

of the preschool educational institution, the public, and also increases the effectiveness of the educational process. Accordingly, one of the important components of the professional image is the readiness of future educators to cooperate in partnership with all participants in the educational process of the IPE. This is a complex phenomenon that includes: awareness of the importance of partnership with parents and other participants in the educational process, positive attitude to cooperation, motivation to establish and maintain partnerships, knowledge of the principles and forms of partnership, communication skills, ability to empathize and understand the needs of others, ability to resolve conflict situations, ability to self-analyze and evaluate the effectiveness of one's own activities, and readiness for continuous self-improvement. The readiness of future educators for partnership is a key aspect of their professional training, which involves the acquisition of not only professional knowledge, skills, abilities, but also personal and professional qualities, motivation to cooperate with all participants in the educational process of preschool educational institutions. The formation of this readiness is a continuous process that is carried out not only in the process of training future specialists in preschool education, but also continues throughout their professional activities.

Keywords: future educators of preschool educational institutions, professional activity, professional image, partnership, readiness, children of early and preschool age.

DOI: <https://doi.org/10.31392/NZ-udu-160.2025.06>

УДК 37.091.2:004.77]:001.102-049.5

Ігнатенко В. О., Мирошніченко Ю. Б.

ІНФОРМАЦІЙНА БЕЗПЕКА В СУЧАСНОМУ ЦИФРОВОМУ ОСВІТНЬОМУ СЕРЕДОВИЩІ

У статті розглядаються актуальні питання інформаційної безпеки в освітньому середовищі, зокрема з акцентом на підготовку майбутніх вчителів інформатики до виховання молодого, свідомого та інформаційно-компетентного покоління. У світлі швидкого розвитку цифрових технологій та їх інтеграції в освітній процес, викладачі повинні не лише оволодіти новітніми знаннями у сфері інформаційних технологій, але й навчити здобувачів освіти критично мислити, розуміти ризики і відповідально використовувати інформаційні ресурси. Методологія дослідження базується на системному аналізі світової наукової літератури, міжнародних досліджень, а також прогресивної педагогічної практики і виховних компонентів підготовки, що дає змогу охопити широкий спектр напрямків у цій важливій темі.

Представлено детальний аналіз основних складових інформаційної безпеки, включаючи технічні, організаційні та педагогічні аспекти, які визначають безпечне навчальне середовище. Зокрема, визначено показники готовності вчителів до забезпечення захищеності інформаційних ресурсів, а також розкрито ключові компетенції вчителя у формуванні цифрової культури та цифрової грамотності здобувачів освіти. Ці компетенції включають в себе не лише знання щодо використання сучасних технологій, але й здатність навчити здобувачів освіти розпізнавати фейки, захищати свої особисті дані та дотримуватись етики у віртуальному просторі. Метою є систематизація існуючих знань та формулювання практичних рекомендацій для викладачів педагогічних університетів, акцентуючи увагу на виховних аспектах у контексті цифровізації, які мають першочергове значення для формування безпечного та ефективного освітнього середовища в умовах сучасного інформаційного суспільства.

Ключові слова: Інформаційна безпека; цифрова епоха; майбутні вчителі інформатики; кібербезпека; педагогічна підготовка; цифрова культура; виховна робота.

Сучасні виклики цифрової епохи ставлять під загрозу традиційні підходи до навчання та підготовки фахівців у всіх сферах освіти. Інформаційна безпека набуває ключового значення не лише на рівні держав, але й на рівні окремих навчальних закладів. Це особливо стосується процесу підготовки майбутніх вчителів інформатики, оскільки вони відіграють центральну роль у вихованні своїх студентів у дусі цифрових компетентностей. В умовах швидких технологічних змін зростає необхідність не лише освоєння сучасних інформаційних технологій, але й формування компетенцій, спрямованих на виховання здобувачів освіти у безпечному та продуктивному цифровому середовищі. Це включає здатність вчитись на досвіді, обирати відповідні інструменти для розв'язання проблем, а також формувати критичне мислення, необхідне для навігації у складному інформаційному просторі. Сучасні вчителі повинні бути не лише споживачами інформаційних технологій, а й активними їх користувачами, впроваджуючи інноваційні методи навчання, які заохочують здобувачів освіти до безпечної і свідомої поведінки в цифровому житті. Важливим є також виховання соціально-етичних аспектів, таких як повага до приватності, розуміння прав інтелектуальної власності та відповідальність за інформацію, якою вони діляться. Таким чином, підготовка педагогічних кадрів в умовах цифровізації є багатогранним процесом, що вимагає інтеграції нових поглядів і сучасних підходів для забезпечення готовності молодого покоління до викликів інформаційного суспільства.

