Содержание:

Введение

При работе в Интернете или с другими устройствами пользователь и его компьютер подвергаются различным опасностям, связанным с загрузкой вредоносных и нежелательных программ или информации. Загрузка таких программ или информации может происходить незаметно для пользователя и без каких-либо осознанных действий с его стороны.

На сегодняшний день наблюдается такой этап, в котором при повышении доступности компьютерной техники и средств выхода в Интернет, уровень грамотности пользователей в сфере информационной безопасности остается низким.

Для повышения компьютерной грамотности пользователей необходимы сбор и упорядочивание информации о приемах безопасной работы в сети Интернет. Объектом исследования в данной работе является всемирная система объединенных компьютерных сетей для хранения и передачи информации Интернет, предметом исследования являются угрозы безопасности в Интернете и меры по их предотвращению.

Исследованием угроз безопасности занимается практически каждый разработчик комплектов программного обеспечения сетевой безопасности. В России наиболее известным считается Лаборатория Касперского, проводящая множественные исследования и публикующая большое количество материалов. Данные исследования несут большую ценность в качестве определяющих направление развития программного обеспечения, обеспечивающего сетевую безопасность.

Целью данной работы является повышение компьютерной грамотности пользователей сети Интернет посредством упорядочивания знаний и приемов безопасной работы. Задачами данной работы являются:

- формирование списка угроз безопасности с кратким перечнем мер по предотвращению этих угроз;
- выделение общих советов по защите информации;
- обзор основных понятий в сфере антивирусного обеспечения;

- выделение основных видов программного обеспечения, реализующих определенный метод сетевой безопасности, предназначенный для защиты пользователя и его компьютера от различного рода вредоносных программ и нежелательной информации при работе в Интернете;
- обзор конкретных примеров защиты информации.

1. Основные понятия борьбы с вирусами

1.1. Виды угроз безопасности

1.1.1. Кибервандализм, мошенническое программное обеспечение и другой вредоносный код

Раньше угрозы пользовательским компьютерам исходили чаще всего от кибервандалов, которые социально самовыражались нанесением компьютерного вреда, что чаще всего являлось самоцелью вандализма. Со временем киберпреступники осознали, что, получая доступ к данным пользователя, они могут использовать эти данные для получения незаконных доходов[1]. Чаще всего такими данными являются PIN-коды, пароли банковских карт, регистрационные данные и так далее. Для получения данных такого рода используются троянские программы. Бывает несколько разновидностей троянских программ: одни из них запоминают последовательность введенных знаков с клавиатуры, другие делают снимки экрана при вводе защищенных значений, третьи перехватывают информацию при отправке ее в интернет, есть и такие, которые предоставляют взломщику полное управление компьютером пользователя[2].

Вредоносные программы создаются на выполнение определенных действий и зачастую их функционал ограничен. Изначально вирусы не наносили вреда, единственной их целью было самораспространение. Но в результате ошибок, код некоторых самораспространяющихся программ мог наносить вредоносное действие. Несмотря на нанесение вреда пользователям, обычно они не были нацелены на сбор данных пользователей[3].

На сегодняшний день, вредоносный код, наоборот, не несет видимых нарушений работы компьютера, чтобы пользователь не обнаружил его присутствие. Такие троянские программы относят к категории шпионского программного обеспечения, которое собирает данные пользователей без их ведома[4] [6, 7, 9].

1.1.2. Хакерские атаки

Современные приложения, используемые пользователями, чрезвычайно сложны, поэтому нет ничего удивительного в том, что они содержат определенное количество неотслеженных уязвимостей. Хакеры занимаются тем, что самостоятельно находят эти уязвимости и используют их с целью получения данных пользователя. Первоначально хакерами считались высококвалифицированные специалисты, которые могли находить уязвимости систем и перекрывать их. Со временем от хакеров отделилась группа, которая стала использовать свои навыки с целью осуществления незаконных операций. Помимо кражи данных или установки вредоносного программного обеспечения, хакеры также могут использовать компьютер пользователя для рассылки спама или DDoS-атак[5].

