Тема урока: Безопасность в сети Интернет.

Цель: информирование учащихся о способах обнаружения опасности в сети Интернет и возможности их избежать.

Задачи:

Образовательные:

- познакомить с понятиями «интернет», «вредоносная программа»;
- сформировать правила безопасной работы в сети Интернет;
- изучить опасные угрозы сети Интернет;
- изучить основы правовых знаний при работе в сети Интернет.

Развивающие:

- изучить основы правовых знаний;
- сформировать навыки коммуникационной культуры в сети Интернет.

Воспитательная:

- способствовать воспитанию у учащихся навыков безопасного и ответственного поведения в современной информационно-телекоммуникационной среде.

Оборудование: портативный персональный компьютер (ноутбук), раздаточный материал, доска, цветные карандаши.

Ход урока:

1. Подготовительный этап.
2. Актуализация знаний.
3. Первичное усвоение материала.
4. Закрепление и применение знаний.
5. Проверка и контроль знаний.
6. Рекомендация к работе дома.
7. Рефлексия.

1. Подготовительный этап.

Развитие глобальной сети изменило наш привычный образ жизни, расширило границы наших возможностей. Теперь появились возможности общения с людьми в разных уголках мира, доступа практически к любой информации, хранящейся на миллионах компьютерах во всём мире. Но давайте посмотрим на это с другой стороны. Все компьютеры, подключённые к интернету, связаны одной сетью. Соответственно, в то время, как вы получаете доступ ко множеству компьютеров, они также могут получить доступ и к вашему ПК. А на нём хранится огромное количество вашей личной информации.

И не сомневайтесь, рано или поздно кто-нибудь захочет воспользоваться данной возможностью.

Наверняка у вас возникнет вопрос: как вообще такое допускается и как избежать этого?

Обо всём поподробнее мы с вами узнаем на нашем уроке.

2. Актуализация знаний.

Прежде, чем приступать к изучению нового материала, давайте попробуем ответить на несколько вопросов.

Как вы думаете, что же вообще такое интернет?

(Учащиеся приводят свои ответы на вопросы)

Интернет – это всемирная информационная компьютерная сеть, связывающая между собой как пользователей компьютерных сетей, так и пользователей отдельных компьютеров для обмена информацией.

Интернет представляет собой огромное количество компьютеров, связанных между собой сетью, как паутиной. Ещё одно название интернета – Всемирная глобальная сеть.

А как пользователи связываются между собой?

(Учащиеся приводят свои ответы на вопросы)

Связь идёт по специальным каналам, как по нитям паутины. То есть по ним и передаётся вся информация.

3. Первичное усвоение материала.

Мы уже с вами узнали, что такое «интернет».

Давайте познакомимся со способами, с помощью которых злоумышленники могут получить доступ к вашем компьютеру и личной информации, а также изучим способы борьбы с этим.

На самом деле получить доступ к вашему компьютеру очень просто. Достаточно, чтобы вы скачали файл с вредоносной программой. Эта программа распространится по вашему компьютеру и будет предоставлять злоумышленнику различную информацию, в частности, логины и пароли от сайтов, информацию о кредитных картах и многое другое.

Вредоносная программа – это любое программное обеспечение, предназначенное для получения несанкционированного доступа к информации, которая хранится на компьютере, с целью причинения вреда владельцу компьютера.

Давайте рассмотрим некоторые типы вредоносных программ: вирусы, черви, троянские и хакерские программы; шпионские и рекламные программы; потенциально опасное программное обеспечение.

В первую группу входят наиболее распространённые и опасные категории вредоносных программ. Такие программы распространяют свои копии по локальным и глобальным сетям. Но в тоже время вредоносные программы, включённые в эту группу, имеют свои отличия. Рассмотрим их более подробно.

Начнём с червей. При активизации червя может произойти уничтожение программ и данных.

Интернет-черви – это разновидность вредоносных программ, которые распространяются через электронную почту и сеть Интернет. Они делятся на почтовых червей и веб-червей.

