Департамент образования администрация г. Перми
Муниципальное бюджетное учреждение
«Центр психолого-педагогической, медицинской и социальной помощи» г. Перми

РАССМОТРЕНО

утверждено на заседании
НМС МБУ «ЦППМСП» г. Перми
Протокол № 4 от 29.12.2022г.

СОГЛАСОВАНО
_____ О.В. Полторак,
начальник управления
воспитания и социализации
департамента образования
администрации города Перми

УТВЕРЖДАЮ
_____ О.А. Митина
и.о. директора МБУ
«ЦППМСП» г. Перми

ПРОГРАММА
киберурок «Безопасность в Интернете»
(для учащихся 11 класса)

г. Пермь, 2022

72. КИБЕРУРОК
«Безопасность в сети Интернет» (для 11 класса)

Цель урока: 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 способностьанализировать 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;

Предварительная подготовка учащихся: материал, изученный на предыдущих урокахинформатики;

Предварительная подготовка учителя: изучение материала урока, написание конспекта,создание презентации, создание теста, подготовка видеофрагмента;

Дидактические основы урока:

Методы обучения: словесные, наглядные, практические.

Тип урока: объяснение нового материала;

Формы учебной работы учащихся: фронтальная, индивидуальная работа.

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

План урока:

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.);
7. **Ход урока:**

Организационный момент, 1-2 мин.:

- ✓ сообщение темы урока (занесение темы в тетрадь), его целей и задач;
- ✓ краткий план деятельности.

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.

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.

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!

Объяснение нового материала (27-30 мин.):

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

- Вредоносные программы
- Кража информации
- Халатность сотрудников
- Хакерские атаки
- Финансовое мошенничество
- Спам
- Аппаратные и программные сбои

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 такоевирусы, и какими они бывают. (Слайд 4)

Компьютерный вирус — разновидность компьютерных программ или вредоносный код, отличительной особенностью которых является способность к размножению (саморепликация).

Классификация (Слайд 5)

В настоящее время не существует единой системы классификации и именования вирусов. Принято разделять вирусы на следующие группы.

По поражаемым объектам (Слайд 6-11)

Файловые вирусы. Это вирусы-паразиты, которые при распространении своих копий обязательно изменяют содержимое исполняемых файлов, при этом файлы, атакованные вирусом, в большинстве случаев полностью или частично теряют работоспособность)

Загрузочные вирусы. Это компьютерные вирусы, записывающиеся в первый сектор гибкого или жесткого диска и выполняющиеся при загрузке компьютера.

Скриптовые вирусы. Требуют наличия одного из скриптовых языков (Javascript, VBScript) для самостоятельного проникновения в неинфицированные скрипты.

Макровирусы. Это разновидность компьютерных вирусов, разработанных намакроязыках, встроенных в такие прикладные пакеты ПО,

как Microsoft Office.

Вирусы, поражающие исходный код. Вирусы данного типа поражают или исходный код программы, либо её компоненты (OBJ-, LIB-, DCU- файлы) а также VCL и ActiveX компоненты.

По поражаемым операционным системам и платформам (Слайд 12-13)

- DOS
- Microsoft Windows
- Unix
- Linux

По технологиям, используемым вирусом (Слайд 14-17)

Полиморфные вирусы. Вирус, который при заражении новых файлов и системных областей диска шифрует собственный код.

Стелс-вирусы. Вирус, полностью или частично скрывающий свое присутствие в системе, путем перехвата обращений к операционной системе, осуществляющих чтение, запись, чтение дополнительной информации о зараженных объектах (загрузочных секторах, элементах файловой системы, памяти и т. д.)

Руткит. Программа или набор программ для скрытия следов присутствия злоумышленника или вредоносной программы в системе.

По языку, на котором написан вирус (Слайд 18-19)

- ассемблер
- высокоуровневый язык программирования
- скриптовый язык
- и др.

По дополнительной вредоносной функциональности (Слайд 20-24)

Бэкдоры. Программы, которые устанавливает взломщик на взломанном им компьютере после получения первоначального доступа с целью повторного получения доступа к системе

Шпионы. Spyware — программное обеспечение, осуществляющее деятельность по сбору информации о конфигурации компьютера, деятельности пользователя и любой другой конфиденциальной информации без согласия самого пользователя.

Ботнеты. Это компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами — автономным программным обеспечением. Обычно используются для нелегальной или неодобряемой деятельности — рассылки спама, перебора паролей на удалённой системе, атак на отказ в обслуживании.

(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.

Физкультминутка (1 мин)

Но сначала, мы немножко отдохнем и проведем физкультминутку. (Слайд 28)

Мы все вместе улыбнемся,
Подмигнем слегка друг другу,
Вправо, влево повернемся
И кивнем затем по кругу.
Все идеи победили,
Вверх взметнулись наши руки.
Груз забот с себя стряхнули
И продолжим путь науки.

