

УДК 378:005.6

DOI <https://doi.org/10.24919/2308-4863/92-1-47>

Анатолій ДМИТРУК,
orcid.org/0000-0002-2393-0193

доктор філософії,
асистент кафедри прикладної математики
Національного університету «Львівська політехніка»
(Львів, Україна) anatolii.a.dmytruk@lpnu.ua

Христина ПИНЯГА,
orcid.org/0009-0009-9737-0940

студентка II курсу факультету прикладної математики
Національного університету «Львівська політехніка»
(Львів, Україна) khrystyna.pyniaha.pm.2024@lpnu.ua

ПЕДАГОГІЧНІ ЗАСАДИ СТРУКТУРУВАННЯ КУРСУ «КРИПТОГРАФІЯ» У ПРОФЕСІЙНІЙ ПІДГОТОВЦІ ІТ-ФАХІВЦІВ

У статті розглянуто педагогічні засади структурування курсу «Криптографія» в системі професійної підготовки майбутніх фахівців з інформаційних технологій. Актуальність дослідження зумовлена потребою адаптації освітнього процесу до умов цифрової трансформації суспільства та зростанням ролі кібербезпеки як ключової складової цифрової компетентності. Метою статті є визначення теоретичних і методичних основ побудови курсу «Криптографія» як міждисциплінарної складової підготовки ІТ-фахівців.

У процесі дослідження використано комплекс теоретичних і емпіричних методів: аналіз і синтез наукових джерел, педагогічне проєктування, моделювання, спостереження за освітнім процесом та узагальнення досвіду викладання дисциплін цифрового профілю. Це дало змогу розробити дидактичну структуру курсу, яка поєднує фундаментальні математичні знання, програмно-інженерні навички та етичні аспекти цифрової безпеки.

Результати дослідження подано у вигляді чотирьох модулів: мотиваційного (формування усвідомлення цифрових ризиків), теоретичного (оволодіння математичними та історичними основами криптографії), практичного (застосування алгоритмів шифрування у сучасних програмних середовищах) і креативно-дослідницького (розвиток критичного мислення, участь у мініпроєктах, етична рефлексія). Така структура забезпечує формування когнітивних, технологічних і ціннісних компетентностей, необхідних для професійної діяльності у сфері інформаційної безпеки.

Підкреслено, що курс «Криптографія» може виступати моделлю інтегрованого навчального середовища, у якому поєднуються наука, технологія та гуманітарна складова цифрової культури. Перспективи подальших досліджень полягають у розробленні методичних рекомендацій для викладачів, створенні електронних освітніх ресурсів і вивченні ефективності застосування гейміфікації та технологій штучного інтелекту у процесі підготовки ІТ-фахівців.

Ключові слова: криптографія, професійна підготовка, цифрова трансформація освіти, кібербезпека, STEM-освіта, компетентнісний підхід, міждисциплінарність.

Anatolii DMYTRUK,
orcid.org/0000-0002-2393-0193

Doctor of Philosophy (PhD),
Assistant Lecturer at the Department of Applied Mathematics
Lviv Polytechnic National University
(Lviv, Ukraine) anatolii.a.dmytruk@lpnu.ua

Khrystyna PYNIAHA,
orcid.org/0009-0009-9737-0940

2nd year student of the Faculty of Applied Mathematics
Lviv Polytechnic National University
(Lviv, Ukraine) khrystyna.pyniaha.pm.2024@lpnu.ua

PEDAGOGICAL PRINCIPLES OF STRUCTURING THE COURSE “CRYPTOGRAPHY” IN THE PROFESSIONAL TRAINING OF IT SPECIALISTS

The article examines the pedagogical foundations of structuring the course “Cryptography” within the professional training system of future information technology specialists. The relevance of the research is determined by the need

to adapt the educational process to the conditions of digital transformation and to strengthen cybersecurity as a key component of digital competence. The purpose of the study is to define the theoretical and methodological basis for designing a multidisciplinary course in cryptography aimed at developing both cognitive and practical skills in the field of information protection.

