МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РД
ГБПОУ РД «КОЛЛЕДЖ ЭКОНОМИКИ И ПРАВА»

ОТЧЕТ
о проведении классного часа
группы 29 ПСО 1
кл. руководитель - Шахбанова К.А.

«11» февраля 2021

КЛАССНЫЙ ЧАС
«Безопасность в сети Интернет»

Цель: знакомство с возможными угрозами в глобальной сети Интернет, правилами безопасной работы в сети.

Задачи:

образовательные:

- ✓ определить уровень знаний студентов о сервисах сети Интернет и возможных угрозах в сети;
- ✓ познакомить с правилами безопасной работы в сети Интернет;
- ✓ научить ориентироваться в информационном пространстве;

воспитательные:

- ✓ формировать ответственное отношение к работе в сети Интернет в режиме online;
- ✓ формировать информационную культуру обучащихся;

развивающие:

- ✓ развивать аналитическое, критическое мышление;
- ✓ развивать познавательный интерес к изучению компьютерных сетей.

Тип классного часа: беседа.

Оборудование: ПК базовой комплектации и проектор с экраном.

Программно-дидактическое обеспечение:

- ✓ Видеоролик о безопасности в сети Интернет,
- ✓ презентация «Безопасность в Интернете»;
- ✓ памятка по безопасности в сети Интернет.

Межпредметная связь: информатика, право, обществознание.

Общаясь в интернете, люди используют **вспомогательные слова, символы, смайлики.** Каждый вкладывает в них свое значение, которое может быть непонятным для других участников. Но с появлением новых on-line-возможностей увеличивается и количество угроз.

*Что же может случиться в реальной жизни через беззаботное виртуальное поведение ребенка?

*Слышали ли вы когда-нибудь о понятии «безопасный интернет»? *Учат ли вас родители on-line-этикету?

(Ответы учащихся.)

Классный руководитель.

7 февраля отмечается Международный день безопасного Интернета, он был учрежден в 2004 году и с тех пор вышел за пределы Европы, в этом году его будут отмечать более 70 стран, в том числе и Россия.

В этот день проводятся различные акции, тренинги, целью которых является информирование детей, их родителей и учителей об интернет-угрозах. Но главным остается обучение несовершеннолетних элементарным правилам безопасного поведения в интернете.

*Что такое «безопасный Интернет»?

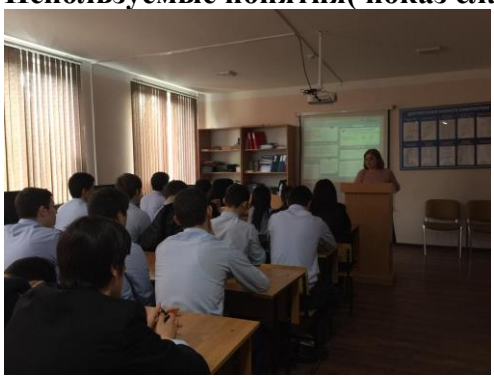
Учащиеся:

-Безопасный интернет-это «когда у тебя есть антивирус и ты качаешь все без вирусов».

- «Безопасный интернет» — это чтобы не «вычислили» тебя и какие-то данные о тебе. - «Безопасный интернет» подсказывает оставлять в сетях не очень точные данные — половину своих данных, половину не своих.

-Какая же опасность нас может подстерегать в интернете? Посмотрим видеоролик. Просмотр Видеоролика о безопасности в сети Интернет, подготовленный портала "Сетевичок" совместно с НП "Лига безопасного Интернета

Используемые понятия(показ слайдов)



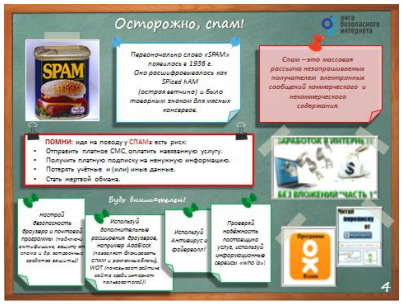
Интернет (англ.) - всемирная система объединенных компьютеров для хранения и передачи информации. Часто упоминается как Всемирная сеть и Глобальная сеть, а также просто Сеть.

