**Оглавление**

**Введение.**

**I. Основная часть**.

1. Интернет: друг или враг?

**2. Методика исследования вопроса «Безопасности в Интернете».**

2.1 Преимущества интернета.

2.2 Тест – исследование «Интернет и ты». Анализ исследования.

2.3 Угрозы, исходящие от интернета.

2.4 Рекомендации при пользовании интернетом.

2. 5 Безопасный интернет детям: как общество защищает ребенка от негативного влияния сети.

**3. Вывод.**

**Заключение**

**Список литературы**

Введение

**«Человек в XXI веке, который не будет уметь пользоваться ЭВМ, будет подобен человеку ХХ века, не умевшему ни читать, ни писать»**

**Академик В. М. Глушков**

Так сказал академик Глушков еще в прошлом веке. И сегодня трудно представить семью или дом без компьютера. Наверное, каждый со мной согласится, что компьютер мы, в основном, используем для выхода в интернет. Да и многие уже скорее всего не знают, как можно жить без интернета. Он уже давно стал незаменимым помощником современного человека. Всемирная сеть - является прекрасным источником для новых знаний, помогает в учебе, занимает досуг. Именно поэтому дети активно пользуются Интернетом, а зачастую проводят в Сети даже больше времени, чем взрослые. Юные пользователи осваивают сервисы мгновенных сообщений и интернет телефонию, общаются на форумах и в чатах, каждый день узнают много новой увлекательной и образовательной информации.

Однако не стоит забывать, что Интернет может быть не только средством для обучения, отдыха или общения с друзьями, но – как и реальный мир – Сеть тоже может быть опасна.

**I Основная часть.**

**Цель моей работы** заключалась в том, чтобы проследить влияние Всемирной глобальной компьютерной сети Интернет на мировоззрение подростков, раскрыть позитивные и негативные стороны влияния социальных сетей на подрастающее поколение и найти способы решения проблем, связанных с времяпровождением подростков в социальных сетях. Т. Е. показать, что интернетом можно пользоваться безопасно.

**Я поставила такие задачи**.

Изучить угрозы, исходящие от интернета.

Провести анкетирование среди учащихся.

Выяснить, как общество реагирует на эти угрозы;

Показать, что делает школа и общественные организации, чтобы научить детей безопасно пользоваться интернетом.

**Гипотеза:** если постепенно знакомиться с миром информационных технологий и осуществлять негласный контроль над работой подростков, то интернет будет не угрозой, а помощником.

**Актуальность:** Интернет может быть не только средством для обучения, отдыха или общения с друзьями, но – как и реальный мир – Сеть тоже может быть опасна. Поэтому общество обязано принимать меры по защите особенно уязвимых членов общества. Я использовала несколько методов работы при написании данной исследовательской. Я искала информацию в интернете и справочниках, создала опрос и провела анкетирование среди учащихся старших классов и учителей. Представить современных подростков без социальных сетей сегодня просто невозможно. Вконтакте, Одноклассники, Фэйсбук заполонили разумы юных школьников. Нужно решить, что же делать и что же предпринять.

**Объект исследования:** поведение учащихся в интернете.

**Предмет исследования:** отношение общества к проблеме негативного влияния интернета и способы .

**1. Интернет: друг или враг?**

Современный мир практически невозможно представить без существования компьютеров и интернета. Почти в каждом доме обязательно есть хотя бы один компьютер и подключение к сети. Стали популярными социальные сети, где молодежь, а также старшее поколение проводит очень много своего времени. Там можно найти вторую половинку, общаться с друзьями, смотреть фильмы, слушать музыку и многое другое. Также очень популярными стали компьютерные игры, где можно зависать не только часами, но и днями. Многие могут не спать ночами, и играть в ролевые игры.

Компьютеры стали частью жизни людей. В транспорте, в магазине, в ресторанах, в кафе, в школах, в университетах и других заведениях можно наблюдать картину, как множество людей смотрят в свой телефон и общаются в социальных сетях. Создаются новые технологии, которые позволяют иметь доступ к сети не только через компьютеры, но и другие способы. Молодежь предпочитает использовать смартфоны, бизнесмены – ноутбуки, а домохозяйки могут обойтись и обычным компьютером.