Формування цифрової культури у школярів

Важливим аспектом освітньої підготовки є формування цифрової культури в здобувачів освіти, що включає знання про етичні принципи використання технологій, а також вміння критично оцінювати інформаційні ресурси [5].

Це допомагає здобувачам освіти не лише адаптуватись до сучасного інформаційного середовища, але й формує в них відповідальність за своє цифрове "я". Важливо, щоб здобувачі освіти вміли розуміти, які дані є конфіденційними, і як захистити свою особисту інформацію, оскільки це стає особливо актуальним у світі, де кіберзагрози присутні на кожному кроці.

Ключовими елементами цифрової культури є також розвиток критичного мислення та медіаграмотності. Здобувачі освіти повинні вміти розпізнавати недостовірну інформацію, аналізувати джерела новин та робити обґрунтовані висновки. Це дозволить їм уникати маніпуляцій і дезінформації, які часто мають місце в інтернет-просторі [3].

Необхідно включати у навчальну програму елементи практичних занять, де здобувачі освіти зможуть вивчати і обговорювати питання етики в технологіях, а також брати участь у різноманітних проектах, що сприятимуть їхній соціальній активності та усвідомленій поведінці в цифровому світі [1]. Таким чином, формування цифрової культури стане не лише важливим

аспектом освітнього процесу, але й запорукою успішної інтеграції молоді в інформаційне суспільство.

Компетентності вчителя щодо формування цифрової грамотності здобувачів освіти

Вчителі повинні володіти знаннями та навичками, які допоможуть їхнім здобувачам освіти стати інформаційно грамотними. Це включає вміння навчати основам безпеки в Інтернеті, а також розвиток аналітичних навичок при роботі з цифровими ресурсами.

Окрім того, вчителі повинні стимулювати критичне мислення здобувачів освіти, заохочуючи їх ставити питання та аналізувати інформацію з різних джерел. Це допоможе здобувачам освіти не лише формувати власну думку, але й розуміти, як і чому інформація може бути упередженою або неправильно представленою. Важливо навчати також етичним аспектам роботи з цифровими матеріалами, такими як дотримання авторських прав і вміння розпізнавати дезінформацію [1]. Крім того, інтеграція практичних завдань в навчальний процес дозволить здобувачам освіти отримати реальний досвід роботи з інформацією, що значно підвищить їхню впевненість у навичках, отриманих під час навчання. Створення активного навчального середовища, де здобувачі освіти можуть обговорювати свої знахідки, ділитися досвідом та спільно вирішувати проблеми, ще більше покращить їхню інформаційну грамотність і підготує до викликів сучасного світу.

Методи виховної роботи в цифровому середовищі

Дослідження показують, що ефективні методи виховної роботи в цифровому середовищі включають інтерактивні навчальні технології, групові проекти та тренінги, які сприяють розвитку командного духу та критичного мислення [1].

Метою статті є проведення системного аналізу сучасних викликів інформаційної безпеки в освіті, оцінка рівня готовності майбутніх вчителів інформатики до виховання молодого, свідомого та інформаційно компетентного покоління, а також розробка практичних рекомендацій щодо покращення підготовки спеціалістів у цій сфері. Аналіз матеріалу ґрунтується на світових наукових дослідженнях, що відображають сучасні тенденції та прогнозують розвиток інформаційної безпеки в контексті педагогічної підготовки, з акцентом на виховні компоненти навчання.