Киберпространство (cyberspace) – это воображаемое пространство возможностей, создаваемое компьютерными системами, в частности Интернетом.

Кибербезопасность (cybersafety) – это состояние защищенности киберпространства;

Проблема интернет-зависимости выявилась с возрастанием популярности сети Интернет. Некоторые люди стали настолько увлекаться виртуальным пространством ,что начали предпочитать Интернет реальности, проводя за компьютером до 18 часов в день. Резкий отказ от Интернета вызывает у таких людей тревогу и эмоциональное возбуждение. Психиатры усматривают схожесть такой зависимости с чрезмерным увлечением азартными играми. Официально медицина пока не признала интернет-зависимость психическим расстройством, и многие эксперты в области психиатрии вообще сомневаются в существовании интернет-зависимости или отрицают вред от этого явления. Можно определить интернет-зависимость как нехимическую зависимость— навязчивую потребность в использовании Интернета, сопровождающуюся социальной дезадаптацией и выраженными психологическими симптомами.

Используемые понятия(показ слайдов)



Интернет (англ.) - всемирная система объединенных компьютеров для хранения и передачи информации. Часто упоминается как Всемирная сеть и Глобальная сеть, а также просто Сеть.

Киберпространство (cyberspace) – это воображаемое пространство возможностей, создаваемое компьютерными системами, в частности Интернетом.

Кибербезопасность (cybersafety) – это состояние защищенности киберпространства;

Наиболее используемые сервисы Интернет

- Веб-страницы. Поиск информации с помощью: Yandex, Google, Rambler и др.
- Файловые архивы: DC, Torrent, Rapid и др.
- Электронная почта
- Блог
- Веб-форум
- Чат
- Социальные сети.

Основные источники киберпреступлений по данным Роскомнадзор:

- принятие субъектом пользовательских соглашений по умолчанию
- использование "серых" мобильных приложений
- фишинг
- передача персональных данных по незащищенным каналам связи;
- использование геолокационных сервисов
- распространение своих персональных данных в открытых источниках;
- общение с незнакомыми людьми в соцсетях и др.

Что такое фишинг?

Фишинг это сетевой вид мошенничества, при котором технически подкованные мошенники выманивают у людей конфиденциальную информацию. Это делают при помощи спама, почтовых и мгновенных сообщений, вредоносных интернет-сайтов.

Главная задача фишинга — получение логина и пароля пользователя для определённого сайта, с дальнейшим их использованием. Это могут быть идентификационные данные вашего банковского кабинета или ПИН-код с номером карточки для вывода на свой счёт ваших денег. Часто фишинг используют для доступа к аккаунтам в соцсетях. В любом случае, когда ваш логин и пароль становятся известны жуликам, последствия для вас будут весьма удручающие.

Представим себе следующую ситуацию:

Например, вам на телефон поступил звонок:

Алло, это Магомедов Магомед Идрисович? – Да.

Вас приветствует сотрудник банка СБЕР Марина. Вы являетесь клиентом банка СБЕР? – Да.

Магомед Идрисович, с вашей карты был произведен перевод, вы подтверждаете перевод? – Нет.

Тогда нам надо отменить перевод, подскажите ваш номер карты и пароль к личному кабинету.

Как защититься от фишинга

При любых проблемах с банковской картой или счетом банк только блокирует карту или счет. И всё. Сотрудники банка не звонят по телефону с такими вопросами.

Помните, что пароль – только ваш, ни одна организация не станет требовать его от вас. Он необходим только для доступа к определённому сервису и только вы должны знать его.

Внимательно проверяйте каждое полученное почтовое сообщение с неизвестного адреса на предмет наличия всевозможных просьб перейти по ссылке.

Всегда проверяйте с помощью адресной строки, на том ли сайте вы вводите свои идентификационные данные. Обычно подделывается и домен, поэтому он бывает похожим на свой оригинал. Различие может заключаться лишь в одной букве (например, mail.ru легко превращается в meil.ru).

