

Франко Юрій<https://orcid.org/0000-0002-1464-1162>

ResearcherID ABE-6157-2020

Scopus Author ID 8224958800

Кандидат технічних наук,
доцент кафедри комп'ютерних технологій,
Тернопільський національний педагогічний
університет імені Володимира Гнатюка
(м. Тернопіль, Україна) E-mail: franko@tnpu.edu.ua

Шимків Назар<https://orcid.org/0009-0001-2322-5187>

Здобувач третього (освітньо-наукового) рівня вищої освіти
спеціальності 015 Професійна освіта,
Асистент кафедри комп'ютерних технологій,
Тернопільський національний педагогічний
університет імені Володимира Гнатюка
(м. Тернопіль, Україна) E-mail: shymkiv_ni@tnpu.edu.ua

ОСНОВНІ ПОЛОЖЕННЯ ПРАКТИЧНОЇ ПІДГОТОВКИ ФАХІВЦІВ ЦИФРОВИХ ТЕХНОЛОГІЙ У ТЕНДЕНЦІЯХ СЬОГОДЕННЯ

Мета статті – розгляд практичних засобів і їх використання у процесі підготовки фахівців цифрових технологій у реаліях сучасної інформаційної безпеки.

Методологія. У дослідженні застосовано системний і проблемний підходи, а також загальнонаукові методи аналізу, синтезу і порівняння. Це визначає основні вимоги до практичних навичок фахівця у галузі кібербезпеки.

Наукова новизна. У статті подано і проаналізовано основні методи практичної підготовки фахівців цифрових технологій у галузі створення захищених мереж.

Основною метою процесу підготовки фахівців цифрових технологій є не лише теоретичні матеріали і рівень їх засвоєння фахівцем, а й основні практичні навички і вміння їх застосовувати у подальшій реалізації себе як фахівця, педагога і можливості навчати інших. Особливості практичного навчання у сучасному світі, де цифрові технології оточують нас у всіх аспектах нашого життя, є актуальним викликом сьогодення, що активно змінюється і пристосування педагогів до викликів сучасних тенденцій підготовки вимагає від них іти в ногу з темпом розвитку сучасних технологій, які розвиваються дуже стрімко. Запропоновані методи практичного навчання є лише частиною можливостей використання підготовки фахівців, як основа для формування змісту і організації діяльності здобувачів, які хочуть стати фахівцями з кібербезпеки і бути практичними педагогами. Основні аспекти підготовки і класифікація практичних навичок майбутніх фахівців є умовною класифікацією і може бути, як основним так і ознайомлювальним матеріалом для періодизації вивчених навичок та вмінь, які формуються у здобувачів різних рівнів освіти та слухачів різних курсів для здобуття нових знань

Висновки. Запропоновані і порівнянні методи практичного навчання є лише частковим охопленням навичок і створення практичної складової навчання майбутніх фахівців цифрових технологій. Ефективність кожного методу практичного навчання аналізується та є взаємозалежними із багатьма методами теоретичного навчання в освітньому процесі майбутніх фахівців.

Ключові слова: практична підготовка, цифрові технології, система підготовки, фахівці цифрових технологій.

Постановка проблеми у загальному вигляді та її зв'язок з важливими науковими та/або практичними завданнями. Сучасний світ технологій розвивається дуже стрімко викликаючи потребу модернізації сучасних систем освіти у галузях комп'ютерних технологій. Підготовка майбутніх фахівців цифрових технологій в умовах поширення інформаційних систем у різних сферах діяльності суспільства переходить на принципово новий рівень і враховуючи сучасні вимоги, можна сформулювати основні навички якими має володіти фахівець у сфері системного адміністрування та захисту даних.

Тому, практичні навички фахівця галузі кібербезпеки є основою підготовки будь яких здобувачів професійної освіти, а особливо в галузях, які стрімко розвиваються і переплітають собою практично усі сфери діяльності.

