https://doi.org/10.26565/2074-8922-2026-86-26
УДК (UDC): 37.014:004.056

Г. І. КАНЮК[1], доктор технічних наук,
завідувач кафедри автоматизації, метрології та енергоефективних технологій
e-mail: genadiykanuk@gmail.com , ORCID: https://orcid.org/0009-0008-0907-9719
Т. М. ФУРСОВА[1], кандидат технічних наук,
доцент кафедри автоматизації, метрології та енергоефективних технологій
e-mail: tatiana2507@ukr.net, ORCID: https://orcid.org/0000-0002-1423-0822
В. В. САБАДАШ[2], , кандидат технічних наук,
завідувач сектору
e-mail: kafedra_tsl@ukr.net , ORCID: https://orcid.org/0000-0001-9815-9009
І. В. САБАДАШ[3], кандидат юридичних наук,
головний державний інспектор-експерт
e-mail: saba-inna@ukr.net , ORCID: https://orcid.org/0000-0003-1967-9271
[1]*Харківський національний університет імені В.Н. Каразіна,*
майдан Свободи, 4, м. Харків, 61022, Україна
[2]*Харківський Науково-Дослідний Інститут Судових Експертиз ім. Засл. проф. М.С.Бокаріуса,*
вул. Золочівська, 8-а, м. Харків, 61177, Україна
[3]*Харківське управління експертиз та досліджень Спеціалізованої лабораторії з питань експертизи та досліджень Держмитслужби,*
вул. Бакуліна 6, м. Харків, 61166, Україна

ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ОСВІТНЬОМУ ПРОЦЕСІ

Мета статті полягає у дослідженні впливу цифровізації освітнього процесу на рівень інформаційної безпеки особистості та розроблення практичних рекомендацій щодо мінімізації ризиків витоку персональних даних у цифровому освітньому середовищі.

Методи, що використовувались для досягнення поставленої мети: аналіз та синтез наукових джерел із проблем цифрової безпеки, порівняльний метод для оцінювання функціональних можливостей сучасних інструментів захисту (менеджерів паролів, засобів шифрування, механізмів двофакторної автентифікації), а також системний підхід до розгляду кібербезпеки як комплексної взаємодії технічних, організаційних і поведінкових чинників. Застосовано узагальнення результатів для формулювання практичних рекомендацій.

Результати. Установлено, що цифровізація освіти суттєво розширює інформаційні можливості, але водночас підвищує рівень кіберризиків, зокрема пов'язаних із формуванням цифрового сліду, компрометацією облікових записів, фішинговими атаками та несанкціонованим збором персональних даних. Обґрунтовано необхідність упровадження принципів цифрової гігієни: використання унікальних паролів, менеджерів паролів із принципом zero-knowledge, багатофакторної автентифікації, регулярного оновлення програмного забезпечення, налаштування конфіденційності соціальних мереж і цифрових пристроїв. Розроблено рекомендації щодо безпечної організації онлайн-навчання, контролю доступу до відеоконференцій та формування культури кіберетики.

Висновки: доведено, що кібербезпека в освітньому процесі є не лише технічним завданням, а й важливою складовою цифрової культури та сталого розвитку суспільства. Формування відповідальної цифрової поведінки, підвищення рівня цифрової грамотності та впровадження комплексних заходів захисту інформації є ключовими умовами забезпечення безпечного, етичного й стійкого функціонування сучасного освітнього середовища.

КЛЮЧОВІ СЛОВА: *інформаційна безпека, цифровізація, технології, освіта, кібергігієна.*

Як цитувати: Канюк Г. І., Фурсова Т. М., Сабадаш В. В., Сабадаш І. В. Дослідження технологій інформаційної безпеки в освітньому процесі. *Проблеми інженерно-педагогічної освіти*. 2026. Вип. 86. С. 325-336. https://doi.org/10.26565/2074-8922-2026-86-26

In cites: Kanyuk G. I., Fursova T. M., Sabadash V. V., Sabadash I. V. (2026). Study of information security technologies in the educational process. *Problems of Engineering Pedagogic Education*, (86), 325-336. https://doi.org/10.26565/2074-8922-2026-86-26 (in Ukrainian)

Постановка проблеми в загальному вигляді

Сучасний етап розвитку інформаційного суспільства характеризується стрімким зростанням обсягів даних і широким упровадженням цифрових технологій у всі сфери людської діяльності. Цифровізація освіти докорінно змінила способи навчання, комунікації та обміну інформацією. Викладачі й студенти щоденно використовують десятки онлайн-ресурсів: освітні платформи, наукові бази, електронну пошту, хмарні сервіси, соціальні мережі. Водночас розширення цифрового середовища супроводжується зростанням ризиків — від несанкціонованого доступу до облікових записів до масштабних витоків персональних даних. Саме тому питання кібербезпеки в освітньому процесі є технічною та етичною проблемою сучасного інформаційного суспільства.

Щоденно зростає кількість і складність кіберзагроз, що зумовлює необхідність удосконалення методів забезпечення інформаційної безпеки. Однак, попри суттєві досягнення у цій сфері, залишається потреба в розробці прикладних методик аналізу та практичних засобів оцінки ефективності систем безпеки, особливо в контексті освітніх і науково-дослідних проєктів студентів. Забезпечення безпечного цифрового простору для студентів і викладачів є важливою передумовою формування культури відповідального користування інформаційними технологіями.