Почтовые черви распространяются через сообщения электронной почты. Это происходит в том случае, если в письме находится прикреплённый файл, который может оказаться вредоносной программой. Если в письме или в сообщении от незнакомого человека содержится ссылка, то нельзя ни в коем случае переходить по ней, так как если по этой ссылке находится червь, то сразу начнётся его загрузка и активация.

Веб-черви распространяются при помощи веб-сервисов. Заразить компьютер таким вирусом можно при посещении заражённого сайта. Чаще всего веб-черви прячутся в активных элементах веб-страниц или скриптах.

Троянские программы (трояны) осуществляют тайные действия по сбору, изменению и передаче информации злоумышленникам.

Хакерские программы предназначены для захвата контроля над удалённым компьютером или сетью компьютеров или же для вывода его из строя.

Во вторую группу входят шпионское и рекламное программное обеспечение. Если на компьютере появляются такие программы, то они могут принести некоторые неудобства пользователю или даже нанести значительный ущерб.

Шпионские программы – это программное обеспечение, которое тайно устанавливается и используется для доступа к информации, хранимой на компьютере.

Рекламные программы отображают рекламные объявления, которые загружаются из интернета. Чаще всего эти объявления появляются в отдельных окнах на рабочем столе или поверх рабочего окна. При закрытии таких окон программа всё равно продолжает работать и следить за действиями пользователя в интернете.

Третья группа – потенциально опасное программное обеспечение. Такие программы, в принципе, не являются вредоносными, но при некоторых обстоятельствах они могут нанести вред компьютеру.

Другими словами, потенциально опасные программы – это программное обеспечение, которое может нанести косвенный вред компьютеру, на котором установлено, или другим компьютерам в сети.

Важно знать, что за создание, использование и распространение вредоносных программ в России и большинстве стран предусмотрена уголовная ответственность.

А сейчас мы с вами переходим непосредственно к защите от вредоносных программ. Для этого существуют антивирусные программы.

Антивирусная программа – это программа, предназначенная для обнаружения и удаления вредоносных программ, а также для эффективной защиты от них.

Работа антивирусной программы заключается в сканировании файлов, загрузочных секторов дисков и оперативной памяти компьютера и выявлении в этих элементах известных или новых вредоносных программ.

Существует три вида антивирусных программ: сканер (функция защиты по требованию пользователя), монитор (функция постоянной защиты) и ревизор.

Антивирусный сканер пользователь может запускать самостоятельно или же задавать время автоматического запуска такой программы. Работа сканера заключается в проверке оперативной памяти и жёстких, и сетевых дисков на наличие вредоносных программ.

Запуск антивирусного монитора происходит автоматически при загрузке операционной системы. Монитор постоянно работает в фоновом режиме и всегда находится в оперативной памяти компьютера. Если пользователь дал команду компьютеру открыть какой-либо файл, то антивирусный монитор сначала проверяет этот файл на наличие вирусов и лишь потом, в зависимости от результатов проверки, разрешает системе открыть файл или запрещает его запуск. То есть антивирусный монитор всегда контролирует все процессы, которые происходят в памяти компьютера, и при наличии вируса выдаёт соответствующее сообщение.

Антивирусный ревизор контролирует изменения, произошедшие с программами и файлами на дисках.

Необходимо помнить, что антивирусные программы требуют постоянного обновления баз данных сигнатур, так как новые вирусы создаются регулярно.

При появлении вируса на вашем компьютере необходимо для начала сохранить нужную информацию на любой носитель информации, после этого следует отключить компьютер от сети и интернета и запустить антивирусную программу. После того как вирусы были найдены, нужно их удалить и перезагрузить компьютер. При перезагрузке антивирусная программа должна проверить ещё раз компьютер до загрузки самой операционной системы.

Также, помимо вирусов, стоит соблюдать некоторые правила использования сети Интернет, в частности, общения. Рассмотрите правила, которые необходимо соблюдать.

Правила безопасного пользования интернетом и мобильной связью:

1. Всегда спрашивайте родителей о незнакомых вещах в интернете. Они расскажут, что безопасно делать, а что нет.

