DOI : https://doi.org/10.51706/2707-3076-2025-12-2
УДК 37:004.946.5:316.772.5-049.5

Маріанна Василівна Швардак
ORCID iD https://orcid.org/0000-0002-9560-9008
докторка педагогічних наук, професорка,
професорка кафедри педагогіки дошкільної, початкової освіти та освітнього менеджменту
Мукачівський державний університет
м. Мукачево, Україна
anna-mari_p@ukr.net

КІБЕРБЕЗПЕКА У ЦИФРОВОМУ ОСВІТНЬОМУ ПРОСТОРІ

Науково-методична стаття присвячена аналізу загроз кібербезпеці у цифровому освітньому просторі задля визначення ефективних стратегій його захисту засобами комплексного підходу. Кібербезпеку в умовах цифрового освітнього простору визначено як комплекс заходів, спрямованих на захист інформації, технологій та користувачів, які взаємодіють у середовищі онлайн-освіти. Видами кібербезпеки визначені: мережева безпека, безпека даних, хмарна безпека, безпека кінцевих пристроїв, соціальна інженерія та кібергігієна, захист від DDoS-атак, криптографічний захист, правовий аспект кібербезпеки. Стратегіями захисту у цифровому освітньому просторі визначені такі: розробка політики кібербезпеки, захист облікових записів та доступу, навчання цифровій грамотності та кібергігієні, шифрування даних та безпечне зберігання інформації, регулярне оновлення програмного забезпечення, моніторинг та реагування на кіберзагрози, захист від шкідливого програмного забезпечення, протидія кібербулінгу та соціальній інженерії, захист освітніх платформ від DDoS-атак, резервне копіювання важливих даних.

Ключові слова: *безпека, кібербезпека, кіберзагроза, цифровий освітній простір, цифрова грамотність.*

Вступ. У сучасному світі цифровізація стала невід'ємною частиною освітнього процесу. Використання цифрових технологій у навчанні відкриває широкі можливості для підвищення якості освіти, забезпечення доступу до інформації та створення інноваційного освітнього середовища. Однак разом із позитивними аспектами цифровізації виникають і серйозні виклики, пов'язані з кібербезпекою. Освітні установи дедалі частіше стають об'єктами кібератак, зокрема через вразливість цифрових платформ, недостатній рівень цифрової грамотності учасників освітнього процесу та недостатнє впровадження сучасних засобів захисту інформації. Зловмисники можуть отримати доступ до персональних даних здобувачів освіти, вчителів/викладачів і батьків, викрасти конфіденційну інформацію чи порушити роботу освітніх платформ. Особливу загрозу становить також низький рівень обізнаності учасників освітнього процесу про основні принципи кібергігієни, що може призводити до небажаних наслідків, включно з витоком даних, шкідливим програмним забезпеченням і навіть загрозами фізичній безпеці через цифрові канали. Таким чином, проблема забезпечення кібербезпеки у цифровому освітньому просторі стає ключовою для забезпечення ефективності, стабільності та довіри до освітніх процесів у цифрову епоху. Дослідження цієї проблематики є необхідним для розробки ефективних стратегій захисту даних та підвищення цифрової грамотності учасників освітнього процесу.

Проблематика кібербезпеки у цифровому освітньому просторі є однією з ключових у сучасних наукових дослідженнях, що зумовлено стрімким упровадженням цифрових технологій у сферу освіти. Зокрема, увага дослідників зосереджена на питаннях забезпечення захисту інформації, підвищення цифрової грамотності учасників освітнього процесу, а також упровадження засобів і стратегій протидії кіберзагрозам. Відтак, В. Савченко та О. Маклюк (2024) у своїй науковій публікації визначають кібербезпеку як фактор ефективного функціонування закладів вищої освіти. Автори наголошують, що цифровізація відкриває нові можливості для освітніх закладів, проте водночас створює ризики, пов'язані з кібератаками, викраденням конфіденційної інформації та

