Массовое внедрение Интернета в школьное образование наблюдается в России в последние несколько лет. Интернет превращается в такой же привычный носитель информации, как пресса, радио или телевидение. Интернет затягивает. В медицинский лексикон всё прочнее входит новый термин, за которым скрывается страшная болезнь - интернет зависимость. Актуальность работы: Современный школьник стремиться в совершенстве овладеть компьютерной техникой и технологией. Задача учителя и родителей состоит в том, чтобы показать возможности использования и применения этой техники и технологии в получении новых знаний, показать ребенку, что компьютер – это не просто игровая установка, а машина, с помощью которой быстро постигается и узнается новое, а также обеспечить безопасность физическому и психическому здоровью. Рассматривая информацию как товар, можно сказать, что информационная безопасность в целом может привести к значительной экономии средств, в то время как ущерб, нанесенный ей, приводит к материальным затратам. Например, раскрытие технологии изготовления оригинального продукта приведет к появлению аналогичного продукта, но от другого производителя, и как следствие нарушения информационной безопасности, владелец технологии, а может быть и автор, потеряют часть рынка и т.д. С другой стороны, информация является субъектом управления, и ее изменение может привести к катастрофическим последствиям в объекте управления.
Объект исследования: является интернет и его ресурсы.
Предмет исследования – интернет угрозы.
Цель работы: изучить безопасные способы работы детей в интернете, разработать рекомендации для родителей и детей по безопасной работе в сети Интернет.

Глава 1. Сеть интернет
1.1 Что такое интернет и как он появился
Несмотря на принятые во многих странах, законы по борьбе с компьютерными преступлениями и разработку специальных программных средств защиты от вирусов, количество новых программных вирусов постоянно растет. Это требует от пользователя персонального компьютера знаний о природе вирусов, способах заражения вирусами и защиты от них. Под безопасностью информационных систем понимается защищенность системы от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, от попыток хищения (несанкционированного получения) информации, модификации или физического разрушения ее компонентов.
1.2 Под угрозой безопасности информации понимаются события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств. Виды угроз безопасности информационных систем Человека, пытающегося нарушить работу информационной системы или получить несанкционированный доступ к информации, обычно называют взломщиком, а иногда «компьютерным пиратом» (хакером). В своих противоправных действиях, направленных на овладение чужими секретами, взломщики стремятся найти такие источники конфиденциальной информации, которые бы давали им наиболее достоверную информацию в максимальных объемах с минимальными затратами на ее получение.
С помощью различного рода уловок и множества приемов и средств подбираются пути и подходы к таким источникам. В данном случае под источником информации подразумевается материальный объект, обладающий определенными сведениями,

представляющими конкретный интерес для злоумышленников или конкурентов. Защита от умышленных угроз – это своего рода соревнование обороны и нападения: кто больше знает, предусматривает действенные меры, тот и выигрывает.
Сегодня можно утверждать, что рождается новая современная технология – технология защиты информации в компьютерных информационных системах и в сетях передачи данных. Реализация этой технологии требует увеличивающихся расходов и усилий. Однако все это позволяет избежать значительно превосходящих потерь и ущерба, которые могут возникнуть при реальном осуществлении угроз информационных систем. Умышленные угрозы делятся на пассивные и активные.07:51
Пассивные угрозы направлены в основном на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на ее функционирование. Например, несанкционированный доступ к базам данных, прослушивание каналов связи и т.д. Активные угрозы имеют целью нарушение нормального функционирования системы путем целенаправленного воздействия на ее компоненты. К активным угрозам относятся, например, вывод из строя компьютера или его операционной системы, искажение сведений в базе данных, разрушение программного обеспечения компьютеров, нарушение работы линий связи и т.д.Источником активных угроз могут быть действия взломщиков, вредоносные программы и т.п.Умышленные угрозы подразделяются на внутренние (возникающие внутри управляемой организации) и внешние. Внутренние угрозы чаще всего определяются социальной напряженностью и тяжелым моральным климатом. Внешние угрозы могут определяться злонамеренными действиями конкурентов, экономическими условиями и другими причинами (например, стихийными бедствиями). По данным зарубежных источников, получил широкое распространение промышленный шпионаж – это наносящие ущерб владельцу коммерческой тайны незаконные сбор, присвоение и передача сведений, составляющих коммерческую тайну, лицом, не уполномоченным на это ее владель
Интернет – это всемирная система объединённых компьютерных сетей, построенная на использовании протокола IP и маршрутизации пакетов данных. Интернет образует глобальное информационное пространство, служит физической основой для Всемирной паутины (World Wide Web (WWW) и множества других систем (протоколов), передачи данных.
Протокол в данном случае — это, образно говоря, «язык», используемый компьютерами, для обмена данными при работе в сети. Чтобы различные компьютеры сети могли взаимодействовать, они должны «разговаривать» на одном «языке», то есть использовать один и тот же протокол. Проще говоря, протокол — это правила передачи данных между узлами компьютерной сети. Систему протоколов Интернет называют «стеком протоколов TCP/IP».[1]
Общие свойства и юридические аспекты сети интернет:
1. У Интернета нет собственника, так как он является совокупностью сетей, которые имеют различную географическую принадлежность.
2. Интернет нельзя выключить целиком, поскольку маршрутизаторы сетей не имеют единого внешнего управления.
3. Интернет стал достоянием всего человечества.
4. У Интернета имеется много полезных и вредных свойств, эксплуатируемых заинтересованными лицами.
5. Интернет, прежде всего, средство открытого хранения и распространения информации. По маршруту транспортировки незашифрованная информация может

