

Содержание

Аннотация наставника

Введение	2
1.Теоретическая часть	
1.1 Безопасный Интернет	3
1.2. Классификация интернет угроз	4
2.Практическая часть	
2.1. Способы защиты от Интернет-угроз	7
Заключение	11
Список литературы	12

Введение.

К выбору данной темы работы нас натолкнули недавно нашумевшие игры в социальных сетях.

Мне стало интересно, а можно ли защитить себя и своих друзей от таких игр, от агрессивного и нелегального контента? Как сделать Интернет безопасным для детей и подростков? Ведь многие дети, регулярно посещают социальные сети, просматривают Интернет. Данная работа посвящается вопросам безопасного интернета дома для детей и их родителей.

В Контакте, Мой мир, You Tube - знаменитые сайты, социальные сети постепенно начинают проживать с нами всё больше и больше времени. Мы сами не замечаем, как уже автоматически кликаем на очередную ссылку, регистрируемся на новом сайте и придумываем логин для еще одного форума. Интернет является прекрасным источником для новых знаний, помогает в учебе, занимает досуг. Но так ли он безобиден?

Цель работы:

- знакомство с интернет угрозами и правилами безопасной работы в сети Интернет

Задачи:

- изучить скрытые и открытые угрозы интернета;
- проанализировать классификацию интернет – угроз
- выделить способы защиты от интернет угроз;
- подготовить материал о том, что должны знать дети, родители, чтобы интернет стал безопасным;
- подготовить и провести анкетирование учащихся нашей школы по данному вопросу;
- структурировать меры безопасного интернета при работе детей за компьютером в школе и дома.

1.1. Безопасный Интернет

В настоящее время Интернет стал неотъемлемой частью повседневной жизни, бизнеса, политики, науки и образования. Использование Интернета дома и в образовательных учреждениях позволяет повысить эффективность обучения, а так же получать свежие новости в интересующей области не только родителям и педагогам, но и учащимся, в том числе школьникам.

Однако, бурное развитие Интернета несет также существенные издержки. Современная научно-образовательная информационная среда характеризуется большим количеством образовательных ресурсов с неструктурированной и мало того, еще и не всегда достоверной информацией. Таким образом, неуклонно возрастает потребность в обеспечении эффективного использования информационных научно-образовательных ресурсов. Кроме того, наряду с полезной и необходимой информацией пользователи сталкиваются ресурсами, содержащими неэтичный и агрессивный контент. Порнография, терроризм, наркотики, националистический экстремизм, маргинальные секты, неэтичная реклама и многое другое-яркие примеры контента, с которыми могут соприкоснуться дети и подростки.

Бесконтрольное распространение нежелательного контента противоречит целям образования и воспитания молодежи. Отказываться от благ информационных технологий бессмысленно, но бесконтрольный доступ детей к интернету может привести к:

- Киберзависимости
- Заражению вредоносными программами при скачивании файлов
- Нарушению нормального развития ребенка
- Неправильному формированию нравственных ценностей
- Знакомству с человеком с недобрыми намерениями.

1.2. КЛАССИФИКАЦИЯ ИНТЕРНЕТ-УГРОЗ

Контентные риски

Контентные риски связаны с потреблении информации, которая публикуется в Интернете и включает в себя незаконный и непредназначенный для детей (неподобающий) контент.

• **Неподобающий контент**

В зависимости от культуры , законодательства, менталитета и указанного возраста согласие в стране определяется группа материалов, считающихся неподобающими. Неподобающий контент включает в себя материалы, содержащие: насилие, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр и наркотических веществ.

• **Незаконный контент**

В зависимости от законодательства страны разные материалы могут считаться нелегальными. В большинстве стран запрещены : материалы сексуального характера с участием детей и подростков , порнографический контент ,описания насилия , в том числе сексуального, экстремизм и разжигание расовой ненависти.

• **Электронная безопасность**

Риски, связанные с электронной безопасностью, относятся к различной кибер деятельности, которая включает в себя: разглашение персональной информации, выход в сеть с домашнего компьютера с низким уровнем защиты (риск подвергнуться вирусной атаке), онлайн - мошенничество и спам.

• **Вредоносные программы**

Вредоносные программы- это программы , негативно воздействующие на работу компьютера.К ним относятся вирусы, программы-шпионы, нежелательное рекламное ПО.

• Спам

Спам — это нежелательные электронные письма, содержащие рекламные материалы . Спам дорого обходится для получателя , так как пользователь тратит на получение большого количества писем свое время и оплаченный интернет-трафик. Также нежелательная почта может содержать, в виде самозапускающихся вложений , вредоносные программы.

• Кибермошенничество

Кибермошенничество-это один из видов киберпреступления ,целью которого является обман пользователей . Хищение конфиденциальных данных может привести к тому , что хакер незаконно получает доступ и каким — либо образом использует личную информацию пользователя, с целью получить материальную прибыль . Есть несколько видов кибермошенничества: нигерийские письма, фишинг, вишинг и фарминг.

Коммуникационные риски

Коммуникационные риски связаны с межличностными отношениями интернет-пользователей и включает в себя контакты педофилов с детьми и киберпреследования.

