Урока по «КИБЕРБЕЗОПАСНОСТИ» в рамках ФГОС ООО

по курсу «Информационное общество. Информационная безопасность»

Цель: формирование представления об информационной безопасности и привитие навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

Обучающие задачи:

- познакомить с понятием информационной безопасности;
- рассмотреть различные угрозы информационной безопасности.

Развивающие задачи:

- совершенствовать коммуникативные навыки через умение излагать мысли, умение вести диалог;
- определить план действий для предотвращения угрозы информационной безопасности.

Воспитательные задачи:

- воспитывать ответственность за свои действия.

Формы работы учащихся фронтальная, индивидуальная.

Оборудование и методические материалы: Мультимедийный проектор + ПК

План урока:

I. Организационный момент (1 мин)

II. Подготовка учащихся к усвоению нового материала (2 мин)

III. Теоретическая часть. Изучение нового материала (25 мин)

IV. Практическая часть. Первичное закрепление знаний (10 мин)

V. Домашнее задание (1 мин)

VI. Итог урока. (1 мин)

Ход урока

I. Организационный момент

Ученики готовятся к уроку, приветствие, проверка присутствующих.

II. Подготовка учащихся к усвоению нового материала

Объявление темы, цели и хода урока.

- Тема урока "Информационная безопасность".

- Цель урока: Формирование представления об информационной безопасности.

Сегодня на уроке Вы узнаете, каковы основные цели и задачи информационной безопасности, что такое информационные угрозы и как они проявляются, что является источником информационных угроз, какие существуют методы защиты информации от информационных угроз. Наиболее актуальным в современном обществе считается вопрос о безопасности в сети Интернет. Развитие глобальной сети изменило наш привычный образ жизни, расширило границы наших знаний и опыта. Теперь появилась возможность доступа практически к любой информации, хранящейся на миллионах компьютерах во всём мире. Но с другой стороны, миллионы компьютеров получили доступ к вашему компьютеру. И не сомневайтесь, они воспользуются этой возможностью. И никогда-то, а прямо сейчас.

III. Теоретическая часть. Изучение нового материала

- Что такое "информационная безопасность"?

Учащиеся высказывают свое мнение, как они понимают этот термин. Обобщая, учитель сообщает определение, которое записывается на доске.

Информационная безопасность.

Многие черты информационного общества уже присутствуют в современной жизни развитых стран. Компьютеры контролируют работу атомных реакторов, распределяют электроэнергию, управляют самолётами и космическими кораблями, определяют надёжность систем обороны страны и банковских систем, т.е. используются в областях общественной жизни, обеспечивающих благополучие и даже жизнь множества людей.

Жизненно важной для общества становится проблема информационной безопасности действующих систем хранения, передачи и обработки информации.

Информационная безопасность – совокупность мер по защите информационной среды общества и человека.

О важности этой проблемы свидетельствуют многочисленные факты. Более 80% компьютерных преступлений осуществляется через глобальную сеть Интернет, которая обеспечивает широкие возможности злоумышленникам для нарушений в глобальном масштабе.

Какие воздействия могут нанести ущерб информации или владельцу, то есть что представляет угрозу информационной безопасности?

Перечислим некоторые виды компьютерных преступлений, когда компьютер является инструментом для совершения преступления, а объектом преступления является информация:

Информационная безопасность - это защищенность информации от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации или ее владельцам

- Какие воздействия могут нанести ущерб информации или владельцу, то есть что представляет угрозу информационной безопасности?

Учащиеся делают свои предположения и определяются 7 направлений:

1. Кража личных данных, утечка информации
2. Вирусы, черви, трояны
3. Спам
4. Хакеры
5. Авторское право, нелицензионное ПО
6. Мошенничество
7. Дезинформация

1. Несанкционированный (неправомерный) доступ к информации. Лицо получает доступ к секретной информации, например, путём подбора шифра (пароля).

Хакерами и взломщиками называют людей, которые взламывают защиту систем данных. Они могут вторгнуться на незащищенный компьютер через Интернет и воспользоваться им со злым умыслом, а также украсть или скопировать файлы и использовать их в противозаконной деятельности.

2. Нарушение работоспособности компьютерной системы. В результате преднамеренных действий ресурсы вычислительной системы становятся недоступными, или снижается её работоспособностью. Примером такого рода преступлений является создание и распространение компьютерных вирусов.

