УДК 378.018:004

Наталія РУБЛЬОВА,
доктор філософії в галузі педагогіки, заступник директора
з науково-педагогічної та освітньо-проєктної діяльності ВІППО
ORCID: https://orcid.org/0000-0001-8341-7095

Значення цифрової безпеки для сучасного педагога – ключові ризики

Розглянуто значення цифрової безпеки як ключової компетентності сучасного педагога в умовах стрімкої цифровізації освіти. Проаналізовано теоретичні засади поняття цифрової безпеки, окреслено правове регулювання у сфері захисту персональних даних та кібербезпеки, а також наведено приклади з освітньої практики, що демонструють актуальні виклики та ризики. Особливу увагу приділено ролі закладу освіти у формуванні культури цифрової безпеки та лідерству педагога як прикладу безпечної поведінки онлайн. Запропоновано практичні орієнтири для педагогів, які включають цифрову гігієну, конфіденційність, використання двофакторної автентифікації та розвиток критичного мислення учнів. Зроблено висновок, що цифрова безпека потребує системного підходу – від індивідуальних навичок до інституційних політик, а заклади освіти мають стати простором формування культури безпечної поведінки у цифровому середовищі.

Ключові слова: *цифрова безпека, сучасний педагог, освітнє середовище, персональні дані, кібербезпека, конфіденційність, критичне мислення, інституційна відповідальність, цифрова гігієна, культура безпечної поведінки.*

Nataliia Rublova. The Importance of Digital Security for Today's Teacher: Key Risks.

The article examines digital security as a key competence of the modern teacher in the context of rapid digitalization of education. Theoretical foundations of digital security are analyzed, legal regulation in the field of personal data protection and cybersecurity is outlined, and practical examples from educational practice are provided to illustrate current challenges and risks. Particular attention is paid to the role of educational institutions in shaping a culture of digital security and to teacher leadership as a model of safe online behavior. Practical guidelines for teachers are proposed, including digital hygiene, confidentiality, two-factor authentication, and the development of students' critical thinking. It is concluded that digital security requires a systemic approach – from individual skills to institutional policies – and that educational institutions should become spaces for cultivating a culture of safe behavior in the digital environment.

Keywords: *digital security, modern teacher, educational environment, personal data, cybersecurity, confidentiality, critical thinking, institutional responsibility, digital hygiene, culture of safe behavior.*

Вступ. Цифрова трансформація освіти в Україні відбувається надзвичайно швидкими темпами. Якщо в багатьох країнах світу процес цифровізації мав поступовий характер, то українське суспільство занурилося у цифровий простір стрімко й без достатньої підготовки. Це призвело до того, що значна частина громадян опинилася беззахисною перед викликами цифрової епохи: одні не змогли скористатися сучасними сервісами, інші – стали жертвами шахрайства, кібербулінгу чи дезінформації.

Актуальність цифрової безпеки в сучасній освіті також зумовлена стрімким розвитком цифрових технологій та їх масовим упровадженням у навчальний процес. Якщо ще кілька років тому цифрові інструменти були тільки допоміжними, то сьогодні вони стали невід'ємною частиною професійної діяльності педагога: електронні журнали, онлайн-платформи, хмарні сервіси, соціальні мережі та цифрові ресурси щодня використовуються для організації навчання й комунікації. Така швидка цифровізація відкриває нові можливості, але водночас створює серйозні ризики – від витоку персональних даних і кібербулінгу до поширення дезінформації та залежності від гаджетів. Саме тому цифрова безпека перестає бути другорядним технічним питанням і стає стратегічною компетентністю педагога, яка визначає якість освітнього процесу, довіру учасників та готовність суспільства до викликів цифрової епохи.

Освітнє середовище в цьому контексті має особливе значення. Педагогічні працівники всіх рівнів освіти щодня взаємодіють із цифровими ресурсами, платформами та інструментами. Вони відкривають нові можливості для навчання, комунікації та управління освітнім процесом, але водночас стикаються з ризиками, що потребують усвідомлення та належного реагування.

Мета цієї статті – розкрити значення цифрової безпеки для педагогічних працівників, визначити ключові ризики цифрового середовища та окреслити

практичні орієнтири для формування культури безпечної поведінки в освіті.

