**МКОУ БГО Губаревская СОШ**

**Внеклассное мероприятие**

**Безопасный интернет**

**Подготовил: учитель**

**Подгузова Л.М.**

**2021 год**

Я в плену у Интернета,  
Тает время, часть бюджета.  
Да и дома меня нет,  
Как войду я в Интернет.  
Я тащусь от Интернета:  
В нём палитра всего света  
Собрана от «А» до «Я».  
Там Вселенская семья!  
В Интернете я как в сказке;  
Рассуждай, живи с подсказкой.  
Заводи друзей, подруг.  
Это лучший в мире – друг!  
Интернет - «Зеркалье» века.  
Новый мир для Человека,  
Его мозг и почти «Клон».  
Всем Творцам от нас поклон

**Цель**: обеспечение информационной безопасности, повышение грамотности учащихся в вопросах безопасности в сети, формировать общепринятые нормы поведения в сети.

**Задачи:**

* Ознакомить учащихся с потенциальными угрозами, которые могут встретиться при работе в сети Интернет.
* Выработать правила безопасного поведения в сети.
* обучить учащихся правилам ответственного и безопасного пользования услугами Интернет и мобильной (сотовой) связи, в том числе способам защиты от противоправных и иных общественно опасных посягательств в информационно-телекоммуникационных сетях, в частности, от таких способов разрушительного воздействия на психику детей, как кибербуллинг (жестокое обращение с детьми в виртуальной среде) и буллицид (доведение до самоубийства путем психологического насилия);

**Техническое и программное обеспечение урока*:*** компьютер, мультимедийный проектор, программа «MSPowerPoint»

**Материалы к уроку:** видеоматериалы «Защита от вредоносных программ», рабочие лист, анкета.

**Ход урока:**

На первый взгляд может показаться, что появление интернета принесло одни плюсы. И действительно, благодаря интернету людям стало проще искать нужную информацию. Если раньше школьникам и студентам приходилось тратить часы на то, чтобы отправиться в библиотеку, найти нужную книжку, изучить ее и выбрать интересующую информацию, то сейчас этот процесс не доставляет никаких неудобств. Включил компьютер, ввел в поисковике интересующий вопрос и через секунду на странице появятся сотни ссылок и огромное количество информации. Но сразу, хочется отметить, что не стоит верить всему, что пишут в интернете и далеко не все ссылки наполнены достоверными фактами. Нужно быть очень внимательным и проверять источники. Очень часто информация в интернете является ложной и ее использование приводит к неприятным последствиям.

А что такое Интернет? Каково его происхождение?

Давайте заслушаем информацию об истории развития, появления сети Интернет.

**Ученик.**Если говорить не о прообразах интернета, а о полноценной сети, то формирование более-менее приемлемой пропускной способности, объединение множества различных сетей и связь через модемные линии приходится 90-ые годы 20 века. Именно тогда начали возникать веб-сайты. Более конкретная дата - 1995 года, время появления интернет-провайдеров. К 19997 году интернет объединял 10 млн. компьютеров и было зарегистрировано более миллиона доменных имён. 50-еы годы 20 века. Начало разработки первых компьютеров и зарождение концепции единой глобальной сети в США, Великобритании и Франции.  
2) 60-ые и 70-ые годы 20 века. Разработки различных протоколов передачи данных и возникновения обособленных сетей - ARPANET, NPL, Telenet, CYCLADES и др.  
6) 2000-ые годы 21 век. Формируется коммерческая часть интернета. Возникают поисковые системы. [Эволюционируют ЭВМ в ПК](https://www.tehpodderzka.ru/2019/03/blog-post_13.html), появляются различные операционные системы. Стремительно развиваются серверные технологии, строятся дата-центры. Растет число сайтов по всему миру.

Перед проведением мероприятия в классе прошло анкетирование

**Анкета для учащихся**

***Безопасность и Интернет***

1. Есть ли у тебя компьютер?

*а) да б) нет*

2. Как часто ты занимаешься за компьютером?

*а) каждый день б) один раз в неделю в) другое (напиши свой ответ) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

3. Если занимаешься, то сколько времени ты проводишь за компьютером в день?

*а) один час б) два часа в) другое (напиши свой ответ) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

4. Подключен твой компьютер к Интернету?

*а) да б) нет*

5. Ты выходишь в Интернет

*а) самостоятельно б) самостоятельно, но под контролем родителей в) вместе с родителями*

6. Стоит ли на твоем компьютере Фильтр (запрет на посещение нежелательных и опасных сайтов)?

*а) да б) нет*

7. Есть ли у тебя мобильный телефон?