Для защиты от хакерских атак рекомендуется установить и регулярно обновлять на своем компьютере такие виды программного обеспечения, как антивирус, защита от шпионских программ, файервол, анти-спам и технологии проактивной защиты. Помимо регулярных обновлений, которые лучше настроить автоматически, также следует осуществлять регулярную проверку системы, отслеживание получаемых файлов и резервное копирование важных данных[6] [6, 11].

1.1.3. Фишинг

Фишинг представляет собой особый вид компьютерного мошенничества, при котором осуществляется кража компьютерных данных через подложные сайты, которые выглядят в точности как оригинальные. Подложный сайт обычно заменяет банковский или другой финансовый и отправляет взломщику данные, введенные пользователем. Для распространения сайта обычно используются спам-рассылки[7] .

Не существует определенных программ для обнаружения фишинга, так как с технической точки зрения ничего вредоносного в данных сайтах нет. Но пользователь может избежать этого вида мошенничества, руководствуясь рядом правил:

- вероятность получения письма от банка с просьбой указания данных крайне мала, в таких случаях следует позвонить в банк для уточнения;
- не стоит переходить по ссылкам в электронных письмах в формате HTML, они могут содержать скрытую ссылку;

- необходимо регулярно проверять банковские выписки с целью своевременного обнаружения неопознанных операций;
- если письмо адресовано не лично Вам, в тексте письма обращение «Уважаемый клиент» или подобное, или адрес получателя не совпадет с вашим, это также подозрительно[8] [3, 11].

1.1.4. Кибер вымогательство

Кибервымогательство подразумевает размещение на компьютере пользователя вредоносного кода, шифрующего или блокирующего данные пользователя. Пользователя уведомляют о блокировке и предлагают перевести деньги на счет злоумышленника[9].

С целью защиты от кибервымогательства необходимо руководствоваться приведенными выше правилами по защите компьютера и регулярно сохранять резервные копии на случай невозможности расшифровки. В случае блокировки доступа к данным крайне не рекомендуется платить киберпреступникам, следует обратиться в службе технической поддержки, где специалисты смогут восстановить доступ[10] [1, 5].

1.1.5. Перехват по беспроводной сети

На сегодняшний день большинство пользователей персональных компьютеров используют беспроводной доступ к интернету, но лишь немногие из них соблюдают правила безопасности при соединении. При несоблюдении мер безопасности, злоумышленник может получить доступ к беспроводной сети или перехватывать передаваемые данные[11].

Для предотвращения получения злоумышленником доступа к сети необходимо установить собственный пароль на беспроводную точку доступа, включить шифрование трафика и сменить идентификатор устройства[12] [6, 11].

1.1.6. Спам

Спам представляет собой анонимные незапрошенные массовые рассылки рекламных сообщений по электронной почте. Лишь малая часть пользователей откликается на подобные рассылки, но даже этого хватает спамерам для получения дохода[13].

Для предотвращения получения спама рекомендуется настроить спам-фильтр, не реагировать на любые предложения в письмах, в том числе на ссылки «отписаться

от рассылки», не подтверждая тем самым активности своего почтового адреса, и не публиковать свой адрес на общедоступных ресурсах[14] [8, 11].

1.2. Общие советы по безопасности работы в Интернете

В первую очередь для безопасности в интернет-среде необходимо внимательно следить за актуальность установленного для безопасности программного обеспечения. Необходимо иметь полный комплект защитных программ, осуществлять регулярные обновления и проверки. Многие программы содержат функционал автоматического обновления и проверок, который следует настроить необходимым образом[15].

Каждую программу для безопасности необходимо настроить определенным образом, чтобы она осуществляла защитные мероприятия наиболее подходящим для конкретной системы образом. Некоторые пользователи имеют привычку отключать защитные программы при навязчивых уведомлениях, для предотвращения такого поведения следует указать в настройках требуемый уровень информирования.

Стоимость программы не всегда является показателем качества, зачастую популярное бесплатное решение выполняет защитный функционал куда лучше платного программного обеспечения[16].