Дослідження кібербезпеки в освіті тісно пов’язане з реалізацією Цілей сталого розвитку ООН (Sustainable Development Goals, SDGs) [10, 18], зокрема:

Ціль 4 — забезпечення інклюзивної та якісної освіти, що передбачає безпечне цифрове середовище для навчання;

Ціль 9 — розвиток інновацій та інфраструктури, включно з надійними цифровими мережами;

Ціль 16 — сприяння побудові мирних і справедливих інституцій, зокрема шляхом захисту інформаційних прав людини та запобігання кіберзлочинності.

Отже, необхідно поєднання теоретичних підходів кіберзахисту з практичними засобами аналізу інформаційної безпеки, доступними для використання в навчальному процесі. Таке поєднання сприяє формуванню цифрової культури, розвитку критичного мислення й підвищенню рівня готовності майбутніх фахівців до протидії кіберзагрозам.

Аналіз останніх досліджень та публікацій

Аналіз сучасних вітчизняних наукових джерел свідчить, що проблема інформаційної безпеки в умовах цифровізації освіти є актуальним напрямом досліджень. У роботі [7] розглянуто специфіку забезпечення інформаційної безпеки викладачів, зокрема в умовах підвищених ризиків, пов’язаних із воєнним станом, що акцентує увагу на організаційних та поведінкових аспектах захисту. Дослідження [3] присвячене функціонуванню інформаційної безпеки в цифровому освітньому середовищі, де підкреслюється роль комплексного підходу до захисту даних. Автори в [2] розглядають цифрову безпеку як складову професійної компетентності педагогів, наголошуючи на необхідності формування цифрової культури.

Технічні аспекти кібербезпеки висвітлено у працях [5], де досліджено захист хмарних сервісів, а також [6]. Робота [4] зосереджуються на математичному моделюванні інформаційних процесів, що створює теоретичну основу для підвищення надійності систем безпеки. Окремо слід відзначити дослідження [1], де розкрито загрози деанонімізації особи за допомогою OSINT, що безпосередньо пов’язано з проблемою цифрового сліду.

У світовій науковій спільноті активно досліджуються питання цифрового сліду й приватності персональних даних. Роботи [9, 14] доводять, що цифровий слід є невід'ємною складовою цифрової взаємодії сучасної людини та виступає показником цифрової грамотності й етичної відповідальності. Ці автори також наголошують, що управління власним цифровим слідом є ключовим елементом цифрової компетентності, особливо в освітньому середовищі, де користувачі часто не усвідомлюють масштабу збору їхніх даних.

Окрему увагу в сучасних дослідженнях приділено ставленню користувачів до приватності та їх готовності використовувати інструменти захисту даних. Праці [19, 17] показують, що навіть за наявності технічних засобів безпеки користувачі часто демонструють низьку активність у їх застосуванні. Це зумовлює потребу в підвищенні рівня цифрової культури, особливо серед молоді. Статті, опубліковані у Frontiers in Education та PMC (2023) [13, 11], підкреслюють, що студенти як активні користувачі цифрових платформ мають недостатні знання щодо управління своїм цифровим слідом, що створює ризики як для особистої безпеки, так і для репутації в професійному майбутньому.

Важливою частиною аналізованих джерел є технічні рішення для збереження приватності — менеджери паролів, шифрування та zero-knowledge системи. Документація та whitepaper компанії Bitwarden [8, 15-12, 16, 20] демонструють, як сучасні інструменти безпеки реалізують принцип клієнтського шифрування і повну конфіденційність користувача. Це має велике практичне значення для навчальних закладів, де забезпечення безпеки облікових даних студентів і викладачів є невід'ємною складовою інформаційної безпеки.

Таким чином, проведений аналіз показує, що більшість досліджень або зосереджені на окремих технічних аспектах кіберзахисту, або розглядають питання цифрової безпеки на загальнотеоретичному рівні. У представленому дослідженні поєднано аналіз цифрового сліду, поведінкових ризиків та конкретних інструментів захисту (менеджери паролів, багатофакторна автентифікація, zero-knowledge підходи), а також розроблено практичні рекомендації для освітнього середовища в контексті сталого розвитку. Це дозволяє забезпечити більш комплексний і прикладний підхід до підвищення інформаційної безпеки в умовах цифровізації освіти. Незважаючи на значну кількість робіт, спостерігається нестача практичних рекомендацій щодо формування навичок цифрової гігієни та управління власним цифровим слідом серед студентів українських університетів. Саме це зумовлює наукову й практичну цінність нашої роботи.

Мета статті - дослідження впливу цивровізації освіти на інформаційну безпеку особистості та розроблення практичних рекомендацій щодо зменшення ризиків витоку персональних даних в освітньому середовищі.

Для досягненя поставленої мети були проведені:

1. Аналіз наукових джерел щодо поняття цифрового сліду, приватності даних та сучасних технологій їх захисту.

2. Визначення основних загроз інформаційній безпеці користувачів, пов'язаних з формуванням і накопиченням цифрових слідів.

3. Розробка рекомендацій та методичних порад щодо безпечного користування цифровими сервісами, менеджерами паролів і засобами шифрування в освітньому середовищі.

Об'єктом дослідження є процес забезпечення кібербезпеки в освітньому середовищі, зокрема під час використання цифрових платформ, онлайн-сервісів та інформаційних систем учасниками освітнього процесу.

У дослідженні використовувались наступні *методи*:

1. Аналіз і синтез — для вивчення наукових джерел щодо проблеми цифрової безпеки, структури цифрового сліду та технологій його контролю.