2. Прежде чем начать дружить с кем-то в интернете, поставьте в известность родителей, спросите у них, как безопасно общаться.

3. При регистрации на сайтах, переходе по ссылкам старайтесь не указывать личную информацию, т. к. она может стать доступной незнакомым людям. Где вы живёте, в какой школе учитесь, номер телефона должны знать только друзья и родственники.

4. Используйте веб-камеру только при общении с людьми, которых вы знаете лично. Проследите, чтобы посторонние люди не имели возможности видеть ваш разговор, т. к. он может быть записан.

5. Нежелательные письма от незнакомых людей называются «спамом». Если вы получили такое письмо, не отвечайте на него, покажите его родителям. В случае, если ответите на подобное письмо, отправитель будет знать, что вы пользуетесь своим электронным почтовым ящиком, и будет продолжать посылать вам «спам».

6. Если вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.

7. Необходимо знать, что, если вы публикуете фото-, видеоматериалы, каждый может посмотреть их.

А сейчас давайте немного отвлечёмся от обсуждения нашей темы.

Итак, компьютер исполняет ваши команды чётко, а давайте проверим, сможете ли вы также правильно выполнять команды.

Встали из-за парт и слушаем внимательно. (*Упражнения из комплекса зрительной гимнастики.)*

Раз – налево, два – направо,
Три – наверх, четыре – вниз.
А теперь по кругу смотрим,
Чтобы лучше видеть мир.
Взгляд направим ближе, дальше,
Тренируя мышцу глаз.
Видеть скоро будем лучше,
Убедитесь вы сейчас.
А теперь нажмём немного
Точки возле своих глаз.
Сил дадим им много-много,
Чтоб усилить в 1000 раз!

4. Закрепление и применение знаний

А сейчас давайте с вами разгадаем кроссворд (Приложение 1).

Молодцы! Проверим ещё наши знания с помощью филворда (Приложение 2).

5. Проверка и контроль знаний

Давайте ответим на несколько вопросов.

1. Можно ли в сети Интернет переходить по рекламным ссылкам? Почему?
2. Следует ли указывать на незнакомых сайтах информацию о зарплатных картах ваших родителей?
3. Если вам написал незнакомый человек и попросил прислать вашу фотографию, как вы поступите?
4. Вы обнаружили у себя на почте новое письмо, отправителя вы не знаете, но там находится прикреплённый файл. Что нужно сделать в этом случае?

5. Какая программа должна стоять на компьютере при использовании сети Интернет и почему?

