

Тема заняття: Інформаційна безпека

Мета:

1. Розповісти учням, що таке інформаційний простір та інформаційна війна і які небезпеки очікують їх в інформаційному просторі.
2. Навчити орієнтуватись у реаліях інформаційної війни.
3. Показати, як потрібно убезпечувати себе від ворожого впливу у соцмережах.
4. Поміркувати, якою може бути участь дитини чи підлітка в інформаційній війні

План заняття:

1. Вчитель формує поняття “інформаційний простір”, “інформаційна війна” та “інформаційна безпека”.
2. Учні засвоюють інформацію, чим небезпечний інформпростір сьогодні та як вберегтись від інформаційних атак (відео).
3. Вчитель та учні роблять висновки з побаченого та складають перелік правил поведінки на випадок інформаційної атаки.
4. Групова гра “Обережно, ворожа атака!”
5. Робота з власними профілями дітей у соцмережах.
6. Бесіда про те, як діти можуть допомогти в інформаційній війні.
7. Підведення підсумків заняття.

Хід заняття:

- 1. Вчитель формує поняття “інформаційний простір” та “інформаційна війна”.**

Визначення, які проєктуються, або записуються на дошці.

Інформаційний простір - це простір, у якому твориться, переміщується та засвоюється інформація.

Питання, які можна поставити учням:

- Ким твориться інформація?

- Звідки ми дізнаємось про створену людьми інформацію?
- За допомогою чого інформація переміщується?
- Що означає засвоєння інформації?

Пояснення вчителя:

Інформація створюється людьми. Вона переміщується в просторі і часі за допомогою носіїв інформації: книг, газет, журналів, сайтів, соцмереж, телебачення тощо. Інформація має найважливіший вплив на створення людиною власної картини світу. Коли ми, наприклад, засвоюємо інформацію про те, що наша планета рухається навколо Сонця, наша картина світу дещо змінюється.

Інформаційна війна - це агресивне втручання в інформаційний простір країни чи групи людей (аудиторії), з метою змінити картину світу людей так, як вигідно агресору.

Питання, які можна поставити учням:

- Хто веде інформаційну війну проти України?
- Які прояви цієї війни ви спостерігали?
- Чому інформаційна війна - це небезпечно, адже на ній нікого не вбивають?

Пояснення вчителя:

Інформаційна війна ведеться за аудиторію. Ви знаєте, що, наприклад, у відомих співаків, або гуртів є своя аудиторія. Хто це? Це - прихильники, люди, які відчують, думають так само, мають ту саму культуру. Якщо ти завоював аудиторію, то можеш спокійно заходити на її територію. Чому? Бо там живуть твої однодумці, вони не чинитимуть спротив. Як приклад - окупація російськими військами Криму. Там довгий час велась підступна інформаційна війна. І в результаті у росіян в Криму з'явилося багато прихильників. Так росія змогла майже без пострілів захопити нашу територію.

Інформаційна безпека - це стан захищеності суспільства і особистості від інформаційних загроз.

Пояснення вчителя:

В інформаційному просторі існує три типи загроз:

1) Особисті загрози:

- Ознайомлення з порнографічними матеріалами, ненормативною лексикою, інформацією суїцидального характеру, расистського, ненависницького чи сектантського змісту.
- Загроза отримання недостовірної чи неправдивої інформації.
- Формування залежності (ігрової, комп'ютерної, інтернет).
- Спілкування з небезпечними людьми (збоченці, шахраї, грифери).
- Залучення до виконання протиправних дій (хакерство, порушення прав та свобод інших).

2) Небезпека для інших людей:

- Поширення матеріалів, існування та використання яких може стати причиною посягання на безпеку оточуючих (наприклад, поширення інформації про створення вибухівки).
- Свідоме та несвідоме введення в оману інших.
- Вчинення протиправних дій, що тягнуть за собою відповідальність згідно з чинним законодавством.
- Кібербулінг – свідоме цькування та приниження, передусім однолітків.

3) Загрози витоку персональної інформації:

- Розголошення персональної та конфіденційної інформації (прізвища, імена, контакти, секретні дані кредитних карток, номери телефонів).
- Загроза зараження ПК вірусами різної категорії.
- Небезпека завантаження програм зі шкідливими функціями.

Під час війни небезпек в інформаційному просторі стає ще більше.