1. Теоретичні основи інформаційної безпеки в освітньому процесі

Інформаційна безпека розглядається не лише як сукупність комплексних заходів, направлених на захист інформаційних ресурсів від несанкціонованого доступу, модифікації або знищення, а й як основа для формування довіри до інформаційних технологій у суспільстві. У контексті сучасної освіти це поняття набуває особливого значення, оскільки забезпечення оперативної захищеності даних стає невід'ємною частиною педагогічної діяльності, що впливає на якість навчального процесу та безпеку особистої інформації здобувачів освіти. Коли здобувачі освіти навчаються в digital-середовищі, їхня здатність розуміти і реагувати на інформаційні загрози є критично важливою для формування відповідальних цифрових громадян [2].

Проте, готовність майбутніх вчителів інформатики до виховання цифрового покоління є критично важливою. Вони повинні не тільки володіти необхідними технічними знаннями, але й бути підготовленими до активного впровадження принципів інформаційної безпеки в свою педагогічну практику. Це включає в себе вміння створювати безпечні інформаційні середовища, навчати здобувачів освіти розпізнавати потенційні загрози та адекватно реагувати на них, а також формувати у них відповідальність за свої дії в онлайн-просторі.

Теоретичні підходи до вивчення інформаційної безпеки формують базис для розуміння функціональних компонентів системи, що включають:

- організаційно-методичне забезпечення; це включає в себе розробку навчальних програм, семінарів та тренінгів, які допоможуть педагогам впроваджувати концепції інформаційної безпеки в навчальний процес;

- технічні засоби захисту; використання програмного забезпечення для шифрування даних, антивірусних програм і фаєрволів, які забезпечують безпечний доступ до навчальних ресурсів;

- правове регулювання та нормативно-правову базу; знання законодавства щодо захисту персональних даних та авторських прав, що стосується освітнього середовища;

- профілактичні заходи та безперервне моніторингове забезпечення; регулярний аудит і перевірка безпеки інформаційних систем, а також проведення навчальних заходів для підвищення свідомості всіх учасників освітнього процесу щодо важливості дотримання заходів інформаційної безпеки.

2. Формування цифрової культури у школярів

У ході підготовки вчителів особливу увагу слід приділити формуванню цифрової культури у школярів, що є критично важливим аспектом їхнього всебічного розвитку. Цей процес охоплює не лише розвиток навичок критичного мислення, але й навчання відповідальному використанню інформаційних технологій, що включає усвідомлення наслідків онлайн-досвіду. Важливим є також виклад етики в цифровому середовищі, яка допомагає здобувачам освіти формувати моральні засади поведінки в інтернеті, взаємодіючи з контентом та іншими користувачами. Вчителі повинні бути готові інтегрувати ці концепції в свої уроки, використовуючи сучасні технології як інструменти для дослідження, обміну ідеями та розвитку творчого підходу до вирішення проблем. Надання здобувачам освіти можливості активно обговорювати питання інформаційної безпеки, а також шукати шляхи ефективного та етичного використання новітніх технологій, допоможе їм стати не лише споживачами контенту, але й свідомими учасниками цифрового суспільства [3].

3. Компетентності вчителя

Однією з основних задач вчителів є розвиток критичного мислення здобувачів освіти, що дозволяє їм ефективно аналізувати інформацію та робити обґрунтовані висновки. Це особливо важливо в умовах, коли доступ до

даних стає майже безмежним, але не завжди якісним. Використання інноваційних технологій, таких як інтерактивні платформи та віртуальні лабораторії, може значно підвищити зацікавленість здобувачів освіти і сприяти глибшому розумінню предметного матеріалу [3].

Крім того, вчителі повинні стежити за новими тенденціями в розвитку цифрової освіти й адаптувати свої методики, щоб гарантувати інтеграцію останніх до навчального процесу. Наприклад, використання неперервного онлайн-навчання та гейміфікації може не лише зробити навчання більш ефективним, але й створити позитивну атмосферу для здобувачів освіти, де вони відчувають підтримку і мотивацію до вивчення нових знань [2].

