Муниципальное бюджетное общеобразовательное учреждение

«Средняя общеобразовательная школа № 65»

Научно-исследовательская работа по информатике

Безопасный Интернет дома

Выполнила учащаяся 7 «В» класса
Бабошина Софья Леонидовна.
Научный руководитель
Пискунова Елизавета Сергеевна,
учитель информатики.

Г. Кемерово, 2018 г.

Оглавление

1. ВВЕДЕНИЕ

Данная работа посвящается вопросам безопасного интернета дома для детей и их родителей. При этом многие дети, регулярно посещают Сеть, просматривают Интернет-сайты с агрессивным и нелегальным контентом, подвергаются кибепреследованиям и виртуальным домогательствам. Как сделать Интернет безопасным для детей?

В Контакте. Мой мир. You Tube. Они у всех на слуху. 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. Как обезопасить себя в Интернете?

Объектом исследования является выявление способов защиты от интернет угроз при работе за компьютером дома.

Предметом исследования является безопасная деятельность в интернете и способы защиты от интернет угроз.

Цель работы:

Определить насколько осведомлены учащиеся и родители о безопасном использовании ресурсов в сети Интернет, дать рекомендации по соблюдению правил безопасной работы в Интернете дома.(в период занятости учащихся после школы, пока родители еще на работе)

Гипотеза: при условии выполнения минимальных рекомендаций по сохранению здоровья при работе за компьютером в школе и дома можно будет избежать возникновению последствий интернет-угроз.

В соответствии с целью исследования и выдвинутой гипотезой были поставлены следующие **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.

Основными методами исследования являются: теоретический анализ научной и методической литературы; отбор информации; анализ; обобщение; описание.

Пока мы спорим "пущать" или "не пущать" учеников школы в Интернет - они уже здесь. Мы снова опоздали. Очевидно, что сейчас невозможно гарантировать стопроцентную защиту детей от нежелательного контента. Никакие фильтры никогда такой гарантии не дадут. Но мы можем формировать у ребят навык "безопасного" поведения в Интернете.

2. ОСНОВНАЯ ЧАСТЬ.

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. 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 материал. Порнография, терроризм, наркотики, националистический экстремизм, маргинальные секты, неэтичная реклама и многое другое — яркие примеры материала, с которым могут соприкоснуться дети и подростки. Бесконтрольное распространение нежелательного материала противоречит целям образования и воспитания молодежи.

2.1 Классификация интернет-угроз

- **Контентные риски**

Контентные риски связаны с потреблением 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 узаконенного возраста согласия 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 кибердеятельности, 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 и различные формы вредоносных кодов.

- Вредоносное ПО - Рекламное ПО - Шпионское ПО - Браузерный эксплойт

Спам

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

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. подробнее

• Коммуникационные риски

Коммуникационные риски связаны с межличностными отношениями интернет-пользователей и включают 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 бойкотирование.

Еще с первого сентября в России вступил в силу закон, согласно которому должен быть закрыт доступ в Интернет несовершеннолетним гражданам РФ через wi-fi.

Предполагается, что в домашних условиях за безопасное использование детьми Интернета несут ответственность родители и заботятся о том, чтобы ребенку были недоступны сайты с вредоносным содержанием.

Теперь, в соответствии с законом, должно быть строго ограничено распространение информации, которая нежелательна для подростков. Видео, аудио и текстовая информация, содержащая нецензурные выражения, пропаганду насилия, жестокости, алкоголя, сигарет и наркотиков не должна быть доступна несовершеннолетним.

Но, по словам экспертов, несмотря на правильность и целесообразность такого решения, его техническое выполнение очень затруднительно. Вся ответственность и заботы по внедрению этого документа в жизнь ложится на

плечи заказчика услуг. Не провайдеры, а именно заказчики должны обеспечить безопасность доступа, или вообще его отсутствие (если нельзя гарантировать безопасность) для несовершеннолетних.

Если владелец кофейни или торгового центра не позаботился о безопасном использовании Интернета несовершеннолетними и не ограничил доступ к нежелательной информации – ему грозит штраф.

2.2 Способы защиты от Интернт-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:

- Будьте в курсе того, чем занимаются ваши дети в Интернете. Попросите их научить Вас пользоваться различными приложениями, которыми вы не пользовались ранее.
- Помогите своим детям понять, что они не должны предоставлять никому информацию о себе в Интернете — номер мобильно телефона, домашний адрес, название/номер школы, а также показывать фотографии свои и семьи. Ведь любой человек в Интернете может это увидеть.
- Если Вы получили спам (нежелательную электронную почту), напомните, что не стоит верить написанному в письмах и ни в коем случае не отвечать на них.
- Помните, что нельзя открывать файлы, присланные от неизвестных Вам людей. Эти файлы могут содержать вирусы или фото/видео с «агрессивным» содержанием.
- Поймите, что некоторые люди в Интернете могут говорить не правду 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 ребенку, как правильно поступать и реагировать на действия других людей в Интернете.

