Министерство науки и образования РД
Государственное бюджетное профессиональное образовательное учреждение
«Колледж экономики и права»

Отчет

Классный час на тему:

«Всероссийский урок безопасности в сети ***Интернет***»

Составил: Алахвердиев Т.Д.

Куратор гр. 19ИСП 2 отделения: «Экономика, бухучет»

29.10.2021

Дербент 2021г.

Цель классного часа:

способствовать формированию знаний о правилах безопасного поведения в современной информационной среде, в частности - сети Интернет.

Задачи:

- **образовательные:** способствовать формированию общего представления о безопасной работе в сети Интернет, систематизации знаний в области использования Интернета;
- **развивающие:** способствовать развитию у обучающихся навыков безопасной работы в Интернете на основании имеющегося у них опыта; привитию навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде; формированию критического отношения к сообщениям и иной информации, распространяемой в сетях Интернет, мобильной (сотовой) связи, посредством иных электронных средств массовой коммуникации;
- **воспитательные:** способствовать воспитанию информационной культуры и толерантного общения при работе в сети Интернет; формированию у обучающихся информационной и коммуникативной компетенции.

Методы: словесный, проблемно - поисковый, наглядный.

«*Интернет несет читателю тонны мусора и крупинки золотого песка, и умение выбрать самое интересное и полезное становится весьма востребованным талантом*»
Марта Кетро

Ход классного часа

Вводное слово.

Здравствуйте, ребята! В настоящее время Интернет стал неотъемлемой частью повседневной жизни, бизнеса, политики, науки и образования. Развитие глобальной сети изменило наш привычный образ жизни, расширило

границы наших знаний и опыта. Интернет открывает перед нами широкие возможности, а это значит, что появилась возможность доступа к любой информации, хранящейся на миллионах компьютерах во всем мире. Но с другой стороны миллионы компьютеров получили доступ к вашему компьютеру. И этот доступ не всегда может быть «полезным». Как же сделать работу в глобальной сети безопасной? - это и есть главный вопрос нашего сегодняшнего мероприятия.

К сожалению, многие подростки и взрослые не очень хорошо представляют себе, какие опасности и неприятности может принести в их дом Интернет. С каждым годом количество преступлений, совершенных при помощи компьютеров возрастает.

Создан специальный отдел, который занимается преступлениями в сфере Интернет. Но в ходе расследования оказывается, что жертвы не соблюдали самых простых правил и пострадали по собственному незнанию.

Чтобы таких случаев становилось меньше, было принято решение каждый год проводить для обучающихся всей страны **единый всероссийский урок по безопасности в сети Интернет**. Мы с вами тоже подключаемся к этой акции. Итак, тема нашего сегодняшнего мероприятия *«Безопасность в сети Интернет».*

Куратор:

Мы живем в век информационных технологий, достаточно много времени проводим в сети в поисках информации, готовясь к занятиям, или просто отдыхая. Мы общаемся с друзьями, участвуем в дискуссиях, обсуждаем новости, оставляем комментарии, выкладываем фотографии. Очень важно научиться правильно вести себя в сети Интернет, знать правила безопасности и этичного поведения. Сегодня мы с вами об этом и поговорим.

20 шокирующих фактов о социальных сетях

1. Причиной каждого третьего в мире развода являются социальные сети.

2. Приблизительно пятнадцатью процентами пользователей социальные сети применяются для организации слежки. Это большей частью практикуется спецслужбами.

3. Среди пользователей соцсетей 37% публикуют в них малоинтересные сведения о собственной личной жизни.

4. Исследованиями установлено, что нахождение в соцсетях ведет к увеличению риска самоубийства, так как человек до минимума сводит свое общение с окружающими и отрешается от действительности.

5. В соответствии со статистикой количество преступлений на сексуальной почве, направленных на несовершеннолетних, выросло из-за соцсетей в 26 раз.

6. Ежегодно около 100 человек лишаются жизни из-за сообщения, оставленного в соцсетях, и эта цифра возрастает.

7. Социальные службы используют для вербовки своих агентов не только спецслужбы, но и различные группировки, в том числе террористической направленности.

8. Социальные сети сужают кругозор человека: он становится зависим от пустых и ненужных сообщений.

