у реальну дієву готовність. Таким чином, результати кореляційного аналізу засвідчили наявність статистично значущих взаємозв'язків між когнітивним, діяльнісним, мотиваційним і рефлексивним компонентами готовності майбутніх фахівців цифрових технологій до

застосування програмного забезпечення захисту даних. Виявлена система кореляційних зв'язків підтверджує внутрішню узгодженість запропонованої структури готовності та свідчить про взаємозалежність її компонентів, що є додатковим аргументом на користь обґрунтованості розробленої моделі підготовки.

Водночас ефективність розробленої методики підтверджено результатами формувального педагогічного експерименту, які засвідчили статистично значуще підвищення рівня готовності майбутніх фахівців спеціальності 015 «Професійна освіта», спеціалізації 015.39 «Цифрові технології» до застосування програмного забезпечення захисту даних у студентів експериментальної групи порівняно з контрольною групою та позитивну динаміку показників за всіма компонентами готовності.

Отримані результати свідчать про доцільність включення запропонованого модуля (3 кредити) до робочих програм дисциплін «Комп’ютерні мережі та захист даних», «Методика професійного навчання» або як окремий вибірковий модуль на 3-4 курсі. Рекомендується масштабувати експеримент на інші ЗВО для отримання більш актуальних даних та подальшого вдосконалення методики.

Таким чином, експериментальна перевірка підтвердила високу ефективність розробленої методики та її відповідність цілям спеціальності 015 Професійна освіта, спеціалізації 015.39 Цифрові технології – підготовці педагога, який не тільки захищає дані сам, а й систематично виховує культуру цифрової безпеки в здобувачів.

Експериментальна перевірка ефективності методики формування готовності студентів спеціальності 015 Професійна освіта, спеціалізації 015.39 Цифрові технології до застосування програмного забезпечення захисту даних дозволила зробити висновки відносно ефективності запропонованої методики.

Аналіз результатів формувального етапу педагогічного експерименту засвідчив суттєве підвищення рівня готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних в умовах професійної діяльності. Зокрема, середнє значення сумарного балу за

розробленою анкетою самооцінювання готовності до застосування програмного забезпечення захисту даних (додаток Б) в експериментальній групі зросло з 14,8 до 22,1 бали із максимально можливих 24 бали. Таким чином, загальний приріст становив 7,3 бали, або 49 %, що свідчить про високу результативність запропонованої методики. Статистична обробка результатів за допомогою критерію Вілкоксона для пов'язаних вибірок підтвердила статистичну значущість виявлених змін ($Z = –4,26$; $p < 0,001$). Розрахований показник розміру ефекту ($r = 0,62$) відповідає великому ефекту, що свідчить про суттєвий вплив упровадженої методики на формування готовності студентів до використання програмного забезпечення захисту даних.

Водночас у контрольній групі також було зафіксовано позитивну динаміку, однак її масштаб виявився значно меншим. Середній приріст сумарного балу становив лише 1,3 бали. Незважаючи на статистичну значущість змін ($p = 0,032$), величина ефекту ($r = 0,32$) відповідає середньому рівню, що свідчить про обмежений вплив традиційної підготовки на формування досліджуваної готовності.

Детальний аналіз компонентної структури готовності показав, що найбільш виражені позитивні зміни відбулися у діяльнісному компоненті. Його середній приріст склав 4,1 бали, що є найвищим показником серед усіх компонентів. Отримані результати можна пояснити активним використанням лабораторних робіт із застосуванням програмних засобів Wireshark, Cisco Packet Tracer та VeraCrypt, а також виконанням практико-орієнтованих проєктних завдань. Саме безпосередня робота зі спеціалізованим програмним забезпеченням сприяла формуванню вмінь аналізувати мережевий трафік, моделювати захищені мережеві середовища, застосовувати засоби шифрування та реалізовувати базові механізми захисту інформації.

Суттєве зростання було також зафіксовано за когнітивним компонентом, приріст якого становив 3,8 бали. Це свідчить про істотне підвищення рівня теоретичної підготовки студентів щодо нормативно-правових засад захисту інформації, сучасних кіберзагроз, принципів інформаційної безпеки та

функціональних можливостей програмного забезпечення захисту даних. Позитивна динаміка підтверджує ефективність оновленого змісту навчання та його відповідність актуальним вимогам цифрового суспільства.

Помітні зміни спостерігалися й у мотиваційному компоненті, середній приріст якого становив 3,6 бали. У результаті впровадження кейс-методу, аналізу реальних кіберзагроз та виконання педагогічно орієнтованих завдань у студентів сформувалося більш усвідомлене ставлення до проблем захисту даних. Значно підвищився рівень особистої відповідальності за дотримання вимог інформаційної безпеки, а також внутрішня мотивація до поширення знань з кібергігієни серед майбутніх фахівців цифрових технологій.

Позитивна динаміка простежувалася і в рефлексивному компоненті, приріст якого становив 2,9 балів. Досягнення таких результатів значною мірою пов’язане із систематичним використанням рефлексивних завдань після виконання лабораторних робіт, аналізом власних дій та оцінюванням рівня сформованості професійних компетентностей. Це сприяло розвитку навичок самоаналізу, самоконтролю та готовності до безперервного професійного самовдосконалення.

Для визначення ефективності запропонованої методики було здійснено порівняння приросту показників експериментальної та контрольної груп. Результати застосування U-критерію Манна–Уітні до різниць між показниками «після експерименту» та «до експерименту» засвідчили статистично значущі відмінності між групами ($U = 42,0$; $p < 0,001$). Значення розміру ефекту $r = 0,68$ відповідає великому ефекту, що підтверджує визначальний вплив спеціально розробленої методики на формування готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних.

Якісний аналіз результатів експерименту також підтвердив позитивні зміни у поведінкових практиках студентів. Після завершення навчання 78 % учасників експериментальної групи почали використовувати двофакторну автентифікацію для захисту власних облікових записів, тоді як на початку дослідження цей показник був суттєво нижчим. Частка студентів, які

систематично перевіряють наявність захищеного з'єднання HTTPS та уникають використання незахищених публічних мереж Wi-Fi для виконання важливих операцій, зросла до 92 % порівняно з 28 % на початку експерименту. Крім того, 85 % студентів почали розглядати захист даних як невід'ємну складову майбутньої професійної діяльності педагога цифрових технологій, тоді як на початковому етапі дослідження такої позиції дотримувалися лише 42 % опитаних. Важливим показником сформованості мотивації до професійного розвитку стало й те, що 67 % студентів самостійно пройшли додаткові онлайн-курси з кібербезпеки та захисту інформації.

Практична значущість отриманих результатів полягає в тому, що середній рівень готовності студентів експериментальної групи фактично перейшов із середнього до високого рівня та досяг значення 22,1 бали із 24 можливих. При цьому студенти не лише підвищили рівень власної цифрової безпеки та професійної компетентності, а й розробили навчально-методичні матеріали (чек-листи, інструкції, пам'ятки, фрагменти занять та конспекти уроків), які можуть бути використані під час педагогічної практики та подальшої професійної діяльності в закладах професійної освіти. Отримані результати підтверджують ефективність розробленої методики та доцільність її впровадження в систему підготовки майбутніх фахівців цифрових технологій.

Розроблена методика (поєднання лабораторних робіт з використанням Wireshark, Cisco Packet Tracer, VeraCrypt, Nmap/Kali Linux, кейс-методу, проєктної діяльності з обов'язковою педагогічною складовою та регулярної рефлексії) є статистично та практично значущою для формування готовності майбутніх фахівців цифрових технологій до застосування засобів захисту даних.

Експеримент довів, що саме інтеграція технічних інструментів з педагогічною практикою (розробка занять, інструкцій, чек-листів для здобувачів) забезпечує не тільки зростання знань і навичок, а й зміну ставлення, мотивації та поведінки.

Отримані результати дозволяють рекомендувати включення аналогічного модуля (3кредитів) до робочих програм дисциплін «Комп'ютерні мережі та

захист даних», «Методика професійного навчання» або як вибірковий курс на 3-4 курсі. Масштабування методики на інші ЗВО та подальше дослідження її довгострокового ефекту (через 1-2 роки після випуску) є перспективним напрямком.

Отже, результати педагогічного експерименту підтвердили висунуту гіпотезу дослідження та засвідчили ефективність розробленої методики підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних. Виявлені статистично та практично значущі зміни свідчать про доцільність її впровадження в систему професійної підготовки здобувачів освіти спеціальності 015.39 «Професійна освіта (Цифрові технології)». Якісний аналіз результатів (рефлексивних звітів, навчальних проєктів, виконаних практичних завдань і створених навчальних матеріалів) засвідчив перехід студентів від пасивного засвоєння навчального матеріалу до проактивної професійної позиції, що виявляється у здатності самостійно аналізувати власну діяльність, оцінювати ефективність використання програмного забезпечення захисту даних і визначати напрями подальшого професійного вдосконалення.

Найбільший приріст зафіксовано за діяльнісним компонентом (+4,1 бала; $p < 0,001$), що пояснюється високою питомою вагою лабораторних робіт, проєктних завдань, використанням спеціалізованого програмного забезпечення, віртуальних лабораторій і кіберполігонів у структурі розробленої методики. Когнітивний (+3,8 бала; $p < 0,001$) і мотиваційний (+3,6 бала; $p < 0,001$) компоненти також продемонстрували статистично значуще зростання. Найменший приріст виявлено за рефлексивним компонентом (+2,9 бала; $p < 0,01$). На нашу думку, така динаміка зумовлена тим, що розвиток професійної рефлексії є тривалим процесом, який потребує систематичного накопичення педагогічного досвіду, багаторазового аналізу власної діяльності та її результатів. Незважаючи на використання у дослідженні рефлексивних звітів, самооцінювання, проєктної діяльності та обговорення результатів виконаних завдань, повноцінне формування рефлексивних умінь потребує більш тривалого

часу, ніж формування знань і практичних навичок. Це свідчить про доцільність подальшого посилення рефлексивної складової методики шляхом розширення використання електронних портфоліо, рефлексивних щоденників, взаємооцінювання, педагогічного коучингу та систематичного аналізу професійних ситуацій.

Запропонована методика є ефективною, статистично значущою та практично значущою для формування комплексної готовності майбутніх педагогів професійної освіти до застосування засобів захисту даних. Вона забезпечує не лише зростання знань і навичок, а й якісну зміну мотивації, етичного ставлення та поведінки, а також формує вміння передавати ці компетентності.

Отримані дані дозволяють рекомендувати впровадження методики (6 кредитів) у робочі програми дисциплін «Комп'ютерні мережі та захист даних», «Методика професійного навчання» або як окремий модуль на 3-4 курсі. Перспективним є подальше масштабування експерименту на інші ЗВО та вивчення довгострокового ефекту (через 1-2 роки після випуску).

Таким чином, дослідження підтверджує доцільність та високу ефективність розробленої методики для підготовки педагогів, здатних виховувати культуру цифрової безпеки в системі професійної освіти України.

Проведене дослідження та експериментальна перевірка дозволяють зробити наступні узагальнені висновки щодо ефективності розробленої методики підготовки студентів спеціальності 015 «Професійна освіта, спеціалізації 015.39 Цифрові технології до застосування програмного забезпечення захисту даних.

Зафіксовано зміни у повсякденній діяльності здобувачів:

– 78 % студентів почали використовувати двофакторну автентифікацію (проти 15 % до експерименту);

– 92 % постійно перевіряють HTTPS та уникають публічних Wi-Fi для важливих дій (проти 28 %);

– 85 % вважають захист даних невід'ємною частиною своєї майбутньої професії педагога (проти 42 %);

– 67 % самостійно пройшли додаткові курси з кібербезпеки після експерименту.

Обов'язкова педагогічна складова (розробка конспектів, інструкцій, чек-листів, пам'яток для здобувачів) виступає зв'язком між технічними навичками та мотивацією. Саме створення навчальних матеріалів для здобувачів забезпечило найвищі кореляції між діяльнісним (ρ=0,84 з мотивацією навчати) та рефлексивним компонентами (ρ=0,67–0,75).

Комбінація лабораторних робіт, кейс-методу, проєктної діяльності, рефлексії та педагогічної орієнтації забезпечує не лише зростання знань і навичок, а й якісну зміну ставлення, мотивації та поведінки, а також формує вміння передавати ці компетентності здобувачам.

Запропоновано включити аналогічний модуль (3 кредити) до робочих програм дисциплін «Комп'ютерні мережі та захист даних», «Методика професійного навчання» або як окремий вибірковий курс (3-4 курси).

Використовувати розроблену анкету самооцінювання готовності до застосування програмного забезпечення захисту даних (8 показників, 24 бали) як інструмент поточного, проміжного та підсумкового контролю.

Проводити дослідження (з періодичністю 1-2 роки) для оцінки довгострокового ефекту методики.

Розроблена методика є ефективним, науково обґрунтованим та практично реалізованим інструментом підготовки майбутніх фахівців цифрових технологій до роботи в умовах цифрової трансформації. Вона дозволяє не тільки підвищити технічну компетентність, а й сформувати відповідального педагога, який свідомо захищає дані в своїй діяльності та систематично виховує культуру цифрової безпеки в здобувачів – ключового елементу сучасної професійної освіти України.