Буквально за несколько лет, весь мир охватила одна сеть, которая объединяет людей со всего мира, с разных городов, стран и материков. Это служит отличной возможностью найти новых знакомых, потерянных друзей. Удивительно, сколько пользы может оказать нам интернет. Сегодня даже сложно представить, как раньше люди обходились без столь необходимой вещи. Кафе и рестораны, в которых есть wi-fi, пользуются большей популярностью, чем обычные. Люди предпочитают идти туда, где можно провести свое время в полном комфорте. А нам ученикам, стало проще находить дополнительную информацию к урокам, выполнять домашнюю работу. Все это делает нашу жизнь намного проще и легче. Не нужно прилагать особых усилий, чтобы что-то сделать. Через компьютер можно заказать еду, одежду, найти друзей и работу. Это очень удобное изменение, которое произошло в мире за последнее время.

Но такое новшество сильно повлияло на общество. Сегодня мы можем заметить, что огромное количество людей больше проводят с техникой, чем со своими родными и близкими. Дети, которые должны бегать по улицам и играть со своими друзьями, целыми днями сидят за компьютером в играх. Исчезает живое общение, которое так необходимо обществу. Все становится виртуальным. Компьютеры стали заменять людей. Такая не очень приятная картина создалась с появлением новых технологий.Очень важно, чтобы люди могли правильно использовать то, что им предоставлено.

Поэтому стоит ставить правильные приоритеты и оптимально использовать время, чтобы компьютеры служили для работы и комфортной жизни, а также для всего, что может помочь вам, а не наоборот. Многие молодые люди тратят свое время на пустых играх, что никак не поможет им в жизни. Компьютеры и интернет нужно использовать правильно, ведь благодаря этим технологиям мир стал активно и очень эффективно развиваться. Чтобы не началась деградация, стоит уделить внимание тому, насколько высокое влияние оказывает интернет лично на вас, и в каких целях вы его используете. Сеть открывает огромные возможности для каждого человека.

**Глава 2. Методика исследования вопроса.**

**2. 1. Преимущества интернета.**

**Коммуникация**

Главной целью сети Интернет всегда была связь. И Интернет преуспел в этой области, более того, новейшие технологии расширяют возможности связи, делая их быстрее и надежнее. С появлением Интернета, общение с любым уголком Земли стало доступно так же просто, как разговор с соседом.

Теперь мы можем общаться с человеком из другой части мира, за доли секунды. На помощь людям приходит электронная почта, которая позволяет нам общаться с родными и близкими целыми часами. Но коммуникационные услуги не ограничиваются электронной почтой. Существует множество услуг, с помощью которых вы легко можете наладить дружбу с человеком, поделиться своими мыслями, изучать культуру самых разных национальностей.

**Информация**

Информация, вероятно, самое большое преимущество, которым располагает Интернет. Сеть стала виртуальным кладезем информации. Любая информация по любой теме доступна в сети Интернет. Поисковые системы, как Google, Yahoo и Яндекс предоставляют свои услуги пользователям сети. Вы можете разыскать любой тип данных и получить ответ на практически любой вопрос. Интернет располагает необъятным количеством информации относительно любого предмета, известного человеку, начиная от законодательства и заканчивая временем проведения ярмарки в вашем районе. Вы сможете получить информацию о рынке, открыть для себя новые идеи, получить техническую поддержку, список возможностей безграничен.

Студенты и дети относятся к числу наиболее активных пользователей, которые занимаются серфингом в сети Интернет в поисках информации. Сегодня Интернет стал необходимостью для студентов, которые используют сеть для подготовки проектов и дипломных работ. Учителя стали давать задания, которые требуют поиска в сети Интернет. С каждым днем, исследования по медицинским вопросам становится всё легче найти в сети. Многочисленные web-сайты доступны в сети и предлагают информацию для людей, которые исследуют различные заболевания.

**Развлечения**

Развлечения являются очередным популярным преимуществом сети Интернет. В самом деле, будучи средством массовой информации, Интернет стал весьма успешным инструментом в области развлечений. Загрузка игр, посещение специализированных сайтов, общение с опытными игроками, Интернет предоставляет любые услуги в области игровой индустрии. Существует множество игр, которые можно загрузить из сети совершенно бесплатно. Индустрия онлайн-игр испытывает огромный рост, привлекая миллионы игроков. Тематические чаты чрезвычайно популярны, поскольку здесь пользователи могут познакомиться с новыми интересными людьми. В самом деле, Интернет успешно используется людьми с целью поиска партнера по жизни. Когда люди обращаются за поиском к сети Интернет, они могут найти что угодно. Музыка, игры, новости и многое другое, всё есть в сети.