порушенням функціонування навчальних платформ. У статті запропоновано організаційні заходи та рекомендації щодо підвищення рівня кібербезпеки. У роботі В. Коваленко та Т. Осипчук (2024) розглядається розвиток цифрової компетентності з кібербезпеки вчителів загальної середньої освіти. Автори акцентують увагу на необхідності інтеграції знань із кібербезпеки до навчальних програм для педагогів, що сприятиме формуванню культури безпечного використання цифрових технологій. С. Доценко (2023) аналізує аспекти забезпечення кібербезпеки учасників освітнього процесу в умовах дистанційного навчання. Автор відзначає, що дистанційна освіта значно посилила вразливість навчальних платформ до кібератак, та пропонує рекомендації щодо захисту персональних даних здобувачів освіти і викладачів. Таким чином, попередні дослідження підкреслюють важливість розвитку цифрової грамотності, впровадження ефективних механізмів захисту даних та інтеграції принципів кібергігієни до освітнього процесу. Однак, потреба в розробці комплексної стратегії забезпечення кібербезпеки залишається актуальною, зважаючи на зростаючі обсяги цифрової інформації та різноманіття кібератак у сучасному освітньому середовищі.

Метою статті є аналіз загроз кібербезпеці у цифровому освітньому просторі задля визначення ефективних стратегій його захисту. Завдання статті: визначити сутність, мету та види кібербезпеки у цифровому освітньому просторі; здійснити аналіз основних кібезагроз; окреслити ефективні стратегії захисту у цифровому освітньому просторі.

Для реалізації поставлених цілей у дослідженні використано такі **методи науково-педагогічного дослідження** як: аналіз наукової літератури – для визначення сутності, мети та видів кібербезпеки у цифровому освітньому просторі; порівняльний аналіз – для дослідження основних кіберзагроз та їхнього впливу на освітній процес; систематизація та узагальнення – для класифікації загроз і формулювання стратегій захисту цифрового освітнього середовища; емпіричний аналіз – для вивчення реальних випадків кіберзагроз у сфері освіти та розробки практичних рекомендацій щодо мінімізації ризиків.

Сутність, мета та види кібербезпеки у цифровому освітньому просторі. Здійснивши аналіз сучасної наукової літератури, кібербезпеку в умовах цифрового освітнього простору розглядаємо як комплекс заходів, спрямованих на захист інформації, технологій та користувачів, які взаємодіють у середовищі онлайн-освіти (Коваленко, Осипчук, 2024). У сучасному світі освітній процес усе більше залежить від цифрових технологій: використання електронних інформаційних систем управління освітою, інформаційно-аналітичних систем, баз даних, освітніх платформ, проведення онлайн-занять, обмін інформацією через хмарні сервіси та застосунки, які стали невід'ємною частиною навчання. У такому контексті кібербезпека відіграє ключову роль, забезпечуючи конфіденційність, цілісність і доступність даних усіх учасників освітнього процесу.

Відповідно, основною метою кібербезпеки є захист конфіденційності, цілісності та доступності даних. Конфіденційність означає, що інформація доступна лише для тих, хто має право її бачити, наприклад, персональні дані, банківська інформація або корпоративні секрети. Цілісність гарантує, що дані залишаються незмінними й достовірними, а доступність забезпечує можливість користуватися ресурсами та інформацією тоді, коли це потрібно.

У сфері освіти кібербезпека потрібна для забезпечення безпечного доступу до навчальних платформ, захисту персональних даних здобувачів освіти і вчителів/викладачів, а також для створення стабільного цифрового середовища, у якому можливо ефективно навчатися й працювати.

Кібербезпека також необхідна для захисту від загроз, які можуть спричинити значні фінансові та репутаційні втрати. Хакерські атаки, витоки даних, програми-вимагачі чи збої у функціонуванні систем можуть паралізувати роботу закладу освіти, державних установ або освітніх платформ. У цьому контексті кібербезпека є основою для безперебійної роботи організацій і збереження довіри користувачів (Баранов, 2014).

Таким чином, кібербезпека є основним інструментом, який забезпечує надійність і безпеку у світі, де цифрові технології стали центральним елементом комунікації, бізнесу, навчання та багатьох інших сфер. Вона сприяє захисту від сучасних загроз, зберігаючи стабільність та ефективність функціонування цифрового середовища.

