

Цифрова безпека школи: захищаємо не тільки дітей

Консультація для членів адміністрації закладів освіти. Сучасна школа — це не лише класи та підручники, а й розгалужена цифрова інфраструктура: облікові записи, освітні платформи, бази даних учнів і педагогів. Кожен із цих елементів є потенційною мішенню для кіберзлочинців. Мета — сформувати системне розуміння цифрових ризиків та практичних кроків захисту.

КІБЕРБЕЗПЕКА

ОСВІТА

АДМІНІСТРАЦІЯ



Розділ 1

Цифрове середовище закладу освіти

Щоб ефективно захищати заклад, потрібно чітко розуміти, що саме потребує захисту. Цифрове середовище сучасної школи охоплює широкий спектр ресурсів, кожен з яких несе власні ризики.

Інформаційні ресурси

Офіційний сайт школи, електронні журнали, документація, накази, звіти, фінансові документи.

Облікові записи

Акаунти адміністрації, педагогів, учнів у Google Workspace, Office 365, ЄДЕБО.

Освітні платформи

На Урок, Всеосвіта, Zoom, Google Classroom, Moodle, Prometheus — місця зберігання даних учасників.

Персональні дані

Особисті дані учнів, батьків, працівників: ПІБ, адреси, телефони, медичні відомості, фото.

Розділ 2

Вразливі точки закладу

Що найбільше під загрозою?

Кіберзлочинці шукають найслабшу ланку. У шкільному середовищі це зазвичай:

- Електронна пошта керівників і бухгалтерії
- Акаунти педагогів із простими паролями
- Спільні пристрої без антивірусного захисту
- Неоновлене програмне забезпечення
- Відкриті Wi-Fi мережі без автентифікації

Реальні сценарії загроз

Електронна пошта

Злам скриньки директора = доступ до всіх офіційних документів і можливість шахрайства від імені закладу.

Бази даних

Витік персональних даних учнів — порушення законодавства та репутаційна катастрофа.

Пристрої

Заражений ноутбук учителя може стати точкою входу для атаки на всю мережу школи.

Розділ 3

Персональні дані: ризики та відповідальність

Заклад освіти є оператором персональних даних відповідно до Закону України «Про захист персональних даних». Несанкціонований доступ, втрата або розголошення даних учасників освітнього процесу – це не лише технічна, а й юридична відповідальність адміністрації.



Ризик втрати даних

Видалення або пошкодження баз даних унаслідок атаки вірусом-шифрувальником може паралізувати роботу закладу на тижні.



Несанкціонований доступ

Зловмисник, який отримав доступ до журналу оцінок або медичних карток, може використати цю інформацію для шантажу чи маніпуляцій.



Розголошення третім особам

Передача даних учнів стороннім сервісам без згоди батьків або публікація фотографій дітей без дозволу – прямі порушення законодавства.

 Адміністрація несе персональну відповідальність за організацію захисту даних. Незнання не звільняє від відповідальності!

Розділ 4

Фішинг, соціальна інженерія та шкідливі вкладення

Як розпізнати загрозу?

1 Підозрілий відправник

Адреса е-пошти, схожа на офіційну, але з незначними відмінностями (наприклад, `g00gle.com` замість `google.com`).

2 Терміновість і тиск

«Терміново підтвердіть дані», «Ваш акаунт буде заблоковано» — маніпуляція страхом спонукає до необдуманих дій.

3 Підозрілі вкладення

Файли з розширеннями `.exe`, `.scr`, `.bat`, а також макроси у документах Word/Excel — потенційно небезпечні.



Типові сценарії зараження

Вкладення-вірус

Лист із «рахунком» або «наказом МОН» містить шкідливий файл. Відкриття — і зловмисник у системі.

Підроблене посилання

Кнопка «Увійти в Google» веде на фейковий сайт, який збирає логін і пароль.

Дзвінок «з МОН»

Шахрай представляється чиновником і просить повідомити пароль або дані доступу.

Розділ 5

Захист облікових записів і безпечне використання платформ



Надійні паролі

Мінімум 12 символів: великі та малі літери, цифри, спецсимволи. Жодних «password123» або дат народження. Використовуйте менеджер паролів.



Двофакторна автентифікація

Обов'язково для всіх акаунтів адміністрації та педагогів. SMS-код або додаток-автентифікатор — навіть при витоку паролю зломисник не увійде.



Розмежування доступу

Кожен працівник має доступ лише до тих ресурсів, які необхідні для його роботи. Регулярно переглядайте список активних доступів.



