Конспект классного часа в 5 - 9 классах
МБОУ Часцовской средней общеобразовательной школы

«Интернет без опасностей. Безопасность детей в Интернете»

Разработала: Трошкина Лидия Александровна, учитель информатики, классный руководитель 7 «В» класса

«Много путей преодоления
опасностей, если
человек хоть что-то готов говорить
и делать".
Сократ

Цель: профилактика правонарушений в интернете, повышение безопасности и правовой защищенности в глобальной сети.

Задачи занятия:

- Формирование навыков поведения в информационном обществе с целью обеспечения информационной безопасности
- Разработка норм и правил поведения детей в сети Интернет
- Расширение кругозора учащихся.

Оборудование: компьютер, проектор, буклет, интерактивная система опроса.

Ход занятия.

Проведение анкетирования с целью выявления интернет-зависимости у учащихся.

1. Чувствуете ли Вы себя зависимым Интернетом (думаете ли Вы о предыдущих онлайн сеансах и предвкушаете ли последующие)?
2. Ощущаете и Вы потребность в увеличении времени, проведенного в Сети?
3. Были ли у Вас безуспешные попытки контролировать, ограничить или прекратить использование Интернета?
4. Чувствуете ли Вы себя усталым, угнетенным или раздраженным при попытках ограничить или прекратить пользование Интернетом?
5. Находитесь ли Вы онлайн больше, чем предполагали?
6. Были ли у Вас случаи, когда Вы рисковали получить проблемы в работе, учебе или в личной жизни из-за Интернета?
7. Случалось ли Вам лгать членам семьи, врачам или другим людям чтобы скрыть время пребывания в Сети?
8. Используете ли Вы Интернет для того, чтобы уйти от проблем или от дурного настроения (например, от чувства беспомощности, виновности, раздраженности или депрессии)?

В случае пяти или более положительных ответов на эти вопрос следует обратить внимание, что у ребёнка интернет-зависимость.

II. Актуализация знаний. Формулировка темы урока. (демонстрация обложки книг)

Представить жизнь без Интернета в наше время невозможно. Но зато можно попытаться научиться пользоваться им умело. Все должны знать, что такое вирусы и антивирусы, спам и спам-фильтры, чем грозят ссылки, обещающие бесплатное скачивание музыки и видео без регистрации, и кнопки, гласящие «нажми меня». Каждый должен попробовать хотя бы раз в жизни не скачать реферат из сети

Вопросы:

1. Назовите причины, по которым вы заходите в Интернет?
1. В каких сетях вы зарегистрированы?
2. Общаетесь ли вы с незнакомцами?
3. Был ли у вас какой-либо неприятный случай в школе или произошедший
4. с вами лично, связанный с Интернетом?
5. Считаете ли вы, что Интернет — это свободное пространство, в котором
6. по своему усмотрению можно делать все, что пожелаешь?
7. Как ты считаешь, вредит ли Интернет твоему физическому здоровью?
8. Как ты считаешь, вредит ли Интернет твоей морали?
9. Как ты считаешь, вредит ли Интернет твоему психическому здоровью?
10. Как ты считаешь, вредит ли Интернет твоему культурному уровню?

III. Рассказ об истории создания сети Интернет.

После запуска Советским Союзом искусственного спутника Земли в 1957 году, Министерство обороны США посчитало, что на случай войны Америке нужна надёжная система передачи информации. Агентство передовых исследовательских проектов США (ARPA) предложило разработать для этого компьютерную сеть. Разработка такой сети была поручена Калифорнийскому университету в Лос-Анджелесе, Стэнфордскому исследовательскому центру, Университету штата Юта и Университету штата Калифорния в Санта-Барбаре. Компьютерная сеть была названа ARPANET (англ. Advanced Research Projects Agency Network), и в 1969 году в рамках проекта сеть объединила четыре указанных научных учреждения, все работы финансировались за счёт Министерства обороны США. Затем сеть ARPANET начала активно расти и развиваться, её начали использовать учёные из разных областей науки.

Первый сервер ARPANET был установлен 1 сентября 1969 года в Калифорнийском университете в Лос-Анджелесе. Компьютер «Honeywell 516» имел 12 КБ оперативной памяти. К 1971 году была разработана первая программа для отправки электронной почты по сети, программа сразу стала очень популярна. В 1973 году к сети были подключены через трансатлантический телефонный кабель первые иностранные организации из Великобритании и Норвегии, сеть стала международной...

