Поляков Р.Н.
Учитель информатики МБОУ «Лицей села Хлевное»
8 класс
Урок информатики в форме ролевой игры по теме «Безопасность в сети Интернет»
Тема урока для обучающихся: «Расследование преступления XXI века»
Цели урока:

- Повторить и обобщить знания об опасностях компьютерных сетей, о правовых аспектах работы с информацией на основе самостоятельного поиска и осмысления дополнительного материала для игры.
- Развитие познавательного интереса, творческой активности учащихся.
- Развитие у учащихся умения излагать мысли, моделировать ситуацию.
- Повторение и закрепление основного программного материала, выраженного в неординарных ситуациях.
- Связать информатику с другими предметами.
- Воспитать уважение к сопернику, умение достойно вести спор, стойкость, волю к победе, находчивость, умение работать в команде.

Задачи урока:

1. развитие познавательного интереса, логического мышления.
2. обобщение и повторение знаний по теме.
3. развитие критического мышления, памяти, внимательности.

Планируемые результаты. Предметные: формирование представлений о безопасном поведении детей в Интернете, организация усвоения основных понятий по данной теме, формирование мировоззрения учащихся, формирование умения распознавать опасные явление в сети Интернет, формирование навыков правильно оценивать степень безопасности ресурсов сети Интернет и основных приемов безопасного поведения в сети.
Метапредметные: *Личностные*: формирование умений управлять своей учебной деятельностью, развитие внимания, памяти, логического и творческого мышления; воспитание гуманизма, положительного отношения к труду, целеустремлённости (в ценностно-ориентационной сфере), формирование умения управлять своей познавательной деятельностью (в познавательной (когнитивной, интеллектуальной) сфере)**.**

Действующие лица:
Судья
Обвиняемые – группа из 10 лиц: компьютерный вирус, сеть WI-FI, социальная сеть, электронные деньги, электронная почта, кибербуллинг, мобильный телефон, Online игры, фишинг, цифровая репутация.
Прокурор
Адвокат
Секретарь суда
Свидетели защиты

Свидетели обвинения
Игрок
Охранники
Присяжные заседатели
В центре кабинета стол и кресло судьи. Слева сидят присяжные и секретарь суда. Справа на скамье обвиняемые и Адвокат. По обе стороны от них и на входе стоят охранники.
Секретарь суда: Встать, суд идет!
Все встают. Входит судья в черной мантии.
Судья: Прошу садиться! Слушается дело по обвинению так называемой организованной бандитской группировки, совершившей **преступление XXI века.**
Есть заявления, отводы суду, прокурору, присяжным?
Слушание объявляется открытым.
Слово предоставляется Прокурору.
Прокурор: (встает) Ваша честь, уважаемая публика и присяжные!
Обвиняемые оплели своей паутиной весь мир. Каждый день ими совершается множество преступлений. Свидетели обвинения многочисленными эпизодами докажут этот факт. Позвольте вызвать свидетеля обвинения.
Судья: Вызываем свидетеля обвинения.
1 Свидетель обвинения: Клянусь говорить правду и только правду. Я обвиняю компьютерный вирус, в том, что он приносит только зло! Компьютерный вирус – это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена заражённая программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.
Адвокат:. Ваша честь! Да, вирусы существуют, но они способствуют прогрессу! Чтобы защитить свои данные, программисты придумывают новые, более совершенные программы! Вирус – это волк, санитар Интернета, он находит и уничтожает слабые программы
Судья: Как вы докажете его невиновность?
Адвокат: Попрошу выступить Свидетеля защиты!
Свидетель защиты: Вирус требует от пользователей применения постоянных мер безопасности: используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
• Постоянно устанавливай патчи (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие 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.
Таким образом, защита от вируса - тоже самое, что мыть руки – приучает к порядку и чистоплотности.
Судья: Попрошу не отвлекаться от сути дела. Слово предоставляется Прокурору.
Прокурор: Ваша честь! В этой банде орудуют многие мошенники! Прошу выслушать еще одного свидетеля обвинения.
2 Свидетель обвинения: Wi-Fi - бренд, марка, которую в 1991 году зарегистрировала нидерландская компания бренд, словосочетание «Wireless Fidelity» переводится как «беспроводная точность».
Да, бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.
Адвокат: Я протестую. Есть же еще положительные примеры. Наличие Wi-Fi сегодня означает более высокий уровень сервиса.
Судья: принимается протест. Обвинение не доказало преступление Wi-Fi.
Адвокат: Зато мой свидетель докажет, что возможно использование Wi-Fi без ущерба для пользователя.
Свидетель защиты: 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 HTTP, 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.
Прокурор: Тогда обвинение выдвигается против всех Социальных Сетей! Социальные сети активно входят в нашу жизнь, многие люди работают и живут

там постоянно, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой всех жителей планеты. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

Адвокат: Давайте выслушаем самого обвиняемого.