2. Порівняльний метод — для зіставлення функціональних можливостей різних менеджерів паролів, засобів шифрування та сервісів з управління конфіденційністю.

3. Системний підхід — для розгляду кібербезпеки в освіті як комплексної взаємодії технічних, організаційних і

поведінкових факторів.

4. Узагальнення результатів — для формулювання висновків і розроблення рекомендацій із підвищення цифрової безпеки в освітньому середовищі.

Виклад основного матеріалу

У сучасному інформаційному суспільстві кожна дія користувача в мережі — від переходу за посиланням до натискання «вподобайки» — залишає певний інформаційний відбиток. Сукупність таких даних формує «цифровий слід» (digital footprint) — персоналізований набір цифрових слідів, які відображають поведінку, інтереси та соціальні зв'язки користувача в онлайн-середовищі. Цей слід створює своєрідну «цифрову тінь» людини, що супроводжує її протягом усього часу використання мережі Інтернет.

Видокремлюють «активний» та «пасивний» цифрові сліди. Активний цифровий слід охоплює дані, які користувач свідомо створює й поширює: дописи в соціальних мережах, коментарі, підписки, участь в онлайн-дискусіях. Пасивний цифровий слід формується автоматично без прямої участі користувача — це IP-адреси, cookies, дані геолокації, час відвідування сайтів тощо. Таким чином, навіть за умови обережної онлайн-поведінки, пасивний цифровий слід здатен формувати більш точну (а подекуди — компрометуючу) інформацію про користувача, ніж публічно оприлюднені дані.

Цифровий слід користувача майже ніколи не залишається приватним. Зібрана інформація має значну цінність для різних суб'єктів цифрової екосистеми. Серед основних груп, що здійснюють збір і аналіз персональних даних, можна виділити:

- роботодавців та освітні заклади, які використовують відкриті джерела для оцінювання кандидатів чи абітурієнтів. Наприклад, понад 90% рекрутерів перевіряють кандидатів у пошукових системах перед прийомом на роботу;
- рекламні компанії та брокери даних, які акумулюють цифрову інформацію, створюючи детальні поведінкові профілі користувачів для цільового маркетингу;
- правоохоронні органи, що застосовують цифрові сліди для розслідування кіберзлочинів та встановлення доказової бази;
- кіберзлочинців, які можуть використовувати персональні дані для фішингових атак, зламу акаунтів або викрадення цифрової ідентичності.

Наслідки неконтрольованого розкриття цифрового сліду варіюються від втрати репутації до фінансових збитків, крадіжки персональних даних і компрометації освітніх чи наукових акаунтів. Це особливо небезпечно у сфері освіти, де цифрова присутність студентів і викладачів тісно пов'язана з науковою діяльністю, результатами навчання та академічною доброчесністю.

Джерелами витоку персональних даних є також соціальні мережі та цифрові гаджети.

Кожна взаємодія користувача — публікація, коментар, позначка «подобається» чи навіть пасивне переглядання контенту — створює великий обсяг метаданих, які використовуються для формування поведінкових профілів. Особливу небезпеку становить публічний характер соціальних мереж, де необережно розміщена інформація може бути використана не лише рекламними компаніями, але й шахраями та зловмисниками.

Для мінімізації ризиків важливо впроваджувати принципи цифрової гігієни у взаємодії з соціальними платформами. Користувачеві слід здійснювати регулярний аудит власних акаунтів: обмежувати доступ до профілю, вмикати максимальні налаштування приватності, переглядати дозволи для додатків, а також видаляти застарілі публікації, що можуть містити чутливі відомості. Ефективним кроком може бути повне видалення облікових записів із попереднім завантаженням копії особистих даних. Такий підхід відповідає загальним принципам безпечного цифрового сліду та сприяє зменшенню ризику соціальної інженерії.

Не менш важливим є контроль за налаштуваннями конфіденційності на цифрових пристроях. Рекомендовано вимикати функції геолокації або обмежувати їх використання лише для

окремих застосунків, переглядати дозволи на доступ до мікрофона, камери та контактів, а також деактивувати параметри персоналізованої реклами. Для користувачів iOS доцільно вимкнути опцію “Allow Apps to Request to Track”, на Android — видалити Advertising ID, а в операційних системах Windows — використовувати локальний обліковий запис замість корпоративного. Ці дії дозволяють мінімізувати кількість даних, що збираються без відома користувача.

Окремої уваги заслуговує питання видалення інформації, зібраної брокерами даних. Протягом багатьох років вони акумулюють великі обсяги персональної інформації з публічних джерел, створюючи ризики повторного розповсюдження або несанкціонованого використання. Користувач може скористатися двома основними підходами: самостійно подавати запити на видалення (через процедури opt-out) або застосовувати спеціалізовані сервіси, такі як Incogni, DeleteMe чи Aura, що автоматизують процес і підвищують ефективність реалізації права на конфіденційність. Згідно з міжнародними нормативними актами, зокрема GDPR (General Data Protection Regulation) та CCPA (California Consumer Privacy Act), право на видалення персональних даних закріплене законодавчо, що надає користувачам реальні механізми захисту цифрової ідентичності.

Таким чином, контроль за активністю в соціальних мережах, налаштуванням гаджетів і управлінням даними є невід’ємними складовими сучасної інформаційної безпеки. Формування відповідальної цифрової поведінки сприяє зниженню ризиків витоку інформації, забезпечує захист приватності та підтримує принципи сталого розвитку інформаційного суспільства.

