УДК 37:004.056

ТЕТЯНА ЖЕЛЄЗНОВА

БЕЗПЕЧНЕ ЦИФРОВЕ ОСВІТНЄ СЕРЕДОВИЩЕ ЯК ОСНОВА ТРАНСФОРМАЦІЇ СУЧАСНОЇ ОСВІТИ

Анотація. *У статті розглянуто проблему формування безпечного цифрового освітнього середовища в умовах активної цифровізації освіти. Проаналізовано основні кіберзагрози, що впливають на учасників освітнього процесу, зокрема витік персональних даних, фішингові атаки, кібербулінг та інформаційні маніпуляції. Визначено практичні підходи до забезпечення цифрової безпеки в закладах освіти, які поєднують організаційні, технічні та педагогічні заходи. Особливу увагу приділено ролі цифрової культури, освітніх інновацій та державних ініціатив у трансформації сучасної освітньої системи.*

Ключові слова: *цифрове освітнє середовище, цифрова безпека, кібербезпека в освіті, цифрова грамотність, кібербулінг, цифрова трансформація освіти, захист персональних даних.*

Abstract. *The article examines the issues of forming a safe digital educational environment in the context of the rapid digitalization of education. The main cyber threats affecting participants in the educational process are analyzed, and practical steps for ensuring digital security in educational institutions are outlined. Particular attention is paid to the role of digital culture, educational innovations, and national initiatives in the transformation of modern education.*

Keywords: *digital educational environment, digital security, cybersecurity in education, digital literacy, cyberbullying, digital transformation of education, personal data protection.*

Вступ. Упродовж останніх десятиліть цифрові технології стали одним із ключових чинників розвитку освітніх систем у світі. Їх інтеграція в навчальний процес сприяє розширенню доступу до освіти, модернізації методів навчання та появі нових форматів освітньої взаємодії.

Водночас активне впровадження цифрових технологій актуалізує питання забезпечення цифрової безпеки в закладах освіти. Сучасне освітнє середовище є не лише простором здобуття знань, а й складною інформаційною екосистемою, у якій обробляються та зберігаються персональні дані здобувачів освіти, педагогічних працівників і батьків, результати навчання, службова документація та управлінська інформація. Неналежний рівень захисту цих даних може створювати ризики як для функціонування закладів освіти, так і для безпеки учасників освітнього процесу.

Цифрова безпека в освіті охоплює комплекс заходів, спрямованих на захист інформаційних ресурсів, технічної інфраструктури та персональних даних, а також на забезпечення психологічного благополуччя учасників освітнього процесу в цифровому середовищі. Вона передбачає поєднання технічних рішень (захист мереж, систем і пристроїв), організаційних механізмів (нормативно-правові документи, політики безпеки, регламенти) та педагогічних підходів, спрямованих на формування цифрової культури та відповідальної поведінки в онлайн-просторі.

Особливої актуальності проблема цифрової безпеки набуває в умовах воєнного стану, зростання кількості кібератак, інформаційних та психологічних впливів. Заклади освіти дедалі частіше стають об'єктами кібершахрайства, дезінформації та атак на інформаційні системи. Водночас діти та молодь є однією з найбільш уразливих груп у цифровому середовищі, що потребує підвищеної уваги до формування медіаграмотності, навичок безпечної онлайн-взаємодії та відповідального використання цифрових ресурсів.

Формування безпечного цифрового освітнього середовища є спільною відповідальністю держави, адміністрації закладів освіти, педагогічних працівників, здобувачів освіти та батьків. Це передбачає не лише впровадження сучасних технологій захисту інформації, а й розвиток цифрової культури, критичного мислення та етичної поведінки в цифровому просторі. Такий підхід сприяє підвищенню стійкості освітньої системи, зміцненню довіри до цифрових інструментів та створенню умов для безпечного й ефективного навчання в умовах цифрової трансформації освіти.