Отримані результати мають теоретичне значення для організації освітнього процесу в закладах вищої та професійної освіти вищої за спеціальністю 015 Професійна освіта, спеціалізації 015.39 Цифрові технології.

Проведене комплексне дослідження нормативно-правового, методичного, психолого-педагогічного та експериментального забезпечення формування готовності майбутніх фахівців спеціальності 015 Професійна освіта, спеціалізації 015.39 Цифрові технології до застосування програмного забезпечення захисту даних дозволило отримати низку теоретичних та практичних висновків.

Отримані результати свідчать, що розроблена методика ефективно впливає не лише на когнітивний і діяльнісний компоненти готовності, а й на мотиваційний компонент, що є одним із найважливіших чинників стійкості сформованої компетентності (рис. 3.6). Зростання мотивації демонструє перехід студентів від формального ставлення до кібербезпеки до усвідомленої та активної позиції щодо захисту даних.

Рис.3.6 Зміна рівня готовності реагування на кіберзагрози

Сформована готовність майбутнього фахівця цифрових технологій до застосування програмного забезпечення захисту даних є багатокомпонентним утворенням, що відображає інтеграцію мотиваційних установок, когнітивних знань, практичних вмінь і рефлексивних здібностей, необхідних для ефективної

професійної діяльності в умовах цифрового освітнього середовища. Водночас для забезпечення об’єктивності її оцінювання та подальшого емпіричного аналізу виникає необхідність у використанні діагностичного інструментарію, що дозволяє комплексно виміряти рівень сформованості відповідних компонентів.

У зв’язку з цим, для визначення рівня сформованості готовності майбутніх педагогів професійного навчання до професійної діяльності в умовах цифрової трансформації освіти було використано анкету самооцінювання, яка містила 20 тверджень, згрупованих за основними компонентами професійної готовності: мотиваційним, когнітивним, діяльнісним та рефлексивним.

Для визначення рівня сформованості готовності майбутніх педагогів професійного навчання до професійної діяльності в умовах цифрової трансформації освіти було використано анкету самооцінювання, яка містила 20 тверджень, згрупованих за основними компонентами професійної готовності: мотиваційним, когнітивним, діяльнісним та рефлексивним. Респондентам пропонувалося оцінити ступінь відповідності кожного твердження власному рівню підготовки за п'ятибальною шкалою, де 1 бал означав повну невідповідність, а 5 балів – повну відповідність. Максимально можлива кількість балів становила 100. Інтерпретація результатів здійснювалася за такими рівнями: високий (85-100 балів), достатній (70-84 бали), середній (50-69 балів) та низький (0-49 балів).

Для визначення рівня готовності майбутніх фахівців цифрових технологій до професійної діяльності було розроблено шкалу оцінювання, що охоплює основні складові професійної готовності: мотиваційно-ціннісну, когнітивну, діяльнісно-практичну та рефлексивну. Шкала містить 20 тверджень, які оцінюються респондентами за п'ятибальною шкалою Лайкерта (від 1 до 5 балів), де вищі значення відповідають вищому рівню сформованості відповідної характеристики. Запропонований інструментарій дає змогу здійснити комплексне оцінювання готовності здобувачів освіти до професійної діяльності в умовах цифрової трансформації освіти та використовується для кількісної інтерпретації результатів педагогічного експерименту (додаток К).

Високий рівень готовності (85-100 балів) характеризує сформованість цілісної системи професійних знань, вмінь, навичок і ціннісних орієнтацій, необхідних для ефективної педагогічної діяльності в галузі цифрових технологій. Студенти цього рівня демонструють стійку професійну мотивацію, усвідомлюють соціальну значущість педагогічної професії, володіють сучасними методиками використання цифрових технологій та програмного забезпечення захисту даних, здатні інтегрувати інформаційно-комунікаційні технології в освітній процес, забезпечувати інформаційну безпеку освітнього середовища, організовувати дистанційне й змішане навчання, а також виявляють готовність до безперервного професійного самовдосконалення.

Достатній рівень готовності (70-84 бали) свідчить про належний рівень сформованості професійної компетентності, достатній для виконання основних професійних функцій. Студенти мають необхідні теоретичні знання та практичні вміння щодо використання цифрових технологій і засобів захисту даних, однак окремі компетентності потребують подальшого розвитку. Вони здатні застосовувати цифрові інструменти у професійній діяльності, хоча в окремих ситуаціях можуть потребувати консультативної підтримки або додаткового методичного супроводу.

Середній рівень готовності (50-69 балів) характеризується частковою сформованістю професійної готовності. Студенти володіють базовими знаннями про цифрові технології та інформаційну безпеку, проте їхні практичні вміння є недостатньо розвиненими для самостійного й ефективного виконання професійних завдань. Використання сучасних цифрових засобів навчання та програмного забезпечення захисту даних має переважно епізодичний характер, а професійна мотивація та готовність до інноваційної діяльності потребують подальшого розвитку.

Низький рівень готовності (0-49 балів) свідчить про недостатню сформованість професійної компетентності та відсутність необхідного рівня підготовки до педагогічної діяльності в цифровому освітньому середовищі. Студенти цього рівня мають фрагментарні знання щодо використання цифрових

технологій, недостатньо володіють сучасними методами організації освітнього процесу, не демонструють впевнених навичок застосування програмного забезпечення захисту даних і потребують комплексної педагогічної підтримки та цілеспрямованого розвитку професійних компетентностей.

Запропонована система інтерпретації результатів дала змогу здійснити комплексне оцінювання рівня готовності майбутніх педагогів професійного навчання до професійної діяльності, визначити динаміку сформованості професійних компетентностей у процесі педагогічного експерименту та об'єктивно оцінити ефективність упровадження авторської методики використання програмного забезпечення захисту даних у професійній підготовці фахівців цифрових технологій.

Таблиця 3.8

Результати приросту рівня готовності (за 100-бальною шкалою)

Група	**До експерименту**	**Після експерименту**	**Приріст (бали)**	**Приріст (%)**
Експериментальна	52,4	87,1	+34,7	+66,2 %
Контрольна	51,8	56,3	+4,5	+8,7 %

Аналіз індивідуальних результатів засвідчив, що після завершення формувального етапу експерименту рівень готовності студентів експериментальної групи до професійної діяльності як фахівців цифрових технологій суттєво зріс (табл. 3.8).

Загальний результат самооцінювання становив 87 балів із 100 можливих, що відповідає високому рівню сформованості професійної готовності. Найвищі оцінки були отримані за показниками, що характеризують усвідомлення соціальної значущості педагогічної професії, мотивацію до професійного саморозвитку, готовність до безперервного вдосконалення компетентностей, знання сучасних методик використання інформаційно-комунікаційних технологій, вміння створювати цифрові навчальні матеріали, організовувати

дистанційне навчання, інтегрувати цифрові технології в освітній процес, а також розвміння принципів інформаційної безпеки й запобігання витоку даних.

Водночас окремі показники були оцінені на рівні чотирьох балів, що свідчить про наявність резервів для подальшого професійного розвитку. Це стосується готовності до впровадження інноваційних цифрових технологій, організації цифрового освітнього середовища, використання інтерактивних методів навчання, здійснення педагогічної взаємодії в онлайн-форматі, формування культури кібергігієни здобувачів освіти, а також практичного застосування спеціалізованого програмного забезпечення захисту даних. Отримані результати підтверджують достатньо високий рівень сформованості як професійно-педагогічних, так і цифрових компетентностей, необхідних для майбутньої професійної діяльності.

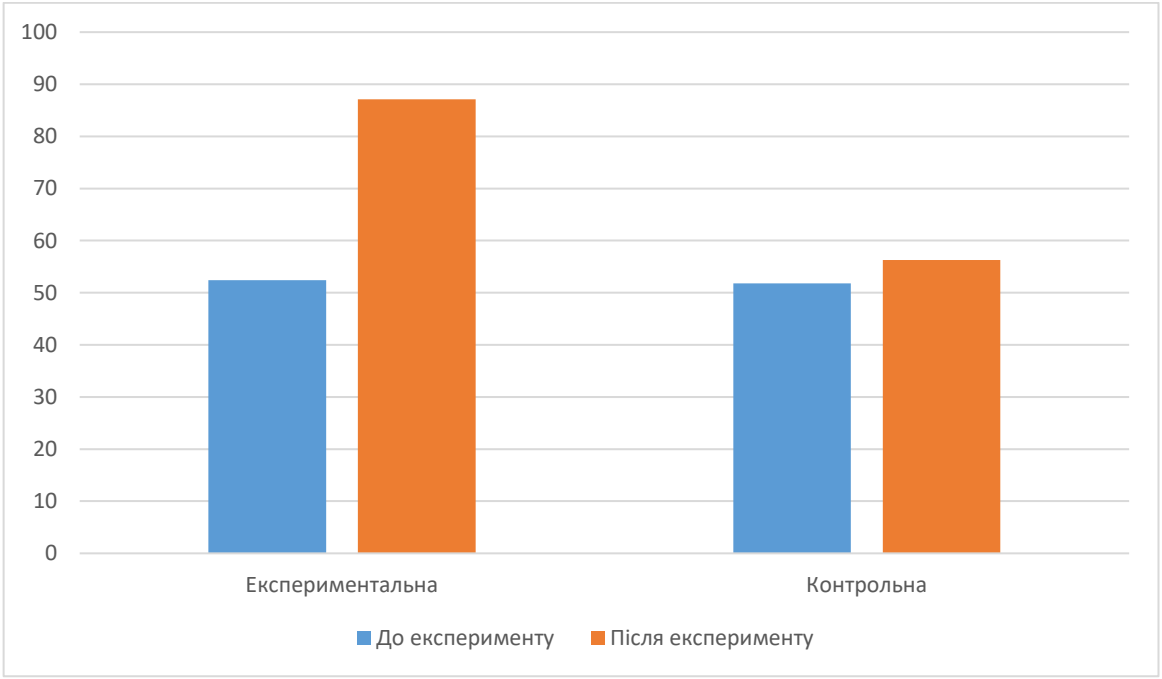

Рис.3.7 Комплексне оцінювання рівня готовності майбутніх фахівців цифрових технологій

Порівняльний аналіз результатів педагогічного експерименту підтвердив позитивну динаміку розвитку готовності студентів експериментальної групи (рис. 3.7). До початку експерименту середній показник готовності становив 52,4

бала, що відповідало середньому рівню сформованості досліджуваної якості. Після впровадження авторської методики цей показник зріс до 87,1 бала, тобто приріст склав 34,7 бала або 66,2 %. Натомість у контрольній групі середній результат змінився лише з 51,8 до 56,3 бала, що відповідає приросту 4,5 бала або 8,7 %.

Порівняння отриманих результатів свідчить, що динаміка розвитку професійної готовності студентів експериментальної групи майже у вісім разів перевищує відповідний показник контрольної групи. Така різниця засвідчує істотний вплив упровадженої методики на формування професійної компетентності майбутніх педагогів цифрових технологій та підтверджує її ефективність.

Особливо важливим є те, що найбільш виражений приріст спостерігався за показниками, пов'язаними з використанням програмного забезпечення захисту даних, розвитком практичних навичок забезпечення інформаційної безпеки, формуванням культури кібергігієни та інтеграцією цифрових технологій у професійну діяльність. Це свідчить про результативність використання розробленої методики, яка поєднувала сучасні цифрові освітні технології, лабораторні роботи, практикоорієнтовані завдання, кейс-метод, проєктну діяльність та роботу із спеціалізованими програмними засобами захисту даних.

Отже, результати самооцінювання та порівняльного аналізу експериментальних даних дають підстави стверджувати, що впровадження авторської методики забезпечило статистично й педагогічно значуще підвищення рівня готовності майбутніх педагогів професійного навчання у сфері цифрових технологій до використання програмного забезпечення захисту даних у професійній діяльності. Отримані результати підтверджують досягнення поставленої мети дослідження та доводять ефективність запропонованої методичної системи професійної підготовки.

Висновки до розділу 3

У третьому розділі дисертаційного дослідження здійснено експериментальну перевірку ефективності розробленої методики підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних. Визначено організаційні засади проведення педагогічного експерименту, обґрунтовано діагностичний інструментарій оцінювання рівня сформованості готовності та здійснено кількісний і якісний аналіз отриманих результатів.

Педагогічний експеримент проводився на базі Тернопільського національного педагогічного університету імені Володимира Гнатюка та Рівненського державного гуманітарного університету. У дослідженні взяли участь 122 здобувачі освіти спеціальності 015 Професійна освіта, спеціалізації 015.39 Цифрові технології, з яких 64 студенти становили експериментальну групу, а 58 – контрольну. Організація експерименту передбачала проведення констатувального, формувального та контрольного етапів, що забезпечило можливість комплексного оцінювання динаміки змін рівня готовності студентів до застосування програмного забезпечення захисту даних.