Результати

З метою мінімізації ризиків витоку інформації та зловживання персональними даними формується концепція «цифрової гігієни» — системи правил і практик, спрямованих на безпечне користування інформаційними технологіями.

Кібергігієна — це не лише сукупність технічних заходів, а насамперед поведінкова культура безпечного користування цифровими ресурсами. В освітньому контексті вона включає такі складові:

- усвідомлення ризиків цифрової присутності (цифровий слід, витоки даних, фішинг);
- відповідальне використання соціальних мереж та хмарних сервісів;
- дотримання етичних принципів цифрової взаємодії (академічна доброчесність, авторське право, повага до приватності інших);
- участь у програмах підвищення цифрової грамотності.

Основні принципи цифрової гігієни включають:

1. Використання складних та унікальних паролів для кожного облікового запису.

Використання одного й того самого пароля для різних акаунтів створює високий ризик компрометації, особливо в умовах, коли кількість освітніх і професійних облікових записів постійно зростає. Повторне застосування одного й того самого пароля - одна з найпоширеніших причин зламу акаунтів.

2. Застосування менеджерів паролів (Bitwarden, NordPass, KeePassXC тощо), які забезпечують генерацію, шифрування та автоматичне збереження паролів.

Менеджери паролів — спеціалізовані програми, що функціонують як зашифровані цифрові сховища. Такі сервіси працюють за принципом zero-knowledge, тобто навіть розробники не мають доступу до збережених даних. Користувач створює єдиний майстер-пароль, який є ключем до всіх облікових записів, і може синхронізувати свої дані між пристроями.

3. Увімкнення двофакторної або багатофакторної автентифікації (2FA/MFA), що додає додатковий рівень захисту при вході до системи.

Двофакторна автентифікація унеможливлює вхід сторонніх осіб навіть у випадку компрометації пароля. Для користувачів однієї екосистеми (наприклад, Google або Apple) прийнятним рішенням можуть бути вбудовані менеджери паролів, проте для роботи з різними платформами доцільніше використовувати незалежні

кросплатформні сервіси.

4. Регулярне оновлення програмного забезпечення — важлива умова усунення вразливостей, які можуть бути використані зловмисниками.

Важливим аспектом цифрової безпеки є також вибір надійного браузера. Так, популярні рішення на кшталт Brave, Mozilla Firefox або Tor Browser мають вбудовані механізми блокування трекерів, захисту приватності та анонімного маршрутизаційного обміну даними. Варто зазначити, що стандартний режим «інкогніто» не гарантує повної анонімності — він лише запобігає збереженню історії переглядів на локальному пристрої.

Для захисту від несанкціонованого збору персональних даних під час роботи в мережі доцільно застосовувати спеціальні браузерні розширення, що блокують трекери та рекламні скрипти, які відстежують онлайн-активність. Зокрема, uBlock Origin і Privacy Badger дозволяють автоматично блокувати потенційно шкідливі елементи сторінок і запобігають передачі даних третім сторонам. Інструмент Global Privacy Control (GPC) дає змогу користувачеві надсилати автоматичний запит «Не продавати мої дані» відповідно до міжнародних норм захисту приватності (наприклад, GDPR та CCPA), що посилює контроль над використанням персональної інформації. Використання таких інструментів є не лише технічним засобом підвищення безпеки, а й важливою складовою формування культури цифрової відповідальності серед користувачів освітнього середовища.

Формування культури цифрової безпеки є важливим елементом освітнього процесу, оскільки саме навчальні заклади виступають першими осередками цифрової соціалізації молоді. Забезпечення кібербезпеки в освіті включає не лише технічні аспекти — захист серверів, мереж і баз даних, — а й розвиток у здобувачів освіти критичного мислення, відповідального ставлення до інформаційних технологій та навичок цифрової гігієни. Такі компетенції стають необхідною умовою для побудови безпечного й етичного інформаційного простору.

Забезпечення безпеки інформаційних ресурсів освітніх установ безпосередньо узгоджується з Цілями сталого розвитку ООН, оскільки цифрова безпека є важливою складовою сталого розвитку суспільства, орієнтованого на знання, інновації та права людини.

Ціль 4 “Якісна освіта” акцентує увагу на необхідності забезпечення інклюзивного, справедливого та безпечного навчального середовища, у якому кожен учасник освітнього процесу має рівний доступ до сучасних технологій, цифрових інструментів і знань. Захист освітніх даних та інформаційних платформ гарантує неперервність навчального процесу, підтримує академічну доброчесність і сприяє розвитку цифрової грамотності. В умовах гібридного та дистанційного навчання саме безпека електронних освітніх середовищ стає основою довіри до нових форматів освіти. Забезпечення кібербезпеки таким чином є важливою умовою реалізації концепції «освіти для всіх» — без бар’єрів, дискримінації та загроз.

Ціль 9 “Індустріалізація, інновації та інфраструктура” спрямована на розвиток стійкої інфраструктури та заохочення інновацій. У контексті освіти це означає створення надійних і захищених цифрових платформ, мережевих систем, баз даних та інструментів для зберігання, обміну й аналізу освітньої інформації. Розбудова таких систем вимагає впровадження сучасних технологій шифрування, автентифікації користувачів, захисту від кібератак і витоків даних. Інноваційні підходи до цифрової безпеки водночас підвищують ефективність управління освітніми процесами, сприяють автоматизації адміністрування та підтримують сталий розвиток освітніх інституцій.

