**Муниципальное автономное образовательное учреждение**

**«Гимназия №7»**

|  |  |  |
| --- | --- | --- |
| РассмотреноНа заседании МО\_\_\_\_\_\_\_\_\_\_\_\_\_Руководитель МО\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Протокол №\_\_\_ от\_\_\_ \_\_\_20\_\_\_г. | СогласованоЗаместитель директора по ВР\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_ 20\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | УтвержденоДиректор МАОУ «Гимназия №7»Исхакова Л.Н.Приказ № \_\_\_ от \_\_\_ \_\_\_ 20\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

**Рабочая программа курса внеурочной деятельности**

 **«Уроки цифровой безопасности»**

**5-7 классы**

*Составитель*

Бояршинов А.А.

педагог-психолог

1 категории

2023-2024 учебный год

г. Пермь

**Правила цифровой безопасности**

*Уважаемые педагоги и родители, вам представляется серия методических разработок уроков, направленных на формирование цифровой грамотности наших детей. Каждый урок содержит: наглядный материал, благодаря которому, ребята смогут лучше понять и запомнить основные правили безопасного использования цифровых устройств; а также практическое задание в виде квеста, благодаря которому дети сумеют лучше отработать и закрепить полученные знания на практике.*

**Цель:**

научить школьников правильно оценивать степень угрозы информации, которую они воспринимают или передают через интернет

**Задачи:**

1. Познакомиться с правилами безопасного использования смартфоном и планшетом.
2. Научить правилам пользования цифровой техники и недопущения её заражения вирусами.
3. Обучить правилам цифрового этикета.
4. Познакомить с правилами безопасного использования цифровой почтой.
5. Профилактика кибербуллинга.
6. Познакомить с правилами безопасности в онлайн-играх.
7. Обучить правилам безопасности с целью не допустить обмана и не стать жертвой интернет мошенников.
8. Научить техникам сохранения своей репутации в сети интернет.
9. Познакомить с правилами использования информации и мерах наказания за нарушения авторского права.
10. Повышение уровня цифровой грамотности.

Оборудование: ноутбук, проектор для презентации, планшеты или смартфоны с выходом в интернет для каждого участника.

Разработка представляет из себя курс из 10 занятий продолжительностью не более 40 минут.

Каждое занятиесодержит наглядный материал в виде презентации, а такжеэлемент проверки-закрепления в виде квест-игры,ссылка на которую, указана после каждого урока.

**Вступление**

Здравствуйте ребята! Мы с вами начинаем курс занятий, направленных на развитие вашей цифровой грамотности. А вы знаете что такое «Цифровая грамотность»?

**Цифровая грамотность** — способность находить, оценивать и чётко передавать информацию с помощью набора текста и других средств массовой информации на различных цифровых платформах. Проще говоря, мы будем с вами учиться, как правильно пользоваться интернетом, компьютером, смартфоном и другими цифровыми устройствами.

А ещё на каждом уроке мы будем с вами проходить интересные цифровые квесты. Вы знаете, что такое квест?

**Квест** — это игра с сюжетной линией, которая заключается в решении различных головоломок и логических заданий. Причём эти квесты вы будете выполнять с помощью ваших телефонов. Да-да-да, как бы это необычно не звучало, но для проверки ваших знаний вам понадобится ваш смартфон с выходом в интернет. Результаты ваших работ будут фиксироваться и поощряться.

**Тематическое планирование**

|  |  |  |
| --- | --- | --- |
| **№** | **Тема урока** | **Примечание** |
| 1 | Как безопасно пользоваться смартфоном или планшетом | Презентация,цифровой квест |
| 2 | Как защищаться от компьютерных вирусов | Презентация,цифровой квест |
| 3 | Как безопасно пользоваться сетью Wi-Fi | Презентация,цифровой квест |
| 4 | Как вести себя в социальных сетях | Презентация,цифровой квест |
| 5 | Как безопасно пользоваться электронной почтой | Презентация,цифровой квест |
| 6 | Как вести себя в случае кибербуллинга | Презентация,цифровой квест |
| 7 | Основные правила безопасности в онлайн-играх | Презентация,цифровой квест |
| 8 | Как вести себя в случае фишинга | Презентация,цифровой квест |
| 9 | Как соблюдать цифровую репутацию | Презентация,цифровой квест |
| 10 | Подведение итогов | Викторина |

**1**

**Как безопасно пользоваться смартфоном или планшетом**

Ребята, наверняка у многих из вас есть смартфон или планшет. Перед началом урока я могу вам рассказать несколько интересных фактов об этих устройствах.