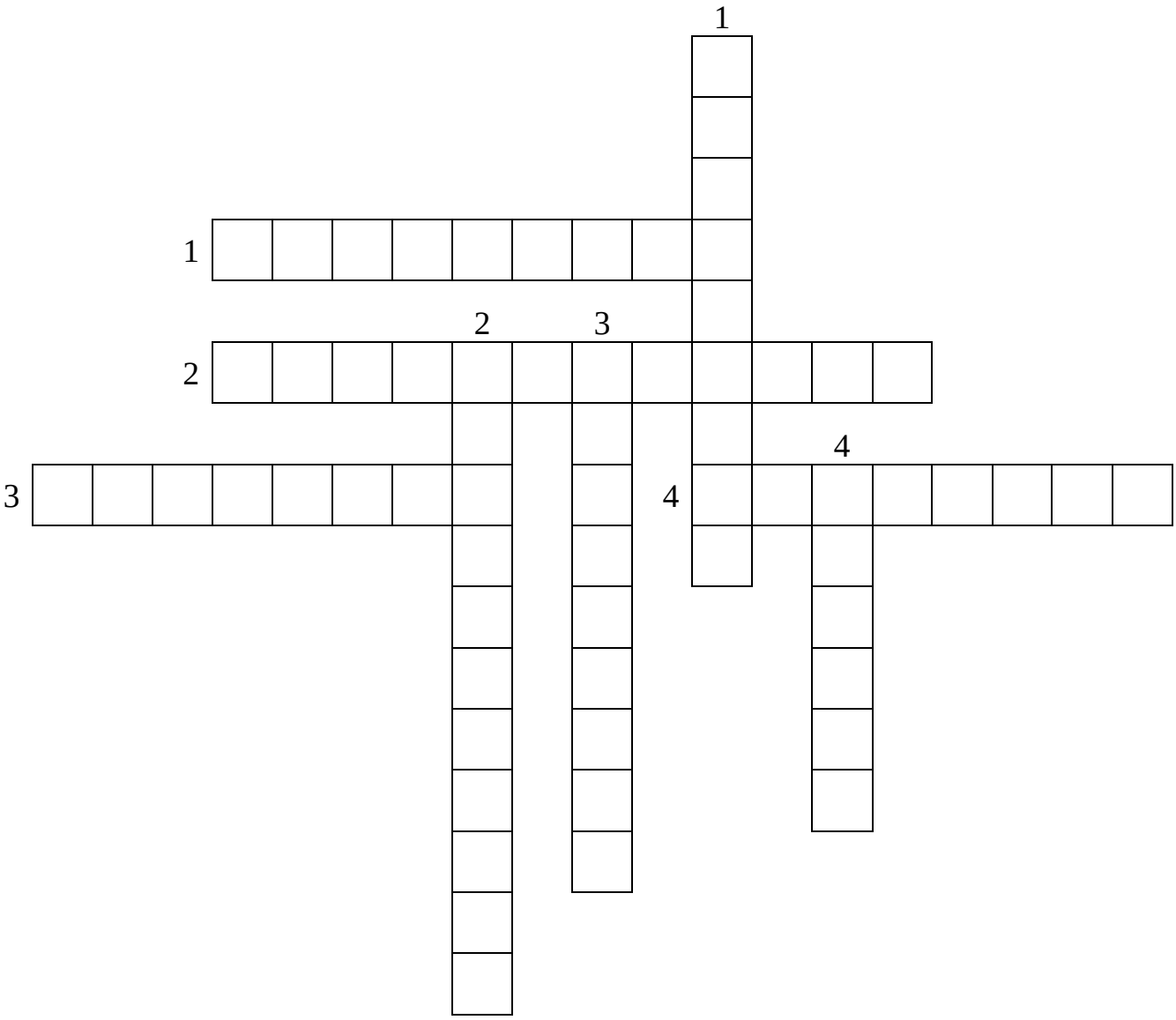
6. Рекомендация к работе дома

Изучите дома свой компьютер, в частности, программы, которые установлены на нём для проверки безопасности (антивирусные программы).

7. Рефлексия

На доске нарисована ваза. Давайте наполним её цветками (Приложение 3). Красный – есть проблема, нужна помощь; жёлтый – не всё понятно; зелёный – всё хорошо.