**Услуги**

Сегодня множество услуг перебрались в сеть. Среди них: оплата жилищных услуг, поиск работы, покупка билетов на любимые фильмы, руководство по кругу вопросов, которые охватывают все аспекты жизни, бронирование отелей, в конце концов. Многие услуги могут быть недоступны в автономном режиме или могут оказаться много дороже.

**Электронная торговля**

Электронная коммерция – понятие, которое используется для любого вида коммерческой деятельности, или делового предложения, которое предполагает передачу информации по всему миру, по средствам сети Интернет. Это определение вовлекает в себя любую коммерческую деятельность в сети. Мы называем это «электронной торговлей» и её щупальца охватили каждый отдельный продукт и сервис, повышая доступность любых услуг. Интернет вовлекает в себя удивительный и широкий спектр продуктов, от бытовых нужд к технологиям и развлечениям.

**2.2 Тест – исследование «Интернет и ты». Анализ исследования.**В рамках данной работы мною было проведено исследование (анкетирование учащихся с 5 по 11 классы), целью которого явилась оценка степени влияния интернета на подростков нашей школы. В анкетировании участвовало 52 ученика и 13 учителей. **Опрос.** Я предложила подросткам максимально честно ответить на опрос. Вопросы были следующими:

1. Сколько времени вы проводите в Интернете?
2. Зарегистрированы ли вы в каких-либо Социальных сетях? (если да, то где именно?)
3. Сможете ли вы прожить без соц. сетей?
4. Влияют ли соц. сети на вашу успеваемость в школе?
5. Заменяет ли Интернет общение в реальном мире?
6. Считаете ли Вы себя Интернет-зависимым?
7. Из каких источников вы узнали о соц. сетях? (или от кого?)
8. 2. Есть ли у тебя доступ к сети Интернет?
9. Сколько времени ты проводишь в сети Интернет?
10. Как ты считаешь – опасен Интернет или нет?
11. Чем занимаешься в Интернете? учусь; общаюсь в социальных сетях; скачиваю программы, пользуюсь e-mail; играю в игры on-line; смотрю Интернет –ТВ, фильмы веду блог, сайт , просматриваю запрещенное родителями
12. Встречал ли ты когда-нибудь угрозы, противоправные призывы в сети Интернет?
13. Как родители относятся к твоей работе в сети Интернет? разрешают свободно; устанавливают временной режим; разрешают заходить в своём присутствии; запрещают пользоваться; не знают о том, что я выхожу в Интернет.

**Анализ и результаты исследования.** Мной были использованы два метода выведения результатов: составление диаграммы и выведение среднего ответа. В результате, я узнала, что все опрашиваемые мною ученики зарегистрированы в социальных сетях, в основном в Одноклассниках и Вконтакте. Большая часть учителей имеет свой аккаунт в социальных сетях, а многие предпочитают Инстаграмм. Ответы на некоторые вопросы тестирования представлены на слайдах. Но самый основной вывод, что учащиеся нуждаются в ознакомлении с угрозами, которые исходят от интернета и способами избежать их пагубного влияния.

**2.3 Угрозы, исходящие от интернета.**

**Кража личной информации**

Если вы используете Интернет на регулярной основе, вы должны знать, что всегда существует вероятность кражи личной информации, как адрес, номер кредитной карты, имя и многое другое. Всё это может быть доступно для преступников по средствам сети, что вызывает некоторое беспокойство.

**Спам**

Спам представляет собой рассылку нежелательных сообщений на адреса электронной почты. Многие сообщения не преследуют никакой цели и просто препятствуют работоспособности всей системы. Этот вид незаконной деятельности может вызывать некоторые проблемы у пользователя, совсем не просто игнорировать массовую рассылку, вы должны приложить усилия, чтобы остановить спам, с тем, чтобы использование сети стало безопасней и удобней.