Ціль 16 “Мир, справедливість та сильні інститути” підкреслює важливість формування прозорих, підзвітних і стійких інституцій, що діють на засадах справедливості, поваги до прав людини та верховенства права — зокрема в цифровому просторі. Для освітньої сфери це означає створення політик цифрової етики, захисту персональних даних, забезпечення конфіденційності академічних результатів і розроблення механізмів реагування на кіберінциденти. Надійна цифрова інфраструктура освіти є основою

довіри між усіма учасниками освітнього процесу — студентами, викладачами, адміністрацією та державними структурами. Таким чином, дотримання принципів Цілі 16 сприяє зміцненню інституційної спроможності освітніх організацій, формуванню цифрової культури доброчесності та зменшенню кіберзагроз у суспільстві загалом.

Отже, цифрова безпека в освіті є не лише технічним аспектом, а й невід'ємним чинником сталого розвитку, що поєднує технологічну інноваційність, етичну відповідальність та соціальну справедливість. Вона забезпечує не лише збереження інформаційних ресурсів, а й формування довіри, прозорості та справедливості в глобальному освітньому просторі.

Упровадження принципів кібербезпеки в освітній процес сприяє не лише захисту персональних даних, а й формуванню цифрової етики, довіри та взаємоповаги у віртуальному просторі. Розвиток цифрової безпеки є стратегічним кроком до сталого функціонування освітньої системи, що відповідає глобальним викликам XXI століття та сприяє реалізації концепції безпечного, відкритого й технологічно розвиненого суспільства знань.

Обговорення

У сучасних умовах цифровізації освіти викладач виступає не лише носієм знань, а й модератором та адміністратором цифрового освітнього середовища. Його завдання — забезпечити безпечну, контрольовану та етично комфортну взаємодію учасників навчального процесу в онлайн-форматі. Захист віртуальних занять від небажаних втручань, технічних збоїв або порушень дисципліни є важливою складовою кібергігієни освітнього процесу. Можна виділити такі заходи:

1. Контроль доступу до навчальних зустрічей

Одним із базових принципів безпеки є обмеження відкритого доступу до онлайн-лекцій. Посилання на відеоконференції не повинні публікуватися у відкритих джерелах (соціальних мережах, публічних форумах, сайтах). Оптимальним є розповсюдження запрошень через офіційні освітні платформи (LMS, Moodle, Google Classroom) або корпоративну електронну пошту. Такий підхід дозволяє контролювати аудиторію, зменшує ризик «захоплення» конференцій сторонніми користувачами та сприяє дотриманню академічної доброчесності.

2. Безпечні налаштування платформ для відеоконференцій

- Zoom:

Під час роботи у Zoom викладач повинен увімкнути такі опції:

*Waiting Room (зал очікування) — забезпечує ручне підтвердження учасників перед входом у кімнату;

*Only authenticated users can join — доступ можливий лише для користувачів, що увійшли під зареєстрованими акаунтами;

*Вимкнення функції "Join before host" — забороняє початок конференції без організатора;

*Обмеження демонстрації екрана виключно для викладача;

*Заборона анотацій сторонніх користувачів під час презентацій.

Крім того, функція "Suspend participant activities" дозволяє миттєво зупинити всі дії учасників у разі порушення безпеки.

- Google Meet:

Для Google Meet рекомендовано створювати зустрічі через корпоративний календар або Google Classroom, що забезпечує автентифікацію запрошених осіб. Додатково слід:

*обмежити доступ лише для користувачів корпоративного домену університету;

*уникати використання постійних посилань;

*блокувати кімнату після початку заняття ("lock meeting").

У налаштуваннях викладач також може регулювати можливість демонстрації екрана, використання чату чи реакцій, що сприяє дисциплінованому перебігу заняття.

- Microsoft Teams:

У Teams безпечний формат роботи передбачає створення дзвінків із попереднім списком учасників. Активовані функції Lobby (зал очікування) та "Only people in my organization" забезпечують

контроль доступу лише для студентів і співробітників університету. Якщо заняття передбачає дискусію, викладач може призначити співмодератора, який допомагає підтримувати порядок та слідкувати за дотриманням етичних норм поведінки.

3. Формування культури кіберетики серед студентів

Забезпечення безпеки онлайн-занять неможливе без участі студентів у дотриманні правил цифрової взаємодії. На початку курсу доцільно обговорити такі принципи:

* заборона передавання посилань на заняття стороннім особам;

* обов'язковий вхід під справжнім іменем та корпоративним акаунтом;

* повідомлення викладача про підозрілі дії чи втручання;

* дотримання поваги, академічної доброчесності та етичного спілкування.

Отже, захист освітнього цифрового середовища є не лише технічною задачею, а й компонентом інформаційної культури університету. Розроблення чітких правил доступу, конфіденційності та реагування на кіберінциденти формує у студентів відповідальне ставлення до власної цифрової поведінки.

На основі аналізу сучасних джерел та практик кіберзахисту сформульовані практичні рекомендації щодо підвищення безпеки цифрової діяльності в освітньому середовищі:

1. Використовувати унікальні паролі та регулярно оновлювати їх для всіх акаунтів.

2. Увімкнути двофакторну автентифікацію для облікових записів навчальних платформ і електронної пошти.

3. Не відкривати невідомі посилання та не завантажувати файли з ненадійних джерел.

4. Використовувати VPN при роботі в публічних мережах.

