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

**Цель занятия**: изучить опасные угрозы сети Интернет и методы борьбы с ними;

**Задачи:**

*Образовательная:* познакомиться с понятием «Интернет», «Вирус», изучить приемы безопасности при работе в сети Интернет;

*Развивающая:*развитие интереса к предмету, информационной культуры; формирование приёмов логического мышления; развитие способность анализировать и обобщать, делать выводы;

*Воспитательная:* воспитание аккуратности, точности, самостоятельности, привитие навыки групповой работы, сотрудничества;

*Здоровьесберегающая:* соблюдение санитарных норм при работе с компьютером, соблюдение правил техники безопасности, оптимальное сочетание форм и методов, применяемых на уроке;

**Оборудование:** ПК, проектор, интерактивная доска (или экран), 12 компьютеров, тетради, презентация «Безопасность в сети Интернет».

**План занятия:**

1. Организационный момент (1-2 мин.);
2. Введение в тему (3-5 мин.);
3. Объяснение нового материала (30-35 мин.);
4. Физкультминутка (1 мин.);
5. Самостоятельная работа (7-10 мин.);
6. Итог урока (2-3 мин.);

**Ход занятия:**

1. **Организационный момент, 1-2 мин.:**
2. **Введение в тему, 3-5 мин.:**

подготовить детей к восприятию темы;

нацелить на продуктивную работу.

Сегодня наш урок посвящен теме «Безопасность в сети Интернет». (Слайд 1)

Примечание. Учащиеся записывают в тетрадь основные определения самостоятельно по ходу лекции.

(Слайд 2) *Интернет* – это объединенные между собой компьютерные сети, глобальная мировая система передачи информации с помощью информационно-вычислительных ресурсов.

**Internet** - всемирная глобальная компьютерная сеть.

Internet объединяет в себе тысячи локальных, отраслевых, региональных сетей всего мира.

Отдельный пользователь, который не является абонентом какой-то из перечисленных сетей, также может подключиться к Internet через ближайший узловой центр.

В настоящее время услугами сети Интернет пользуется более 1 млрд. человек.

Интернет предоставляет пользователям разнообразные услуги: электронную почту, телеконференции, файловые архивы, Интернет-телефонию, форумы прямого общения (chat).

Самой новой и самой интересной услугой, предоставляемых пользователям глобальной сети, с недавних пор стала возможность работы с информационной системой WorldWideWeb (WWW).

**WorldWideWeb**- всемирная паутина: распределенная по всему миру информационная система с гиперсвязями, существующая на технической базе мировой сети Internet.

Всемирной Паутине исполнилось всего 16 лет.

Датой рождения WorldWideWeb (WWW) считается 6 августа 1991 года.

В этот день Тим Бернерс-Ли, работавший в Европейском центре ядерных исследований в Женеве (Швейцария), опубликовал краткое описание проекта WWW.

На сегодняшний день практический каждый человек, так или иначе, пользуется сетью Интернет. Возможности Интернет безграничны: учеба, поиск необходимой информации, перевод денежных средств, отдых и многое другое. Однако, многие пользователи даже не задумываются о том, какая опасность поджидает нас во всемирной паутине.

Интернет - технологии стали неотъемлемой частью жизни современного человека, особенно популярны они среди детей и молодежи. Однако виртуальное пространство полно опасностей. Угрозы, хулиганство, вымогательство, неэтичное и агрессивное поведение – все это нередко можно встретить. Еще одна опасность подстерегает любителей чатов. Виртуальное общение не может заменить живой связи между людьми. Человек, погрузившийся в вымышленный мир под чужой маской, постепенно теряет свое лицо, теряет и реальных друзей, обрекая себя на одиночество. Так же как и в обычной жизни, в Интернете появились свои хулиганы, которые осложняют жизнь другим пользователям Интернета.  По сути, они те же дворовые хулиганы, которые получают удовольствие, хамя и грубя окружающим. Большую опасность для наших компьютеров представляют вредоносные программы. К вредоносным программам относятся вирусы, черви и “троянские кони” – это компьютерные программы, которые могут нанести вред вашему  компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными с Интернетом и даже использовать ваш компьютер для распространения своих копий на компьютеры ваших друзей, родственников, коллег и по всей остальной глобальной Cети.

Давайте подумаем и вспомним, какие угрозы вы уже встречали во время работы за компьютером, а может, о каких-то угрозах, вы слышали от своих друзей? (ответ учащихся)

Молодцы!

1. **Объяснение нового материала (27-30 мин.):**

А теперь давайте обратимся к статистике в сети Интернет. Рейтинг самых опасных угроз распределяется следующим образом (Слайд 3):

1. Вредоносные программы
2. Кража информации
3. Халатность сотрудников
4. Хакерские атаки
5. Финансовое мошенничество
6. Спам
7. Аппаратные и программные сбои

***ПРЕЗЕНТАЦИЯ***

Как вы видите, угроз достаточно много и все они связаны между собой, например, из-за халатности сотрудников может произойти кража информации, а кража информации в свою очередь, может быть связана с финансовым мошенничеством.

Но, конечно же, лидером среди угроз являются вирусы. Давайте посмотрим, что такое вирусы, и какими они бывают. (Слайд 4)

1. **Компью́терныйви́рус** — разновидность компьютерных программ или вредоносный код, отличительной особенностью которых является способность к размножению (саморепликация).

 (Слайд 25-26) Каждый день появляются все новые и новые вирусы. Вам необходимо знать, что создание и распространение вредоносных программ (в том числе вирусов) преследуется в России согласно Уголовному кодексу РФ (глава 28, статья 273).

