

УДК 37:004.65

DOI: 10.31499/2307-4914.2(32).2025.348585

ФОРМУВАННЯ ЗМІСТУ КУРСУ «ЗАХИСТ ІНФОРМАЦІЇ» ДЛЯ МАЙБУТНІХ ВЧИТЕЛІВ ІНФОРМАТИКИ

Ірина Лупан, кандидат педагогічних наук, доцент, доцент кафедри інформаційних та цифрових технологій, Центральноукраїнський державний університет імені Володимира Винниченка.

ORCID: 0000-0002-4791-0445

E-mail: ilupan@cuspu.edu.ua

Анна Пузікова, кандидат фізико-математичних наук, доцент кафедри інформаційних та цифрових технологій, Центральноукраїнський державний університет імені Володимира Винниченка.

ORCID: 0000-0002-6843-5583

E-mail: a.v.puzikova@cuspu.edu.ua

У статті обґрунтовано зміст програми навчальної дисципліни «Захист інформації» для студентів спеціальності «Середня освіта» (Інформатика)». Наведено відповідність змісту запропонованого курсу фаховим компетентностям майбутніх вчителів інформатики та результатам навчання здобувачів середньої освіти. Зроблено висновки про те, що запропонований зміст враховує сучасні нормативні вимоги до шкільної інформатичної освіти, а також очікування ІТ-компаній щодо цифрових компетентностей випускників шкіл.

Ключові слова: захист даних; інформаційна безпека; захист баз даних; підготовка майбутніх вчителів інформатики; компетентності; освітня програма; очікувані результати навчання; шкільний курс інформатики.

FORMATION OF THE COURSE “INFORMATION PROTECTION” CONTENT FOR FUTURE TEACHERS OF COMPUTER SCIENCE

Iryna Lupan, Candidate of Pedagogical Sciences, Associate Professor, Associate Professor at the Department of Information and Digital Technologies, Volodymyr Vynnychenko Central Ukrainian State University.

ORCID: 0000-0002-4791-0445

E-mail: ilupan@cuspu.edu.ua

Anna Puzikova, Candidate of Physical and Mathematical Sciences, Associate Professor, Associate Professor at the Department of Information and Digital Technologies, Volodymyr Vynnychenko Central Ukrainian State University.

ORCID: 0000-0002-6843-5583

E-mail: a.v.puzikova@cuspu.edu.ua

The needs of the IT industry, changes in the field of digital technologies, require updating the educational programs of the school computer science course and the corresponding dynamic adaptation of the content of the future teachers training. Analysis of recent research and publications has shown that one of the priority content lines of the school computer science course is the line

“Security and Responsibility”. The task of the course “Information Protection”, included in the educational program “Information Science and Robotics” of the specialty “A4 Secondary Education A4.09 Informatics” at the V. Vynnychenko Central Ukrainian State University, defines competencies for future computer science teachers that are consistent with the expected learning outcomes of secondary education students and the current needs of IT companies.

The article substantiates the content of the program of the educational discipline “Information Protection” for future teachers. The correspondence of the professional competencies of future computer science teachers and the learning outcomes of secondary school students to the content of the proposed course, which includes, in particular, such topics as “General concepts of information protection”, “Basics of cybersecurity”, “Cyberattacks”, “Methods of protecting data, devices and networks” and others, is presented.

It is also noted that certain issues of data and information systems security are also considered in the course “Databases and information systems”.

In the article it is concluded that the proposed content of the academic discipline “Information Protection” for the training of future computer science teachers takes into account modern regulatory requirements for school computer education, as well as the expectations of IT companies regarding the digital competencies of school graduates. Further research is planned to be directed towards the creation of a holistic methodological system for teaching the discipline “Information Protection” for students majoring in Secondary Education (Informatics).

Keywords: data protection; information security; database protection; training of future computer science teachers; competencies; educational program; expected learning outcomes; school computer science course.

