

• 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:

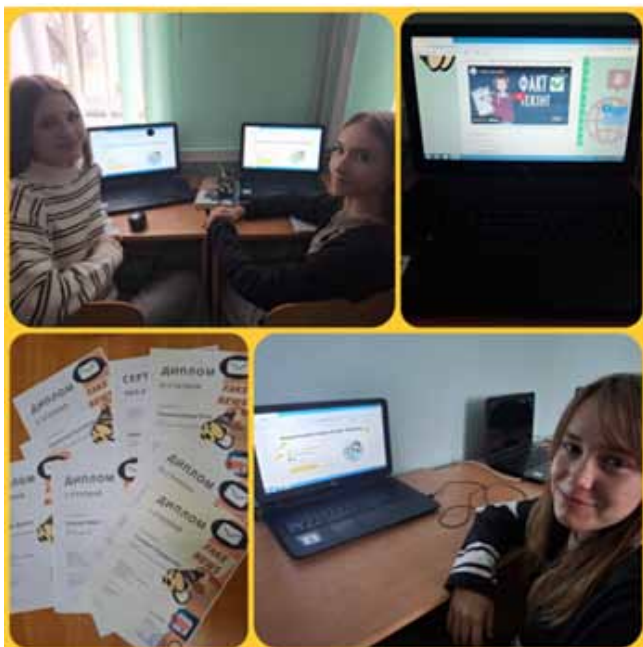
- Тиждень медіа та інформаційної грамотності (остання декада жовтня).
- Місяць цифрової грамотності (листопад).
- День безпечного Інтернету (другий вівторок лютого).
- День паролів (перший четвер травня).
- Участь у всеукраїнських онлайн-уроках з кібербезпеки.
- Створення учнівських проєктів (відеоролики,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

• Різноманітні тренінги для дітей і батьків щодо цифрової безпеки.

Такий комплексний підхід сприяє формуванню у школярів не лише базових навичок захисту інформації, а й відповідальної цифрової культури, що є необхідною умовою безпечної та ефективної діяльності в сучасному інформаційному середовищі.

Щороку ми долучаємось до таких ініціатив та проводимо безліч цікавих заходів, які мають на меті формування цифрової грамотності наших учнів. Різноманітні заходи на уроках інформатики стали гарним нагадуванням про важливість кібербезпеки у повсякденному житті.

Здобувачі освіти нашого закладу беруть учні у Всеукраїнському уроці медіаграмотності, метою якого є розвиток критичного мислення та навчання розрізняти факти від маніпуляцій, формування навичок безпечної поведінки в інформаційному просторі, підвищення стійкості до дезінформації, опанування інструментів перевірки фактів, зміцнення культури усвідомленого споживання контенту та ефективна протидія ворожим інформаційним впливам у цифровому середовищі.



Освітній проєкт «На Урок» дає можливість долучати дітей до конкурсів, що допомагають розрізняти фейки та інші підступні види інформаційних повідомлень в інтернеті та ЗМІ, дізнаватися захопливі факти про інформаційне суспільство та передумови його появи, допомагають сформувати інформаційну грамотність та вберегти від неприємностей, що можуть очікувати в мережі. Це такі конкурси, як «#StopFake», «Fake: як розпізнати та протидіяти?», «Твій кіберпростір: правила безпечного інтернету», активними учасниками яких є учні нашого навчального закладу.

Також з учнями долучаємось до заходів з платіжної безпеки від Національного банку України, щоб підвищити фінансову грамотність учнів, навчити їх захищати персональні дані та ефективно протидіяти кібершахрайству.

В рамках Місячника кібербезпеки на уроках інформатики учні 9-х класів знайомилися з основними типами кіберзагроз: вірусами, шкідливим програмним забезпеченням,

фішингом та іншими. Учні навчалися розпізнавати ці загрози та дізнавалися про ефективні способи захисту від них.



Для закріплення знань учні пройшли тест «Що ти знаєш про кібербезпеку?» від <https://nus.org.ua/>, який допоміг перевірити та поглибити їх розуміння безпечної поведінки в цифровому світі.

Учні 7-х класів долучились до активності «Місія: надійний пароль».

Під час заходу учні дізналися:

- які паролі вважаються слабкими і легко зламуються;
- які помилки найчастіше припускають користувачі;
- як виглядає дійсно надійний пароль;
- де і як безпечно зберігати свої паролі.