Кібербезпека в цифровому освітньому просторі охоплює кілька ключових видів захисту, які допомагають убезпечити дані, користувачів та інформаційні системи. Виділимо основні види кібербезпеки в освітньому середовищі:

1. Мережева безпека – захист локальних і глобальних мереж закладів освіти від кібератак, вірусів, несанкціонованого доступу та витоку даних. Включає використання міжмережевих екранів (фаєрволів), систем виявлення вторгнень (IDS/IPS) та шифрування даних.
2. Безпека даних – заходи щодо захисту особистих даних здобувачів освіти, вчителів/викладачів і співробітників від витоку, крадіжки або маніпуляцій. Включає резервне копіювання, контроль доступу та політику конфіденційності.
3. Хмарна безпека – захист інформації, що зберігається у хмарних сервісах (Google Classroom, Moodle, Microsoft Teams тощо). Важливими заходами є багатофакторна автентифікація, моніторинг активності та шифрування файлів.
4. Безпека кінцевих пристроїв – охоплює захист комп'ютерів, планшетів, смартфонів, що використовуються для навчання. Включає встановлення антивірусних програм, оновлення програмного забезпечення та контроль за встановленням додатків.
5. Соціальна інженерія та кібергігієна – заходи щодо підвищення обізнаності користувачів про можливі загрози, такі як фішинг, шахрайські повідомлення, маніпуляції з боку зловмисників. Важливо проводити тренінги та роз'яснювальну роботу серед учасників освітнього процесу.
6. Захист від DDoS-атак – необхідний для стабільної роботи онлайн-платформ і освітніх сайтів. Включає використання спеціальних систем фільтрації трафіку та серверних рішень для протидії масовим атакам.
7. Криптографічний захист – застосовується для шифрування електронних повідомлень, файлів та баз даних, щоб забезпечити конфіденційність інформації.
8. Правовий аспект кібербезпеки – дотримання законодавчих норм щодо обробки персональних даних (GDPR, Закон України «Про захист персональних даних»), розробка внутрішніх політик інформаційної безпеки (Фурашев, 2012).

Ефективна кібербезпека в освіті забезпечується комплексним підходом, що включає технічні рішення, організаційні заходи та освітню роботу.

Цифровізація освітнього процесу суттєво розширила можливості навчання, проте разом із цим виникли нові кіберзагрози, які можуть завдати шкоди учасникам освітнього процесу та інфраструктурі закладів освіти. Основні загрози кібербезпеці в цифровій освіті подано у таблиці 1:

Таблиця 1.

Основні загрози кібербезпеці в цифровій освіті

Кіберзагроза	**Суть загрози**	**Можливі наслідки**	**Як запобігти**
Несанкціонований доступ до освітніх платформ	Зловмисники можуть отримати доступ до особистих акаунтів учасників освітнього процесу через слабкі паролі, фішинг або використання вразливостей у системах.	– Викрадення персональних даних. – Видалення або зміна навчальних матеріалів. – Маніпуляція оцінками або іншими важливими даними.	– Використання двофакторної автентифікації (2FA). – Регулярна зміна паролів. – Використання складних паролів.
Фішинг та соціальна інженерія	Фішингові атаки – це спроби шахраїв отримати конфіденційну	– Викрадення облікових записів та персональних даних. – Розповсюдження шкідливого	– Не відкривати підозрілі листи та посилання. – Перевіряти достовірність

	інформацію (логіни, паролі, банківські дані) шляхом надсилання підроблених електронних листів або повідомлень.	програмного забезпечення. – Втручання в освітній процес.	відправників. – Використовувати антивірусне програмне забезпечення.
Витік персональних даних	Вразливості в освітніх системах або хакерські атаки можуть призвести до викрадення персональної інформації здобувачів освіти, викладачів і співробітників.	– Використання даних у шахрайських цілях. – Продаж особистої інформації в «темному інтернеті». – Використання викрадених даних для кібератак.	– Захист баз даних за допомогою шифрування. – Використання VPN та безпечних каналів зв'язку. – Обмеження доступу до конфіденційної інформації.
Кібербулінг (кіберзнущання)	Анонімність у цифровому середовищі сприяє поширенню цькування, погроз і образ серед здобувачів через соціальні мережі, чати, форуми тощо.	– Психологічний тиск і стрес у постраждалих. – Зниження академічної успішності. – Суїцидальні настрої у жертв кібербулінгу.	– Контроль комунікацій у навчальних платформах. – Створення правил безпечного спілкування в освітньому просторі. – Наявність механізмів анонімного повідомлення про кібербулінг.
Віруси та шкідливе програмне забезпечення	Віруси, трояни та програми-вимагачі можуть потрапляти на комп'ютери через заражені файли, посилання або підроблені програми.	– Втрата або пошкодження навчальних матеріалів. – Блокування доступу до файлів (віруси-вимагачі). – Витік конфіденційної інформації.	– Регулярне оновлення антивірусного програмного забезпечення. – Не завантажувати файли з ненадійних джерел. – Перевіряти програми перед встановленням.
DDoS-атаки на освітні сервіси	DDoS-атаки перевантажують сервери навчальних платформ та онлайн-курсів, що робить їх	– Зрив дистанційного навчання. – Неможливість доступу до важливих ресурсів. – Фінансові витрати на відновлення роботи	– Використання систем моніторингу кіберзагроз. – Захист серверів від перевантаження. – Оптимізація інфраструктури для