Оновлення освітніх програм шкільного курсу інформатики, що активно відбувається протягом останніх років, потребує відповідної динамічної адаптації змісту підготовки майбутніх вчителів. Однак освітні програми педагогічних університетів та програми курсів підвищення кваліфікації вчителів не завжди встигають за змінами концепції предмета та новітніми технологіями. Особливо це стосується внесення до освітніх програм закладів вищої освіти з інформатики нових тематичних блоків відповідно до потреб ІТ-індустрії та новітніх цифрових технологій. У повній мірі сказане можна віднести до питань інформаційної безпеки, які у діючому Державному стандарті базової середньої освіти [1] та у впроваджуваному Державному стандарті профільної середньої освіти [2], представлені у значно більшому обсязі, ніж у попередньому стандарті [3]. Отже проблема формування змісту дисципліни «Захист інформації» для майбутніх вчителів інформатики залишається актуальною.

У дослідженні Н. Морзе, Т. Нанаєвої та О. Пасічник [4] запровадження у програму шкільного курсу інформатики змістової лінії «Безпека та відповідальність» обґрунтовано результатами опитування вчителів, викладачів ЗВО та представників ІТ-компаній: для всіх опитаних груп інформаційна безпека входить до ТОП-6 за пріоритетністю вивчення (з 18 запропонованих тем). У висновках автори прямо зазначають, що «важливою складовою навчальних програм усіх рівнів з інформатики мають стати розділи, присвячені інформаційній безпеці та службам інтернету».

У монографії Н. Пономарьової та А. Петришина також констатується, що за результатами опитування, проведеного в рамках дослідження, найбільший інтерес здобувачів вищої педагогічної освіти за спеціальністю 014 Середня освіта (Інформатика) у фаховій предметній підготовці викликають дисципліни інформаційні системи, теоретичні основи інформатики, об’єктно-орієнтоване програмування, основи штучного інтелекту та захист інформації [5, с. 103].

У дослідженні В. Ігнатенко та І. Мирошніченко [6] зазначено, що інформаційна

безпека набуває ключового значення при підготовці вчителів інформатики, що, у свою чергу, «вимагає оновлення навчальних програм для інтеграції сучасних стандартів у цифровій освіті, що включає теоретичну базу та практичні навички захисту інформаційних ресурсів».

Дослідники І. Вербовський та А. Мельник [7] аналізують сучасні тенденції підготовки майбутніх учителів інформатики в умовах цифрової трансформації освіти. Автори вказують на те, що не слід обмежуватися лише кодуванням і програмуванням, а необхідно інтегрувати у навчальні плани такі дисципліни як наука про дані, штучний інтелект, кібербезпека та взаємодія людини з комп'ютером.

У роботі В. Овдійчук [8] зазначено, що серед цифрових знань, навичок, умінь та ціннісних орієнтирів, якими повинні володіти теперішні учителі інформатики, не останнє місце посідають ті, що пов'язані з пошуком та критичним осмисленням інформації, упорядкуванням, збереженням, захистом та її використанням у освітньому процесі.

Слід зазначити, що засоби захисту даних розглядаються як невід'ємна складова цифрового освітнього середовища і для учнів, і для фахової підготовки майбутніх учителів інформатики [9].

Мета статті – обґрунтування змісту програми навчальної дисципліни «Захист інформації» при підготовці майбутніх вчителів інформатики відповідно до сучасних нормативних вимог до змісту шкільного курсу інформатики та очікувань ІТ-компаній.

Освітня програма «Інформатика та Робототехніка» спеціальності «А4 Середня освіта А4.09 Інформатика» у Центральнотериторіальному державному університеті імені Володимира Винниченка [10] визначає для здобувачів освіти компетентності, які узгоджуються з очікуваними результатами навчання шкільного курсу інформатики та актуальними потребами ІТ-компаній. Складовими фахових компетентностей (СФК) майбутніх вчителів інформатики відповідно до цієї освітньої програми є, зокрема:

СФК1. Здатність організовувати безпечне цифрове середовище.

