

Комунальний заклад «Кіровоградський обласний інститут післядипломної педагогічної освіти імені Василя Сухомлинського»
Комунальний заклад «Житомирський обласний інститут післядипломної педагогічної освіти» Житомирської обласної ради
Комунальний заклад «Запорізький обласний інститут післядипломної педагогічної освіти» Запорізької обласної ради
Комунальний заклад вищої освіти «Вінницька академія безперервної освіти»
Тернопільський національний педагогічний університет імені Володимира Гнатюка
Центральноукраїнський національний технічний університет
Донецький державний університет внутрішніх справ
Центральноукраїнський інститут розвитку людини Університету «Україна»
Кіровоградський науково-дослідний експертно-криміналістичний центр МВС України
Комітет Національної асоціації адвокатів України з питань сімейного права

IV Всеукраїнська науково-практична конференція «БЕЗПЕКА ДІТЕЙ В ІНТЕРНЕТІ: ПОПЕРЕДЖЕННЯ, ОСВІТА, ВЗАЄМОДІЯ»

10-14 лютого 2025 року



[Сайт конференції](#)



[Сторінка матеріалів
учасників конференції](#)



[Відеозапис пленарного
засідання конференції](#)

Кропивницький

2025

УДК 004.738.5-049.5:37.015.3-053.5/6(063)

Б 39

Безпека дітей в Інтернеті: попередження, освіта, взаємодія: збірник матеріалів IV Всеукраїнської науково-практичної конференції, м. Кропивницький, 10-14 лютого 2025 року / уклад. С.М. Єфіменко; за заг. ред. Г.В.Скрипки. Кропивницький: КЗ «КОІППО імені Василя Сухомлинського», 2025. 451 с.

*Друкується за рішенням вченої ради
комунального закладу «Кіровоградський обласний інститут післядипломної педагогічної освіти імені Василя Сухомлинського»
(від 11 березня 2025 року, протокол №2)*

Рецензенти:

Буртовий С.В. – кандидат педагогічних наук, заступник директора з науково-дослідної діяльності та міжнародного співробітництва комунального закладу «Кіровоградський обласний інститут післядипломної педагогічної освіти імені Василя Сухомлинського»;

Волобоєв А.О. – доктор філософії, завідувач кафедри оперативно-розшукової діяльності та інформаційної безпеки Донецького державного університету внутрішніх справ.

Відповідальний за випуск – Віталій ДМИТРУК

Збірник матеріалів конференції містить основні результати науково-практичних пошуків освітян, правоохоронців, представників громадських організацій та державних органів різних областей України щодо осмислення, виявлення та поширення ефективних практик, які сприяють забезпеченню безпеки дітей в Інтернеті, а також розвитку кіберграмотності педагогічної спільноти.

Матеріали опубліковані в авторській редакції.

© КЗ «КОІППО імені Василя Сухомлинського»

© Автори матеріалів

IV Всеукраїнська науково-практична конференція «Безпека дітей в Інтернеті: попередження, освіта, взаємодія»
стійкої та безпечної поведінки в медіасередовищі, що є надзвичайно важливим у сучасних умовах війни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кузьма І. І. Формування медіаграмотності дітей старшого дошкільного віку: теорія і технологія: монографія / за наук. ред. проф. В. М. Чайки. Тернопіль: Осадца Ю.В., 2019. 188 с.
2. Листопад О. А., Мардарова І. К. Теоретико-методичні засади формування готовності майбутніх вихователів до використання інформаційно-комунікаційних технологій в організації пізнавальної діяльності дошкільників: моногр. Одеса: Видавець Букаєв В. В., 2021. 206 с.
3. *Наскрізна медіаосвіта в умовах війни: зб. навч. медіаосвітніх програм* / Найдьонова Л. А. та ін.; за ред. Л. А. Найдьонової ; уклад. Н. Ф. Умеренкова ; Інститут соціальної та політичної психології НАПН України. Київ, 2023. 264 с.

КІБЕРГІГІЄНА І КІБЕРБЕЗПЕКА ОСВІТНЬО-ЦИФРОВОГО СЕРЕДОВИЩА

Ірина МАРДАРОВА, Наталя ЛИСТОПАД

Сьогодні в Україні коли цифрові технології стали невід'ємною частиною навчання та повсякденного життя проблема кібергігієни та кібербезпеки набуває все більшої ваги в умовах військової агресії та організації дистанційного навчання здобувачів освіти. Поняття «кібербезпека» розглядається як захищеність життєво важливих інтересів учасників освітнього процесу під час використання кіберпростору, за наявності якої забезпечується сталий розвиток інформаційного суспільства та освітньо-цифрового середовища. Створення безпечного освітньо-цифрового середовища в закладах фахової передвищої та вищої освіти вимагає комплексного підходу, що містить технічні, методичні та організаційні аспекти.

Технічна інфраструктура закладів фахової передвищої, вищої освіти є основою для створення сучасного освітньо-цифрового середовища, яке

забезпечує ефективне навчання, управління та комунікацію між усіма учасниками освітнього процесу. Вона передбачає обладнання, програмне забезпечення, мережі та інші технічні ресурси, необхідні для функціонування закладу освіти. Без надійної технічної бази неможливо забезпечити ефективне цифрове навчання та кібербезпеку учасників освітнього процесу. Окреслимо основні компоненти.

