



Галина РОМАНОВА,
вчителька математики та інформатики ліцею №15
імені Олександра Співачука м.Хмельницького

Як навчати учнів кібербезпеки в школі

Вступ

Смартфон у руках дитини — це не просто гаджет для розваг, а повноцінне вікно у світ, де поруч із безмежними знаннями чатують реальні небезпеки. Соціальна інженерія, фішинг, кібербулінг та дезінформація стали частиною повсякденного життя школярів. Саме тому навчання кібербезпеці перестало бути «додатковою темою» на уроках інформатики — тепер це базова навичка виживання, така ж важлива, як знання правил дорожнього руху.

Кібербезпека — це сукупність технічних і соціальних засобів, стратегій, принципів для забезпечення захисту суспільства від загроз та впливів з небажаними наслідками, що походять від інтернет-середовища. Кібербезпека — це процес застосування заходів безпеки з метою забезпечення конфіденційності, цілісності та доступності даних. Кібербезпека покликана захистити дані на етапі їх обміну та збереження. В законі України «Про основні засади здійснення кібербезпеки України» кіберпростір визначається як «середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних», а кібербезпека, як «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі».

У зв'язку з цим важливого значення набуває проблема культури безпечної поведінки у кіберпросторі. Згаданий вище закон зазначає, що розвиток безпечного, стабільного і надійного кіберпростору має полягати в тому числі і завдяки «підвищенню цифрової грамотності громадян та культури безпечного поводження в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських проєктів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту». В сучасних закладах освіти комп'ютерні технології використовуються майже при вивченні всіх навчальних предметів. Саме тому необхідно вдосконалювати сучасну професійну підготовку педагогів у сфері інформаційних технологій, а отже, і у сфері кібербезпеки [2].

Школа має стати платформою, де дитина вчиться не просто натискати кнопки, а критично оцінювати контент, захищати свої кордони та відповідати за власну «цифрову тінь». Наше завдання як педагогів — перетворити страх перед невідомими загрозами мережі на свідому цифрову грамотність. У цій статті ми розберемо, як зробити навчання кібергігієні цікавим, інтерактивним та, головне, ефективним для учнів різного віку.

Діти часто не усвідомлюють усіх ризиків, пов'язаних із використанням інтернету. Вони можуть:

- а) ділитися особистою інформацією;
- б) переходити за небезпечними посиланнями;
- в) спілкуватися з незнайомцями;
- г) ставати жертвами кібербулінгу.

В освітньому просторі кібербезпека перестала бути вузькою технічною темою. Сьогодні це частина життєвої компетентності. Однак традиційні методи «лекція-конспект» у цифровій сфері не працюють: діти сприймають їх як відірвані від реальності повчання. Щоб навчання було ефективним, педагог має використовувати активні та інтерактивні методи [3].

1. Метод ігрової симуляції (Гейміфікація)

Це найпотужніший інструмент для залучення учнів, особливо молодшої та середньої школи. Як це працює: використання спеціалізованих ігор, де дитина приймає рішення в безпечному віртуальному середовищі.

Приклад. Гра Interland від Google. Учні подорожують островами, де борються з фішерами, вчать бути ввічливими в мережі та створювати надійні паролі.

Результат. Формування навичок на рівні рефлексів: бачу підозріле посилання — не клікаю.

2. Метод аналізу кейсів (Case-study)

Підлітки краще вчать на реальних історіях, аніж на абстрактних правилах.

Як це працює. Розгляд реальних ситуацій (анонімних або медійних). Наприклад: «Учня зламали через те, що він перейшов за посиланням на безкоштовні ігрові скіни. Що він зробив не так і як повернути доступ?».

Результат. Розвиток аналітичного мислення та розуміння причинно-наслідкових зв'язків.

3. Метод «Цифрового детективу» (Пошукова діяльність)

Цей метод найкраще демонструє поняття «цифрового сліду».

Як це працює. Вчитель пропонує знайти інформацію про вигаданого персонажа, використовуючи лише відкриті дані (OSINT-техніки для початківців). Учні бачать, як за фотографією біля школи можна дізнатися адресу, розпорядок дня та інтереси людини.