*а) да б) нет*

8. Подключен ли твой мобильный телефон к Интернету?

*а) да б) нет*

9. Подключен ли твой мобильный телефон к безопасному (детскому) Интернету ?

*а) да б) нет*

10. В каких целях ты используешь Интернет?

*а) поиск информации б) общение с друзьями в) игры г) другое (напиши свой ответ)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

11. Знаешь ли ты какие сайты таят опасность?

*а) да б) нет*

12. Сколько тебе лет?

*а) до 10 лет б) 10-12 лет в) 13-14 лет г) старше 14 лет*

По итогам анкетирования были проведены дебаты

**Условия проведения дебатов.**Учащиеся делятся на группы «За» и «Против». Первая группа собирала информацию и будет анализировать полезные стороны использования Интернета Вторая группа- отрицательные, негативные.

**По итогам дебатов составили**

1. памятку правила Безопасного поведения в сети Интернет
2. Заполнили рабочий листа «Плюсы и минусы сети Интернет»

.

**Просмотр видеоролика. Обсуждение.**

1. Какую роль в жизни современного человека играет Интернет.
2. С какой целью мы посещаем интернет?
3. Сколько времени в целом человек проводит в сети?

Учитель. Используя данные анкетирования и статистические данные т ой же сети Интернет мы составили перечень наиболее опасных угроз.

* **Первая опасность, которая нас подстерегает- это Интернет- зависимость.**

**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 13 % пользователей во всём мире. Российские психиатры считают, что сейчас в нашей стране таковых 13%. 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.

**Технические угрозы**

Основными техническими угрозами для пользователей являются вредоносные программы, ботнеты и иDoS и DDoS-атаки.

**Угроза**– это потенциально возможное событие, действие, которое посредством воздействия на объект защиты может привести к нанесению ущерба.

**Вредоносные программы**

Цель вредоносных программ – причинить ущерб компьютеру, серверу или компьютерной сети. Они могут, например, испортить, украсть или стереть данные, хранящиеся на компьютере, замедлить или полностью остановить работу устройства. Вредоносные программы часто «прячутся» в письмах и сообщениях с заманчивыми предложениями от неизвестных лиц и компаний, в страницах новостных сайтов или других популярных ресурсах, которые содержат уязвимости. Пользователи заходят на эти сайты, и вредоносные программы незаметно проникают на компьютер.

Также вредоносные программы распространяются через электронную почту, съемные носители информации или скачанные из Интернета файлы. Файлы или ссылки, присланные по электронной почте, могут подвергать устройство заражению.

Вредоносные программы могут скрываться и под видом звуковых или графических сообщений. Например, красивая экранная заставка, которой с удовольствием любуется пользователь, может оказаться троянской программой (что это такое, читайте ниже). Ссылки, которые появляются во всплывающих окнах и в рекламных объявлениях на различных сайтах, также могут содержать вирусы.

К вредоносным программам относятся вирусы, черви, троянские программы.

**Вирус** – разновидность компьютерной программы, отличительной особенностью которой является способность к размножению (саморепликации) и незаметному для пользователя внедрению в файлы, загрузочные секторы дисков и документы. Название «вирус» по отношению к компьютерным программам пришло из биологии именно по признаку способности к саморазмножению. Лежащий в виде зараженного файла на диске вирус не опасен до тех пор, пока его не открыть или не запустить. Он начинает действовать только тогда, когда пользователь его активирует. Вирусы разработаны, чтобы копировать себя, заражая компьютеры, при этом обычно они уничтожают файлы.

**Черви** – это разновидность вирусов. Они полностью оправдывают свое название, поскольку распространяются путем «переползания» из устройства в устройство. Так же, как и вирусы, они представляют собой саморазмножающиеся программы, но в отличие от вирусов, червю не нужна помощь пользователя, чтобы распространиться. Он сам находит лазейку.

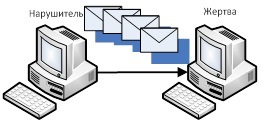
**Троянские программы** – вредоносные программы, которые целенаправленно внедряются злоумышленниками для сбора информации, ее разрушения или модификации, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях. Внешне троянские программы выглядят как легальные программные продукты и не вызывают подозрений. В отличие от вирусов, они полностью готовы к выполнению своих функций. На это и делается расчет злоумышленников: их задача – сделать такую программу, которую пользователи не побоятся запускать и использовать.