IV. Возможные опасности в сети и их предупреждение. Класс делится

на группы каждой группе предлагается сформулировать памятку по правилам работы в сети оформить в виде web-страницы.
Требование к созданию WEB-страниц
1.Установить фон.
2.Добавить название памятки
3.Добавить основные пункты памятки
4.Добавить кнопки следующая и предыдущая
5.Добавить фото или картинку из указанной папки
6. Сохранить документ в формате. html

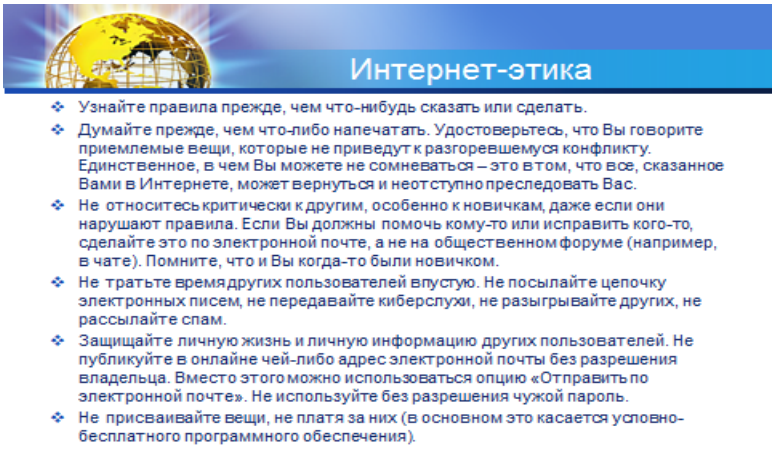
Г1. Правила безопасности при работе с сайтами и по приему почты

1. Не ходите на незнакомые сайты.
2. Если ходите, то выключайте (на всякий случай) поддержку языка Java и использование cookies.
3. Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на макровирусы.
4. Если пришел exe-файл, даже от знакомого, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину в вашей программе чтения почты. Бывали случаи рассылки вирусов. Вот недавно хакерами был вскрыт один из крупнейших узлов бесплатной почты Hotmail. Так что не исключено, что с адреса вашего знакомого придет вирус.
5. Не заходите на сайты, где предлагают бесплатный Интернет (не бесплатный e-mail, это разные вещи).
6. Никогда, никому не посылайте свой пароль.
7. Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв. А еще лучше создайте его специальной программой или попросите сделать это своего провайдера.

Г2.Правила Интернет этики

1.Узнайте правила прежде, чем что-нибудь сказать или сделать.
2.Думайте прежде, чем что-либо напечатать. Удостоверьтесь, что Вы говорите

приемлемые вещи, которые не приведут к разгоревшемуся конфликту. Единственное, в чем Вы можете не сомневаться – это в том, что все, сказанное
Вами в Интернете, может вернуться и неотступно преследовать Вас.
3.Не относитесь критически к другим, особенно к новичкам, даже если они нарушают правила. Если Вы должны помочь кому-то или исправить кого-то, сделайте это по электронной почте, а не на общественном форуме (например, в чате). Помните, что и Вы когда-то были новичком.
4.Не тратьте время других пользователей впустую. Не посылайте цепочку электронных писем, не передавайте киберслухи, не разыгрывайте других, не рассылайте спам.
5.Защищайте личную жизнь и личную информацию других пользователей. Не публикуйте в онлайне чей-либо адрес электронной почты без разрешения владельца. Вместо этого можно использоваться опцию «Отправить по электронной почте». Не используйте без разрешения чужой пароль.
5.Не присваивайте вещи, не платя за них (в основном это касается условно-бесплатного программного обеспечения).



Г3.Правила общение в Чатах
1. Не доверяйте никому вашу личную информацию.
2. Сообщайте администратору чата о проявлениях оскорбительного поведения
участников.
3. Если вам неприятно находиться в чате, покиньте его.
4. Если вам что-то не понравилось, обязательно расскажите об этом родителям.
5. Будьте тактичны по отношению к другим людям в чате.

Г4.Правила защиты компьютера от вредоносных программ

1. Постоянно обновляйте все программное обеспечение (включая веб-браузер), используя Центр обновления Microsoft.