Для оцінювання результатів дослідження розроблено критерії оцінювання готовності до застосування ПЗ захисту даних, що охоплюють когнітивний, діяльнісний, мотиваційний та рефлексивний компоненти готовності. Діагностика здійснювалася на основі анкетування, тестування, оцінювання лабораторних і проєктних робіт, аналізу навчальних матеріалів та електронних портфоліо студентів.

У процесі формувального етапу експерименту реалізовано комплекс навчальних заходів, що включав використання програмного забезпечення Wireshark, Cisco Packet Tracer, VeraCrypt, Nmap, Splunk, виконання лабораторних робіт, аналіз практичних кейсів, проєктну діяльність, роботу у віртуальних лабораторіях і середовищах моделювання кіберзагроз. Важливою особливістю методики стало поєднання технічної підготовки з педагогічною складовою, що

забезпечило формування здатності не лише застосовувати програмні засоби захисту даних у професійній діяльності, а й навчати цьому майбутніх здобувачів освіти.

Результати контрольного етапу експерименту засвідчили суттєве підвищення рівня готовності студентів експериментальної групи. Середній сумарний показник готовності зріс з 14,8 до 22,1 бали із максимально можливих 24 балів, що становить приріст 7,3 бала або 49 %. Найбільш виражені позитивні зміни зафіксовано за діяльнісним, когнітивним та мотиваційним компонентами готовності, що свідчить про ефективність практико-орієнтованого навчання та використання спеціалізованого програмного забезпечення захисту даних.

У експериментальній групі ($n = 64$) встановлено статистично значуще зростання показників готовності до застосування програмного забезпечення захисту даних ($Z = -4,26$; $p < 0,001$). Розмір ефекту становив $r = 0,53$, що відповідно до загальноприйнятих критеріїв інтерпретації свідчить про великий практичний ефект впливу запропонованої методики на результати професійної підготовки майбутніх фахівців цифрових технологій.У контрольній групі ($n = 58$) також зафіксовано статистично значуще підвищення показників готовності ($Z = -2,14$; $p = 0,032$), проте розмір ефекту виявився суттєво меншим і становив $r=0,28$, що відповідає малому практичному ефекту. Це свідчить про позитивний вплив традиційного освітнього процесу на рівень готовності здобувачів освіти, однак інтенсивність цих змін є значно нижчою порівняно з результатами експериментальної групи.

Якісний аналіз результатів дослідження дозволив встановити позитивні зміни у ставленні здобувачів освіти до питань інформаційної безпеки та захисту даних. У студентів експериментальної групи підвищився рівень усвідомлення значущості кібербезпеки у професійній діяльності, зросла мотивація до самоосвіти, використання сучасних засобів захисту інформації та поширення знань з кібергігієни в освітньому середовищі. Результати проєктної діяльності, розроблені методичні матеріали, чек-листи та інструкції підтвердили

сформованість у студентів здатності інтегрувати технічні та педагогічні компетентності у сфері захисту даних.

Таким чином, результати педагогічного експерименту підтвердили ефективність розробленої методики підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних. Отримані результати доводять доцільність упровадження запропонованої методики в систему професійної підготовки майбутніх фахівців цифрових технологій та підтверджують висунуту гіпотезу дослідження щодо можливості суттєвого підвищення рівня їхньої готовності до професійної діяльності у сфері захисту даних шляхом комплексного поєднання сучасних програмних засобів, практико-орієнтованого навчання та педагогічно спрямованої підготовки.

ВИСНОВКИ

У дисертаційному дослідженні запропоновано вирішення актуальної науково-педагогічної проблеми підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних в умовах цифровізації освіти та зростання вимог до забезпечення інформаційної безпеки. Здійснено теоретичне обґрунтування, розробку методики підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних, а також експериментальну перевірку її ефективності в освітньому процесі закладів вищої освіти. Результати проведеного дослідження підтвердили досягнення поставленої мети, виконання визначених завдань та дали підстави для формулювання таких узагальнених висновків:

1. На основі аналізу наукової літератури, нормативно-правових документів та сучасних тенденцій розвитку цифрового суспільства встановлено, що проблема підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних набуває особливої актуальності в умовах зростання кіберзагроз та цифровізації освітнього середовища. Визначено, що сучасний фахівець цифрових технологій повинен володіти не лише технічними компетентностями у сфері інформаційної безпеки, а й здатністю забезпечувати захист інформаційних ресурсів у професійній діяльності. Узагальнення нормативно-правової бази дало змогу визначити ключові вимоги до підготовки майбутніх фахівців у сфері захисту даних, серед яких провідне місце займають дотримання принципів конфіденційності, цілісності та доступності інформації, використання сучасних засобів кіберзахисту та формування культури безпечної роботи з даними.

2. Проведено аналіз сучасного програмного забезпечення захисту даних та особливостей його використання у професійній діяльності майбутніх фахівців цифрових технологій. Встановлено, що найбільший дидактичний потенціал для професійної підготовки мають програмні засоби Wireshark, Cisco Packet Tracer, VeraCrypt, Nmap, Kali Linux, Splunk, TryHackMe та інші сучасні інструменти

кібербезпеки. Обґрунтовано доцільність їх використання в освітньому процесі як засобів формування практичних навичок аналізу мережевого трафіку, моделювання мережевої інфраструктури, виявлення вразливостей, криптографічного захисту інформації, моніторингу подій безпеки та реагування на кіберінциденти. Доведено, що систематичне використання спеціалізованого програмного забезпечення сприяє інтеграції теоретичних знань і практичної діяльності здобувачів освіти.

3. Теоретично обґрунтовано структуру готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних. У процесі дослідження уточнено структуру готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних, до складу якої включено когнітивний, діяльнісний, мотиваційний та рефлексивний компоненти.

Для кожного компонента визначено відповідні критерії, показники та рівні сформованості рівні сформованості готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних, а саме: низький, середній, достатній та високий. Для кожного рівня конкретизовано характерні ознаки розвитку когнітивного, діяльнісного, мотиваційного та рефлексивного компонентів готовності до застосування програмного забезпечення захисту даних. Низький рівень характеризується фрагментарністю знань, недостатнім рівнем практичних вмінь і слабко вираженою готовністю до використання засобів захисту даних; середній – наявністю базових знань і здатністю виконувати типові професійні завдання; достатній – системним застосуванням програмного забезпечення захисту даних у професійній діяльності та сформованою потребою у професійному саморозвитку; високий – творчим і самостійним використанням сучасних засобів кібербезпеки, здатністю розробляти власні методичні рішення та здійснювати освітню діяльність у сфері захисту даних. Запропоновані критерії оцінювання готовності до застосування програмного забезпечення захисту даних стали основою для діагностики результатів педагогічного експерименту та дала змогу об’єктивно оцінити

динаміку формування готовності здобувачів освіти до професійної діяльності в умовах цифрового суспільства.

Розроблено методику підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних, яка передбачає інтегроване використання лабораторних робіт, кейс-методу, проєктного навчання, кіберполігонів і віртуальних лабораторій. Практична реалізація методики здійснювалася з використанням сучасних програмних засобів захисту даних, зокрема Wireshark, Cisco Packet Tracer, VeraCrypt, Kali Linux, Nmap, Splunk та навчальних платформ кібербезпекового спрямування. Особливістю запропонованої методики стало поєднання технічної підготовки із педагогічною складовою, що забезпечувало формування здатності не лише використовувати відповідні програмні засоби у професійній діяльності, а й навчати основам кібергігієни та захисту даних майбутніх здобувачів.

4. Визначено та теоретично обґрунтовано педагогічні умови підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних, реалізація яких забезпечує ефективне формування їхньої готовності до професійної діяльності в умовах цифрової трансформації освіти та зростання вимог до інформаційної безпеки. До таких педагогічних умов віднесено: інтеграцію змісту професійної підготовки із сучасними технологіями захисту даних і вимогами кібербезпеки; забезпечення практико-орієнтованого навчання шляхом використання професійного програмного забезпечення захисту даних; використання цифрового освітнього середовища та засобів моделювання кіберзагроз; реалізацію міждисциплінарної інтеграції у процесі підготовки до застосування програмного забезпечення захисту даних; мотивацію навчально-пізнавальної діяльності здобувачів освіти засобами проєктного та дослідницького навчання. Реалізація визначених педагогічних умов забезпечує формування професійних компетентностей, розвиток практичних умінь застосування програмного забезпечення захисту даних, готовності до розв'язання професійних завдань у сфері інформаційної та кібербезпеки, а також здатності до безперервного професійного саморозвитку.

На основі узагальнення результатів теоретичного аналізу наукових джерел, нормативно-правових документів та сучасних тенденцій розвитку цифрового суспільства обґрунтовано й розроблено структурно-функціональну модель підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних. Запропонована модель являє собою цілісну педагогічну систему, що охоплює методологічний, змістовий, організаційно-процесуальний та результативний блоки та педагогічні умови, які функціонують у взаємозв'язку та забезпечують досягнення поставленої мети дослідження. Методологічний блок ґрунтується на інтеграції компетентнісного, системного, діяльнісного, особистісно орієнтованого, практико-орієнтованого та технологічного підходів, що визначають концептуальні засади професійної підготовки. Змістовий блок передбачає інтеграцію питань інформаційної безпеки, кібербезпеки та використання програмного забезпечення захисту даних у професійно орієнтовані дисципліни. Організаційно-процесуальний блок охоплює форми, методи та засоби навчання, зокрема лабораторні роботи, кейс-метод, проєктне навчання, моделювання кіберзагроз, використання віртуальних лабораторій, кіберполігонів і спеціалізованого програмного забезпечення захисту даних. Результативний блок забезпечує оцінювання рівня сформованості готовності майбутніх фахівців цифрових технологій за когнітивним, діяльнісним, мотиваційним та рефлексивним компонентами відповідно до визначених критеріїв, показників і рівнів. Встановлено, що ефективність реалізації моделі забезпечується комплексом педагогічних умов, серед яких провідне значення мають оновлення змісту професійної підготовки відповідно до сучасних вимог інформаційної безпеки, практико-орієнтоване використання програмного забезпечення захисту даних, міждисциплінарна інтеграція, застосування цифрових освітніх технологій та розвиток рефлексивної й дослідницької діяльності здобувачів освіти.

5. Експериментально перевірено ефективність розробленої методики підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних. Результати педагогічного

експерименту засвідчили статистично значуще підвищення рівня сформованості всіх компонентів готовності студентів експериментальної групи порівняно з контрольною. Встановлено позитивну динаміку переходу здобувачів освіти з низького та середнього рівнів на достатній і високий рівні готовності. Найбільший приріст зафіксовано за діяльнісним, когнітивним та мотиваційним компонентами, що підтверджує ефективність практико-орієнтованого використання спеціалізованого програмного забезпечення захисту даних, лабораторних робіт, кейс-завдань і проєктної діяльності. Результати статистичної обробки експериментальних даних підтвердили достовірність отриманих змін та дозволили зробити висновок про ефективність запропонованої методики підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних.

Експериментальна перевірка розробленої методики підтвердила її ефективність. Установлено статистично значуще підвищення рівня готовності студентів експериментальної групи до застосування програмного забезпечення захисту даних. Середній сумарний бал за матрицею оцінювання зріс з 14,8 до 22,1 бала із максимальних 24 балів, що свідчить про перехід студентів від середнього до високого рівня готовності. Результати статистичного аналізу підтвердили достовірність виявлених змін та засвідчили ефективність розробленої методики і наявність її значущого педагогічного ефекту.

Виявлено, що найбільш суттєві позитивні зміни відбулися в діяльнісному, когнітивному та мотиваційному компонентах готовності. Це свідчить про ефективність практико-орієнтованого навчання, використання реальних кейсів із захисту даних, моделювання кіберінцидентів та виконання проєктних завдань, максимально наближених до умов майбутньої професійної діяльності. Водночас позитивна динаміка рефлексивного компонента підтвердила доцільність систематичного використання рефлексивних методик та інструментів самооцінювання результатів навчання.

Практична значущість результатів дослідження полягає у можливості використання розробленої методики, структурно-функціональної моделі,

системи педагогічних умов, діагностичного інструментарію, навчально-методичних матеріалів, лабораторних робіт, кейсів та проєктних завдань у процесі професійної підготовки здобувачів освіти спеціальності 015 Професійна освіта, спеціалізації 015.39 Цифрові технології. Запропоновані методичні розробки можуть бути використані в закладах вищої освіти для вдосконалення підготовки майбутніх педагогів цифрових технологій до забезпечення інформаційної безпеки та застосування сучасних програмних засобів захисту даних.

Отримані результати підтверджують досягнення мети дослідження, розв’язання поставлених завдань та доводять ефективність розробленої методики підготовки майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних. Перспективи подальших наукових досліджень вбачаються у розробленні адаптивних цифрових курсів з кібербезпеки, удосконаленні системи оцінювання сформованості компетентностей у сфері захисту даних та впровадженні технологій штучного інтелекту в процес професійної підготовки майбутніх фахівців цифрових технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Андрущенко, В. П., Бех, І. Д., Волощук, І. С., та ін. (2008). *Педагогіка вищої школи* (В. Г. Кремень, В. П. Андрущенко, В. І. Луговий, ред.). Педагогічна думка.