Используйте последние версии интернет-браузеров и лицензионные антивирусные программы.

При входе на банковские сайты следите за тем, чтобы было установлено защищённое соединение https.

Если вы подозреваете, что подверглись атаке фишеров, то сразу же поменяйте пароль своего аккаунта. После этого обратитесь в службу безопасности компании, данные от которой получили мошенники.

Социальные сети

Представим себе такую ситуацию. Магомед пришел устраиваться на работу (здесь сценка)

Магомед: Здравствуйте! Это отдел кадров?

Л.К.: Да, проходите.

Магомед: Я Исмаилов Магомед, пришел устраиваться на работу. Вот моё резюме.

Л.К.: Так, так. Окончили КЭиП г. Дербент. Средний бал 4.9. Хорошо. А вообще, чем увлекаетесь, в свободное время что делаете?

Магомед: нууу ммм.

Л.К.: Страница есть в социальных сетях?

Магомед: Да

Л.К.: Ну посмотрим…Спасибо, Магомед, что пришли к нам. Я вам перезвоню.

После сценки:

Информация о вас может повлиять сейчас и в будущем (репутация, работа).

Вы можете заинтересовать не только кибер, но и других преступников (воры).

Можно спровоцировать травлю себя со стороны пользователей сети.

Что делать?

- Ограничить список друзей.
- Не указывать пароли, телефон, адрес, дату рождения.
- Следить за репутацией.
- Настройки конфиденциальности аккаунта (только друзья или др.).
- Запросы в друзья только тех, кого знаете.
- Не размещать фото и видео с друзьями без их разрешения.
- Не открывать подозрительные ссылки.

Безопасность в публичных сетях

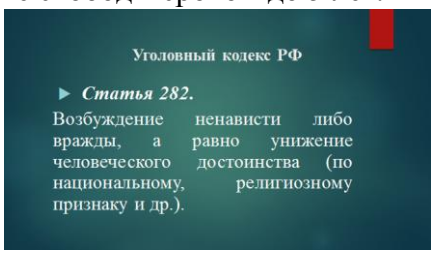
- Не передавать личную информацию через общедоступные сети WI-FI сети.
- Обновлять антивирус и брандмауэр.
- При использовании WI-FI отключить функцию «Общий доступ к файлам и принтерам».
- В мобильном телефоне отключить «Подключение к WI-FI автоматически».

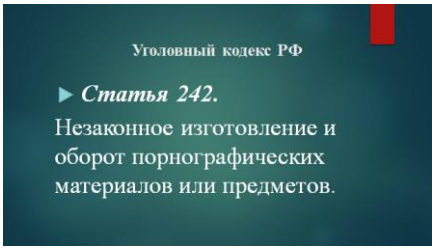
Защита беспроводной сети и маршрутизатора

- Не используйте пароль, установленный по умолчанию
- Не разрешайте беспроводному устройству сообщать о своем присутствии. Отключите вещание сетевого имени (SSID)
- Измените SSID устройства
- Шифруйте данные.
- Обязательно установите надежный антивирус на всех компьютерах и устройствах.

Уголовный кодекс РФ

предусматривает за нарушения в сфере информации, как денежные штрафы, так и лишение свободы сроком до 5 лет.





Статья 282. Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (по национальному, религиозному признаку и др.).

Статья 242. Незаконное изготовление и оборот порнографических материалов или предметов.

Статья 280. Публичные призывы к осуществлению экстремистской деятельности.

Экстреми́зм (от лат. extremus — крайний, чрезмерный) — приверженность крайним взглядам, методам действий. Провокация беспорядков, террористические акции, насильственное свержение власти.

Подведение итогов

Есть такая шутка: компьютер защищен на 100%, когда он находится в сейфе, сейф залит бетоном и находится в середине океана. Мы с вами сегодня уже не можем обойтись без компьютеров и интернета. Поэтому, если мы будем соблюдать рекомендации, которые были озвучены сегодня, это поможет нам минимизировать проблемы при использовании интернета на компьютере, смартфоне и любом устройстве. Надеюсь, что мероприятие было для вас полезным. Спасибо за внимание!