5. Обмежити доступ до персональних даних у профілях соціальних мереж.

6. Періодично очищати цифровий слід — видаляти застарілі або непотрібні облікові записи.

7. Підвищувати власну цифрову компетентність через онлайн-курси з кібербезпеки (наприклад, Coursera, edX, Cybrary).

Реалізація цих рекомендацій сприятиме формуванню безпечного цифрового освітнього середовища, у якому зберігається баланс між відкритістю знань і захистом особистої інформації.

Кібербезпека в освітньому процесі — це не лише технічне завдання, а й частина цифрової культури сучасного викладача й студента. Безпечне зберігання паролів, усвідомлення власного цифрового сліду, використання інструментів приватності та регулярна цифрова гігієна формують основу інформаційної безпеки особистості.

Висновки

У результаті проведеного дослідження встановлено, що процес цифровізації освіти суттєво підвищив ефективність навчання, проте водночас створив нові ризики для безпеки персональних даних та інформаційної цілісності освітнього середовища. Кібербезпека сьогодні є невід'ємним компонентом сталого розвитку системи освіти, оскільки гарантує захист інформаційних ресурсів, академічної доброчесності та приватності всіх учасників навчального процесу.

Проведений аналіз показав, що основними загрозами для користувачів освітнього простору є компрометація облікових записів, фішингові атаки, витоки даних і формування неконтрольованого цифрового сліду. Це потребує від студентів і викладачів свідомого підходу до цифрової гігієни, який включає використання унікальних паролів, менеджерів паролів, двофакторної автентифікації та безпечних браузерів.

Особливе значення в забезпеченні кібербезпеки мають спеціалізовані інструменти для управління паролями (Bitwarden, KeePassXC, NordPass тощо), що функціонують за принципом нульового розголошення та забезпечують надійний захист конфіденційної інформації. Вони сприяють підвищенню цифрової грамотності та мінімізують людський фактор у питаннях безпеки.

Визначено, що формування культури цифрової безпеки в освіті є

стратегічним завданням, узгодженим із Цілями сталого розвитку ООН, зокрема Ціль 4 «Якісна освіта», Ціль 9 «Індустріалізація, інновації та інфраструктура», Ціль 16 “Мир, справедливість та сильні інститути”.

Таким чином, упровадження системних підходів до захисту персональних даних, підвищення цифрової грамотності та розвиток культури інформаційної безпеки серед учасників освітнього процесу є ключовими умовами стійкого функціонування сучасного освітнього середовища.

Конфлікт інтересів

Автори заявляють, що конфлікту інтересів щодо публікації цього рукопису немає. Крім того, автори повністю дотримувались етичних норм, включаючи плагіат, фальсифікацію даних та подвійну публікацію.

Внесок авторів: усі автори зробили рівний внесок у цю роботу.

У роботі не використано ресурс штучного інтелекту.

Список використаної літератури

1. Главацька, А., Ангельська, О., Опірський, І. Дослідження технології використання OSINT як нової загрози з деанонімізації особи в інтернет просторі. *Кібербезпека: освіта, наука, техніка*. 2024. Том 1, №25. С. 19-50. https://doi.org/10.28925/2663-4023.2024.25.1950
2. Запорожченко, М., Шевченко, Г. Цифрова безпека як складник професійної компетентності педагогічних працівників. *Вересень.* 2025. Том 105, №2. https://doi.org/10.54662/veresen.2.2025.03
3. Ігнатенко, В. О., Мирошніченко, Ю. Б. Інформаційна безпека в сучасному цифровому освітньому середовищі. *Наукові записки НПУ*. 2025. №160. С. 44-53. https://doi.org/10.31392/NZ-udu-160.2025.06
4. Рудницький, В., Лада, Н., Підласий, Д., Мельник, О. Синтез дискретно-алгебраїчних моделей елементарних функцій операцій керованих інформацією. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2024. Вип. 3(23). С. 6–16. https://doi.org/10.28925/2663-4023.2024.23.616
5. Смірнова, Т., Конопліцька-Слободенюк , О., Буравченко, К., Смірнов, С., Кравчук , О., Козірова, Н., Смірнов, О. Дослідження технологій забезпечення кібербезпеки хмарних сервісів IAAS, PAAS та SAAS. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2024. Вип. 4(24). С. 6–27. https://doi.org/10.28925/2663-4023.2024.24.627
6. Толкачова, А., Посувайло, М.-М. Тестування на проникнення з використанням глибокого навчання з підкріпленням. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2024. Вип. 3(23). С. 17–30. https://doi.org/10.28925/2663-4023.2024.23.1730
7. Чорномидз, А. В. Інформаційна безпека викладачів вищих навчальних закладів в умовах воєнного стану: виклики та практичні рекомендації. *Медична освіта*. 2025. №2. С. 67–71. https://doi.org/10.11603/m.2414-5998.2025.2.15490
8. Bitwarden Security Whitepaper. (n.d.). Bitwarden. URL: https://bitwarden.com/help/bitwarden-security-white-paper/
9. Buitrago-Ropero, M. E., Ramírez-Montoya, M. S., Chiappe Laverde, A. Digital footprints (2005–2019): a systematic mapping of studies in education. *Interactive Learning Environments*. 2023. Vol. 31(2). Pp. 876-889. https://doi.org/10.1080/10494820.2020.1814821
10. Contributing to the UN Sustainable Development Goals with ISO standards. 2018. URL: https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100429.pdf
11. Di Cara, N., Zelenka, N., Davis, O., Haworth, C. Using Data Hazards to support safe and ethical digital footprint research. *Int J Popul Data Sci*. 2023. Vol. 8(3), 2279. https://doi.org/10.23889/ijpds.v8i3.2279
12. Encryption Protocols – Bitwarden. (n.d.). Bitwarden. URL: https://bitwarden.com/help/what-encryption-is-used/
13. McDonald, R., Skatova, A., Maple, C. Attitudes towards Sharing Digital Footprint Data: a Discrete Choice Experiment. *Int J Popul Data Sci*. 2023. Vol. 8(3),2287. https://doi.org/10.23889/ijpds.v8i3.2287
14. Micheli, M., Lutz, C., Büchi, M. Digital footprints: An emerging dimension of digital inequality.

