

DOI: <https://doi.org/10.31392/NZ-udu-157.2024.15>

УДК 378.147:004.056

Шумків Н. І.

АКТУАЛЬНІ ПРОБЛЕМИ ЗАХИСТУ ДАНИХ У ПРОЦЕСІ ПІДГОТОВКИ МАЙБУТНІХ ФАХІВЦІВ ЦИФРОВИХ ТЕХНОЛОГІЙ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ПРОФЕСІЙНОЇ ОСВІТИ

У статті обґрунтовано необхідність обов'язкового включення тем кібербезпеки та захисту персональних даних в освітні програми спеціальності 015.39 «Професійна освіта (Цифрові технології)» в період активної цифрової трансформації професійної (професійно-технічної) освіти України 2024-2026 років.

Проведено аналіз впливу впровадження єдиної цифрової системи «Мрія», Стратегії цифрової трансформації освіти до 2027 року, зростання кіберзагроз у воєнний період та поширення технологій штучного інтелекту на вимоги до підготовки майбутніх педагогів. Показано опис експерименту в навчальному закладі, який можна провести в рамках спеціальності 015.39 Професійна освіта (Цифрові технології) з прикладами таблиць оцінювання та результатами експерименту. Використання розробленої матриці оцінювання (8 показників, 24 бали) як інструмент поточного, проміжного та підсумкового контролю для визначення результатів діяльності студентів.

Наведено результати педагогічного експерименту, що підтвердив ефективність розробленої методики (лабораторні роботи з Wireshark, Cisco Packet Tracer, VeraCrypt, кейс-метод, проектна діяльність з обов'язковою педагогічною складовою). Обґрунтовано рекомендації до впровадження сучасної програми захисту даних.

Проведено аналіз матриці компетентностей – ключового елементу освітньо-професійної програми (ОПП), що регулює прозорість і системність підготовки фахівців. Запропоновано методичні рекомендації щодо включення 4-кредитного модуля «Кібербезпека та захист даних у професійній освіті» до робочих програм дисциплін «Комп'ютерні мережі та захист даних» і «Методика професійного навчання». Результати мають практичне значення для педагогічних ЗВО та П(ПТ)О.

Ключові слова: Педагогічні методи, навчальні технології, , практичне навчання, цифрові технології, підготовка фахівців, адаптивне навчання, цифрова трансформація, система підготовки.

Цифрова трансформація освіти в Україні є одним із пріоритетних напрямків державної політики. Впровадження єдиної цифрової екосистеми «Мрія», оновлення Стратегії цифрової трансформації освіти і науки до 2027 року, активне використання штучного інтелекту та перехід на дистанційні та гібридні форми навчання кардинально змінюють вимоги до підготовки педагогічних кадрів. Водночас воєнний стан і зростання кіберзагроз (фішинг, витоки даних, атаки на освітні платформи) роблять кібербезпеку не додатковою, а обов'язковою компетентністю педагога.

Спеціальність 015.39 «Професійна освіта (Цифрові технології)» займає особливе місце, оскільки її випускники готують майбутніх робітників і техніків для цифрової економіки. Вони повинні не лише самі володіти засобами захисту даних, а й формувати культуру кібербезпеки в учнів П(ПТ)О. Однак

аналіз освітньо-професійних програм показує, що кібербезпека в більшості випадків представлена фрагментарно, без системної педагогічної складової.

Аналіз сучасних освітньо-професійних програм (ОПП) спеціальності 015.39 «Професійна освіта (Цифрові технології)» дозволяє оцінити, наскільки підготовка майбутніх педагогів відповідає реальним викликам цифрової трансформації професійної освіти 2024-2026 років. Особливу увагу приділено ступеню інтеграції тем кібербезпеки та захисту персональних даних, адже саме ці компетентності стають обов'язковими для педагога, який працює з учнями П(ПТ)О в умовах єдиної цифрової екосистеми «Мрія», зростання кібератак та поширення штучного інтелекту.