Постановка проблеми та обґрунтування актуальності дослідження. Сучасний розвиток інформаційних технологій суттєво впливає на трансформацію освітньої системи. Використання цифрових платформ, онлайн-ресурсів, систем дистанційного та змішаного навчання розширює можливості організації освітнього процесу, підвищує доступність навчання та сприяє інтеграції нових педагогічних підходів. Разом із тим активне впровадження цифрових інструментів зумовлює появу нових ризиків, пов'язаних із захистом інформації та безпечним використанням цифрових технологій у сфері освіти.

Освітні установи сьогодні функціонують у середовищі, де постійно обробляється значний обсяг інформації, включно з персональними даними учнів, студентів, педагогічних працівників і батьків. Неналежний рівень захисту таких даних, недостатня обізнаність користувачів щодо правил безпечної поведінки в цифровому просторі та поширення кіберзагроз можуть призводити до порушення конфіденційності інформації, несанкціонованого доступу до освітніх ресурсів і дестабілізації роботи інформаційних систем закладів освіти.

Актуальність проблеми посилюється в умовах стрімкого зростання кіберзагроз, поширення фішингових атак, шкідливого програмного забезпечення, випадків кібербулінгу та інформаційних маніпуляцій у цифровому просторі. Особливо вразливою групою користувачів є діти та молодь, які активно використовують цифрові технології у навчанні та комунікації, але не завжди володіють достатніми навичками безпечної онлайн-поведінки.

У зв'язку з цим формування безпечного цифрового освітнього середовища набуває особливої значущості для стабільного функціонування закладів освіти та забезпечення захисту всіх учасників освітнього процесу. Це потребує комплексного підходу, що поєднує організаційні, технологічні та педагогічні заходи, спрямовані на підвищення рівня цифрової безпеки та формування відповідальної культури використання цифрових ресурсів.

Аналіз останніх досліджень і публікацій. Проблема цифрової безпеки в освіті активно досліджується як в Україні, так і за кордоном. Міжнародні дослідження показують, що інтеграція цифрових технологій у навчальний процес відкриває нові освітні можливості, але водночас підвищує ризики витоку даних, кібербулінгу та несанкціонованого доступу до інформаційних систем. У сучасному науковому та нормативно-аналітичному дискурсі проблема безпечного цифрового освітнього середовища розглядається як міждисциплінарна, оскільки поєднує питання цифровізації освіти, захисту персональних даних, кібербезпеки, цифрової грамотності та психологічної безпеки учасників освітнього процесу. У міжнародних аналітичних та методичних документах наголошується, що ефективне використання цифрових технологій в освіті потребує не лише належної технічної інфраструктури, а й чітких етичних, організаційних та правових механізмів захисту [9; 10]. Важливе значення мають також дослідження, присвячені цифровій культурі, цифровому громадянству та безпечній поведінці дітей і молоді в онлайн-середовищі. В українському контексті питання розвитку цифрових компетентностей та безпечного використання цифрових ресурсів актуалізуються в нормативно-правових актах щодо кібербезпеки, захисту персональних даних і розвитку цифрових компетентностей громадян.

Особлива увага приділяється питанням кібербулінгу та психологічної безпеки здобувачів освіти. За матеріалами UNICEF, ці явища є поширеним ризиком для дітей і підлітків у цифровому середовищі та потребує системної профілактики, просвітницької роботи й своєчасного реагування з боку закладів освіти [8]. У нормативно-правових документах наголошується, що впровадження освітніх програм із медіаграмотності та цифрової безпеки сприяє зменшенню негативного впливу цифрових ризиків і підвищенню рівня критичного мислення здобувачів освіти [3–5].

Дослідження останніх років також показують, що ефективність цифрової безпеки залежить від інтеграції сучасних технологій, політик безпеки та навчання користувачів. При цьому міжнародна практика демонструє успішність впровадження державних платформ, освітніх центрів цифрової грамотності та програм підготовки цифрових лідерів, що підвищують стійкість освітніх установ до кіберзагроз.

Таким чином, сучасні дослідження підтверджують необхідність системного підходу до формування безпечного цифрового освітнього середовища, що враховує одночасно технічні, організаційні

та педагогічні аспекти, а також забезпечує розвиток цифрової культури та критичного мислення серед здобувачів освіти.