2. Учні засвоюють інформацію, чим небезпечний інформпростір сьогодні та як вберегтись від інформаційних атак (відео).

<https://www.youtube.com/watch?v=l9SKMWfzBoo>

3. Вчитель та учні роблять висновки з побаченого та складають перелік правил поведінки на випадок інформаційної атаки.

Питання, які можна поставити учням:

- Скільки соціальних мереж ви можете пригадати? У скількох ви присутні?
- З якою метою ви використовуєте соцмережу? Що ви знаєте про безпеку в мережі?
- Як ви вирішуєте, чи додавати до друзів якогось користувача чи ні?
- Як ви вважаєте, чи можна за постами у мережах скласти портрет людини, визначити його характеристики?

Завдання учням:

- Назвіть правила інформаційної безпеки вже відомі вам.

4. Групова гра “Обережно, ворожа атака!”

Хід гри:

Учнів об’єднують у групи, роздають по одній ситуації та пропонують виробити варіанти дій для таких випадків:

- Ви отримуєте SMS із незнайомого номера: “Привіт, це Аня, ми познайомились улітку. Пам’ятаєш мене?”
- Після уроку англійської мови з Тетяною Василівною на ваш телефон надходить повідомлення: “Привіт, це Марк. Ти зрозумів, що нам задала Тетяна Василівна?”
- Людина, на яку ви не підписані, надсилає вам таке повідомлення: “Привіт! Я просто в захваті від твоїх дописів, ти такий дотепний!!! Напиши мені свій номер телефону, я хочу з тобою поспілкуватися!”

- Якесь незнайома пише вам у чаті: “Я бачила тебе сьогодні на перерві. Ти дуже симпатичний!!! Де ти живеш? Я можу прийти до тебе в гості”.

Учні пропонують свої варіанти дій.

Вчитель підводить підсумки про важливість розуміння безпеки таких алгоритмів.

Ситуації з варіантами дій:

Ви отримуєте SMS із незнайомого номера: “Привіт, це Таня, ми познайомились у таборі. Пам’ятаєш мене?”

- 1) Заблокувати Таню. Якщо ви дійсно знайомі, то можете її образити. Блокуйте цю людину, тільки якщо цього літа ви точно не знайомилися ні з ким на ім’я Таня (або ж пам’ятаєте цю дівчинку, але просто не хочете з нею спілкуватися).
- 2) Проігнорувати Таню. Як уже говорилося вище, якщо ви не знаєте цю людину, можна просто нічого їй не відповідати.
- 3) “Привіт, Таню. Нагадай, будь ласка, як ми зустрілися”. Це безпечний варіант, якщо ви не впевнені, що робити.
- 4) “Привіт! Як справи? Я дуже рада, що ти мені написала!” Так можна відповідати, тільки якщо ви дійсно пам’ятаєте цю людину з літа.
- 5) “Ти ж та дівчинка з рудою косою?” Якщо ви не впевнені, що знаєте цю людину, можна спробувати розпитати її – можливо, тоді ви її пригадаєте.
- 6) “Я тебе не пам’ятаю, але можемо зустрітися”. Це дуже погана ідея. Ніколи не варто пропонувати незнайомій людині зустрітися.

Після уроку англійської мови з Мариною Василівною на ваш телефон надходить повідомлення: “Привіт, це Марк. Ти зрозумів, що нам задала Марина Василівна?”

- 1) Проігнорувати Марка. Як завжди – якщо ви не знаєте цю людину, можна їй не відповідати.
- 2) Заблокувати Марка. Якщо ви впевнені, що у вашому класі немає ніякого Марка, то варто зробити саме так.
- 3) “Привіт, Марку. Ти ж той новенький із задньої парти?” Якщо ви не впевнені, що знаєте цю людину, можна розпитати її детальніше.
- 4) “Звісно. Після школи поясню”. Так можна відповісти, тільки якщо ви впевнені, що знаєте цю людину.
- 5) “Я не в курсі, я з підгрупи Івана Павловича”. Якщо повідомлення цієї людини виглядає підозріло, краще просто проігнорувати його. І в жодному разі не слід повідомляти їй свою особисту інформацію, наприклад ім'я вашого вчителя англійської мови.
- 6) “Дзвони, поясню. Мій номер (012) 345-67-89”. Якщо ви не впевнені, що знаєте цю людину, повідомляти їй свою особисту інформацію – погана ідея

Людина, на яку ви не підписані, надсилає вам таке повідомлення: “Привіт! Я просто в захваті від твоїх дописів, ти такий дотепний!!! Напиши мені свій номер телефону, я хочу з тобою поспілкуватися!”