Цифрова трансформація професійної освіти в Україні 2024-2026 рр.

Цифрова трансформація професійної освіти відбувається під впливом кількох ключових факторів:

- Впровадження єдиної цифрової екосистеми «Мрія» (електронні журнали, платформи дистанційного навчання, цифрові профілі учнів).

- Затвердження змін до стандартів вищої освіти (накази МОН № 924 від 26.06.2024 та № 1435 від 18.11.2020 зі змінами).

- Посилення кіберзагроз у воєнний період (зростання атак на освітні установи в 2024-2025 рр.).

- Поширення штучного інтелекту (генеративні моделі, deepfake, автоматизований фішинг).

Ці процеси вимагають від педагогів не лише технічних навичок, а й уміння формувати в учнів П(ПТ)О відповідальне ставлення до даних.

Мета статті – обґрунтувати рекомендацію включення кібербезпеки в ОПП спеціальності 015.39 Професійна освіта (Цифрові технології) та описати конкретні методичні рекомендації щодо її впровадження.

Для порівняльного аналізу обрано дві репрезентативні програми, акредитовані МОН України та оновлені на 2024-2025 навчальний рік:

1. ОПП Тернопільського національного педагогічного університету імені Володимира Гнатюка (Інженерно-педагогічний факультет, кафедра комп'ютерних технологій);

2. ОПП Житомирського державного університету імені Івана Франка (Фізико-математичний факультет, кафедра прикладної математики та інформатики).

Обидві програми відповідають чинному стандарту вищої освіти за спеціальністю 015 (наказ МОН № 1460 від 21.11.2019 зі змінами), однак суттєво відрізняються за глибиною та характером представлення кібербезпеки.

У освітній програмі ТНПУ імені Володимира Гнатюка кібербезпека інтегрована системно та практично орієнтована. Обов'язковим освітнім компонентом є дисципліна «Комп'ютерні мережі та захист даних» (ОК 1.2.13) обсягом 6 кредитів ECTS з підсумковим контролем у формі екзамену. Зміст дисципліни охоплює принципи захисту інформації в комп'ютерних мережах, базові механізми автентифікації (паролі, двофакторна автентифікація),

шифрування даних, налаштування firewall та засобів контролю доступу, виявлення типових загроз (фішинг, шкідливе ПЗ, несанкціонований доступ), правові аспекти (Закон України «Про захист персональних даних» № 2297-VI, рекомендації Уповноваженого Верховної Ради України з прав людини щодо обробки персональних даних в освіті). Важливо, що дисципліна передбачає значний обсяг практичних лабораторних робіт із використанням реальних інструментів: Cisco Packet Tracer (моделювання мереж та ACL), Wireshark (аналіз трафіку), VeraCrypt (створення зашифрованих контейнерів).

Сучасний напрямок підготовки фахівців цифрових технологій формується на основі глобальних цифрових трансформацій, що викликає потребу в актуальних вміннях та навичках. Основними вимогами до сучасних освітніх програм є:

- Гнучкість та адаптивність – програма не може бути сталою, а має будуватися під сучасні тенденції розвитку технологій. Також частково можна розглядати інтеграцію сучасних сертифікованих курсів від технологічних гігантів, що дозволяє завжди тримати практичну частину в актуальних завданнях.

- Практикоорієнтованість та проектне навчання – теоретична складова навчання без закріплення її практичною частиною це даремно витрачений час, що не дає конкретних результатів. Також можливість поєднання навчання із практичними завданнями на підприємствах, що дозволяє використовувати знання на реальних задачах.

- Впровадження штучного інтелекту – використання ШІ як інструменту, що проводить міжпредметний зв'язок у навчальному процесі. Основа має полягати у вмінні використанні AI-асистентів, а також етичні аспекти їх використання при виконанні завдань.

- Використання навичок командної роботи та розвиток навичок – вміння вирішувати складні завдання у команді та робота над спільними проектами, дозволяє розподілити обов'язки а також правильно виконувати свій спектр робіт.