СФК2. Здатність орієнтуватися в інформаційному просторі, критично оцінювати інформацію, оперувати нею у професійній діяльності.

СФК3. Здатність демонструвати знання, розуміння та навички використання наукових фактів, теорій, принципів і методів інформатики.

СФК4. Здатність забезпечувати інформаційну безпеку комп'ютерних мереж та інформаційних систем.

Зміст курсу «Захист інформації» створено відповідно до визначених компетентностей.

У табл. 1. наведено відповідність фахових компетентностей майбутніх вчителів інформатики, результатів навчання здобувачів середньої освіти до змісту запропонованого курсу «Захист інформації».

Таблиця 1

Відповідність змісту курсу «Захист інформації» та компетентностей
здобувачів освіти

Тема	Компетентності	Основні освітні результати	Вимоги до обов'язкових результатів навчання учнів та орієнтири для оцінювання в інформатичній освітній галузі [1], [2] ²
Тема 1. Загальні поняття та положення із захисту інформації. Значення інформації і її захисту. Задачі сучасної інформаційної безпеки. Основні поняття. Класифікація криптографічних алгоритмів. Види криптоаналітичних атак. Поняття стійкості алгоритму шифрування.	СФК 1, СФК 2, СФК4.	- Знання основних понять та завдань інформаційної безпеки. - Розуміння основних ризиків роботи в цифровому середовищі і необхідність застосування політик безпеки.	- наводить приклади і застосовує заходи безпеки та захисту особистого інформаційного простору, пристроїв і даних [6 ІФО 4.1.2-1] - пояснює поняття конфіденційності, цілісності та доступності даних [12 ІФО 4.1.2-2 П]
Тема 2. Симетричні криптосистеми. Поняття криптосистеми. Класифікація криптографічних систем. Криптосистеми з симетричними ключами та їх властивості. Стандарт блокового симетричного шифрування даних DES. Стандарт блокового симетричного шифрування AES. Національний стандарт блокового симетричного шифрування ДСТУ 7624:2014.	СФК2, СФК3.	- Розуміння алгоритмічних засад захисту даних. Розуміння принципів роботи симетричних і асиметричних криптографічних систем. - Вміння застосовувати криптографічні методи та алгоритми у практичних ситуаціях. - Розуміння принципів приховування даних у цифрових носіях.	- пояснює стандартні принципи інформаційної безпеки і застосовує способи захисту особистих даних і конфіденційності у цифрових середовищах [9 ІФО 4.1.2-3] - застосовує засоби та стратегії захисту конфіденційності та цілісності даних [12 ІФО 4.1.2-4 П] - дотримується принципів кібербезпеки, самостійно застосовує процедури організації інформаційної безпеки для себе, власних пристроїв і даних [9 ІФО 4.1.2] - порівнює заходи та засоби інформаційної безпеки за наданими критеріями та аргументовано обирає їх [12 ІФО 4.1.2-3 П]
Тема 3. Асиметричні криптосистеми. Модель криптосистеми з публічними ключами. Поняття односторонньої функції-пастки. Шифр RSA. Ключі сеансу. Алгоритм шифрування сеансового ключа. Протокол Діффі-Хеллмана.			критично оцінює нові інформаційні технології щодо їх відповідності засадам кібербезпеки [12 ІФО 4.1.2-5 П]
Тема 4. Стеганографія. Стеганографічні системи.			

² У стовпці у квадратних дужках наведено результати навчання та орієнтири для оцінювання за освітніми стандартами.

