

Проект классного часа, посвященного вопросам безопасности использования компьютерных технологий и Интернет.

Аудитория: учащиеся 2-11 классов.

Содержание работы:

- Анкеты для учащихся.
- Материал беседы (выступления) для классного часа. Основные моменты, при желании, можно вынести на слайды презентации.
- Заготовка в Excel для оперативной обработки анкет с построением диаграмм, с возможностью демонстрации результатов анкетирования детей
- Материал для изготовления памяток.

Подготовка к классному часу:

1. Подготовка анкет для обучающихся. Анкетирование учащихся класса (анонимное), обработка анкет.
2. Подготовка памяток детям.
3. Подготовка мультимедийного компьютера с проектором и колонками для возможности демонстрации материалов.

дополнительно может быть сделано:

4. стенд, папки-раскладушки, папки с материалами по теме («Негативное воздействие компьютера на психическое здоровье детей», «Основы мобильной безопасности» и др. по материалам курсов).

Анкета для учащихся

А Н К Е Т А

Уважаемый участник анкетирования!

Ты окажешь помощь в исследовании «Интернет и школьники». Анкету подписывать не надо. Просим правдиво ответить на вопросы, отметив в каждом выбранный вариант ответа.

1. Сколько времени (в среднем) ты проводишь за компьютером (один вариант ответа):

- Менее 2 часов в неделю
- 2-3 раза в неделю по 1 час.
- Ежедневно, 0,5 – 1 час в день
- Ежедневно, 1-2 часа в день
- Ежедневно, 2-3 часа в день
- Ежедневно, 3-4 часа в день
- Ежедневно, более 4 часов

2. Сколько времени (в среднем) ты проводишь в сети Интернет, включая с iPhone, iPad и др. (один вариант ответа):

- Менее 2 часов в неделю
- 2-3 раза в неделю по 1 час.
- Ежедневно, 0,5 – 1 час в день
- Ежедневно, 1-2 часа в день
- Ежедневно, 2-3 часа в день
- Ежедневно, 3-4 часа в день
- Ежедневно, более 4 часов

3. Интернет для тебя (можно выбрать несколько вариантов):

- Ведение страницы, дневника, блога

- Поиск информации для подготовки к урокам, экзаменам
 - Общение в чате, на форуме, личная переписка
 - Книги в электронном виде
 - Музыка
 - Просмотр фильмов
 - Он-лайн игры
4. Что ты думаешь о правилах этикета в Интернете (один вариант ответа):
- Интернет - пространство свободное от правил
 - В особых случаях надо соблюдать правила этикета
 - Да, как и в реальной жизни
5. Как ты понимаешь «безопасный Интернет» (можно выбрать несколько вариантов):
- защита от вирусов, вредоносных программ
 - соблюдение интернет-этикета
 - защита от взлома личной информации
 - защита от спама и нежелательной информации
 - безопасность при навигации по сайтам и скачиванию файлов
 - соблюдение осторожности при общении с незнакомыми людьми

Проведение классного часа

1. Объявление темы классного часа.

2. Демонстрация социального ролика «Безопасный интернет - детям!» с сайта «Первый психологический портал г. Пятигорска, раздел «Медиатека», «Безопасность детей в интернете - подборка материалов»
- <http://5psy.ru/raznoe/bezopasnost-deteie-v-internete-podborka-materialov.html>

3. Постановка проблемных вопросов.

"Ребенок дома, за компьютером - значит, все в порядке, он в безопасности". Так считают многие родители. И ошибаются. Детей эры поисковых систем и социальных сетей опасности подстерегают не только на улице. Через мониторы компьютеров угроз на них обрушивается отнюдь не меньше.

Сегодня мы ответим для себя на такие вопросы:

- Всегда ли полезны современные технологии?
- Какие опасности ждут наших детей в Интернет?
- Как уберечь наших детей от этих опасностей?

4. **Всегда ли полезны современные технологии?** Отвечая на этот вопрос, каждый, наверняка, сможет перечислить массу преимуществ, которые так щедро предоставили нам Интернет и мобильная связь. И, несомненно, будет прав. Интернет для активного пользователя - это в большей степени информационная база и электронная библиотека.