A set of theoretical and empirical methods was applied, including the analysis and synthesis of scientific sources, pedagogical design, modeling, observation of the educational process, and generalization of teaching experience in digital disciplines. The proposed didactic model combines fundamental mathematical knowledge, programming and engineering skills, and the ethical dimension of digital security.

The course structure includes four modules: motivational (raising awareness of digital risks), theoretical (mastering the mathematical and historical foundations of cryptography), practical (implementation of encryption algorithms in programming environments), and creative-research (developing critical thinking and ethical reflection). This structure promotes the formation of cognitive, technological, and value-based competencies essential for the professional activity of IT specialists in the field of cybersecurity.

It is concluded that the course "Cryptography" can serve as an integrated educational model that unites science, technology, and the humanistic aspects of digital culture. Further research should focus on methodological recommendations for instructors, the development of electronic learning tools, and studying the effectiveness of gamification and artificial intelligence technologies in teaching information security disciplines.

Key words: cryptography, professional training, digital transformation of education, cybersecurity, STEM education, competency-based approach, interdisciplinarity.

Постановка проблеми. Сучасні процеси цифровізації освіти зумовлюють необхідність переосмислення змісту професійної підготовки фахівців технічного профілю, зокрема у сфері інформаційної безпеки. Одним із найважливіших напрямів підготовки майбутніх ІТ-фахівців є опанування основ криптографії як теоретичної та прикладної дисципліни, що забезпечує формування компетентностей із захисту інформації та кібербезпеки (ЦТО, 2024: 12).

Попри зростання уваги до проблеми цифрової компетентності та безпеки, педагогічне проектування курсів криптографічного спрямування залишається недостатньо систематизованим. У науковій літературі наголошується, що ефективна професійна підготовка в умовах цифрової трансформації можлива лише за умови інтеграції фундаментальної математичної підготовки, прикладного програмування, інженерних технологій і цифрової етики (ЦТВНОС, 2024: 14–16; Магілевський, 2025: 116).

Дослідники цифрової освіти (Смутчак, Карташова, Сорочан, Овдійчук, Морзе, Кузьмінська та ін.) підкреслюють, що формування цифрової компетентності майбутніх фахівців передбачає розвиток не лише технічних умінь, а й критичного мислення, інформаційної культури та усвідомленої поведінки у цифровому середовищі (ЦТО, 2024: 24–26; Овдійчук, 2025: 65). Це вимагає переосмислення дидактичних моделей навчання у технічних університетах та розроблення нових курсів, зорієнтованих на компетентнісний і міждисциплінарний підходи.

Паралельно у педагогічних дослідженнях зростає роль STEM/STEAM-підходів, що забезпечують інтеграцію природничих, технічних і математичних дисциплін (Олійник та ін., 2020: 130;

Bybee, 2013: 58; Honey et al., 2014: 32). Такий підхід є особливо релевантним для курсу «Криптографія», який поєднує теоретичні знання з математичної логіки, алгебри, теорії чисел із практикою програмування, алгоритмізації та застосування сучасних засобів захисту даних.

Водночас сучасні освітні стандарти (IEEE/ACM, 2022: 7) наголошують на необхідності включення криптографії, безпечного програмування, управління ризиками та цифрової етики до навчальних програм з інформаційних технологій. Такі рекомендації узгоджуються з національними тенденціями впровадження кібербезпекових елементів у підготовку ІТ-фахівців (Магілевський, 2025: 112).

У міжнародних дослідженнях також обґрунтовується необхідність спеціального конструювання змісту курсу криптографії відповідно до рівня підготовки студентів та вимог галузі (Alhamdani, Griskell, 2005: 31).

З педагогічної точки зору проблема полягає у відсутності структурованої моделі курсу «Криптографія», що враховувала б когнітивний, діяльнісний та ціннісний компоненти навчання. Традиційні підходи часто або надмірно теоретизовані, або обмежуються інструментальними аспектами, що ускладнює формування у студентів системного бачення процесів захисту інформації (Грбовський, 2015: 136; Ягупов, 2011: 29).

Отже, постає необхідність розроблення педагогічно обґрунтованої структури курсу з криптографії, яка інтегрує математичну теорію, інженерну практику та етику цифрової безпеки, забезпечуючи цілісне формування професійних компетентностей майбутніх ІТ-фахівців.

