**Конспект урока информатики**

**(можно использовать для проведения классного часа)**

**3-4 класс**

Тема урока: «Защита информации в компьютерных сетях»

**Цель**: сформулировать рекомендации, направленные на повышение безопасности работы пользователя в Интернете.

Требования к знаниям:

Учащиеся должны *знать:*

· Способы безопасной работы в сети Интернет;

· методы предупреждения информационной опасности в сети Интернет;

· воспитывать негативное отношение к созданию и распространению вредоносных программ;

· формировать навыки самостоятельной работы.

**Оборудование урока**: Персональные компьютеры.

Программное обеспечение: Microsoft PowerPoint.

Ход урока

1. Сообщение темы и цели урока

Учитель сообщает учащимся тему и цели урока.

2. Актуализация знаний

Вспомнить и обсудить с учащимися, уже известное им понятие защиты информации и компьютерных сетей. Послушать мнения учащихся о том, что они знают о защите информации в компьютерных сетях.

3. Объяснение нового материала

Учитель:

Решение проблем безопасности Интернета возможно только в комплексе с информационной безопасностью в обществе. Законодательство Интернета должно следовать из социальных нормативов.

С появлением информационной техники появилась и необходимость в информационной безопасности. Компьютер является самым многообещающим орудием совершения преступлений. Уже сейчас экономический ущерб от компьютерных преступлений сопоставим с преимуществами, получаемыми от внедрения компьютера, а социальные и моральные потери вообще не поддаются оценке.

Сформулируем следующие рекомендации, направленные на повышение безопасности работы пользователя в Интернете.

1. Установить антивирусное программное обеспечение с самыми последними обновлениями антивирусной базы. Проверять новые файлы, сохраняемые на компьютере. Периодически проверять компьютер полностью.

2. Отслеживать появление новых версий операционных систем и своевременно устанавливать обновления к ним, устраняющие обнаруженные ошибки.

3. Настроить операционную систему так, чтобы обеспечивались основные правила безопасности при работе в сети.

4. Регулярно обновлять пользовательское программное обеспечение для работы в сети, такое, как Internet Explorer, Outlook Express, устанавливая самые последние обновления.

5. Выполнить настройки почты, браузера Internet Explorer и клиентов других используемых сервисов, уменьшающие риск воздействия вредоносных программ и подверженность сетевым атакам.

6. Никогда не устанавливать и не сохранять файлы, полученные из ненадежных источников: скаченные с неизвестных web-сайтов, присланные по электронной почте, полученные в телеконференциях, - без предварительной проверки антивирусной программой. Подозрительные файлы лучше немедленно удалять.

7. При получении извещений о недоставке почтовых сообщений обращать внимание на причину и в случае автоматического оповещения о возможной отправке вируса немедленно проверять компьютер антивирусной программой.

8. По возможности, не сохранять в системе пароли (для установки соединений с Интернетом, для электронной почты и др.), периодически их менять. Регулярно выполнять резервное копирование важной информации.

9. Подготовить и иметь в доступном месте системную загрузочную дискету, закрытую на запись или загрузочный диск. В случае подозрения на заражение компьютера вредоносной программой загрузить систему с дискеты или диска и проверить антивирусной программой.

Данную лекцию лучше представить в виде презентации, которая может сопровождаться иллюстрациями к каждому пункту.

4. Проверка знаний учащихся и подведение итогов урока

Обсудить с учащимися те меры, которые они применяют для повышения безопасности в сети Интернет.

Самые активные учащиеся получают оценку.

5. Домашнее задание

Выучить данную тему.

Двум ученикам, по выбору, подготовить рефераты на темы: «Компьютерные вирусы» и «Антивирусные программы».