9. Чрезмерная увлеченность соцсетями, по данным исследований, ведет к снижению иммунитета, сердечно-сосудистым болезням и душевной дисгармонии. Активные, но не дающие развития мыслительные процессы наряду с малой подвижностью способствуют развитию заболеваний эндокринной системы.

10. В соцсетях знакомится каждая пятая семья в мире.

11. Средний пользователь посещает аккаунт дважды в день.

12. У среднего пользователя друзьями числится 195 человек.

13. К 2010 году доступ к соцсетям имело уже 96% населения всей планеты.

14. Наиболее активна Интернет-аудитория в России: средний пользователь проводит в нем 6,6 часов в неделю, просматривая 1307 Интернет-страниц.
30. 80% компаний мира подбирают сотрудников с помощью соцсетей.

15. У Бритни Спирс и Эштона Катчера фолловеров (*это **единомышленник, подписчик**. В переводе с английского (follow) означает «следующий, идущий за кем-то»)* столько же, сколько населения в Ирландии, Панаме или Норвегии.

16. Популярные соцсервисы продолжают хранить удаленные пользователями изображения.

17. По числу пользователей в мире лидирует Facebook – 1 миллиард.

18. В сети популярность социальных сетей по результатам проведенного опроса составила: Одноклассники - 73%, Вконтакте - 62%, Facebook - 18%, Twitter - 9%, Livejournal - 3%, LiveInternet - 2%. **И 1% респондентов не знает о сетях ничего.**

19. Еженедельно в социальных сетях дети проводят: от 7 до 14 часов – 23%, 14-21 час – 57% и больше 21 часа – 20%.

20. Каждый пятый ребенок из семи дней недели один тратит на соц. сеть [2].

Виртуальная реальность, как и любое пространство, несомненно, обладает и достоинствами и недостатками. Существование кибер-опасностей так же неоспоримо, как польза и удовольствие от использования Интернет-ресурсов. За безопасностью пользователей следят государственные структуры, а также и сотрудники Интернет сервисов, администраторы сайтов, модераторы. Однако ежедневно появляются новые жертвы, пострадавшие чаще всего из-за отсутствия грамотности в вопросах безопасности.

Угрозы в Сети.

1. Спам и фишинг

Спам — это электронный эквивалент бумажной рекламы, которую бросают в ваш почтовый ящик. Однако спам не просто надоедает и раздражает. Он опасен, особенно если является частью фишинга.

Во время чтения электронной почты или просмотра страниц в Интернете следует помнить про мошенников, которые стремятся похитить ваши личные данные или деньги, а, как правило, и то, и другое. Такие мошеннические действия или схемы называются *«фишингом»* (от английского слова «fish», что означает «рыба» или «рыбачить»), так как их цель – «выудить» у вас ваши персональные данные.

Спам в огромных количествах рассылается по электронной почте спамерами и киберпреступниками. Как защитить себя от спама и фишинга?

Советы от команды экспертов «Лаборатории Касперского»

- **Заведите себе несколько адресов электронной почты.**
  Лучше всего иметь по крайней мере два адреса электронной почты.
  - **Личный адрес электронной почты.**
    Этот адрес должен использоваться только для личной корреспонденции.
  - **«Публичный» электронный адрес.**
    Используйте этот электронный адрес для регистрации на общедоступных форумах и в чатах, а также для подписки на почтовую рассылку и другие интернет-услуги.

- **Никогда не отвечайте на спам**.
- **Подумайте, прежде чем пройти по ссылке «Отказаться от подписки».**
- **Своевременно обновляйте браузер** [3].

2. **<u>Грубость в интернете.</u> Как не испортить себе настроение при общении в сети и не опуститься до уровня «веб-агрессора**

Существует в Интернете особая категория пользователей, с которой лучше никогда не встречаться. Это так называемые сетевые хамы и форумные тролли, развлекающиеся провокациями своих собеседников в Интернете.

Зачем они это делают? Чтобы получить удовольствие от негативной реакции других людей. Такие пользователи преднамеренно идут на конфликт и доводят собеседника до нервного срыва, который может выплеснуться в онлайн. Чаще всего этим занимаются люди с комплексами неполноценности, которых обижают в реальной жизни – и потому они пытаются отыграться в Интернете. Анонимность в Сети позволяет им представлять себя совершенно другими и – главное – быть уверенными в своей безнаказанности, поэтому они пишут и делают такие вещи, которые в реальной жизни никогда бы не рискнули сотворить в присутствии оппонента. По причине как неизвестности, так и недосягаемости, «травить», оскорблять и провоцировать людей, кажется им забавным занятием. Как показывает практика, больше половины сетевых грубиянов являются детьми, скучающими в Интернете или не ладящими со сверстниками. Однако случаются и вполне взрослые профессиональные Интернет-скандалисты, для которых довести виртуального собеседника является своего рода искусством. Встретить сетевых хамов можно в любом уголке Интернета: в чатах, в аське, в социальных сетях, на сайтах знакомств, на форумах и по электронной почте.

