Тема урока : Информационная безопасность учащихся в сети Интернет

(для 9-11 класса)

Цель: сформировать у школьников активную позицию в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им.

Задачи: ознакомить учащихся:

– с правилами ответственного и безопасного поведения в современной информационной среде, способах защиты от противоправных посягательств в сети Интернет;

– как критически относиться к сообщениям в СМИ (в т.ч. электронных), как отличить достоверные сведения от недостоверных, как избежать вредной и опасной для них информации, как распознать признаки злоупотребления их доверчивостью и сделать более безопасным свое общение в сети Интернет;

– как общаться в социальных сетях (сетевой этикет), не обижая своих виртуальных друзей, и избегать выкладывать в сеть компрометирующую информацию или оскорбительные комментарии и т.д.

Оборудование: плакаты по данной тематике (на доске), медиапроектор, экран, презентация Microsoft Power Point “Проблемы информационной безопасности в сети Интернет”.

Ведущие понятия: угроза, безопасность, информация, угроза информационной безопасности.

Ход занятия

1. Вступительная часть — сообщение цели занятия, основные правила, продолжительность и режим предстоящей работы.

2. Проведение экспресс-опроса участников об их ожиданиях от предстоящей работы.

3. Беседа учителя и учащихся строится на основе работы с материалами презентации “Проблемы информационной безопасности”

Слайд 1. Тема.

Учитель предлагает учащимся высказать мнение о том, как они понимают понятия “угроза”, “безопасность”, “информация”, “угроза информационной безопасности”.

Слайд 2. Знакомство с основными понятиями.

Безопасность – отсутствие угроз, либо состояние защищенности от угроз.

Информация – сведения или сообщения.

Угроза информационной безопасности — совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства в информационной сфере.

Учитель просит учащихся назвать, какие они знают источники информации.

Слайд 3. Источники информации.

Средства массовой коммуникации, в т.ч. Интернет.

Литература.

Образование.

Личное общение.

Искусство.

Система социально-воспитательной работы и др.

Вывод. Любое из этих средств может быть использовано на благо или во вред личности!

Слайд 4-7. Справочная информация.

По последним данным, в России:

средний возраст начала самостоятельной работы в Сети - 10 лет (в 2009 году - 11 лет); и сегодня наблюдается тенденция к снижению возраста до 9 лет;

30% несовершеннолетних проводят в Сети более 3 часов в день (при норме 2 часа в неделю!).

Ежедневная детская аудитория Рунета:

46% (13-14 лет),

54% (15-16 лет);

самые "любимые" детьми ресурсы – социальные сети (78%); в них проводится до 60 минут в день.

Помимо социальных сетей, среди несовершеннолетних популярны следующие виды и формы онлайн-развлечений:

- сетевые игры;
- просмотр и скачивание фильмов, клипов, аудиофайлов, программ;
- обмен файлами;
- использование электронной почты, сервисов мгновенного обмена сообщениями, чатов;
- ведение блогов и пр.
- 4% детей сталкиваются в Интернете с порнографической продукцией

- 40% получают непосредственные предложения о встречах "в реале".

4. Давайте вместе подумаем. Вопросы для коллективного обсуждения:

– Почему тема информационной безопасности является важной и почему эти вопросы должны обсуждаться в школе?
– Из возможных причин, какие можно выделите аспекты, связанные с сущностью Интернета и его значимостью как средства общения.

5. Работа в группах:

задание для групповой работы — подготовка коллективного ответа на вопрос: “Какие основные правила безопасного поведения в Интернете вы можете предложить?”, “Какими правилами отбора (пользования) информации вы рекомендуете сверстникам пользоваться?”, “Как оградить себя от кибер-преступлений?”. (Возможные варианты работы: группы обсуждают все три вопроса. Каждая группа обсуждает только один из вопросов.).

6. Обсуждение результатов работы.

7. Продолжение работы с презентацией “Проблемы информационной безопасности”.

Слайды 8-11. Три основных правила безопасного поведения в сети.

Защитите свой компьютер.

- Регулярно обновляйте операционную систему.
- Используйте антивирусную программу.
- Применяйте брандмауэр.
- Создавайте резервные копии важных файлов.
- Будьте осторожны при загрузке содержимого

Помните! После публикации информации в Интернете ее больше невозможно будет контролировать и удалять каждую ее копию.

Защитите себя в Интернете.

- Думайте о том, с кем разговариваете.
- Никогда не разглашайте в Интернете личную информацию, за исключением людей, которым вы доверяете. При запросе предоставления личной информации на веб-сайте всегда просматривайте разделы “Условия использования” или “Политика защиты конфиденциальной информации”, чтобы убедиться в предоставлении оператором веб-сайта сведений о целях использования получаемой информации и ее передаче другим лицам.
- Всегда удостоверяйтесь в том, что вам известно, кому предоставляется информация, и вы понимаете, в каких целях она будет использоваться.

Помните! В Интернете не вся информация надежна и не все пользователи откровенны.

Думай о других пользователях.

- Закону необходимо подчиняться даже в Интернете.
- При работе в Интернете будь вежлив с другими пользователями Сети.
- Имена друзей, знакомых, их фотографии и другая личная информация не может публиковаться на веб-сайте без их согласия или согласия их родителей.
- Разрешается копирование материала из Интернета для личного использования, но присвоение авторства этого материала запрещено.
- Передача и использование незаконных материалов (например, пиратские копии фильмов или музыкальных произведений, программное обеспечение с надорванными защитными кодами и т.д.) является противозаконным.
- Копирование программного обеспечения или баз данных, для которых требуется лицензия, запрещено даже в целях личного использования.

Помните! Неразрешенное использование материала может привести к административному взысканию в судебном порядке, а также иметь прочие правовые последствия

Слайд 12. Дополнительные правила безопасного поведения в сети Интернет.

Закрывайте сомнительные всплывающие окна! Всплывающие окна — это небольшие окна с содержимым, побуждающим к переходу по ссылке. При отображении такого окна самым безопасным способом его закрытия является нажатие значка X (обычно располагается в правом верхнем углу). Невозможно знать наверняка, какое действие последует после нажатия кнопки “Нет”.

Остерегайтесь мошенничества! В Интернете легко скрыть свою личность. Рекомендуется проверять личность человека, с которым происходит общение (например, в дискуссионных группах).

Помните! Большая часть материалов, доступных в Интернете, является непригодной для несовершеннолетних.

Слайд 13. Подведение итогов работы. Учащиеся высказывают свое мнение, оправдались ли их ожидания от проделанной работы.

8. Размещение в дневниках правил безопасного поведения в сети.

9. Учитель благодарит учащихся за работу

10. Оценка учащимися занятия (на доску крепятся флажки. Красный – занятие понравилось; зеленый – занятие оставило равнодушным; синий – занятие не понравилось).