Мета дослідження. Метою статті є проаналізувати сучасні загрози цифровій безпеці в освітньому середовищі та визначити ефективні організаційні, технічні та педагогічні заходи, спрямовані на формування безпечного цифрового освітнього простору в закладах освіти України.

Виклад основного матеріалу дослідження

Основні кіберзагрози в освітньому середовищі

Сучасне освітнє середовище становить складну цифрову екосистему, що інтегрує інформаційні системи, онлайн-платформи, персональні пристрої та великий контингент користувачів із різним рівнем цифрової компетентності. Така відкритість і багатокомпонентність підвищує вразливість закладів освіти до численних кіберзагроз, які мають як технічний, так і соціально-психологічний характер.

По-перше, *це порушення конфіденційності та витік персональних даних*. Заклади освіти обробляють значні обсяги персональної інформації, включно з даними учнів, студентів, педагогів, результатами навчання, медичною та соціальною інформацією. Цифровізація освітнього процесу актуалізує ризики витоку персональних даних та несанкціонованого доступу до освітніх платформ, що зумовлює необхідність дотримання вимог законодавства у сфері захисту персональних даних і кібербезпеки [1; 2; 6].

По-друге, *фішингові атаки та методи соціальної інженерії* залишаються одними з найбільш поширених загроз у цифровому освітньому середовищі, оскільки орієнтовані насамперед на людський фактор. Підроблені електронні повідомлення, фейкові сторінки входу, шахрайські посилання та фальшиві акаунти можуть використовуватися для викрадення облікових даних користувачів або зараження пристроїв шкідливим програмним забезпеченням.

По-третє, *шкідливе програмне забезпечення та програми-вимагачі*. Віруси, трояни, spyware та ransomware можуть блокувати роботу навчальних платформ, знищувати матеріали та вимагати викуп за відновлення доступу. Особливо небезпечними для закладів освіти є атаки із застосуванням шкідливого програмного забезпечення та програм-вимагачів (ransomware), які можуть призводити до блокування доступу до навчальних платформ, втрати навчальних матеріалів, порушення безперервності освітнього процесу та необхідності відновлення даних із резервних копій.

Важливою загрозою є *несанкціонований доступ до освітніх платформ*. Слабкі паролі, відсутність двофакторної автентифікації та спільні облікові записи підвищують ризик несанкціонованого доступу до систем управління навчанням, електронних журналів та відеоконференцій. Використання слабких паролів, відсутність двофакторної автентифікації та спільне користування обліковими записами істотно підвищують ризик несанкціонованого доступу до освітніх платформ і цифрових сервісів закладу освіти [2; 6].

Кібербулінг і цифрове насильство. Онлайн-цькування, приниження та розповсюдження особистої інформації негативно впливають на психологічний стан здобувачів освіти, знижують мотивацію до навчання та ускладнюють соціальну адаптацію. За матеріалами міжнародних організацій, зокрема UNICEF, кібербулінг розглядається як поширений ризик цифрового середовища для дітей і підлітків, що негативно впливає на психологічне благополуччя, самооцінку та навчальну мотивацію [8]. Це зумовлює необхідність системної профілактичної роботи в закладах освіти, спрямованої на формування безпечної онлайн-поведінки та своєчасне реагування на випадки цифрового насильства.

Слід додати дезінформацію та інформаційно-психологічні впливи. Саме поширення фейкових новин, маніпулятивних матеріалів і пропаганди становить загрозу для формування критичного мислення учасників освітнього процесу. Особливо це актуально в умовах війни, коли дезінформація може впливати на психологічну стабільність дітей та молоді.

Окрему групу ризиків становить *використання особистих пристроїв* (BYOD) в освітньому процесі. Воно розширює можливості доступу до цифрових ресурсів, однак водночас підвищує ризики зараження локальної мережі, несанкціонованого доступу до освітніх платформ та витоку інформації. За відсутності чітких правил використання особистих пристроїв і належних технічних обмежень такі ризики істотно зростають.