Сфери застосування стеганографії. Методи стеганографії. Приховування даних у нерухомих цифрових зображеннях, відеофайлах та аудіофайлах. Атаки на стеганографічні системи.			
Тема 5. Кодування. Методи стиснення даних. Загальні принципи архівації. Класифікація методів стиснення даних. Алгоритм Гаффмана (Huffman). Алгоритм Лемпеля-Зіва. Алгоритм Лемпеля-Зіва-Велча.	СФК1, СФК2, СФК3.	– Знання загальних принципів і методів кодування та стиснення даних. – Навички застосовувати кодування та стиснення даних для забезпечення надійності передавання інформації.	– пояснює сутність кодування і виконує його відповідно до окреслених правил [9 ІФО 1.2.4] – пояснює сутність методу кодування [9 ІФО 1.2.4-1] – виконує кодування даних різних типів згідно з окресленими правилами [9 ІФО 1.2.4-2] – пояснює принципи представлення та опрацювання даних різних типів (числа, текст, звуки, зображення) у двійковому та інших видах кодування [9 ІФО 1.2.4-3] – пояснює принципи кодування цифрових даних, які використовуються в різних галузях, і враховує їх під час створення інформаційних продуктів і розв'язування задач [12 ІФО 1.2.2] – пояснює особливості кодування цифрових даних, які використовуються в обраній галузі, і враховує їх під час створення інформаційних продуктів і розв'язування задач [12 ІФО 1.2.2-1] – розуміє та пояснює принципи кодування і декодування цифрових даних, які використовуються в обраній галузі, і враховує їх під час створення інформаційних продуктів [12 ІФО 1.2.2-1 П] – пояснює принципи стиснення даних, обґрунтовано обирає метод стиснення, враховуючи можливість їх втрати [12 ІФО 1.2.2-2 П] – обґрунтовано обирає формати файлів під час створення та збереження інформаційних продуктів з урахуванням принципів кодування цифрових даних, які використовуються в обраній галузі [12 ІФО 1.2.2-4 П]
Тема 6. Основні положення кібербезпеки. Сутність кібербезпеки інформаційного	ФК5, ФК10, ФК17	– Усвідомлення загроз цифрового середовища. – Знання	– пояснює стандартні принципи інформаційної безпеки і застосовує способи захисту особистих даних і конфіденційності у цифрових

суспільства. Характеристика основних завдань управління кібербезпекою. Кіберінциденти: передумови скоєння та наслідки. Дії у кіберпросторі та їх особливості. Напрями забезпечення кібербезпеки України.		стандартних принципів і базових правил кібербезпеки. – Ознайомлення з законодавчою базою щодо напрямів забезпечення кібербезпеки України.	середовищах [9 ІФО 4.1.2-3] – демонструє відповідальну поведінку, поводить розважливо в Інтернеті та застосовує кілька способів захисту себе та інших осіб від порушень прав людини з використанням інформаційних та комунікаційних технологій [9 ІФО 4.2.1-3] – дотримується у власній інформаційній діяльності законів щодо захисту людської гідності і прав людини, захисту даних, інтелектуальної і приватної власності, пояснює відповідальність за їх порушення [9 ІФО 4.3.2]
Тема 7. Кібератаки. Характеристика сучасних кібератак на інформаційні системи та інформаційні ресурси. Типи зловмисного ПЗ. Методи проникнення. Соціальна інженерія. DoS, DDoS та SEO-атаки.	СФК1, СФК2, СФК4.	– Усвідомлення цифрових ризиків і правил безпечної поведінки в мережі. – Здатність орієнтуватися в інформаційному просторі. – Вміння класифікувати типи кібератак та розуміти їх наслідки для ІТ-систем. – Знання методів протидії та попередження інцидентів.	– наводить приклади переваг і небезпек використання цифрових технологій для навколишнього середовища і добробуту у знайомих ситуаціях [6 ІФО 4.1.1-1] – дотримується правил кібербезпеки [6 ІФО 4.1.2] – аргументовано доводить/спростовує автентичність медіа (зображень, відео, аудіо тощо) [9 ІФО 1.4.2] – наводить приклади переваг і небезпек використання цифрових технологій для навколишнього середовища і добробуту в нових ситуаціях [9 ІФО 4.1.1-1] – наводить приклади вразливостей інформаційних систем і можливих наслідків зловмисного їх використання [12 ІФО 4.1.2-1 П] – розпізнає маніпулятивні впливи, які здійснюються цифровими та іншими каналами передавання інформації [12 ІФО 1.4.2-3 П] – використовує різні методи для захисту/протидії маніпуляціям, зокрема в цифровому світі [12 ІФО 1.4.2-1]
Тема 8. Ідентифікація. Автентифікація. Санкціонований доступ. Стратегії контролю доступу. Ідентифікація користувача. Задачі автентифікації. Протоколи авторизації та ідентифікації.	СФК1, СФК4.	– Розуміння важливості захисту облікових даних. – Навички створення безпечних паролів. – Навички налаштування механізмів доступу, облікових записів тощо.	– створює і використовує надійні паролі [6 ІФО 4.1.2-2] – наводить приклади і застосовує заходи безпеки та захисту особистого інформаційного простору, пристроїв і даних [6 ІФО 4.1.2-1] – дотримується правил кібербезпеки [6 ІФО 4.1.2]