Барановська, Л. В., & Заслужена, А. А. (2023). Особистісно зорієнтовані освітні технології в підготовці фахівців соціономічних професій. *Слобожанський науковий вісник. Серія: Філологія*, (3), 118–122. https://doi.org/10.32782/philspu/2023.3.22

Биков, В. (2020). Цифрове навчальне середовище: нові технології та вимоги до здобувачів знань. Сучасні інформаційні технології та інноваційні методики навчання в підготовці фахівців: методологія, теорія, досвід, проблеми, (55), 11–22.

Биков, В. Ю., & Овчарук, О. В. (2017). Оцінювання інформаційно-комунікаційної компетентності студентів та педагогів в умовах євроінтеграційних процесів в освіті. Київ: Педагогічна думка. 160.

Биков, В., Спірін, О., & Пінчук, О. (2020). Сучасні завдання цифрової трансформації освіти. Грамотність у цифрову епоху: журнал кафедри ЮНЕСКО «Неперервна професійна освіта XXI століття», 1, 27–36. https://doi.org/10.35387/ucj

Близнюк, М., & Радько, Я. (2025). Теоретичні основи цифрової компетентності майбутніх викладачів професійної освіти у фаховій підготовці. *Ukrainian Professional Education = Українська професійна освіта*, (17), 60–79. https://doi.org/10.33989/2519-8254.2025.17.342369

Бурячок, В. Л., & Богуш, В. М. (2018). Recommendations for development and implementation of the professional modelcompetences in the sphere of training of specialists for of the national cyber-security system. *Ukrainian Information Security Research Journal*, *20*(2), 72–78. https://doi.org/10.18372/2410-7840.20.12862

Верховна Рада України. (1996). *Конституція України: Закон України від 28.06.1996 № 254к/96-ВР*. https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80

Верховна Рада України. (2003). *Цивільний кодекс України: Закон України від 16.01.2003 № 435-IV*. https://zakon.rada.gov.ua/laws/show/435-15

Верховна Рада України. (2010). *Про захист персональних даних: Закон України № 2297-VI від 01.06.2010*. https://zakon.rada.gov.ua/go/2297-17

Верховна Рада України. (2017). *Закон України "Про основні засади забезпечення кібербезпеки України" № 2163-VIII*. https://zakon.rada.gov.ua/laws/show/2163-19

Верховна Рада України. (2022). *Закон України "Про хмарні послуги"*. https://zakon.rada.gov.ua/laws/show/2075-20

ГО «Прометеус». (2026). *Офіційний вебсайт Prometheus*. https://prometheus.org.ua/

Гуревич, Р., Бойчук, В., Коношевський, Л., Коношевський, О., & Костенко, Н. (2023). Використання інноваційних технологій у навчальному процесі. *Молодь і ринок*, (5/213), 18–23. https://doi.org/10.24919/2308-4634.2023.282829

Державне підприємство «Інфоресурс». (2025). Інформація про діяльність підприємства. https://www.inforesurs.gov.ua/

Золотухіна, С. Т., & Лозова, В. І. (2019). Експеримент у системі педагогічного дослідження. Психолого-педагогічні проблеми вищої і середньої освіти в умовах сучасних викликів: теорія і практика. Матеріали IV Міжнар. наук.-практ. конф., (Харків, 12 груд. 2019 р.). (С. 174–176). Харків. нац. пед. унт ім. Г. С. Сковороди, Харків.

Зубик, Л. (2016). Модель формування професійних компетентностей майбутніх ІТ-фахівців у процесі вивчення фахових дисциплін. Науковий вісник 245 Миколаївського національного університету імені В. О. Сухомлинського. Педагогічні науки, (1), 83–89.

Карплюк, С. (2019). Особливості цифровізації освітнього процесу у вищій школі. Інформаційно-цифровий освітній простір України: трансформаційні процеси і перспективи розвитку (с. 188–197). Київ.

Керекеша-Попова, О. В. (2020). Формування управлінської компетентності майбутніх інженерів-педагогів у процесі професійно-педагогічної підготовки. (Дис. … канд. пед. наук за спеціальністю 13.00.04). Бердянський держ пед. ун-тет. Бердянськ, 317.

Козловський, Ю. М. (2018). Методологія педагогічного дослідження. [Навч. посібник]. Львів: Видавництво Львівської політехніки, 196. Колеснікова, І. В., & Орлова, О. А. (2023).

Криштанович, С. В., & Криштанович, М. Ф. (2023). Педагогічні умови формування педагогічної компетентності майбутніх викладачів у процесі змішаного навчання в закладі вищої освіти . Академічні візії, (25). вилучено із https://www.academy-vision.org/index.php/av/article/view/717

Кулакова, Л., & Онокало, О. (2025). Психологічні особливості готовності фахівців у галузі інформаційних систем і технологій до професійної діяльності. *Науковий часопис НПУ імені М. П. Драгоманова. Серія 12. Психологічні науки,* 113–124. https://doi.org/10.31392/udu-nc.series12.2025.28(73).10

Лапаєнко, С. В. (2023). Теоретико-методологічне забезпечення цифрової трансформації освіти і педагогіки. Інноваційна педагогіка, 55(3), 9–13.

Литвин, А., & Мацейко, О. (2013). Методологічні засади поняття «педагогічні умови». Педагогіка і психологія професійної освіти, (4), 43–63.

Литвиненко О. В., . (2003). Інформаційні впливи та операції: теоретико-аналітичні нариси: монографія. К: Національний ін-т стратегічних досліджень.

Литвинова, С. Г. (2020). Цифрова компетентність сучасного педагога: структура та рівні сформованості. Освітній вимір, (4(68)), 22–30.

Лубко, Д. В., & Мірошниченко, М. Ю. (2024). Механізми безпеки інформації та їх виклики. *Науковий вісник Таврійського державного агротехнологічного університету*, *14*(2). https://doi.org/10.32782/2220-8674-2024-24-2-26

Малежик, П. М. (2020). Теоретичні й методичні засади технічної підготовки майбутніх фахівців з інформаційних технологій. (Дис. д. пед. наук : 13.00.02). Київ: Національний педагогічний університет імені М.П.Драгоманова, 487.

Манойленко, Н. В. (2017). *Діяльнісний підхід у формуванні ключових компетенцій у процесі підготовки вчителів технологій*. Матеріали IV Міжнародної науково-практичної онлайн-інтернет конференції «Проблеми та інновації в природничо-математичній, технологічній і професійній освіті». Центральноукраїнський державний педагогічний університет імені Володимира Винниченка. https://phm.cuspu.edu.ua/ojs/index.php/NZ-PMFMTO/article/view/1215

Міністерство освіти і науки України. (2021). *Стандарт вищої освіти України: перший (бакалаврський) рівень, галузь знань 01 «Освіта / Педагогіка», спеціальність 015 «Професійна освіта (за спеціалізаціями)»*. https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/2021/07/28/015-Profosvita-bakalavr.pdf

Міністерство освіти і науки України. (2021). *Стандарт фахової передвищої освіти освітньо-професійного ступеня «фаховий молодший бакалавр», галузь знань 01 «Освіта / Педагогіка», спеціальність 015 «Професійна освіта (за спеціалізаціями)»*. https://mon.gov.ua

Морзе, Н. (2019). Опис цифрової компетентності педагогічного працівника (проєкт). Відкрите освітнє е-середовище сучасного університету, спецвипуск, 1–53.

Морзе, Н. В., & Варченко-Троценко, Л. О. (2020). Розвиток цифрової компетентності педагогів у системі неперервної освіти. Київ, 350.

Морзе, Н. В., & Овчарук, О. В. (2019). Модель цифрової компетентності вчителя. Інформаційні технології і засоби навчання, 70(2), 15–27.

Морзе, Н., & Буйницька, О. (Ред.) (2021). Модернізація освіти в цифровому вимірі. [Монографія]. Київ: Київ. ун-т ім. Б. Грінченка, 300.

Національна бібліотека України імені В. І. Вернадського. (n.d.). *Наукова електронна бібліотека України (IRBIS-NBUV)*. https://irbis-nbuv.gov.ua/ulib/item/ukr0000025303

Носенко, Ю. Г. (2018). Адаптивні системи навчання: сутність, характеристика, стан використання у вітчизняних закладах педагогічної освіти. Фізикоматематична освіта, 3(17), 73–78.

Олійник, М. (2023). Глобальна проблема цифрової нерівності та її ключові форми. Економіка та суспільство, (57). https://doi.org/10.32782/2524-0072/2023-57-20

Освітні тренди у підготовці майбутніх ІТ-фахівців. Актуальні питання сучасної інформатики, (5), 126–129.

Особливості підготовки студентів ІТспеціальностей до здійснення науково-технічного дослідження. Педагогічна Академія: наукові записки, (10). https://doi.org/10.5281/zenodo.13895015

Петренко, Л. М., Кучерявий, О. Г. & Лавріненко, О. А. (2024). Теоретичні і методичні засади підготовки майбутнього викладача закладу вищої педагогічної освіти до професійної діяльності в умовах цифровізації суспільства : монографія. Київ : Вид-во ТОВ «Юрка Любченка», 246.

Петренко, С. (2023). Проблема професійної підготовки майбутніх ІТ-фахівців у рецепціях вітчизняних науковців останнього десятиріччя. Педагогічна наука і освіта XXI століття, (1), 115–129. Підгорна, Т. В., & Пурський, О. І. (2024).

Побірченко, Н. С. (2012). Компетентнісний підхід у вищій школі: теоретичний аспект. Освіта та педагогічна наука, 3, 24–31

Престижність професійної освіти в Україні (2025): результати досліджень. Міністерство освіти і науки України. (2025, 24 жовтня). Взято з:

https://eo.gov.ua/prestyzhnist-profesiynoi-osvity-v-ukraini-rezultatydoslidzhen/2025/10/24/

Прокопова, О. П., Ляска, О. П. & Голіней, В. (2023). Інноваційна складова у вищій освіті: методо-теоретичні підходи та практична реалізація. Наукові інновації та передові технології, 4 (18), 517–527. DOI: https://doi.org/10.52058/2786-5274-2023-4(18)-517-527

Професійний розвиток педагогів в умовах цифровізації освіти. Інноваційна педагогіка, 64(2). 186-189. https://doi.org/10.32782/2663-6085/2023/64.2.35

Ростока, М. Л., Кравченко, Ю. А. (2024). Феномен штучного інтелекту в системі інформаційно-аналітичного супроводу цифрової трансформації освіти і педагогіки. Науково-педагогічні студії, 8, 282–300. https://doi.org/10.32405/2663-5739-2028-8-283-3002023/64.2.35

Сажко, Г. І. (2021). Цифровізація освітнього процесу підготовки майбутніх інженерів-педагогів: теоретичний аспект. Problems of EngineerPedagogical Education, 5(70), 45–53.

Семенишина, І. В., Кочарян, А. Б., & Савастру, Н. І. (2023). Майбутнє вищої освіти: роль онлайн-курсів та адаптивних підходів. Вісник науки та освіти, 10(16), 807–821. https://doi.org/10.52058/2786-6165-2023-10(16)-807-821

Сисоєва, С. О. (2015).*Назва документа (як у PDF)*. Київський університет імені Бориса Грінченка. https://elibrary.kubg.edu.ua/id/eprint/36043/1/Sysoeva%20S.A.%202015.pdf

Сікора, Я. (2025). Стандартизація іт-освіти на сучасному етапі: порівняльний аспект. *Науковий вісник Ужгородського університету. Серія: «Педагогіка. Соціальна робота»*, (1(52), 195–201. https://doi.org/10.24144/2524-0609.2023.52.195-201

Співаковський, О. В., Осипова, Н. В., & Сніжко, М. В. (2010). *Педагогічний експеримент для перевірки ефективності методичної системи організації алгоритмічного тестування в процесі підготовки майбутніх учителів математики*. Інформаційні технології в освіті, 8, 23–30. https://lib.iitta.gov.ua/id/eprint/438/

Спірін, О., Олексюк, В., Василенко, Я., & Сіренко, О. (2024). A model for the development of digital competence of research and teaching staff. *Information Technologies and Learning Tools, 104*(6), 156–179. https://doi.org/10.33407/itlt.v104i6.5889

Сторонська, О. С. (2023). Принципи побудови сучасного цифрового освітнього середовища. Академічні візії, (27). https://academyvision.org/index.php/av/article/view/779

Тесля, Ю. М., & Заспа, Г. О. (2020). Розробка концентричної інформаційної технології цифрової трансформації закладів вищої освіти. Управління розвитком складних систем, (44), 105–115. https://doi.org/10.32347/2412-9933.2020.44.105-115

Тітова, Л. (2022). Онлайн-засоби формування інформаційно-цифрової компетентності майбутніх педагогів в умовах дистанційного навчання. Multidisciplinární mezinárodní vědecký magazín «Věda a perspektivy», 5(12), 132–143.