Аналіз основних досліджень і публікацій з порушеної проблеми. У наукових дослідженнях практичної підготовки здобувачів приділяють велику увагу складним процеси, які вивчаються на основі їх систематизованого засвоєння знань та навичок їх використання у практичній діяльності.

Формулювання мети статті. Мета статті полягає у формуванні сучасних вимог і практичних навичок для майбутніх фахівців цифрових технологій в умовах стрімкого розвитку цифрового суспільства і зростанню загроз від зловмисників.

Висвітлення процедури теоретико-методологічного дослідження із зазначенням методів дослідження. У дослідженні застосовано проблемний, системний і синергетичний підходи, а також загальнонаукові методи аналізу, синтезу і порівняння. Це сприяло формуванню сучасних практичних навичок педагогів, що демонструє відкриту і динамічну системи підготовки майбутніх фахівців цифрових технологій.

Динамічність і розвиток сучасного світу цифрових технологій змушує розвивати у сучасних фахівців цифрових технологій практичні навички для проведення педагогічної діяльності і відображенні зв'язку між теоретичним відомостями і практичним матеріалом що подається на заняттях при підготовці фахівців [1].

Сучасний світ цифрових технологій, в якому інформаційно-комунікаційні системи проникають і переплітаються із всіма галузями діяльності людини, захист мереж і даних від впливу шкідливих чинників стає критично важливим. Кіберзлочинність, хакерські атаки та витоки даних можуть мати серйозні наслідки для організацій та окремих осіб. Тому підготовка кваліфікованих фахівців у галузі кібербезпеки є потребою сьогодення і актуальною темою для підготовки фахівців.

Провівши аналіз пропозицій у сучасних ЗВО і виділивши основні популярні напрямки підготовки фахівців цифрових технологій із напрямком пов'язаним із захистом інформації та кібербезпекою, можна виділити основну десятку програм оцінивши їх вартість і тривалість із наявних на сьогоднішній день (рис. 1).