Но можно ли быть уверенным, что свободный доступ к столь разнообразной информации не окажется опасным?

Многие уже сталкивались в Интернете с нежелательной информацией (например, экстремистского, порнографического, рекламного содержания) и с заражением компьютера вирусами.

Большинство респондентов (88%) проведенного компанией «Билайн» исследования в 2010 году в пяти крупнейших городах России (Москве, Санкт-Петербурге, Нижнем Новгороде, Екатеринбурге, Новосибирске) вкладывали в понятие "безопасный Интернет" защиту от вирусов, вредоносных программ, 70% - защиту от взлома личной информации,

54% - защиту от спама, и практически половина (45%) опрошенных понимала "безопасный Интернет" как защиту детей от нежелательной информации.

Интернет-грамотность важна для любого современного человека, и в особенности для детей. Интернет-грамотность это не только умение осуществить поиск информации и пользоваться важнейшими сетевыми ресурсами, но и осведомленность об угрозах безопасности в Интернете. Большинство из нас предпочитает использовать базовые средства безопасности, и при этом считают, что обеспечивать безопасность в Интернете самостоятельно довольно сложно. Проблемы зачастую решают по мере поступления. В качестве основного средства обеспечения своей безопасности используют антивирусные программы.

Тем не менее, количество негативных интернет-ресурсов ежедневно растёт. По данным Генпрокуратуры РФ, хотя работа в этом направлении и ведется, в настоящее время насчитывается более нескольких тысяч террористических сайтов, где в подробностях учат, как сделать взрывчатку или совершить теракт. Можно утверждать, что дети впервые сталкиваются с порно, как только начинают пользоваться Интернетом. Не заставляют ждать своего появления и новые интернет-угрозы.

Дети, часто не задумываясь, рассказывают своим онлайн-друзьям, где они живут или по какому графику работают их родители, отправляют дорогостоящие SMS мошенникам и часами сидят в социальных сетях, что не может не сказаться на их психическом и физическом здоровье. Кроме того, в последнее время участились случаи преследования и запугивания детей через различные интернет-сервисы.

Детская аудитория Рунета насчитывает сейчас 8-10 млн. пользователей – детей до 14 лет. При этом некоторые дети, регулярно посещающие Сеть, просматривают Интернет-сайты с агрессивным и нелегальным контентом, подвергаются киберпреследованиям и виртуальным домогательствам. По данным нескольких опросов, в среднем, каждый второй подросток сталкивался с унижениями и оскорблениями в Сети.

В таких условиях вопрос защиты детей должен стать неотъемлемой частью родительской заботы, и рано или поздно каждый родитель задаётся вопросом, как надёжно защитить своих детей в Интернете, вне зависимости от их возраста и уровня компьютерной грамотности.

Возможные опасности, с которыми сопряжен доступ детей к Интернету:

- Неприемлемые материалы. В Интернете ребенок может столкнуться с материалами, связанными с сексом, провоцирующими возникновение ненависти к кому-либо или побуждающими к совершению опасных либо незаконных действий.
- Неприятности, связанные с нарушением законов или финансовыми потерями. У ребенка могут обманым путем узнать номер вашей кредитной карточки, и это вызовет финансовые потери. Ребенка также могут склонить к совершению поступков, нарушающих права других людей, что, в конечном счете, приведет к возникновению у вашей семьи проблем, связанных с нарушением законов.
- Разглашение конфиденциальной информации. Детей и даже подростков могут уговорить сообщить конфиденциальную информацию. Сведения личного характера, такие как имя и фамилия ребенка, его адрес, возраст, пол, и информация о семье могут легко стать известными злоумышленнику. Даже если сведения о вашем ребенке запрашивает заслуживающая доверия организация, вы все равно должны заботиться об обеспечении конфиденциальности этой информации.
- Дети могут быть подвержены притеснениям со стороны других пользователей Сети (чаще всего злоумышленниками оказываются другие дети), которые грубо ведут себя в Интернете, пишут оскорбления и угрожают. А также дети могут стать жертвой киберманьяков, ищущих личной встречи с ребенком.