Виклад основного матеріалу. Цифрова безпека є інтегративним поняттям, що поєднує елементи інформаційної та кібербезпеки. Якщо коротко їх означити, то це виглядатиме так:

Інформаційна безпека охоплює захист будь-якої інформації незалежно від її форми – паперових документів, усних повідомлень, електронних файлів чи знань, які людина зберігає у пам'яті. Її мета – забезпечити цілісність, доступність та конфіденційність даних. *Кібербезпека* є вузьким сегментом, що стосується лише цифрових технологій: комп'ютерів, мобільних пристроїв, інтернету та локальних мереж. Вона спрямована на захист електронних даних від хакерських атак, вірусів, фішингу та інших кіберзагроз. Відповідно, *цифрова безпека* – це практичний комплекс знань, навичок і правил, що забезпечують безпечну взаємодію людини з цифровими технологіями в освітньому середовищі.

У контексті освіти цифрова безпека включає кілька аспектів, які варто розглядати в сукупності, а саме:

– *технічні аспекти* – захист пристроїв, акаунтів, освітніх платформ, електронних журналів, хмарних сервісів;

– *організаційні аспекти* – правила доступу, політики конфіденційності, дотримання законодавства («Про захист персональних даних», GDPR);

– *етичні аспекти* – повага до приватності учасників освітнього процесу, відповідальне використання цифрових ресурсів;

– *практичні навички* – створення надійних паролів, використання двофакторної автентифікації, регулярне оновлення програм, перевірка безпечності сайтів, критичне мислення щодо цифрового контенту.

Таким чином, цифрова безпека в освітній галузі, про яку ми говоримо, це не лише технічний захист комп'ютера від вірусів, а комплексна культура безпечної поведінки всіх учасників освітнього процесу: школярів, педагогів, адміністрації та батьків загалом.

Тож цифрова безпека в освітньому середовищі не може розглядатися лише як набір технічних навичок чи рекомендацій, оскільки має чітке правове підґрунтя, яке визначає обов'язки педагогів, адміністрацій закладів освіти та державних інституцій. В Україні ключовими нормативними документами у площині порушеної проблеми є Закон України «Про захист персональних даних» (2010 р., № 2297-VI) та Закон України «Про основні засади забезпечення кібербезпеки України» (2017 р.). Крім того, дедалі більшого значення у світлі євроінтеграційних процесів нашої держави набуває Загальний регламент Європейського Союзу про захист даних (GDPR, 2018 р.), який задає міжнародні стандарти конфіденційності та безпеки.

Закон України «Про захист персональних даних» визначає: «Персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована» [1, ст. 2]. Для освітнього середовища це означає, що інформація про учнів, студентів чи працівників (електронні журнали, списки, анкети, результати навчання) має оброблятися виключно з їхньої згоди та з дотриманням принципів конфіденційності. Порушення цих норм може призвести не лише до втрати довіри, а й до юридичної відповідальності. Таким чином, педагогічний працівник виступає не лише користувачем цифрових ресурсів, а й гарантом дотримання правових норм у сфері захисту освітніх даних.

Закон України «Про основні засади забезпечення кібербезпеки України» спрямований на захист цифрових систем і даних від зовнішніх загроз. Він визначає правові та організаційні основи запобігання кіберінцидентам, а також установлює вимоги до захисту критичної інформаційної інфраструктури. «Кібербезпека України – це стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави у кіберпросторі» [2]. Для закладів освіти це означає необхідність застосування технічних заходів – антивірусного захисту, резервного копіювання, регулярного оновлення програмного забезпечення, а також розробки внутрішніх політик безпеки. Освітні платформи, електронні журнали та системи управління навчальним процесом можуть стати об'єктом атак, і саме тому педагоги повинні усвідомлювати свою роль у забезпеченні кіберстійкості освітнього середовища.

Згаданий вище документ GDPR (General Data Protection Regulation), ухвалений у Європейському Союзі 2018 року, встановлює високі міжнаціональні стандарти захисту персональних даних. Його ключовим принципом є право кожної особи контролювати, як її дані збираються, зберігаються та використовуються, а також право на «забуття» – видалення інформації за вимогою користувача: «Суб'єкт даних має право вимагати від володільця без зайвих зволікань

видалення персональних даних, що стосуються його особи» [3].

Хоча GDPR прямо діє лише в країнах ЄС, його положення дедалі частіше інтегруються в українську практику, особливо у сфері міжнародних освітніх проєктів. Для педагогів це означає необхідність дотримання міжнародних стандартів при роботі з даними здобувачів, особливо якщо заклад бере участь у програмах академічної мобільності чи співпрацює з європейськими партнерами.