Аналіз досліджень. Проблематика професійної підготовки майбутніх фахівців ІТ-галузі в умо-

вах цифровізації освіти активно розробляється в сучасній педагогіці. Дослідники підкреслюють, що цифрова трансформація навчального процесу змінює методологічні підходи до організації навчання, висуваючи вимогу інтеграції традиційних знань із цифровими компетентностями (ЦТО 2024: 25).

Суттєвий внесок у формування теоретичних засад цифрової освіти зробили українські вчені В. Сергієнко, Н. Франчук, В. Овдійчук, Н. Морзе, О. Кузьмінська, які визначають цифрову компетентність як інтегральну характеристику фахівця, що поєднує інформаційну культуру, технічну грамотність і відповідальне ставлення до технологій (Овдійчук, 2025: 67). Їхні підходи узгоджуються з ідеями розвитку інноваційного освітнього середовища, де важливими стають гнучкість, адаптивність і міждисциплінарність навчального змісту (ЦТО, 2024: 24–26).

У межах концепції STEM/STEAM-освіти акцент зроблено на інтеграції природничих, технічних і математичних дисциплін, що формує аналітичне мислення та здатність розв'язувати комплексні завдання (Олійник та ін., 2020: 136; Bybee, 2013: 58; Honey et al., 2014: 32). Для курсу «Криптографія» цей підхід є методологічно доцільним, оскільки поєднує фундаментальні знання з математики з практикою програмування та розробок у сфері безпеки даних.

Дослідники цифрової освіти відзначають, що поєднання теоретичної та практичної підготовки в умовах цифрової трансформації є найбільш ефективним у форматі змішаних моделей навчання. Використання хмарних сервісів та віртуальних лабораторій дозволяє організувати навчальний процес як гнучке інтерактивне середовище, у якому студент отримує можливість самостійного аналізу, перевірки рішень і поступового ускладнення навчальних задач. Такий підхід сприяє формуванню навичок самоосвіти, дослідницької діяльності та аналітичного мислення (ЦТВНОС, 2024: 165, 188, 197).

Питання інтеграції елементів кібербезпеки в освітні програми висвітлено у працях В. Магілевського, Д. Ніколаєва, Г. Бреда, Р. Прасада, які наголошують на необхідності узгодження академічного навчання з практичним опануванням технологій захисту інформації (Магілевський, 2025: 112). У міжнародних дослідженнях (Moore et al., 2022: 6131; Papadakis, 2021: 79) підкреслюється роль дисципліни «Криптографія» в розвитку етичної культури поведінки з цифровими даними, а також важливість навчання через практику та кейси.

Важливим елементом методологічного забезпечення є міжнародні стандарти (IEEE/ACM,

2022: 7), які рекомендують включення до програм навчання модулів із криптографії, безпечного програмування, управління ризиками та цифрової етики. Ці положення підтримуються українськими педагогами, які акцентують на потребі формування відповідальної цифрової поведінки й етики (Сугоняк та ін., 2022: 294; Грабовський, 2015: 134).

Отже, аналіз літератури свідчить, що хоча питання цифрової освіти, STEM-інтеграції та кібербезпеки активно досліджуються, педагогічні засади побудови курсу «Криптографія» залишаються недостатньо розробленими. Відсутня узгоджена модель, яка б забезпечувала єдність математичної, технологічної та етичної складових професійної підготовки майбутніх ІТ-фахівців.

Мета статті. Враховуючи результати проведеного аналізу наукових джерел та виявлену потребу в педагогічному обґрунтуванні побудови курсу «Криптографія» у системі професійної підготовки ІТ-фахівців, сформульовано мету дослідження – визначити та теоретично обґрунтувати педагогічні засади структурування курсу «Криптографія» як складової професійної підготовки майбутніх фахівців з інформаційних технологій.