Вирус - это программа, которая может проникнуть в компьютер различными путями и вызвать эффекты, начиная от просто раздражающих восприятие до очень

разрушительных. Вирусы могут проникать в компьютеры через электронную почту, Интернет, различные виды дисков и т.д., и имеют следующие характеристики:

- они способны размножаться, заражая другие файлы и программы.
- когда они активны, то способны выполнять раздражающие или разрушительные действия на Вашем компьютере.

3. Подделка (искажение или изменение), т.е. нарушение целостности компьютерной информации. Эта деятельность является разновидностью неправомерного доступа к информации. К подобного рода действиям можно отнести подтасовку результатов голосования на выборах, референдумах и т.д. путем внесения изменений в итоговые протоколы.

В ходе представления информационных угроз, учащиеся вырабатывают действия, которые нужно предпринять, чтобы обеспечить себя от таких угроз. По мере обсуждения, вырабатывается памятка.

Меры обеспечения информационной безопасности.

Кража личных данных, утечка информации

- старайтесь не "светить" номер кредитки в Сети;
- совершая онлайновую покупку, обращайте внимание на защищенность канала передачи данных;
- отслеживайте файлы cookies на жестком диске, регулярно проверяйте их принадлежность и удаляйте подозрительные.

Вирусы, черви, трояны.

- приобретите хороший антивирусный пакет, установите его в режиме максимальной безопасности, и своевременно обновляйте;

Спам.

- не сообщайте посторонним ваш адрес электронной почты, особенно тот, который предоставлен провайдером или особенно важен для вас;
- пользуйтесь почтовыми серверами с установленными фильтрами.

Хакеры.

- никогда не храните пароли на винчестере (даже в зашифрованном виде), не ленитесь каждый раз набирать их вручную;
- отсоединяйтесь от Internet при подозрении на хакерскую атаку, запускайте антивирусную программу, изменяйте пароли;
- старайтесь меньше пользоваться общедоступными программами сомнительного происхождения;
- просматривайте чаще системный реестр на предмет подозрительных записей;
- обязательно делайте резервные копии данных на дискеты или CD R/RW;

Авторское право, нелицензионное ПО

- укрепление законодательной базы;
- пресекайте попытки воровства вашего творчества;
- используйте только лицензионное ПО.

Мошенничество (денежное надувательство).

- просто будьте более скептичными и менее доверчивыми.

Дезинформация.

- разумный скептицизм плюс ее проверка в других средствах массовой информации.

Задачи информационной безопасности сводятся к минимизации ущерба, а также к прогнозированию и предотвращению таких воздействий.

Первичное закрепление учебного материала

Проведение Анкеты «Осторожно вирус!» (Приложение 1)

Проведение Анкеты «Осторожно Интернет!» (Приложение 2)

III. Практическая работа.

«Что можно? Что нельзя? К чему надо относиться осторожно?»

Обучающимся предлагается посмотреть ресурсы:

http://contentfiltering.ru/

http://www.microsoft.com/

http://www.youtube.com/

Учащимся необходимо прочитать и сформулировать правила безопасной работы. (Приложение 3, 4).

Закрепление изученного материала.

Интернет – это новая среда взаимодействия людей. В ней новое звучание приобретают многие правила и закономерности, известные людям с давних времен. Попробую сформулировать некоторые простые рекомендации, используя хорошо известные образы. Современный Интернет – это не только обширная, но и настраиваемая среда обитания! В нем хорошо тому, кто может обустроить в нем собственное пространство и научиться управлять им. Записывайте свои впечатления в блог, создавайте галереи своих фотографий и видео, включайте в друзья людей, которым вы доверяете. Тогда вместо бессмысленного блуждания по сети ваше Интернет-общение будет приносить пользу. И помните, Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Но – как и реальный мир – Сеть тоже может быть опасна!

V. Домашнее задание

Информация о домашнем задании. Инструкция о его выполнении:

1. Дать определение понятию «информационная безопасность».

2. Составить информационный лист-памятку «Моя безопасная сеть».

VI. Итог урока

Оценивание обучающихся. Подведение итога урока, выставляет оценки

Приложение 1

Анкета №1

«Осторожно, вирус!»