Кроссворд



Вопросы

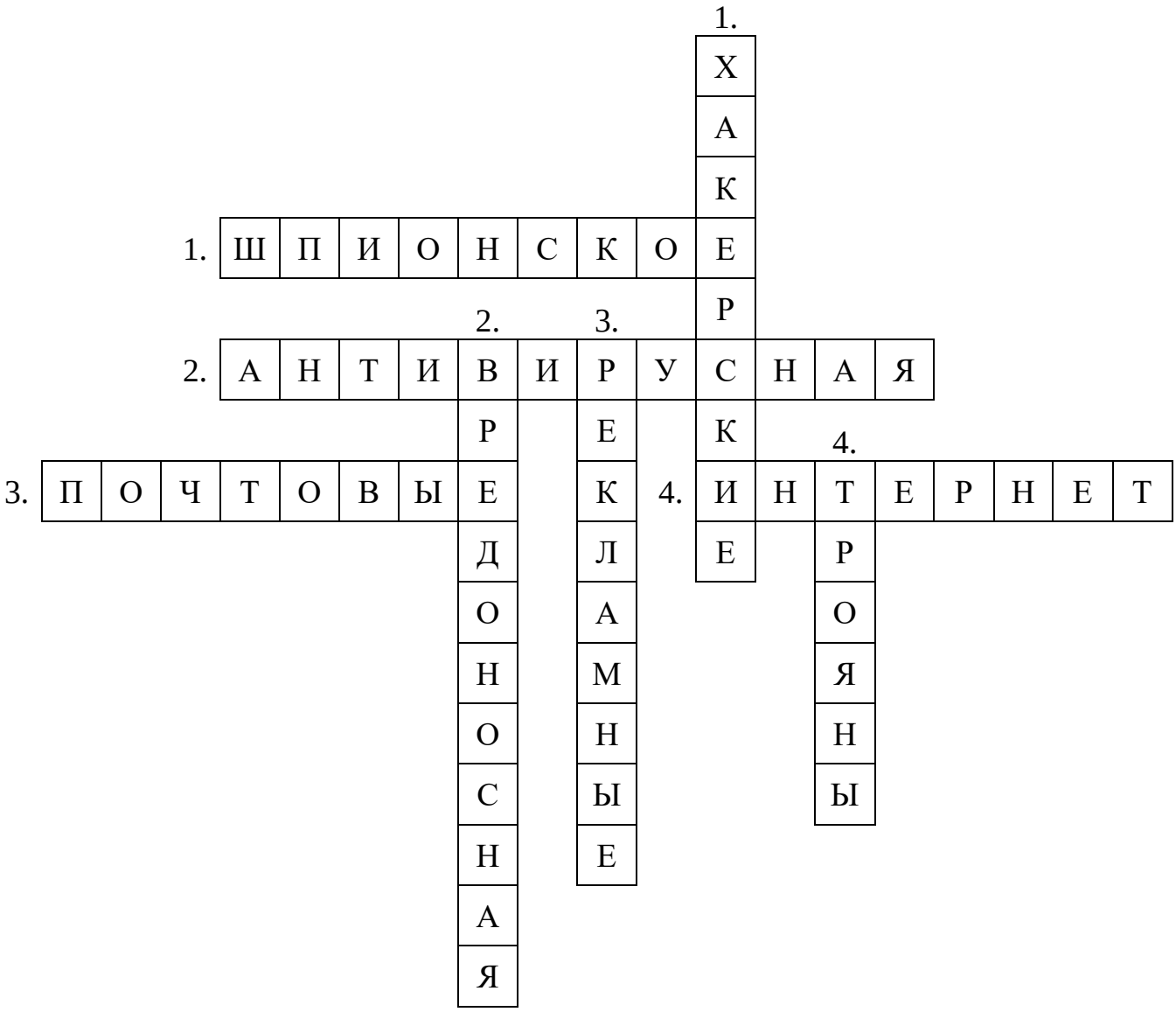
По горизонтали:

1. Как называется программное обеспечение, которое тайно устанавливается и используется для доступа к информации, хранимой на компьютере?
2. Как называется программа, предназначенная для обнаружения и удаления вредоносных программ, а также для эффективной защиты от них?
3. Как называется вид вредоносной программы (червей), которые распространяются через электронную почту?
4. Всемирная информационная компьютерная сеть, связывающая между собой как пользователей компьютерных сетей, так и пользователей отдельных компьютеров для обмена информацией.

По вертикали:

1. Как называются программы, предназначенные для захвата контроля над удалённым компьютером или сетью компьютеров или же для вывода его из строя?
2. Как называется программа, с помощью которой злоумышленник может получить доступ к вашему компьютеру?
3. Запишите названия программ, которые отображают рекламные объявления, загружаемые из интернета.
4. Сокращённое название троянских программ.

Ответы:


1.
Х
А
К
1. Ш П И О Н С К О Е
Р
2. 3.
2. А Н Т И В И Р У С Н А Я
Р Е К
4.
3. П О Ч Т О В Ы Е К 4. И Н Т Е Р Н Е Т
Д Л Е Р
О А О
Н М Я
О Н Н
С Ы Ы
Н Е
А
Я