https://unity.gov.ua/en/2024/03/11/mine-safety-for-children-useful-videos/ (дата звернення: 05.02.2026)

6. Курс з протимінної безпеки «СтопМіна» [Електронний ресурс]. – Режим доступу:
https://surl.li/oviler (дата звернення: 05.02.2026)

7. Онлайн-курс «Як навчати дітей мінної безпеки» [Електронний ресурс]. – Режим доступу:
https://surl.li/gmuxad (дата звернення: 05.02.2026)

8. Абетка безпеки ДСНС України [Електронний ресурс]. – Режим доступу:
https://surl.lt/rznuwx (дата звернення: 05.02.2026)

9. Новий бот «Дитячий лікар на війні» [Електронний ресурс]. – Режим доступу:
https://surli.cc/qipcrk (дата звернення: 05.02.2026)

10. Соціально-педагогічна та психологічна допомога сім'ям з дітьми в умовах війни [Електронний ресурс] / Андрєєнкова В.Л. та ін. – Режим доступу:
http://iitta.gov.ua (дата звернення: 05.02.2026)

11. Матеріали Naurok.com.ua з вправами для дітей у стресових ситуаціях [Електронний ресурс]. – Режим доступу:
https://naurok.com.ua (дата звернення: 05.02.2026)

12. Ігри та вправи для психоемоційної підтримки дітей від UNICEF (Світлана Ройз) [Електронний ресурс]. – Режим доступу:
https://surl.li/ksryqw (дата звернення: 05.02.2026)

13. Resilience for the Resilient (Smart Osvita) [Електронний ресурс]. – Режим доступу: https://smartosvita.org (дата звернення: 05.02.2026)

14. Relax Kids Ukraine — вправи та медитації для дітей [Електронний ресурс]. – Режим доступу: https://relaxkids.com.ua (дата звернення: 05.02.2026)

15. Відео-інструкції «Що робити, коли лунає сигнал» (YouTube) [Електронний ресурс]. – Режим доступу:
https://www.youtube.com (дата звернення: 05.02.2026)

16. Telegram-канал з аудіоказками для дітей «Павлуша і Ява» [Електронний ресурс]. – Режим доступу:
https://t.me/pavlusha_yava (дата звернення: 05.02.2026)

17. Мультфільм ЮНІСЕФ Україна про мінну безпеку: безпечні канікули (дата звернення: 05.02.2026)

18. Мультфільм ЮНІСЕФ Україна про мінну безпеку: лісовий скарб (дата звернення: 05.02.2026)

19. Мультфільм ЮНІСЕФ Україна про мінну безпеку: повітряний змій (дата звернення: 05.02.2026)

Важливо усвідомлювати тісний зв'язок фізичної безпеки з психоемоційним станом дитини. Постійні повітряні тривоги, інформаційне напруження та переживання за близьких знижують концентрацію уваги, викликають страх і тривожність, що може призводити до травматичних ситуацій. Тому педагогічна практика повинна включати елементи психологічної підтримки, вправи на саморегуляцію, ігрові паузи та арттерапевтичні методики. Створення атмосфери довіри й стабільності сприяє підвищенню адаптивності дітей до складних умов.

Ефективна безпека неможлива без активної взаємодії з батьками. Інформування родин про алгоритми дій під час тривог, правила перебування дітей у закладі освіти та потенційні ризики формує єдину систему захисту дитини як у школі, так і поза її межами. Спільні заходи, консультації та пам'ятки сприяють підвищенню рівня безпекової культури в громаді.

Отже фізична безпека учасників освітнього процесу в умовах війни є комплексною педагогічною та управлінською проблемою, що потребує поєднання нормативного регулювання, практичної організації захисту, системної освітньої роботи та психологічної підтримки. Лише цілісний підхід дозволяє мінімізувати ризики й забезпечити відносну стабільність освітнього середовища навіть у надзвичайно складних умовах воєнного стану.

Андрій КУЧЕРУК,
методист НМЦ професійного розвитку педагогічних працівників з охорони праці, безпеки життєдіяльності та цивільного захисту ХОІППО ім.А.Назаренка

Кібербезпека в закладах освіти: стратегічний вимір та практичні рішення

Анотація: У статті аналізується трансформація підходів до кіберзахисту в освітньому секторі України. Розглядаються впровадження нових державних стандартів, виклики, пов'язані з використанням штучного інтелекту, та методи підвищення цифрової стійкості учасників освітнього процесу.