	недоступними для користувачів.	систем.	протидії атакам.
Вразливості у програмному забезпеченні	Використання застарілих або незахищених навчальних платформ створює ризики для користувачів.	– Несанкціонований доступ до даних. – Маніпуляція результатами навчання. – Впровадження шкідливого коду.	– Регулярне оновлення програмного забезпечення. – Використання ліцензійних навчальних платформ. – Перевірка програм перед установкою.

Цифрова освіта має величезний потенціал, але її безпека залежить від комплексного підходу до захисту інформації, підвищення кіберграмотності учасників освітнього процесу та використання сучасних технологій безпеки. Впровадження надійних механізмів кіберзахисту допоможе уникнути загроз та створити безпечне освітнє середовище.

Стратегії захисту цифрового освітнього простору. Ефективний захист цифрового освітнього середовища вимагає комплексного підходу, що включає технічні, організаційні та освітні заходи. Безпека повинна бути пріоритетом як для освітніх установ, так і для здобувачів освіти та викладачів, які користуються цифровими технологіями.

1. Розробка політики кібербезпеки. Освітні заклади повинні мати чітко сформульовану політику кібербезпеки, яка містить правила використання цифрових ресурсів, управління обліковими записами, збереження конфіденційної інформації та реагування на інциденти. Така політика має бути офіційно затвердженою, а її положення – доступними для всіх учасників освітнього процесу.
2. Захист облікових записів та доступу. Використання двофакторної автентифікації (2FA) є обов'язковим для викладачів та керівництва, а також бажаним для здобувачів освіти. Паролі повинні бути складними та унікальними для кожного облікового запису. Адміністратори освітніх платформ повинні контролювати рівні доступу, щоб уникнути несанкціонованого входу та змін у системі.
3. Навчання цифровій грамотності та кібергігієні. Освітні заклади мають регулярно проводити тренінги з кібербезпеки для здобувачів освіти, викладачів і технічного персоналу. Користувачі повинні знати, як розпізнавати фішингові атаки, уникати кібербулінгу, безпечно працювати з онлайн-ресурсами та захищати особисті дані. Важливо формувати культуру відповідального використання цифрових технологій (Коваленко, Осипчук, 2024).
4. Шифрування даних та безпечне зберігання інформації. Персональні дані здобувачів освіти та викладачів, а також освітні матеріали повинні зберігатися у зашифрованому вигляді. Захищене хмарне середовище або локальні сервери з багаторівневим контролем доступу дозволяють мінімізувати ризики витоку конфіденційної інформації.
5. Регулярне оновлення програмного забезпечення. Операційні системи, навчальні платформи та антивірусне програмне забезпечення повинні оновлюватися своєчасно, щоб усувати вразливості, які можуть використовувати зловмисники. Автоматичні оновлення та контроль за безпекою додатків знижують ймовірність кібератак (Bakhmat et al., 2022).
6. Моніторинг та реагування на кіберзагрози. Освітні установи мають використовувати системи моніторингу мережевого трафіку та виявлення аномальної активності. Регулярний аналіз кіберзагроз дозволяє вчасно реагувати на потенційні атаки та мінімізувати їх наслідки. Крім того, важливо мати план дій у разі виникнення інцидентів, щоб швидко відновити роботу систем.
7. Захист від шкідливого програмного забезпечення. Всі пристрої, що використовуються для навчання, мають бути захищені сучасним антивірусним програмним забезпеченням. Заборонено встановлення невідомих програм, а завантаження файлів має здійснюватися лише з перевірених джерел. Контроль доступу до USB-накопичувачів та інших зовнішніх носіїв допоможе уникнути зараження вірусами.