Полезные программы

На сегодняшний день существуют программы **«Интернет Цензор»,** которая устанавливается на компьютер и обеспечивает фильтрацию для всех веб-браузеров и программ.(Жаль, но это только Российское программное обеспечение)

2.3 Советы учащимся "Безопасный Интернет"

В Сети ты можешь встретить все, что угодно – от уроков истории и новостей до нелепых картинок. Но не стоит думать, что, раз информация появилась в Интернете, она является достоверной.

Чтобы разобраться, какой информации в Сети можно, а какой нельзя доверять, следуй простым советам:

Относись к информации осторожно. То, что веб-сайт здорово сделан, еще ни о чем не говорит. Спроси себя: за что этот сайт выступает? В чем меня хотят убедить ее создатели? Чего этому сайту не достает? Узнай об авторах сайта: зайди в раздел “О нас” или нажми на похожие ссылки на странице. Узнай, кто разместил информацию. Если источник надежный, например, университет, то, вполне возможно, что информации на сайте можно доверять.

Как предоставлять достоверную информацию?

•Будь ответственным – и в реале, и в Сети. Простое правило: если ты не будешь делать что-то в реальной жизни, не стоит это делать в онлайне.

•Не занимайся плагиатом. То, что материал есть в Сети, не означает, что его можно взять без спроса. Если ты хочешь использовать его - спроси разрешения.

•Сообщая о неприемлемом контенте, ты не становишься доносчиком. Наоборот, ты помогаешь делу безопасности Сети.

•Когда ты грубишь в Интернете, ты провоцируешь других на такое же поведение. Попробуй оставаться вежливым или просто промолчать. Тебе станет приятнее.

•Все, что ты размещаешь Интернете навсегда останется с тобой – как татуировка. Только ты не сможешь эту информацию удалить или контролировать ее использование.

ПОМНИ:

И в Интернете, и в реальной жизни соблюдай правила. Агрессия, кража, обман – запрещены. Сообщай о тех, кто ведет себя подобным образом.

Защищай себя – сейчас и в будущем. Подумай, прежде чем что-либо разместить в Интернете.

2.4 Советы родителям "Безопасный Интернет"

Начинать свое знакомство с виртуальной реальностью ребенок должен под присмотром взрослых. Именно родители и преподаватели смогут ответить на все "почему" и "как", а также предостеречь от возможных опасностей и ошибок. Основные советы: Прежде, чем позволить ребенку пользоваться Интернетом, расскажите ему о возможных опасностях Сети (вредоносные программы, небезопасные сайты, интернет-мошенники и др.) и их последствиях.

- ✓ Объясните ребенку, что при общении в Интернете (чаты, форумы, сервисы мгновенного обмена сообщениями, онлайн-игры) и других ситуациях, требующих регистрации, нельзя использовать реальное имя..
- ✓ Объясните ребенку, что нельзя разглашать в Интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т.д.).
- ✓ Четко определите время, которое Ваш ребенок может проводить в Интернете, и сайты, которые он может посещать.
- ✓ Помогите ребенку понять, что далеко не все, что он может прочесть или увидеть в Интернете - правда. Приучите его спрашивать то, в чем он не уверен.
- ✓ Не позволяйте Вашему ребенку встречаться с онлайн-знакомыми без Вашего разрешения или в отсутствии взрослого человека.

- ✓ Объясните ребенку, что нельзя открывать файлы, полученные от неизвестных пользователей, так как они могут содержать вирусы или фото/видео с негативным содержанием.
- ✓ Убедитесь, что на компьютерах установлены и правильно настроены антивирусные программы, средства фильтрации контента и нежелательных сообщений.
- ✓ Контролируйте деятельность ребенка в Интернете с помощью специального программного обеспечения.

Всем известно, что если у подростка не складываются отношения со сверстниками, он ищет общения в социальных сетях, и порой находит друзей в кругу наркоманов или бандитов. Не ради любопытства и контроля личной жизни, а чтобы не упустить переломный момент в жизни ребенка рекомендуется установить на компьютер программу родительского контроля.

Существует очень много разновидностей программ для родительского контроля. Программное обеспечение родительского контроля позволяет настроить определенный график на неделю, с указанием конкретного времени, когда Интернет будет доступен пользователю. Не менее важной функцией подобных программ является создания отчета о деятельности конкретного пользователя. То есть, родители смогут ежедневно просматривать отчет, о сайтах, которые посещал их ребенок.