Результат. Усвідомлення важливості налаштувань приватності та небезпеки овершерінгу.

4. Рольова гра та соціальне моделювання

Метод допомагає підготувати учнів до психологічного тиску з боку зловмисників.

Як це працює. Моделювання ситуацій соціальної інженерії. Один учень грає роль «працівника техпідтримки», інший — «користувача». Завдання першого — виманити код з SMS, завдання другого — розпізнати маніпуляцію.

Результат. Психологічна готовність сказати «ні» та припинити підозрілу розмову.

5. Проектна діяльність та метод «Рівний — рівному»

Учні стають не просто слухачами, а амбасадорами безпеки.

Як це працює. Старшокласники створюють пам'ятки, відеоролики в TikTok або квести для молодших класів на тему кібергігієни.

Результат. Коли підліток пояснює тему іншому, він сам засвоює її на 90%. Це підвищує авторитет знань у молодіжному середовищі.

6. Метод інтегрованого навчання

Кібербезпека не повинна обмежуватися уроками інформатики.

Математика: розрахунок кількості комбінацій для зламу пароля різної складності.

Іноземна мова: аналіз англійських фішингових листів.

Мистецтво: створення плакатів або цифрових банерів про правила безпеки в інтернеті.[9]

Ефективне навчання кібербезпеці базується на переході від концепції «заборони» до концепції «критичного вибору». Використовуючи ці методи, вчитель допомагає учням збудувати власний «цифровий імунітет», який захистить їх краще за будь-який антивірус.

5 «золотих правил» цифрової гігієни для учнів

- Приватність — це сила. Твоя адреса, номер школи та плани на вихідні не мають бути публічними. Поясни концепцію «цифрового сліду», який залишається назавжди.

- Пароль — як зубна щітка. Він має бути складним, індивідуальним і його не можна давати «покористуватися» навіть найкращим друзям.

- Двофакторна автентифікація (2FA). Це «другий замок» на дверях до акаунту, який захистить дані, навіть якщо пароль дізнаються сторонні.

- Критичне мислення. Не все, що написано в мережі — правда. Навчіть дітей ставити три запитання: Хто це написав? Навіщо? Де докази?

- Скріншот — твоя зброя. У разі кібербулінгу чи дивних повідомлень важливо зберегти докази та негайно звернутися до дорослих, яким довіряєш.[10]

Висновки

Навчання кібербезпеки є важливою складовою сучасної освіти. Школа має стати платформою, де дитина вчиться не просто натискати кнопки, а критично оцінювати контент та захищати власні межі. Кібербезпека — це не про обмеження, а про свободу бути в безпеці. Навчаючи дітей цим навичкам сьогодні, ми будемо стійке та свідоме суспільство майбутнього.

Використані джерела

1. Конституція України: Закон від 28.06.1996 № 254к/96-ВР.

2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII.

3. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI.

4. Концепція безпеки закладів освіти: Розпорядження Кабінету Міністрів України від 07.03.2025 № 202-р.

5. Базові правила кібергігієни: корисні матеріали для учнів і вчителів. Нова українська школа. 2024.

URL: nua.org.ua (дата звернення: 27.03.2026).

6. Методичні рекомендації щодо викладання інформатики у 2024/2025 навчальному році. Міністерство освіти і науки України.

7. Мужанова Т. Основні підходи та напрями розвитку політики ЄС у сфері кібербезпеки. Кібербезпека: освіта, наука, техніка. 2024. № 24.

8. Petrenko L. Digital Security within the framework of digital competence. Edukacja zawodowa i ustawiczna. 2023. № 8. С. 93–107.

9. Дія.Освіта: національна едьютейнмент-платформа. Освітні серіали з кібергігієни. URL: osvita.dia.gov.ua.

10. На Урок: освітній проект. База методичних розробок з кібербезпеки. URL: naurok.com.ua.

11. Всеосвіта: спільнота активних освітян. Матеріали до Тижня безпечного інтернету. URL: vseosvita.ua.

12. Кіберполіція України: офіційний портал. Рекомендації щодо захисту від онлайн-шахрайства. URL: cyberpolice.gov.ua.