**Угроза вирусов**

Вирус не что иное, как программа, которая нарушает нормальное функционирование компьютерных систем. Компьютеры, подключенные к сети Интернет, гораздо чаще подвержены вирусным атакам, которые, в конечном итоге, могут нарушить работу жесткого диска, чем доставят немало проблем пользователю.

**Сайты с недетским контентом**

Это, пожалуй, самая большая угроза, которая может вредить психологическому здоровью ваших детей. Очень серьезная и больная тема относительно сети Интернет. В Интернете существуют тысячи порнографических сайтов, которые могут быть легко найдены и становятся пагубным фактором, поскольку открыты в свободном доступе каждому пользователю Интернета.

**2.4 Рекомендации при пользовании интернетом.**

Несмотря на то, что Интернет располагает множеством пагубных факторов, его польза превышает любые недостатки. Поэтому перед подключением к Интернет, надо подумать о том, как обезопасить себя и свои данные.За очень короткий промежуток времени в интернете без надлежащей защиты, можно серьезно навредить своему компьютеру.  
**Установка обновлений для операционной системы**  
После подключения к Интернету, операционная система станет автоматически скачивать обновления с сервера Microsoft.  Со временем обновления собираются в специальный комплект — Servise Pack. Некоторые пользователи отключают автоматическое обновление, опасаясь, что может слететь активация операционной системы Windows. Сами же обновления, если посмотреть на установленные, почти полностью касаются проблем безопасности операционной системы. Так Microsoft закрывает обнаруженные уязвимости в операционной системе. После установки обновлений система будет работать более стабильнее и безопаснее.  
 Компьютер, подключенный к Интернету, подвергается множеству угроз.

Жертвами киберпреступников, как правило, становятся не продвинутые программисты и эксперты, а обычные пользователи, которых сегодня в сети подавляющее большинство. Злоумышленники пользуются тем, что рядовой пользователь мало информирован о потенциальных опасностях интернета, и вследствие этого совершает типичные ошибки – месяцами не меняет пароли, оставляет избыточную информацию о себе в открытом доступе, не пользуется защитными программами. Вот пример тех угроз, что могут ожидать каждого из нас при работе в сети Интернет.  
**Вирусы -** компьютерные вирусы, сетевые и почтовые черви могут распространяться самостоятельно. Например, если вам приходит подозрительное электронное письмо с вложением – весьма высока вероятность того, что оно содержит компьютерный вирус, который может заразить некоторые файлы на вашем компьютере, испортить или украсть какие-нибудь данные. Троянские программы самостоятельно не распространяются, распространяться с помощью компьют. вирусов. Их основные цели красть и уничтожать.

**Неосторожное поведение пользователя** - неосторожность пользователя – это серьезная проблема, которая ставит под удар даже самую защищенную систему, даже данные, которые расположены на отключенном от Интернета компьютере. Например, задавая слишком простой пароль для почтового ящика, вы делаете его взлом сравнительно легким, неприятны последствия случайного удаления важных данных.  
Не думая о безопасности в интернете, люди совершают  ошибки.  Например, регистрируясь в какой либо социальной сети, где просят указывать верные личные данные- фамилия и имя, это для начала. Пользователи бездумно вводят все это, разумеется это же не секрет, какая мол тут интернет безопасность.  Далее, разумеется нужно фото, и тут вроде бы нет никакой угрозы безопасности в интернете. Для удобства поиска ваших потенциальных друзей вам порекомендуют заполнить профайл. Такой себе маленький файлик, где нужно заполнить личные данные о себе. Ну так вот, в профайле вам нужно будет к примеру, заполнить ряд колонок. Это может быть школа, ВУЗ, ваши интересы, увлечения и прочее, прочее. На первый взгляд безобидная информация ведь, тем более применимо к данному сайту – на котором вы все это заполняете. Сайты это могут вам предлагать заполнить даже под предлогом заботы о вашей безопасности. Затем попросят указать номер телефона, вроде бы на случай если забудете пароль сайта-Вам будет выслан код для смены пароля. А иногда просят ввести паспортные данные и находятся такие,кто вводит. Последствия самые плачевные: фото может быть использованно в непристойных местах интернета с самыми грязными подписями,вместо забытого пароля исчезнут деньги со счёта телефона,появится кредит на Ваше имя и на немалую сумму и так далее до бесконечности и всё из за Вашей же небрежности к безопастности в интернете.  
 Для чего кому-то нужно взламывать ваш компьютер? Даже если вы самый что ни на есть обыкновенный пользователь и на вашем компьютере нет какой-либо ценной и секретной информации, не нужно пребывать в иллюзии, что ваш компьютер никому (в плане его взлома) не интересен. С точки зрения хакеров и людей, распространяющих вредоносные программы, он всё равно будет представлять ценность. Сегодня вредоносные программы стараются маскироваться и скрывать свою деятельность, чтобы в тайне выполнять заложенные в них функции.