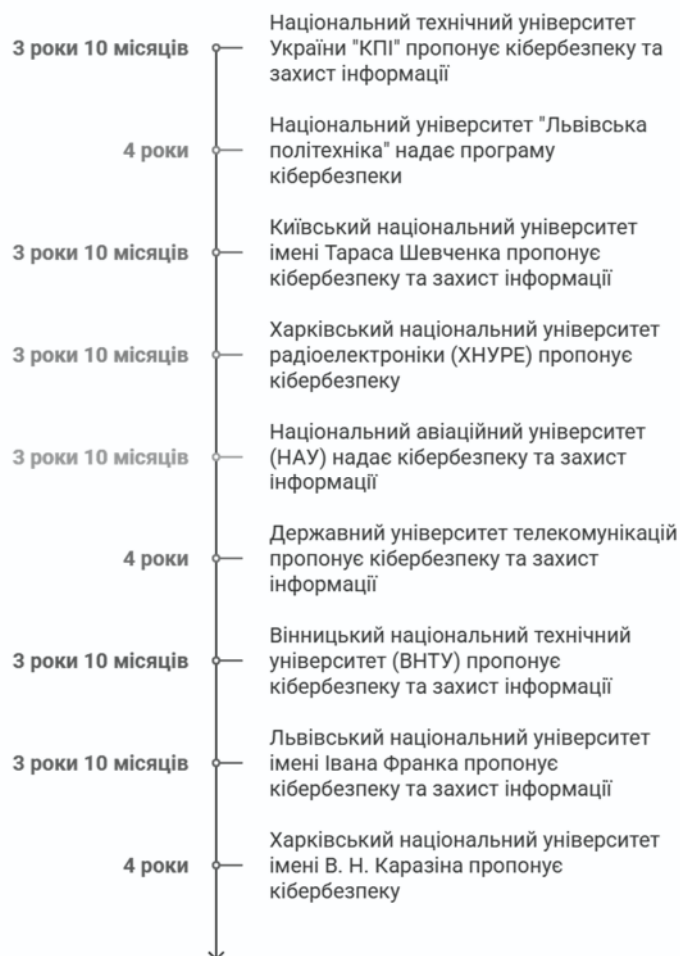


Рис. 1. Назви освітніх програм

У XXI столітті цифрові технології стали невід'ємною частиною повсякденного життя. Разом із ними зросла і потреба в безпеці даних, які передаються й зберігаються в комп'ютерних системах та мережах. Захист інформації набуває стратегічного значення не лише для державного сектору, а й для приватних компаній, освітніх установ, банків та кожного користувача. У зв'язку з цим, професійна освіта у сфері захисту мереж і даних відіграє вирішальну роль у підготовці фахівців, здатних протистояти сучасним кіберзагрозам [1].

Значення кібербезпеки в сучасному світі.

Кібербезпека – це комплекс заходів, методів та інструментів, спрямованих на захист інформаційних систем від несанкціонованого доступу, втрати даних, атак програм-вимагачів, фішингу, зламу паролів та іншого шкідливого впливу [7].

Основні напрями навчання в професійних закладах.

Професійні навчальні заклади України, що готують спеціалістів у галузі кібербезпеки, формують навчальні програми з урахуванням вимог ринку праці та державних стандартів [2, 3]. Основні модулі таких програм зазвичай включають (рис. 2).



Рис. 2. Основні модулі навчальних програм

Методи навчання та підходи.

Навчання поєднує теоретичні та практичні компоненти. Студенти виконують лабораторні роботи, на яких симулюють реальні атаки, та приймають участь в командних хакатонах, розв'язують кейси із захисту мереж, створюють власні проєкти кібербезпеки.

Практична підготовка фахівців реалізується через стажування на підприємствах, роботу в ІТ-компаніях, використання віртуальних тренажерів і платформи для тестування систем на вразливості.

Сучасні освітні технології – такі як дистанційне навчання, платформи для онлайн-тестування, інтерактивні симулятори – активно інтегруються в освітній процес, що дозволяє покращити доступність та гнучкість навчання.

Кваліфікації та професійні можливості випускників.

Після завершення навчання випускники можуть претендувати на такі посади, які наведені на рисунку 3.

Ці професії є одними з найзатребуваніших на сучасному ринку праці. Заробітна плата фахівців з кібербезпеки в Україні має тенденцію до зростання і залежить від досвіду, місця працевлаштування та рівня знань.

Виклики та перспективи галузі.

Серед основних викликів підготовки фахівців можна виділити:

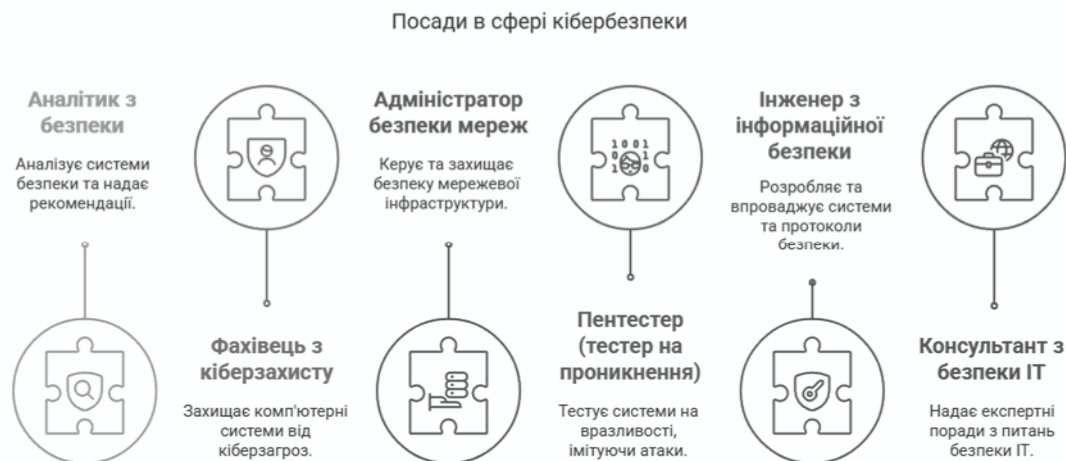


Рис. 3. Перспективні посади випускників

Швидкий розвиток технологій, що вимагає постійного оновлення освітніх програм і сучасних знань викладачів для повного і актуального подання інформації на заняттях.

Недостатня кількість кваліфікованих викладачів у сфері кібербезпеки, яка частково спричинена зовнішніми чинниками, особливо, збройною агресією росії відносно України.

Висока конкуренція за ресурси, їх вартість і вміння застосовувати ці ресурси.

Проте ці виклики супроводжуються й значними перспективами. Кібербезпека вважається однією з галузей, яка швидко розвивається, і галузей в якій дуже важко оцінити перспективи цього розвитку. До основних напрямків розвитку кібербезпеки можна віднести: інвестиції в освіту; міжнародна співпраця; створення центрів компетенцій та регіональних хабів.

Навчання навичкам захисту комп'ютерних мереж та даних у закладах освіти – це не просто освітній процес, а стратегічна інвестиція у безпеку не лише державних структур, а і роботу та функціонування бізнесу, суспільства. Професійні програми з кібербезпеки формують нове покоління експертів, які здатні забезпечити захист критичної інфраструктури, захистити дані користувачів і зробити цифровий простір безпечнішим. В умовах гібридної війни та глобальної цифровізації важливість таких фахівців лише зростатиме [5].

Системна підготовка, міждисциплінарний підхід, практична орієнтація та державна підтримка – основні чинники, що забезпечують ефективність освітнього процесу в галузі кібербезпеки.

Практичні навички студентів при вивченні захисту систем і мереж. Однією з ключових складових якісної підготовки фахівців у галузі кібербезпеки є формування глибоких і всебічних практичних навичок. Безпосередня робота з інформаційними системами, застосування знань у реальних або змодельованих ситуаціях дозволяє студентам не лише краще засвоїти матеріал, а й підготуватися до викликів, які очікують їх у професійній діяльності (рис. 4).

Навички здобувачів, які навчаються за фахом цифрових технологій у галузі захисту мереж і систем [6].

1. Створення та налаштування захищених мереж.

Створення і проєктування мереж на основі сучасних вимог корпоративної безпеки, налаштування впровадження VLAN, базові вміння налаштовувати безпеку на маршрутизаторах, навички сегментування мережі.

2. Адміністрування та захист операційних систем.

Вивчення основних засобів безпечного адміністрування Windows та Linux – розглядається як ключовий етап підготовки. Студенти мають освоїти такі навички як створення облікових записів користувачів з безпековими правами, розуміння основних функцій групових політик, ведення журналу подій та вміння правильно його «читати», впровадження багатфакторної автентифікації та розуміння основних принципів та методів шифрування даних.

3. Використання криптографічних засобів.

Навички такі, як генерація захищених ключів, застосування алгоритмів симетричного та асиметричного шифрування, створення цифрових сертифікатів, організацію VPN-з'єднань, налаштування HTTPS для вебресурсів та реалізацію електронного цифрового підпису є базовими навичками. Це дозволяє студентам оволодіти методами захищеного та шифрованого обміну даними.

4. Аналіз і протидія кіберзагрозам.

Аналіз мережі та систем для вміння виявляти такі проблеми: фішинг; DOS, DDOS; вразливості мережі.

Вивчення поведінки шкідливого програмного забезпечення (ПЗ у контрольованому середовищі (sandbox), використовують інструменти для аналізу трафіку (Wireshark), логів (Splunk) і дійсних загроз.



