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

Кібербезпека в закладах загальної середньої освіти

У статті проаналізовано сучасні виклики кібербезпеки в закладах середньої освіти, систематизовано ключові загрози та слабкі місця 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 глибинно розкрити кожен аспект проблематики та забезпечити практичну цінність дослідження для керівників освітніх установ, учителів та фахівців із цифрової безпеки.

Цифрова трансформація освіти останніми роками значно пришвидшилася: електронні щоденники, системи управління навчанням (LMS), інтерактивні платформи, онлайн-тести, хмарні сервіси. Проте разом із перевагами зростає й кількість кіберінцидентів, що загрожують роботі шкіл, конфіденційності персональних даних та психологічній безпеці учнів.

Школи, на відміну від комерційних компаній, часто мають обмежене фінансування, недостатній рівень IT-експертизи, а працівники та учні не завжди володіють базовими навичками цифрової безпеки. Усе це робить навчальні заклади привабливою мішенню для кіберзлочинців.

Мета статті — комплексно дослідити сучасні кіберзагрози в школах та запропонувати ефективну модель кіберзахисту, адаптовану до умов середньої освіти.

1. Сучасні кіберзагрози для шкіл

1.1. Фішинг і соціальна інженерія

Фішингові листи часто маскуються під повідомлення адміністрації, сервісів електронних журналів або державних установ. У шкільному середовищі ці атаки успішні через:

- низьку культуру перевірки джерел інформації;
- відсутність корпоративних систем фільтрації;
- довіру до «офіційних» листів;
- одночасне використання особистих та шкільних акаунтів.

Наслідки успішного фішингу включають крадіжку облікових записів, доступ до електронного журналу, зміну оцінок, витік особистих даних.

1.2. Віруси, трояни, шпигунське ПЗ та ransomware

Програми-вимагачі становлять найбільшу загрозу, оскільки можуть повністю заблокувати роботу школи. Злочинці шифрують базу даних учнів, мережеві диски, навчальні матеріали, після чого вимагають викуп.

Поширені шляхи зараження:

- відкриття шкідливих вкладень у листах;
- використання неліцензійного ПЗ;
- завантаження «безкоштовних» програм учнями;
- вразливості у застарілих ОС.

1.3. Витоки та крадіжка даних

Школи зберігають великі масиви конфіденційної інформації: персональні дані, медичні довідки, психологічні характеристики, відомості про сім'ю. Витік таких даних може мати серйозні правові та етичні наслідки.

Причини витоків:

- слабкі паролі;
- незахищені бази даних;
- необмежений доступ великої кількості працівників;
- використання USB-носіїв.

1.4. DDoS (Distributed Denial of Service) атаки – це кібератака, спрямована на перевантаження цільового онлайн-ресурсу (сайту, сервера, мережі) величезним потоком фальшивого трафіку або запитів з безлічі заражених пристроїв (ботнета), щоб зробити його недоступним для звичайних користувачів, виводячи з ладу або сповільнюючи. Атака використовує розподілену мережу компрометованих пристроїв (комп'ютери, смартфони) для створення масивного, нелегітимного трафіку, який вичерпує ресурси сервера.

Навіть учні можуть ініціювати DDoS-атаку на шкільний сайт чи електронний журнал, що призводить до неможливості використання онлайн-ресурсів.

1.5. Внутрішні загрози

Навмисні чи ненавмисні дії користувачів становлять значну частку інцидентів:

- учні намагаються обійти фільтри, змінити оцінки, зламати Wi-Fi;
- учителі можуть ненавмисно завантажити шкідливий файл.

2. Нормативно-правова база кібербезпеки в освіті

Розуміння нормативних вимог є ключовим для безпечної роботи школи.

2.1. GDPR (General Data Protection Regulation) — це регламент ЄС, що захищає персональні дані громадян європейського союзу, надаючи їм більше контролю над інформацією та встановлюючи суворі правила для організацій щодо збору, обробки та зберігання цих даних. він стосується будь-якої компанії, яка обробляє дані мешканців ЄС, незалежно від її розташування, і поширюється на імена, ір-адреси та інші ідентифікувальні дані.