- Проблемы технологического характера. По недосмотру ребенка, открывшего непонятное вложение электронной почты или загрузившего с веб-узла небезопасный код, в компьютер может попасть вирус, “червь”, “троянский конь” или другой код, разработанный со злым умыслом.

5. Правила безопасного пользования Сетью.

Некоторым родителям Интернет представляется местом более опасным, чем реальная темная улица рядом с домом. Но Интернет не только источник угроз, он открывает большие возможности для общения и саморазвития. Полезнее будет энергию, которая тратится на это беспокойство, перевести в активную и осмысленную заботу о том, чтобы ребенок с первых шагов в Интернете мог чувствовать себя уверенно и постепенно научился быть осторожным и защищаться от нежелательного влияния.

Чтобы Интернет приносил пользу, а не вред, родителям необходимо научить детей правилам безопасного пользования Сетью так же, как они учат их не переходить дорогу на красный свет светофора. Примерно до 12 лет можно достаточно жестко контролировать поведение ребенка в сети (например, ограничивать список сайтов, которые он может посещать), а с подростком нужно будет скорее договариваться о том, как он будет соблюдать правила безопасности, и полагаться на его доверие.

Первое, что необходимо сделать, — это объяснить детям, что нахождение в Интернете во многом напоминает пребывание в общественном месте. В Интернете не водятся каких-то особенных, «компьютерных» преступников – они те же, что могут встретиться ребенку на улице, в магазине, в кинотеатре. Многие опасности, подстерегающие пользователя Интернета, очень схожи с риском, возникающим при общении с чужими людьми, и дети должны понимать, что, если они не знают человека, с которым вступили в контакт, лично, это означает, что они общаются с незнакомцем, что запрещено и в реальной, а не только в виртуальной действительности. Не стоит ребенку рассказывать в подробностях, кто такие педофилы или что такое мошенничество с платежными средствами, – достаточно кратко объяснить, что некоторые люди в силу психического нездоровья или плохого воспитания могут нанести серьезный вред здоровью ребенка, бюджету семьи, безопасности и спокойствию вашей жизни. Даже если ребенок не поймет в точности, чего ему следует опасаться, он может почувствовать ваше беспокойство и заботу о нем, и с готовностью будет делать то, что вы попросите. Четко объясните детям, посещение каких веб-узлов является приемлемым и какими правилами нужно руководствоваться при пользовании Интернетом. Приведите ясные и наглядные примеры того, что следует искать, и убедитесь в том, что дети обратятся к вам, если столкнутся с не внушающими доверия или смущающими их материалами.

Определите правила, по которым в вашей семье принято пользоваться Интернетом. При этом должны быть упомянуты права и обязанности каждого члена семьи. Установите компьютер в помещении, используемом всеми членами семьи, а не в комнате ребенка. Это упростит контроль за пребыванием детей в Интернете. Ваши преимущественные права (например, проверять его почту или журнал посещений страниц) вы можете объяснить ребенку по аналогии с правами администратора сайта: он тоже имеет право отслеживать поведение посетителей сайта и принимать меры предосторожности.

Составьте список того, что можно и чего нельзя делать любому члену вашей семьи при использовании Интернета. Например: Нельзя разглашать информацию личного характера. Объясните детям, что они не должны сообщать свою фамилию, адрес, номер телефона или давать свою фотографию. Ребенок ни в коем случае не должен соглашаться на личную встречу с “виртуальным” другом без разрешения и присутствия родителей. Нельзя ничего покупать через веб-узел, деятельность которого осуществляется через небезопасный сервер. Перед тем как совершить покупку, необходимо всегда спрашивать разрешения взрослых.

Предупредите детей о том, что они не должны никому сообщать свои пароли, даже если человек утверждает, что является сотрудником вашего поставщика Интернет-услуг

(например, представляется вашим провайдером). Поставщик услуг Интернета никогда не будет спрашивать, какой у вас пароль.

Следует либо не допускать использования ребенком чата, либо контролировать это занятие. Кроме того, нужно убедиться в том, что выбранный им чат является управляемыми и поддерживается заслуживающей доверия компанией или организацией.