(Слайд 27) Также в нашей стране существует доктрина информационной безопасности РФ, согласно которой в России должен проводиться правовой ликбез в школах и вузах при обучении информатике и компьютерной грамотности по вопросам защиты информации в ЭВМ, борьбы с компьютерными вирусами, детскими порносайтами и обеспечению информационной безопасности в сетях ЭВМ.

Поэтому сегодня я расскажу вам о том, как обезопасить себя, свих друзей, свой личный или рабочий компьютер, чтобы не стать жертвой сетевых угроз.

***Установите комплексную систему защиты.*** (Слайд 30)

Установка обычного антивируса – вчерашний день. Сегодня актуальны так называемые «комплексные системы защиты», включающие в себя антивирус, файрволл, антиспам-фильтр и еще пару-тройку модулей для полной защиты вашего компьютера. Новые вирусы появляются ежедневно, поэтому не забывайте регулярно обновлять базы сигнатур: лучше всего настроить программу на автоматическое обновление.

***Будьте осторожны с электронной почтой***(Слайд 31)

Не стоит передавать какую-либо важную информацию через электронную почту. Установите запрет открытия вложений электронной почты, поскольку многие вирусы содержатся во вложениях и начинают распространяться сразу после открытия вложения. Программы MicrosoftOutlook и WindowsMail помогают блокировать потенциально опасные вложения.

***Пользуйтесь браузерами MozillaFirefox, GoogleChrome и AppleSafari.***(Слайд 32)

Большинство червей и вредоносных скриптов ориентированы под InternetExplorer и Opera. В рейтинге популярности лидирует IE, но лишь потому, что он встроен в Windows. Браузер Opera очень популярен в России из-за ее призрачного удобства и очень большого числа настроек. Уровень безопасности имеет ряд недостатоков как у одного, так и у второго браузера, поэтому лучше ими не пользоваться вовсе.

***Обновляйте операционную систему Windows.***(Слайд 33)

Постоянно обновляйте операционную систему Windows. Корпорация Microsoft периодически выпускает специальные обновления безопасности, которые могут помочь защитить компьютер. Эти обновления могут предотвратить вирусные и другие атаки на компьютер, закрывая потенциально опасные точки входа.

***Не отправляйте SMS-сообщения.***(Слайд 34)

Сейчас очень популярны сайты, предлагающие доступ к чужим SMS и распечаткам звонков, также очень часто при скачивании файлов вам предлагают ввести свой номер, или внезапно появляется блокирующее окно, которое якобы можно убрать с помощью отправкиSMS.

При отправке SMS, в лучшем случае, можно лишиться 300-600 рублей на счету телефона – если нужно будет отправить сообщение на короткий номер для оплаты, в худшем – на компьютере появится ужасный вирус.

Поэтому никогда не отправляйте SMS-сообщения и не вводите свой номер телефона на сомнительных сайтах при регистрации.

1. ***Пользуйтесь лицензионным ПО.***(Слайд 35)

Если вы скачиваете пиратские версии программ или свеженький взломщик программы, запускаете его и сознательно игнорируете предупреждение антивируса, будьте готовы к тому, что можете поселить вирус на свой компьютер. Причем, чем программа популярнее, тем выше такая вероятность.

Лицензионные программы избавят Вас от подобной угрозы!

1. ***Используйте брандмауэр.***(Слайд 36)

Используйте брандмауэр Windows или другой брандмауэр оповещают о наличии подозрительной активности при попытке вируса или червя подключиться к компьютеру. Он также позволяет запретить вирусам, червям и хакерам загружать потенциально опасные программы на компьютер.

1. ***Используйте сложные пароли.***(Слайд 37)

Как утверждает статистика, 80% всех паролей — это простые слова: имена, марки телефона или машины, имя кошки или собаки, а также пароли вроде 123. Такие пароли сильно облегчают работу взломщикам. В идеале пароли должны состоять минимум из семи, а лучше двенадцати символов. Время на подбор пароля из пяти символов — два-четыре часа, но чтобы взломать семисимвольный пароль, потребуется два-четыре года. Лучше использовать пароли, комбинирующие буквы разных регистров, цифры и разные значки.

1. ***Делайте резервные копии.***(Слайд 38)

При малейшей угрозе ценная информация с вашего компьютера может быть удалена, а что ещё хуже – похищена. Возьмите за правило обязательное создание резервных копий важных данных на внешнем устройстве – флеш-карте, оптическом диске, переносном жестком диске.

1. ***Функция «Родительский контроль» обезопасит вас.***(Слайд 39)

Для детской психики Интернет – это постоянная угроза получения психологической травмы и риск оказаться жертвой преступников.

Не стремитесь утаивать от родителей круг тем, которые вы обсуждает в сети, и новых Интернет-знакомых, это поможет вам реально оценивать информацию, которую вы видите в сети и не стать жертвой обмана.

Соблюдая эти не сложные правила, вы сможете избежать популярных сетевых угроз.(Слайд 40).

**4.Использованы материалы:**

1. Мельников В.П. Информационная безопасность и защита информации: учеб.пособие для студентов высших учебных заведений; 3-е изд., стер.-М.: Издательский центр «Академия», 2008. – 336 с.
2. Безопасный компьютер и Интернет для детей: новая программа повышения квалификации преподавателей АПКиППРО //Microsoft в образовании. — [Электронный ресурс]. — Электрон.дан. – cop. 2008 – Режим доступа: [http://www.ms-education.ru](http://www.ms-education.ru/).
3. Википедия – свободная энциклопедия [http://ru.wikipedia.org/wiki/Компьютерный\_вирус](http://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D0%B9_%D0%B2%D0%B8%D1%80%D1%83%D1%81)