Необходимо уметь отличать их от нормальных собеседников, дабы не тратить время и нервы впустую. Если вы замечаете, что вам грубят, провоцируют на ссору или намеренно злят, самым верным решением будет немедленно закончить разговор или игнорировать сообщения данного пользователя на форуме/сайте. Не доставить грубияну удовольствия видеть ваш гнев или обиду будет лучшим наказанием для него, ибо его цель не достигнута.

Психологи утверждают, что агрессия другого человека - это просьба о любви. Возможно, этому человеку не хватает друзей, теплых

отношений, быть может он одинок, или у него неприятности. Будьте внимательны, не торопитесь отвечать на грубость.

3. Кибер-буллинг.

Кибер-буллинг (cyber-bullying), подростковый виртуальный террор, получил свое название от английского слова bull — бык, с родственными значениями: агрессивно нападать, бередить, задирать, придираться, провоцировать, донимать, терроризировать, травить. В молодежном сленге является глагол аналогичного происхождения — быковать.

Итак, **кибер-буллинг** — это нападения с целью нанесения психологического вреда, которые осуществляются через электронную почту, сервисы мгновенных сообщений, в чатах, социальных сетях, на web-сайтах, а также посредством мобильной связи. Такое многократно повторяемое агрессивное поведение имеет целью навредить человеку и базируется на дисбалансе власти (физической силы, социального статуса в группе. Кибер-буллинг включает целый спектр форм поведения, на минимальном полюсе которого — шутки, которые не воспринимаются всерьез, на радикальном же — психологический виртуальный террор, который наносит непоправимый вред, приводит к суицидам и смерти. Есть также понятие буллицида — гибели жертвы вследствие буллинга.

Исследователи выделили **восемь основных типов буллинга:**

1. **Перепалки, или флейминг** — обмен короткими эмоциональными репликами между двумя и более людьми, разворачивается обычно в публичных местах Сети. Иногда превращается в затяжной конфликт (holywar — священная война). На первый взгляд, флейминг — борьба между равными, но при определенных условиях она может превратиться в неравноправный психологический террор. Неожиданный выпад может вызвать у жертвы сильные эмоциональные переживания.
2. **Нападки**, постоянные изнурительные атаки (harassment) — повторяющиеся оскорбительные сообщения, направленные на жертву
3. **Клевета** (denigration) — распространение оскорбительной и неправдивой информации.
4. **Самозванство**, перевоплощение в определенное лицо— преследователь позиционирует себя как жертву, используя ее пароль доступа к аккаунту в социальных сетях, ведет переписку.
5. **Надувательство**, выманивание конфиденциальной информации и ее распространение— получение персональной информации и публикация ее в интернете или передача тем, кому она не предназначалась.

6. **Отчуждение** (остракизм, изоляция). Любому человеку присуще желание быть включенным в группу. Исключение же из группы воспринимается как социальная смерть.
7. **Киберпреследование** — скрытое выслеживание жертвы с целью организации нападения, избиения, изнасилования и т.д.
8. **Хеппислепинг** (Happy Slapping — счастливое хлопанье, радостное избиение) — название происходит от случаев в английском метро, где подростки избивали прохожих, тогда как другие записывали это на камеру мобильного телефона. Сейчас это название закрепилось за любыми видеороликами с записями реальных сцен насилия.
Различия кибербуллинга от традиционного реального обусловлены особенностями интернет-среды: анонимностью, возможностью фальсификации, наличием огромной аудитории, возможностью достать жертву в любом месте и в любое время.

Несколько советов, для преодоления этой проблемы:
1. **Не спеши выбрасывать свой негатив в кибер-пространство**.
2. **Создавай собственную онлайн-репутацию, не покупайся на иллюзию анонимности**.
3. **Храни подтверждения фактов нападений**.
4. **Игнорируй единичный негатив**
5. **Блокируй агрессоров**.
6. **Не стоит реагировать на агрессивные сообщения** [4].

