«Что такое кибертерроризм?»

Васильева Валентина Сергеевна

МБОУ школа – интернат № 13 г. Челябинска

27.11.2024 год

**Цель:** сформировать у обучающихся навыки безопасного поведения в Интернете, умение вовремя заметить активное вовлечение в экстремистские группы и сообщества, знание как себя вести в данной ситуации.

**Задачи**: дать определение кибертерроризма;

Разобрать способы вербовки в экстремистские киберорганизации;

Обсудить, что такое ктберпреступления и система наказаний за данные деяния;

Познакомить с правилами безопасного поведения в киберпространстве;

Научить правилам подбора безопасного пароля.

Примерное время занятия 45 – 50 минут.

**Вовлечение детей в кибертерроризм: кому выгодно и как этого избежать?**

Детей вербуют для рассылок о ложных минированиях недружественные России государства.

В стране фиксируются массовые рассылки заведомо ложных сообщений об актах терроризма в государственных и муниципальных учреждениях, в том числе образовательных организациях. Об этом сообщает пресс-служба киберполиции МВД России. Кроме того, выявлены факты вербовки гражданами недружественных России государств несовершеннолетних для участия в подобных преступлениях. Какую цель преследуют злоумышленники и как помочь ребенку не стать их жертвой.

Этот вопрос возник не сегодня. Вбросы информации о массовых ложных минированиях связаны еще с 2013 годом, до воссоединения Крыма с Россией, и с началом 2022 года, еще до начала специальной военной операции. Мы тогда выявили большую часть всех тех, кто занимался распространением подобной информации. Целью их является дестабилизация обстановки в стране.

Злоумышленникам нужны потрясения. Часть подобных киберпреступлений совершается школьниками, часть сотрудниками спецслужб. Также делаются рассылки от имени лиц, которые вообще не имеют отношения к этим сообщениям.

Подростки 12-17 лет еще не способны в полной мере критично оценивать информацию, определять ее достоверность. Они не могут противостоять психологической угрозе.

Подросткам обещают большие деньги, вывезти за рубеж, дать жилье и образование. Но ничего этого не будет. Мы очень много с этим сталкивались на допросах. Важно понимать, что любой диверсант, в том числе виртуальный, – это разменная монета. Никто не будет вас спасать, вам помогать. Обещанные деньги вам не дадут. Кураторы благополучно разделят их между собой. А все диверсанты всегда ловятся. И последствия для них самые суровые".

**Три типа информации в соцсетях, которую используют мошенники.**

В поисках жертв в интернете мошенники собирают о людях самые разные сведения, которые впоследствии используют для обмана и манипуляций. В этом смысле в число потенциально опасных откровений пользователей в сети входит три типа информации.

**Интересы** В этом случае получить ключ к жертве мошенники легко могут из постов о поездках и привычках, впечатлениях и планах.

"Вы выложили фотографию с лошадью – вам может написать мошенник и предложить покататься на лошади в два раза дешевле, и вы перейдете на фишинговый сайт. Вы рассказали, что любите ходить в кафе и рестораны, – вам придет фейковое предложение купить бонусную карту со скидкой 50%".

 Если люди делятся впечатлениями об отдыхе, продолжая находиться на курорте, то их публикация может заинтересовать не только мошенников, но и обыкновенных домушников.

**Документы**

Подобрать ключ к пользователю сети легко, если он размещает в интернете снимки каких-то своих документов. Это могут быть водительские права, фото новенького загранпаспорта, авиабилеты и прочее.

При этом главным объектом посягательств являются персональные данные граждан.

Всегда будет существовать опасность для наших граждан похищения их персональных данных. Может даже произойти подмена цифровой личности, например, на портале госуслуг. Такие случаи есть. И кредиты могут быть получены. (Персональные данные) – это то, что нужно очень бережно хранить.

Мошенники преследуют главную цель – монетизацию.

Их в любом случае будут интересовать те данные, которые позволят нас с вами однозначно идентифицировать. Именно эти данные позволяют защитить наши с вами материальные и конфиденциальные активы, сведения, составляющие медицинскую конфиденциальную информацию, сведения о вкладах и банковских картах".

**Коммерческая тайна.**

Если это российский производитель, конкуренты интересуются. Сюда надо добавить секреты производства".

Самым эффективным способом противодействия попыткам завладения информацией является грамотность в сфере информационной безопасности.

Важно понимать, что информационная безопасность существует не только в большом аэропорту и на заводе, она также существует в администрации маленького поселка городского типа или города, или в департаменте, и там эти процессы тоже происходят. Общая информационная грамотность очень важна.

В этом случае злоумышленники получают целый комплект психологических инструментов, которыми потом будут вас атаковать, говорит эксперт.

Молодые водители, особенно девушки, получив права, тут же начинают делать их фотографии на фоне автомобилей. Злоумышленники могут этим воспользоваться: самое простое – создать клон таких же прав. Или позвонить и представиться инспектором ГИБДД, который увидел нарушение и просит оплатить штраф.

**Фото детей**

Размещенные в сети фотографии детей для преступников – особый тип информации, которой они находят очень разное применение. И самое безобидное из них – охота за фото с целью собрать деньги на вымышленное лечение.

Идет особая охота злоумышленников за фотографиями с детьми, потому что их затем выставляют на разных ресурсах и собирают под них деньги, утверждая, что ребенок болен".

Пользователям социальных сетей рекомендуется закрывать свои аккаунты и предоставлять доступ к ним только друзьям.