Школярі отримали рекомендації щодо захисту персональної інформації в інтернеті та повторили ключові правила кібергігієни в мережі.



Учні 6-их брали участь в інтерактивній грі «Впізнай загрозу», мета якої — зіставити популярні кіберзагрози з їх правильним описом. Така вправа допомагає школярам краще розпізнавати потенційні небезпеки в Інтернеті та зрозуміти, як від них захиститися.



Учні 8-их класів долучилися до освітнього міні-сеансу «Відеопauза з кібербезпеки», під час якого переглянули короткий ролик про кібербезпеку, як уберегтися від злочинців в мережі.

Після перегляду відео провели коротку бесіду, де школярі обговорили важливість надійних паролів, розпізнавання фішингових листів і захист особистих даних.

Під час інтерактивного "КіберКвесту" школярі на практиці опанували навички цифрового захисту: вчилися розрізняти факти та фейки, розпізнавати фішингові атаки, створювати надійні паролі та дотримуватися правил безпеки в соцмережах і онлайн-сервісах для захисту власних акаунтів.



Через ігрові та практичні завдання, інтерактивні вправи ми обговорюємо правила безпечної поведінки в мережі, захист персональних даних і культуру онлайн-спілкування, як обходити пастки в мережі.

Окрему увагу приділяємо темі кіберзагроз: шахрайству, фішингу, небезпечним посиланням і надмірному поширенню особистої інформації. Розбираємо реальні приклади та алгоритми дій у ризикованих ситуаціях.

До Дня безпечного інтернету, учні нашої школи занурилися у вивчення правил цифрового світу. Учні 9-х класів провели захід «Інтернет: можливості, загрози та безпечний вибір».

Наші старшокласники поділилися з іншими важливими знаннями:

- Від ARPANET до сьогодення: короткий екскурс в історію виникнення інтернету.
- Знай ворога в обличчя: детально розібрали основні загрози (фішинг, віруси, кібербулінг).
- Алгоритм захисту: як не потрапити на гачок шахраїв.
- Етика в мережі: нагадали про правила відповідально-го користування та повагу до інших.
- Цифрова варт: аналіз впливу надмірного перебування в мережі на здоров'я.

Учням нагадали про важливість балансу між онлайн-активністю та реальним життям, активним відпочинком і живим спілкуванням.

Отже, формування цифрової культури учнів через розвиток кібербезпеки є важливою складовою освітнього процесу. Системна, поетапна робота на уроках інформатики та позаурочних заходах забезпечує не лише засвоєння теоретичних знань про кіберзагрози, а й розвиток практичних навичок безпечної поведінки в цифровому середовищі.

Особливо ефективним є використання інтерактивних вправ, вебквестів, перегляду навчальних відеоматеріалів та ігрових завдань, які дозволяють учням:

- засвоїти правила безпечної роботи в мережі;
- навчитися розпізнавати фішингові листи, віруси та інші кіберзагрози;
- створювати надійні паролі та захищати особисті дані;
- критично оцінювати інформацію та протидіяти поширенню фейків;
- усвідомлювати відповідальність за власну поведінку в цифровому середовищі.

Поєднання традиційних уроків, інтерактивних активностей і тематичних заходів (Місячник кібербезпеки, День безпечного Інтернету, вебінари, проєктна діяльність) сприяє формуванню цілісної цифрової культури та відповідальної поведінки учнів у мережі.

Завдяки такому комплексному підходу школярі отримують не лише знання про безпеку, а й практичні компетентності, що дозволяють їм ефективно та безпечно користуватися цифровими технологіями, зберігаючи баланс між онлайн-активністю та реальним життям.

Використані джерела

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII.
2. Концепція розвитку цифрових компетентностей громадян України (схвалена розпорядженням Кабінету Міністрів України від 03.03.2021 № 167-р).
3. Міністерство освіти і науки України. Навчальна програма з інформатики для закладів загальної середньої освіти.
4. Міністерство цифрової трансформації України. Дія. Цифрова освіта: національна онлайн-платформа з розвитку цифрової грамотності.
5. Національний банк України. Матеріали з платіжної безпеки та фінансової грамотності.
6. Нова українська школа. Матеріали з медіаграмотності та кібербезпеки. – <https://nus.org.ua/>
7. Освітній проєкт «На Урок». Онлайн-курси та конкурси з інформаційної грамотності. – <https://naurok.com.ua/>