4. Интернет-зависимость.

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.

По данным различных исследований, интернет-зависимыми сегодня являются около 10 % пользователей во всём мире. Российские психиатры считают, что сейчас в нашей стране таковых 4—6%. Несмотря на отсутствие официального признания проблемы, интернет-зависимость уже принимается

в расчёт во многих странах мира. Например, в Финляндии молодым людям с интернет-зависимостью предоставляют отсрочку от армии.

Основные 5 типов интернет-зависимости таковы:

1. Навязчивый веб-серфинг— бесконечные путешествия по Всемирной паутине, поиск информации.
2. Пристрастие к виртуальному общению и виртуальным знакомствам— большие объёмы переписки, постоянное участие в чатах, веб- форумах, избыточность знакомых и друзей в Сети.
3. Игровая зависимость — навязчивое увлечение компьютерными играми по сети.
4. Навязчивая финансовая потребность— игра по сети в азартные игры, ненужные покупки в интернет-магазинах или постоянные участия в интернет-аукционах [5].

Самый простой и доступный способ решения зависимости — это приобретение другой зависимости. Любовь к здоровому образу жизни, общение с живой природой, путешествия по родному краю, творческие прикладные увлечения, занятия спортом, как правило, выводят человека из зависимости.

Пять советов, которые помогут обеспечить безопасность в Интернете (от Центра безопасности компании Microsoft)

1. **Защитите свой компьютер**

Постоянно обновляйте все программное обеспечение (включая веб-браузер)
Установите законное антивирусное программное обеспечение
Брандмауэр должен быть всегда включен.
Установите на беспроводном маршрутизаторе защиту с помощью пароля.
Всегда проверяйте флеш-накопители (или USB-накопители)
Не переходите по ссылкам и не нажимайте кнопки во всплывающих сообщениях, которые кажутся подозрительными.

1. **Обеспечьте защиту секретной личной информации**

Прежде чем вводить секретные сведения в веб-форме или на веб-странице, обратите внимание на наличие таких признаков, как адрес веб-страницы, начинающийся с префикса https и значка в виде закрытого замка ( ) рядом с адресной строкой, который обозначает безопасное соединение.
Никогда не отвечайте на просьбы прислать деньги от «членов семьи», на сообщения о розыгрышах лотереи, в которых вы не участвовали, или другие мошеннические сообщения.

1. **Используйте надежные пароли и храните их в секрете.**

Придумайте пароли, представляющие собой длинные фразы или предложения и содержащие сочетание строчных, прописных букв, цифр и символов. Используйте на разных сайтах разные пароли.

1. **Позаботьтесь о своей безопасности и репутации в Интернете**

Узнайте, какая информация о вас существует в Интернете, а также периодически производите оценку найденных сведений. Создавайте себе положительную репутацию.

1. **Более безопасное использование социальных сетей**

Никогда не публикуйте информацию, которую вы не хотели бы видеть на доске объявлений. Периодически анализируйте, кто имеет доступ к вашим страницам, а также просматривайте информацию, которую эти пользователи публикуют о вас. Настройте список пользователей, которые могут просматривать ваш профиль или фотографии. Подходите избирательно к предложениям дружбы [6].

Тест

1. **Ваши друзья говорят, что вы рассылаете им спам-сообщения. Что будете делать?**
   a. Сменю пароль к аккаунту в социальной сети. *
   b. Ничего не буду делать, такое бывает и потом само проходит.
   c. Подумаю, что друзья просто шутят
2. **Вам пришло письмо: «Чтобы выиграть миллион в нашей лотерее, вам нужно зарегистрироваться на этом сайте (ссылка на сайт). Регистрация закрывается завтра. Не пропустите!». Что вы сделаете?**
   a. Зайду на сайт и посмотрю, что за лотерея.
   b. Напишу в ответ письмо, где попрошу прислать подробности о лотерее.
   c. Удалю письмо, я ничего не знаю об этом сайте и авторе письма. *

3. **Какую информацию в Интернете можно выкладывать в открытом доступе?**

   a. Номер телефона
   b. Хобби, увлечение *
   c. Информацию о родственниках

4. **Ваш друг в социальной сети прислал вам файл и сообщение: «Привет! В этом файле наши с тобой фотки с дня рождения. Смотри!». Но вы не были с ним на дне рождении. Как вы поступите?**

   a. Открою файл и посмотрю фотографии.
   b. Прежде чем открыть файл, зайду в социальную сеть и спрошу у друга, что это за фотки.
   c. Позвоню другу, чтобы выяснить, не взломан ли его аккаунт. *