Такими функциями могут быть:  
1) кража паролей от ваших электронных кошельков, почтовых ящиков, icq, сайтов, аккаунтов в различных сервисах и т. д. Украв пароль от почтового ящика, вредоносная программа может от вашего имени разослать по имеющимся в вашей адресной книге адресам письма с вложенными в них троянами или вирусами и т. д.

2) достаточно прибыльным "бизнесом" в наше время является организация DDoS-атак, которые могут направляться на любой сайт или сервер, даже не имеющий каких-либо существенных уязвимостей. В результате таких атак сервер перегружается запросами, идущими с многочисленных компьютеров в разных регионах мира и сайт, на который направлена атака, таким образом отключается. Многочисленные случаи DDoS-атак на различные сайты были бы невозможны, если бы в распоряжении организаторов этих атак не находилось большое количество компьютеров обычных ничего не подозревающих пользователей, заражённых троянами, которые по сигналу извне начинают все вместе посылать запросы на сервер, выбранный в качестве жертвы.

3) организация массовых рекламных рассылок также является, к сожалению, прибыльным бизнесом, и для таких целей также практикуется заражение компьютеров обычных пользователей троянов.

4) перечисленные цели являются наиболее типичными, но, в принципе, цели могут быть ограничены лишь фантазией автора троянов и вирусов. Троян может зашифровать, например, некоторые из имеющихся на вашем компьютере файлов и затем требовать плату за восстановление информации, заставлять ваш модем звонить на платные телефонные номера и т. д. Последние 2 года были отмечены эпидемией т. н. "блокировщиков" Windows, когда попавшие на компьютер вирусы блокировали работу компьютера и требовали отправить платную смс для его разблокировки.

**Источники опасностей.** Подхватить вредоносную программу, к сожалению, значительно легче, чем многие себе представляют. Для взлома компьютеров пользователей сети и кражи важных данных, например, паролей электронных платёжных систем, применяются следующие методы:

1) социальная инженерия - метод основанный на психологических приёмах, который существует и эффективно используется с самого начала развития компьютерных сетей и которому не грозит исчезновение. Список уловок, придуманных хакерами в расчёте на доверчивость пользователей, огромен. Вам могут прислать письмо от имени администрации сервиса с просьбой выслать им якобы утерянный пароль или письмо, содержащее безобидный, якобы файл, в который на самом деле спрятан троян, в расчёте на то, что из любопытства вы сами его откроете и запустите вредоносную программу.   
2) трояны и вирусы могут быть спрятаны в различных бесплатных, доступных для скачивания из интернета программах, которых огромное множество или на пиратских дисках, имеющихся в свободной продаже.   
3) взлом вашего компьютера может быть произведён через дыры в распространённом программном обеспечении, которых, к сожалению, довольно много и всё новые уязвимости появляются регулярно. Хакеры, в отличие от большинства пользователей, не следящих за уязвимостями и часто не скачивающих устраняющие их патчи, за обнаружением новых уязвимостей следят и используют их в своих целях. Для того, чтобы компьютер, имеющий уязвимости, был заражён, достаточно, например, всего лишь зайти на определённую страничку (ссылку на эту страничку хакер может прислать в письме).  
4) в последнее время получил распространение фишинг - создание поддельных сайтов, копирующих сайты известных фирм, сервисов, банков и т. д. Заманить вас на такой поддельный сайт могут разными способами, а цель - украсть данные вашего аккаунта (т. е. логин и пароль), которые вы обычно вводите на странице настоящего сайта.