Для досягнення поставленої мети передбачалося розв'язати такі завдання:

1. Проаналізувати сучасні підходи до викладання дисциплін цифрового профілю у закладах вищої освіти.
2. Визначити основні дидактичні принципи проєктування курсу з криптографії в контексті компетентнісного, STEM/STEAM-орієнтованого та міждисциплінарного підходів.
3. Розробити логіко-структурну модель курсу, що поєднує мотиваційний, теоретичний, практичний і креативно-дослідницький модулі.
4. Обґрунтувати методичні умови ефективного засвоєння навчального матеріалу з урахуванням інтеграції фундаментальної (математичної) та прикладної (інженерно-програмної) підготовки.

Виклад основного матеріалу. Проєктування навчального курсу «Криптографія» у системі професійної підготовки ІТ-фахівців передбачає поєднання фундаментальних математичних знань, прикладних навичок програмування, елементів інженерії та етики цифрової безпеки. Зміст курсу побудовано відповідно до принципів компетентнісного, міждисциплінарного та STEM/STEAM-підходів, які забезпечують цілісність навчального процесу та формування у студентів аналітичного мислення, здатності до інноваційної діяльності й критичної оцінки інформаційних ризиків.

Мотиваційний блок: формування усвідомлення цифрових ризиків. Початковий модуль курсу спрямований на створення у студентів уявлення про акту-

альні проблеми цифрової безпеки. Здобувачі освіти знайомляться з видами загроз – фішингом, зламами паролів, витоком персональних даних, підміною ідентичності – та їх соціальними наслідками.

Обговорення реальних кейсів (наприклад, втрати баз даних великими компаніями або злами державних серверів) сприяє формуванню ціннісно-мотиваційної складової компетентності – розуміння значущості захисту інформації.

На цьому етапі відбувається діагностика початкового рівня цифрової грамотності, анкетування щодо досвіду безпечної поведінки в мережі, що допомагає викладачу адаптувати подальший зміст до індивідуальних потреб групи.

Таким чином, мотиваційний блок виконує функцію усвідомленого входження студента в предметну сферу криптографії та забезпечує когнітивну готовність до вивчення складних теоретичних тем.

Теоретичний блок: фундаментальні та історичні основи. Другий модуль присвячено розвитку системного бачення криптографії як науки. Студенти знайомляться з її еволюцією – від античних шифрів (цезаревого, вігнерового) до сучасних методів симетричного, асиметричного та квантового шифрування.

Теоретична частина курсу має два взаємопов'язаних напрями:

Історико-науковий – демонструє розвиток ідей криптографії як відповіді на нові виклики інформаційної безпеки, що формує в студентів розуміння логіки наукового поступу та значення міждисциплінарності.

Математико-алгоритмічний – розкриває використання теорії чисел, алгебри, модульної арифметики, комбінацій і ймовірності у створенні криптосистем.

Вивчення цих тем сприяє формуванню когнітивної компетентності – здатності оперувати математичними моделями процесів шифрування, розуміти їхню стійкість і межі застосування.

Для підвищення мотивації використовуються інтерактивні методи – математичні ігри з кодування повідомлень, командні задачі з дешифрування тощо. Для створення індивідуалізованих навчальних завдань широко застосовуються інструменти штучного інтелекту, що дозволяє підвищити залученість і забезпечити диференціацію навчання (Dmytruk et al., 2025).

Практичний блок: застосування алгоритмів і технологій. На цьому етапі основна увага приділяється практичному застосуванню знань. Здобувачі освіти опановують програмні інструменти та бібліотеки криптографії, зокрема Python

(PyCryptodome, cryptography), C++ (Crypto++, OpenSSL), Java (javax.crypto), JavaScript (Web Crypto API).

Практичні завдання передбачають:

- реалізацію класичних алгоритмів шифрування (AES, RSA, DES);
- створення цифрових підписів та перевірку автентичності даних;
- аналіз слабких місць реалізації алгоритмів;
- моделювання типових кібератак у контрольованому середовищі (white hacking).

Такий формат роботи дозволяє сформувати операційно-технологічну компетентність – уміння застосовувати криптографічні алгоритми для вирішення реальних завдань, оцінювати їх ефективність і безпечність.

Паралельне вивчення математики та програмування забезпечує інтеграцію теоретичного і практичного навчання, що відповідає принципам інженерно-прикладної освіти.