Рис. 4. Практичні навички здобувачів 1

5. Проведення тестування на проникнення (пентестинг).

Вміння самостійно знаходити вразливості налаштованої системи і мережі за допомогою симуляції атак і можливих вразливостей інфраструктури.

6. Розробка політик безпеки і планів реагування на інциденти.

Особливе місце приділяється створенню документації, інструкцій, карт мережі, правил поведінки користувачів та дій користувачів при виникненні загрози, моделювання кризової ситуації.

7. Автоматизація та скрипти безпеки.

Практичні заняття зводяться не лише до вміння налаштовувати систему, а й практичним навичкам автоматизації та аналізу логів, які мають записувати і зберігати усі сучасні маршрутизатори, використовувати інструменти фільтрації трафіку. Це сприяє підвищенню ефективності та адаптивності систем безпеки.

8. Використання хмарних технологій і захист хмарних сервісів.

У час цифрової трансформації студенти вивчають особливості забезпечення безпеки в AWS, Azure, Google Cloud, Apache Cloudstack. Що значно підвищує безпеку системи, адже віртуалізація сервісів завжди має додатковий ступінь захисту.

9. Робота з SIEM-системами.

На практичних заняттях студенти вивчають базові навички володіння інструментами управління інформацією та подіями безпеки (SIEM) – наприклад, ArcSight, QRadar або Splunk. Вони збирають, аналізують, корелюють дані про події з різних джерел, виявляють загрози й створюють попередження для своєчасного реагування.

10. Командна взаємодія та комунікація.

Практична частина занять формує не лише технічні навички, але й умінню працювати в команді, обмінюватися інформацією, розподіляти ролі, проводити брифінги, вести документацію, аргументовано

пояснювати технічні рішення. Це особливо важливо для роботи у великій організації або під час реагування на інциденти.

Таким чином, система практичної підготовки у сфері захисту систем і мереж формує не лише компетентних, а й адаптивних фахівців, здатних діяти в умовах реальних загроз. Різноманітність завдань, використання актуального ПЗ, моделювання кризових ситуацій – усе це забезпечує високу конкурентоспроможність випускників на ринку праці.

Ефективне викладання дисциплін, пов'язаних із кібербезпекою, вимагає від викладача не лише глибоких теоретичних знань, а й широкого спектру практичних навичок, педагогічної майстерності та здатності постійно адаптуватися до змін у галузі (рис. 5).