Таким чином, правове регулювання цифрової безпеки в освіті формує комплексну систему вимог, яка поєднує національні та міжнародні стандарти. Воно забезпечує не лише технічний захист даних, а й гарантує права учасників освітнього процесу, створюючи основу для формування культури цифрової безпеки як невід'ємної складової професійної компетентності сучасного педагога.

У нашому контексті варто розглянути не лише правові рамки врегулювання порушеного питання, а й приклади з освітньої практики, оскільки цифрова безпека в освіті проявляється не тільки у використанні технічних засобів захисту, а й у щоденній роботі педагогів, оскільки щоденна практика з цифровими ресурсами неминуче супроводжується низкою небезпек, які можуть мати серйозні наслідки як для окремого педагога, так і для закладу освіти загалом. Усвідомлення цих загроз є необхідною передумовою формування культури безпечної поведінки у цифровому середовищі. Саме тому наступним кроком нашого аналізу є окреслення ключових ризиків, з якими стикається сучасний педагог у процесі професійної діяльності:

– Витік персональних даних – приклади з електронних журналів, освітніх платформ.

– Кібербулінг та онлайн-агресія – вплив на психіку учнів, роль педагога як модератора.

– Фішинг та шахрайство – типові сценарії, як освітяни можуть стати жертвами.

– Маніпуляції та дезінформація – приклади фейкових новин, формування критичного мислення.

– Залежність від цифрових технологій – баланс між реальним і віртуальним життям.

– Технічні загрози та збої – віруси, атаки, несправність обладнання.

Одним із найбільш показових прикладів є робота з електронними журналами та системами управління навчальним процесом. У таких системах зберігається значний масив персональних даних: прізвища та імена учнів, результати навчання, інформація про відвідування занять, а також контактні дані батьків та особисті – здобувачів, і будь-яка необережність у використанні цих ресурсів може призвести до витоку конфіденційної інформації. Тому педагоги мають дотримуватися правил доступу, використовувати надійні паролі та двофакторну автентифікацію, а також уникати практики передачі логінів і паролів стороннім особам. У такому контексті цифрова безпека стає не лише технічним завданням, а й елементом професійної етики педагога.

Іншим важливим прикладом є конфіденційність комунікації між педагогами та батьками. У сучасних умовах значна частина спілкування відбувається через електронну пошту, месенджери чи освітні платформи. Важливо пам'ятати, що навіть звичайне повідомлення про успішність учня чи його поведінку містить персональні дані, які підлягають захисту відповідно до Закону України «Про захист персональних даних». Саме тому педагог повинен обирати безпечні канали комунікації, уникати надмірного поширення інформації та дотримуватися принципу мінімізації даних – передавати лише ті відомості, які є необхідними для вирішення конкретної ситуації, максимально анонімізуючи особистість здобувача.

Ці приклади демонструють, що цифрова безпека в освітньому середовищі виходить далеко за межі технічних налаштувань комп'ютера чи смартфона. Вона охоплює щоденні практики педагогів, їхню відповідальність за захист інформації та формування довіри між усіма учасниками освітнього процесу. Саме через такі конкретні дії – захист електронних журналів, конфіденційність розмов із батьками, обережність у використанні цифрових платформ – формується культура цифрової безпеки, яка стає невід'ємною складовою професійної компетентності сучасного педагога, а цифрова безпека в освітньому середовищі проявляється у щоденних діях педагогів, які часто здаються рутинними, але мають стратегічне значення для захисту даних та довіри учасників освітнього процесу. Це формує культуру відповідального ставлення до інформації та підвищує довіру між школою та родинами.

Ще одним прикладом є використання хмарних сервісів для зберігання навчальних матеріалів. З одного боку, вони забезпечують зручність доступу та можливість спільної роботи, з іншого – створюють ризики витоку даних у разі неналежного налаштування доступу. Педагог має чітко розмежовувати особисті та професійні акаунти, встановлювати обмеження для сторонніх користувачів та регулярно перевіряти

налаштування конфіденційності усіх навчальних матеріалів та освітнього контенту загалом.

Окремої уваги заслуговує й використання соціальних мереж у навчальному процесі. Вони можуть бути ефективним інструментом комунікації та мотивації учнів, але водночас несуть ризики надмірного поширення особистої інформації, кібербулінгу чи маніпуляцій. Педагог, який використовує соціальні мережі для освітніх цілей, має демонструвати приклад відповідальної поведінки онлайн: уникати публікації персональних даних учнів, формувати критичне ставлення до інформації та пояснювати здобувачам освіти правила безпечної взаємодії у цифровому середовищі, а також правила і механізми протидії кібербулінгу.