Злоумышленники могут заражать компьютер, чтобы сделать его частью   **ботнета**– сети из зараженных устройств, расположенных по всему миру. Крупные ботнеты могут включать в себя десятки и сотни тысяч компьютеров. Пользователи часто даже не догадываются, что их компьютеры заражены вредоносными программами и используются злоумышленниками. Ботнеты создаются путем рассылки разными способами вредоносных программ, а зараженные машины в дальнейшем регулярно получают команды от администратора ботнета, так что оказывается возможным организовать согласованные действия компьютеров-ботов по атаке других устройств и ресурсов.

**DoS и DDoS атаки**

DoS-атака (отказ в обслуживании) – это атака, приводящая к парализации работы сервера или персонального компьютера вследствие огромного количества запросов, с высокой скоростью поступающих на атакуемый ресурс.

Суть DoS-атаки заключается в том, что злоумышленник пытается сделать временно недоступным конкретный сервер, перегрузить сеть, процессор или переполнить диск. Цель атаки – просто вывести компьютер из строя, а не получить информацию, захватить все ресурсы компьютера-жертвы, чтобы другие пользователи не имели к ним доступа. К ресурсам относятся: память, процессорное время, дисковое пространство, сетевые ресурсы и т. д.



* Следующая опасность **Опасные группы в социальных сетях.**

Опасные группы в социальных сетях В соцсетях ВК и в Инстаграмм появляются хештеги. Хэштеги — это ссылки, нажав на которые попадаешь на определенную страничку в соцсетях. Такие хэштеги — это уже повод для серьезного беспокойства. Ребенок, кликая на ссылки, попадает в опасную группу. Здесь с ним связывается «куратор». Он дает задания и проверяет, готов ли ребенок «играть». Ведется переписка. Ребенок, кликая на ссылки, попадает в опасную группу. Здесь с ним связывается «куратор». Он дает задания и проверяет, готов ли ребенок «играть». Ведется переписка. Куратор выясняет психологическое состояние ребенка, узнает, где он проживает. И дает задания Дети выполняют задания, наносят себе увечья, делают метки на руках лезвием.

Как распознать опасные группы? У каждой группы есть свой знак, логотип. Это или символика богов, изображения ножей, лезвий, крови. Также присутствуют фотографии в черных, серых и красных тонах. Также в группе может присутствовать соответствующая музыка, которая погружает в транс и депрессию. Если подросток находится в таком состоянии, им легко управлять.

***Положительные стороны сети Интернет***

**Обучение.** Интернет используют как поддержку для получения образования. В нем можно найти обучающую информацию и программы, а также ответ на любой вопрос.Можно научиться ремонтировать разного рода технику, играть на музыкальных инструментах, делать разные поделки, используя самоучитель

**Интернет – это средство информации и информационных ресурсов.** Он имеет очень большое количество возможностей, которые в наше время широко используются. Например, поиск информации. С помощью интернета можно найти любого рода информацию. Для этого используют поисковые машины (поисковики). Эта система позволяет найти, например, любой товар и его цены по всему миру, поставщиков и рынки сбыта, узнать прогноз погоды и почитать новости. Можно также посмотреть с помощью специальных программ на любой уголок земли.  
**Получение информации**. Скачать с интернета и перенести себе на компьютер можно различную информацию: любимую музыку, фильмы, игры, программы. Информацию большого объема нужно сначала закачать на свой компьютер, а затем с помощью специальных программ открывать.

**Развлечение**. Набрав в поисковой системе слово «игры», откроются ссылки с огромным выбором развлекательных ресурсов. Найти также можно огромное количество интересных фотографий. Художники и писатели выкладывают свои работы на специальных форумах.

**Общение.** Интернет – это средство коммуникации. С помощью социальных сетей, электронной почты, форумов можно общаться со всем миром. Эта система позволяет получать письма с другого конца земли в течение нескольких минут. Так же это практически единственная возможность общения для людей с ограничениями в здоровье.

**Заработок в интернете.** Зарабатывать деньги можно с помощью сети, например, вкладывая денежные средства в биржи, также рекламируется различный заработок в сети. Что продавать и на чем заработать? Проследить за интересами и нуждами пользователей можно, благодаря зафиксированным последним запросам поисковиков. Но к заработку в интернете нужно относиться очень осторожно, так как сегодня встречается множество мошенников. Существует большое количество коммерческих сайтов. За содержание такого рода сайта нужно платить деньги, поэтому большинство их направлены на получение прибыли (продажа, оказание услуг, размещение рекламы).

**Учитель**: Как сделать работу в сети безопасной?

**Ученик. Защита информации. Способы.**

В эпоху информационных технологий остро стоит вопрос о том, как защитить данные на компьютере. Пароли и логины от социальных сетей, банковских систем управления счетами, данные учетной записи, приватные фото и другие файлы – все это может заинтересовать злоумышленников.  
Чтобы не стать жертвой хакеров, необходимо уделять внимание безопасности хранения персональных данных. Как можно защитить личную информацию на компьютере, расскажет эта статья.