- 1) Проігнорувати користувача @nastusik122. Якщо ви не хочете відповідати цій людині, то можете просто промовчати.
- 2) Заблокувати користувача @nastusik122. Якщо ця людина видається вам підозрілою, можна просто заблокувати її, і тоді вона вам більше не писатиме.
- 3) “Привіт, ми знайомі?” Якщо ви не впевнені, що знаєте цю людину, розпитайте її, перш ніж надавати будь-які відомості про себе.
- 4) “Добре, ось мій номер...” Так робити не можна! Навіть якщо ви впевнені, що вам пишуть не з фіктивного профілю, ніколи не варто надсилати свою особисту інформацію через соціальні мережі. Зв'яжіться іншим способом: через батьків, учителів або через того, кому довіряєте

Якась незнайомка пише вам у чаті: “Я бачила тебе сьогодні на перерві. Ти дуже симпатичний!!! Де ти живеш? Я можу прийти до тебе в гості”.

- 1) Проігнорувати цю людину. Це розумний вибір.
- 2) Заблокувати цю людину. Якщо вона підозріла, блокуйте її без вагань.
- 3) “Ти хто?” Так робити не варто. Якщо повідомлення виглядає підозріло, краще просто не відповідати на нього чи взагалі заблокувати відправника.
- 4) “Це ти, Оксано? Ти теж мені дуже подобаєшся!!! Я живу на Шевченка , буд. 2”. Це дуже погана ідея, навіть якщо ви вважаєте, що знаєте відправника. Перш ніж давати комусь свою адресу або іншу особисту інформацію, обов’язково ретельно перевірте, хто ця людина.

5. Робота з власними профілями дітей у соцмережах.

Обговорення попередньої справи:

- Які підсумки учасники зробили після справи?
- Які б ще пункти ви хотіли додати до правил інформаційної безпеки після цієї гри?

Завдання:

- Перевірте власні налаштування соціальних мереж: хто може надсилати запит на дружбу? хто може бачити і коментувати ваші дописи?
- Перевірте своїх друзів і виявити ботів (профілі, створені для збирання інформації, провокацій, поширення різних меседжів).
- Подивіться список друзів у мережі і знайдіть того, кого ви ніколи не зустрічали й нічого не знаєте про нього.
- Відкрийте профіль незнайомця – подивіться коли цей користувач зареєстрований, чи є там реальні фото, чи є дописи

й коментарі, чи є інформація про користувача – про навчання, роботу, родичів, чи є спільні друзі.

6. Бесіда про те, як діти можуть допомогти в інформаційній війні.

Пояснення вчителя:

Діти дуже хочуть бути помічниками і щось робити для нашої спільної перемоги у війні. Проте, потрібно розуміти, що війна, в тому числі й інформаційна, - то справа дорослих. Тут, якщо діяти самому, можна дуже постраждати. Тому всі питання інформаційної безпеки й інформаційної боротьби треба узгоджувати з дорослими. Якщо ви пообіцяєте мені це зробити, я розповім, як можна воювати на інформаційному фронті.

- 1) Війна тут іде за аудиторію. Отже наша задача №1 - не стати аудиторією російських агентів. Як нею не стати? Ігнорувати!
- 2) У соціальних мережах є інструменти боротьби. Які вони? Правильно, це - скарга і бан. Отже, якщо ми бачимо, що канал, сторінка чи акаунт поширюють підозрілу інформацію, ми показуємо її батькам і разом скажимося і банимо.
- 3) Для найбільш просунутих користувачів є український Телеграм-канал СБУ, який видає списки, на кого поскаржитись і кого банити, який створений спеціально для молодих юзерів соцмереж. Але посилання на нього я дам лише тільки вашим батькам. З міркувань інформаційної безпеки.



7. Підведення підсумків заняття.

Учні заповнюють табличку:

Що нового я	Чого я більше не	Чого я
-------------	------------------	--------

дізнався/лась	буду робити?	навчився/лась
---------------	--------------	---------------