Відповідальність за платформи

При реєстрації в новому сервісі перевіряйте політику конфіденційності. Не передавайте дані учнів платформам без відповідних угод.

Розділ 6

Фільтрація шкідливого контенту

Організаційні заходи

- **Політика використання** — затвердіть внутрішній документ із переліком допустимих і заборонених дій у цифровому середовищі школи.
- **Навчання працівників** — щонайменше раз на рік проводьте інструктаж із кібербезпеки для всіх педагогів і технічного персоналу.
- **Контроль пристроїв** — обмежте встановлення неавторизованого ПЗ на шкільних комп'ютерах.

Технічні заходи

- Налаштуйте DNS-фільтрацію (наприклад, CleanBrowsing, NextDNS) для блокування шкідливих сайтів
- Увімкніть безпечний пошук у всіх браузерях
- Встановіть антивірусне ПЗ на всі пристрої
- Налаштуйте брандмауер мережі закладу
- Регулярно оновлюйте операційні системи та програми

⚠️ Ключовий розділ

Кіберінцидент: поняття та ознаки

Кіберінцидент — це будь-яка подія, що загрожує конфіденційності, цілісності або доступності інформаційних ресурсів закладу. Вчасне розпізнавання інциденту — перший крок до мінімізації збитків.

- 1 Злам облікового запису**
Педагог або керівник не може увійти в систему; виявлено вхід із незнайомого пристрою чи місця; змінені дані без відома власника.
- 2 Втрата або шифрування даних**
Файли зникли, стали недоступні або мають незрозумілі розширення; на екрані з'явився вимога викупу (ransomware).
- 3 Підозріла активність у мережі**
Комп'ютери працюють повільно; незрозумілі підключення; масова розсилка листів від імені працівника без його участі.
- 4 Отримання шкідливого листа або посилання**
Хтось із працівників відкрив підозрілий файл; система безпеки спрацювала; з'явилися незрозумілі програми на пристрої.
- 5 Витік персональних даних**
Дані учнів або працівників з'явилися у відкритому доступі; отримано повідомлення про компрометацію бази даних.

⚠ Алгоритм дій адміністрації

Що робити при кіберінциденті: покроковий план

Повідомлення та документація

Повідомте керівництво, зафіксуйте докази.

Виявлення та ізоляція

Розпізнайте інцидент, від'єднайте пристрої.

Стимування та відновлення

Змініть паролі, відновіть з резервної копії.

Аналіз і запобігання

Дослідіть причини, оновіть політики.

Алгоритм реагування на кіберінцидент складається з чотирьох послідовних фаз: виявлення та ізоляція, повідомлення та документування, стимування та відновлення, аналіз і запобігання. Кожна фаза є критично важливою для мінімізації наслідків.

📞 Кого інформувати?

- **Внутрішньо:** директор, відповідальний за ІТ, засновник/управління освіти
- **Технічно:** системний адміністратор або зовнішній ІТ-підрядник
- **Державно:** Держспецзв'язку (кіберполіція) — при серйозних інцидентах
- **Учасники:** батьки — якщо скомпрометовано дані учнів

🚫 Чого НЕ робити?

- | Не видаляйте файли та логи — вони потрібні для розслідування
- | Не сплачуйте викуп при ransomware-атаці — це не гарантує відновлення
- | Не повідомляйте про інцидент у соцмережах до офіційного повідомлення
- | Не ігноруйте інцидент — навіть «невеликий» злам може мати серйозні наслідки

Підсумок

Розподіл відповідальності та ключові висновки

Директор

Загальна відповідальність, прийняття рішень, інформування засновника та контролюючих органів.

Педагоги

Дотримання правил безпеки, негайне повідомлення про підозрілі події, захист своїх акаунтів.

Відповідальний за ІТ

Технічне реагування, ізоляція загроз, відновлення систем, ведення журналів подій.

Усі працівники

Знання ознак фішингу, використання надійних паролів, регулярне оновлення ПЗ.

Три головні принципи

Проактивність

Захищайтеся до інциденту, а не після нього. Навчання, політики, технічний захист.

01

Системність

Безпека — це не разова дія, а безперервний процес оцінки ризиків і вдосконалення.

02

Відповідальність

Кожен працівник — ланка в ланцюгу безпеки. Слабка ланка компрометує весь заклад.

03

Пам'ятайте

Кібербезпека школи — це не лише технічне питання. Це питання репутації закладу, довіри батьків і, насамперед, захисту дітей у цифровому просторі.

Ваша обізнаність і готовність діяти — найкращий захист для вашої школи.