Комплексний характер кіберзагроз у цифровому освітньому середовищі вимагає системного підходу до їхньої протидії.

Усвідомлення технічних, організаційних та соціально-психологічних ризиків є першим кроком до побудови ефективної системи цифрової безпеки у закладах освіти.

Практичні підходи до забезпечення цифрової безпеки в освітньому середовищі

Створення безпечного цифрового освітнього середовища є комплексним і системним процесом, що передбачає інтеграцію управлінських рішень, технічних засобів та педагогічних практик. Ефективність цього процесу значною мірою залежить від чіткої організації роботи закладу освіти, рівня цифрової компетентності педагогів та усвідомленої поведінки здобувачів освіти. Нижче представлені ключові підходи до забезпечення цифрової безпеки з прикладами практичної реалізації.

Політика цифрової безпеки закладу

Розроблення та впровадження внутрішніх політик цифрової безпеки є основою системного захисту інформаційних ресурсів закладу. Це передбачає затвердження нормативних документів: правил користування інформаційними системами, алгоритмів дій у разі кіберінцидентів та процедур захисту персональних даних. Чітко сформульовані політики дозволяють визначити відповідальність адміністрації, педагогів та здобувачів освіти, а також стандартизувати процес реагування на загрози.

Приклад реалізації:

- Впровадження правил доступу до електронних журналів та платформ дистанційного навчання, включно з вимогами до паролів і обмеженням спільного користування акаунтами.
- Алгоритм повідомлення про підозрілі електронні листи та інциденти кібербезпеки серед педагогів і учнів.

Технічні рішення

Технічні заходи є ключовими для забезпечення захисту інформаційної інфраструктури. Вони включають: використання ліцензованого антивірусного програмного забезпечення, регулярне оновлення операційних систем і додатків, резервне копіювання даних, впровадження складних паролів та двофакторної автентифікації.

Приклад реалізації:

- Установка корпоративних антивірусних рішень і брандмауерів для шкільних серверів.
- Використання хмарних сховищ з шифруванням даних для навчальних матеріалів.
- Моніторинг підозрілих входів до систем управління навчанням.

Регулярне оновлення операційних систем і програмного забезпечення, використання складних паролів, резервного копіювання даних та двофакторної автентифікації суттєво підвищують рівень захисту освітніх платформ і зменшують ризик несанкціонованого доступу до облікових записів.

Підвищення цифрової компетентності педагогів

Педагоги є ключовими агентами формування безпечного цифрового середовища. Підвищення їхньої компетентності з кібербезпеки, медіаграмотності та етики онлайн-спілкування дозволяє своєчасно виявляти загрози і навчати цьому учнів.

Приклад реалізації:

- Онлайн-курси та тренінги на платформі «Дія. Освіта» з цифрової грамотності та кібербезпеки.
- Регулярні внутрішні семінари для педагогів із використанням кейсів кіберінцидентів у школах.
- Підготовка методичних матеріалів з правил безпечної поведінки онлайн.

Формування культури безпечної поведінки учнів

Формування у здобувачів освіти усвідомленої цифрової поведінки є не менш важливим, ніж технічний захист. Це включає навчання правилам безпечного спілкування в мережі, критичному оцінюванню інформації, захисту персональних даних, дотриманню цифрової етики та розвитку відповідального цифрового громадянства.

Приклад реалізації:

- Інтеграція тем кібербезпеки та медіаграмотності у навчальні предмети та виховні заходи.
- Проведення інтерактивних уроків і тренінгів із розпізнавання фейкової інформації.
- Використання ігрових платформ та симуляторів для практичного навчання безпечної поведінки онлайн.

Протидія кібербулінгу

Кібербулінг негативно впливає на психологічне благополуччя здобувачів освіти і знижує ефективність навчання. Важливо впроваджувати системи попередження та реагування на випадки цифрового насильства.

Приклад реалізації:

- Створення внутрішніх положень для повідомлення про кібербулінг.