Настройте веб-обозреватель в режиме обеспечения безопасности. Регулярно просматривайте журнал веб-обозревателя. Из него вы узнаете, какие веб-узлы посещали ваши дети, и как часто они это делали. Контролируйте входящие и исходящие сообщения электронной почты своего ребенка. Знакомьтесь с его “виртуальными” друзьями подобно тому, как вы знакомитесь с “реальными”.

Эти простые меры, а также доверительные беседы с детьми о том, каких правил им следует придерживаться при использовании Интернета, позволят вам чувствовать себя спокойно, отпуская ребенка в познавательное и безопасное путешествие по Всемирной сети.

Памятка для детей:

Это важно знать!

- Я не скажу о себе ничего (ни адреса, ни телефона, ни других сведений) без разрешения родителей.
- Я никогда не передам по Интернет своей фотографии.
- Я никогда не встречу ни с кем, кого знаю только по Интернет, без разрешения родителей. На встречу я пойду с отцом или с матерью.
- Я никогда не отвечу на сообщение, которое заставляет меня краснеть, будь то электронное письмо или общение в чате.
- Я буду разговаривать об Интернет с родителями.
- Я буду работать только тогда, когда они разрешат мне, и расскажу им обо всем, что я делал в Интернет.

(Эти правила составлены на основании статьи Л. Дж. Меджида <http://www.ncmec.org/>)

Безопасность при хождении по сайтам и по приему электронной почты:

- Не ходите на незнакомые сайты.
- Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на макровирусы.
- 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.
- Не заходите на сайты, где предлагают бесплатный Интернет (не бесплатный e-mail, это разные вещи.)
- Никогда никому не посылайте свой пароль.
- Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв.

6. **Практическая часть. Демонстрация возможностей** Windows и Internet Explorer (как наиболее распространенных в домашнем пользовании) и **установки** какой-нибудь программы «родительского контроля».

Полезными могут быть также:

- Программа для родительского контроля М.Негодова NetPolice Lite - http://www.pc-user.ru/view_post.php?id=40 .
- Программное приложение родительского контроля от Norton - <http://ru.norton.com/norton-family-premier/> .
- Программное приложение Time Boss родительского контроля от Nicekit - <http://nicekit.ru/parental-control/time-boss.php>.

7. **Представление результатов анкетирования** (анкеты родителей, как и детей, уже собраны и обработаны).

Анализ результатов, сравнение, обсуждение.

8. **Подведение итогов родительского собрания.** Рефлексия (устно).

Полезные ссылки:

1. <http://www.scrf.gov.ru/documents/90.html> - Совет безопасности РФ.
2. <http://www.saferinternet.ru/> - Портал Российского Оргкомитета по проведению Года Безопасного Интернета.
3. http://www.pushkinlib.spb.ru/safetyinternet_link.html - электронные ресурсы для детей и родителей по безопасной работе в Интернет.
4. http://www.kaspersky.ru/keeping_children_safe Интернет и дети. А также программное приложение от Лаборатории Касперского - <http://support.kaspersky.ru> .

=====

Материал для памяток

Основные правила для школьников младших классов

Вы должны это знать:

- Всегда спрашивайте родителей о неизвестных вещах в Интернете. Они расскажут, что безопасно делать, а что нет.
- Прежде чем начать дружить с кем-то в Интернете, спросите у родителей как безопасно общаться.
- Никогда не рассказывайте о себе неизвестным людям. Где вы живете, в какой школе учитесь, номер телефона должны знать только ваши друзья и семья.
- Не отправляйте фотографии людям, которых вы не знаете. Не надо чтобы неизвестные люди видели фотографии Вас, Ваших друзей или Вашей семьи.
- Не встречайтесь без родителей с людьми из Интернета вживую. В Интернете многие люди рассказывают о себе неправду.
- Общаясь в Интернете, будьте дружелюбны с другими. Не пишите грубых слов, читать грубости так же неприятно, как и слышать. Вы можете нечаянно обидеть человека.
- Если вас кто-то расстроил или обидел, обязательно расскажите родителям.