Если вы стали жертвой киберпреступников, вы должны сообщить об этом в полицию. Даже если вам кажется, что это незначительное мошенничество, вполне вероятно, что вы поможете обезвредить профессиональную группу хакеров. В конце концов, борьба с киберпреступностью – это дело каждого.

**Кибертерроризм** — это вид терроризма, который использует компьютеры, средства связи и интернет для достижения своих целей.

**Кибертерроризм** — это комплексная акция, выражающаяся в преднамеренной, политически мотивированной атаке на информацию, обрабатываемую компьютером и компьютерными системами, создающей опасность для жизни или здоровья людей либо наступления других тяжких последствий.

 Такие действия осуществляют с целью нарушения общественной безопасности,

запугивания населения, провокации военного конфликта.

**Киберпреступления представляют собой** разнообразные незаконные действия, осуществляемые с использованием компьютерных технологий. Основные виды киберпреступлений включают:

**Фишинг –** вид интернет – мошенничества, цель которого – получить конфиденциальные данные пользователя.

**Кибер-вымогательство** – это преступление с требованием денег, имущества или иного действия в обмен на прекращение атаки.

**Аферы с кредитными картами**

**Вирусы и вредоносное ПО**

**Основные правила защиты от** **киберугроз**

1.**Не входите** на незнакомые сайты.

 2.Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть**, обязательно проверьте его на вирусы.**

3.Если пришло незнакомое вложение, ни в коем случае **не запускайте его**, а лучше сразу удалите и очистите корзину.

4.Никогда не посылайте никому свой **пароль.**

5. Старайтесь использовать для паролей **трудно запоминаемый набор цифр и букв.**

 6.При общении в Интернет не указывайте свои личные данные, **а используйте псевдоним (ник).**

 7.Ни в коем случае **не встречайтесь** с людьми, с которыми познакомились в сети Интернет.

8. Если в сети необходимо пройти регистрацию, то вы должны сделать ее так, чтобы в ней **не было указано** никакой личной информации.

 9.В настоящее время существует множество программ, которые производят **фильтрацию** содержимого сайтов.

10.Не всей той информации, которая размещена в сети Интернет, можно доверять.

**Приложение**

**А ЗНАЕТЕ ЛИ ВЫ?**

1. Необходимо ли использование антивирусных программ?

ДА

НЕТ, можно обойтись и без них

1. Использование сложных уникальных паролей для каждой службы – это безопасность личных данных?

ДА, они необходимы

НЕТ, они добавляют сложности при входе в приложения

1. Регулярное обновление программного обеспечения…

 ЭТО необходимость

ЭТО прихоть разработчиков и программистов, а мне не нужно

1. Ограничение личной информации в соцсетях: фотографии, имена и фамилии, родственные связи, места отдыха, домашний адрес, ваш банк, номер телефона — это безопасность?

ДА, я так и делаю

НЕТ, друзья не найдут меня

1. Вы отслеживаете информацию о нарушении безопасности ваших данных на сайтах, на которых вы зарегистрированы?

ДА, безусловно

НЕТ, мне это не нужно, сайты безопасны

1. Вы открываете письма на электронной почте, если не уверены в отправителе?

КОНЕЧНО, это безопасно

НЕТ, их открывать нельзя

1. Можно ли нажимать на кнопки, ссылки и баннеры, если не знаете, на какой ресурс они ведут?

МОЖНО, я всегда нажимаю

ЭТО опасно, я не нажимаю

1. Вы подключаетесь к сомнительному WiFi?

ДА, там бесплатный интернет

НЕТ, это небезопасно

1. Проверяете ли вы информацию, прежде чем в нее поверить? ДА. НЕТ.
2. Проверяете ли аккаунт пользователя, прежде чем добавлять его в друзья?

ДА. НЕТ.

**Основные правила защиты от киберугроз**

1.**Не входите** на незнакомые сайты.

 2.Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть**, обязательно проверьте его на вирусы.**

3.Если пришло незнакомое вложение, ни в коем случае **не запускайте его**, а лучше сразу удалите и очистите корзину.

4.Никогда не посылайте никому свой **пароль.**

5. Старайтесь использовать для паролей **трудно запоминаемый набор цифр и букв.**

 6.При общении в Интернет не указывать свои личные данные, **а использовать псевдоним (ник).**

 7.Ни в коем случае **не встречаться** с людьми, с которыми познакомились в сети Интернет.

8. Если в сети необходимо пройти регистрацию, то должны сделать ее так, чтобы в ней **не было указано** никакой личной информации.

 9.В настоящее время существует множество программ, которые производят **фильтрацию** содержимого сайтов.

10.Не всей той информации, которая размещена в сети Интернет, можно доверять.

 Какие пароли самые безопасные?

12345

123456

1234567890

яНикитаЯхороший!

12.12.2012ВАСЯ

ПАРОЛЬ

!»№;%:?\*

ЯТЕБЯЛЮБЛЮ

11111111

2Я3Ч4С5М6И7

12СА!13ША\*

Ф\*А!нт»АН

9(Ме)7%?4в5С

Составьте свой безопасный пароль

|  |
| --- |
|  |
|  |

|  |
| --- |
| **Киберпреступления** |
| **Фишинг** |
| **Кибер-вымогательство** |
| **Аферы с кредитными картами** |
| **Вирусы и вредоносное ПО** |
| **Киберугроза** |