Journal of Information, Communication & Ethics in Society. 2018. Vol. 16(3). Pp. 242–251. https://doi.org/10.1108/JICES-02-2018-0014
15. Quach, S, Thaichon, P, Martin, K. D., Weaven, S, Palmatier, R. W. Digital technologies: tensions in privacy and data. *J Acad Mark Sci*. 2022. Vol. 50(6). Pp. 1299-1323. https://doi.org/10.1007/s11747-022-00845-y
16. Rakow, K .E., Upsher, R. J., Foster, J. L. H., Byrom, N. C., Dommett, E. J. Student perspectives on their digital footprint in virtual learning environments. *Front. Educ*. 2023. Vol. 8, 1208671. https://doi.org/10.3389/feduc.2023.1208671
17. Sharma, I., Aggarwal, A. Digital Footprints and the Battle for Data Sovereignty: Digital Privacy, Security, and Ownership. In *Driving Decentralization and Disruption With Digital Technologies*. 2024. Pp. 74–83. https://doi.org/10.4018/979-8-3693-3253-5.ch005
18. The Sustainable Development Goals as a Framework for COVID-19 Recovery in Cities and Regions. OECD, 2022. URL: https://www.un.org/sustainabledevelopment/sdgs-framework-for-covid-19-recovery/
19. Vervier, L., Zeissig, E.-M., Lidynia, C., & Ziefle, M. Perceptions of Digital Footprints and the Value of Privacy. *2nd International Conference on Internet of Things, Big Data and Security*. 2017. https://doi.org/10.5220/0006301000800091
20. Zero-knowledge encryption: What you need to know (Bitwarden). (n.d.). Bitwarden Resources. URL: https://bitwarden.com/resources/zero-knowledge-encryption/

Стаття надійшла до редакції 22.03.2026
Стаття рекомендована до друку 30.04.2026
Опубліковано 31.05.2026

G. I. KANYUK[1], DSc (Technical Sciences),
Head of the Department of Automation, Metrology and Energy-Efficient Technologies
e-mail: genadiykanuk@gmail.com , ORCID: https://orcid.org/0009-0008-0907-9719
T. M. FURSOVA[1], PhD (Technical Sciences),
Associate Professor of the Department of Automation, Metrology, and Energy-Efficient Technologies
e-mail: tatiana2507@ukr.net , ORCID: https://orcid.org/0000-0002-1423-0822
V. V. SABADASH[2], PhD (Technical Sciences),
Head of Sector
e-mail: kafedra_tsl@ukr.net, ORCID: https://orcid.org/0000-0001-9815-9009
I**. V. SABADASH**[3], PhD (Law),
Chief State Inspector-Expert
e-mail: saba-inna@ukr.net , ORCID: https://orcid.org/0000-0003-1967-9271
[1]*V.N. Karazin Kharkiv National University*,
4 Svobody Square, Kharkiv, 61022, Ukraine
[2]*Hon. Prof. M.S. Bokarius Kharkiv Research Institute of Forensic Examinations*,
8-a Zolochivska St., Kharkiv, 61177, Ukraine
[3]*Kharkiv Department of Expertise and Research of the Specialized Laboratory for Expertise and Research of the State Customs Service*,
6 Bakulina St., Kharkiv, 61166, Ukraine

STUDY OF INFORMATION SECURITY TECHNOLOGIES IN THE EDUCATIONAL PROCESS

The purpose of this article is to examine the impact of the digitization of the educational process on individual information security and to develop practical recommendations for minimizing the risks of personal data leaks in the digital educational environment.

The methods used to achieve the goal: analysis and synthesis of scientific sources on digital security issues, a comparative method for assessing the functional capabilities of modern protection tools (password managers, encryption tools, two-factor authentication mechanisms), as well as a systematic approach to considering cybersecurity as a complex interaction of technical, organizational and behavioral factors. The results were generalized to formulate practical recommendations.

Results. It was established that the digitalization of education significantly expands information

capabilities, but at the same time increases the level of cyber risks, in particular those associated with the formation of a digital trace, compromise of accounts, phishing attacks and unauthorized collection of personal data. The need to implement the principles of digital hygiene is substantiated: the use of unique passwords, password managers with the zero-knowledge principle, multi-factor authentication, regular software updates, privacy settings for social networks and digital devices. Recommendations have been developed for the safe organization of online learning, access control to video conferences, and the formation of a culture of cyberethics.

Conclusions: it is proven that cybersecurity in the educational process is not only a technical task, but also an important component of digital culture and sustainable development of society. The formation of responsible digital behavior, increasing the level of digital literacy, and the implementation of comprehensive information protection measures are key conditions for ensuring the safe, ethical, and sustainable functioning of a modern educational environment.