Основные правила для школьников средних классов

Вы должны это знать:

- При регистрации на сайтах, старайтесь не указывать личную информацию, т.к. она может быть доступна неизвестным людям. Так же, не рекомендуется размещать свою фотографию, давая, тем самым, представление о том, как вы выглядите, посторонним людям.
- Используйте веб-камеру только при общении с друзьями. Проследите, чтобы посторонние люди не имели возможности видеть ваш разговор, т.к. он может быть записан.
- Нежелательные письма от неизвестных людей называются «Спам». Если вы получили такое письмо, не отвечайте на него. В случае, если Вы ответите на подобное письмо, отправитель будет знать, что вы пользуетесь своим электронным почтовым ящиком и будет продолжать посылать вам спам.
- Если вам пришло сообщение с неизвестного адреса, его лучше не открывать. Подобные письма могут содержать вирусы.
- Если вам приходят письма с неприятным и оскорбляющим вас содержанием, если кто-то ведет себя в вашем отношении неподобающим образом, сообщите об этом.

- Если вас кто-то расстроил или обидел, расскажите все взрослому.

Основные правила для школьников старших классов

Вы должны это знать:

- Не желательно размещать персональную информацию в Интернете.
- Персональная информация — это номер вашего мобильного телефона, адрес электронной почты, домашний адрес и фотографии вас, вашей семьи или друзей.
- Если вы публикуете фото или видео в интернете — каждый может посмотреть их.
- Не отвечайте на Спам (нежелательную электронную почту).
- Не открывайте файлы, которые прислали неизвестные Вам людей. Вы не можете знать, что на самом деле содержат эти файлы – в них могут быть вирусы или фото/видео с «агрессивным» содержанием.
- Не добавляйте незнакомых людей в свой контакт лист в IM (ICQ, MSN messenger и т.д.).
- Помните, что виртуальные знакомые могут быть не теми, за кого себя выдают.
- Если рядом с вами нет родственников, не встречайтесь в реальной жизни с людьми, с которыми вы познакомились в Интернете. Если ваш виртуальный друг действительно тот, за кого он себя выдает, он нормально отнесется к вашей заботе о собственной безопасности!
- Никогда не поздно рассказать взрослым, если вас кто-то обидел.

Основные правила для учителей и преподавателей

Чтобы помочь учащимся, Вы должны это знать:

- Подготовьтесь. Изучите технику безопасности в Интернете, чтобы знать виды Интернет — угроз, уметь их распознать и предотвратить. Выясните, какими функциями обладают компьютеры подопечных, а так же какое программное обеспечение на них установлено.
- Прежде чем позволить ребенку работу за компьютером, расскажите ему как можно больше о виртуальном мире, его возможностях и опасностях.
- Не позволяйте детям самостоятельно исследовать Интернет-пространство, они могут столкнуться с агрессивным контентом.
- Выберите интересные ресурсы и предложите детям изучить их вместе.
- Убедитесь, что на компьютерах установлены и правильно настроены средства фильтрации контента, спама и антивирусы.

Инструкция по безопасному общению в чатах и Интернет-этика.

Каждый должен помнить о внутренних правилах переписки в Интернет.

- Узнайте правила чата или форума прежде, чем что-нибудь сказать или сделать.
- Не доверяйте никому вашу личную информацию.
- Нельзя отклоняться от темы разговора на форуме.
- Будьте тактичны по отношению к другим людям в чате или форуме. Думайте прежде, чем что-либо напечатать. Нельзя печатать ЗАГЛАВНЫМИ БУКВАМИ, что может рассматриваться как крик, провоцирующий спор или конфликт
- 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. Помните, что и Вы когда-то были новичком.
- Нельзя размещать ложную информацию или грубые высказывания о другом человеке.
- Не тратьте время других пользователей впустую. Не посылайте электронную почту рекламного содержания, не передавайте киберслухи, не разыгрывайте других, не рассылайте спам.
- Сообщайте администратору чата о проявлениях оскорбительного поведения участников.
- Если вам неприятно находиться в чате, покиньте его.
- Если вам что-то не понравилось, обязательно расскажите об этом родителям.

- Не присваивайте вещи, не платя за них (в основном это касается условно-бесплатного программного обеспечения).
- Нельзя отправлять большие вложенные файлы, не спросив разрешения у получателя.