• Залучення практичного психолога, соціального педагога та класних керівників до профілактичної й корекційної роботи відповідає міжнародним підходам щодо запобігання кібербулінгу та підтримки безпечного цифрового середовища для дітей і підлітків.

• Доцільним є використання всеукраїнських просвітницьких ініціатив і методичних матеріалів, спрямованих на запобігання кібербулінгу та формування безпечної онлайн-поведінки здобувачів освіти [5; 8].

Співпраця з батьками та громадськістю

Батьки та громадськість є важливими партнерами у формуванні безпечного цифрового середовища. Поінформованість батьків про цифрові ризики дозволяє забезпечити комплексний підхід до безпеки учнів як у школі, так і вдома.

Приклад реалізації:

• Проведення батьківських зборів і вебінарів з кібербезпеки та безпечного використання соціальних мереж.

• Публікація на сайті закладу рекомендацій для батьків щодо налаштування пристроїв учнів.

• Включення батьків у шкільні комітети з цифрової безпеки для спільного планування заходів.

Комплексне впровадження політик безпеки, технічних заходів, підвищення компетентності педагогів, формування культури безпечної поведінки учнів та активної участі батьків забезпечує системний підхід й сприяє підвищенню стійкості закладу освіти до кіберзагроз, зниженню ризиків витоку персональних даних і формуванню відповідальної цифрової культури всіх учасників освітнього процесу.

Державні ініціативи та інноваційні проєкти для забезпечення цифрової безпеки в освіті України

У контексті цифрової трансформації освіти важливу роль відіграють державні програми та практичні ініціативи, спрямовані на розвиток цифрових компетентностей населення, підвищення рівня кібербезпеки та впровадження сучасних освітніх технологій. В Україні реалізується низка інструментів, що формують основу для розвитку безпечного цифрового освітнього середовища та сприяють інтеграції сучасних підходів у національну систему освіти [3; 4].

Національна платформа цифрової освіти «Дія. Освіта»

Однією з ключових державних ініціатив є національна освітня платформа «Дія. Освіта», яка спрямована на розвиток цифрових навичок громадян та формування культури безпечного користування цифровими технологіями. Платформа пропонує освітні серіали, інтерактивні курси, симулятори й тести, що допомагають користувачам підвищити рівень цифрової грамотності та цифрової стійкості [4].

Важливим інструментом оцінювання цифрової грамотності на платформі «Дія. Освіта» є освітній портал «Цифрограм», розроблений на основі рамки цифрової компетентності для громадян України. Його використання сприяє діагностиці рівня цифрових компетентностей і визначенню напрямів подальшого професійного та особистісного розвитку учасників освітнього процесу [5].

Важливими для закладів освіти є також рекомендації Міністерства освіти і науки України щодо безпеки дітей у цифровому просторі та безпечного використання інтернету в закладах освіти. Такі матеріали мають практичне значення для формування внутрішніх політик цифрової безпеки, профілактики кібербулінгу, фільтрації контенту та організації просвітницької роботи з педагогами, учнями й батьками [6; 7].

Окремим напрямом розвитку цифрової освіти є офлайн-хаб цифрової грамотності, у якому користувачі можуть отримати консультації, пройти навчальні курси та підвищити рівень цифрових компетентностей. Такі простори відіграють важливу роль у поширенні знань про безпечне використання цифрових технологій, особливо серед педагогів, учнів та батьків [4].

Отже, державні ініціативи та практичні освітні інструменти відіграють важливу роль у формуванні безпечного цифрового освітнього середовища в Україні. Вони сприяють розвитку цифрової грамотності, поширенню кібергігієни, підвищенню рівня обізнаності щодо захисту персональних даних та формуванню культури відповідального використання цифрових ресурсів [3–7].

Висновки та перспективи подальших розвідок напряму

Цифрова трансформація освітньої системи суттєво змінює організацію освітнього процесу та відкриває нові можливості для розвитку сучасної освіти. Використання онлайн-платформ, цифрових сервісів та інноваційних

технологій сприяє підвищенню доступності освіти, розширенню освітніх ресурсів і розвитку нових форм навчальної взаємодії. Водночас активне впровадження цифрових інструментів зумовлює появу нових ризиків, пов'язаних із забезпеченням інформаційної та кібербезпеки в освітньому середовищі.