Судья: Слово предоставляется обвиняемому Социальные сети.

Социальные сети: В сети, как и в любом обществе, действуют правила поведения, соблюдение которых обезопасит от неприятностей. 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.

Судья: защита доказала невиновность обвиняемого Социальные сети. Слово предоставляется Прокурору.

Прокурор: Я обвиняю Электронные деньги в воровстве наличных у пользователей и вызываю своего свидетеля.

Свидетель обвинения: Электронные деньги появились совсем недавно и сразу стали очень популярны у пользователей. Однако одновременно появились и мошенники. В первую очередь мошенники пытаются узнать логин и пароль от вашего электронного сейфа. Работа воришек начинается со сбора личной информации. В таком деле лучшие помощники - социальные сети, в которых о вас написано все. И дата рождения, и как кошку зовут, и где отдыхать любите. Так что пароль подобрать не так уж и сложно. Узнать логин тоже не составит труда - чаще всего он совпадает с почтовым.

Второй способ компьютерщики называют "социальная инженерия". Вы получаете электронное письмо от администратора вашей платежной системы. В послании вас просят поделиться логином и паролем, объясняя это сбоем в системе. Третий способ еще сложнее. Мошенники создают поддельный сайт,

оформление которого напоминает официальный сайт известной компании. Ничего не подозревая, вы вводите свои данные в предложенную форму. Вы так и не попадете в свой электронный кошелек. Зато у жуликов теперь есть все необходимое, чтобы украсть ваши деньги. Еще один способ - для самых продвинутых преступников. Чтобы завладеть чужими богатствами, они пишут вредоносную программу - троян - и запускают ее через интернет. В вашем компьютере электронный вирус маскируется под полезные файлы. Как только вы их запустите, он сам найдет все ваши логины, пароли и передаст хозяину.

Адвокат: свидетель сам назвал настоящих преступников – это люди – мошенники. Электронные деньги сами по себе ни в чем не виноваты. Именно поэтому мой свидетель предлагает правила пользования с электронными деньгами.

Судья: Слово предоставляется свидетелю защиты.

Свидетель защиты: Соблюдайте "сетевую гигиену"! Что это значит?

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. Не стоит также переходить по сомнительным ссылкам и открывать вложения, которые приходят к вам вместе с письмами на электронную почту. Как говорят компьютерщики, соблюдайте "сетевую гигиену"!

Судья: Слово предоставляется прокурору!

Прокурор: Следующий член преступной банды- Электронная почта. Электронная почта — это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя_пользователя@имя_домена. Также кроме передачи простого текста, имеется возможность передавать файлы.

Судья: А как электронная почта может навредить? Это же очень удобно, я и сам пользуюсь ею!

Прокурор: Многим может показаться, что проблема безопасности в сети Интернет касается лишь крупных компаний или тех пользователей, которые зарабатывают в Интернете. Это не совсем правильное мнение. Действительно, файлы обычных пользователей хакеров интересуют мало. Какая им от этого польза? А вот навредить ради забавы, либо с возможностью извлечения выгоды – это можно. Помимо забавы доступ к чужому почтовому ящику может открыть злоумышленнику доступ к персональным данным его обладателя, включая электронные кошельки, и другие, вполне материальные ресурсы. Так

что взлом почты либо ее повреждение – это еще и попытка стать обладателем чужой информации и чужих денег.
Адвокат: Попасть впросак с помощью электронной почты вам поможет соблюдение простых правил. Позвольте предоставить слово моему Свидетелю.
Свидетель: 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».
Судья: Надо запомнить! Спасибо Вам за полезную информацию!
Прокурор: Однако следующему обвиняемому вы спасибо не скажете, это я гарантирую! Его нужно упечь за решетку! Предъявляю обвинение кибербуллингу! Это преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.
Адвокат: Кибербуллинг – это слово, ярлык, под которым прячутся люди, занимающиеся преследованием и травлей в соцсетях! Запретим слово, но люди, которые этим занимаются, никуда не исчезнут! Давайте выслушаем моего свидетеля, который знает. Как сделать кибербуллинг неэффективным!
Свидетель: 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.
Судья: Все же я согласен с прокурором, но последнее слово за Присяжными!
Прокурор: А я выдвигаю обвинения против мобильного телефона! Уж сколько раз твердили родителям: не давайте детям телефон! И что мы видим? Современный смартфон или планшет есть у каждого. Они содержат в себе вполне взрослый функционал, могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений. Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность. Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.
Адвокат: Вас послушать, так прогресс вообще надо запретить! Давайте вернемся в каменный век! Вот там-то было по-настоящему безопасно! Однако я предлагаю для начала выслушать моего свидетеля.
Свидетель: 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.
Прокурор: А теперь послушаем, как вы станете защищать следующего обвиняемого - Online игры! От них точно нет никакой пользы! Игры какие-то! Современные онлайн-игры объединяют сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. За удовольствие они платят:

покупают диск, оплачивают абонемент или приобретают какие-то опции. Все эти средства идут на поддержание и развитие игры, а также на саму безопасность: совершенствуются системы авторизации, выпускаются новые патчи (цифровые заплатки для программ), закрываются уязвимости серверов. В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр.
Адвокат: Сразу видно, что вы сами не играли! Любой продвинутый игрок знает основные правила безопасности. Прошу вызвать Игрока для дачи показаний.
Игрок: Основные советы по безопасности твоего игрового аккаунта:
• Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков;
• Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов;
• Не указывай личную информацию в профайле игры;
• Уважай других участников по игре;
• Не устанавливай неофициальные патчи и моды;
• Используй сложные и разные пароли;
• Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.
Прокурор: Вы юлите, однако это вам не поможет! Я обвиняю следующего члена банды – Фишинг! Кто не знает - это кража личных данных. Обычной кражей денег и документов сегодня уже никого не удивишь, но с развитием интернет-технологий злоумышленники переместились в интернет, и продолжают заниматься «любимым» делом. Так появилась новая угроза: интернет-мошенничества или фишинг, главная цель которого состоит в получении конфиденциальных данных пользователей — логинов и паролей. Воровство в чистом виде! Что Вы на это скажете?
Судья: да, что?!
Адвокат: Фишинг –опасная вещь, но опасными его делают люди – кибермошенники! Вызываю своего Свидетеля – специалиста по фишингу!
Свидетель: 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;
Прокурор: горько видеть, как в эту банду вовлекли прекрасную даму – Цифровую репутацию! Ох и настрадалась она с подельниками! Давайте предоставим ей слово!
Цифровая репутация: Я - это негативная или позитивная информация в сети о тебе. Компрометирующая информация размещенная в интернете может серьезным образом отразиться на твоей реальной жизни. «Цифровая репутация» - это твой имидж, который формируется из информации о тебе в интернете. Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких – все это накапливается в сети.
Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу.
Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающее люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой – как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.
Адвокат: Из слов обвиняемой совершенно ясно, что она невиновна! Она страдает из-за чьих-то опрометчивых или глупых поступков. Давайте ей поможем! Приглашаю последнего Свидетеля защиты.
Свидетель защиты: Основные советы по защите цифровой репутации**:**
• Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;
• В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только «для друзей»;
• Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.
Судья: Мы выслушали обе стороны. Обвиняемые! Ваше последнее слово!
Обвиняемые: Мы и связанные с нами процессы в глобальной сети Интернет несут как пользу, так и вред. Пусть каждый для себя решить вопрос о своей безопасности в сети Интернет!
Судья: Попрошу присяжных вынести вердикт.
Присяжные: обвиняемые – это явления, которые созданы человеком. Человек придумал нож и придумал правила безопасного обращения с ножом. Компьютерный вирус, сеть WI-FI, социальная сеть, электронные деньги, электронная почта, кибербуллинг, мобильный телефон, Online игры, фишинг, цифровая репутация – не принесут вреда при правильном с ними обращением. Невиновны!
Судья: Освободите обвиняемых, но помните:
1. Защитите свой компьютер
Регулярно обновляйте операционную систему.

Используйте антивирусную программу.
Применяйте брандмауэр.
Создавайте резервные копии важных файлов.
Будьте осторожны при загрузке содержимого.

2. Защитите себя в Интернете

С осторожностью разглашайте личную информацию.
Думайте о том, с кем разговариваете.
Помните, что в Интернете не вся информация надежна и не все пользователи откровенны.

3. Соблюдайте правила

Закону необходимо подчиняться даже в Интернете.
При работе в Интернете не забывайте заботиться об остальных так же, как о себе

Использованные Интернет – источники

http://sch062.petersburgedu.ru/post/view/8293
http://krivaksin.ru/edinyiy-urok-po-bezopasnosti-pamyatka-po-bezopasnosti-v-internete/
http://ped-kopilka.ru/blogs/tatjana-vladimirovna-orlova/pamjatka-bezopasnosti-shkolnikov-v-seti-internet.html