Как считаете, что является самым дорогим элементом смартфона?

1. Самыми дорогими элементами смартфона считаются экран и память.
2. В основе каждого смартфона лежит операционная система.
3. В Южной Корее была придумана «болезнь» от смартфона – цифровое слабоумие. Было доказано, что если увлекаться использованием смартфона, то у человека теряется способность сосредоточиться.
4. Дословно «смартфон» переводится как «умный телефон».
5. Номофобией называется страх остаться без смартфона.
6. В 2011 году миру был представлен первый треугольный планшет, но эту идею не удалось реализовать, так как она оказалась глупой.

***Презентация урока***

* Смартфоны и планшеты представляют собой небольшие стационарные компьютеры. Опасность в том, что программного обеспечения по их защите очень мало. Вирусы и вредоносные программы очень быстро могут вывести смартфон или планшет из строя.
* В Интернете нет ничего, что является по-настоящему бесплатным. В предложенном бесплатном контенте чаще всего скрыты платные услуги.
* Прежде чем отправить смс-сообщение, фото или видео, необходимо знать, кому они попадут, не используют ли их компьютерные мошенники.
* Необходимо почаще обновлять операционную систему смартфона или планшета.
* Нужно использовать только лицензионные антивирусные программы для мобильных телефонов.
* Для безопасности смартфона или планшета приложения можно загружать только из известного источника. Это позволит избежать вредоносного программного обеспечения.
* После посещения любого сайта, в котором была введена личная информация, нужно зайти в настройки браузера и удалить cookies.

Cookie (куки) — это **небольшие текстовые файлы, в которые браузер записывает данные с посещенных вами сайтов**. Файлы cookie позволяют сайтам «запоминать» своих посетителей, например, чтобы каждый раз не переспрашивать их логин и пароль.

* Периодически нужно проверять, какие платные услуги активированы на номере мобильного телефона.
* Номер своего мобильного телефона, а также адрес электронной почты можно давать только знакомым людям, которым доверяешь.
* Следует регулярно проверять Bluetooth: он должен быть выключен, когда им не пользуются.

**Практическая работа:** <https://joyteka.com/100112953>

**2**

**Как защищаться от компьютерных вирусов**

С любым цифровым устройством: телефоном, ноутбуком, телевизором и другими может возникнуть проблема. А как называется то, что вызывает проблему на устройстве?

**Компьютерный вирус** — это небольшая программа, которая распространяется с одного компьютера на другой и мешает работе компьютера. Компьютерный вирус может повредить или удалить данные на компьютере, распространить его на другие компьютеры с помощью почтовой программы или даже удалить все данные на жестком диске.

Интересные факты.

1. Однажды утром многие люди по всему миру получили электронные письма с заголовком «Я люблю тебя», причём письма приходили с адресов друзей и коллег. За любовным признанием скрывался компьютерный вирус, который нанес ущерб мировой экономике в 10 миллиардов евро. Вирус "I LoveYou" (именно так он назывался) был занесен в Книгу Рекордов Гиннесса как самый разрушительный компьютерный вирус в мире. Он поразил более 3 миллионов компьютеров на планете, став ещё и самым дорогим за всю историю.
2. Каждый год проходит чемпионат мира по борьбе с вирусами. Несколько лет назад на этом чемпионате одержала победу россиянка, которая показала лучший результат. Она легко обезвредила 9600 вирусов из 10.000 возможных.
3. Как говорит статистика, компьютерный вирус содержится в каждом 200-том электронном письме, которое отправляется в мире.
4. Сегодня в мире более 50 компаний-разработчиков антивирусного программного обеспечения. Более 5000 вирусологов по всему миру занимаются проблемами компьютерных вирусов. Изобретено уже более 300 различных антивирусных программ.
5. Вирусы могут находится в документах, вложениях и даже в аудио и видеофайлах. Сейчас не осталось таких типов файлов, которые невозможно заразить вирусом. Также набирают обороты специальные вирусы, которые путешествуют между мобильными телефонами и другими устройствами, в которых используется программное обеспечение.