Також, важливим аспектом формування цифрової грамотності є навчання здобувачів освіти безпеки в Інтернеті. Вчителі мають навчити їх, як захищати особисті дані, розпізнавати фейкову інформацію та уникати кібербулінгу. Це не лише сприятиме безпеці здобувачів освіти, але й виховувати відповідальних користувачів цифрових технологій.

В умовах глобалізації цифрових технологій, вчителі також повинні звертати увагу на міжкультурну компетенцію. Це означає, що їхнє навчання має охоплювати питання різноманітності та глобального громадянства, оскільки здобувачі освіти будуть взаємодіяти з однолітками з різних країн та культур. Успішне впровадження цих навичок допоможе підготувати молодих людей до викликів сучасного світу.

Остаточо, вчителі мають також постійно вдосконалювати свої професійні навички через участь у курсах підвищення кваліфікації та обмін досвідом з колегами. Важливо, щоб їхня готовність до навчання не зупинялася, адже технології і методики навчання постійно розвиваються, і тільки адаптувавшись до нових викликів, вони зможуть забезпечити якісну освіту своїм здобувачам освіти.

4. Аналіз сучасних викликів інформаційної безпеки в освіті

Завданням даного розділу є систематизація основних викликів, які постають у контексті забезпечення інформаційної безпеки, з особливою увагою до готовності майбутніх вчителів інформатики виховувати молоде, свідоме та інформаційно компетентне покоління. Основні проблеми включають [4]:

1. Низький рівень цифрової грамотності. Підготовка майбутніх вчителів не завжди охоплює комплекс питань щодо кібербезпеки та виховання цифрової грамотності, що призводить до недоосвітлення потенційних ризиків. Вчителі повинні навчити здобувачів освіти не лише користуватись технологіями, а й розуміти їхній вплив.

2. Недостатнє практичне застосування сучасних технологій захисту. У багатьох освітніх установах спостерігається слабка інтеграція інноваційних підходів до забезпечення кібербезпеки, що у свою чергу обмежує можливості вчителів у формуванні цифрової культури у школярів.

3. Психологічні аспекти безпеки. Ризики, пов'язані з соціальною інженерією та маніпуляціями, вимагають додаткової уваги у процесі підготовки

фахівців. Вчителі повинні бути готовими не лише у технологічному, а й у психологічному аспекті для виховання свідомих здобувачів освіти.

У рамках даного розділу важливо розглянути методи виховної роботи в цифровому середовищі, які дозволять педагогу ефективно формувати цифрові компетентності здобувачів освіти. Педагогічні аспекти підготовки вчителів включають навички, необхідні для навчання здобувачів освіти основам цифрової грамотності та розуміння інформаційної безпеки. Вони мають адаптувати навчальні програми до потреб сучасного цифрового покоління.

Відповідно до даних міжнародних досліджень, ключовим напрямом покращення ситуації є інтеграція модулів інформаційної безпеки до навчальних програм педагогічних університетів із залученням сучасних практик та кейс-стаді. Особливу увагу слід приділити готовності майбутніх вчителів інформатики до виховання молодого, свідомого та інформаційно компетентного покоління. Це вимагає від педагогів не лише знань у сфері технологій, але й розуміння виховних аспектів, які сприяють формуванню цифрової культури у школярів.

Для забезпечення успішної реалізації цих цілей необхідно створити інноваційні навчальні програми, які передбачають використання сучасних технологій. Наприклад, інтерактивні платформи і вебінари можуть стати ефективними засобами передачі знань про цифрові інструменти, дозволяючи вчителям практично ознайомлюватись із сучасними можливостями. А також розробка онлайн-курсів, які включають модулі не лише з цифрової грамотності, а й з етики використання інформаційних технологій, може сприяти глибшому усвідомленню здобувачам освіти важливості безпеки в цифровому просторі.

