**Государственное бюджетное общеобразовательное учреждение Самарской области средняя общеобразовательная школа имени Героя Советского Союза А.М. Вьюшкова с. Андросовка муниципального района Красноармейский Самарской области**

**Методическая разработка урока**

***Тема: «Безопасность в сети Интернет»***

Подготовил: учитель информатики,

Карпова Ирина Александровна

с.Андросовка, 2016 г.

**Класс: 7-11**

**Цель урока:** обеспечение информационной безопасности учащихся путем привития им навыков ответственного и безопасного поведения в современной информационно-коммуникационной среде, профилактика правонарушений в интернете, повышение безопасности и правовой защищенности в глобальной сети.

|  |  |  |
| --- | --- | --- |
| **Планируемые образовательные результаты** | | |
| Предметные | Метапредметные | Личностные |
| 1. Развитие умений работать с информационными ресурсами (анализировать, извлекать необходимую информацию), точно и грамотно выражать свои мысли.  2. Формирование навыков поведения в информационном обществе с целью обеспечения информационной безопасности. | 1. умение самостоятельно определять цели своего обучения, ставить и формулировать для себя новые задачи в учёбе и познавательной деятельности, развивать мотивы и интересы своей познавательной деятельности;  2. умение определять понятия, создавать обобщения, устанавливать аналогии, устанавливать причинно-следственные связи, строить логическое рассуждение, умозаключение и делать выводы;  3. умение организовывать учебное сотрудничество и совместную деятельность с учителем и сверстниками; находить общее решение и разрешать конфликты на основе согласования позиций и учёта интересов; формулировать, аргументировать и отстаивать своё мнение;  4. формирование и развитие компетентности в области использования информационно-коммуникационных технологий. | 1. формирование ответственного отношения к учению, готовности и способности обучающихся к саморазвитию и самообразованию на основе мотивации к обучению и познанию;  2. формирование целостного мировоззрения, соответствующего современному уровню развития науки и общественной практики;  3. формирование осознанного, уважительного и доброжелательного отношения к другому человеку, его мнению, мировоззрению, готовности и способности вести диалог с другими людьми и достигать в нём взаимопонимания;  4. формирование нравственных чувств и нравственного поведения, осознанного и ответственного отношения к собственным поступкам;  5. формирование коммуникативной компетентности в общении и сотрудничестве со сверстниками в процессе образовательной деятельности. |

|  |  |
| --- | --- |
| Ход урока | Время (мин.) |
| 1. Организационный момент | 2 |
| 1. Актуализация знаний | 5 |
| 1. Изучение нового материала | 10 |
| 1. Практическая часть | 17 |
| 1. Подведение итогов урока | 4 |
| 1. Домашнее задание | 1 |
| 1. Выставление оценок за урок | 1 |