***Презентация урока***

* Использовать современные операционные системы, имеющие большой уровень защиты от вредоносныхпрограмм и вирусов.
* Включать режим автоматического обновления своей операционной системы, скачивать программные обновления только с официального сайта разработчика операционной системы. Устанавливать патчи.

***Запла́тка, или патч*** — информация, предназначенная для автоматизированного внесения определённых изменений в компьютерные файлы.

* Работать на своем компьютере как пользователь, а не администратор. В этом случае большинство вредоносных программ не смогут инсталлироваться (установиться) на персональном компьютере.
* Использовать антивирусные программные продукты известных разработчиков с автоматическим обновлением баз.
* Посторонние лица не должны иметь доступ к вашему смартфону или планшету.
* Перед использованием внешних носителей следует проверять их на наличие вирусов.
* Прежде чем открывать подозрительные компьютерные файлы, нужно проверить, из каких источников они поступили. Если источник ненадежен, файл не открывать и удалить его.

**Практическая работа:** <https://joyteka.com/100127769>

**3**

**Как безопасно пользоваться сетью Wi-Fi**

* Многие считают, что бесплатный доступ в Интернет через сети Wi-Fi в кафе, отелях и аэропортах является безопасным. Это не так.

С помощью анализатора пакетов данных (например, Wireshark или CommView) можно узнавать на какие страницы люди заходили с подключенных устройств и что вводили в формы на сайтах, которые используют протокол http. Это могут быть данные для входа, тексты писем, сообщения.

* Нельзя передавать свою личную информацию через общедоступные сети Wi-Fi: вводить свои пароли доступа, логины и какие-то номера.
* При работе через Wi-Fi нужно использовать брандмауэр и систематически обновлять антивирусные программы.

Брандмауэр, он же **фаервол** (firewall)**, он же межсетевой экран** — это технологический барьер, который защищает сеть от несанкционированного или нежелательного доступа. Проще говоря, фаервол — охранник вашего компьютера, как и антивирус.

* При использовании Wi-Fi нельзя подключать функцию «Общий доступ к файлам и принтерам».
* Следует использовать только защищенное соединение через HTTPS, а не НТТР, т. е. при наборе веб-адреса вводить именно «https://».
* В мобильном телефоне нужно отключить функцию «Подключение к Wi-Fi автоматически»; не допускать автоматического подключения устройства к сетям Wi-Fi без вашего согласия.

**Практическая работа:** <https://joyteka.com/100128678>

**4**

**Как вести себя в социальных сетях**

**Социа́льная сеть (сокр. соцсеть)** — онлайн-платформа, которая используется для общения, знакомств, создания социальных отношений между людьми, которые имеют схожие интересы или офлайн -связи, а также для развлечения (музыка, фильмы) и работы.

Социальные сети так прочно вошли в нашу жизнь, что многие люди работают и общаются там постоянно. Например, в Facebook уже зарегистрирована седьмая часть жителей планеты, а это около 1 млрд человек. Помните, что информация, размещенная в социальных сетях, может быть найдена и использована кем угодно, в том числе с недобрыми намерениями.

* Следует ограничить список друзей, среди них не должно быть случайных и незнакомых людей.
* Не указывать в социальных сетях пароли, телефоны, адреса, дату рождения, другую личную информацию и информацию о своей семье.
* Прежде чем что-то опубликовать, написать и загрузить, необходимо подумать, нужно ли, чтобы это видели другие пользователи.
* При общении с незнакомыми людьми не использовать свое реальное имя и другую личную информацию, не называть место жительства, место учебы или работы.
* Не размещать в Интернете фотографии, по которым можно определить ваше местоположение.
* При регистрации в социальной сети использовать только сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8.
* Для социальной сети, почты и других сайтов использовать разные пароли.