Також необхідно звернути увагу на колаборативні проєкти, що об'єднують здобувачів освіти, вчителів та батьків у процесі навчання. Залучення всіх зацікавлених сторін до обговорення проблем інформаційної безпеки та розвитку цифрових навичок сприяє формуванню єдиного бачення відповідального використання технологій. Для цього можна проводити семінари та тренінги, що навчають батьків основам цифрової грамотності, адже вони також відіграють важливу роль у вихованні підлітків.

Крім того, варто розглянути можливість реалізації програм з менторства, де досвідчені вчителі ділились би своїми знаннями та практичними порадами з молодими спеціалістами. Це сприятиме не лише підвищенню рівня кваліфікації, але й створенню спільноти професіоналів, які підтримують один одного у використанні передових методів навчання.

Не менш важливим є інтеграція сучасних досліджень і наукових напрацювань у навчальний процес. Використання даних про поведінку здобувачів освіти і їхні інтереси в цифровому середовищі дозволить вчителям адаптувати свої методи навчання для досягнення кращих результатів. Розуміння сучасних тенденцій у використанні технологій в освіті, таких як штучний інтелект і віртуальна реальність, відкриває нові горизонти для

педагогічної практики, що, в свою чергу, може істотно вплинути на бажання здобувачів освіти вчитися.

5. Показники готовності майбутніх вчителів до забезпечення інформаційної безпеки

Оцінка рівня готовності майбутніх вчителів до вирішення завдань інформаційної безпеки передбачає аналіз декількох показників [6]:

1. **Теоретична база знань.** Розуміння фундаментальних принципів інформаційної безпеки та нормативної бази, що регулює дану сферу, у контексті виховання здобувачів освіти у цифровому середовищі.

2. **Практичні навички.** Застосування отриманих знань у конкретних ситуаціях, в тому числі симуляційних та реальних кейсах, з акцентом на виховання цифрової грамотності.

3. **Аналітичні здібності.** Уміння оцінити ризики та оперативно реагувати на кібератаки за допомогою сучасних технологічних засобів, не забуваючи про роль технологій у виховному процесі.

4. **Етична свідомість.** Розуміння етичних аспектів використання інформаційних технологій, захисту особистих даних та виховання свідомого ставлення здобувачів освіти до цифрового контенту.

Дані показники сприяють формуванню комплексної картини готовності майбутнього педагога до роботи в умовах постійної інформаційної небезпеки, стимулюючи впровадження нових підходів у викладацьку діяльність та виховання здобувачів освіти. Важливо розробити методи виховної роботи в цифровому середовищі, які допоможуть сформувати у школярів цифрову культуру і грамотність, необхідні для успішної самореалізації у сучасному світі.

6. Результати актуальних досліджень з інформаційної безпеки

Останні міжнародні дослідження виявили декілька ключових трендів у сфері інформаційної безпеки в освіті з акцентом на педагогічні аспекти [3]:

– **Інтенсифікація кіберзагроз.** Активізація хакерських атак на освітні заклади свідчить про необхідність перегляду існуючих стратегій безпеки, а також підготовки вчителів до виховання обізнаності здобувачів освіти.

– **Розширення спектру інструментів захисту.** Введення нових технологій та методик дозволяє суттєво підвищити рівень захищеності інформаційних систем, одночасно вимагаючи від вчителів формування цифрової культури у школярів.

– **Інтеграція навчальних курсів кібервиховання.** Результати досліджень показують, що впровадження спеціалізованих курсів позитивно впливає на загальну обізнаність викладачів щодо ризиків цифрової епохи та формування цифрової грамотності здобувачів освіти.

– **Міжнародна співпраця.** Обмін досвідом між країнами сприяє формуванню більш ефективних моделей забезпечення інформаційної безпеки, які можуть включати виховні компоненти у процес навчання.

Аналіз цих даних підтверджує необхідність системного підходу до підготовки майбутніх вчителів інформатики з урахуванням глобальних кіберзагроз, впровадження сучасних технологічних рішень у навчальні

програми та розвитку методів виховної роботи в цифровому середовищі.