Тема 9. Цифровий підпис. Сертифікати. Криптографічні хеш-функції та їх властивості. Алгоритми утворення цифрового підпису.	СФК2, СФК3.	– Розуміння алгоритмів утворення електронного цифрового підпису й сертифікаційної інфраструктури. – Вміння створювати та перевіряти автентичність підпису та цілісність документів. – Розуміння алгоритмів утворення сертифікатів.	– дотримується правил кібербезпеки [6 ІФО 4.1.2] – пояснює особливості реалізації та захисту прав людини в контексті інформаційних технологій [12 ІФО 4.3.1-6 П] – застосовує засоби та стратегії захисту конфіденційності та цілісності даних [12 ІФО 4.1.2-4 П]
Тема 10. Методи захисту даних, пристроїв і мережі. Проблеми захисту даних: у стані спокою, в процесі передачі, під час обробки. Модель кібербезпеки ISO. Способи захисту від атак. Пристрої безпеки: міжмережіві екрани, системи автоматизованого пошуку погроз, системи ідентифікації вторгнень, захист від шкідливого ПЗ, віртуальні захищені мережі (VPN). Інструменти для запобігання та виявлення інцидентів.	СФК1, СФК2, СФК3, СФК4.	– Знання основних методів захисту пристроїв, мережевої інфраструктури та даних. – Уміння організовувати безпечний цифровий простір у закладі освіти. – Навички налаштування мінімальних політик безпеки: управління доступом, моніторинг, резервування. – Навички попередження інцидентів і захисту персональних даних учнів.	– дотримується правил кібербезпеки [6 ІФО 4.1.2] – наводить приклади і застосовує заходи безпеки та захисту особистого інформаційного простору, пристроїв і даних [6 ІФО 4.1.2-1] – дотримується принципів кібербезпеки, самостійно застосовує процедури організації інформаційної безпеки для себе, власних пристроїв і даних [9 ІФО 4.1.2] – використовує стратегії захисту/протидії маніпуляціям, зокрема в цифровому світі [12 ІФО 1.4.2] – використовує різні методи для захисту/протидії маніпуляціям, зокрема в цифровому світі [12 ІФО 1.4.2-1] – обирає і застосовує стратегію кібербезпеки для власного інформаційного середовища [12 ІФО 4.1.2] – порівнює заходи та засоби інформаційної безпеки за наданими критеріями та аргументовано обирає їх [12 ІФО 4.1.2-3 П] – застосовує засоби та стратегії захисту конфіденційності та цілісності даних [12 ІФО 4.1.2-4 П] – критично оцінює нові інформаційні технології щодо їх відповідності засадам кібербезпеки [12 ІФО 4.1.2-5 П]

Слід зауважити, що процес формування здатності забезпечувати безпеку даних

та інформаційних систем розглядається також в курсі «Бази даних та інформаційні системи» [11] під час вивчення наведених нижче тем.