- Сучасна освітня програма в галузі підготовки фахівців цифрових технологій це не лише перелік дисциплін, а й поєднання фундаментальних дисциплін та прикладного програмного забезпечення, що дозволяє логічно вибудувати структуру підготовки.

- Збалансована освітня програма в галузі ІТ – це не просто перелік дисциплін, а гармонійне поєднання фундаментальної підготовки (математика, теорія алгоритмів) та прикладних інструментів (фреймворки, хмарні сервіси).

Педагогічна складова є невід'ємною частиною програми: студенти не лише набувають технічних навичок, а й розробляють конспекти уроків, інструкції, чек-листи та пам'ятки з кібергігієни, адаптовані саме для учнів професійно-технічних закладів. Додаткові елементи захисту даних присутні в дисциплінах «Основи програмування» (безпечне кодування), «Системи управління базами даних» (захист від SQL-ін'єкцій), «Технології штучного інтелекту» (приватність даних у ШІ) та «Методика професійного навчання»

(методика викладання питань кібербезпеки). Загалом частка контенту, пов'язаного з кібербезпекою, становить приблизно 8-10 % від загального обсягу ОПП, що робить програму ТНПУ однією з найсильніших у Західному регіоні за цим напрямком.

На противагу цьому ОПП Житомирського державного університету імені Івана Франка приділяє меншої уваги до практичних аспектів кібербезпеки. Особливої дисципліни, присвяченої комплексному захисту даних, в освітній програмі «015.39 Професійна освіта (Цифрові технології)». Основний акцент зроблено на дисципліні «Криптологія», яка зосереджена переважно на математичних основах шифрування, алгоритмах та теоретичних аспектах криптографії. Елементи захисту даних присутні фрагментарно в дисциплінах «Комп'ютерні мережі», «Програмування», «Веб-технології», однак практичні лабораторні роботи з інструментами на кшталт Wireshark, Cisco Packet Tracer чи VeraCrypt або відсутні, або представлені в мінімальному обсязі. Педагогічна складова також слабка: студенти практично не виконують завдань із розробки навчальних матеріалів з кібергігієни для учнів П(ПТ)О. Частка контенту, пов'язаного з кібербезпекою, становить лише 3-4 % від загального обсягу програми і має переважно теоретичний, математичний характер, а не практико-педагогічний.

Порівняльний аналіз двох програм дозволяє зробити такі висновки. По-перше, наявність окремої обов'язкової дисципліни обсягом 4 кредитів із значним практичним компонентом і обов'язковою педагогічною складовою є суттєвою перевагою програми ТНПУ. По-друге, відсутність такого блоку в інших ОПП призводить до фрагментарного представлення кібербезпеки, що не відповідає сучасним вимогам компетентності інженера-педагога. По-третє, навіть в окремих програмах педагогічна спрямованість захисту даних (розробка матеріалів для учнів ПТО) часто недостатньо акцентована.

Розроблена методика (поєднання лабораторних робіт, кейс-методу, проєктної діяльності, рефлексії та обов'язкової педагогічної складової – створення навчальних матеріалів для учнів ПТО) є ефективною, статистично та практично значущою. Вона дозволяє не тільки підвищити технічну компетентність, а й сформуванню у майбутніх викладачів внутрішню мотивацію, етичне ставлення та вміння передавати знання з кібербезпеки учням професійної освіти.

Отже, цифрові трансформації 2024-2026 років (впровадження «Мрії», посилення кіберзагроз, поширення ШІ) вимагають переходу від фрагментарного до системного та обов'язкового включення кібербезпеки в усі ОПП спеціальності 015.39. Без цього випускники не зможуть повноцінно формувати культуру цифрової безпеки в учнів професійно-технічних закладів.