быть перехвачена и прочитана.
6. Интернет может связать каждый компьютер с любым другим, подключённым к Сети, так же, как и телефонная сеть. Если телефон имеет автоответчик, он способен распространять информацию, записанную в него, любому позвонившему.
7. Сайты в Интернете распространяют информацию по такому же принципу, то есть индивидуально, по инициативе читателя.
8. Спам - серверы и «зомби-сети» распространяют информацию по инициативе отправителя и забивают почтовые ящики пользователей электронной почты спамом точно так же, как забивают реальные почтовые ящики распространители рекламных листовок и брошюр.
9. Интернете имеет ту же природу, что и слухи в социальной среде. Если к информации есть большой интерес, она распространяется быстро и широко, нет интереса — нет распространения.
10. Чтение информации, полученной из Интернета или любой другой сети ЭВМ, относится, как правило, к непубличному воспроизведению произведения. За распространение информации в Интернете (разглашение), если это государственная или иная тайна, клевета, другие запрещённые законом к распространению сведения, вполне возможна юридическая ответственность по законам того места, откуда информация введена.
11. 3 июня 2011 года была принята резолюция ООН признающая доступ в Интернет базовым правом человека. Отключение конкретных регионов от Интернета с июня 2011 года считается нарушением прав человека.

На сегодняшний день интернет это одно из главных средств телекоммуникации. Нам он доступен практически везде, где бы мы ни находились. Но мало кто знает как, где и для каких целей создавался интернет. Интернет зародился в 70-х годах прошлого века. В течение 1970-х высшее военное руководство задалось вопросом, как американские власти смогут общаться после ядерной войны. Надо начинать с какой-нибудь сети с центральным пультом управления. Решением стала сеть, которая всегда считалась ненадежной. Каждый узел в сети будет суперкомпьютером. Все узлы будут считаться равными по статусу происхождения, получения и отправления посланий. Сами послания будут разделены па пакеты, отправляемые отдельно. Каждый пакет будет начинаться с некоторого конкретного узла и отправляться по указанному направлению. Каждый пакет в каждом сообщении будет проходить по независимому пути внутри сети, а послание будет собираться в готовую форму на конечном пункте. [7]Сеть быстро развивалась, и к 1972 г. в ней было уже 32 узла. Люди использовали ее для сетевой работы на компьютерах, но главной ее функцией был обмен сообщениями при совместной работе над исследовательскими проектами. Очень скоро новости начали появляться одна за другой. Так как компьютеры стали более доступны, их начали соединять с растущей сетью. Узлы в сети были разделены на шесть доменов: gov, com, edu, org, milи net, чтобы классифицировать организации, владеющие данными узлами.