**План-конспект урока**

|  |  |
| --- | --- |
| **Содержание урока. Методы и приемы работы** | **Способ организации деятельности учащихся** |
| **I. Организационный момент**  -Здравствуйте дети, садитесь. Кто у нас сегодня отсутствует?  -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. | Слушают учителя. |
| **II. Актуализация знаний**  - Что же такое «Информационная безопасность»?  Информационная безопасность — состояние сохранности информационных ресурсов и защищенности законных прав личности и общества в информационной сфере, а также процесс обеспечения конфиденциальности, целостности и доступности информации (*запись определения в тетрадях*).  - Давайте поиграем в игру «За или против». Вы увидите несколько высказываний. Попробуйте привести аргументы, отражающие  противоположную точку зрения.  1. Интернет имеет неограниченные возможности дистанционного образования. И это хорошо!  2. Интернет – это глобальный рекламный ресурс. И это хорошо!  3. Общение в Интернете – это плохо, потому что очень часто подменяет реальное общение виртуальному.  4. Интернет магазины – это плохо, потому что это наиболее популярный вид жульничества в Интернете.  5. В Интернете можно узнать сведения о человеке (место проживания и адрес электронной почты, номер мобильного телефона). И это хорошо! | Слушают учителя, отвечают на вопросы, записывают информацию в тетради. |
| **III. Изучение нового материала**  На сегодняшний день все больше и больше пользовательских компьютеров подключаются к сети Интернет.  Разработка сети началась в 1957 году американскими военными, в 1969 году был установлен первый сеанс связи. Технология Всемирной паутины. Всемирной Паутине исполнилось всего 23 года. Датой рождения World Wide Web (WWW) считается 6 августа 1991 года.  Изначально сеть развивалась вне какого-либо контроля, в настоящее время она содержит огромное количество информации, причем далеко не всегда безопасной. В связи с этим и с тем, что возраст, в котором человек начинает работать с сетью Интернет, становится все моложе, возникает проблема обеспечения безопасности детей.  - Какие возможности дает нам сеть Интернет? *(работа в группах: пишут список возможностей, по очереди каждая группа называет один пункт*).  С помощью сети Интернет происходит поиск информации, рассылаются сообщения, устраиваются видеоконференции, выставки, интервью, осуществляются покупки, осуществляется дистанционное обучение и многое-многое другое. Обычный пользователь имеет возможность заказать по Интернету любой товар с доставкой на дом, узнать погоду, познакомиться, пообщаться, посмотреть фильмы, послушать музыку и еще много чего.  - Как вы думаете, какие опасности сети Интернет могут Вас подстерегать?  - Давайте составим схему «Самые опасные угрозы в сети Интернет» и перенесем ее в тетрадь (*составление схемы и запись ее в тетради*).  Самые опасные угрозы в сети Интернет: вредоносные программы, кража информации - фишинг, хакерские атаки, спам, аппаратные и программные сбои, вторжение в частную жизнь, кража личной информации, интернет-мошенничество, кибербуллинг (издевательство) и т.д. | Слушают учителя, отвечают на вопрос, работают в группах. |
| **IV. Практическая часть**  - Давайте выработаем правила безопасной работы в сети Интернет (*работа в группах*).  Каждой группе дается задание на составление правил в одной из сфере сети Интернет:   1. **Методы защиты от вредоносных программ.** 2. Советы по безопасности работе в общедоступных сетях Wi-fi. 3. Основные советы по безопасности в социальных сетях. 4. Основные советы по безопасной работе с электронными деньгами. 5. Основные советы по безопасной работе с электронной почтой. 6. Кибербуллинг или виртуальное издевательство. 7. Основные советы для безопасности мобильного телефона. 8. Основные советы по борьбе с фишингом.   **Методы защиты от вредоносных программ:**  • Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;  • Постоянно скачивай обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;  • Ограничь физический доступ к компьютеру для посторонних лиц;  • Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;  • Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;  • Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;  • Не открывай компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.  **Советы по безопасности работе в общедоступных сетях Wi-fi:**  • Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;  • Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;  • При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют её для удобства использования в работе или учебе;  • Не используй публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту;  • Ипользуй только защищенное соединение через HTTPS, а не НТТР, т.е. при наборе веб-адреса вводи именно «https://»;  • В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.  **Основные советы по безопасности в социальных сетях:**  • Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;  • Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;  • Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;  • Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;  • Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;  • При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;  • Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.  **Основные советы по безопасной работе с электронными деньгами:**  • Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства;  • Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;  • Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли — это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п. Например, $tR0ng!;  • Не вводи свои личные данные на сайтах, которым не доверяешь.  **Основные советы по безопасной работе с электронной почтой:**  • Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;  • Не указывай в личной почте личную информацию. Например, лучше выбрать «музыкальный\_фанат@» или «рок2013» вместо «тема13»;  • Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;  • Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;  • Если есть возможность написать самому свой личный вопрос, используй эту возможность;  • Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;  • Не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;  • После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».  **Основные советы по борьбе с кибербуллингом:**  • Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;  • Управляй своей киберрепутацией;  • Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;  • Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;  • Соблюдай свой виртуальную честь смолоду;  • Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;  • Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;  • Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.  **Основные советы для безопасности мобильного телефона:**  • Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;  • Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?  • Необходимо обновлять операционную систему твоего смартфона;  • Используй антивирусные программы для мобильных телефонов;  • Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;  • После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies;  • Периодически проверяй какие платные услуги активированы на твоем номере;  • Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;  • Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.  **Основные советы по борьбе с фишингом:**  • Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;  • Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;  • Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем;  • Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;  • Установи надежный пароль (PIN) на мобильный телефон;  • Отключи сохранение пароля в браузере;  • Не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы. | Слушают учителя, отвечают на вопросы, работают в группах. |
| **V. Подведение итогов урока**  Рефлексия (*каждому ученику раздаются карточки с вопросами*)  Ответьте на вопросы, отметив тот вариант, который вы считаете верным.  1. Была ли полезной информация на сегодняшнем уроке?  да нет  2. Была ли для вас услышанная на уроке информация новой?  да нет  3. Закончите, пожалуйста, предложение:  Самым главным правилом безопасной работы в сети интернет для меня является следующее правило\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Слушают учителя, отвечают на вопросы. |
| **VI. Домашнее задание**  Составить универсальную памятку по безопасности в сети Интернет. | Записывают домашнее задание в тетрадь. |
| **VII. Выставление оценок за урок** |  |

**Список используемых источников:**

1. Интернет магазины – как не стать жертвой мошенников [Электронный ресурс] / Электронные текстовые данные – режим доступа: [http://virusinfo.info](http://virusinfo.info/showthread.php?t=70984)

2. Причины компьютерной зависимости [Электронный ресурс] / Электронные текстовые данные – режим доступа: [http://www.psypodderjka.ru](http://www.psypodderjka.ru/content/view/84/)

3. Спам и другие угрозы безопасности [Электронный ресурс] / Электронные текстовые данные – режим доступа: [https://ru-ru.facebook.com/help/](https://ru-ru.facebook.com/help/287137088110949/)

4. Угринович, Н.Д. Информатика. Учебник для 7 класса [Текст]: учебник для школы / Н.Д. Угринович.  – Москва: БИНОМ. Лаборатория знаний, 2015 – 46-48 с.

5. Хлобыстова, И.Ю. Информатика. УМК для основной школы [Текст]: мет. пособие для учителя / И.Ю. Хлобыстова, М.С. Цветкова. – Москва: БИНОМ. Лаборатория знаний, 2012.

6. Что такое вредоносное ПО [Электронный ресурс] / Электронные текстовые данные – режим доступа: [https://support.google.com](https://support.google.com/webmasters/answer/163633?hl=ru)