Експериментальна перевірка ефективності методики

У 2024-2025 навчальному році проведено педагогічний експеримент (експериментальна група n=24, контрольна n=22). Методика включала лабораторні

роботи (Wireshark, Cisco Packet Tracer, VeraCrypt), кейс-метод, проєктну діяльність і обов'язкову педагогічну складову (створення навчальних матеріалів для учнів ПТО).

Результати:

1. Приріст готовності в експериментальній групі +7,3 бала (+49 %, $p < 0,001$, $r = 0,62$).
2. Контрольна група – лише +1,3 бала.
3. Якісні зміни: 78 % студентів почали використовувати 2FA, 92 % постійно перевіряють HTTPS, 85 % вважають кібербезпеку частиною професії педагога.

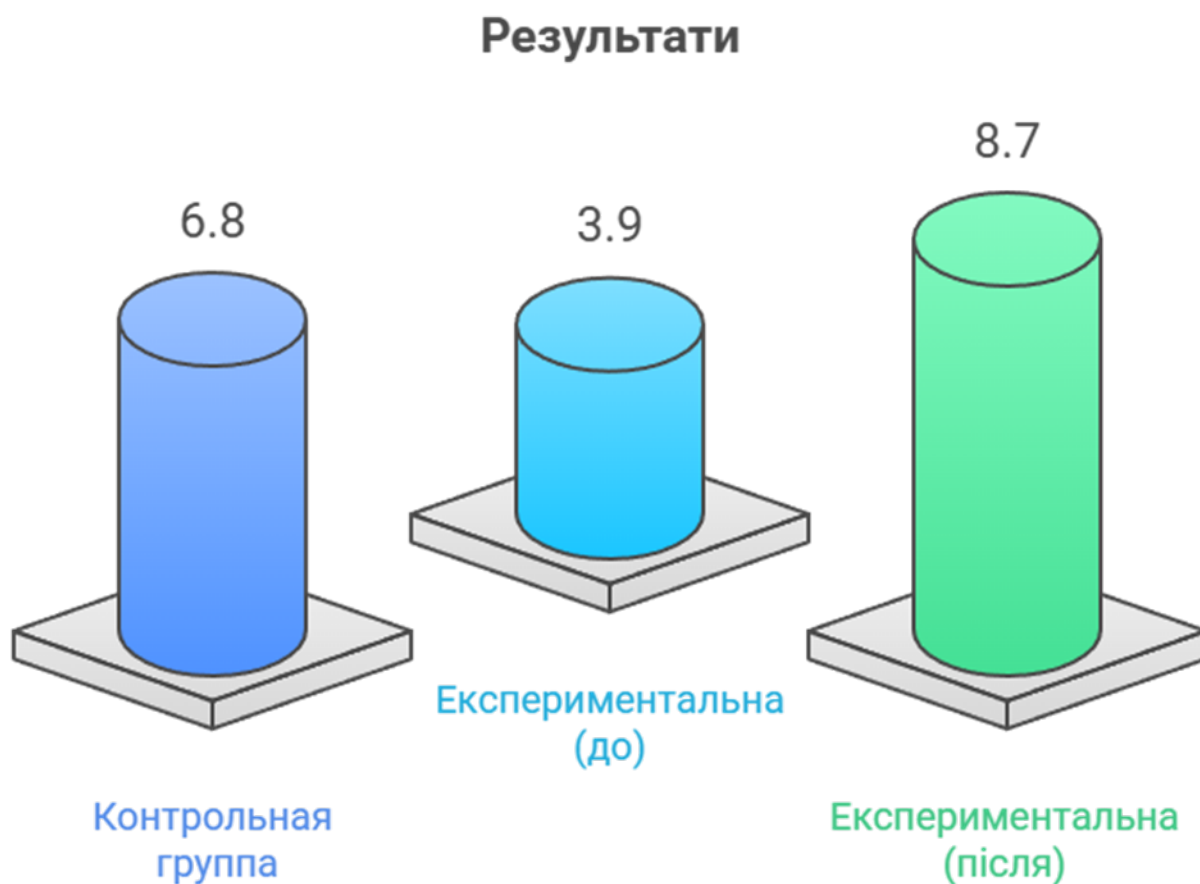


Рис. 1 Результати експериментального дослідження

Методичні рекомендації щодо обов'язкового включення кібербезпеки.