GDPR встановлює суворі правила щодо:
- обробки персональних даних;
- права учнів та батьків на доступ до своїх даних;
- зберігання та видалення інформації;
- повідомлення про інциденти протягом 72 годин.

2.2. Державні стандарти безпеки
Вони вимагають:
- захищених каналів зв'язку в освітніх установах;
- політики безпеки;
- захищених реєстрів інформації;
- регулярного навчання персоналу.

2.3. Міжнародні стандарти
ISO/IEC 27001 і 27002 встановлюють вимоги до управління активами, контролю доступу, криптографічного захисту, моніторингу та аудиту.

3. Технічна інфраструктура кіберзахисту

3.1. Захист мережі
Сюди входить:
- міжмережевий екран;
- VLAN-сегментація (розділення учнівської, адміністративної та гостьової мережі);
- шифрування Wi-Fi та прихований SSID;
- регулярне оновлення роутерів.

3.2. Контроль доступу
Школам рекомендовано застосовувати:
- багатофакторну автентифікацію;
- складні паролі й регулярний їх перегляд;
- доступ «мінімально необхідного рівня».

3.3. Захист кінцевих пристроїв
Комп'ютери вчителів та учнів мають бути оснащені:
- антивірусами;
- обмеженими правами доступу;
- системами моніторингу.

3.4. Резервне копіювання
Рекомендовано:
- щоденні інкрементні копії;
- щотижневі повні копії;
- зберігання у хмарі та офлайн.

3.5. Хмарні сервіси
Хмара має відповідати стандартам GDPR, забезпечувати шифрування в русі та спокої.

4. Людський фактор: цифрова грамотність та кібергігієна

4.1. Підготовка персоналу
Учителі повинні вміти:
- розпізнавати фішингові повідомлення;
- користуватися менеджерами паролів;
- перевіряти достовірність сайтів.

4.2. Навчання учнів
Учні мають розуміти:
- як створювати надійні паролі;
- як уникати онлайн-шахрайства;
- що таке цифровий слід.

4.3. Роль адміністрації
Адміністрація відповідає за організацію тренінгів, створення політик і моніторинг виконання вимог.

5. Організаційні політики безпеки

5.1. Політика інформаційної безпеки
Вона визначає:
- категорії інформації;
- правила доступу;
- процедури обробки файлів;
- відповідальних осіб.

5.2. Політика паролів
Рекомендується:
- мінімум 12 символів;
- заборона повторного використання;
- зміна раз на 90 днів.