В любом случае необходимо помнить, что не существует абсолютной защиты, поэтому требуется проводить определённый комплект мер по устранению дальнейших неприятностей. В первую очередь обязательно стоит делать резервные копии всех важных данных во избежание их утраты. Важную информацию не стоит хранить в открытом виде на подключенном к сети компьютере. Наиболее приемлемым решением будет перенос данных на систему, не подключенную к интернету, или шифрование[17] [6, 11].

1.3. Понятие компьютерного вируса

Компьютерный вирус — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные

области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи. Целью вируса является нарушение работы программно-аппаратных комплексов, удаление файлов, блокирование работы пользователей, приведение в негодность структур размещения данных или же приведение в негодность аппаратных комплексов компьютера[18].

Даже если автор вируса не планировал действий вредоносных эффектов, вредоносное программное обеспечение приводить к сбоям компьютера из-за ошибок, неучтенных тонкостей взаимодействия с операционной системой и другими программами. Кроме того, файлы вирусов обычно занимают некоторое место на накопителях информации и отбирают некоторые другие ресурсы системы. Поэтому вирусы относят к вредоносным программам[19].

Некомпетентные пользователи ошибочно относят к компьютерным вирусам и другие виды вредоносных программ — программы-шпионы и прочее. Известны десятки тысяч компьютерных вирусов, которые распространяются через Интернет по всему миру[20] [1, 3, 8].

На данный момент существует много разновидностей вирусов, различающихся по основному способу распространения и функциональности. Если изначально вирусы распространялись на дискетах и других носителях, то сейчас доминируют вирусы, распространяющиеся через Интернет. Также меняется функциональность вирусов, которую они перенимают от других видов программ[21].

Попытка создать стандарт предпринималась на встрече CARO в 1991 году, но, тем не менее, в настоящее время не существует единой системы классификации и именования вирусов. Обычно вирусы принято разделять:

- по поражаемым объектам (файловые вирусы, загрузочные вирусы, сценарные вирусы, макровирусы, вирусы, поражающие исходный код), файловые вирусы дополнительно подразделяют по механизму заражения:
  - паразитирующие, добавляющие себя в исполняемый файл, перезаписывающие невосстановимо портят зараженный файл;
  - «спутники», идущие отдельным файлом[22];
- по поражаемым операционным системам и платформам (DOS, Microsoft Windows, Unix, Linux);
- по технологиям, используемым вирусом (полиморфные вирусы, стелс-вирусы, руткиты);

- по языку, на котором написан вирус (ассемблер, высокоуровневый язык программирования, сценарный язык и др.);
- по дополнительной вредоносной функциональности (бэкдоры, кейлоггеры, шпионы, ботнеты и др.)[23] [3, 6, 7].

1.4. Способы распространения компьютерных вирусов

Компьютерные вирусы являются программами, которые могут «размножаться» и скрытно внедрять свои копии в файлы, загрузочные сектора дисков и документы.

В настоящее время известно несколько десятков тысяч вирусов, заражающих компьютеры различных операционных систем и распространяющихся по компьютерным сетям. Обязательное свойство компьютерного вируса — способность к самокопированию[24].

Активизация компьютерного вируса нередко вызывает уничтожение программ и данных.

По «среде обитания» вирусы разделяют на файловые, загрузочные, макровирусы и сетевые[25] [1, 8].

Файловые вирусы

Файловые вирусы различными способами внедряются в исполняемые файлы (программы) и обычно активизируются при их запуске. После запуска зараженной программы вирусы находятся в оперативной памяти компьютера и остаются активными (т. е. могут заражать другие файлы) вплоть до момента выключения компьютера или перезагрузки операционной системы[26].

Профилактическая защита от файловых вирусов состоит в том, чтобы не запускать на исполнение файлы, полученные из сомнительного источника и предварительно не проверенные антивирусными программами[27] [3].

Загрузочные вирусы

Загрузочные вирусы записывают себя в загрузочный сектор диска. При загрузке операционной системы с зараженного диска вирусы внедряются в оперативную память компьютера[28].

Профилактическая защита от таких вирусов состоит в отказе от загрузки операционной системы с гибких дисков и установке в BIOS вашего компьютера защиты загрузочного сектора от изменений[29] [6, 8].