Креативно-дослідницький блок: розвиток критичного мислення. Заключний модуль курсу орієнтовано на формування аналітико-дослідницької компетентності. Студенти залучаються до виконання міні-проектів і досліджень, спрямованих на аналіз сучасних загроз, розроблення нових підходів до захисту даних або оцінювання ефективності існуючих протоколів.

Особливе місце відведено ознайомленню з основами криптоаналізу, що допомагає майбутнім фахівцям усвідомити, як порушуються системи шифрування, і чому без глибокого розуміння цих процесів неможливо створити надійну систему захисту.

Методи навчання – кейс-стаді, дослідницькі мінігрупи, елементи гейміфікації, моделювання ситуацій із реальних атак – сприяють розвитку критичного мислення, креативності та професійної рефлексії.

Компетентнісний результат. Після завершення курсу студенти повинні продемонструвати сформованість таких результатів навчання:

№	Компетентність	Очікувані результати навчання
1.	Цифрова та інформаційна	Усвідомлює загрози кіберпростору, розуміє принципи захисту даних
2.	Математична	Застосовує математичні моделі шифрування і дешифрування
3.	Інженерно-програмна	Реалізує алгоритми криптографії у програмному середовищі
4.	Етична	Дотримується принципів цифрової відповідальності, конфіденційності
5.	Дослідницька	Аналізує ефективність методів криптографії, пропонує інновації

Таким чином, курс «Криптографія» виступає не лише засобом фахової підготовки, а й моделлю інтегрованого навчального середовища, що об'єднує фундаментальні знання, практичний досвід і гуманістичні орієнтири цифрової доби.

Висновки. У процесі дослідження обґрунтовано педагогічні засади побудови курсу «Криптографія» як складової професійної підготовки майбутніх ІТ-фахівців у контексті цифрової трансформації освіти. Проаналізовано сучасні підходи до структурування змісту дисциплін цифрового профілю, які ґрунтуються на компетентнісному, STEM/STEAM-орієнтованому та міждисциплінарному підходах.

Розроблена структура курсу складається з чотирьох логічно взаємопов'язаних модулів. Мотиваційного, що забезпечує усвідомлення студентами ролі криптографії в системі цифрової безпеки та формує ціннісно-мотиваційний компонент професійної компетентності. Теоретичного, у якому узагальнено історичний розвиток криптографії та розкрито її математичні засади, що забезпечують формування когнітивної компетентності. Практичного, спрямованого на розвиток операційно-

технологічних умінь через використання сучасних криптографічних бібліотек і програмних середовищ. Креативно-дослідницького, що формує навички аналітичного мислення, самостійного пошуку інноваційних рішень і відповідального ставлення до етичних аспектів цифрової безпеки.

Завдяки інтеграції фундаментальної (математичної) та прикладної (програмної й інженерної) підготовки курс виконує функцію міждисциплінарного освітнього середовища, у якому поєднуються теоретичні знання, практичні навички та етичні орієнтири цифрової доби. Його реалізація сприятиме підготовці фахівців нового типу – здатних не лише користуватися засобами захисту інформації, а й проєктувати їх, оцінювати вразливості систем і формувати культуру безпечної поведінки в інформаційному просторі.