• Незаконный контакт

Незаконный контакт- это общение между взрослым и ребенком, при котором взрослый пытается установить более близкие отношения для сексуальной эксплуатации ребенка.

• Киберпреследования

Киберпреследование — это преследование человека сообщениями, содержащими оскорбления, агрессию, сексуальные домогательства с помощью интернет-коммуникаций.

Также, киберпреследование может принимать такие формы, как обмен информацией, контактами или изображениями, запугивание, подражание, хулиганство (интернет-троллинг) и социальное *байкотирование*.

Электронные риски

Электронные риски — это возможность столкнуться с хищением персональной информации, риск подвергнуться вирусной атаке, онлайн-мошенничеству, спам-атаке, шпионским программам и т.д. Вредоносное ПО (Программное Обеспечение) использует широкий спектр методов для распространения и проникновения в компьютеры, не только через компакт-диски или другие носители, но и через электронную почту посредством спама или скачанных из Интернета файлов.

- **вирусы, черви и «троянские кони»** – это компьютерные программы, которые могут нанести вред вашему семейному компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными с Интернетом и даже использовать ваш компьютер для распространения своих копий на компьютеры ваших друзей, родственников, коллег и по всей остальной глобальной Сети. Защита в социальных сетях — это задача, которая не так давно стала актуальна для их пользователей. Буквально несколько месяцев назад, взлом страниц в социальных сетях превратился в один из основных способов распространения спама в Интернете.
- **Мошенничество в сети Интернет (кибермошенничество)** — один из видов киберпреступления, целью которого является обман пользователей. Хищение конфиденциальных данных может привести к тому, что хакер незаконно получает доступ и каким-либо образом использует личную информацию пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.), с целью причинить материальный и финансовый ущерб.

Потребительские риски.

Потребительские риски – злоупотребление в интернете правами потребителя. Включают в себя: риск приобретения товара низкого качества, различные подделки, контрафактная и фальсифицированная продукция, потеря денежных средств без приобретения товара или услуги, хищение персональной информации с целью кибер-мошенничества, и др. Также дети, зачастую совершая онлайн покупки, могут растратить значительные суммы своих родителей, если каким-либо способом имели или получили к ним доступ. Одним из самых распространенных видов данного типа рисков является мошенничество — это умышленный обман или злоупотребление доверием с целью получения какой-либо выгоды.

Мошенничество, как правило, является преступлением. Поскольку мошенничество в сети интернет совершается с помощью различных технических средств и разнообразного количества программ, то некоторые его виды могут быть отнесены и к группе электронных рисков, а часть к группе коммуникационных, поскольку включает в свою схему установления более близкого контакта с жертвой в течение какого-либо времени (например, с помощью электронных писем и смс, которые могут привести и к реальным встречам с мошенниками).

2.1. Способы защиты от Интернет-угроз

Комплексное решение в области использования сети Интернет

Опираясь на мировой опыт и анализируя ситуацию в России можно сказать, что решение вопроса по обеспечению безопасного использования Интернет представляет комплексное решение.

Оно включает в себя:

Административные (нормативно-правовые) меры, которые обеспечивает государство посредством создания (изменения) законопроектов. Воспитание и обучение пользователей эффективной работе с информацией, которым занимаются специальные ресурсы. Обучением работе в Интернете детей должны так же заниматься родители и педагоги. Использование современных технологических решений в области повышения эффективности использования Интернет. Разработкой специального программного обеспечения занимаются частные компании.

Правила безопасной работы в Интернет

Родителям

Чтобы помочь своим детям, вы должны это знать:

- Будьте в курсе того, чем занимаются ваши дети в Иинтернете. Попросите их научить Вас пользоваться различными приложениями, которые Вы не использовали ранее.
- Помогите своим детям понять, что они не должны предоставлять никому информацию о себе в интернете — номер мобильного телефона, домашний адрес, название и номер школы, а так же показывать свои фотографии и своей семьи, ведь любой человек в Интернете может это увидеть.
- Если ваш ребенок получает спам (нежелательную информацию), напомните ему, чтобы он не верилнаписанному в письмах и ни в коем случае не отвечал на них.
- Объясните детям, что нельзя открывать файлы, присланные от неизвестных Вам людей. Эти файлы могут содержать вирусы или фото 9видео0 с агрессивным содержанием.
- Помогите ребенку понять, что некоторые люди в Интернете могут говорить неправду и быть не теми, за кого себя выдают. Дети никогда не должны встречаться с сетевыми друзьями в реальной жизни самостоятельно без взрослых.
- Постоянно общайтесь со своими детьми. Никогда не поздно рассказать своему ребенку, как правильно поступать и реагировать на действия других людей в Интернете.
- Научите своих детей как реагировать в случае, если их кто-то обидел или они получили

агрессивный контекст с Интернета. Так же расскажите, куда обращаться в подобном случае.

- Убедитесь, что на компьютере установлены и правильно настроены средства фильтрации.

Полезные программы

Программа «**Интернет Цензор**» устанавливается на ПК и обеспечивает фильтрацию всех интернет-браузеров и программ. Отличительной особенностью полной версии является высокий уровень надежности и защиты от взлома.