Уповноважений Верховної Ради України з прав людини. (2014). *Про затвердження Типового порядку обробки персональних даних* (Order No. 1/02-14, January 8, 2014). Official Bulletin of Ukraine. https://zakon.rada.gov.ua/laws/show/v0001900-14

Уповноважений Верховної Ради України з прав людини. (2021). *Рекомендації щодо захисту персональних даних під час дистанційного надання освітніх послуг*. https://ombudsman.gov.ua/assets/uploads/files/rekomendacii_shchodo_zahistu_personalnikh_danikh_v_osviti.pdf

Харагірло, В. Є. (2018). Сутність і структура готовності до інноваційної діяльності педагогічних працівників закладів професійно-технічної освіти. Професійна освіта, 1 (178), 34–38

Швачич, Г. Г. (2017). Сучасні інформаційно-комунікаційні технології. Дніпро: НМетАУ, 230.

Шевчук, С. С. (2024). Методологічні аспекти компетентнісного підходу до професійної підготовки кваліфікованих фахівців. Імідж сучасного педагога, 1(214), 58–66. https://doi.org/10.33272/2522-9729-2024-1(214)-58-66

Шишенко, І., & Кравченко, І. (2021). Теоретичні аспекти цифрової трансформації професійної підготовки майбутніх фахівців. Науковий вісник Ужгородського університету. Серія «Педагогіка. Соціальна робота», (2(49)), 241–244.

Шишенко, І. (2022). Деякі аспекти впливу цифрових технологій на освітній процес закладів вищої освіти: огляд проблем та викликів. *Education. Innovation. Practice*, *10*(5), 42–47. https://doi.org/10.31110/2616-650x-vol10i5-006

Adaptive Instructional Systems, (2023): Proceedings of the 5th International Conference AIS 2023, held as part of the 25th International Conference on Human-Computer Interaction, (Copenhagen-Denmark, July 23–28, 2023). Berlin : Springer, 250 p

Aikido Security. (n.d.).*Prevent OWASP Top 10 vulnerabilities*. Aikido. https://www.aikido.dev/use-cases/prevent-owasp-top-10-vulnerabilities

Amazon Web Services. (n.d.). *AWS documentation*. https://docs.aws.amazon.com/

Andress, J. (2021). *The Basics of Information Security* (3rd ed.). Syngress.

Baker, R. & Siemens, G. (2023). Personalized learning and adaptive systems: Future perspectives in education. International Review of Research in Open and Distributed Learning, 24(2), 50–67. DOI: https://doi.org/10.1234/irrodl.2023.0024

Basis Technology. (n.d.). *Autopsy digital forensics platform*. https://www.autopsy.com/

Beatty, J. F., Hill, P. L., & Spengler, M. (2024). Sense of purpose and social-emotionalbehavioral skills during university. Personality and Individual Differences. https://doi.org/10.1016/j.paid.2024.112870

Bezymiannyi, O., & Shapoval, N. (2023). Filter for confidential information. *Electronics and Control Systems*, *4*(78), 21–25. https://doi.org/10.18372/1990-5548.78.18256

Brooks, C. J., Grow, C., & Craig, P. (2021). *Cybersecurity Essentials*. Wiley.

Cisco Systems, Inc. (n.d.). *Cisco Networking Academy (NetAcad)*. https://www.cisco.com/site/us/en/learn/training-certifications/training/netacad/index.html

Cisco Systems, Inc. (n.d.). *Cisco networking products and solutions*. https://www.cisco.com/

Cisco Systems, Inc. (n.d.). *Cisco Packet Tracer*. https://www.netacad.com/courses/packet-tracer (netacad.com)

Conklin, W. A., & White, G. B. (2022). *Principles of Computer Security* (6th ed.). McGraw-Hill Education.

Council of Europe. (2018). *Convention 108+: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*.

Council of Europe. (2018). *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223)*. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=223

Council of the European Union. (2018). Council recommendation on key competences for lifelong learning. https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=uriserv%3AOJ.C_.2018.189.01.0001.01.ENG

Cybersecurity and Infrastructure Security Agency. (2024). *Cybersecurity Best Practices for Education*. https://www.cisa.gov/education

Easttom, C. (2023). *Computer Security Fundamentals* (5th ed.). Pearson IT Certification.

Erickson, J. (2008). *Hacking: The Art of Exploitation* (2nd ed.). No Starch Press.

European Commission, Joint Research Centre. (n.d.). *Digital Competence Framework (DigComp)*. https://joint-research-centre.ec.europa.eu/projects-and-

activities/education-and-training/digital-transformation-education/digital-competence-framework-digcomp_en

European Commission. (2020). *Digital Education Action Plan (2021–2027)*. https://education.ec.europa.eu/focus-topics/digital-education/action-plan

European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)*. https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Union Agency for Cybersecurity. (2022–2025). *Cybersecurity Skills Framework*. https://www.enisa.europa.eu/topics/cybersecurity-education/cybersecurity-skills-framework

European Union Agency for Cybersecurity. (2022–2025). *Cybersecurity Skills Framework*. https://www.enisa.europa.eu/topics/cybersecurity-education/cybersecurity-skills-framework

European Union Agency for Cybersecurity. (2024). *National Cybersecurity Education Framework*. https://www.enisa.europa.eu/publications/national-cybersecurity-education-framework

European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation)*. Official Journal of the European Union, L119/1.

GitHub. (n.d.). *Kali Linux topics on GitHub*. https://github.com/topics/kali-linux

Habrusiev, V., Tereshchuk, H., Panchenko, V., Martyniuk, S., Sysoiev, O., & Henseruk, H. (2023, September). Enhancing Online Learning in LCM Moodle through Interactive Adaptive Learning. In 2023 13th International Conference on Advanced Computer Information Technologies (ACIT) (pp. 650-655). (Scopus)

Hevko, I. Lutsyk, O. Potapchuk, I. Lutsyk, V. Borysov. Implementation of web resources using cloud technologies to demonstrate and organize students' research work. Journal of Physics: Conference Series, Volume 1946, XIII International Conference on Mathematics, Science and Technology Education (ICon-MaSTEd 2021), Kryvyi Rih, Ukraine, 2021. ISSN: 1742-6596. DOI:

https://iopscience.iop.org/article/10.1088/1742-6596/1946/1/012019/meta . (Scopus).

International Organization for Standardization. (2019). *ISO/IEC 27701:2019 Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*. ISO.

International Organization for Standardization. (2022). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls*. https://www.iso.org/standard/27002

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. https://www.iso.org/standard/27001

International Organization for Standardization. (2022). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls*. ISO.

International Telecommunication Union. (2024). *Digital Skills Insights 2024*. https://www.itu.int

Khoroshko, V., Khokhlachova, Y., & Vyshnevska, N. (2023). DECOMPOSITION OF COMPUTER NETWORK TECHNOLOGY IN THEIR DESIGN. *Ukrainian Scientific Journal of Information Security*, *29*(3), 130–137. https://doi.org/10.18372/2225-5036.29.18072

Kniazheva, I. A. (2023). TECHNOLOGICAL APPROACH IN PEDAGOGICAL EDUCATION. *Innovate Pedagogy*, *1*(63), 163–166. https://doi.org/10.32782/2663-6085/2023/63.1.30

Kovalchuk, V. I., Maslich, S. V., Movchan, L .G., Lytvynova, S. H., Kuzminska, O. H. (2022). Digital transformation of vocational schools: Problem analysis. CEUR Workshop Proceedings, 3085, 107–123. https://doi.org/10.33407/ITLT.V6014.1681

Lakhno, V., Adilzhanova, S., Kryvoruchko, O., Desiatko, A., Buriachok, V. (2021). Allocation of Organizational and Financial Resources of the Information Protection Side Using a Genetic Algorithm. In: Silhavy, R. (eds) Informatics and

Cybernetics in Intelligent Systems. CSOC 2021. Lecture Notes in Networks and Systems, vol 228. Springer, Cham. https://doi.org/10.1007/978-3-030-77448-6_5

Lande, D., Andriichuk, O., Dmytrenko, O., Tsyganok, V., & Porplenko, Y. (2020). Building of knowledge bases of decision support systems using the directed networks of terms during information operations research. *Collection «Information Technology and Security»*, *8*(2), 153–163. https://doi.org/10.20535/2411-1031.2020.8.2.222597

Latham, A., Crockett, K., & McLean, D. (2014). An adaptation algorithm for an intelligent natural language tutoring system. Computers & Education, 71, 97–110. DOI: https://doi.org/10.1016/j.compedu.2013.09.014

Lazarenko, N. I., Gurevych, R. S., Kobysia, A. P., Kobysia, V. M. & Opushko, N. R. (2023). Modelling of the preparation of masters of professional education for activities in the information and digital environment. Information Technologies and Learning Tools, 96 (4), 137–151, DOI: https://doi.org/10.33407/itlt.v96i4.5275

Leshchenko, M., Lavrysh, Y., Halatsyn, K., Feshchuk, A., & Prykhodko, D. (2023). Technology-Enhanced Personalized Language Learning: Strategies and Challenges. International Journal of Emerging Technologies in Learning, 13(18), 120–136.

Lim, L., Lim, S. H., & Lim, W. Y. R. (2023). Efficacy of an adaptive learning system on course scores. Systems, 11(1), 31. DOI: https://doi.org/10.3390/systems11010031

Linux Foundation. (n.d.). *Kernel-based Virtual Machine (KVM)*. https://linux-kvm.org/

Makedon, V., Mykhailenko, O., & Dzyad, O. (2023). Modification of Value Management of International Corporate Structures in the Digital Economy. European Journal of Management Issues, 31(1), 50- 62. https://doi.org/10.15421/192305

Meeuwisse, R. (2022). *Cybersecurity for Beginners*. Cyber Simplicity Ltd.

Microsoft. (n.d.). *Azure virtual machines documentation*. https://learn.microsoft.com/en-us/azure/virtual-machines/

Ministry of Education and Science of Ukraine. (2023). *Про затвердження Порядку обробки та захисту персональних даних в Міністерстві освіти і науки України* (Order No. 1249, July 10, 2023). Official Bulletin of Ukraine. https://zakon.rada.gov.ua/laws/show/z1249-23

Mitnick, K. D., & Simon, W. L. (2002/2023). *The Art of Deception: Controlling the Human Element of Security*. Wiley.

Nárosy, T., Schmölz, A., Proinger, J., & Domany-Funtan, U. (2022). Digitales Kompetenzmodell für Österreich: DigComp 2.3 AT [Digital competence model for Austria: DigComp 2.3 AT]. Medienimpulse, 60(4), 1-103. https://doi.org/10.21243/mi-04-22-23

National Institute of Standards and Technology. (2024). *Cybersecurity Framework 2.0*. https://www.nist.gov/cyberframework

National Institute of Standards and Technology. (2024). *NICE Cybersecurity Workforce Framework*. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-cybersecurity-workforce-framework

National Institute of Standards and Technology. (2024). *NICE Cybersecurity Workforce Framework*. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-cybersecurity-workforce-framework

Nian, L., Wei, J., & Yin, C. (2019). The promotion role of mobile online education platform in students' self-learning. International Journal of Continuing Engineering Education and Life-Long Learning, 29(1–2), 56–71. https://doi.org/10.1504/IJCEELL.2019.099244

Oberländer, M., Beinicke, A., Bipp, T. (2020). Digital competencies: A review of the literature and applications in the workplace. Computers & Education, 146, 103752, https://doi.org/10.1016/j.compedu.2019.103752

Offensive Security. (n.d.). *Kali Linux: Penetration testing and ethical hacking Linux distribution*. https://www.kali.org/

Offensive Security. (n.d.). *Kali Linux: Penetration testing and ethical hacking Linux distribution*. https://www.kali.org/

Open Worldwide Application Security Project. (2021–2025). *OWASP Top 10 Web Application Security Risks*. https://owasp.org/www-project-top-ten/

Open Worldwide Application Security Project. (2021–2025). *OWASP Top 10 Web Application Security Risks*. https://owasp.org/www-project-top-ten/

Open Worldwide Application Security Project. (2025). *Secure Coding Practices Quick Reference Guide*. https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/

Oracle. (n.d.). *Oracle VM VirtualBox*. https://www.virtualbox.org/

Ovcharuk, O. V. (2023). TOOL FOR SELF-ASSESSMENT OF TEACHER'S DIGITAL COMPETENCE AS A COMPONENT OF EDUCATION QUALITY MONITORING. *Academic Notes. Series: Pedagogical Sciences*, (210), 42-47. https://doi.org/10.36550/2415-7988-2023-1-210-42-47

Polischuk, N. V. (2022). PERSONALLY-ORIENTED APPROACH IN THE PROCESS OF TRAINING FUTURE TEACHERS OF TECHNOLOGIES: CURRENT STATE AND FEATURES OF IMPLEMENTATION. *Innovate Pedagogy*, (47), 206–209. https://doi.org/10.32843/2663-6085/2022/47.39

PortSwigger. (n.d.). *Burp Suite: Web application security testing, scanning & penetration testing tools*. https://portswigger.net/burp

Potapchuk O. Current trends in the development of pedagogical systems of ukraine in the conditions of digitalization of society. Journal of Education, Health and Sport. 2023. 13(1):300-309. eISSN 2391-8306. DOI http://dx.doi.org/10.12775/JEHS.2023.13.01.045

Redecker, C. (2017). *European framework for the digital competence of educators: DigCompEdu* (EUR 28775 EN). Publications Office of the European Union. https://doi.org/10.2760/159770

Roemintoyo, P. T. & Budiarto, M. K. (2023). Project-based learning model to support 21st century learning: Case studies in vocational high schools. Journal of

Education Research and Evaluation, 7(4), 662–670. DOI https://doi.org/10.23887/jere.v7i4.63806

SadovyiM. I., & Tryfonova, O. M. (2022). ANALYTICAL APPROACH TO THE FORMATION OF THE NORMATIVE BASE OF EDUCATIONAL TRAINING OF STUDENTS. *Academic Notes. Series: Pedagogical Sciences*, (208), 56-63. https://doi.org/10.36550/2415-7988-2023-1-208-56-63

Serdenko, T. V., & Reis, T. T. (2025). Персоналізація навчання за допомогою інформаційних систем. Вісник Херсонського національного технічного університету, 2(2), 41–55. DOI: https://doi.org/10.35546/kntu2078-4481.2025.2.2.41

Singer, P. W., & Friedman, A. (2014/2024). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

Spirin, O. M. (Ed.)., Ivanova, S. M., Vakaliuk, T. A., Kilchenko, A. V., Labzhynskyi, Yu. A., Mintii, I. S., Novytska, T. L., Oleksiuk, V. P., Osadcha, K. P., Sikora, Ya. B., Semerikov, S. O., Tkachenko, V. A., Franchuk, N. P., Shymon, O. M., Shynenko, M. A., Chyzhmotria, O. V., & Yaskova (Vozniuk), N. V. (2025). *Розвиток цифрової компетентності наукових і науково-педагогічних працівників засобами відкритих освітньо-наукових інформаційних систем*. ІЦО НАПН України.

