



Оксана САВИЧ,
вчителька інформатики Маниковецького ліцею
Деражнянської міської ради

Кібербезпека: небезпеки та шляхи їх подолання в освітньому середовищі

Проблеми кібербезпеки досліджуються в межах педагогіки, інформаційних технологій та психології. Науковці наголошують на необхідності формування інформаційної культури, розвитку критичного мислення та навичок безпечної поведінки в мережі.

Серед найпоширеніших небезпек кіберзагроз можна виділити:

Фішинг — шахрайські спроби отримати конфіденційну інформацію (паролі, банківські дані). До цього виду можна віднести так звані дитячі інтернет-ігри, де шахраї просять у дітей номер банківської картки батька чи матері, щоб оплатити перехід на «новий рівень гри». Такий випадок був у моєї роботи. Дівчинка (учениця 3 класу) прийшла до мами і попросила номер банківської картки батька. Мати провела бесіду з донькою про безпеку, яка її чекала.

Кібербулінг — цькування в онлайн-середовищі, яке особливо небезпечне для дітей та підлітків. Зазвичай, це діти, яких не сприймають однолітки через певні вади у здоров'ї чи «недостатньо багатий» одяг. Найбільшого цькування зазнають діти, які не можуть дати відсіч, не можуть повідомити батькам про ситуацію, яка склалась, через страх перед їх рішеннями.

Шкідливе програмне забезпечення — віруси, трояні, які можуть пошкодити дані або отримати доступ до пристрою.

Соціальна інженерія — маніпуляції людьми з метою отримання інформації.

Витік персональних даних — через необережність або недостатній рівень захисту.

Особливо вразливою категорією є учні, які часто не усвідомлюють усіх ризиків цифрового середовища.

Актуальність проблеми кібербезпеки підтверджується численними реальними випадками, які демонструють масштаб і наслідки цифрових загроз. У період активного впровадження дистанційного навчання почастишали випадки отримання учнями та педагогами фальшивих листів, які імітують повідомлення від популярних освітніх сервісів (наприклад, Google Classroom або електронних щоденників). Користувачі переходили за посиланням і вводили свої логіни та паролі, після чого їх акаунти ставали доступними для злоумисників.

Наслідки:

- втрата доступу до навчальних матеріалів;
- розсилка спаму від імені користувача;
- витік персональних даних.

У багатьох школах фіксуються випадки створення анонімних Telegram-каналів або чатів, де поширюються

образливі повідомлення, фото чи відео про учнів або навіть учителів.

Наслідки:

- зниження самооцінки;
- страх відвідувати школу;
- емоційні розлади.

Один із поширених випадків — встановлення учнями неліцензійних програм або ігор із сумнівних сайтів. Разом із ними на комп'ютер потрапляють віруси або шпигунське програмне забезпечення. Учні часто публікують у відкритому доступі особисту інформацію: номер телефону, адресу, геолокацію, фото документів.

У світі та в Україні фіксуються випадки кібератак на школи та університети, що призводить до блокування роботи систем. Наприклад, під час глобальної кібератаки вірусом-шифрувальником Wanna Cry ransomware attack було паралізовано роботу багатьох установ, включаючи освітні.

Наслідки:

- втрата даних;
- призупинення навчального процесу;
- фінансові витрати на відновлення систем.

Реальні приклади підтверджують, що кіберзагрози мають не лише технічний, але й соціально-психологічний характер. Це підкреслює необхідність комплексного підходу до формування кібербезпеки в освітньому середовищі.

Основними причинами виникнення кіберзагроз є:

- недостатній рівень цифрової грамотності;
- відсутність системного навчання з кібербезпеки;
- необережна поведінка користувачів;
- слабкий захист інформаційних систем;
- активне використання соціальних мереж без належного контролю.

Які ж є шляхи вирішення проблем кібербезпеки?

Освітні заходи:

- впровадження уроків і тренінгів з кібербезпеки;
- проведення інформаційних кампаній;
- формування навичок критичного мислення.

Технічні заходи:

- використання антивірусного програмного забезпечення;
- регулярне оновлення систем;
- створення складних паролів та двофакторна аутентифікація.

Педагогічна підтримка:

- формування культури безпечної поведінки в Інтернеті (тижні безпечного Інтернету, уроки безпеки в Інтернеті);
- розвиток відповідальності за власні дії в мережі;

• співпраця з батьками щодо контролю цифрової активності дітей (уроки для батьків щодо безпеки в Інтернеті, батьківські збори).