**Практическая работа:**<https://joyteka.com/100131036>

**5**

**Как безопасно пользоваться электронной почтой**

**Электронная почта** (англ. email, от англ. electronicmail) — технология и служба по пересылке и получению электронных сообщений (называемых «письма»), это один из самых быстрых способов обмена сообщениями в интернете.

Чтобы сохранить конфиденциальность учетной записи и обезопасить себя от фишинга, вирусов и злонамеренных программ, следует придерживаться нескольких простых правил при использовании электронной почты.

* Используйте отдельные учетные записи электронной почты

Это поможет не только повысить безопасность, но и её производительность. Используйте одну учетную запись для интеграции с социальными сетями и другими онлайн-аккаунтами, вторую –для переписки с друзьями, третью – только для деловых сообщений.

* Воспользуйтесь виртуальной частной сетью (VPN)

Чтобы обезопасить компьютер и переписку по электронной почте, лучшее, что можно сделать, это загрузить VPN. Протоколы шифрования частной виртуальной сети гарантируют анонимность и конфиденциальность в интернете, защищают электронную почту от взлома и кражи информации. Поскольку VPN обеспечивает маскировку IP-адреса, отследить действия пользователя в интернете практически невозможно.

* Используйте разные пароли

Наличие нескольких учетных записей электронной почты бесполезно, если для них используется одинаковый пароль. В случае взлома одного из аккаунтов, взломщикам не составит труда украсть информацию и с других.Итак, для каждой учетной записи должен быть свой уникальный пароль. Чтобы запоминать новые сложные пароли лучше всего воспользоваться менеджером паролей.

* Остерегайтесь фишинга

**Фишинг** – это вид киберпреступности, когда мошенники связываются по электронной почте с пользователями от имени известных веб-сайтов (например, eBay, Amazon, Facebook и т. д.). Под предлогом проблем с учетными записями и проверки подлинности они просят отправить конфиденциальные сведения такие, как личная информация, платежные реквизиты, данные кредитной карты, пароли.

Никогда не открывайте фишинговые письма! Остерегайтесь их! Подумайте всякий раз, когда вас просят предоставить данные об учетной записи или поручают обновить имя пользователя и пароль. Внимательно посмотрите на источник и убедитесь, что он является законным, прежде чем что-либо делать.

* Никогда не нажимайте на ссылки в сообщениях электронной почты

Единственным исключением может выступить факт ожидания регистрации на каком-либо форуме или сообщение об активации учетной записи.

То же касается и спама, в сообщениях которого появляются ссылки для предоставления каких-либо услуг или продуктов. Никогда не переходите по этим ссылкам –неизвестно, куда они приведут.

Если приходят сообщения из банка или любой другой службы с просьбой об оплате, следует перейти на веб-сайт не по предоставленной ссылке, а набрать адрес вручную в строке поиска интернет-браузера.

* Не открывайте неизвестные вложения

Не пытайтесь открыть вложения в электронных письмах, если отправитель неизвестен. Не доверяйте таким письмам, даже если вложенный файл выглядит невинным. Открытие файлов из неизвестного источника может сделать компьютер уязвимым для вирусов. Удаляйте их без просмотра.

* Перед закрытием почтового ящика обязательно нажать кнопку «Выйти».

**Практическая работа:**<https://joyteka.com/100131684>

**6**

**Как вести себя в случае кибербуллинга**

**Кибербуллинг** - это травля, оскорбления или угрозы, высказываемые жертве с помощью средств электронной коммуникации, в частности, сообщений в социальных сетях, мгновенных сообщений, электронных писем и СМС.