8. Протидія кібербулінгу та соціальній інженерії. Заклади освіти повинні впроваджувати механізми анонімного повідомлення про випадки кібербулінгу, а також проводити роз'яснювальну роботу серед здобувачів освіти про наслідки цькування в інтернеті. Викладачі та адміністрація мають активно відстежувати прояви агресії в цифровому середовищі та оперативно реагувати на такі випадки.

9. Захист освітніх платформ від DDoS-атак. Сервери освітніх платформ повинні бути оптимізовані для роботи під навантаженням, а також захищені від атак типу «відмова в обслуговуванні» (DDoS). Використання хмарних сервісів із вбудованими механізмами захисту дозволяє мінімізувати ризики зриву освітнього процесу.

10. Резервне копіювання важливих даних. Регулярне створення резервних копій навчальних матеріалів, баз даних здобувачів освіти і викладачів допомагає швидко відновити інформацію у разі збоїв, атак програм-вимагачів або технічних несправностей. Копії повинні зберігатися на захищених серверах та бути доступними лише адміністраторам.

Комплексне впровадження цих стратегій допоможе значно підвищити рівень безпеки цифрового освітнього простору та захистити всіх його учасників від кіберзагроз.

Висновки. Цифровізація освіти значно покращила доступ до навчальних матеріалів і зробила освітній процес більш гнучким, водночас спричинила серйозні виклики у сфері кібербезпеки. Зростання кількості кібератак, витоків персональних даних, фішингових схем і DDoS-атак свідчить про необхідність комплексного підходу до захисту освітнього простору. Аналіз проблеми підтвердив, що ефективна кібербезпека базується на трьох ключових складових: технологічному захисті, організаційних заходах та підвищенні цифрової грамотності учасників освітнього процесу. Сучасні освітні заклади мають упроваджувати надійні системи захисту даних, такі як шифрування інформації, багатофакторна автентифікація та регулярне оновлення програмного забезпечення. Важливим аспектом є формування культури кібергігієни серед здобувачів освіти і викладачів, що передбачає навчання безпечному використанню цифрових технологій та вміння розпізнавати потенційні загрози. Загалом, забезпечення кібербезпеки у цифровому освітньому просторі є необхідною умовою для стабільного функціонування закладів освіти та захисту всіх учасників освітнього процесу. Комплексний підхід до вирішення цієї проблеми дозволить мінімізувати ризики та забезпечити безпечне використання цифрових технологій в освіті.

Подальші дослідження у цій сфері будуть зосереджені на розробці більш ефективних механізмів захисту освітніх платформ, удосконаленні методів запобігання витоку даних та впровадженні штучного інтелекту для автоматизованого моніторингу кіберзагроз. Також актуальним залишається питання адаптації міжнародних стандартів кібербезпеки до національної освітньої системи та розробка спеціальних освітніх програм із цифрової безпеки.

Література

Баранов О. А. Про тлумачення та визначення поняття «кібербезпека». *Правова інформатика.* 2014. № 2(42). С. 54–62.

Доценко С. О. Кібербезпека учасників освітнього процесу в умовах дистанційного навчання. *Психолого-педагогічні проблеми вищої і середньої освіти в умовах сучасних викликів: теорія і практика : матеріали VII Міжнар. наук.-практ. конф.*, Харків, 16–18 берез. 2023 р. Харків : ХНПУ ім. Г. С. Сковороди, 2023. С. 207–209.

Коваленко В., Осипчук Т. Проблема розвитку цифрової компетентності з кібербезпеки вчителів закладів загальної середньої освіти. *Фізико-математична освіта*. 2024. № 39(2). С. 35–41. DOI : https://doi.org/10.31110/fmo2024.v39i2-05

Савченко В., Маклюк О. Кібербезпека як фактор ефективності функціонування закладів вищої освіти. *Економіка та суспільство*. 2024. № 60. DOI : https://doi.org/10.32782/2524-0072/2024-60-24

Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*. 2012. № 2. С. 162–169.