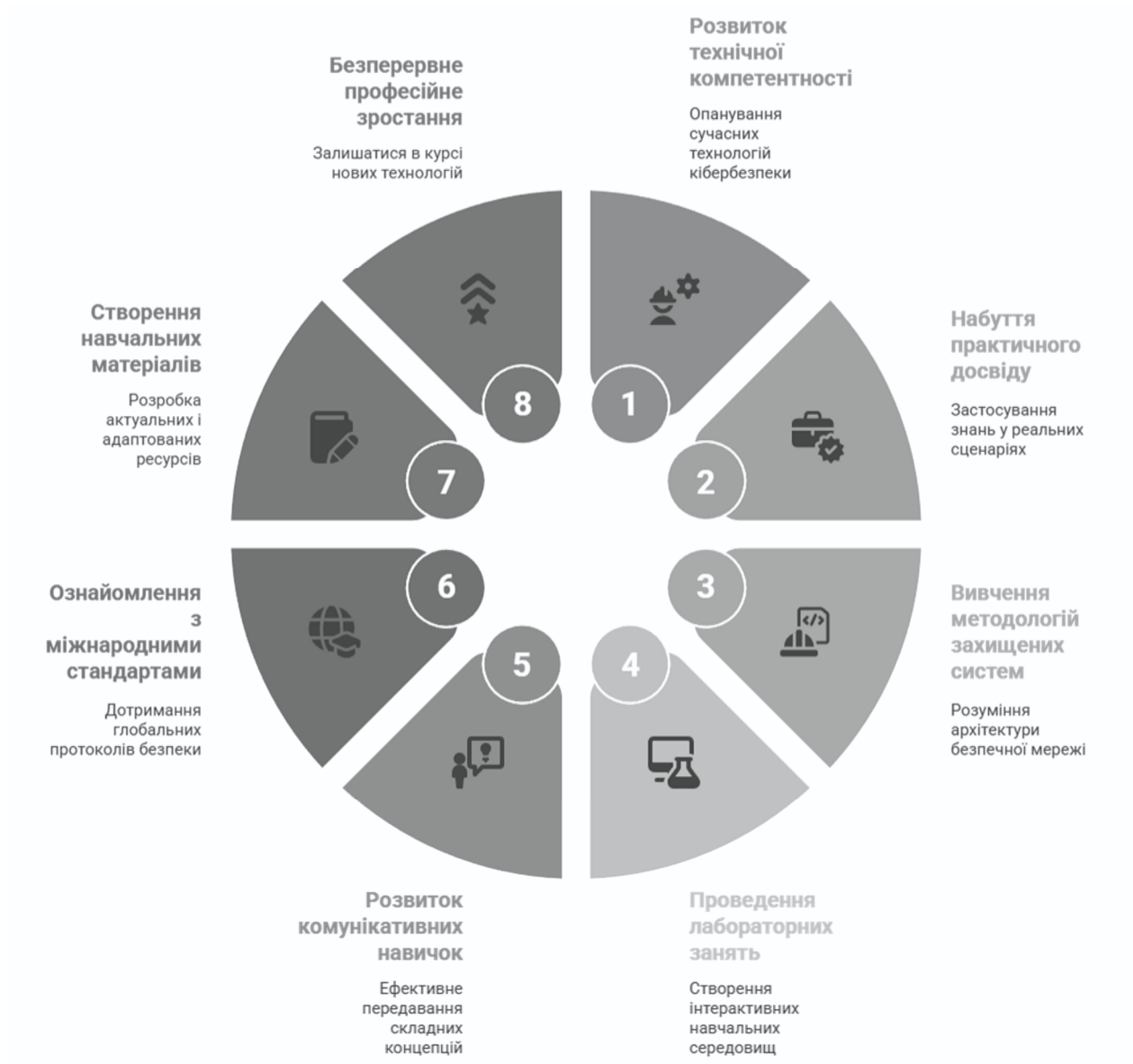


Рис. 5. Компетенції викладача

References

1. Биков В. Ю., Спірін О. М., Пінчук О. П. Проблеми та завдання сучасного етапу інформатизації освіти. *Наукове забезпечення розвитку освіти в Україні: актуальні проблеми теорії і практики (до 25-річчя НАПН України)*. Київ: НАПН України, 2017. С. 191–198. URL: <https://lib.iitta.gov.ua/id/eprint/709026> (дата звернення: 21.03.2024).