1. Что является основным каналом распространения компьютерных вирусов?
   - Веб-страницы
   - Электронная почта
   - Флеш-накопители

2. Для предотвращения заражения компьютера вирусами следует:
   - Не пользоваться Интернетом
   - Устанавливать и обновлять антивирусные средства
   - Не чихать и не кашлять рядом с компьютером
3. Если вирус обнаружен, следует:
   - Удалить его и предотвратить дальнейшее заражение
   - Удалить его и предотвратить дальнейшее заражение
   - Удалить его и предотвратить дальнейшее заражение
   - Установить какую разновидность имеет вирус
   - Выяснить как он попал на компьютер
4. Что не дает хакерам проникать в компьютер и просматривать файлы и документы:
   - Применение брандмауэра
   - Обновления операционной системы
   - Антивирусная программа
5. Какое незаконное действие преследуется в России согласно Уголовному Кодексу РФ?
   - Уничтожение компьютерных вирусов
   - Создание и распространение компьютерных вирусов и вредоносных программ
   - Установка программного обеспечения для защиты компьютера

Приложение 2

Анкета №2

«Осторожно, Интернет!»

1. Какую информацию нельзя разглашать в Интернете
   - Свои увлечения
   - Свой псевдоним
   - Домашний адрес
2. Чем опасны социальные сети?
   - Личная информация может быть использована кем угодно в разных целях
   - При просмотре неопознанных ссылок компьютер может быть взломан
   - Все вышеперечисленное верно
3. Виртуальный собеседник предлагает встретиться, как следует поступить?
   - Посоветоваться с родителями и ничего не предпринимать без их согласия
   - Пойти на встречу одному
   - Пригласить с собой друга
4. Что в Интернете запрещено законом?
   - Размещать информацию о себе
   - Размещать информацию других без их согласия
   - Копировать файлы для личного использования
5. Действуют ли правила этикета в Интернете?
   - Интернет - пространство свободное от правил
   - В особых случаях
   - Да, как и в реальной жизни

Приложение 3

Правила безопасности в сети Интернет

1. Не входите на незнакомые сайты.

2. Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на вирусы.

3. Если пришло незнакомое вложение, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину.

4. Никогда не посылайте никому свой пароль.

5. Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв.

6. При общении в Интернет не указывать свои личные данные, а использовать псевдоним (ник).

7. Без контроля взрослых ни в коем случае не встречаться с людьми, с которыми познакомились в сети Интернет.

8. Если в сети необходимо пройти регистрацию, то должны сделать ее так, чтобы в ней не было указано никакой личной информации.

9. В настоящее время существует множество программ, которые производят фильтрацию содержимого сайтов. Между членами семьи должны быть доверительные отношения, чтобы вместе просматривать содержимое сайтов.

10. Не всей той информации, которая размещена в Интернете, можно верить.

11. Не оставляйте без присмотра компьютер с важными сведениям на экране.

12. Опасайтесь подглядывания через плечо.

13. Не сохраняйте важные сведения на общедоступном компьютере.

Приложение 4

Итоговое тестирование

"Безопасный Интернет"

1. Что такое Интернет?
2. Какие опасности существуют в Интернете?
3. Использование Интернета является безопасным, если:
   a) защитить свой компьютер, защитить себя в Интернете, соблюдать правила
   b) разглашать личную информацию, заботиться об остальных, регулярно обновлять операционную систему
   c) защитить компьютер, создавать резервные копии документов, закону надо подчиняться даже в Интернете
4. Как защитить себя в Интернете?
   a) защитить свой компьютер, расширять круг знакомств с неизвестными людьми
   b) стараться давать как можно меньше информации о себе
   c) азмещать фотографии свои, друзей и родственников
5. Как обезопасить свой компьютер?
   a) a) выключить и спрятать в шкаф
   b) b) установить антивирусную программу
6. Что надо делать, чтобы антивирусная программа была
   a) лучше не иметь антивирусную программу
   b) обновлять антивирусную базу
   c) не посещать сайты, где нет достоверности, что сайт находится под защитой
7. Кто создаёт опасные программы
   a) чёрный властелин
   b) хакеры
   c) шпионы
   d) пожиратели смерти
8. Перечислите правила поведения в Интернете
9. А что для вас является "Безопасным Интернетом