Перспективи подальших досліджень полягають у розробленні методичних рекомендацій для викладачів щодо реалізації курсу «Криптографія» у різних освітніх програмах, створенні електронних навчальних ресурсів і вивченні ефективності інтеграції елементів гейміфікації та штучного інтелекту в освітній процес підготовки ІТ-фахівців.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Цифрова трансформація освіти: теоретико-методичні засади : монографія / за заг. ред. В. П. Сергієнка ; за наук. ред. Н. П. Франчук. – Київ : Вид-во Українського державного університету імені Михайла Драгоманова, 2024. – 382 с.
2. Ягупов В. В. Компетентнісний підхід до професійної підготовки майбутніх фахівців у системі професійно-технічної освіти. Креативна педагогіка. 2011. № 4. С. 28–34.
3. Сугоняк І. І., Коротун О. В., Марчук Г. В., Хропонюк О. Ю. Розробка та використання системи дистанційного навчання «eLearning» у закладах вищої освіти. Information Technologies and Learning Tools. 2022. Т. 87, № 1. С. 288–305. DOI: 10.33407/itlt.v87i1.4231.
4. Цифрова трансформація відкритих науково-освітніх середовищ : монографія / Ін-т цифровізації освіти НАПН України ; [колектив авторів ; за ред. О. М. Спіріна, О. П. Пінчук]. Київ, 2024. 308 с.
5. Олійник В. В., Самойленко О. М., Бацуровська І. В., Доценко Н. А. STEM-освіта в системі підготовки майбутніх інженерів. Information Technologies and Learning Tools. 2020. Т. 80, № 6. С. 127–139. DOI: 10.33407/itlt.v80i6.3635.
6. Овдійчук В. Цифрова компетентність як одна з базових компетентностей майбутніх учителів інформатики. Education Innovation Practice. 2025. Т. 13, № 3. С. 64–69. DOI: 10.31110/2616-650X-vol13i3-010.
7. Грабовський П. П. Критерії, показники і рівні розвитку інформаційної компетентності вчителя природничо-математичних предметів. Інформаційні технології в освіті. 2015. № 24. С. 134–146. <https://ekhsuir.kspu.edu/handle/123456789/17452>.
8. Магілевський В. В. Сучасні аспекти захисту інформації в освітньому середовищі цифрової доби. Інноваційна педагогіка. 2025. Вип. 83, т. 2. С. 111–117. DOI: 10.32782/2663-6085/2025.83.2.22.
9. Alhamdani W., Griskell I. J. A proposed curriculum of cryptography courses. Proceedings of the 6th Conference on Information Technology Education (SIGITE). 2005. P. 31–36. DOI: 10.1145/1107622.1107625.
10. Bybee R. W. The Case for STEM Education: Challenges and Opportunities. Arlington, VA: National Science Teachers Association Press, 2013. 206 p.
11. Dmytruk A., Hrytsiv V., Babkina M., Skril I., Vyslobodska I., Smilevska M. Integration of artificial intelligence technologies into the digital transformation of professional higher education in technical fields. In V. Dmytruk (Ed.), PROFESSIONAL EDUCATION AND PERSONNEL TRAINING, pp. 110–143. Kharkiv: TECHNOLOGY CENTER PC, 2025. <https://doi.org/10.15587/978-617-8360-16-0.ch5>
12. Honey M., Pearson G., Schweingruber H. (Eds.). STEM Integration in K–12 Education: Status, Prospects, and an Agenda for Research. Washington, DC: National Academies Press, 2014. 272 p.
13. IEEE/ACM Joint Task Force on Computing Curricula. Curriculum Guidelines for Undergraduate Degree Programs in Computing. New York: ACM Press, 2022. 192 p.
14. Moor C., Shah P., Chandran L., Papadakis S. Cybersecurity Education in Higher Institutions: From Theory to Practice. Education and Information Technologies, 2022, Vol. 27, No. 5, pp. 6127–6145.
15. Papadakis S. Digital Ethics and Responsible Behavior in Cybersecurity Education. International Journal of Emerging Technologies in Learning (iJET), 2021, Vol. 16, No. 12, pp. 75–85.