Splunk Inc. (n.d.). *Splunk Enterprise*. https://www.splunk.com/en_us/products/splunk-enterprise.html

Splunk. (n.d.). *About Splunk AI Assistant*. Splunk Help Center. https://help.splunk.com/en/splunk-cloud-platform/search/splunk-ai-assistant/2.0.0/about-splunk-ai-assistant/about-splunk-ai-assistant

Splunk. (n.d.). *Welcome to Splunk Enterprise 10.4*. Splunk Help Center. https://help.splunk.com/en/splunk-enterprise/release-notes-and-updates/release-notes/10.4/whats-new/welcome-to-splunk-enterprise-10.4

Stallings, W. (2020). *Cryptography and Network Security: Principles and Practice* (8th ed.). Pearson.

Strielkowski, W. (2025). AI-driven adaptive learning for sustainable educational development. Sustainable Development, 33(2), 291–305. DOI: https://doi.org/10.1002/sd.3221

Sushchenko, L., Andryushchenko, O., & Sushchenko, P. (2022). Digital Transformation of Higher Education Institutions in the Context of Digitalization of Society: Challenges and Prospects. *Pedagogical sciences reality and perspectives*, 146–151. https://doi.org/10.31392/npu-nc.series5.2022.spec.2.28

Tan, L. Y. (2025). Artificial intelligence-enabled adaptive learning platforms. Computers in Education, 172, 104250. DOI: https://doi.org/10.1016/j.compedu.2025.104250 276

Theoretical and practical scientific achievements: research and results of their implementation : with proceedings of the VI International Scientific and Theoretical Conference, Pisa, April 26, 2024. Pisa, Italian Republic, 2024. C. 70-74

Thompson, C. & Zhao, Y. (2023). The role of AI in shaping adaptive learning environments. Educational Research and Development Journal, 39(3), 243–260. DOI: https://doi.org/10.1234/erdj.2023.0039

TryHackMe. (2025). *Pre Security & Defensive Security Learning Paths*. https://tryhackme.com/paths

TryHackMe. (n.d.). *TryHackMe: Learn cyber security through hands-on labs and guided learning paths*. https://tryhackme.com/

UNESCO. (2023). *Digital Skills for Life and Work: A Global Perspective*. UNESCO.

V. Hevko, O. I. Potapchuk, I. B. Lutsyk, V. V. Yavorska, L. S. Hiltay, O. B. Stoliar. A novel pedagogical approach to equipping prospective IT professionals with skills in 3D modelling and reconstruction of architectural heritage. CEUR Workshop Proceedings : 7th International Workshop on Augmented Reality in Education, AREdu 2024. Kryvyi Rih : CEUR-WS, 2025. Vol. 3918. P. 85-101. URL.: https://ceur-ws.org/Vol-3918/paper026.pdf (Scopus).

Vacca, J. R. (2023). *Computer and Information Security Handbook* (4th ed.). Morgan Kaufmann.

Vilkov, V. . (2021). Dialectical and historical materialism in the structure of marxism-leninism philosophical teaching and politico-ideological doctrine. *Bulletin of Taras Shevchenko National University of Kyiv. Philosophy*, *4*(4), 114-141. https://doi.org/10.17721/2523-4064.2021/4-12/12

VMware. (n.d.). *VMware virtualization software solutions*. https://www.vmware.com/

Volatility Foundation. (n.d.). *Volatility: Open source memory forensics framework*. https://www.volatilityfoundation.org/

Williamson, B., Eynon, R., & Potter, J. (2020). Pandemic politics, pedagogies and practices: Digital technologies and distance education during the coronavirus emergency. Learning, Media and Technology, 45(2), 107–114. https://doi.org/10.1080/17439884.2020.1761641

Wireshark Foundation. (2025). *Wireshark User's Guide*. https://www.wireshark.org/docs/wsug_html_chunked/

Wireshark Foundation. (2025). *Wireshark User's Guide*. https://www.wireshark.org/docs/wsug_html_chunked/

Wireshark Foundation. (n.d.). *Wireshark download (Windows 64-bit all versions)*. https://www.wireshark.org/download/win64/all-versions/

Wireshark Foundation. (n.d.). *Wireshark: Network protocol analyzer*. https://www.wireshark.org/

Work.ua. (2026). *About Work.ua — Ukraine's #1 job search service*. https://www.work.ua/

Yechkalo, Y. V., Tkachuk, V. V., Semerikov, S. O., Khotskina, S. M., Markova, O. M., & Kravets, A. S. (2025). Developing digital competence in computer science education: an integrated framework for theory-driven pedagogical innovation. *Educational Dimension*, *13*, 104-125. https://doi.org/10.55056/ed.945

Yudin, O., Yudin, O., Chernysh, L., & Telyushchenko, V. (2024). Methods of implementation of the european cybersecurity skills framework in the formation of the content of the professional standard "head of the structural unit for

information security and cyber defence". *Science-Based Technologies*, *62*(2), 164–174. https://doi.org/10.18372/2310-5461.62.18710

ДОДАТКИ

Додаток А

Пам'ятка щодо відповідального використання програмного забезпечення захисту даних для майбутніх фахівців цифрових технологій

- **Завжди ставити захист даних на перше місце** – у будь якому проєкті, коді, системі чи навчальному матеріалі, який я створюю.
- **Мінімізувати збір даних** – збирати лише ту інформацію, яка дійсно необхідна для виконання завдання.
- **Використовувати надійні інструменти захисту** – шифрувати важливі файли (VeraCrypt), застосовувати двофакторну автентифікацію, регулярно оновлювати ПЗ.
- **Не передавати конфіденційні дані відкритим текстом** – завжди перевіряти, чи використовується захищене з'єднання (HTTPS), VPN у публічних мережах.
- **Бути обережним з паролями** – використовувати складні унікальні паролі, не зберігати їх у незахищених місцях, застосовувати менеджери паролів.
- **Відповідально працювати з персональними даними здобувачів і клієнтів** – отримувати згоду на обробку, не публікувати фото, відео чи оцінки без дозволу.
- **Аналізувати ризики** перед впровадженням нових технологій або змін у системі.
- **Постійно підвищувати свою кваліфікацію** у сфері кібербезпеки та кібергігієни.
- **Навчати інших** – передавати знання про безпечну роботу з даними учням, колегам та майбутнім фахівцям.
- **Негайно реагувати** на будь які підозрілі ситуації чи можливі витоки даних.

Пам'ятай: Кожен твій необережний крок може призвести до витоку даних, втрати довіри та юридичних наслідків. Відповідальне ставлення до безпеки даних – це не додаткова робота, а невід'ємна частина моєї професійної етики.

Додаток Б

Діагностичний інструментарій для визначення готовності до застосування ПЗ захисту даних

Анкета оцінювання готовності до застосування ПЗ захисту даних

Інструкція для респондента:

Оцініть кожне твердження відповідно до рівня власної підготовленості:

- **0 балів** – відсутній рівень
- **1 бал** – низький рівень
- **2 бали** – середній рівень
- **3 бали** – високий рівень

Виберіть один варіант відповіді для кожного твердження.

Когнітивний компонент

1. Я володію знаннями нормативно-правової бази та принципів захисту даних.

   0 ☐ 1 ☐ 2 ☐ 3 ☐

2. Я орієнтуюся в інструментах програмного забезпечення захисту даних.

   0 ☐ 1 ☐ 2 ☐ 3 ☐

Діяльнісний компонент

3. Я вмію застосовувати інструменти захисту даних у практичній діяльності.

   0 ☐ 1 ☐ 2 ☐ 3 ☐

4. Я здатний(а) розробляти навчально-методичні матеріали з використанням цифрових технологій.

   0 ☐ 1 ☐ 2 ☐ 3 ☐

Мотиваційний компонент

Продовження додатка Б

5. Я усвідомлюю значущість інформаційної безпеки в професійній діяльності.

   0 ☐ 1 ☐ 2 ☐ 3 ☐

6. Я маю мотивацію до професійного розвитку та навчання інших у сфері цифрових технологій.

   0 ☐ 1 ☐ 2 ☐ 3 ☐

Рефлексивний компонент

7. Я здатний(а) здійснювати самоаналіз власної професійної діяльності.

   0 ☐ 1 ☐ 2 ☐ 3 ☐

8. Я готовий(а) до систематичної самоосвіти та професійного вдосконалення.

   0 ☐ 1 ☐ 2 ☐ 3 ☐

Додаток В

Розробка лабораторних робіт по тематиці захисту даних

ЛАБОРАТОРНА РОБОТА № 1

Тема: Оцінка ризиків витоку персональних даних у повсякденних та професійних ситуаціях

Мета роботи: Навчитися визначати категорії персональних даних, оцінювати ризики їх витоку, аналізувати можливі наслідки порушення конфіденційності та розробляти комплекс заходів щодо їх захисту.

Очікувані результати навчання

Після виконання лабораторної роботи здобувач освіти повинен:

- знати поняття персональних даних та їх класифікацію;
- уміти визначати рівень конфіденційності інформації;
- аналізувати можливі сценарії витоку персональних даних;
- оцінювати наслідки реалізації загроз;
- розробляти технічні, організаційні та поведінкові заходи захисту;
- створювати інформаційні матеріали щодо безпечного поводження з персональними даними.

Обладнання та програмне забезпечення

- персональний комп'ютер;
- доступ до мережі Інтернет;
- текстовий редактор (Microsoft Word або LibreOffice Writer);
- електронні таблиці (Microsoft Excel або Google Sheets);
- методичні матеріали до лабораторної роботи.

Теоретичні відомості

Перед виконанням лабораторної роботи необхідно ознайомитися з такими питаннями:

- поняття персональних даних відповідно до Закону України «Про захист персональних даних»;
- категорії персональних даних;
- рівні конфіденційності інформації;
- основні джерела та причини витоку персональних даних;
- способи захисту персональної інформації;
- принципи інформаційної безпеки та кібергігієни.

Хід виконання роботи

Завдання 1. Класифікація персональних даних

1. Ознайомтеся з переліком персональних даних, наведеним у таблиці.
2. Для кожного виду даних визначте рівень конфіденційності:
   - загальнодоступні;
   - обмежені;
   - конфіденційні (чутливі).
3. Запишіть результати у відповідну колонку таблиці.

Завдання 2. Аналіз можливих ризиків витоку даних

1. Для кожного виду обмежених або конфіденційних даних визначте один або два можливі сценарії їх витоку.
2. Під час аналізу використовуйте реальні приклади можливих загроз, зокрема:
   - фішингові повідомлення;
   - використання незахищених Wi-Fi-мереж;
   - соціальну інженерію;
   - зараження комп'ютера шкідливим програмним забезпеченням;
   - людський фактор;
   - помилки адміністрування;
   - втрату або викрадення пристроїв.
3. Запишіть сценарії у відповідну колонку таблиці.

Завдання 3. Визначення можливих наслідків витоку інформації

1. Для кожного визначеного сценарію опишіть можливі наслідки витоку персональних даних.
2. Під час виконання завдання зверніть увагу на можливі:
   - фінансові втрати;
   - репутаційні ризики;
   - несанкціонований доступ до облікових записів;
   - крадіжку персональної інформації;
   - порушення вимог законодавства;
   - інші негативні наслідки.

Завдання 4. Розроблення заходів захисту

1. Для кожного сценарію витоку запропонуйте комплекс заходів захисту.
2. Заходи необхідно розподілити за категоріями:

- технічні;
- організаційні;
- поведінкові.