**Меры по защите.**   
1) Установить файрволл (firewall). Хотя в Windows, начиная с версии XP и появился встроенный файрволл, его функциональность оставляет желать лучшего. Поэтому установить надёжный файрволл.  Некоторые из подобных программ можно скачать бесплатно или за небольшую сумму.   
2) Установите антивирусное и антишпионское ПО. Они должны быть свежими и регулярно скачивать базы с обновлениями через интернет. Антивирусное ПО должно запускаться автоматически при загрузке Windows и работать постоянно, проверяя запускаемые вами программы, в фоновом режиме. Обязательно проверяйте на вирусы перед первым запуском любые программы, которые вы где-либо скачиваете, покупаете. **Использование антивирусных программ**

Вирусы (в этой статье под этим словом подразумевается все вредоносное программное обеспечение) могут проникнуть на компьютер из Интернета, со съемных носителей, с оптических дисков и тому подобного. Чтобы противостоять этому, прежде всего, следует обязательно установить на компьютер антивирус. Существует большое разнообразие антивирусных решений, как платных, так и бесплатных. Вам придется самим решить, каким решением воспользоваться. Из бесплатных антивирусов наиболее популярны[Avast](http://softuhitel.com/besplatnye-antivirusy/avast-free-antivirus/)!, [Avira AntiVir](http://softuhitel.com/besplatnye-antivirusy/avira-free-antivirus/" \t "_blank), [AVG Antivirus](http://softuhitel.com/besplatnye-antivirusy/avg-anti-virus-free/), [Microsoft Security Essentials](http://softuhitel.com/besplatnye-antivirusy/microsoft-security-essentials/" \t "_blank) (при установке данной программы будет проверяться подлинность вашей копии Windows). Платные решения имеют некоторые преимущества перед бесплатными, в частности более частые обновления антивирусных баз, дополнительные модули безопасности и другие компоненты. Не существует 100% защиты от вирусного заражения, потому что сначала разрабатывается вирус, а уже потом появляются средства для его нейтрализации.

Убедитесь, что у вас в настройках системы включен сетевой экран — брандмауэр (файрволл). Брандмауэр защищает компьютер от сетевых атак и контролирует выход программ в Интернет. В операционную систему Windows установлен штатный брандмауэр. Правда он уступает специализированным брандмауэрам, но лучше такая защита, чем вообще никакой.

Если с вирусами справиться невозможно, то можно воспользоваться специальным загрузочным диском с антивирусной программой. Такие диски созданы многими производителями антивирусов и такой образ можно скачать с сайта производителя совершенно бесплатно, например Dr.Web Live CD, Kaspersky Rescue Disk и другие им подобные решения. Кроме официальных, существует также много подобных самодельных образов. Такие образы включают большое количество программ. После скачивания образ нужно записать на диск, а после этого уже загружаться с диска для сканирования и лечения компьютера. Проверить файлы на компьютере можно и в Интернете, через онлайн-сканеры антивирусных компаний. Например, сервис VirusTotal проверяет файл с помощью 43 (на сегодняшний день) онлайновых программ.

Следует помнить, что в Интернете существует множество фальшивых антивирусов. Вы наверняка встречали в Интернете такие всплывающие объявления, в которых написано,  что ваш компьютер заражен. Фальшивые антивирусы находят на вашем компьютере множество вирусов и предлагают загрузить программу для лечения вашего компьютера. Эта программа сама затем станет источником вирусов.

Для лечения от вирусов-блокираторов в антивирусных компаниях созданы специальные онлайновые службы, на которых вы можете бесплатно получить код разблокировки для вашего компьютера. Также для решения этой проблемы были созданы специальные программы.

3) Своевременно скачивайте и устанавливайте все критические обновления для Windows, Internet Explorer и т. п.   
4) Не устанавливайте или удалите лишние ненужные службы Windows, которые не используете, например, службу доступа к файлам и принтерам и т. п. Это ограничит возможности хакеров по доступу к вашему компьютеру.   
5) Не открывайте подозрительные письма странного происхождения, не поддавайтесь на содержащиеся в них сомнительные предложения лёгкого заработка, не высылайте никому пароли от ваших аккаунтов, не открывайте прикреплённые к письмам подозрительные файлы.