Таким чином, приклади з освітньої практики – захист електронних журналів, конфіденційність розмов із батьками, робота з хмарними сервісами та соціальними мережами – показують, що цифрова безпека в освітньому середовищі є багатовимірним явищем, що охоплює технічні, організаційні та етичні аспекти, які разом формують культуру безпечної поведінки в освіті. Саме через такі конкретні дії педагоги стають провідниками цифрової безпеки, забезпечуючи довіру, якість освітнього процесу та готовність суспільства до викликів цифрової епохи.

Усвідомлення розглянутих ризиків цифрового середовища є лише першим кроком на шляху до формування культури безпечної поведінки в освітньому середовищі. Проте індивідуальні зусилля окремих педагогів не можуть повністю гарантувати захист усіх учасників освітнього процесу. Цифрова безпека потребує системного підходу, який охоплює не лише особисту відповідальність, а й організаційні рішення на рівні закладу освіти. Саме інституційна підтримка, чіткі правила та колективні практики створюють умови для того, щоб цифрова безпека стала невід'ємною частиною освітньої культури. Тому наступним важливим аспектом нашого аналізу є визначення ролі закладу освіти у формуванні та підтримці цієї культури.

Інституційна відповідальність закладу освіти у сфері цифрової безпеки полягає насамперед у створенні та впровадженні внутрішніх політик, які регламентують роботу з цифровими ресурсами. Такі політики мають визначати правила доступу до електронних журналів, освітніх платформ, хмарних сервісів та інших цифрових інструментів, що використовуються у навчальному процесі, а також «внутрішні політики закладу освіти у сфері цифрової безпеки мають бути не формальністю, а реальним інструментом регулювання доступу до ресурсів та захисту даних учасників освітнього процесу» [4, с. 57], адже вони забезпечують єдиний стандарт поведінки для всіх учасників освітнього середовища та знижують ризики витоку даних чи порушення конфіденційності.

Важливим аспектом інституційної відповідальності є організація системи контролю доступу: заклад освіти має визначати рівні прав користувачів, обмежувати доступ до конфіденційної інформації лише для тих працівників, які безпосередньо працюють із нею, та впроваджувати технічні засоби захисту – від паролів і двофакторної автентифікації до регулярного моніторингу безпеки систем. Такий підхід дозволяє не лише захистити дані, а й формує у педагогів та адміністрації усвідомлення власної відповідальності за цифрову безпеку.

Не менш значущим є включення цифрової безпеки до навчальних програм закладу освіти. Це стосується як підготовки педагогів, так і формування компетентностей учнів, а інтеграція тем цифрової гігієни, захисту персональних даних, критичного мислення щодо інформації у навчальні курси сприяє тому, що культура цифрової безпеки стає частиною освітнього процесу, а не додатковою чи факультативною практикою. Таким чином, заклад освіти виконує роль не лише адміністратора цифрових ресурсів, а й провідника знань та навичок у сфері цифрової безпеки.

Зрештою, інституційна відповідальність закладу освіти полягає у створенні середовища довіри. Коли учні, батьки та педагоги впевнені, що їхні дані захищені, а правила цифрової поведінки є зрозумілими та прозорими, уніфікованими та сталими, це підвищує якість освітнього процесу та зміцнює авторитет закладу. Цифрова безпека у цьому випадку виступає не лише технічним чи правовим аспектом, а й важливим чинником формування позитивного іміджу освітньої установи та її готовності до викликів сучасного інформаційного суспільства.

У такому контексті лідерство педагога у сфері цифрової безпеки проявляється насамперед у його здатності демонструвати приклад відповідальної поведінки в цифровому середовищі, адже здобувачі освіти часто наслідують дії своїх наставників, тому саме педагог стає для них орієнтиром у питаннях безпечного використання технологій. Використання надійних паролів, обережність у поширенні особистої інформації, критичне ставлення до цифрового контенту – усе це формує в учнів практичні навички,

які вони переймають через щоденну взаємодію з учителем. А надважливою складовою лідерства є здатність педагога не лише дотримуватися правил цифрової гігієни, а й пояснювати їх значення учням. Коли освітянин відкрито говорить про ризики кібербулінгу, фішингу чи дезінформації, він формує у здобувачів освіти критичне мислення та навички самозахисту, і саме такий підхід перетворює педагога на наставника, який не просто навчає предмета, а й виховує культуру безпечної поведінки у цифровому світі.