1.3 Безопасное поведение родителей и детей в Интернете

Дети могут не захотеть рассказывать о том, как они используют Интернет. Они могут быть против вмешательства родителей в процесс использования Интернета, особенно

если они считают, что родители ограничат их в этом. Важно помнить о том, что Интернет является огромным ресурсом с большим объемом увлекательной и образовательной информации. Кроме того, важно не слишком остро реагировать или чрезмерно ограничивать детей в использовании Интернета. Чтобы дети могли извлечь самое лучшее из такого ресурса и для обеспечения их безопасности, необходимо осознавать все связанные с этим риски. Дети учатся, экспериментируя, путем проб и ошибок. Если вы сами увлекаетесь Интернетом и знакомы со всеми его аспектами, это очень поможет вам при обсуждении Интернета с детьми. Кроме того, вам будет проще выяснить, как ваш ребенок использует Интернет, и непрерывно вести диалог, который будет длиться до достижения детьми совершеннолетия.[4]
Чем больше вы знаете о том, как ваш ребенок использует Интернет, тем проще будет определить и объяснить, что является приемлемым и безопасным. У ребенка могут быть превосходные навыки использования Интернета, но жизненный опыт взрослых может оказаться бесценным при объяснении детям принципов поведения в виртуальном мире.
Установите компьютер в общей для всей семьи комнате
В этом случае разговор об Интернете и наблюдение за его использованием станет естественным в повседневной жизни. Обсуждение проблем может стать проще, если компьютер находится в общей комнате. Кроме того, Интернетом можно пользоваться вместе.
Обсуждайте Интернет
Проявляйте интерес к действиям ребенка и его/ее друзей как в Интернете, так и в реальной жизни. Расскажите ребенку о прекрасных и увлекательных вещах, которые возможны в Интернете, а также о трудностях, с которыми можно столкнуться. Обсудите с ребенком действия, которые необходимо предпринять, если чувствуется неловкость в какой-либо ситуации в Интернете.
Узнайте больше об использовании компьютера
Если вы сами являетесь пользователем Интернета, вам будет проще определить правильную тактику для детей и помочь им найти в Интернете полезный материал.
Используйте Интернет вместе
Найдите сайты, которые подходят для детей, или узнайте о способах поиска полезной информации: запланируйте совместную туристическую поездку, просмотрите образовательные сайты для помощи в школьных заданиях или найдите информацию об увлечениях детей. Просматривая веб-сайты в Интернете вместе, можно также помочь ребенку оценить значимость найденной информации. > Даночка Мег: Можно добавить любимые сайты в папку «Избранное», чтобы совместно просмотренные ранее веб - сайты можно было открыть одним щелчком мыши.
Договаривайтесь с ребенком о способе и времени использования Интернета
Может оказаться полезным согласовать с ребенком время, которое он проводит за компьютером, а также список веб-сайтов, которые он может посещать. Это необходимо обсудить с детьми и прийти к определенному решению, которое всех устраивает.

Глава 2. Рекомендации для безопасной работы детей в Интернете

Родителям необходимо постоянно вести разъясни тельную работу, т.к. без понимания данной проблемы невозможно ее устранить силами только учителей.
Очень часто родители не понимают или недооценивают те угрозы, которым подвергается школьник, находящийся в сети Интернет. Некоторые из них считают, что ненормированное «сидение» в сети лучше, чем прогулки в сомнительных компаниях.
Родители, с ранних лет обучая ребенка основам безопасности дома и на улице, тому, как вести себя с незнакомыми людьми, что можно говорить о себе, а что нет, между тем, «выпуская» его в сеть Интернет, не представляют себе, что точно так же нужно обучить его основам безопасности в сети Интернет.
Ребенок абсолютно беззащитен перед потоком информации. Дома необходимо выработать общие правила, которые бы сводились к следующему:

Какие сайты могут посещать дети и что они могут там делать;
Сколько времени дети могут проводить в сети Интернет;
Как защитить личные данные;
Как следить за безопасностью;
Как вести себя вежливо;
Как пользоваться чатами, группами новостей, службами

2.1.Рекомендации для родителей

В наше время поголовной компьютеризации, главным помощником во многих делах становится интернет. В интернете можно найти нужную нам.
информацию, документы, рецепты и тому подобное. Но не надо забывать, что у медали всегда две стороны. И если для взрослого человека, занимающегося делом интернет – помощник и друг, то для детей – это большой соблазн и опасность. Самое главное для родителей и взрослых людей обеспечить безопасный интернет для детей.

Естественно, что в первую очередь, обеспечение безопасности интернета для детей ложится на родителей и людей, отвечающих за детей. Вот несколько рекомендаций для того, чтобы сделать интернет безопасным и полезным для детей.

Внимательно, но не навязчиво контролируйте деятельность ребенка в интернете. Это особенно важно во время обучения работе с интернетом, ребенок должен получить ответы на появившиеся вопросы и правила поведения, что можно делать, что нельзя от родителей. Именно родители должны заложить основы безопасности в интернете. Для этого разговаривайте с ребенком, узнавайте у него, что произошло, что он узнал нового.