- Bykov, V. Yu., Spirin, O. M., Pinchuk, O. P. (2017). Problemy ta zavdannia suchasnoho etapu informatyzatsii osvity [Problems and tasks of the modern stage of education informatization]. *Naukove zabezpechennia rozvytku osvity v Ukraini: aktualni problemy teorii i praktyky (do 25-richchia NAPN Ukrainy) – Scientific Support for the Development of Education in Ukraine: Actual Problems of Theory and Practice (to the 25th Anniversary of the National Academy of Pedagogical Sciences of Ukraine)*. Kyiv, Ukraine: NAPN Ukrainy. 191–198. Retrieved from: <https://lib.iitta.gov.ua/id/eprint/709026> [in Ukrainian].
2. Кібербезпека: негативні наслідки кібератак. *Mklegalservice*. 2020. URL: <https://mklegalservice.com/tpost/4ayrl3aza1-kberbezpeka-negativn-nasldki-kberatak> (дата звернення: 20.03.2025).
Kiberbezpeka: nehatyvni naslidky kiberatak (2020). [Cybersecurity: negative consequences of cyberattacks]. *Mklegalservice*. Retrieved from: <https://mklegalservice.com/tpost/4ayrl3aza1-kberbezpeka-negativn-nasldki-kberatak> [in Ukrainian].
 3. Cybersecurity. Minimize exposure to cyberattacks and build secure and resilient K-12 cyber systems. Retrieved from: <https://www.schoolsafety.gov/cybersecurity> [in English].
 4. Кібербезпека – програма, що готує нове покоління експертів для захисту світу від цифрових загроз. *Kyiv School of Economics*. URL: <https://kse.ua/ua/> (дата звернення: 12.03.2025).
Kiberbezpeka – prohrama, shcho hotuie nove pokolinnia ekspertiv dlia zakhystu svitu vid tsyfrovyykh zahroz [Cybersecurity is a program that trains a new generation of experts to protect the world from digital threats]. *Kyiv School of Economics*. Retrieved from: <https://kse.ua/ua/>. [in Ukrainian]
 5. Освітня програма «Кібербезпека». Маріупольський державний університет. URL: <https://mu.edu.ua/educational-programs/kiberbezpeka> (дата звернення: 14.02.2025).
Osvitnia prohrama «Kiberbezpeka» [Educational program «Cyber Security»]. Mariupolskyi derzhavnyi universytet. Retrieved from: <https://mu.edu.ua/educational-programs/kiberbezpeka>. [in Ukrainian].
 6. Дембіцька С., Кобилянський О. Формування професійної компетентності майбутніх фахівців з професійної освіти засобами цифрових технологій. *Педагогіка безпеки*. 2023. Т. 8, № 1-2. С. 1–7. URL: http://nbuv.gov.ua/UJRN/pedbez_2023_8_1-2_3 (дата звернення: 12.03.2025).
Dembitska, S., Kobylanskyi, O. (2023). Formuvannia profesiinoi kompetentnosti maibutnikh fakhivtsiv z profesiinoi osvity zasobamy tsyfrovyykh tekhnolohii [Developing the professional competence of future vocational education specialists using digital technologies]. *Pedahohika bezpeky – Safety education*. 8. 1-2. 1–7. Retrieved from: http://nbuv.gov.ua/UJRN/pedbez_2023_8_1-2_3. [in Ukrainian].
 7. Франко Ю. П., Гевко І. В., Сіткарь Т. В., Белюх К. В. Системне адміністрування та безпека інформаційних і комунікаційних систем: лабораторний практикум для студентів другого (магістерського) рівня вищої освіти спеціальності 015 Професійна освіта спеціалізації 015.39 Цифрові технології. Тернопіль: ТНПУ ім. В. Гнатюка, 2023. 138 с.
Franko, Yu. P., Nevko, I. V., Sitkar, T. V., Beliukh, K. V. (2023). Systemne administruvannia ta bezpeka informatsiinykh i komunikatsiinykh system: laboratornyi praktykum dlia studentiv druhoho (mahisterskoho) rivnia vyshchoi osvity spetsialnosti 015 Profesiina osvita spetsializatsii 015.39 Tsyfrovii tekhnolohii [System administration and security of information and communication systems: laboratory workshop for second-level (master's) students majoring in 015 Professional Education, specialization 015.39 Digital Technologies]. Ternopil, Ukraine: TNPU im. V. Hnatiuka. 138. [in Ukrainian].
 8. Франко Ю. П., Солонинка М. В. Особливості формування навичок системного адміністрування серверів у студентів технічних коледжів. Актуальні проблеми та перспективи технологічної і професійної освіти: матеріали VII всеукраїнської науково-практичної інтернет-конференції (м. Тернопіль, 20-21 квітня 2023 р.). Тернопіль: ТНПУ ім. В. Гнатюка, 2023. С. 87–89.
Franko, Yu. P., Solonynka, M. V. (2023). Osoblyvosti formuvannia navychok systemnoho administruvannia serveriv u studentiv tekhnichnykh koledzhiv [Features of developing server system administration skills in technical college students]. *Aktualni problemy ta perspektyvy tekhnolohichnoi i profesiinoi osvity: materialy VII vseukrainskoi naukovo-praktychnoi internet-konferentsii (Ternopil, 20.04.2023) – Current issues and prospects for technological and vocational education: materials from the VII All-Ukrainian Scientific and Practical Internet Conference (Ternopil, April 20-21, 2023)*. Ternopil, Ukraine: TNPU im. V. Hnatiuka. 87–89. [in Ukrainian].
 9. Stallings, W. (2020). Network Security Essentials: Applications and Standards. 6th ed. Boston: Pearson. 480. [in English].
 10. 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: 10.1016/j.future.2017.07.060. [in English].