Bakhmat N., Popadych O., Derkach L., Shvardak M., Lukashchuk M., Romanenko V. Using Information Technologies to Train Today Teachers in the Educational Environment. *Revista Romaneasca Pentru Educatie Multidimensionala*, 2022. Vol. 14(2). P. 479–499. DOI : https://doi.org/10.18662/rrem/14.2/591

References

Bakhmat, N., Popadych, O., Derkach, L., Shvardak, M., Lukashchuk, M., & Romanenko, V. (2022). Using information technologies to train today teachers in the educational environment. *Revista Romaneasca Pentru Educatie Multidimensionala*, *14*(2), 479–499. https://doi.org/10.18662/rrem/14.2/591 (eng).

Baranov, O. A. (2014). On the interpretation and definition of the concept of "cybersecurity". *Legal Informatics*, *2*(42), 54–62 (ukr).

Dotsenko, S. O. (2023). Cybersecurity of educational process participants in the conditions of distance learning. *Psychological and Pedagogical Problems of Higher and Secondary Education in the Conditions of Modern Challenges: Theory and Practice: Materials of the VII International Scientific and Practical Conference*, 16–18 March 2023 : H. S. Skovoroda KhNPU, 207–209 (ukr).

Furashev, V. M. (2012). Cyber space and information space, cybersecurity and information security: essence, definitions, differences. *Information and Law*, *2*, 162–169. (ukr).

Kovalenko, V., & Osypchuk, T. (2024). The problem of developing digital competence in cybersecurity among teachers of general secondary education institutions. \ *Physical and Mathematical Education*, *39*(2), 35–41. https://doi.org/10.31110/fmo2024.v39i2-05 (ukr).

Savchenko, V., & Makliuk, O. (2024). Cybersecurity as a factor of the efficiency of higher education institutions. *Economy and Society*, 60. https://doi.org/10.32782/2524-0072/2024-60-24 (ukr).

CYBERSECURITY IN THE DIGITAL EDUCATIONAL SPACE

Marianna Shvardak, doctor of pedagogical sciences, professor, professor of the department of pedagogy of preschool, primary education and educational management, Mukachevo State University, Mukachevo, Ukraine, e-mail: anna-mari_p@ukr.net

The article is devoted to the problem of ensuring cybersecurity. The purpose of the article is to analyze cybersecurity threats in the digital educational space in order to determine effective strategies for its protection using a comprehensive approach. The essence and purpose of cybersecurity in the digital educational space are determined. Cybersecurity in the digital educational space is defined as a set of measures aimed at protecting information, technologies and users who interact in the online education environment. The main goal of ensuring cybersecurity is to protect the confidentiality, integrity and availability of data. The types of cybersecurity are outlined (network security, data security, cloud security, end device security, social engineering and cyber hygiene, protection against DDoS attacks, cryptographic protection, legal aspect of cybersecurity). An analysis of the main cyber threats was conducted: unauthorized access to educational platforms, phishing and social engineering, personal data leakage, cyberbullying, viruses and malware, DDoS attacks on educational services, software vulnerabilities. The essence of each threat was revealed, possible consequences and practical advice on preventing a cyber threat were outlined. Protection strategies in the digital educational space were identified. In particular: developing a cybersecurity policy, protecting accounts and access, teaching digital literacy and cyber hygiene, data encryption and secure storage of information, regular software updates, monitoring and responding to cyber threats, protecting against malware, countering cyberbullying and social engineering, protecting educational platforms from DDoS attacks, backing up important data. The comprehensive implementation of these strategies will help to significantly increase the level of security of the digital educational space and protect all its participants from cyber threats. Ensuring cybersecurity in the digital educational space is a necessary condition for the stable functioning of educational institutions and the protection of all participants in the educational process. A comprehensive approach to solving this problem will minimize risks and ensure the safe use of digital technologies in education.

Keywords: *security, cybersecurity, cyber threat, digital educational space, digital literacy.*

Стаття надійшла до редакції / Received 15.03.2025
Прийнята до друку / Accepted 25.04.2025
Унікальність тексту 98,3 % («StrikePlagiarism» ID 331142087)

© Швардак Маріанна Василівна, 2025