Макровирусы

Макровирусы заражают файлы документов Word и электронных таблиц Excel. Макровирусы фактически представляют собой макрокоманды (макросы), которые встраиваются в документ[30].

После загрузки зараженного документа в приложение макровирусы постоянно присутствуют в памяти компьютера и могут заражать другие документы. Угроза заражения прекращается только после закрытия приложения[31].

Профилактическая защита от макровирусов состоит в предотвращении запуска вируса. При открытии документа в приложениях Word и Excel сообщается о присутствии в них макросов и предлагается запретить их загрузку. Выбор запрета на загрузку макросов надежно защитит ваш компьютер от заражения макровирусами, однако отключит и полезные макросы, содержащиеся в документе [32] [3, 7, 9].

Сетевые вирусы

По компьютерной сети могут распространяться и заражать компьютеры любые обычные вирусы. Это происходит, например, при получении зараженных файлов с серверов файловых архивов. Однако существуют и специфические сетевые вирусы, которые используют для своего распространения электронную почту и Всемирную паутину[33].

«Почтовый» вирус содержится во вложенных в почтовое сообщение файлах. Если получатель сообщения откроет вложенный файл (вирус), то произойдет заражение компьютера. Этого не случится после чтения самого почтового сообщения, так как заражено не почтовое сообщение, а вложенный в него файл[34] [6, 7].

1.5. Виды программ для защиты компьютера при работе в Интернете

Межсетевой экран

Межсетевой экран или брандмауэр предназначен для защиты компьютера от несанкционированного доступа к нему из локальной сети или Интернета. Он также позволяет подключаться к сети только тем программам, установленным на компьютере пользователя, которым это разрешено[35].

В первую очередь межсетевой экран помогает предотвратить попадание в компьютер вредоносных программ, заблокировать вредоносным программам, попавшим в компьютер иными путями, доступ в Интернет (для передачи похищенной информации, самообновления и т.д.) и предотвратить несанкционированный доступ к информации, находящейся в памяти компьютера [36] [7, 9].

Антивирус

Антивирус предназначен для обнаружения, предотвращения выполнения и удаления вредоносных программ, а также «лечения» программ и файлов пользователя, зараженных компьютерными вирусами. Некоторые антивирусы умеют также противодействовать более широкому спектру вредоносных программ, которые не относятся к компьютерным вирусам, например, программам для показа рекламы, кражи персональных данных и подобным. Антивирус помогает в борьбе с компьютерными вирусами не только при работе в Интернете[37].

В первую очередь антивирус помогает предотвратить порчу или кражу информации, размещенной в памяти компьютера[38] [6, 11].

Программа для борьбы со шпионскими и рекламными программами

Программа для борьбы со шпионскими и рекламными программами предназначена для обнаружения, предотвращения выполнения и удаления соответствующих программ, а также «лечения» программ и файлов пользователя, зараженных ими. Часто аналогичными функциями обладают и антивирусы[39].

В первую очередь программа для борьбы со шпионскими и рекламными программами помогает предотвратить кражу информации, размещенной в памяти компьютера, и демонстрацию пользователю нежелательной рекламы[40] [5, 7].

Программа для блокирования рекламы

Программа для блокирования рекламы служит для удаления баннеров и иных видов рекламы с просматриваемых пользователем веб-страниц. Часто такие программы могут использоваться для удаления из просматриваемых страниц

различных элементов, представляющих потенциальную угрозу для пользователей и их приватности, например, счетчиков посещений веб-страниц[41].

В первую очередь программа для блокирования рекламы предназначена для очистки просматриваемых страниц от «информационного мусора», затрудняющего доступ к интересующей пользователя информации, угрожающего безопасности его компьютера и конфиденциальности пользователя[42] [4, 9].

Контентный фильтр

Контентный фильтр предназначен для ограничения доступа к размещенной в Интернете информации по различным критериям, например – содержащей ненормативную лексику или порнографические изображения[43].

В первую очередь контентный фильтр предназначен для предотвращения доступа детей к неподходящей для них информации[44] [5, 7].