Цифровізація освіти в Україні, прискорена спочатку пандемією, а згодом – повномасштабною війною, створила безпрецедентні можливості для дистанційного навчання. Водночас це призвело до появи нових критичних вразливостей. Сьогодні заклади освіти розглядаються не лише як осередки навчання, а й як власники великих масивів персональних даних та інтелектуальної власності, що робить їх привабливою мішенню для кіберзлочинців [1].

Згідно зі Стратегією кібербезпеки України, захист інформаційної інфраструктури освітніх установ є пріоритетом національної безпеки, оскільки успішна атака на систему (наприклад, злам ЄДЕБО чи локальних хмарних сховищ) може паралізувати навчальний процес у масштабах країни [4].

У 2025-2026 роках кібератаки стають дедалі автоматизованішими. Фахівці виділяють три ключові напрямки, за якими вони здійснюються:

– Соціальна інженерія 2.0: Використання генеративного ШІ дозволяє створювати фішингові листи, які неможливо відрізнити від офіційних повідомлень адміністрації чи Міністерства освіти. Це змушує користувачів переходити за шкідливими посиланнями або розголошувати паролі [7];

– Вразливості хмарних сервісів: перехід на Google Workspace та Microsoft 365 вимагає жорсткої політики доступу. Несанкціонований доступ до одного акаунта вчителя може призвести до витоку даних цілого класу чи школи [2];

– DDoS-атаки на освітні портали: часто застосовуються під час вступних кампаній або сесій, що має на меті дестабілізацію психологічного стану суспільства [3].

Для розуміння пріоритетів захисту адміністрації закладу важливо розрізняти типи атак за рівнем складності та потенційними наслідками.

Характеристика актуальних кіберзагроз

Тип загрози	Об’єкт атаки	Основний інструментарій	Потенційні наслідки
AI-керований фішинг	Персонал, бухгалтерія	Генеративні моделі (GPT-4o та аналоги)	Викрадення фінансових ресурсів, доступ до адмін-панелей
Ransomware (Вимагачі)	Сервери, хмарні сховища	Шкідливе ПЗ для шифрування даних	Блокування роботи закладу, втрата наукових робіт, шантаж
DDoS-атаки	Сайти ЗВО, системи НМТ/ЄДЕБО	Ботнети (мережі заражених пристроїв)	Неможливість подання заяв абітурієнтами, зрив іспитів
Витік даних (Data Breach)	Бази даних студентів/ учнів	Експлуатація вразливостей застарілого ПЗ	Оприлюднення конфіденційної інформації, судові позови

Держава реагує на ці виклики шляхом оновлення нормативної бази. Важливим кроком стало розпорядження КМУ щодо реалізації Стратегії кібербезпеки на 2025 рік, яке зобов’язало заклади освіти запровадити багаторівневу систему захисту [4].

Особливу увагу приділено єдиним підходам до оцінювання стану кіберзахисту, впровадженим Держспецзв'язком у 2026 році. Тепер заклади освіти мають проходити регулярні аудити та заповнювати профілі безпеки, що дозволяє виявляти "слабкі місця" до того, як ними скористаються хакери [3]. Також було оновлено методичні рекомендації щодо безпеки дітей у цифровому просторі, які наголошують на важливості фільтрації контенту в шкільних мережах [2].

Попри потужні технічні засоби захисту, людина залишається найслабшою ланкою в системі кібербезпеки. Сьогодні цей виклик набув особливої гостроти через поєднання двох чинників: дефіциту фахівців та професійного вигорання освітян.

За статистичними даними 2024/2025 навчального року, систему освіти залишили близько 12% педагогічних працівників [6]. Це призвело до того, що навантаження на вчителів, які залишилися, зросло в середньому на 30-40%. У стані хронічної втоми та стресу здатність людини розпізнавати загрози суттєво знижується. Виникає явище, яке дослідники називають «безпековою амнезією»: педагог, знаючи правила цифрової гігієни, свідомо ігнорує їх (наприклад, не виходить з облікового запису на загальному комп'ютері або використовує один пароль для пошти та електронного журналу), щоб заощадити час.