Franko Yuriy<https://orcid.org/0000-0002-1464-1162>

ResearcherID ABE-6157-2020

Scopus Author ID 8224958800

Associate Professor, PhD in Technical Sciences,
Ternopil Volodymyr Hnatiuk National Pedagogical University
(Ternopil, Ukraine) E-mail: franko@tnpu.edu.ua

Shymkiv Nazar<https://orcid.org/0009-0001-2322-5187>

PhD Student, Department of Computer Technologies,
Assistant Lecturer, Department of Computer Technologies,
Ternopil Volodymyr Hnatiuk National Pedagogical University
(Ternopil, Ukraine) E-mail: shymkiv_ni@tnpu.edu.ua

KEY PRINCIPLES OF PRACTICAL TRAINING FOR DIGITAL TECHNOLOGY SPECIALISTS IN THE CONTEXT OF CONTEMPORARY TRENDS

The article explores the practical aspects of training digital technology specialists in the context of modern challenges related to information security. The study emphasizes the importance of developing practical skills alongside theoretical knowledge to ensure effective professional performance and the ability to teach others.

Purpose. This article aims to explore practical tools and their application in the training of digital technology specialists under the conditions of contemporary information security challenges.

Methodology. The study employs a systematic and problem-oriented approach, as well as general scientific methods such as comparative analysis and generalization. This approach helps define the core requirements for the practical skills of cybersecurity professionals.

Scientific Novelty. The article presents and analyzes key methods of practical training for digital technology specialists, particularly in the area of secure network development. The primary objective of training future digital technology specialists is not limited to mastering theoretical knowledge but also focuses on acquiring essential practical skills and the ability to apply them in real-world professional contexts. This includes their potential role as educators capable of teaching others. The unique nature of practical training in today's world, where digital technologies permeate nearly every aspect of daily life, represents a current and evolving challenge. Adapting teachers to the demands of modern training trends requires them to keep pace with rapidly developing technologies. The proposed practical training methods represent only a fraction of the possible approaches to preparing specialists. They serve as a foundation for shaping the content and organization of training activities for learners aspiring to become cybersecurity professionals and hands-on educators. The key aspects of training and the classification of practical skills for future specialists are presented as a conditional framework. This can serve both as core material and as an introductory resource for the staged development of skills and competencies in learners across various educational levels and professional courses.

Conclusions. The proposed and compared methods of practical training represent only a partial coverage of the skills needed. Building the practical component of training for future digital technology specialists is a critical part of the educational process, equally important as theoretical instruction. The effectiveness of each practical training method is analyzed and shown to be interdependent with numerous theoretical teaching methods within the broader educational process for future professionals.

Keywords: practical training, digital technologies, training system, digital technology specialists, cybersecurity.

Стаття надійшла до редакції 11.06.2025 р.

Рецензент: доктор педагогічних наук, професор **Гевко І. В.**