Рекомендація включити до ОПП 4-кредитний обов'язковий модуль «Кібербезпека та захист даних у професійній освіті» (3-4 курс).

Структура дисципліни:

Модуль 1. Теорія та нормативна база та технічні засоби захисту (1 кредит).

Модуль 2. Захист даних в освіті та професійній діяльності (1 кредит).

Модуль 3. Практично-проектна робота (2 кредити).

Також рекомендується активно інтегрувати теми кібербезпеки в дві ключові дисципліни – «Комп'ютерні мережі та захист даних» та «Методика професійного навчання». Це дозволить студентам не тільки вивчати технічні аспекти захисту, а й навчатися, як ефективно передавати ці знання своїм майбутнім учням.

Для оцінки рівня підготовки студентів пропонується використовувати спеціальну матрицю готовності, яка включає 8 показників і має максимум 24 бали. Цю матрицю зручно застосовувати як для поточного, так і для підсумкового контролю.

Приклад матриці оцінювання

Таблиця 1

Приклад результатів студента відповідно матриці оцінювання

№	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	1	3	+2
3	Діяльнісний	Самостійне застосування інструментів	1	3	+2
4	Діяльнісний	Розробка навчальних матеріалів з теми	2	3	+1
5	Мотиваційно-ціннісний	Усвідомлення відповідальності та етичне ставлення	2	3	+1
6	Мотиваційно-ціннісний	Мотивація навчати інших	2	3	+1
7	Особистісно-рефлексивний	Здатність до самоаналізу та рефлексії	2	3	+1
8	Особистісно-рефлексивний	Готовність до самоосвіти	2	2	0
Загальна сума			14	23	+9

Окрім цього, важливо обов'язково включати педагогічну складову: кожен студент повинен самостійно розробити урок, інструкцію або чек-лист з кібергігієни, який можна буде використовувати в роботі з учнями професійно-технічних закладів.

Висновки

Цифрова трансформація професійної освіти 2024-2026 років робить кібербезпеку обов'язковою компетентністю педагога спеціальності 015.39. Експериментально доведено, що запропонована методика забезпечує значний приріст готовності (+49 %) і формує не лише технічні навички, а й педагогічну майстерність. Рекомендується включити 4-кредитний модуль кібербезпеки до всіх ОПП спеціальності 015.39 Професійна освіта (Цифрові

технології) як обов'язковий компонент.

Використана література:

1. Адарюкова Л. Б. Самоосвіта студентів технічних університетів у сфері кібербезпеки. *Вісник Національного університету «Львівська політехніка»*. Серія : Інформаційні системи та мережі. 2024. № 12. С. 78-85.
2. Башуцька О. В. Психолого-педагогічні умови формування цифрової компетентності майбутніх педагогів професійної освіти. *Наукові записки Тернопільського національного педагогічного університету імені Володимира Гнатюка*. Серія : Педагогіка. 2024. № 2. С. 34-42.
3. Білоус О. В. Формування інформаційної безпеки майбутніх педагогів професійної освіти. *Наукові записки Вінницького державного педагогічного університету імені Михайла Коцюбинського*. Серія: Педагогіка і психологія. 2025. Вип. 68. С. 89-97.
4. Дембіцька С. В. Діяльнісний підхід у підготовці педагогів до використання цифрових технологій. *Педагогіка і психологія професійної освіти*. 2023. № 3. С. 56-64.
5. Дзюба С. П. Використання віртуальних лабораторій у підготовці педагогів до викладання кібербезпеки. *Інформаційні технології і засоби навчання*. 2024. № 4 (102). С. 1-14.
6. Stallings W. *Network Security Essentials: Applications and Standards*. 6th ed. Boston : Pearson. 2020. 480 p.
7. Conti M., Dehghantanha A., Franke K., Watson S. Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*. 78, 2018. P. 544-546. DOI: <https://doi.org/10.1016/j.future.2017.07.060>.