Безперечно, лідерство педагога у сфері цифрової безпеки має також інституційний вимір, адже вчитель, який демонструє приклад безпечної поведінки онлайн, стає агентом змін у закладі освіти, впливаючи на колег та адміністрацію, його практики можуть бути інтегровані у внутрішні політики закладу, а його досвід – використаний для розробки методичних рекомендацій. У своїх працях В. О. Ігнатенко та Ю. Б. Мирошніченко підкреслюють: «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» [5]. Таким чином, лідерство окремого педагога виходить за межі індивідуальної відповідальності й стає чинником формування колективної культури цифрової безпеки.

Як бачимо, інституційна відповідальність закладу освіти і лідерство педагога гармонійно взаємодоповнюють одне одне: освітня установа створює правила, політики та навчальні програми, які забезпечують системний рівень цифрової безпеки, тоді як педагог у щоденній практиці демонструє приклад безпечної поведінки онлайн, а саме таке поєднання інституційних та індивідуальних зусиль формує цілісну культуру цифрової безпеки, яка стає невід'ємною частиною освітнього процесу.

Важливо наголосити, що цифрова безпека не може бути ефективною без узгодженості дій усіх учасників освітнього середовища. Якщо заклад освіти забезпечує технічні та організаційні умови, а педагог демонструє відповідальну поведінку, то учні та студенти отримують не лише знання, а й практичні навички безпечної взаємодії з цифровими технологіями, що створює основу для формування критичного мислення, відповідального ставлення до інформації та здатності протидіяти цифровим загрозам.

Зрештою, роль закладу освіти та лідерство педагога у сфері цифрової безпеки виходять за межі суто технічних завдань. Вони стають чинниками формування довіри між учасниками освітнього процесу, підвищення якості навчання та зміцнення авторитету освітньої установи. Саме завдяки такій взаємодії цифрова безпека перетворюється на стратегічну компетентність, що визначає готовність суспільства до викликів сучасної інформаційної епохи. Про це наголошує В. В. Олійник: «Формування цифрової компетентності педагога неможливе без усвідомлення ризиків інформаційної безпеки та відповідального ставлення до захисту персональних даних» [6].

Отже, розглянувши попередні пункти, можемо виділити певні практичні орієнтири для педагогів у площині цифрової безпеки, котрі включають *у першу чергу* використання надійних паролів, регулярне їх оновлення та застосування різних комбінацій символів, що ускладнюють несанкціонований доступ. Важливим є також систематичне оновлення програмного забезпечення, адже саме застарілі версії часто стають уразливими для атак. Не менш значущим є створення резервних копій даних, що дозволяє уникнути їхньої втрати у випадку технічних збоїв чи вірусних атак: це так звана базова цифрова гігієна, що є базовим рівнем захисту, який кожен педагог має інтегрувати у свою щоденну діяльність.

Другим важливим орієнтиром є дотримання конфіденційності та захисту персональних даних. Педагогічні працівники щодня працюють із великим масивом інформації про здобувачів та їхні родини, тому будь-яка необережність може призвести до серйозних наслідків. Використання лише захищених каналів комунікації, обмеження доступу до конфіденційних даних та дотримання принципу мінімізації інформації – це ті практики, які мають стати нормою. У такому контексті особливу увагу слід приділити використанню двофакторної автентифікації. Це один із найефективніших інструментів захисту акаунтів, який значно знижує ризик несанкціонованого доступу навіть у випадку компрометації пароля, тож для педагогів, які працюють із освітніми платформами чи електронними журналами, двофакторна автентифікація має стати стандартом. Вона не лише забезпечує додатковий рівень захисту, а й формує у здобувачів освіти приклад відповідальної поведінки у цифровому середовищі.

Третім орієнтиром у площині цифрової безпеки є формування навичок критичного мислення у здобувачів освіти. Педагоги повинні систематично інтегрувати у навчальний процес вправи, що допомагають учням

аналізувати джерела інформації, перевіряти факти та розпізнавати маніпулятивні повідомлення, адже це не лише знижує ризик поширення дезінформації, але й формує культуру відповідального використання цифрових ресурсів. І, відповідно, критичне мислення стає базовою компетентністю, яка забезпечує стійкість освітнього середовища до інформаційних атак.