KEY WORDS: *information security, technologies, education, cyber hygiene.*

Conflict of interest

The authors declare that there is no conflict of interest regarding the publication of this manuscript. Furthermore, the authors has fully adhered to ethical standards, including those related to plagiarism, data falsification, and duplicate publication.

Authors Contribution: all authors have contributed equally to this work.

The work does not use artificial intelligence resources.

References

1. Hlavatska, A., Anhelska, O., Opirskyy, I. (2024). Investigation of the use of OSINT technology as a new threat of de-anonymized persons on the internet space. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, 1(25), 19–50. https://doi.org/10.28925/2663-4023.2024.25.1950 (in Ukrainian).
2. Zaporozhchenko, M., Shevchenko, Г. (2025). Digital security as a component of professional competence for teaching stuff. *Veresen,* 105(2). https://doi.org/10.54662/veresen.2.2025.03 (in Ukrainian).
3. Ihnatenko, V. O., Myroshnichenko, YU. B. (2025). Information security in the modern digital educational environment. *Scientific notes NPU*, (160), 44-53. https://doi.org/10.31392/NZ-udu-160.2025.06 (in Ukrainian).
4. Rudnytskyi, V., Lada, N., Pidlasyi, D., Melnyk, O. (2024). Synthesis of discrete and algebraic models of elementary functions of data-controlled operations. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, 3(23), 6–16. https://doi.org/10.28925/2663-4023.2024.23.616 (in Ukrainian).
5. Smirnova, T., Konoplitska-Slobodeniuk, O., Buravchenko, K., Smirnov, S., Kravchuk, O., Kozirova, N., Smirnov, O. (2024). Research of cyber security technologies of cloud services IAAS, PAAS and SAAS. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, 4(24), 6–27. https://doi.org/10.28925/2663-4023.2024.24.627 (in Ukrainian).
6. Tolkachova, A., Posuvailo, M.-M. (2024). Penetration testing using deep reinforcement learning. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, 3(23), 17–30. https://doi.org/10.28925/2663-4023.2024.23.1730 (in Ukrainian).
7. Chornomydz, A. V. (2025). Faculty information security in higher education institutions amidst martial law: challenges and practical guidelines. *Medical Education*, (2), 67–71. https://doi.org/10.11603/m.2414-5998.2025.2.15490 (in Ukrainian).
8. Bitwarden Security Whitepaper. (n.d.). Bitwarden. https://bitwarden.com/help/bitwarden-security-white-paper/
9. Buitrago-Ropero, M. E., Ramírez-Montoya, M. S., Chiappe Laverde, A. (2023). Digital footprints (2005–2019): a systematic mapping of studies in education. *Interactive Learning Environments*, 31(2), 876-889. https://doi.org/10.1080/10494820.2020.1814821
10. Contributing to the UN Sustainable Development Goals with ISO standards. (2018). https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100429.pdf
11. Di Cara, N., Zelenka, N., Davis, O., Haworth, C. (2023). Using Data Hazards to support safe and ethical digital footprint research. *Int J Popul Data Sci*, 8(3), 2279.

https://doi.org/10.23889/ijpds.v8i3.2279
12. Encryption Protocols – Bitwarden. (n.d.). Bitwarden. https://bitwarden.com/help/what-encryption-is-used/
13. McDonald, R., Skatova, A., Maple, C. (2023). Attitudes towards Sharing Digital Footprint Data: a Discrete Choice Experiment. *Int J Popul Data Sci*, 8(3), 2287. https://doi.org/10.23889/ijpds.v8i3.2287
14. Micheli, M., Lutz, C., Büchi, M. (2018). Digital footprints: An emerging dimension of digital inequality. *Journal of Information, Communication & Ethics in Society*, 16(3), 242–251. https://doi.org/10.1108/JICES-02-2018-0014
15. Quach, S, Thaichon, P, Martin, K. D., Weaven, S, Palmatier, R. W. (2022). Digital technologies: tensions in privacy and data. *J Acad Mark Sci*, 50(6), 1299-1323. https://doi.org/10.1007/s11747-022-00845-y
16. Rakow, K .E., Upsher, R. J., Foster, J. L. H., Byrom, N. C., Dommett, E. J. (2023). Student perspectives on their digital footprint in virtual learning environments. *Front. Educ*, 8, 1208671. https://doi.org/10.3389/feduc.2023.1208671
17. Sharma, I., Aggarwal, A. (2024). Digital Footprints and the Battle for Data Sovereignty: Digital Privacy, Security, and Ownership. In *Driving Decentralization and Disruption With Digital Technologies* (pp. 74–83). https://doi.org/10.4018/979-8-3693-3253-5.ch005
18. The Sustainable Development Goals as a Framework for COVID-19 Recovery in Cities and Regions. (2022). OECD. https://www.un.org/sustainabledevelopment/sdgs-framework-for-covid-19-recovery/
19. Vervier, L., Zeissig, E.-M., Lidynia, C., Ziefle, M. (2017). Perceptions of Digital Footprints and the Value of Privacy. *2nd International Conference on Internet of Things, Big Data and Security*. https://doi.org/10.5220/0006301000800091
20. Zero-knowledge encryption: What you need to know (Bitwarden). (n.d.). Bitwarden Resources. https://bitwarden.com/resources/zero-knowledge-encryption/

The article was received by the editors 22.03.2026
The article is recommended for printing 30.04.2026
Published 31.05.2026