**Способ 1: надежные пароли**

Самый простой способ защитить данные на компьютере – это использование надежных паролей. О том, что специалисты по безопасности не рекомендуют использовать в качестве ключа простые комбинации цифр и букв (qwerty, 12345, 00000), известно большинству пользователей. Если злоумышленник знает потенциальную жертву лично, нетипичный, но простой ключ (дата рождения, адрес, имя домашнего питомца) тоже подбирается с легкостью.  
**Способ 2: шифрование данных**

Чтобы защитить личную информацию на компьютере в случае предприятия злоумышленником попытки доступа к нему, рекомендуется применять шифрование данных. Корпоративные и профессиональные версии Windows оснащаются инструментом BitLocker. Системный механизм позволяет зашифровать информацию на одном или нескольких разделах жесткого диска. Доступ к файлам становится возможным только при использовании специального ключа.  
**Способ 3: использование антивирусной программы**

Для получения доступа к чужому ПК взломщики используют вспомогательное программное обеспечение, устанавливаемое на компьютер жертвы. Вирусы-трояны занимаются перехватом информации, вводимой с клавиатуры, подменяют сайты копиями, созданными мошенниками, занимаются пересылкой личных данных. Чтобы защитить личные данные, желательно установить актуальную версию антивирусного ПО и следить за ее обновлениями.

**Способ 3: системы родительского контроля.**

Если компьютером пользуются дети, риск подхватить вредоносное ПО значительно увеличивается. Чтобы защитить личные данные на ПК, можно создать для ребенка учетную запись с ограниченными правами доступа. Тем не менее, учитывая, что рядовые пользователи редко становятся жертвами хакеров такого уровня, обезопасить личные данные можно.

**Работа в группах. Анализ ситуаций**.

**1.Ситуация**: в личную почту Вам пришло письмо от незнакомца.

**2.Ситуация**: при поиске нужной информации всплывает окно «Поздравляем! Вы стали тысячным пользователем нашего сайта! Кликните и получите приз!!!»

**3.Ситуация.** Вам пришло смс.Например: «Мама, я попал в аварию, срочно нужны деньги, переведи их, пожалуйста, на этот номер телефона». «Папа, у меня проблемы, я в больнице, срочно нужны деньги, кинь их, пожалуйста, на этот кошелек. Маме не говори».

**4. Ситуация**. Ваня 13 лет – поклонник игры WorldofWarcraft. Он играет в нее уже три года и развил своего персонажа до очень высокого уровня. Год назад Ваня познакомился в игре с Колей (15лет), когда они вместе с другими участниками выполняли одно из групповых заданий. После этого они еще не раз сражались вместе и по ходу игры общались и переписывались. Однажды Ваня даже купил у Коли «Большой меч яростного гладиатора», переведя деньги ему на электронный кошелек. Вчера же Коля написал, что приезжает на выходные в Санкт-Петербург, где живет Ваня, и хотел бы как-нибудь пересечься, чтобы познакомиться в реальности. Коля также предлагает Ване купить у него особый щит, о котором мальчик давно мечтал.

**Вопросы для анализа ситуации**

* Стоит ли Ване согласиться на встречу? Почему?
* Что вас настораживает в ситуации? Доверяете ли вы Коле?
* Какие могут быть последствия встречи?
* Какими способами Ваня мог бы себя обезопасить?

***Учитель:***Много аргументов было приведено «за» и «против» сети Интернет. Но и это далеко не всё, что можно было бы сказать. Ребята! Подводя итоги нашей с вами встречи, я ещё раз хочу вас спросить: « Интернет нам друг или враг? Кто-то поменял своё мнение и решил, что для него в данный момент Интернет больше враг? Вы можете пересесть на другую сторону.

**Рефлексия «Клубок».**

Учитель: Итак, мы с вами поговорили, а сейчас каждый из вас попробует выразить свою мысль, чувства по поводу темы нашего классного часа, употребив только одно предложение, начиная его словами: …Для меня Интернет - это….При том мы будем передавать клубок.

Ребята, посмотрите, у нас получилась «Всемирная паутина», но мы сегодня общались с вами в реальной жизни.

Итак, мы можем сказать, что интернет может быть и другом и врагом. Всё дело в его пользователе. Пусть Интернет будет вашим надёжным другом и помощником!И помните, Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Но – как и реальный мир – Сеть тоже может быть опасна!

Спасибо за внимание!