1. Апаратне забезпечення: пристрої, що використовуються для навчання, управління та підтримки освітнього процесу. Комп'ютерне обладнання для студентів, викладачів та адміністративного персоналу, сервери для зберігання даних, хостингу навчальних платформ та управління мережею, спеціалізоване обладнання, що використовують для лабораторій, майстерень та інших практичних занять (наприклад, 3D-принтери, роботизовані комплекси) тощо.

2. Мережева інфраструктура забезпечує зв'язок між пристроями та доступ до швидкого і стабільного інтернету з достатньою пропускнуою здатністю, що є критично важливим для сучасного навчання. Локальна мережа (LAN) для об'єднання комп'ютерів та пристроїв у межах закладу освіти; Wi-Fi бездротовий доступ до інтернету для студентів, викладачів та адміністрації закладу освіти.

3. Програмне забезпечення є ключовими для організації освітньо-цифрового середовища, управління даними та комунікації. Наприклад, системи управління навчанням (LMS) Moodle, Google Classroom, Canvas, Blackboard, використовуються для розміщення навчальних матеріалів, проведення тестів та моніторингу успішності студентів; інструменти для організації дистанційної освіти та проведення онлайн-занять Zoom, Microsoft Teams, Google Meet; електронні журнали та бази даних для ведення обліку успішності, відвідуваності та управління освітнім процесом; хмарні сервіси: Google Workspace, Microsoft 365 для зберігання даних, спільної роботи та комунікації.

Організаційні аспекти кібербезпеки в закладах фахової передвищої, вищої освіти передбачають: формування інфраструктури кібербезпеки в закладі освіти (впровадження автоматизованих систем моніторингу та реагування на кіберзагрози, використання антивірусного програмного забезпечення,

IV Всеукраїнська науково-практична конференція «Безпека дітей в Інтернеті: попередження, освіта, взаємодія»

міжмережевих екранів (firewall), захист серверів та баз даних закладу освіти від атак DDoS та несанкціонованого доступу) тощо; управління доступом і автентифікація (використання одноразових паролів (OTP), двофакторної автентифікації (2FA) для входу в освітні платформи, надання студентам і викладачам індивідуальних акаунтів із різними рівнями доступу) тощо; кібербезпека під час онлайн-навчання (контроль ідентифікації студентів під час дистанційного навчання (антисписування, захист відеоконференцій), запровадження безпечних методів проведення онлайн-іспитів та тестувань, упровадження технологій AI-аналізу поведінки користувачів для виявлення підозрілої активності); захист персональних даних (шифрування важливих файлів і листування, впровадження політики «мінімізації збору даних» (обмеження збору та обробки непотрібної інформації), контроль за передачею та зберіганням персональних даних студентів, викладачів тощо).

Системи зберігання та захисту даних є критично важливими для забезпечення конфіденційності та цілісності інформації. Системи зберігання даних у різні сховища, де заклади фахової передвищої, вищої освіти тримають інформацію про студентів, викладачів, навчальні матеріали тощо. Захист даних містить методи запобігання несанкціонованому доступу, втраті чи витоку інформації. Основні елементи: хмарні сховища (Google Drive, Dropbox, OneDrive); локальні сервери для зберігання великих обсягів даних; системи резервного копіювання для запобігання втраті даних у разі збоїв; захист даних використання шифрування, антивірусів, фаєрволів та інших засобів кібербезпеки.

В Україні діє закон «Про захист персональних даних», що вимагає від закладів освіти забезпечувати захист персональних даних студентів і співробітників. Персональні дані відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Не допускається обробка даних про фізичну особу, які є конфіденційною інформацією, без її згоди, крім випадків, визначених зазначеним законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [1].

У законі «Про основні засади забезпечення кібербезпеки України» зазначається, що національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури. Визначені вимоги до суб'єктів забезпечення кібербезпеки у межах своєї компетенції, зокрема: розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту; забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління; здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору [2].

Методичними аспектами організації кібербезпеки в освітньо-цифровому середовищі наразі є: розробка нормативно-правової бази закладу фахової передвищої, вищої освіти, впровадження внутрішніх політик і регламентів щодо кібербезпеки закладу освіти, відповідність національним і міжнародним стандартам кібербезпеки (ISO/IEC 27001, NIST, GDPR), регламентація правил доступу до цифрових ресурсів і обробки персональних даних; інтеграція кібербезпеки в освітньо-професійні програми, включення дисциплін із основ кібергігієни у навчальні плани всіх спеціальностей, організація тренінгів та майстер-класів для викладачів та адміністративного персоналу; методична підтримка та ресурси, створення навчально-методичних матеріалів: посібників, відеолекцій, вебінарів, презентацій, розробка гейміфікованих навчальних платформ для перевірки знань студентів і викладачів, проведення регулярних семінарів та конференцій із кібербезпеки.