Тема 1. Захист даних. Створення облікових записів в системі управління базами даних MySQL. Привілеї доступу. Рівні привілеїв. Визначення прав доступу для користувацьких представлень.

Вивчення цієї теми має на меті формування умінь налаштовувати механізми доступу, облікові записи, застосовувати техніки резервного копіювання, шифрування, керування правами доступу, та, відповідно, забезпечує формування компетентностей СФК1, СФК3, СФК4.

Тема 2. Механізми підтримки цілісності баз даних. Функції систем управління базами даних. Резервування і відновлення даних. Транзакції та їх властивості. Журнал транзакцій. Відновлення БД після збоїв.

У результаті опанування зазначених тем студенти засвоюють базові принципи захисту та збереження даних у інформаційних системах, включно з механізмами підтримки цілісності та надійності баз даних, отримують навички виконувати резервне копіювання об'єктів бази даних тощо. Вивчення цієї теми забезпечує формування компетентностей СФК3, СФК4.

Таким чином, для формування у студентів цілісного розуміння методів і засобів захисту даних застосовується міждисциплінарний підхід, що передбачає інтеграцію знань і навичок з різних дисциплін для вирішення складних проблем.

Висновки. Підсумовуючи зазначимо, що продуманий відбір тем з інформаційної безпеки у підготовці вчителів інформатики окреслює коло питань для формування у них професійних компетентностей, необхідних для ефективного навчання учнів безпечному використанню цифрових технологій. Запропонований зміст навчальної дисципліни «Захист інформації» для підготовки майбутніх вчителів інформатики враховує сучасні нормативні вимоги до шкільної інформатичної освіти, а також очікування ІТ-компаній щодо цифрових компетентностей випускників шкіл. Встановлено відповідність між темами курсу, компетентностями, які формуються при їх вивченні, та результатами навчання здобувачів середньої освіти, визначеними освітніми стандартами.

Подальші дослідження передбачено спрямувати на створення цілісної методичної системи навчання дисципліни «Захист інформації» для студентів спеціальності Середня освіта (Інформатика), зокрема вивчити досвід авторів дослідження [12], які пропонують для підвищення ефективності підготовки майбутніх вчителів інформатики, в тому числі при вивченні дисциплін «Захист інформаційних ресурсів» та «Безпека комп'ютерних систем і мереж», для самостійного опанування матеріалу запроваджувати масові відкриті онлайн-курси.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Державний стандарт базової середньої освіти. Постанова КМУ від 30 вересня 2020 р. № 898. URL: <https://www.kmu.gov.ua/npas/pro-deyaki-pitannya-derzhavnih-standartiv-povnoyi-zagalnoyi-serednoyi-osviti-i300920-898> (дата звернення: 10.10.2025).
2. Державний стандарт профільної середньої освіти. Постанова КМУ від 25 липня 2024 р. № 851. URL: <https://www.kmu.gov.ua/npas/pro-zatverdzhennia-derzhavnoho-standartu-profilnoi-serednoi-osvity-851-250724> (дата звернення: 10.10.2025).
3. Державний стандарт базової і повної загальної середньої освіти. Постанова КМУ від 23