7. Практичні кроки з покращення підготовки вчителів

На основі проведеного аналізу можна виділити низку практичних рекомендацій, спрямованих на підвищення готовності майбутніх вчителів інформатики до виховання свідомого та інформаційно компетентного покоління [6]:

1. Розробка оновлених навчальних програм. Інтеграція модулів, присвячених формуванню цифрової культури у школярів, включаючи практичні семінари, лабораторні роботи та симуляційні заняття, які акцентують увагу на виховних компонентах.

2. Залучення експертів галузі. Організація майстер-класів, вебінарів та конференцій за участю професіоналів з реального сектору для обміну досвідом у виховній діяльності в цифровому середовищі.

3. Підвищення кваліфікації викладачів. Проведення регулярних курсів та тренінгів для викладачів педагогічних університетів з метою оновлення знань та практичних навичок не лише в сфері захисту інформації, але й у формуванні цифрової грамотності здобувачів освіти.

4. Співпраця з міжнародними організаціями. Використання ресурсів та методичних матеріалів провідних світових організацій для створення сучасних платформ обміну інформацією та досвідом у виховній діяльності.

5. Методи виховної роботи в цифровому середовищі. Розробка та впровадження нових методів виховної роботи, які враховують специфіку навчання у цифровому просторі.

6. Моніторинг та оцінка ефективності підготовки вчителів до виховання цифрового покоління. Розробка критеріїв та показників для періодичного аналізу рівня готовності майбутніх вчителів інформатики до виховання молодого, свідомого та інформаційно компетентного покоління. Це включає формування цифрової культури у школярів та впровадження виховних компонентів у навчальні програми, що сприятиме розвитку цифрової грамотності здобувачів освіти.

Реалізація цих заходів дозволить не лише підвищити рівень обізнаності майбутніх вчителів інформатики, а й створити основу для формування стійкої системи захисту інформаційних ресурсів в освітній сфері. Важливим аспектом є формування компетенцій вчителя щодо виховання цифрової грамотності здобувачів освіти, що включає методи виховної роботи в цифровому середовищі.

Висновки. Дослідження підтверджує, що виклики інформаційної безпеки в освіті є складними і потребують комплексного підходу. Підготовка майбутніх вчителів інформатики вимагає оновлення навчальних програм для інтеграції сучасних стандартів у цифровій освіті, що включає теоретичну базу та практичні навички захисту інформаційних ресурсів. Основним завданням є формування готовності вчителів до виховання здобувачів освіти, які можуть адекватно реагувати на цифрові виклики. Запропоновані практичні заходи включають формування цифрової культури у школярів та розмаїття методів

виховної роботи в цифровому середовищі. Стаття містить аналіз педагогічних аспектів підготовки вчителів та рекомендації для викладачів педагогічних університетів, спрямовані на вдосконалення системи підготовки фахівців з інформаційної безпеки та виховання свідомої молоді.

Використана література:

1. Горська К. Кібербезпека та інноваційне цифрове освітнє середовище. URL : [https://www.researchgate.net/profile/Kateryna-Horska/publication/348054972_CYBERSECURITY AND INNOVATIVE DIGITAL EDUCATIONAL ENVIRONMENT/links/62f2213145322476938f3c26/CYBERSECURITY-AND-INNOVATIVE-DIGITAL-EDUCATIONAL-ENVIRONMENT.pdf?tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmVpY2F0aW9uIiwicGFnZSI6InB1YmVpY2F0aW9uIn19](https://www.researchgate.net/profile/Kateryna-Horska/publication/348054972_CYBERSECURITY_AND_INNOVATIVE_DIGITAL_EDUCATIONAL_ENVIRONMENT/links/62f2213145322476938f3c26/CYBERSECURITY-AND-INNOVATIVE-DIGITAL-EDUCATIONAL-ENVIRONMENT.pdf?tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmVpY2F0aW9uIiwicGFnZSI6InB1YmVpY2F0aW9uIn19) http://kabfizroippo.at.ua/Seminar/Book_AVV.pdf.
2. NCC Group. Формування кіберстійкості у вищій освіті / NCC Group. URL : <https://www.timeshighereducation.com/campus/building-cyber-resilience-higher-education>
3. Гамбург І. Деякі нові тенденції в освіті та підготовці з кібербезпеки для підприємств. URL : [https://www.researchgate.net/publication/372443237_Some_Emerging_Trends_in_Cybersecurity Education and Training for Entrepreneurs/fulltext/64b72fe195bbbe0c6e467a43/Some-Emerging-Trends-in-Cybersecurity-Education-and-Training-for-Entrepreneurs.pdf?tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmVpY2F0aW9uIiwicGFnZSI6InB1YmVpY2F0aW9uIn19](https://www.researchgate.net/publication/372443237_Some_Emerging_Trends_in_Cybersecurity_Education_and_Training_for_Entrepreneurs/fulltext/64b72fe195bbbe0c6e467a43/Some-Emerging-Trends-in-Cybersecurity-Education-and-Training-for-Entrepreneurs.pdf?tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmVpY2F0aW9uIiwicGFnZSI6InB1YmVpY2F0aW9uIn19) http://kabfizroippo.at.ua/Seminar/Book_AVV.pdf.
4. Гільєн-Гамес Ф. Д. Цифрова безпека в освітніх контекстах: цифрова компетентність та виклики для належної практики. URL : <https://www.tandfonline.com/doi/epdf/10.1080/07380569.2024.2390319?needAccess=true>
5. Муковіз О., Красюк Л., Моцик Р. Педагогічні умови формування інформаційно-цифрової компетентності в молодших школярів на уроках інформатики. URL : https://library.udpu.edu.ua/library_files/zbirnik_nayk_praz/2023/1/2.pdf
6. Торрес-Ернандес Н., Гальєго-Арруфат М-Х. Індикатори для оцінювання цифрової компетентності майбутніх учителів у галузі безпеки: Систематичний огляд. URL : <https://link.springer.com/content/pdf/10.1007/s10639-022-10978-w.pdf>

References:

1. Horska K. Cybersecurity and innovative digital educational environment. URL : [https://www.researchgate.net/profile/Kateryna-Horska/publication/348054972_CYBERSECURITY AND INNOVATIVE DIGITAL EDUCATIONAL ENVIRONMENT/links/62f2213145322476938f3c26/CYBERSECURITY-AND-INNOVATIVE-DIGITAL-EDUCATIONAL-ENVIRONMENT.pdf?tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmVpY2F0aW9uIiwicGFnZSI6InB1YmVpY2F0aW9uIn19](https://www.researchgate.net/profile/Kateryna-Horska/publication/348054972_CYBERSECURITY_AND_INNOVATIVE_DIGITAL_EDUCATIONAL_ENVIRONMENT/links/62f2213145322476938f3c26/CYBERSECURITY-AND-INNOVATIVE-DIGITAL-EDUCATIONAL-ENVIRONMENT.pdf?tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmVpY2F0aW9uIiwicGFnZSI6InB1YmVpY2F0aW9uIn19) http://kabfizroippo.at.ua/Seminar/Book_AVV.pdf. [in Ukrainian].
2. NCC Group. Building cyber resilience in higher education / NCC Group. URL : <https://www.timeshighereducation.com/campus/building-cyber-resilience-higher-education> [in Ukrainian].
3. Hamburg I. Some Emerging Trends in Cybersecurity Education and Training for Entrepreneurs. URL : [https://www.researchgate.net/publication/372443237_Some_Emerging_Trends_in_Cybersecurity Education and Training for Entrepreneurs/fulltext/64b72fe195bbbe0c6e467a43/Some-Emerging-Trends-in-Cybersecurity-Education-and-Training-for-Entrepreneurs.pdf?tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmVpY2F0aW9uIiwicGFnZSI6InB1YmVpY2F0aW9uIn19](https://www.researchgate.net/publication/372443237_Some_Emerging_Trends_in_Cybersecurity_Education_and_Training_for_Entrepreneurs/fulltext/64b72fe195bbbe0c6e467a43/Some-Emerging-Trends-in-Cybersecurity-Education-and-Training-for-Entrepreneurs.pdf?tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmVpY2F0aW9uIiwicGFnZSI6InB1YmVpY2F0aW9uIn19) http://kabfizroippo.at.ua/Seminar/Book_AVV.pdf. [in Ukrainian].
4. Guillén-Gámez F. D. Digital Security in Educational Contexts: Digital Competence and Challenges for Good Practice. URL : <https://www.tandfonline.com/doi/epdf/10.1080/07380569.2024.2390319?needAccess=true> [in Ukrainian].
5. Mukoviz O., Krasnyuk L., Motsyk P. Pedagogical conditions for the formation of information and digital competence in younger school students at computer science lessons. URL : https://library.udpu.edu.ua/library_files/zbirnik_nayk_praz/2023/1/2.pdf [in Ukrainian].
6. Torres-Hernández N., Gallego-Arrufat M-J. Indicators to assess preservice teachers' digital competence in security: A systematic review. URL : <https://link.springer.com/content/pdf/10.1007/s10639-022-10978-w.pdf> [in Ukrainian].