Не менш важливим аспектом виступає кібергігієна учасників освітнього процесу. Дане поняття розглядають як комплекс правил, заходів та навичок,

IV Всеукраїнська науково-практична конференція «Безпека дітей в Інтернеті: попередження, освіта, взаємодія»
спрямованих на забезпечення інформаційної безпеки від загроз у кіберпросторі. Кібергігієна є показником цифрової культури учасників освітнього процесу.

Основні принципи кібергігієни для викладачів та студентів закладів фахової передвищої, вищої освіти: дотримання безпеки акаунтів та паролів, використання складних паролів і їх регулярна зміна, двофакторної автентифікації (2FA), уникнення використання одного пароля для різних освітніх платформ тощо; захист пристроїв і програмного забезпечення, що передбачає регулярне оновлення операційної системи та програм, використання ліцензійного антивірусного програмного забезпечення, уникнення встановлення «піратських програм» з ненадійних джерел, уникнення поширення конфіденційної інформації; робота з навчальними платформами, захист доступу до LMS-систем (наприклад, Moodle, Google Classroom), контроль прав доступу, збереження резервних копій навчальних матеріалів, використання лише офіційних, перевірених сайтів для завантаження ресурсів, обережність при підключенні до публічних Wi-Fi мереж (через VPN), безпечне користування освітніми платформами, використання офіційних акаунтів закладу освіти для входу в навчальні системи (Офіс 365, Google Classroom тощо), дотримання безпеки паролів, регулярне створення резервних копій освітніх матеріалів; запобігання кібербулінгу та інформаційним загрозам передбачає моніторинг онлайн-активності студентів щодо проявів кібербулінгу, ознайомлення студентів із правилами безпечного користування цифровими технологіями, використання цифрового етикету під час онлайн-лекцій та спілкування в мережі тощо.

Отже, формування цифрової культури та навчання учасників освітнього процесу навичкам кібербезпеки та кібергігієни допомагає захистити персональні дані, запобігти кібератакам та створити безпечне освітньо-цифрове середовище закладу фахової передвищої, вищої освіти. Основними напрямками організації забезпечення кібербезпеки та кібергігієни учасників освітнього процесу є:

- проведення тренінгів і семінарів в рамках освітнього процесу, регулярні лекції та вебінари з основ кібербезпеки; інтеграція кібербезпеки в робочі програми (наприклад, з дисципліни «Інформатика», «Діджиталізація

IV Всеукраїнська науково-практична конференція «Безпека дітей в Інтернеті: попередження, освіта, взаємодія» освітнього процесу» тощо), запрошення фахівців із кібербезпеки (експертів, представників ІТ-компаній тощо), проведення практичних занять із кібергігієни (наприклад, захист акаунтів, налаштування безпеки пристроїв симуляції кібератак, фішингові листи, атаки на паролі, практичні кейси щодо кібербулінгу та захисту персональних даних, навчання безпечного використання Wi-Fi у громадських місцях);

- впровадження курсів підвищення кваліфікації із проблем кібергігієни та кібербезпеки, розробка онлайн-курсів на платформах Moodle, Coursera або Google Classroom, створення коротких відеоуроків і гейміфікованих тестів для перевірки знань, перегляд освітніх серіалів, гайдів, цифрограм платформи Дія. Освіта «Кібергігієна для молоді», «Базові знання з кібергігієни», «Аналітик із кібербезпеки», «Навіщо Вам кібергігієна?», «Кіберграм» [3] тощо;
- інформаційна кампанія в закладах фахової передвищої, вищої освіти (наприклад, розміщення інформаційних стендів із правилами кібергігієни, регулярна розсилка інформаційних бюлетенів із порадами щодо безпеки, проведення тематичних днів кібербезпеки з конкурсами, квестами та вікторинами) тощо;
- співпраця з фахівцями та організаціями, що передбачає запрошення представників кіберполіції, ІТ-компаній, громадських організацій, участь у міжнародних програмах кібербезпеки та грантах (наприклад, European Cyber Security Month тощо).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 01.02.2025).
2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 01.02.2025).
3. Кібербезпека. Дія. Освіта: онлайнплатформа. URL: <https://osvita.diia.gov.ua/catalog/topic/cyber-security> (дата звернення: 01.02.2025).

**Матеріали IV Всеукраїнської
науково-практичної конференції
«БЕЗПЕКА ДІТЕЙ В ІНТЕРНЕТІ: ПОПЕРЕДЖЕННЯ,
ОСВІТА, ВЗАЄМОДІЯ»
(м. Кропивницький, 10-14 лютого 2025 року)**

Відповідальний редактор: Скрипка Г.В.
Укладач: Єфіменко С. М.

Підписано до друку 05.05.2025 р.
Формат 60x84 1/16. Папір офсетний. Гарнітура «Times New Roman».
Друк – принтер. Тираж 100 прим.
Зам. № 463

КЗ «КОІППО імені Василя Сухомлинського», вул. Велика
Перспективна, 39/63, м. Кропивницький, 25006.
Віддруковано в лабораторії інформаційно-методичного
забезпечення освітнього процесу КЗ
«КОІППО імені Василя Сухомлинського», вул. Велика Перспективна
39/63, Кропивницький, 25006