Четвертим важливим аспектом можемо виділити самонавчання педагогів у сфері цифрової безпеки. Регулярне ознайомлення з новими інструментами захисту, участь у тренінгах та використання практичних кейсів дозволяють підтримувати актуальний рівень компетентності. Тож самонавчання сприяє не лише професійному розвитку, але й підвищує довіру з боку учнів та батьків, адже педагог демонструє готовність відповідати на сучасні виклики цифрового середовища.

Нарешті, *п'ятий орієнтир* безсумнівно стосується інституційної підтримки та створення спільнот практики. Заклади освіти мають забезпечувати педагогів методичними матеріалами, рекомендаціями та платформами для обміну досвідом. Формування професійних спільнот, де обговорюються проблеми цифрової безпеки та поширюються успішні практики, сприяє колективному підвищенню рівня захисту. Такий підхід дозволяє не лише стандартизувати вимоги, але й створює атмосферу взаємної підтримки, що є ключовим чинником у формуванні культури цифрової безпеки в освітньому середовищі.

Висновки. Цифрова безпека сьогодні є ключовою компетентністю сучасного педагога, котра визначає не лише якість освітнього процесу, а й рівень довіри між учасниками освітнього середовища. Педагог, який володіє знаннями та навичками цифрової безпеки, здатен не лише захистити власні дані, а й сформувати у здобувачів освіти культуру відповідальної поведінки у цифровому просторі, що перетворює цифрову безпеку на стратегічний чинник професійної діяльності та має безпосередній вплив на розвиток суспільства в умовах інформаційної епохи.

Важливо усвідомлювати, що цифрова безпека не може бути ефективною без системного підходу та комплексних узгоджених рішень, як на індивідуальному рівні вчителя, так і на рівні закладу освіти та державному – законодавчому загалом. Індивідуальні навички педагога – використання надійних паролів, двофакторної автентифікації, критичне ставлення до інформації – є лише частиною загальної системи. Вони мають бути доповнені інституційними політиками закладу освіти, які регламентують правила доступу, конфіденційність даних та організацію цифрової гігієни, бо лише поєднання індивідуальних і колективних практик забезпечує комплексний захист освітнього середовища.

Заклади освіти повинні бути простором формування культури цифрової безпеки для всіх учасників освітнього процесу, що означає не лише створення технічних умов для захисту даних, а й інтеграцію тем цифрової гігієни та критичного мислення у навчальні програми. Освітні установи повинні виховувати у здобувачів освіти навички безпечної взаємодії з цифровими технологіями, адже саме вони визначатимуть готовність майбутніх поколінь до викликів інформаційного суспільства. Зрештою, цифрова безпека в освіті є не другорядним технічним питанням, а фундаментальною складовою професійної компетентності педагога та стратегічною потребою суспільства. Вона поєднує правові, технічні, організаційні та етичні аспекти, створюючи цілісну систему захисту, тож саме завдяки цьому цифрова безпека стає гарантією довіри, якості освітнього процесу та стійкості суспільства перед викликами сучасної епохи.

Використані джерела

1. Закон України «Про захист персональних даних» від 01 червня 2010 р. № 2297-VI. *Відомості Верховної Ради України.* 2010. № 34. Ст. 481. URL: https://zakon.rada.gov.ua/laws/show/2297-17?utm_source#Text

2. Закон України «Про основні засади забезпечення кібербезпеки України» від 05 жовтня 2017 р. № 2163-VIII. *Відомості Верховної Ради України.* 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19?utm_source#Text

3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR). Official Journal of the European Union. L. 119. 2016. 4 May. P. 1–88. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&utm_source

4. Рубльова Н. О. Цифрова безпека в освітньому середовищі: від основ до практики : наук.-практ. посіб. Луцьк : ФОП Мажула Ю. М., 2026. 132 с.

5. Ігнатенко В. О., Мирошніченко Ю. Б. Інформаційна безпека в сучасному цифровому освітньому середовищі. *Наукові записки.* 2025. № 160. DOI: https://doi.org/10.31392/NZ-udu-160.2025.06

6. Стойка О. Я. Особливості цифрової трансформації професійної підготовки вчителів в Україні. *Педагогічні науки* : *зб. наук. пр.* 2023. Вип. 102. С. 54–61. URL: https://ps.journal.kspu.edu/index.php/ps/article/view/4547