- листопада 2011 р. № 1392. URL: <https://zakon.rada.gov.ua/laws/show/1392-2011-%D0%BF#Text> (дата звернення: 10.10.2025).
4. Морзе Н., Нанаєва Т., Пасічник О. Стан та перспективи навчання інформатики в закладах загальної середньої освіти України. *Інформаційні технології і засоби навчання*. 2022. Т. 92, №6. С. 1–20. DOI: <https://doi.org/10.33407/itlt.v92i6.5138>.
2. Пономарьова Н. Підготовка майбутніх учителів інформатики в Польщі та в Україні : монографія / Н. Пономарьова, А. Петришин ; Харків. нац. пед. ун-т ім. Г. С. Сковороди. Харків : ХНПУ ім. Г. С. Сковороди, 2025. 112 с. URL: <https://dspace.hnpu.edu.ua/server/api/core/bitstreams/7feddf81-4acc-4c34-abee-3d0566547d49/content> (дата звернення: 25.10.2025)
3. Ігнатенко В. О., Мирошніченко Ю. Б. Інформаційна безпека в сучасному цифровому освітньому середовищі. *Наукові записки. Педагогічні науки*. 2025. Вип. 160. С. 44–53. DOI: <https://doi.org/10.31392/NZ-udu-160.2025.06>.
4. Вербовський І. А., Мельник А. В. Сучасні тенденції підготовки майбутніх учителів інформатики в умовах цифрової трансформації освіти. *Вісник Житомирського державного університету імені Івана Франка. Педагогічні науки*. 2023. Вип. 1(112). С. 5–28. DOI: [https://doi.org/10.35433/pedagogy.1\(112\).2023.5-28](https://doi.org/10.35433/pedagogy.1(112).2023.5-28).
5. Овдійчук В. Цифрова компетентність як одна з базових компетентностей майбутніх учителів інформатики. *Освіта. Інноватика. Практика*. 2025. Т. 13, № 3. С. 64–69. DOI: <https://doi.org/10.31110/2616-650X-vol13i3-010>.
6. Павлова Н. С. Проектування цифрового освітнього середовища як чинника методичної підготовки майбутніх учителів інформатики. *Педагогічна Академія: наукові записки*. 2024. № 8. DOI: <https://doi.org/10.5281/zenodo.13166409>.
7. Освітня програма «Інформатика та Робототехніка» спеціальності «А4 Середня освіта. А4.09 Інформатика». URL: https://cusu.edu.ua/images/download-files/OP_quality-education/bakalavr/2025/Informatyka_ta_Robototekhnika_Bakalavr.pdf (дата звернення: 10.10.2025).
8. Пузікова А. В., Матяш В. В. Формування змісту курсу «Бази даних та інформаційні системи» для майбутніх учителів інформатики. *Наукові записки. Серія: Педагогічні науки*. 2020. № 191. С. 131–135.
9. Медведєва М. О., Жмурко О. І., Криворучко І. І., Ковтанюк М. С. Використання масових відкритих онлайн-курсів у підготовці майбутніх учителів інформатики. *Інноваційна педагогіка*. 2021. Вип. 33(2). С. 159–164. DOI: <https://doi.org/10.32843/2663-6085/2021/33-2.31>.

REFERENCES

1. Derzhavnyi standart bazovoi serednoi osvity [State Standard of Basic Secondary Education] dated on 30.09.2020. № 898. URL: <https://www.kmu.gov.ua/npas/pro-deyaki-pitannya-derzhavnih-standartiv-povnoyi-zagalnoyi-serednoi-osviti-i300920-898> (access date: 10.10.2025). [in Ukrainian].
2. Derzhavnyi standart profilnoi serednoi osvity [State Standard of Specialized Secondary Education]. dated on 25.07.2024. № 851. URL: <https://www.kmu.gov.ua/npas/pro-zatverdzhennia-derzhavnoho-standartu-profilnoi-serednoi-osvity-851-250724> (access date: 10.10.2025). [in Ukrainian].
3. Derzhavnyi standart bazovoi i povnoi zahalnoi serednoi osvity [State Standard of Basic and Complete General Secondary Education] dated on 23.11.2011. № 1392. URL: <https://zakon.rada.gov.ua/laws/show/1392-2011-%D0%BF#Text> (access date: 10.10.2025). [in Ukrainian].
4. Morze, N., Nanaieva, T., & Pasichnyk, O. (2022). Stan ta perspektyvy navchannia informatyky v zakladyakh zahalnoi serednoi osvity Ukraini. [Teaching Computer Science In General Education In Ukraine: Status And Prospects]. *Information Technologies and Learning Tools*, 92 (6), 1–20. DOI: <https://doi.org/10.33407/itlt.v92i6.5138> [in Ukrainian].
5. Ponomarova, N., & Petryshyn, A. (2025) Pidhotovka maibutnikh uchyteliv informatyky v Polshchi ta v Ukraini [Training future computer science teachers in Poland and Ukraine]. Kharkiv : KhNPU im. H. S. Skovorody. 112 p. URL: <https://dspace.hnpu.edu.ua/server/api/core/bitstreams/7feddf81-4acc-4c34-abee-3d0566547d49/content> (access date: 10.10.2025) [in Ukrainian].
6. Ihnatenko, V. O., & Myroshnichenko, Yu. B. (2025). Informatsiina Bezpeka V Suchasnomu Tsyfrovomu Osvitnomu Seredovyshchi [Information Security In The Modern Digital Educational Environment]. *Naukovi zapysky. Pedagogichni nauky*, (160), 44–53. DOI: <https://doi.org/10.31392/nz->