Необходимо, на первых этапах работы в интернете, объяснить детям, что в интернете можно встретить не только «хорошее», но и «плохое». И надо подготовить детей к встрече с «плохим». Ребенок должен быть готов, что в интернете его могут обмануть, попытаться воспользоваться его неопытностью и, столкнувшись с такими фактами или заподозрив это, дети должны сразу сообщить об этом взрослым. Необходимо научить детей правильному поиску нужной информации и проверки ее на безопасность и соответствие.
Объясните детям опасность скачивания платной информации и регистраций, особенно, с помощью отправки СМС или через номер сотового телефона. Наладьте с

детьми доверительные отношение и приучите их к тому, что все финансовые действия в интернете должны проводиться после согласования с родителями.
Составьте, вместе с ребенком, подборку нужных и безопасных интернет ресурсов, «белый список», которыми ребенок может пользоваться свободно.
На компьютере, на котором занимаются дети, установите необходимое программное обеспечение. Надежный антивирус, с постоянно обновляемыми базами, с поддержкой функции «Родительского контроля». Вместе с ним должен быть установлен и хороший фаервол (сетевой экран).

Если дети проводят много времени дома одни, то необходимо ограничивать время нахождения его в интернете.
Установите хороший браузер, например, Mozilla Firefox. Установите на него необходимые дополнения для удобной и безопасной работы в интернете и научите пользоваться браузером детей.
При использовании компьютера другими членами семьи, ни в коем случае не устанавливайте его в комнате ребенка. Для обеспечения безопасности в интернете, сделайте разные учетные записи. Учетные записи детей сделайте с ограниченными правами, не делайте записи с правами администратора детям, особенно младшего возраста. Свои учетные записи и администратора защитите паролем.
Возьмите за правило каждый день проверять, на какие интернет ресурсы заходили ваши дети. Обязательно настройте сохранение истории, журнал браузера. Если заметите попытки редактирования записей журнала, это повод задуматься и поговорить с детьми.
Постоянно развивайте свои компьютерные знания, чтобы сделать работу в интернете безопасной для своих детей и для себя. Узнавайте, как настроить и правильно настройте компьютер, следите за новинками программного обеспечения и компьютерных составляющих. Следите за обновлением системы и постоянно устанавливайте обновления безопасности в интернете зависит, в основном, от их знаний и навыков.
Windows. Знайте принцип работы компьютера, принцип работы лазерного принтера… Делитесь своими знаниями со своими близкими и детьми, их безопасность
Не бросайте на самотек, действия детей, конечно, это удобно сидит ребенок за компьютером, всегда на ваших глазах, вас не беспокоит, не мешается под ногами. Но, как было сказано выше, безопасность в интернете ваших детей зависит от вас.
Использование Интернета является безопасным, если выполняются три основных правила:
Защитите свой компьютер
· Регулярно обновляйте операционную систему.
· Используйте антивирусную программу.
· Применяйте брандмауэр.
· Создавайте резервные копии важных файлов.
· Будьте осторожны при загрузке новых файлов.
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.
Соблюдайте правила
разом. Каждый должен помнить о следующих внутренних правилах чата. · Закону необходимо подчиняться даже в Интернете.
· При работе в Интернете не забывайте заботиться об остальных так же, как о себе.
Инструкции по безопасному общению в чатах
Дети, которые общаются в чатах, должны знать, как делать это безопасным об
Вот на что следует обратить внимание родителям, чтобы во время заметить, что ребенок стал жертвой кибербуллинга: -Беспокойное поведение Даже самый замкнутый школьник будет переживать из-за происходящего и обязательно выдаст себя своим поведением. Депрессия и нежелание идти в школу –самые явные признаки того, что ребенок подвергается агрессии.-Неприязнь к ИнтернетуЕсли ребенок любил проводить время в Интернете и внезапно перестал это делать, следует выяснить причину. В очень редких случаях детям действительно надоедает проводить время в Сети. Однако в большинстве случаев внезапное нежелание пользоваться Интернетом связано с проблемами в виртуальном мире.- Нервозность при получении новых сообщений Негативная реакция ребенка на звук письма на электронную почту должна насторожить родителя. Если ребенок регулярно получает сообщения, которые расстраивают его, поговорите с ним и обсудите содержание этих сообщений.