2. Установите законное антивирусное и антишпионское программное обеспечение, такое как Microsoft Security Essentials.

3. Брандмауэр должен быть всегда включен.(Брандма́уэр Windows — встроенный в Microsoft Windows межсетевой экран. Появился в Windows XP SP2. Одним из отличий от предшественника (Internet Connection Firewall) является контроль доступа программ в сеть. Брандмауэр Windows является частью Центра обеспечения безопасности Windows.)

4. Не вставляйте неизвестные флеш-накопители (или USB-накопители) в свой компьютер. Если на них имеется вирус, этот вирус может заразить ваш компьютер.

5. Прежде чем открывать вложение или переходить по ссылке, приведенной в сообщении электронной почты, мгновенном сообщении или в социальной сети, убедитесь, что отправитель действительно отправлял сообщение.

6.Не переходите по ссылкам и не нажимайте кнопки во всплывающих сообщениях, которые кажутся подозрительными.

Г5.Правила защиты секретной личной информации

1.Прежде чем вводить секретные сведения в веб-форме или на веб-странице, обратите внимание на наличие таких признаков, как адрес веб-страницы, начинающийся с префикса https и значка в виде закрытого замка ( ) рядом с адресной строкой, который обозначает безопасное соединение.

2.Никогда не предоставляйте секретные сведения (такие как номер счета или пароль) в ответе на сообщение электронной почты, мгновенное сообщение или социальной сети.

3.Никогда не отвечайте на просьбы прислать деньги от «членов семьи», на предложения о сделке, которые слишком хороши, чтобы быть правдой, на сообщения о розыгрышах лотереи, в которых вы не участвовали, или другие мошеннические сообщения.

4.Придумайте пароли, представляющие собой длинные фразы или предложения и содержащие сочетание строчных, прописных букв, цифр и символов.

Используйте на разных сайтах разные пароли, особенно на тех, где хранится

финансовая информация.
5.С помощью нашего средства проверки паролей узнайте, насколько надежными являются ваши пароли.
6.Используйте закрытый профиль в социальных сетях. В таких службах, как Facebook и Twitter, чтобы настроить список пользователей, которые могут просматривать ваш профиль или фотографии, помеченные вашим именем, контролировать способы поиска информации и добавления комментариев о вас, а также узнать, как можно заблокировать некоторых пользователей.
7.Подходите избирательно к предложениям дружбы. Периодически анализируйте, кто имеет доступ к вашим страницам, а также просматривайте информацию, которую эти пользователи публикуют о вас.
Результат работы в группе- веб-страница определённого формата созданная в конструкторе сайтов FrontPage, для последующего создания электронного пособия в формате.exe.
V. Подведение итогов. Выступление групп. Защита памяток.
Рекомендуем посетить сайты:

VI. Выполнение тестирования с помощью системы опроса.

VII. Рефлексия. Представьте себе окно антивирусной программы Касперский.
Вы знаете, что цвет верхней части диалогового окна может менять цвет в зависимости от степени защищённости. У вас стикеры 3 цветов: красный – опасность, жёлтый – безопасность под угрозой, зелёный – защищённость. Пусть каждый из вас определит на сколько его защитят знания, полученные сегодня на уроке и приклеит соответствующий стикер на картинку с антивирусной программой. (*обучающиеся подходят к доске прикрепляют стикеры к картинке с антивирусом)*.
VIII. Вручение буклетов «Интернет БЕЗ опасностей».

АННОТАЦИЯ.

Данный классный час ориентирован на обучающихся 5-9 классов и может быть использовано учителями информатики. В начале урока проводится анкетирование «Интернет - зависимость». Занятие состоит из теоретической и практической части. Первая часть включает в себя ответы учащихся на поставленные вопросы, формулирование темы совместно с учащимися, рассказ учителя об опасностях сети Интернет и истории его создания. Формулируется план работы на уроке. Вторая часть носит практический характер. Детям предлагается разделиться на группы и сформулировать памятки для работы в сети, оформив их в виде web-страниц для дальнейшего создания электронного пособия. Заключительным этапом является выполнение теста и решения ситуационных задач по средством системы опроса, с последующим выводом результатов на экран, либо предлагается пойти тест, созданный редактором тестов. В конце занятия детям раздаются буклеты о правилах поведения в сети Интернет.