* Если через Интернет в ваш адрес поступили угрозы или оскорбления, не нужно отвечать аналогично. Следует посоветоваться с учителем или родителями, как себя вести.
* Старайтесь постоянно поддерживать свою киберрепутацию, даже если вы находитесь под вымышленным именем. Существует множество способов определить, кто стоит за анонимным аккаунтом.
* Не хулиганить в Интернете: он запоминает все действия и сохраняет их. Удалить эту информацию невозможно.
* Помнить, что простая единичная агрессия, если на нее не обращать внимания, прекращается на начальной стадии.
* Блокировать агрессора. В программах обмена сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов.

**Практическая работа:**<https://joyteka.com/100131717>

**7**

**Основные правила безопасности в онлайн-играх**

Онлайн-игры — это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. В процессе игры игроки получают удовольствие, имеют возможность общаться, совместно выполняют задания, ведут битвы. Они покупают диски, оплачивают абонемент или приобретают какие-то опции.

Все полученные разработчиками средства идут на поддержание и развитие игры, а также обеспечение безопасности.

* В играх стоит опасаться кражи вашего пароля, на котором основана система авторизации большинства игр.
* Если другой игрок ведет себя плохо или создает вам неприятности, следует заблокировать его в списке игроков.
* Можно пожаловаться администраторам игры на плохое поведение игрока, желательно приложить какие-то доказательства в виде скринов.
* Нельзя указывать свою личную информацию в профайле игры. В игру всегда следует заходить под вымыленным именем.
* Нужно уважать других участников игры. Не оскорбляйте, не используйте грубых слов, не угрожайте.
* Не устанавливать неофициальные патчи (обновления).
* Использовать сложные и разные пароли.
* Даже во время игры не стоит отключать антивирус; пока вы играете, компьютер могут заразить.

**Практическая работа:**<https://joyteka.com/100131733>

**8**

**Как вести себя в случае фишинга**

В одной из предыдущих тем «Как безопасно пользоваться электронной почтой» мы уже затрагивали тему «фишинг». Так или иначе, с возрастом каждый человек начинает активно пользоваться электронными ресурсами по обмену информацией с окружающими. И на сегодняшний день электронная почта – это самый распространённый ресурс этого плана. К сожалению, этим ресурсом очень часто пользуются и злоумышленники, чтобы обманывать нас.

Воры и мошенники существовали всегда. Кража денег и документов для нас неудивительна. Но с появлением Интернета воры и мошенники активно перемещаются в Сеть. Так появилась новая угроза: интернет- мошенничество, или фишинг; главная цель мошенников — получение логинов и паролей, использующихся в дальнейшем для кражи денег и документов.

* Необходимо следить за своим аккаунтом. Если вы подозреваете, что ваша страничка была взломана, то необходимо заблокировать ее и сообщить об этом администраторам ресурса.
* Использовать только безопасные веб-сайты.
* Использовать сложные и разные пароли.
* Если страничку взломали, нужно срочно предупредить всех друзей в социальной сети об этом и о том, что от твоего имени возможна рассылка спама и ссылок на фишинговые сайты.
* Установить надежный пароль (PIN) на мобильный телефон.
* Отключить сохранение пароля в браузере.
* Не открывать подозрительные файлы и другие вложения в письмах, даже если они пришли от друзей, лучше уточнить у них, отправляли ли они эти файлы.

**Практическая работа:**<https://joyteka.com/100132200>

**9**

**Как соблюдать цифровую репутацию**

Сетевой имидж пользователя формируется из информации о нем в Интернете. Данные о месте жительства, учебы, о финансовом положении, особенностях характера и рассказы о близких — все это накапливается и хранится в сети. Удалить эти сведения до конца невозможно.

Многие пользователи легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Порой невозможно догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять вас на работу или учебу.

Комментарии, фотографии, видео и другие действия пользователя могут не исчезнуть даже после их удаления. Ведь неизвестно, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли, а главное — что подумают о человеке другие люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой — как из добрых побуждений, так и с намерением причинить вред.

* Прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети, надо как следует подумать.
* В настройках профиля лучше установить ограничения на просмотр своего профиля и его содержимого и сделать его видимым только для друзей.
* Не следует размещать и указывать информацию, которая может кого-либо оскорблять или обижать. На тебя могут пожаловаться, заблокировать и даже удалить твою страницу.
* Нельзя заниматься агитационными и другими противоправными действиями даже навымышленных (фейковых) страницах. Тебя легко могут вычислить и назначить наказание, даже если ты несовершеннолетний.
* Не позволяй другим размещать о тебе оскорбительную и ложную информацию. В случае обнаружения нужно немедленно сообщить родителям или пожаловаться администраторам сайта.
* Не добавляй в друзья и не делись личной информацией и переживаниями с теми, кого не знаешь.

**Практическая работа:**<https://joyteka.com/100132205>

**10**

**Подведение итогов**

**Викторина**

Подведём итоги того, что мы изучили на наших занятиях. Итоговым уроком у нас будет викторина. Вам необходимо разделиться на несколько команд.

**Правила:**

* Не выкрикивать ответы (отвечаем по поднятой руке)
* Возможность ответить будет только у одного участника команды (тот, кто первым поднял руку из вашей команды – тот и отвечает)
* Каждый вопрос имеет своё количество баллов
* В конце всех этапов мы подведём итоги и узнаем, кто займёт 1, 2, 3 место.

Викторина содержит 5 разделов, в каждом из которых по 5 вопросов, каждый вопрос оценивается от 100 до 500 баллов.

Все вопросы содержат информацию, которую мы с вами изучали на нашем курсе кибербезопасности.

Всем удачи!

*Приложение 1.*

Учитель в течении заключительного занятия заполняет «таблицу результатов» команд.

**Таблица результатов**

|  |  |
| --- | --- |
| **Тема** | **Баллы заданий** |
| **Как безопасно пользоваться смартфоном и планшетом** | 100 | 200 | 300 | 400 | 500 |
| **Как защищаться от компьютерных вирусов** | 100 | 200 | 300 | 400 | 500 |
| **Как безопасно пользоваться сетью Wi-Fi и электронной почтой** | 100 | 200 | 300 | 400 | 500 |
| **Как вести себя в социальных сетях и в случае кибербуллинга** | 100 | 200 | 300 | 400 | 500 |
| **Основные правила безопасности в онлайн-играх** | 100 | 200 | 300 | 400 | 500 |

Можно придумать командам названия или выбрать свой цвет и обозначать полученный той или иной командой баллы определённым цветом.

**Практическая работа:**<https://joyteka.com/100139728>

**Ответы викторины**

**1. Тема «Как безопасно пользоваться смартфоном и планшетом»**

**100** – Вирусы

**200** – Открытый вопрос. Почему не нужно отвечать незнакомцам?

**300** – Лицензионные

**400** - Сookie

**500**–Bluetooth

**2. Тема «Как защищаться от компьютерных вирусов»**

**100** – Заплатка, «патч»

**200** – Как пользователь

**300** – Открытый вопрос. Почему нельзя разрешить никому пользоваться вашим телефоном или планшетом?

**400** - Вирус

**500** –Антивирус Касперского, Dr.Web, Avast, ESET, AVG

**3. Тема «Как безопасно пользоваться сетью Wi-Fi и электронной почтой»**

**100** – Фишинг

**200** – Фаервол (firewall)

**300** – Открытый вопрос. Почему бесплатный интернет не безопасен?

**400**–Выход

**500** –VPN

**4. Тема «Как вести себя в социальных сетях и в случае кибербуллинга»**

**100** – Не отвечать

**200** – Геолокация (местоположение)

**300** – Репутация

**400** – Открытый вопрос. Что не стоит указывать в социальных сетях?

**500 –** Достойно

**5. Тема «Основные правила безопасности в онлайн-играх»**

**100** – Заблокировать

**200** – Администраторам сайта

**300** – Пиратские обновления

**400** – Ограничения

**500 –**Открытый вопрос.

**Литература.** Основы кибербезопасности : учебно-методическое пособие. 5—11 классы / С. Н. Вангородский. — М. : Дрофа, 2019.