References:

1. Adariukova L. B. (2024). Samo-osvita studentiv tekhnichnykh universytetiv u sferi kiberbezpeky [Self-education of students of technical universities in the field of cybersecurity]. *Visnyk Natsionalnoho universytetu «Lvivska politehnika»*. Serii: Informatsiini systemy ta merezhi, (12), 78-85 [in Ukrainian].
2. Bashutska O. V. (2024). Psykholoho-pedahohichni umovy formuvannia tsyfrovoy kompetentnosti maibutnykh pedahohiv profesiinoi osvity. *Naukovi zapysky Ternopilskoho natsionalnoho pedahohichnoho universytetu imeni Volodymyra Hnatiuka*. Serii: Pedahohika, (2), 34-42 [in Ukrainian].
3. Bilous O. V. (2025). Formuvannia informatsiinoi bezpeky maibutnykh pedahohiv profesiinoi osvity. *Naukovi zapysky Vinnytskoho derzhavnoho pedahohichnoho universytetu imeni Mykhaila Kotsiubynskoho*. Serii: Pedahohika i psykholohiia, (68), 89-97 [in Ukrainian].
4. Dembitska S. V. (2023). Diialnisnyi pidkhid u pidhotovtsi pedahohiv do vykorystannia tsyfrovyykh tekhnolohii. *Pedahohika i psykholohiia profesiinoi osvity*, (3), 56-64 [in Ukrainian].
5. Dziuba S. P. (2024). Vykorystannia virtualnykh laboratorii u pidhotovtsi pedahohiv do vykladannia kiberbezpeky. *Informatsiini tekhnolohii i zasoby navchannia*, 102(4), 1-14 [in Ukrainian].
6. Stallings W. (2020). *Network Security Essentials: Applications and Standards*. 6th ed. Boston : Pearson. 480 p. [in English].
7. Conti M., Dehghantanha A., Franke K., Watson S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*. 78. 544-546. DOI: <https://doi.org/10.1016/j.future.2017.07.060> [in English].

N. Shymkiv. Current issues of data protection in the training of future digital technology specialists in the context of digital transformation of vocational education.

The article substantiates the necessity of the mandatory inclusion of cybersecurity and personal data protection topics in the educational programmes of speciality 015.39 “Professional Education (Digital Technologies)” during the period of active digital transformation of vocational (vocational and technical) education in Ukraine in 2024-2026. The study analyses the impact of the introduction of the unified digital system “Mriia,” the Digital Transformation Strategy for Education until 2027, the growth of cyber threats during the wartime period, and the spread of artificial intelligence technologies on the requirements for training future educators.

The article presents an experiment conducted at an educational institution within the framework of speciality 015.39 “Professional Education (Digital Technologies)” and includes sample assessment

tables and experimental results. The developed assessment matrix (8 indicators, 24 points) is presented as a tool for continuous, interim, and final assessment of student performance.

The results of a pedagogical experiment are presented, confirming the effectiveness of the proposed methodology, which includes laboratory work with Wireshark, Cisco Packet Tracer, and VeraCrypt, as well as the case study method and project-based activities with an embedded pedagogical component. Recommendations for implementing a modern data protection curriculum are substantiated.

Purpose the competency matrix, a key element of the educational-professional programme (EPP) that ensures transparency and systematic organisation of specialist training, is analysed. Methodological recommendations are proposed for incorporating a 4-credit module “Cybersecurity and Data Protection in Professional Education” into the syllabi of the courses “Computer Networks and Data Protection” and “Methodology of Professional Training”.

The findings have practical significance for higher education institutions and vocational education institutions.

Keywords: pedagogical methods, educational technologies, practical training, digital technologies, specialist training, adaptive learning, digital transformation, training system.