6) Не используйте простые пароли. Нельзя в качестве паролей использовать простые комбинации символов, вроде "qwerty" или "666666". Такой пароль будет взломан программой для перебора паролей за считанные секунды. Не используйте короткие пароли (меньше 6 символов), не используйте в качестве паролей слова, которые есть в словаре.

7) Будьте осторожны при выходе в интернет из мест общего пользования (например, интернет-кафе), а также при использовании прокси-серверов. Пароли, который вы вводите, в этом случае, с большей вероятностью могут быть украдены.  
8) Не посещайте сайты сомнительной тематики. Подобные сайты являются основным источником впаривания троянов пользователям интернета, при помощи использования уязвимостей в Internet Explorer и др. подобных программах.   
10) Даже если у вас безлимитный доступ, всё равно следите за траффиком - его непонятное возрастание может быть свидетельством активности вредоносной программы, а также отключайте соединение с интернетом тогда, когда оно не используется.

**2.3 Безопасный интернет детям: как общество защищает ребенка от негативного влияния сети.**

30 октября в рамках Всероссийского инфоурока, который был инициирован Советом Федерации РФ, в нашей школе проходил день безопасного интернета.

На уроках информатики и на классных часах были проведены уроки безопасности школьников в сети Интернет. Они были нужны для обеспечения информационной безопасности несовершеннолетних обучающихся и воспитанников путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде. В рамках урока «Интернет-безопасность» обучающиеся познакомились с международными стандартами в области информационной безопасности детей, которые отражены в российском законодательстве. Особое внимание обучающихся обращено на классификацию вредоносных информационных ресурсов: - информация, причиняющая вред здоровью и (или) развитию детей; - информация, запрещенная для распространения среди детей; - информация, ограниченная для распространения среди детей определенных возрастных категорий. На уроке затронуты следующие аспекты: - перечень рисков, подстерегающих ребенка в сети Интернет; - рекомендации по грамотному использованию электронной почты; - технологии безопасного общения в средах мгновенного обмена сообщениями.

Основной ожидаемый результат - в ходе урока Интернет - безопасности – дети должны научиться делать более безопасным и полезным свое время пребывания в сети Интернет и иных информационно телекоммуникационных сетях, а именно: - критически относиться к сообщениям и иной информации, распространяемой в сетях Интернет, мобильной (сотовой) связи, посредством иных электронных средств массовой коммуникации; - отличать достоверные сведения от недостоверных, вредную для них информацию от безопасной; - избегать навязывания им информации, способной причинить вред их здоровью, нравственному и психическому развитию, чести, достоинству и репутации; распознавать признаки злоупотребления их неопытностью и доверчивостью, попытки вовлечения их в противоправную и иную антиобщественную деятельность; - распознавать манипулятивные техники, используемые при подаче рекламной и иной информации; критически относиться к информационной продукции, распространяемой в информационно-телекоммуникационных сетях; - анализировать степень достоверности информации и подлинность ее источников; применять эффективные меры самозащиты от нежелательных.

Мы узнали о полезных ссылках **(**1) http://www.kaspersky.ru – антивирус «Лаборатория Касперского»; 2) http://www.onlandia.org.ua/rus/ - безопасная web-зона; 3) http://www.interneshka.net – международный онлайн-конкурс по безопасному использованию Интернета; 4) http://www.saferinternet.ru – портал Российского Оргкомитета по безопасному использованию Интернета; 5) http://content-filtering.ru – Интернет СМИ «Ваш личный Интернет»; 6) http://www.rgdb.ru – Российская государственная детская библиотека), о существовании лиги безопасного интернета, ее деятельности, организаторах и руководителях.

**Лига безопасности интернета** – организация, осуществляющая мониторинг сети Интернет. Сегодня является самым востребованным кластером у большинства населения планеты, у которых вызывает определенные сомнения по поводу безопасности в сети. Она была создана для решения проблем защиты участников сети 6 лет назад. Цель деятельности данного объединения заключается в противодействии хакерским атакам, а также в распространении программ контроля над популяризацией в интернете запрещенного видео. Лигу учредили с надеждой на решение глобальных проблем сети, связанных с распространением вирусных ботов и незаконного контента. Спектр деятельности и участники организации Лига безопасного интернета создавалась на базе 5 крупных провайдеров, которые должны были организовать специальную группу сотрудников, отслеживающих ситуацию в сети, и решать проблемы, связанные с внедрением вирусов на определенные сайты. Лига распространяет тематические рекламные ролики, заставляющие человека задуматься о том, что он просматривает и необходима ли эта информация ему на самом деле. Организация имеет постоянно обновляющуюся базу запрещенных сайтов, и любой человек может ознакомиться с перечнем страниц, представляющих опасность для пользователя. Компания безопасности интернета имеет в своем бюджете более 50 миллионов долларов, которые расходуются на зарплату сотрудникам и разработку новых антишпионских программ.