5. **Вам пришло письмо: «Добрый день! Мы предлагаем вам учиться за рубежом! Обучение, проживание, перелет — за наш счет. Нужно только оплатить пересылку документов — 1500 рублей. Не упустите свой шанс!». В письме есть реквизиты. Как вы поступите?**

   a. я не против бесплатно слетать в за границу
   b. уточню, нет ли у них программы обучения в Китае.
   c. удалю письмо, оно выглядит подозрительно. *

6. **Что в Интернете запрещено законом?**

   a. размещать информацию о себе
   b. размещать информацию других без их согласия *
   c. копировать файлы для личного использования

7. **Какой пароль является самым сложным?**

   a. Natalia1993
   b. Mar!nA_1993 *

c. veronica1093

8. Когда можно доверять письму от неизвестного отправителя?

a. Отправитель использует официальный логотип
b. Отправитель обращается к вам по имени отчеству
c. Никогда нельзя доверять письму от неизвестного отправителя *

9. Что такое брутфорс?

a. Подбор пароля*
b. Подбор секретного кода
c. Подбор ответа на контрольный вопрос

10. ВКонтакте вдруг просят повторно ввести ваши логин и пароль, чего раньше никогда не было. Что вы сделаете?

a. Введу, раз нужно.
b. Проверю доменный адрес сайта. Если он не совпадает с настоящим, закрою сайт.
c. Введу, так как мой аккаунт привязан к мобильному номеру, а значит, защищен от любого мошенничества.

11. Если компьютер работает в нормальном режиме, означает ли это, что он не заражен?

a. Да
b. Если антивирус ничего не показывает, компьютер чист
c. Нет *

12. Межсетевой экран (firewall)- это…

a. Устройство, кеширующее сетевой трафик
b. Устройство, считывающее сетевой трафик
c. Устройство блокирующее сетевой трафик, за исключением разрешенных данных*

13. Какой интернет-протокол обеспечивает безопасный просмотр сайтов (первые буквы в адресной строке браузера)

a. http://
b. https://*
c. ftp://

14. Что такое аутентификация?

a. Это предоставление легальным пользователям прав доступа к ресурсам системы
b. Это присвоение субъектам и объектам доступа уникального номера, шифра, кода и т.п. с целью получения доступа к информации
c. Это проверка подлинности пользователя по предъявленному им идентификатору.*

15. Скрытое перенаправление пользователей на поддельные сайты, осуществляемое с помощью внедренного вредоносного вируса или инфицирования целого сервера DNS

a. фарминг *
b. кардинг
c. фишинг

Спасибо.

Использованные Интернет-ресурсы.

1. http://nick-name.ru/about/
2. http://smonews.ru/48-shocking-facts
3. http://www.kaspersky.ru/internet-security-center/threats/spam-phishing
4. http://psyfactor.org/lib/cyber-bullying.htm
5. http://www.nvppl.ru/show_dict_812.htm
6. http://www.microsoft.com/ru-ru/security/default.aspx
7. http://www.saferunet.ru/teenager/
8. http://liubavyshka.ru/

Памятка
по безопасному поведению в Интернете

- ✓ Никогда не сообщайте свои имя, номер телефона, адрес проживания или учебы, пароли или номера кредитных карт, любимые места отдыха или проведения досуга.
- ✓ Используйте нейтральное экранное имя, не выдающее никаких личных сведений.
- ✓ Защитите свой компьютер.
- ✓ Используйте надежные пароли и храните их в секрете.
- ✓ Используйте фильтры электронной почты для блокирования спама и нежелательных сообщений.
- ✓ Не допускайте грубости в интернете, блокируйте веб-агрессоров.
- ✓ Не добавляйте незнакомых людей в свои контакты
- ✓ Помните, что виртуальные знакомые могут быть не теми, за кого себя выдают.
- ✓ Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернете.
- ✓ Прекращайте любые контакты по электронной почте, в системе обмена мгновенными сообщениями или в чатах, если кто-нибудь начинает задавать вам вопросы личного характера или содержащие сексуальные намеки.