Проведений аналіз показав, що сучасні заклади освіти стикаються з різноманітними кіберзагрозами, серед яких порушення конфіденційності персональних даних, фішингові атаки, поширення шкідливого програмного забезпечення, несанкціонований доступ до освітніх платформ, кібербулінг і дезінформація. Ці загрози мають комплексний характер і впливають не лише на функціонування інформаційних систем, а й на психологічну безпеку учасників освітнього процесу [1; 2; 6; 8].

У ході дослідження встановлено, що ефективне формування безпечного цифрового освітнього середовища потребує системного підходу, який поєднує організаційні, технологічні та педагогічні заходи. До ключових напрямів забезпечення цифрової безпеки належать розроблення внутрішніх політик безпеки в закладах освіти, впровадження сучасних технічних засобів захисту, підвищення цифрової компетентності педагогічних працівників, формування культури безпечної поведінки здобувачів освіти та активна взаємодія з батьками [1–7; 9; 10].

Важливу роль у розвитку безпечного цифрового освітнього середовища відіграють державні ініціативи України, зокрема національна платформа цифрової освіти, інструменти оцінювання цифрових компетентностей і рекомендації для закладів освіти щодо безпечного використання цифрових ресурсів [3–7].

Отже, формування безпечного цифрового освітнього середовища є важливим чинником сталого розвитку освітньої системи в умовах цифровізації. Перспективи подальших досліджень полягають у розробленні ефективних моделей управління цифровою безпекою закладів освіти, адаптації міжнародних практик до українського контексту та впровадженні інноваційних інструментів захисту освітніх інформаційних систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2297-17 (дата звернення: 23.03.2026).

2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2163-19 (дата звернення: 23.03.2026).

3. Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації: розпорядження Кабінету Міністрів України від 03.03.2021 № 167-р // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/167-2021-%D1%80 (дата звернення: 23.03.2026).

4. Дія. Освіта: національна платформа цифрової освіти / Міністерство цифрової трансформації України. URL: https://osvita.diia.gov.ua/ (дата звернення: 24.03.2026).

5. Безпека дітей у цифровому просторі – МОН надає рекомендації для педагогічних працівників та батьків / Міністерство освіти і науки України. 11.03.2021. URL: https://mon.gov.ua/news/bezpeka-ditey-u-tsifrovomu-prostori-mon-nadae-rekomendatsii-dlya-pedagogichnikh-pratsivnikiv-ta-batkiv (дата звернення: 23.03.2026).

6. Безпечний інтернет у закладах освіти: затверджено рекомендації щодо фільтрації контенту / Міністерство освіти і науки України. 27.01.2026. URL: https://mon.gov.ua/news/bezpechnyi-internet-u-zakladakh-osvity-zatverdzheno-rekomendatsii-shchodo-filtratsii-kontentu (дата звернення: 23.03.2026).

7. Рамка цифрової компетентності для громадян України / Міністерство цифрової трансформації України. URL: https://osvita.diia.gov.ua/ (дата звернення: 24.03.2026).

8. Cyberbullying: What is it and how to stop it / UNICEF. URL: https://www.unicef.org/end-violence/how-to-stop-cyberbullying (дата звернення: 24.03.2026).

9. Digital citizenship education handbook / Council of Europe. Strasbourg : Council of Europe, 2019. URL: https://book.coe.int/en/human-rights-democratic-citizenship-and-interculturalism/7851-digital-citizenship-education-handbook.html (дата звернення: 24.03.2026).

10. Global Education Monitoring Report 2023: Technology in Education: A Tool on Whose Terms? / UNESCO. Paris : UNESCO, 2023. URL: https://www.unesco.org/en/articles/global-education-monitoring-report-2023-technology-education-tool-whose-terms (дата звернення: 24.03.2026).