3. При розробленні рекомендацій використовуйте сучасні засоби захисту інформації, зокрема:

- двофакторну автентифікацію;
- використання складних паролів;
- менеджери паролів;
- VPN;
- резервне копіювання;
- антивірусне програмне забезпечення;
- регулярне оновлення програмного забезпечення;
- навчання користувачів правилам кібергігієни.

Завдання 5. Розроблення інформаційного матеріалу

1. Оберіть одну із професій (педагог, адміністратор, бухгалтер, менеджер, працівник державної установи тощо).
2. Розробіть один із запропонованих інформаційних матеріалів:
   - чек-лист «Як захистити персональні дані на робочому місці»;
   - коротку інструкцію щодо безпечної роботи з персональними даними.
3. Документ повинен містити 8–10 практичних рекомендацій.

Завдання 6. Аналіз отриманих результатів

1. Проаналізуйте виконані завдання.
2. Зробіть висновок щодо:
   - найбільш поширених загроз персональним даним;
   - найбільш ефективних способів їх запобігання;
   - ролі працівника у забезпеченні інформаційної безпеки організації.

Зміст звіту

Звіт повинен містити:

1. Назву лабораторної роботи.
2. Мету роботи.
3. Виконані завдання.
4. Заповнену таблицю аналізу ризиків.
5. Розроблений чек-лист або інструкцію.
6. Висновки.

Продовження додатка В

Контрольні запитання

1. Що належить до персональних даних?
2. Які категорії персональних даних існують?
3. Які основні причини витоку персональних даних?
4. Які види соціальної інженерії найчастіше використовуються зловмисниками?
5. Для чого застосовується двофакторна автентифікація?
6. Які технічні засоби використовуються для захисту персональних даних?
7. Чим відрізняються технічні, організаційні та поведінкові заходи захисту?
8. Які можливі наслідки витоку персональних даних для працівника та організації?

Додаток Г

Структура курсу «Кібербезпека та захист даних у професійній освіті»

№	Тема	Результати навчання	Завдання
1	Нормативно-правові основи захисту персональних даних в Україні та ЄС (Закон №2297-VI, GDPR)	Аналізує основні положення національного та європейського законодавства у сфері захисту персональних даних; визначає вимоги до обробки та зберігання даних у професійній діяльності	Завдання до лабораторної роботи, контрольні питання, тестові завдання
2	Юридична відповідальність за порушення законодавства у сфері захисту даних	Застосовує знання нормативно-правової бази для визначення видів відповідальності за порушення правил обробки персональних даних	Завдання до лабораторної роботи, контрольні питання, тестові завдання
3	Ризик-орієнтований підхід до захисту інформації. Класифікація даних та вплив сучасних технологій (штучний інтелект)	Ідентифікує та оцінює ризики витоку інформації; аналізує вплив сучасних цифрових технологій, зокрема штучного інтелекту, на безпеку даних	Завдання до лабораторної роботи, контрольні питання, тестові завдання
4	Забезпечення безпеки персональних даних у системах дистанційного навчання (Zoom, Teams, Google Classroom, Moodle)	Застосовує правила безпечної роботи з цифровими освітніми платформами для захисту персональних даних користувачів	Завдання до лабораторної роботи, контрольні питання, тестові завдання
5	Криптографічні методи захисту даних та сучасні інструменти шифрування (VeraCrypt, BitLocker)	Використовує базові криптографічні методи та програмні засоби шифрування для забезпечення конфіденційності даних	Завдання до лабораторної роботи, контрольні питання, тестові завдання
6	Моніторинг та аналіз мережевого трафіку	Виконує базовий аналіз мережевого трафіку за допомогою спеціалізованого програмного забезпечення та інтерпретує результати	Завдання до лабораторної роботи, контрольні питання, тестові завдання
7	Виявлення вразливостей у мережевих протоколах	Ідентифікує основні вразливості мережевих протоколів та оцінює рівень їх захищеності	Завдання до лабораторної роботи, контрольні питання, тестові завдання
8	Проєктування захищених локальних обчислювальних мереж	Проєктує базові моделі захищених локальних мереж із урахуванням вимог інформаційної безпеки	Завдання до лабораторної роботи, контрольні питання, тестові завдання
9	Базові механізми захисту інформації (ACL, паролі, сегментація мереж)	Налаштовує та застосовує базові механізми захисту інформації у мережевих середовищах	Завдання до лабораторної роботи, контрольні питання, тестові завдання

Додаток Д

Тестові завдання з курсу «Кібербезпека та захист даних у професійній освіті»

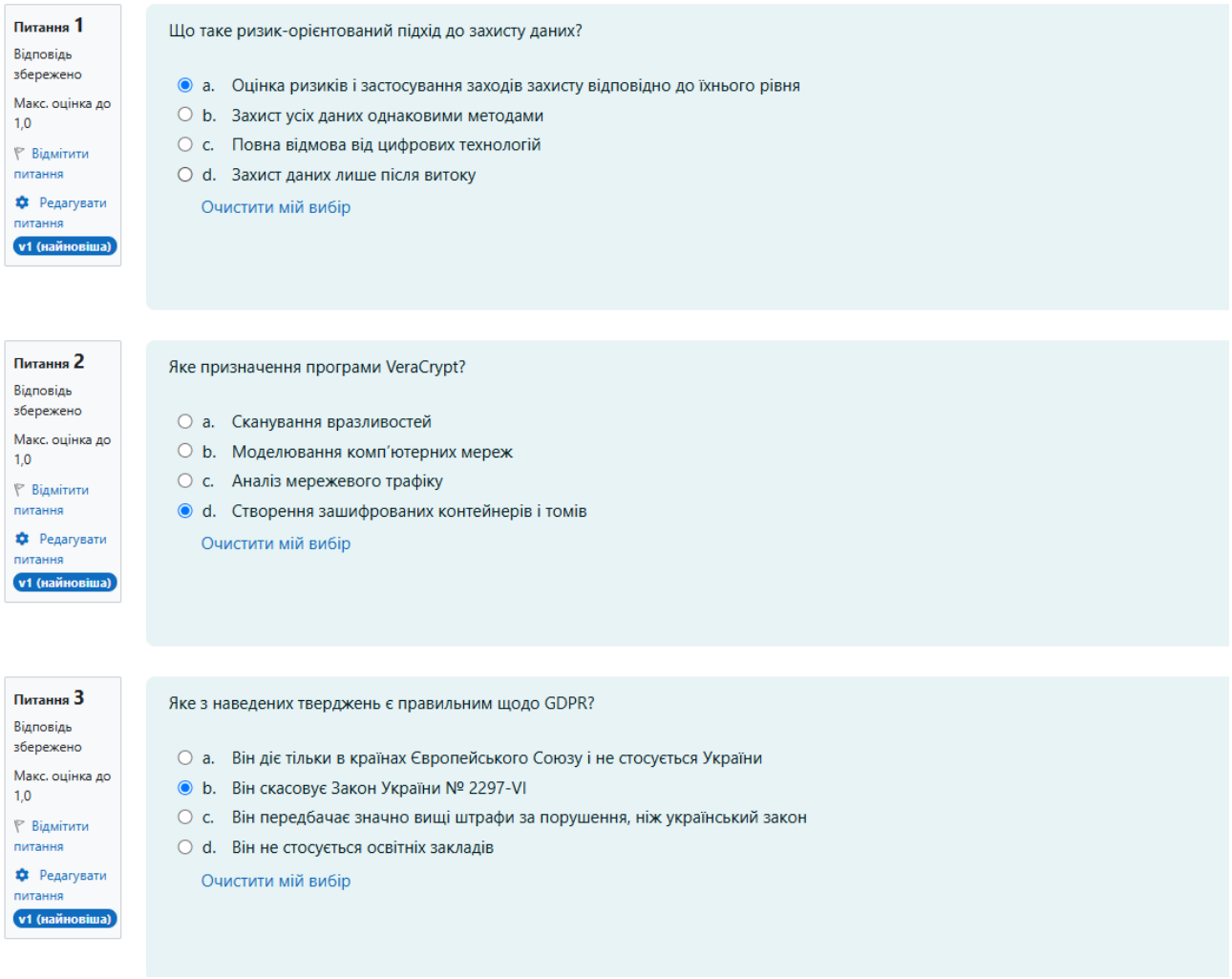

Рис. Д.1 Тестові завдання з курсу «Кібербезпека та захист даних у професійній освіті»

Додаток Е

Таблиця Е.1

Приклад прогресу здобувача в процесі перевірки методики від 16 до 24 балів

№	Компонент	Ключовий показник	До експерименту	Після експерименту	Приріст
1	Когнітивний	Знання нормативної бази та принципів захисту даних	2	3	+1
2	Когнітивний	Знання інструментів ПЗЗД	2	3	+1
3	Діяльнісний	Самостійне застосування інструментів	2	3	+1
4	Діяльнісний	Розробка навчальних матеріалів з теми	2	3	+1
5	Мотиваційний	Усвідомлення відповідальності та етичне ставлення	2	3	+1
6	Мотиваційний	Мотивація навчати інших	2	3	+1
7	Рефлексивний	Здатність до самоаналізу та рефлексії	2	3	+1
8	Рефлексивний	Готовність до самоосвіти	2	3	+1
Загальна сума			**16**	**24**	**+8**

Додаток Ж

Приклад тестових завдань курсу «Захист даних у професійній діяльності»

1.Для чого використовується інструмент Nmap?

A) Для шифрування файлів

B) Для сканування портів і виявлення служб у мережі

C) Для створення резервних копій

D) Для аналізу відеоуроків

ANSWER: B

2.Для чого використовується інструмент Wireshark?

A) Для шифрування файлів

B) Для захоплення та аналізу мережевого трафіку

C) Для створення віртуальних мереж

D) Для резервного копіювання даних

ANSWER: B

3.Хто є володільцем персональних даних учнів у закладі освіти?

A) Кожен викладач окремо

B) Заклад освіти

C) Батьки учнів

D) Міністерство освіти і науки України

ANSWER: B

4.Хто несе головну відповідальність за захист персональних даних здобувачів у закладі освіти?

A) Кожен викладач окремо

B) Заклад освіти як володілець даних

C) Батьки учнів

D) Міністерство освіти і науки України

ANSWER: B

5.Що є найкращою практикою при роботі з конфіденційними даними на флешці?

A) Залишати флешку без пароля для зручності

B) Використовувати VeraCrypt для створення зашифрованого контейнера

C) Зберігати дані у звичайних папках

D) Копіювати дані на кілька флешок

ANSWER: B

6.Що означає поняття «конфіденційні дані»?

A) Дані, які можна вільно публікувати

B) Дані, розголошення яких може завдати значної шкоди особі або організації

C) Дані, які зберігаються тільки в паперовому вигляді

D) Дані, які не підлягають захисту

ANSWER: B

7.Що означає принцип «privacy by design»?

A) Захист даних починається після виникнення проблеми

B) Захист даних вбудовується на етапі проектування системи чи навчального процесу

C) Захист даних стосується тільки фінансової інформації

D) Захист даних — це виключно технічне завдання адміністратора

ANSWER: B

8.Що означає термін «Privacy by Design»?

A) Захист даних починається тільки після інциденту

B) Захист даних вбудовується в систему чи навчальний процес з самого початку

C) Захист даних — це виключно технічне завдання

D) Захист даних стосується лише конфіденційної інформації

ANSWER: B

9.Що таке «Zoombombing»?

A) Швидке завантаження уроку

B) Несанкціоноване підключення сторонніх осіб до онлайн-заняття

C) Автоматичний запис уроку

D) Перевірка присутності студентів

ANSWER: B

10.Що таке «прихований том» у програмі VeraCrypt?

A) Том, який видно тільки адміністратору

B) Додатковий зашифрований том, існування якого неможливо довести без правильного пароля

C) Тимчасовий том для тестування

D) Том, який автоматично видаляється після виходу

ANSWER: B

11.Що таке ACL у контексті захисту мереж?

A) Антивірусна програма

B) Список контролю доступу

C) Автоматична система резервного копіювання

D) Програма для шифрування паролів

ANSWER: B

12.Що таке двофакторна автентифікація (2FA)?

A) Використання двох однакових паролів

B) Підтвердження входу двома різними способами
C) Зміна пароля раз на рік
D) Використання лише біометрії
ANSWER: B

13.Що таке персональні дані згідно із Законом України «Про захист персональних даних»?
A) Будь-яка інформація, що стосується конкретної фізичної особи, яку можна прямо чи опосередковано ідентифікувати
B) Тільки інформація, яка зберігається в державних реєстрах
C) Лише паспортні дані та номер телефону
D) Інформація про юридичних осіб
ANSWER: A

14.Що таке персональні дані згідно із Законом України «Про захист персональних даних»?
A) Будь-яка інформація, що стосується конкретної фізичної особи, яку можна прямо чи опосередковано ідентифікувати
B) Тільки інформація, яка зберігається в державних реєстрах
C) Лише паспортні дані та номер телефону
D) Інформація про юридичних осіб
ANSWER: A

15.Що таке ризик-орієнтований підхід до захисту даних?
A) Захист усіх даних однаковими методами
B) Оцінка ризиків і застосування заходів захисту відповідно до їхнього рівня
C) Захист даних лише після витоку
D) Повна відмова від цифрових технологій
ANSWER: B

16.Яка найкраща практика захисту даних на флеш-накопичувачі?