Y. MYROSHNICHENKO, V. IHNATENKO. Information security in the modern digital educational environment.

The article examines current issues of information security in the educational environment, with a particular focus on preparing future computer science teachers to educate a young, conscious, and information-literate generation. In light of the rapid development of digital technologies and their integration into the educational process, teachers must not only acquire up-to-date knowledge in the field of information technology but also teach students to think critically, understand risks, and use information resources responsibly. The research methodology is based on a systematic analysis of global scientific literature, international studies, as well as advanced pedagogical practices and educational components of teacher training, allowing for a comprehensive approach to this important topic.

A detailed analysis of the key components of information security is presented, including technical, organizational, and pedagogical aspects that define a secure learning environment. In particular, indicators of teachers' readiness to ensure the protection of information resources are identified, and the key competencies of teachers in fostering students' digital culture and digital literacy are explored. These competencies encompass not only knowledge of modern technologies but also the ability to teach students to recognize fake information, protect their personal data, and adhere to ethical principles in the virtual space. The aim is to systematize existing knowledge and formulate practical recommendations for educators in pedagogical universities, emphasizing educational aspects in the context of digitalization, which are crucial for creating a safe and effective educational environment in today's information society.

Keywords: Information security; digital age; future computer science teachers; cybersecurity; pedagogical training; digital culture; educational work.

DOI: <https://doi.org/10.31392/NZ-udu-160.2025.07>

УДК 004.056:070:355/359:37.091.3:37.016:316.774

Ільченко О. А.

**ІНФОРМАЦІЙНА БЕЗПЕКА ОФІЦЕРІВ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ:
ЕЛЕМЕНТИ МЕДІАГРАМОТНОСТІ В ОСВІТНІЙ ПАРАДИГМІ ЗДОБУВАЧІВ**

Інформаційна безпека посідає чільне місце у сфері національної безпеки, особливо у світлі зростаючих загроз кіберпростору. У сучасному світі, коли технології швидко розвиваються, необхідність захисту інформаційного простору стає пріоритетним завданням для військових структур. Ця розвідка присвячена дослідженню аспектів інформаційної безпеки офіцерів Національної гвардії України, зокрема аналізу елементів медіаграмотності в освітній парадигмі здобувачів вищої військової освіти.

Метою статті є виявлення сучасних загроз в інформаційному просторі та розробка рекомендацій щодо впровадження медіаграмотності як ключового елемента підготовки майбутніх офіцерів. Інформаційна безпека включає не лише технічні аспекти захисту даних, але й здатність офіцерів критично оцінювати медіаконтент, розпізнавати маніпуляції та протидіяти інформаційним атакам. Викладання елементів медіаграмотності у навчальних програмах Національної академії Національної гвардії України сприяє формуванню навичок медіаграмотного користувача і генератора медіапродукції, що є вкрай важливим для забезпечення національної безпеки.

У статті представлено аналіз сучасних методів і підходів до навчання