Итак, как же бороться с сетевыми угрозами? (Слайд 29)

1. ***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.

2. ***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 Microsoft Outlook и Windows Mail помогают блокировать потенциально опасные вложения.

3. ***Пользуйтесь браузерами Mozilla Firefox, Google Chrome и Apple Safari.*** (Слайд 32)

Большинство червей и вредоносных скриптов ориентированы под Internet Explorer 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 второгобраузера, поэтому лучше ими не пользоваться вовсе.

4. ***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.

5. ***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, вхудшем – на компьютере появится ужасный вирус.

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

6. ***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!

7. ***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.

8. ***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.

9. ***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.

10. ***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 видитев сети и не стать жертвой обмана.

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

Самостоятельная работа (7-10 мин.);

Закрепление материала - компьютерное тестирование.

А теперь, давайте проверим, насколько внимательно вы сегодня

слушали данныйматериал.

- ✓ Займите места за компьютером.
- ✓ Загрузите программу My Test Student.
- ✓ Выберите файл «Безопасность в сети Интернет»

Тест содержит 10 вопросов, в каждом вопросе есть только один правильный ответ.

По результатам теста, вы увидите окно со своими результатами. Оценка, которую поставит вам компьютер, и будет вашей оценкой за сегодняшний урок.

Тест:

1. Закончите предложение: Создание и распространение вредоносных программ (в том числе вирусов) преследуется в России согласно…

- ○ Административному кодексу
- ○ Трудовому кодексу
- ○ Уголовному кодексу
- ○ Гражданскому кодексу

2. Какой классификации вирусов на сегодняшний день не существует?

- ○ По поражаемым объектам
- ○ По поражаемым операционным системам и платформам
- ○ По количеству поражаемых файлов
- ○ По дополнительной вредоносной функциональности

3. Какой из приведенных паролей является более надежным

- ○ 123456789
- ○ qwerty
- ○ annaivanova
- ○ 13u91A_Ivanova

4. Для того, чтобы антивирусные программы обеспечивали наилучшую безопасность вашего ПК, необходимо:

- ○ Установить несколько антивирусных программ
- ○ Удалить все файлы, загруженные из сети Интернет
- ○ Своевременно обновлять антивирусные базы
- ○ Отключить компьютер от сети Интернет

5. Какой из браузеров считается менее безопасным, чем остальные:

- ○ Mozilla Firefox
- ○ Internet Explorer
- ○ Google Chrome
- ○ Opera

6. Какие действия не рекомендуется делать при работе с электронной почтой?

- ○ Отправлять электронные письма
- ○ Добавлять в свои электронные письма фотографии
- ○ Открывать вложения неизвестной электронной почты
- ○ Оставлять электронные письма в папке Отправленные

7. Что необходимо сделать, если на экране появилось окно с просьбой отправить SMS для дальнейшей работы?

- ○ Отправить SMS сообщение
- ○ Выполнить форматирование жесткого диска

- Перезагрузить компьютер
- Не отправлять SMS сообщение

8. Согласно какому документу в России проводится правой ликбез по вопросам защиты информации в ЭВМ?

- Трудовому кодексу РФ
- Доктрине информационной безопасности РФ
- Стратегии развития информационного общества РФ
- Конвенции о правах ребенка

9. Зачем необходимо делать резервные копии?

- Чтобы информация могла быть доступна всем желающим
- Чтобы не потерять важную информацию
- Чтобы можно было выполнить операцию восстановления системы
- Чтобы была возможность распечатать документы

10. Что необходимо сделать, если на сайте в Интернет, вдруг появилось сообщение о быстрой проверке ПК с просьбой перезагрузки компьютера?

- Перезагрузить компьютер
- Отформатировать жесткий диск
- Закрыть сайт и выполнить проверку ПК
- Выключить компьютер.

Итог урока (2-3 мин.);

Домашнее задание.

Ребята, домашнее задние у вас будет тоже связано с нашей темой. Разделимся на группы – вы сидите за компьютерами и по номеру компьютера мы и определим, какая группа будет готовить материал:

11. Учащиеся за компьютерами №1-№4 – Вам необходимо найти информацию о праздниках, связанных с информацией и сетью Интернет, которые отмечаются в нашей стране.
12. Учащиеся за компьютерами №5-№8 – Вам необходимо найти правила общения в сети, которые называются «Сетевым этикетом»
13. Учащиеся за компьютерами №9-№12 – Вам необходимо найти информацию об антивирусных программах – их виды и краткую характеристику популярных антивирусов.