A) Залишати флешку без пароля для швидкого доступу

B) Використовувати VeraCrypt для створення зашифрованого контейнера

C) Копіювати дані на кілька флешок

D) Зберігати дані у звичайних папках

ANSWER: B

17.Яка основна мета використання Cisco Packet Tracer у вивченні захисту даних?

A) Шифрування файлів

B) Моделювання захищених мереж, налаштування firewall та ACL

C) Аналіз трафіку в реальному часі

D) Сканування вразливостей

ANSWER: B

18.Яка основна небезпека використання слабких паролів у професійному середовищі?

A) Зменшення швидкості роботи комп’ютера

B) Легкий доступ зловмисників до систем і даних

C) Збільшення обсягу пам’яті

D) Погіршення якості інтернет-з’єднання

ANSWER: B

19.Яке з наведених тверджень є правильним щодо GDPR?

A) Він діє тільки в країнах Європейського Союзу і не стосується України

B) Він передбачає значно вищі штрафи за порушення, ніж український закон

C) Він не стосується освітніх закладів

D) Він скасовує Закон України № 2297-VI

ANSWER: B

20.Яке призначення програми VeraCrypt?

A) Аналіз мережевого трафіку

B) Створення зашифрованих контейнерів і томів

C) Моделювання комп’ютерних мереж

D) Сканування вразливостей

ANSWER: B

21.Який з наведених документів є основним у сфері захисту персональних даних в Україні?

A) Закон «Про освіту»

B) Закон України «Про захист персональних даних» № 2297-VI

C) Закон «Про вищу освіту»

D) Закон «Про електронне урядування»

ANSWER: B

22.Який інструмент найкраще підходить для повного шифрування жорсткого диска в операційній системі Windows?

A) Wireshark

B) BitLocker

C) Nmap

D) Cisco Packet Tracer

ANSWER: B

23.Який порт найбільш часто використовується для віддаленого доступу до робочого столу (RDP)?

A) 80

B) 443

C) 3389

D) 22

ANSWER: C

24.Який протокол забезпечує шифрування даних під час передачі в інтернеті?

A) HTTP

B) HTTPS

C) FTP

D) Telnet

ANSWER: B

25.Який тип автентифікації вважається найбезпечнішим на сьогодні?

A) Лише пароль

B) Багатофакторна автентифікація (MFA)

C) Логін і прізвище

D) Графічний пароль

ANSWER: B

Додаток К

Шкала оцінювання рівня готовності майбутніх фахівців цифрових технологій до застосування програмного забезпечення захисту даних у професійній діяльності

Таблиця К.1

Опитувальник самооцінювання готовності майбутніх фахівців цифрових технологій до професійної діяльності та застосування програмного забезпечення захисту даних

№	Твердження	Оцінка (1–5)
1	Усвідомлюю соціальну значущість професії педагога професійного навчання	
2	Відчуваю інтерес до педагогічної діяльності у сфері цифрових технологій	
3	Прагну до постійного професійного самовдосконалення в галузі ІТ	
4	Вважаю цифрове освітнє середовище необхідною умовою сучасного навчання	
5	Готовий(а) впроваджувати інноваційні цифрові технології у навчальний процес	
6	Знаю сучасні методики використання ІКТ у професійному навчанні	
7	Орієнтуюся в принципах організації цифрового освітнього середовища	
8	Володію знаннями з інформаційної етики та цифрової безпеки	
9	Розумію специфіку підготовки фахівців цифрових технологій	
10	Знаю способи оцінювання навчальних результатів у цифровому середовищі	
11	Умію створювати цифрові навчальні матеріали (презентації, інструкції, чек-листи)	
12	Використовую інтерактивні методи навчання в цифровому середовищі	
13	Можу організовувати дистанційне або змішане навчання	
14	Умію здійснювати педагогічну взаємодію в онлайн-форматі	
15	Здатний(а) інтегрувати ІКТ у професійно орієнтоване навчання	
16	Володію практичними навичками використання програмного забезпечення захисту даних	
17	Розумію ризики витоку даних та вмію їх запобігати	
18	Готовий(а) формувати культуру кібергігієни	
19	Аналізую власну готовність до педагогічної діяльності в цифровому середовищі	
20	Готовий(а) постійно вдосконалювати свої компетентності у сфері кібербезпеки	

Додаток Л

Структура електронного навчально-методичного комплексу з дисципліни «Кібербезпека та захист даних у професійній освіті»

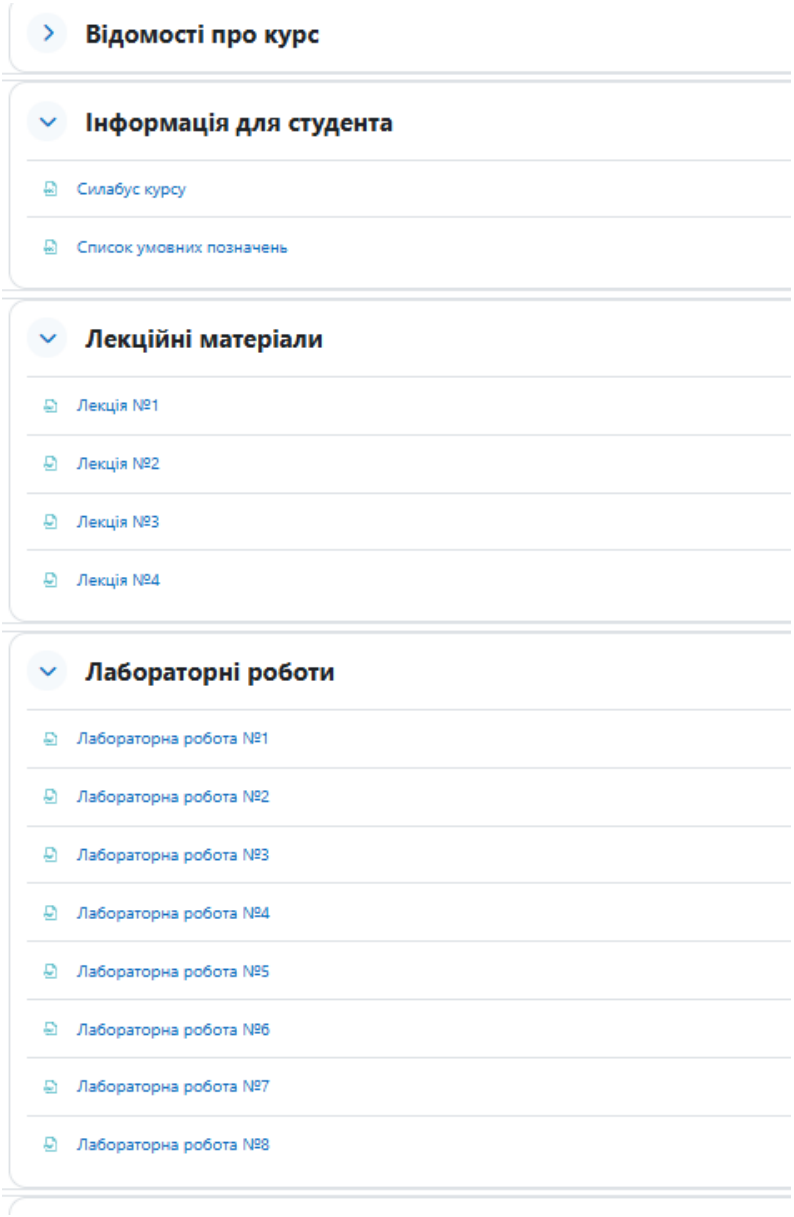

Рис.Л.1 Організація навчальних матеріалів електронного курсу в системі дистанційного навчання LMS Moodle

Додаток М

Довідки, що засвідчують апробацію результатів дисертаційного дослідження

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

РІВНЕНСЬКИЙ ДЕРЖАВНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

вул.Ст.Бандери, 12, м. Рівне, 33028, тел. (0362) 63-42-24
E-mail: rectorat@rshu.edu.ua, код ЄДРПОУ 25736989

26.06.26 № 01-12/68 На № _____

ДОВІДКА
про впровадження результатів дослідження
Шимківа Назара Ігоровича на тему
«Методика підготовки фахівців цифрових технологій до застосування програмного забезпечення захисту даних»
поданої на здобуття наукового ступеня доктора філософії
зі спеціальності 015 Професійна освіта

Матеріали та практичні результати дисертаційного дослідження Н. І. Шимківа впроваджено в освітній процес факультету математики та інформатики Рівненського державного гуманітарного університету. Інтеграція наукових здобутків здійснювалася протягом 2024–2026 навчальних років під час підготовки здобувачів вищої освіти першого (бакалаврського) рівня спеціальності 015 «Професійна освіта» (спеціалізація «Цифрові технології»).

Зокрема, науково-педагогічні працівники кафедри цифрових технологій та методики навчання інформатики використали в освітньому процесі розроблені навчально-методичні матеріали модуля «Кібербезпека та захист даних у професійній освіті». Практична реалізація результатів дослідження забезпечувалася шляхом активного застосування цифрових технологій, спеціалізованих онлайн-платформ, віртуальних симуляторів та інтерактивних інструментів візуалізації даних. Це дозволило ефективно цифровізувати освітній контент та поглибити знання й уміння здобувачів освіти.

Ефективність запроваджених методичних рішень підтверджено під час апробації. Викладачі та здобувачі освіти позитивно оцінили якість й актуальність матеріалів дисертаційної роботи Н. І. Шимківа, що засвідчує доцільність їх подальшого використання в практиці підготовки фахівців у закладах вищої освіти України.

Довідку підготовлено за підсумками обговорення на засіданні кафедри цифрових технологій та методики навчання інформатики РДГУ (протокол №8 від «24» червня 2026 року).

Завідувач кафедри цифрових технологій та методики навчання інформатики — Наталія ПАВЛОВА

Т. в.о. ректора — Ігор ВОЙТОВИЧ

УКРАЇНА
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ВОЛОДИМИРА ГНАТЮКА (ТНПУ)
вул. М.Кривоноса, 2, м. Тернопіль, 46027,
тел. (0352) 43-58-80, факс (0352) 43-60-02
e-mail: info@tnpu.edu.ua, код ЄДРПОУ 02125544

UKRAINE
MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
TERNOPIL VOLODYMYR HNATIYK NATIONAL PEDAGOGICAL UNIVERSITY (TNPU)
2 M.Kryvonosa st., Ternopil, 46027, Ukraine
tel. +38 0352 43-58-80, fax:+38 0352 43-60-02
e-mail: info@tnpu.edu.ua

Від «03» 06 2026 р. №774/20.03-33 На № _____ від «____» _____ 20___ р.

ДОВІДКА

про впровадження результатів дослідження
Шимківа Назара Ігоровича
Тема дисертації:

Методика підготовки фахівців цифрових технологій до застосування програмного забезпечення захисту даних
поданої на здобуття наукового ступеня доктора філософії зі спеціальності 015 Професійна освіта.

Дана довідка підтверджує, що результати наукового дослідження впроваджено в освітній процес **Тернопільського національного педагогічного університету імені Володимира Гнатюка**.

Дослідження присвячене теоретичному обґрунтуванню та експериментальній перевірці ефективності методики підготовки фахівців цифрових технологій до застосування програмного забезпечення для захисту даних, а також розробці навчально-методичних матеріалів до дисципліни «Комп'ютерні мережі та захист даних» шляхом включення модуля «Кібербезпека та захист даних у професійній освіті».

З цією метою впродовж 2023-2025 років на кафедрі комп'ютерних технологій Тернопільського національного педагогічного університету імені Володимира Гнатюка здобувачем було організовано та проведено педагогічний експеримент, який підтвердив ефективність розробленої методики, організаційно-педагогічних умов, а також методів і засобів її реалізації.

Також підтверджено, що структурно-функціональна модель підготовки фахівців цифрових технологій до застосування програмного забезпечення захисту даних в освітньому процесі є цілісною системою взаємопов'язаних компонентів, спрямованих на формування професійної компетентності майбутніх фахівців у сфері захисту інформації та кібербезпеки.

Зазначене вище дозволяє зробити висновок, що дисертаційне дослідження Назара Шимківа є науково важливим і актуальним, а його результати доцільно впроваджувати в освітні програми, що здійснюють підготовку фахівців за спеціальністю 015 Професійна освіта, спеціалізацією 015.39 Цифрові технології.

Довідку про впровадження результатів дисертаційного дослідження було обговорено та затверджено на засіданні кафедри комп'ютерних технологій Тернопільського національного педагогічного університету імені Володимира Гнатюка (протокол № 11 від «28» травня 2026).

Проректор з наукової роботи
та міжнародного співробітництва — Ірина ЗАДОРОЖНА

Завідувач кафедри
комп'ютерних технологій — Юрій ФРАНКО