REFERENCES

1. Sergiienko, V. P. (ed.), Franchuk, N. P. (scient. ed.). (2024). *Tsyfrova transformatsiia osvity: teoretyko-metodychni zasady* [Digital transformation of education: theoretical and methodological principles]. Kyiv: Vyd-vo Ukrainського derzhavnogo universytetu imeni Mykhaila Drahomanova. 382 p. [in Ukrainian].
2. Yahupov, V. V. (2011). Kompetentnisnyi pidkhid do profesiinoi pidhotovky maibutnikh fakhivtsiv u systemi profesiino-tekhnichnoi osvity [Competence-based approach to professional training of future specialists in the system of vocational education]. *Kreatyvna pedahohika*, (4), 28–34. [in Ukrainian].
3. Suhoniak, I. I., Korotun, O. V., Marchuk, H. V., Khroponok, O. Yu. (2022). Rozrobka ta vykorystannia systemy dystantsiinoho navchannia “eLearning” u zakladakh vyshchoi osvity [Development and use of the eLearning distance learning system in higher education institutions]. *Information Technologies and Learning Tools*, 87(1), 288–305. <https://doi.org/10.33407/itlt.v87i1.4231> [in Ukrainian].
4. Spirin, O. M., Pinchuk, O. P. (eds.). (2024). *Tsyfrova transformatsiia vidkrytykh naukovo-osvitnikh seredovyshech* [Digital transformation of open scientific and educational environments]. Kyiv: Instytut tsyfrovizatsii osvity NAPN Ukrainy. 308 p. [in Ukrainian].
5. Oliinyk, V. V., Samoilenko, O. M., Batsurovska, I. V., Dotsenko, N. A. (2020). STEM-osvita v systemi pidhotovky maibutnikh inzheneriv [STEM education in the system of training future engineers]. *Information Technologies and Learning Tools*, 80(6), 127–139. <https://doi.org/10.33407/itlt.v80i6.3635> [in Ukrainian].
6. Ovdychuk, V. (2025). Tsyfrova kompetentnist yak odna z bazovykh kompetentnostei maibutnikh uchyteliv informatyky [Digital competence as one of the basic competencies of future computer science teachers]. *Education Innovation Practice*, 13(3), 64–69. <https://doi.org/10.31110/2616-650X-vol13i3-010> [in Ukrainian].
7. Hrabovskyi, P. P. (2015). Kryterii, pokaznyky i rivni rozvytku informatsiinoi kompetentnosti vchytelia pryrodnycho-matematychnykh predmetiv [Criteria, indicators and levels of development of information competence of science teachers]. *Informatsiini tekhnologii v osviti*, (24), 134–146. URL: <https://ekhsuir.kspu.edu/handle/123456789/17452> [in Ukrainian].
8. Mahilevskyi, V. V. (2025). Suchasni aspekty zakhystu informatsii v osvitnomu seredovyshechi tsyfrovoy doby [Modern aspects of information security in the digital educational environment]. *Innovatsiina pedahohika*, 83(2), 111–117. <https://doi.org/10.32782/2663-6085/2025.83.2.22> [in Ukrainian].
9. Alhamdani, W., & Griskell, I. J. (2005). A proposed curriculum of cryptography courses. In *Proceedings of the 6th Conference on Information Technology Education (SIGITE)* (pp. 31–36). <https://doi.org/10.1145/1107622.1107625>
10. Bybee, R. W. (2013). *The Case for STEM Education: Challenges and Opportunities*. Arlington, VA: National Science Teachers Association Press. 206 p.
11. Dmytruk, A., Hrytsiv, V., Babkina, M., Skril, I., Vyslobodska, I., & Smilevska, M. (2025). Integration of artificial intelligence technologies into the digital transformation of professional higher education in technical fields. In V. Dmytruk (Ed.), *PROFESSIONAL EDUCATION AND PERSONNEL TRAINING* (pp. 110–143). Kharkiv: TECHNOLOGY CENTER PC. <https://doi.org/10.15587/978-617-8360-16-0.ch5>
12. Honey, M., Pearson, G., & Schweingruber, H. (Eds.). (2014). *STEM Integration in K–12 Education: Status, Prospects, and an Agenda for Research*. Washington, DC: National Academies Press. 272 p.
13. IEEE/ACM Joint Task Force on Computing Curricula. (2022). *Curriculum Guidelines for Undergraduate Degree Programs in Computing*. New York: ACM Press. 192 p.
14. Moor, C., Shah, P., Chandran, L., & Papadakis, S. (2022). Cybersecurity education in higher institutions: From theory to practice. *Education and Information Technologies*, 27(5), 6127–6145. <https://doi.org/10.1007/s10639-022-11033-3>
15. Papadakis, S. (2021). Digital ethics and responsible behavior in cybersecurity education. *International Journal of Emerging Technologies in Learning (iJET)*, 16(12), 75–85. <https://doi.org/10.3991/ijet.v16i12.23681>

Дата першого надходження рукопису до видання: 28.10.2025

Дата прийнятого до друку рукопису після рецензування: 28.11.2025

Дата публікації: 19.12.2025