



Олег ВАСИЛИШИН,
старший викладач кафедри менеджменту та освітніх технологій
ХОІППО ім.А.Назаренка, доктор філософії в галузі воєнних наук,
національної безпеки, безпеки державного кордону

Основні висновки комплексного дослідження сучасних кіберзагроз у школах

Анотація

У статті проаналізовано сучасні виклики кібербезпеки в закладах середньої освіти, систематизовано ключові загрози та вразливості інформаційної інфраструктури шкіл. Визначено роль цифрової грамотності та організаційних політик у забезпеченні кіберстійкості. Запропоновано комплексну модель кіберзахисту, що охоплює технічні, організаційні, освітні та психологічні компоненти. Розширений виклад дозволяє глибше розкрити проблематику та забезпечує практичну цінність дослідження для керівників освітніх установ, педагогів і фахівців із цифрової безпеки.

Вступ

Цифрова трансформація освіти в останні роки суттєво прискорилася: активно впроваджуються електронні щоденники, системи управління навчанням (LMS), інтерактивні платформи, онлайн-тестування та хмарні сервіси. Водночас із розширенням цифрових можливостей зростає і кількість кіберінцидентів, що створюють загрози для стабільності освітнього процесу, конфіденційності персональних даних і психологічної безпеки учнів.

На відміну від комерційних організацій, заклади середньої освіти часто функціонують в умовах обмеженого фінансування, нестачі кваліфікованих ІТ-фахівців та недостатнього рівня цифрової компетентності користувачів. Це робить їх уразливими до кіберзагроз і привабливими для зловмисників.

Метою статті є комплексне дослідження сучасних кіберзагроз у школах та розроблення ефективної моделі кіберзахисту, адаптованої до умов середньої освіти.

Сучасні кіберзагрози для шкіл

Фішинг і соціальна інженерія

Фішингові повідомлення часто маскуються під офіційні листи адміністрації, електронних журналів або державних установ. Їх ефективність у шкільному середовищі зумовлена низьким рівнем перевірки джерел інформації, довірою до «офіційних» повідомлень та використанням змішаних (особистих і робочих) акаунтів.

Наслідками таких атак можуть бути компрометація облікових записів, несанкціонований доступ до освітніх платформ, зміна оцінок та витік персональних даних.

Шкідливе програмне забезпечення

Віруси, трояни, шпигунське ПЗ та програми-вимагачі (ransomware) становлять одну з найсерйозніших загроз. Вони здатні блокувати доступ до інформаційних ресурсів школи та шифрувати критичні дані з подальшою вимогою викупу.

Основні шляхи зараження включають відкриття шкідливих вкладень, використання неліцензійного програмного забезпечення, завантаження небезпечних файлів та експлуатацію застарілих систем.

Витоки та крадіжка даних

Освітні заклади обробляють значні обсяги конфіденційної інформації, включаючи персональні, медичні та соціальні дані учнів. Недостатній рівень захисту може призвести до їх витоку, що має як правові, так і етичні наслідки.

Серед основних причин — слабкі паролі, відсутність контролю доступу, використання незахищених носіїв інформації.

DDoS-атаки

Розподілені атаки відмови в обслуговуванні спрямовані на перевантаження серверів великим обсягом фальшивих запитів, що робить онлайн-ресурси недоступними. У шкільному середовищі навіть учні можуть ініціювати такі атаки, що призводить до збоїв у роботі електронних журналів та освітніх платформ.

Внутрішні загрози

Значна частина інцидентів пов'язана з діями користувачів — як навмисними, так і випадковими. Це можуть бути спроби обходу обмежень, несанкціонований доступ до систем або завантаження небезпечного контенту.

Нормативно-правова база кібербезпеки

GDPR (англ. General Data Protection Regulation, GDPR; Regulation (EU) 2016/679)

Регламент ЄС щодо захисту персональних даних встановлює вимоги до їх обробки, зберігання та захисту. Він передбачає право доступу до даних, обов'язок повідомлення про інциденти та відповідальність організацій за порушення.