В Лиге сейчас находится несколько десятков различных крупных организаций, представляющих широкий спектр: начиная с мобильных операторов и заканчивая поисковыми системами. Самыми известными такими компаниями являются: Антивирусная сеть Касперского; Сеть Мой Мир; МегаФон; Группа Ростелеком.

Главными задачами, выполняемыми Лигой, являются: Искоренение детской порнографии; Борьба с террористическими течениями посредством сети; Фильтр сайтов на предмет педофилии; Создание добровольческих кибердружин для осуществления постоянного мониторинга сайтов.

Различными спонсорами Лиге ежегодно перечисляются специальные пожертвования, которые тратятся на корректировку курса компании и изменение ее политики. При этом, по сведениям некоторых российских провайдеров, компания создавалась не с целью контроля безопасности, а для защиты от распространения антиправительственных выступлений.

Сотрудники Организации безопасности интернета по большей части работают на добровольных началах, а провайдеры вносят ежегодные суммы в специальный фонд для борьбы с хакерами и экстремистами. Кибердружины также осуществляют поиск интернет-мошенников и преступников, пытающихся обогатиться посредством создания липовых компаний и незаконных сайтов. Фирмой инициирована организация информационного блока, который запрещает сайты с недетским контентом, допуская к просмотру только белые каналы и тем самым ограждая детей от опасных сведений.  
**Волонтерское движение.**

У нас в школе очень активно волонтерское движение. Мы волонтеры не остались в стороне и от акции «безопасный интернет». Участниками акции стали обучающиеся 4-11 классов, Волонтерами были подготовлены 5 - классов пятиминутки безопасности «Дети в Интернете», а также презентации, памятки, листовки, буклеты. В течение всего дня волонтёры провели беседы, смотрели вместе с малышами видеоролики на портале http://detionline.com/video/professiona «Безопасный Интернет детям», «Интернет может помочь в образовании», «Интернет зависимость» и другие.

Детей интересовали такие вопросы, как: Сколько времени можно проводить в Интернете?  
Что такое интернет-зависимость и как с ней бороться? Что такое персональные данные и как защитить их в Интернете?  
В рамках акции «Безопасный Интернет» были проведены встречи психолога с родителями, в которых приняли участие 42 человека. Главная цель мероприятия – информирование обучающихся и родителей об основных онлайн-рисках, с которыми российские школьники сталкиваются в Интернете, а также о способах профилактики и эффективного совладания с ними. Администрация школы порекомендовала основные темы, поднимаемые для собраний с участием психолога: Как защитить ребёнка от негативного контента в Интернете? Что делать, если ребёнок завёл профиль в социальной сети? Как защититься от онлайн-мошенников?

**3. Вывод.**

Если ваш компьютер подключен к интернету, вы должны обеспечить ему максимальную защиту, от атак хакеров и от различного рода вредоносного программного обеспечения: компьютерных вирусов, сетевых червей и троянских программ.

Еще до того момента, как вы произвели подключение к интернету, вы должны подумать о том, как обезопасить себя в интернете. Проведя всего пару минут в интернете без надлежащей защиты, можно серьезно навредить своему компьютеру.

Для того, чтобы работа в интернете стала более или менее безопасной, необходимо следовать правилам безопасности как для компьютера, так и для себя.

**Заключение**   
Нет никакой разницы с какого устройства и с каким программным обеспечением вы заходите в интернет. Это может быть компьютер, ноутбук, планшет, смартфон, телефон — все равно. Интернет- радости и интернет - угрозы рядом с нами.  
Никто, однажды, узнав о преимуществах интернета, не сможет отказать от них. Но нельзя становиться рабом интернета информации, надо стараться стать хозяином информации.