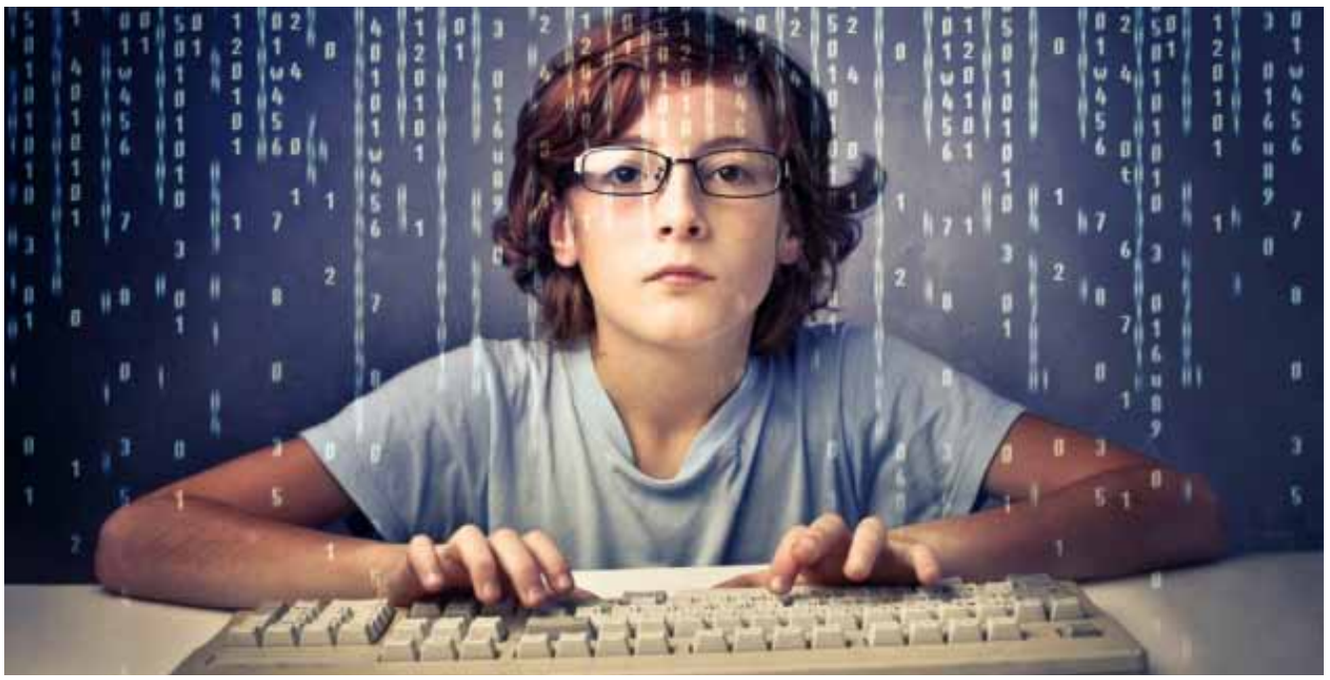
5.3. Політика реагування на інциденти
Має містити:
- алгоритм дій під час атаки;
- відповідальних осіб;
- плани відновлення.

5.4. Політика використання пристроїв
Передбачає правила роботи з:
- шкільними ноутбуками;
- особистими смартфонами;
- USB-носіями.

6. Оцінювання та управління кіберризиками

6.1. Етап оцінювання
- ідентифікація активів;
- визначення вразливостей;
- оцінювання ймовірності загрози.

6.2. Матриця ризиків
Школи можуть використовувати просту матрицю «ймовірність × вплив», щоб визначити найкритичніші ризики.



6.3. Міт
Стратегії:
● технічні (антивіруси, MFA);
● організаційні (навчання, політики);
● процесні (аудит, журналювання).

7. Кібербулінг і цифрова безпека учнів

7.1. Форми кібербулінгу
● погрози;
● висміювання;
● розповсюдження приватних фото;
● створення фейкових акаунтів.

7.2. Профілактика
Школа повинна:
● проводити уроки цифрової етики;
● створити безпечний механізм повідомлення;
● співпрацювати з батьками.

7.3. Технічні засоби
● фільтри контенту;
● системи моніторингу мережі;
● налаштування приватності на шкільних платформах.

8. Найкращі практики кіберзахисту

Технічні
● обов'язкові оновлення;
● резервне копіювання;
● сегментація мереж.
Освітні
● щорічні тренінги;
● інтеграція цифрової грамотності в навчальні програми.
Організаційні
● аудит двічі на рік;
● чіткі посадові інструкції;
● звіти про інциденти.

9. Комплексна модель кіберзахисту для шкіл

Модель включає чотири рівні:
9.1. Технічний рівень:
● міжмережеві екрани;
● контроль доступу;
● шифрування.
9.2. Організаційний рівень;
● політики;
● моніторинг;
● аудит.
9.3. Освітній рівень:
● навчання персоналу;
● уроки кібергігієни.
9.4. Психологічний рівень:
● підтримка жертв кібербулінгу;
● робота психолога;
● взаємодія з батьками.

Кібербезпека в закладах середньої освіти є однією з ключових умов стабільної роботи навчального процесу. Школам необхідно впроваджувати комплексні технічні рішення, систематизовані організаційні політики та ефективні програми навчання. Запропонована модель кіберзахисту дозволяє створити стійку інфраструктуру, зменшити ризики інцидентів і забезпечити безпеку всіх учасників освітнього процесу.

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.