Net Police Lite. Облегченная версия персонального фильтра, который представляет собой важные функции для ограничения доступа пользователей к негативным, нежелательным и опасным Интернет-ресурсам. Поддерживаются самые необходимые категории и функции для безопасного пользования сетью Интернет.

Детям и подросткам

Школьникам младших классов

Если ты любишь сидеть в Интернете, запомни эти правила безопасности!

Правило 1.

Не указывай настоящее имя и фамилию. Придумай себе НИК.

Правило 2.

Не размещай на сайтах свои фотографии. Пользуйся аватаркой или картинками.

Правило 3.

Не говори никому свой адрес или номер телефона. Общайся только в Интернете.

Правило 4.

Не встречайся с людьми, которых ты знаешь только по Интернету. Если кто-то приглашает тебя встретиться или оскорбляет тебя — срочно расскажи об этом родителям.

Школьникам средних классов

Вы должны это знать:

- При регистрации на сайтах, не старайтесь указывать личную информацию, так как она может быть доступна незнакомым 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, так как он может быть записан.

- Нежелательные письма от незнакомых 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 незнакомого 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 взрослому.

Школьникам старших классов

Вы должны это знать:

- Не желательно размещать персональную информацию в Интернете. Это номер вашего мобильного телефона, адрес электронной почты, домашний адрес и фотографии вас,
- Если вы публикуете фото или видео в Интернете — каждый может посмотреть их.
- Не отвечайте на спам (нежелательную почту).
- Не открывайте файлы, которые прислали неизвестные вам люди. 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.
- Помните, что виртуальные люди 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 кто-то обидел вас!

Учителям и преподавателям

Чтобы помочь учащимся, вы должны это знать:

- Подготовьтесь. Изучите технику безопасной работы в Интернете, чтобы знать виды Интернет-угроз, уметь их распознавать и предотвращать. Выясните, какими функциями обладают компьютеры подопечных вам учащихся, а так же, какое программное обеспечение на них установлено.
- Прежде чем позволять ребенку работу за компьютером, расскажите ему как можно больше о

виртуальном мире, его возможностях и опасностях.

- Не позволяйте детям самостоятельно исследовать Интернет-пространство, так как они могут столкнуться с агрессивным контекстом.
- Выберите интересные ресурсы и предложите детям вместе их изучить.
- Убедитесь, что на компьютерах установлены и правильно настроены средства фильтрации контекста, спама и антивирусные программы.

Использование Интернет является безопасным, если выполняются три основных правила:

1. Защитите свой компьютер:

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

2. Защитите себя в Интернете:

- С осторожностью разглашайте личную информацию.
- Думайте о том, с кем разговариваете.
- Помните, что в Интернете не вся информация надежна и не все пользователи откровенны.

3. Соблюдайте правила:

- Закону необходимо подчиняться даже в Интернете.
- При работе в Интернете не забывайте заботиться об остальных так же, как о себе.

Заключение

Современная научно-образовательная информационная среда характеризуется большим количеством образовательных ресурсов с неструктурированной и мало того, еще и не всегда достоверной информацией. Объем подобных ресурсов растет в геометрической прогрессии. Таким образом, неуклонно возрастает потребность в обеспечении эффективного использования информационных научно-образовательных ресурсов.

Кроме того, наряду с полезной и необходимой информацией пользователи сталкиваются ресурсами, содержащими неэтичный и агрессивный контент. Порнография, терроризм, наркотики, националистический экстремизм, маргинальные секты, неэтичная реклама и многое другое — яркие примеры контента, с которым могут соприкоснуться дети и подростки.

Бесконтрольное распространение нежелательного контента противоречит целям образования и воспитания молодежи. Отказываться от благ информационных технологий бессмысленно, но бесконтрольный доступ детей к Интернету может привести к скрытым угрозам.

Список использованных источников информации:

1. Левский Н.А. Чего опасаться в Интернете. Самые опасные сайты. Вредоносные программы. [Электронный ресурс] // Журнал ComputerBild – 2013, - Режим доступа - <http://www.windxp.com.ru/acpeg.htm> , свободный.
2. Добреля Т.В. Чего опасаться в Интернете [Электронный ресурс] / Тимофей В. Добреля – 2013, Режим доступа - <http://tim-plus.ru/opasnost-v-internete-i-kak-ee-izbezhat.html>, свободный.
3. Дергунова О.К. Безопасность детей в Интернете. [Электронный ресурс] // Книга «Безопасность детей в Интернете» - 2006 – Режим доступа - www.ifap.ru/library/book099.pdf , свободный.
4. [Памятка для родителей](#)
5. <http://www.microsoft.com/rus/athome/security/children/backtoschool.msp> - сайт корпорации Microsoft, посвященный проблемам безопасности в сети Интернет.
6. <http://stopcrack.narod.ru/> - сайт посвящен всем тем, кто интересуется проблемами компьютерной безопасности в интернет.
7. http://www.compdoc.ru/secur/internet/securpolicy/glava5_2.shtml - сайт посвящен Политике безопасности.