Державні стандарти

Національні вимоги передбачають впровадження політики інформаційної безпеки, захищених каналів зв'язку та регулярного навчання персоналу.



Міжнародні стандарти

Стандарти ISO/IEC 27001 і 27002 визначають підходи до управління інформаційною безпекою, включаючи контроль доступу, аудит і криптографічний захист.

Технічна інфраструктура кіберзахисту

Захист мережі передбачає використання міжмережних екранів, сегментацію мережі (VLAN), шифрування Wi-Fi та регулярне оновлення обладнання. Контроль доступу реалізується через багатофакторну автентифікацію та принцип мінімальних привілеїв.

Кінцеві пристрої повинні бути захищені антивірусними рішеннями та системами моніторингу. Важливим елементом є резервне копіювання даних із використанням комбінованого підходу (локального та хмарного зберігання).

Людський фактор

Цифрова грамотність є ключовим елементом кібербезпеки. Педагоги повинні володіти навичками розпізнавання загроз, а учні — основами безпечної поведінки в Інтернеті. Адміністрація закладу відіграє провідну роль у впровадженні освітніх програм і контролі їх ефективності.

Організаційні політики безпеки

Ефективна система кіберзахисту передбачає наявність чітко визначених політик: інформаційної безпеки, управління пароллями, реагування на інциденти та використання пристроїв. Вони регламентують доступ до інформації, порядок обробки даних і дії у кризових ситуаціях.

Управління кіберризиками

Оцінювання ризиків включає ідентифікацію активів, аналіз вразливостей та визначення потенційного впливу загроз. Використання матриці ризиків дозволяє пріоритизувати заходи захисту.

Ефективне управління ризиками базується на поєднанні технічних, організаційних та процесних рішень.

Кібербулінг і безпека учнів

Кібербулінг є важливою складовою цифрової безпеки. Його прояви включають погрози, приниження, поширення приватної інформації та створення фейкових акаунтів.

Профілактика передбачає освітні заходи, створення безпечних каналів повідомлення та співпрацю з батьками. Важливу роль відіграють також технічні інструменти контролю та фільтрації контенту.

Найкращі практики кіберзахисту

Ефективний кіберзахист поєднує технічні заходи (оновлення систем, резервне копіювання, сегментація мереж), освітні ініціативи (тренінги, інтеграція цифрової грамотності) та організаційні рішення (аудити, регламенти, звітність).

Комплексна модель кіберзахисту

Запропонована модель включає чотири взаємопов'язані рівні:

- технічний (захисна інфраструктура);
- організаційний (політики та контроль);
- освітній (підготовка користувачів);
- психологічний (підтримка учасників освітнього процесу).

Їх поєднання забезпечує комплексний підхід до кібербезпеки.

Висновки

Кібербезпека в закладах середньої освіти є критично важливою умовою стабільного функціонування освітнього процесу в умовах цифровізації. Ефективний захист можливий лише за умови комплексного підходу, що поєднує технічні рішення, організаційні механізми та розвиток цифрової компетентності користувачів. Запропонована модель кіберзахисту дозволяє мінімізувати ризики кіберінцидентів, підвищити рівень захищеності інформаційних систем і створити безпечне освітнє середовище для всіх учасників.

Використані джерела

1. Anderson R. Security Engineering. Wiley, 2021.
2. ENISA. Cybersecurity in Education Report, 2023.
3. Johnson M. Cybersecurity for Schools: Best Practices. Routledge, 2022.
4. Kello L. The Virtual Weapon and International Order. Yale University Press, 2017.
5. NIST. Framework for Improving Critical Infrastructure Cybersecurity, 2020.
6. U.S. Department of Education. Data Privacy and Cybersecurity Guidance, 2023.
7. West J. Digital Safety in Education. Oxford University Press, 2022.