Например, **Детский браузер Гогуль** (Бесплатный браузер)

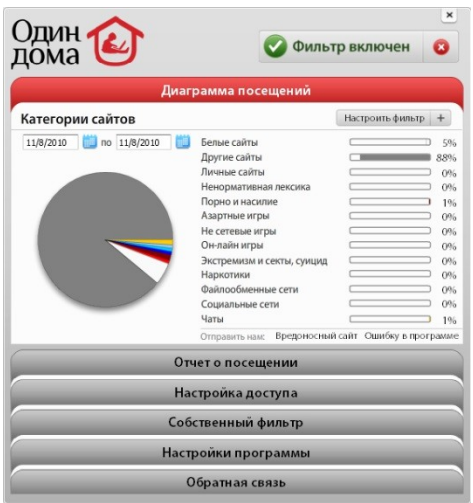
Гогуль ведёт статистику посещённых сайтов для контроля родителями, а

также может ограничивать время пребывания ребёнка в интернете.

Также родители могут получить детальный отчёт о том, какие сайты посещали их дети, и добавить или удалить сайты из перечня доступных к просмотру.

Отбором ресурсов, фото- и видеоматериалов, допущенных в Гогуль, занимается специально созданная команда, состоящая из родителей, профессиональных детских психологов и педагогов из различных регионов России.

Или **«Один Дома»**



Программный комплекс, отвечающий за безопасность детей в Интернете.

Программа «Один Дома» включает в себя: Гибкий и мощный Интернет фильтр для детей, блокирующий все потенциально опасные данные.

Возможность принудительного отключения целых категорий интернет-активности, среди которых есть социальные сети, он-лайн игры, чаты и т.д.

Наглядная диаграмма, сообщающая, на какие сайты пытался зайти ребёнок.

Платная программа

3. ЗАКЛЮЧЕНИЕ

Пока мы спорим пускать или не пускать учеников в Интернет - они уже здесь. Мы снова опоздали. Очевидно, что сейчас невозможно гарантировать стопроцентную защиту детей от нежелательного контента. Никакие фильтры никогда такой гарантии не дадут. Но мы можем формировать у ребят навык "безопасного" поведения в Интернете.

Использование Интернета является безопасным, если выполняются три основные правила.

1. Защитите свой компьютер

Используйте антивирусную программу. 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.

Таким образом, цели и задачи, поставленные в исследовательской работе:

- изучить скрытые и открытые угрозы интернета;
- определить насколько осведомлены учащиеся и родители о безопасном использовании ресурсов в сети Интернет, дать рекомендации по соблюдению правил безопасной работы в Интернете дома.(в период занятости учащихся после школы, пока родители еще на работе)
- 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 успешно достигнуты.

Данная работа (мои исследования) посвящены одной из актуальных проблем – безопасный интернет.

Теоретическая значимость исследования определяется тем, что рассмотрены типы Интернет -угроз, а так же структурированы меры борьбы с интернет-угрозами.

Практическая значимость исследования состоит в разработке рекомендаций родителям и учащимся по мерам безопасного нахождения в сети Интернет дома.

В последнее время в Интернете появляется много материалов агрессивного и социально опасного содержания. Взрослым нужно помнить о существовании подобных угроз и уделять повышенное внимание вопросу обеспечения безопасности детей в Интернете.

4. СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Интернет- цензор интернет фильтр для детей. http://www.icensor.ru/
2. Безопасное использование сети Интернет. http://www.friendlyrunet.ru/
3. Безопасный Интернет. http://laste.arvutikaitse.ee/rus/html/etusivu.htm
4. Как сделать Интернет для детей более безопасным http://shperk.ru/sovety/kak-sdelat-internet-dlya-detej-bolee-bezopasnym.html
5. Интернет – СМИ «Ваш личный Интернет».http://content-filtering.ru/Eduandinet/goodlink/
6. Ловушки интернета – примеры и методы защиты от них. http://www.securrity.ru/articles/571-lovushki-interneta-primery-i-metody-zashhity-ot.html
7. Продукция компании «Один дома». http://www.odindoma.ru/about/company.html
8. Правила безопасного использования Интернета._ http://www.gym075.edusite.ru/bezopasnostinet.html
9. Защитим ребенка от информационного яда. http://www.ug.ru/archive/48232
10. Безопасность детей в интернете - http://www.detskipark.ru/text1.html
11. Безопасность ребенка в сети интернет http://nsportal.ru/shkola/materialy-dlya-roditelei/library/sovety-roditelyam-po-obespecheniyu-bezopasnosti-detei-v-seti