Классный час «Информационная безопасность»

Цель: формирование представления учащихся об информационной безопасности.

Задачи:

обучающие:

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

развивающие:

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

воспитывающие:

- воспитывать ответственность за свои действия.

Ход урока:

1. Организационный момент.(__1_ мин)

Проблема обеспечения информационной безопасности учащихся в Интернете становится все более актуальной в связи с существенным возрастанием численности несовершеннолетних пользователей. В современных условиях развития общества компьютер стал для школьников и «другом» и «помощником» и даже «воспитателем», «учителем». Между тем существует ряд аспектов при работе с компьютером, а в частности, с сетью Интернет, негативно влияющих на физическое, моральное, духовное здоровье подрастающего поколения, порождающих проблемы в поведении у психически неустойчивых школьников, представляющих для детей угрозу.

Знание ребенком элементарных правил отбора информации, а также умение ею пользоваться способствует развитию системы защиты прав детей.

2. Изучение нового материала.

Международный день защиты информации – 30 ноября. Праздник начал существовать в 1998 году (с праздника есть даже сайт) т.к. в 1988 г. была зафиксирована первая массовая эпидемия червя, получившего название по имени своего «творца» – Морриса. Праздник существует и признан международным благодаря американской Ассоциация компьютерного оборудования. Цель этого Дня — напомнить всем о необходимости защиты компьютерной информации, а также обратить внимание производителей и пользователей аппаратных и программных средств на проблемы безопасности.

Международный день безопасного Интернета – второй вторник февраля (введен в 2004 году).

В РФ существует законодательство в области информационной безопасности детей (Федеральный закон Российской Федерации № 436-ФЗ от 29.12.2010 г. «О защите детей от информации, причиняющей вред их здоровью и развитию»).

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

Дети 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

- Задачи информационной безопасности сводятся к минимизации ущерба, а также к прогнозированию и предотвращению таких воздействий. Давайте разделимся на группы и установим, какие действия нужно предпринять, чтобы обезопасить себя от таких воздействий.

Работа группами по карточкам, обсуждение - 10 минут, затем представители от каждой группы сообщают всем свои методы защиты (принимая или оспаривая), учитель принимает участие в обсуждении - разрабатывается памятка

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

- 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.

- Рассмотрим, как можно защитить информацию из своего файла от посторонних глаз, защитить файл от изменений.

Игра «За и против».

Учитель предлагает игру «За или против». На слайде - несколько высказываний. Попробуйте привести аргументы, отражающие противоположную точку зрения.

Давайте попробуем выработать правила работы в Интернете (записывать на слайде)

- Что можно? Что нельзя? К чему надо относиться осторожно?

Выработка правил работы 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. Никогда не посылайте никому свой пароль.
4. Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв.
5. Если в сети необходимо пройти регистрацию, то должны сделать ее так, чтобы в ней не было указано никакой личной информации.
6. Не всей той информации, которая размещена в Интернете, можно верить.
7. Не сохраняйте важные сведения на общедоступном компьютере.

3. Закрепление изученного материала.

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!

Анкетирование.