Психологічний аспект:

- створення безпечного освітнього середовища;
- підтримка учнів у випадках онлайн-агресії;
- розвиток емоційного інтелекту.

Сучасні дослідження та аналітичні звіти підтверджують стрімке зростання кіберзагроз у світі та їх значний вплив на освітню сферу. У першій половині 2025 року кількість атак програм-вимагачів на освітні установи зросла на 23%, що свідчить про підвищену зацікавленість кіберзлочинців до цього сектору. У середньому організації у світі зазнають понад 2000 кібератак щотижня, що демонструє глобальний масштаб проблеми. Освітні установи є одними з найуразливіших через велику кількість користувачів і недостатній рівень захисту.

Близько 15-16% підлітків повідомляють про власний досвід кібербулінгу протягом року. До 37% молоді віком 12–17 років хоча б раз стикалися з онлайн-цькуванням. У

деяких дослідженнях показано, що до 75% учнів можуть бути залучені до кібербулінгу (як жертви або учасники). Водночас понад 50% дітей не повідомляють дорослим про випадки кібербулінгу.

В Україні близько 100 000 учнів долучилися до програм підвищення цифрової грамотності лише в межах однієї освітньої ініціативи. При цьому лише 12% учнів мають доступ до систематичного навчання з кібербезпеки, що вказує на значний освітній розрив. Освітні заклади входять до числа найбільш атакованих секторів через наявність великої кількості персональних даних.

Дослідження показують, що навіть самі учні інколи стають джерелом кіберінцидентів, що підкреслює важливість формування відповідальної цифрової поведінки. Статистичні дані свідчать про те, що кіберзагрози в освітньому середовищі мають системний характер і тенденцію до зростання. Високий рівень кібербулінгу, недостатня цифрова грамотність та зростання кібератак на освітні установи підкреслюють необхідність комплексного підходу до формування кібербезпеки.



Людмила САВЧУК,
вчителька інформатики гімназії №25 імені Вадима Ангела
м.Хмельницького, вчитель-методист

Цифрова культура школярів як результат системної роботи з кібербезпеки

Сучасні школярі активно користуються соціальними мережами, онлайн-платформами та цифровими сервісами, що підвищує ризик їхньої вразливості до кіберзагроз.

У курсі інформатики питання кібербезпеки розглядається як наскрізна змістова лінія, інтегрована у вивчення інформаційних процесів, комп'ютерних мереж, алгоритмізації, опрацювання даних та цифрової комунікації. Формування компетентностей з кібербезпеки здійснюється поетапно та враховує вікові особливості учнів.

На уроках інформатики учні початкової ланки засвоюють:

- правила безпечної роботи за комп'ютером;
- поняття персональних даних;
- принципи створення надійних паролів;
- основи безпечного онлайн-спілкування;
- розпізнавання підозрілих повідомлень і шкідливих посилань.

У такий спосіб формується первинне уявлення про відповідальність за власну цифрову діяльність.

Зміст середньої ланки в питанні інформаційної безпеки ускладнюється та охоплює:

- поняття шкідливого програмного забезпечення;
- фішинг і соціальну інженерію;
- налаштування конфіденційності в цифрових сервісах;
- академічну доброчесність та авторське право;

- критичне оцінювання інформації та протидію фейкам;
- цифровий слід та його наслідки;
- кібербулінг і способи його запобігання.

Учні аналізують реальні ситуації кіберзагроз, відпрацьовують алгоритми дій у разі небезпеки та навчаються захищати власні облікові записи.

У старших класах середньої школи розглядаються:

- принципи захисту інформаційних систем;
- резервне копіювання даних;
- безпека локальних і глобальних мереж;
- правові аспекти відповідальності за порушення кібербезпеки;
- базові засади криптографічного захисту інформації.

Ефективність формування компетентностей з кібербезпеки підсилюється через проведення тематичних заходів та проєктів, зокрема:

- Тиждень медіа та інформаційної грамотності (остання декада жовтня).
- Місяць цифрової грамотності (листопад).
- День безпечного Інтернету (другий вівторок лютого).
- День паролів (перший четвер травня).
- Участь у всеукраїнських онлайн-уроках з кібербезпеки.
- Створення учнівських проєктів (відеоролики, презентації, пам'ятки).