- udu-160.2025.06 [in Ukrainian].
7. Verbovskiy, I. A. & Melnyk, A. V. (2023). Suchasni tendentsii pidhotovky maibutnikh uchyteliv informatyky v umovakh tsyfrovoy transformatsii osvity [Modern Trends In The Training Of Future Computer Science Teachers In The Conditions Of Digital Transformation Of Education]. *Zhytomyr Ivan Franko State University Journal. Pedagogical Sciences*, 1 (112), 5–28. DOI: [https://doi.org/10.35433/pedagogy.1\(112\).2023.5-28](https://doi.org/10.35433/pedagogy.1(112).2023.5-28) [in Ukrainian].
 8. Ovdiihchuk, V. (2025). Tsyfrova kompetentnist yak odna z bazovykh kompetentnostei maibutnikh uchyteliv informatyky [Digital Competenceas One Of The Basic Competences Of Future Teachers Of Computer Science]. *Education. Innovation. Practice*, 13(3), 64–69. DOI: <https://doi.org/10.31110/2616-650x-vol13i3-010> [in Ukrainian].
 9. Pavlova, N. S. (2024). Proiektuvannia tsyfrovoho osvitnoho seredovyscha yak chynnyka metodychnoi pidhotovky maibutnikh uchyteliv informatyky . [Designing a digital educational environment as a factor in the methodological training of future computer science teachers]. *Pedahohichna Akademiia: naukovy zapysky*, (8). DOI: <https://doi.org/10.5281/zenodo.13166409> [in Ukrainian].
 10. Osvitnia prohrama «Informatyka ta Robototekhnika» spetsialnosti «A4 Serednia osvita. A4.09 Informatyka» [Educational program «Informatics and Robotics» specialty «A4 Secondary Education. A4.09 Informatics»] URL: https://cusu.edu.ua/images/download-files/OP_quality-education/bakalavr/2025/Informatyka_ta_Robototekhnika_Bakalavr.pdf (access date: 10.10.2025) [in Ukrainian].
 11. Puzikova, A. V., & Matiash, V. V. (2020). Formuvannia zmistu kursu «Bazy danykh ta informatsiini systemy» dlia maibutnikh uchyteliv informatyky [Formation of the Content of the Course «Databases and Information Systems» for Future Computer Science Teachers]. *Naukovy zapysky. Serii: Pedahohichni nauky*, 191, 131–135 [in Ukrainian].
 12. Medvedieva, M. O., Zhmurko, O. I., Kryvoruchko, I. I. & Kovtaniuk M. S. (2021). Vykorystannia masovykh vidkrytykh onlain-kursiv u pidhotovtsi maibutnikh uchyteliv informatyky [Use of Massive Open Online Courses in Training Future Teachers of Informatics]. *Innovate Pedagogy*, 33(2), 159–164. DOI: <https://doi.org/10.32843/2663-6085/2021/33-2.31> [in Ukrainian]