2.3.Рекомендации для самих пользователей-детей.

В Интернет ты заходишь через компьютер. Это может быть школьный или библиотечный компьютер, твой личный или тот, которым пользуется вся семья. Любому компьютеру могут повредить вирусы, их еще иногда называют вредоносными программами. Они могут уничтожить важную информацию или украсть деньги через Интернет.
Для защиты компьютера на нём установлены специальные защитные программы и фильтры. Не меняй ничего в их настройках!
Не сохраняй подозрительные файлы и не открывай их.

> Даночка Мег: Если антивирусная защита компьютера не рекомендует, не заходи на сайт, который считается «подозрительным».

Никому не сообщай свой логин с паролем и не выкладывай их в Интернете – относись к ним так же бережно, как к ключам от квартиры.
Ты знаешь, что вне дома и школы есть вероятность столкнуться с людьми, которые могут причинить тебе вред или ограбить. В Интернете также есть злоумышленники – ты должен помнить об этом и вести себя так же осторожно, как и на улице или в незнакомых местах.
Не сообщай свой адрес или телефон незнакомым людям и никогда не выкладывай в Интернете.
Никогда не высылай свои фотографии без родительского разрешения. Помни, что преступники могут использовать эту информацию против тебя или твоих родных.
Если ты хочешь поучаствовать в каком-нибудь конкурсе, где нужно указывать свои данные, посоветуйся с родителями. Никогда не соглашайся прийти в гости к человеку, с которым ты познакомился в Интернете. Если назначается встреча, она должна проходить в людном месте и желательно с при- отсутствием родителей. Помни, что

под маской твоего ровесника может скрываться взрослый человек с преступными намерениями. Кроме преступников в Интернете есть просто злые и невоспитанные люди. Ради собственного развлечения они могут обидеть тебя, прислать неприятную картинку или устроить травлю. Ты можешь столкнуться с такими людьми на самых разных сайтах, форумах и чатах. Помни: ты не виноват, если получил оскорбительное сообщение. Не нужно реагировать на грубых людей – просто прекрати общение. Если тебе угрожают по Интернету, не стесняйся сообщить об этом родителям. Помни, что цель угроз – испугать тебя и обидеть. Но подобные люди боятся ответственности. Коллективное преследование – это крайнее проявление жестокости. Жертву забрасывают оскорблениями и угрозами, его фотографию искажают и все данные публикуют. Никогда не участвуй в травле и не общайся с людьми, которые обижают других. Всегда советуйся с родителями во всех указанных случаях.

Заключение

Родители сталкиваются с одинаковыми трудностями как с Интернетом, так и с увлечениями детей. Родителям важно знать о намерениях своих детей и поддерживать их в этих действиях.

Дети могут не захотеть рассказывать о том, как они используют Интернет. Они могут быть против вмешательства родителей в процесс использования Интернета, особенно если они считают, что родители ограничат их в этом. Важно помнить о том, что Интернет является огромным ресурсом с большим объемом увлекательной и образовательной информации. Кроме того, важно не слишком остро реагировать или чрезмерно ограничивать детей в использовании Интернета. Чтобы дети могли извлечь самое лучшее из такого ресурса и для обеспечения их безопасности, необходимо осознавать все связанные с этим риски. Дети учатся, экспериментируя, путем проб и ошибок. Если вы сами увлекаетесь Интернетом и знакомы со всеми его аспектами, это очень поможет вам при обсуждении Интернета с детьми. Кроме того, вам будет проще выяснить, как ваш ребенок использует Интернет, и непрерывно вести диалог, который будет длиться до достижения детьми совершеннолетия.

Самым безопасным способом путешествия по просторам Интернета для детей является создание безопасного пространства или области, в которой разрешен просмотр сайтов, одобренных доверенным взрослым человеком. Для разрешения детям доступа к определенным безопасным сайтам можно использовать параметры обозревателя. В этом случае, если ребенку необходимо посетить новый сайт, сначала необходимо добавить его адрес в список разрешенных сайтов. В операционной системе Windows XP можно легко создавать безопасные пространства.

Наше исследование имело цель - изучить безопасные способы работы детей в интернете, разработать рекомендации для родителей и детей по безопасной работе в сети Интернет.

Мы составили опросник для родителей и детей, в котором было 6 вопросов. Нами было опрошено 25 родителей и 50 школьников.