Іншим аспектом кадрової кризи є критична нестача системних адміністраторів та фахівців із кібербезпеки безпосередньо в штаті закладів (особливо середньої освіти). Через неконкурентну заробітну плату в державному секторі кваліфіковані ІТ-кадри переходять у приватний бізнес. Як наслідок:

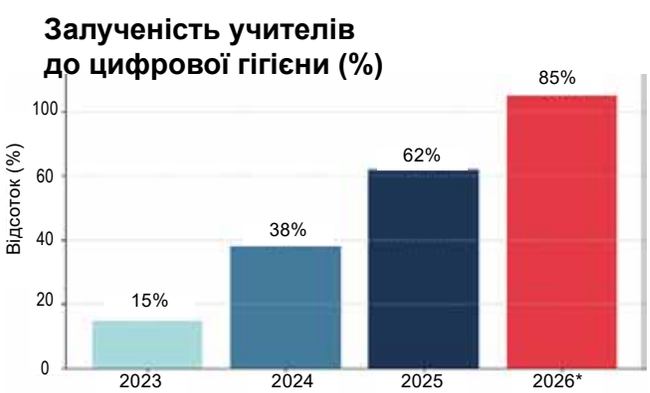
- Застаріле програмне забезпечення (ПЗ): оновлення систем безпеки проводиться нерегулярно або формально.

- Відсутність моніторингу: у багатьох школах не здійснюється належний контроль за трафіком, що дозволяє прихованим загрозам перебувати в мережі місяцями.

- «Тіньове ІТ» (Shadow IT): вчителі часто використовують сторонні месенджери та незахищені сервіси для передачі конфіденційних даних учнів, оскільки офіційні платформи здаються їм надто складними.

Важливим аспектом є віковий склад та рівень адаптивності педагогічного колективу. У 2026 році державна політика спрямована на перехід від «страху перед технологіями» до «свідомого управління ризиками». Впровадження концепції Lifelong Learning (навчання впродовж життя) дало змогу підвищити рівень залученості освітян до тренінгів на 62% (Рис. 1). Проте ключовим завданням залишається трансформація знань у стійку звичку.

Освіта сьогодні потребує не просто користувачів ПК, а «цифрових громадян», які здатні ідентифікувати ознаки соціальної інженерії на рівні рефлексів. Як зазначається в методичних рекомендаціях [2], успішна модель кібербезпеки в закладі можлива лише тоді, коли адміністрація стимулює культуру відкритості: вчитель не повинен боятися повідомити про випадковий клік на підозріле посилання, оскільки швидке реагування мінімізує збитки. Згідно з моніторингом впровадження Стратегії кібербезпеки, спостерігається позитивна динаміка охоплення педагогів спеціалізованим навчанням. Це пов’язано з появою обов’язкових модулів у програмах підвищення кваліфікації.



На основі аналізу останніх досліджень та рекомендацій [5, 7], пропонується наступна модель захисту:

1. Технічний рівень: впровадження обов'язкової двофакторної автентифікації (2FA) для всіх працівників. Використання сертифікованих хмарних сервісів із шифруванням даних;

2. Освітній рівень: інтеграція модулів із кібербезпеки у предмети "Інформатика" та "Я досліджую світ". Проведення щорічних тренінгів для вчителів;

3. Організаційний рівень: створення плану реагування на кіберінциденти. Кожен працівник має знати, куди звертатися у разі підозри на злам акаунта.

Кібербезпека в закладах освіти перестала бути суто технічним питанням і перейшла в площину управлінської стратегії. У 2026 році успіх освітнього закладу залежить від його здатності захистити свої дані та навчити учнів безпечно існувати в цифровому світі. Синергія між державними стандартами та особистою відповідальністю кожного освітянина є єдиним шляхом до створення безпечного освітнього середовища.

Використані джерел:а

1. Кібербезпека: цифрове життя без ризиків. Поради для освітян / Державна служба якості освіти України. 2025. URL: https://surl.li/rnaqci

2. Цифрова безпека дітей у закладах освіти : методичні рекомендації / МОН України, Профспілка працівників освіти і науки України. 2026. URL: https://surl.lu/ojjjjs

3. Держспецзв'язку впроваджує єдині підходи до оцінювання стану кіберзахисту / Урядовий портал. 2026. URL: https://surl.li/nsehog

4. Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України : Розпорядження Кабінету Міністрів України № 204-р. URL: https://surl.li/vmxsfi

5. Кібербезпека: освіта, наука, техніка : наук. журн. / Київ. ун-т ім. Б. Грінченка. 2026. Вип. 32. URL: https://surl.lt/klvxkz

6. Статистичний звіт щодо кадрового забезпечення галузі освіти у 2024/2025 н.р. / Інтерфакс-Україна. 2025. URL: https://interfax.com.ua/news/general/1147228.html

7. 8 ефективних способів захисту особистих даних в інтернеті : аналіт. огляд / DAN-IT Education. 2025. URL: https://surl.li/fxfedn

8. Цифрова трансформація освіти: звіт про стан кіберграмотності педагогічних працівників (2026) / Аналітичний центр освітніх реформ. МОН України. 2026. URL: https://mon.gov.ua