Системы комплексной защиты

Системы комплексной защиты сочетают в себе сразу несколько функций вышеописанных программ, например – межсетевого экрана и антивируса. Такие системы предназначены для предотвращения сразу нескольких видов угроз, но не обязательно так же эффективны, как несколько отдельных программ, каждая из которых имеет лишь одну функцию[45] [4].

1.6. Понятие антивирусной программы

Антивирусная программа является специализированной программой для обнаружения компьютерных вирусов и нежелательных программ как таковых и восстановления измененных такими программами файлов, а также для предотвращения заражения отдельных файлов или всей системы вредоносным кодом[46].

На данный момент антивирусное программное обеспечение разрабатывается, в основном, для операционных систем семейства Windows от компании Microsoft. Данная популярность вызвана большим количеством вредоносных программ именно под эту платформу, что, в свою очередь, вызвано большой популярностью этого семейства. В настоящий момент на рынок начинают выходить продукты для других операционных систем, таких как Linux и Mac OS X. Это вызвано началом

распространения компьютерных вирусов и под эти платформы, хотя UNIX-подобные системы традиционно пользуются репутацией более устойчивых к воздействию вредоносных программ[47].

Пользователи операционных систем для мобильных устройств также подвержены риску заражения вредоносным программным обеспечением, поэтому некоторые разработчики антивирусных программ выпускают дополнительные версии продуктов для таких устройств[48] [1, 5, 6].

По итогам данной работы можно сделать вывод, что сфера вирусов разрастается с каждым днем и требуются контрмеры в виде постоянно развивающейся сферы антивирусного обеспечения.

2. Обзор конкретных примеров защиты информации

2.1 Идентификации и аутентификации

Идентификация в информационных системах представляет собой процедуру выявления идентификатора для субъекта идентификации, однозначно идентифицируя данного субъекта в информационной системе. При выполнении процедуры идентификации в информационной системе субъекту предварительно назначается соответствующий идентификатор[49].

В системах защиты после процедуры идентификации чаще всего следует аутентификация, подтверждающая идентификацию субъекта. При этом достоверность идентификации полностью определяется уровнем достоверности выполненной процедуры аутентификации[50].

Существует 3 фактора аутентификации: что-то, что мы знаем; что-то, что мы имеем; что-то, что является частью нас.

«Что-то, что мы знаем» является паролем, представляющим собой некоторые тайные сведения, которыми должен обладать только авторизованный субъект. Паролем обычно представляет собой текстовое слово, речевое слово, комбинацию для замка или личный идентификационный номер.

«Что-то, что мы имеем» является устройством аутентификации, представляющим собой неповторимый предмет, которым обладает субъект, представляющим собой неповторимый предмет, которым обладает субъект. Неповторимый предмет обычно представляет собой ключ от замка, личную печать, файл данных для компьютера.

«Что-то, что является частью нас» является биометрикой, которая представляет собой физическую особенность субъекта. Сущность обычно представляет собой отпечаток пальца или ладони, портрет, голос или особенность глаза[51].

Биометрические системы аутентификации представляют собой системы аутентификации, которые используют для удостоверения личности людей их биометрические данные.

Биометрическая аутентификация является процессом проверки подлинности и доказательства заявленного пользователем имени, через предъявление пользователем своего биометрического образа и путем преобразования этого образа в соответствии с заранее определенным протоколом аутентификации[52].

Не следует путать данные системы с системами биометрической идентификации, которыми являются такие как системы распознавания лиц водителей или биометрические средства учёта рабочего времени.

Биометрические системы идентификации самостоятельно оформляют заявку пользователя на имя при сканировании биометрических данных. Биометрические системы аутентификации работают в активном, а не пассивном режиме и почти всегда подразумевают авторизацию.

Основным достоинством биометрических систем является удобство для пользователей, так как человеческие параметры не могут быть скопированы или украдены[53] [2, 5, 7].

2.2 Ограничения доступа в системах электронного документооборота

При электронном документообороте документы в организации распространяются не физически, а путем предоставления сотрудникам, имеющим на это право доступа к электронным копиям документов, хранящимся на сервере системы.

Такой механизм доступа к документам позволяет организовать работу всех сотрудников территориально-распределенной компании в едином информационном пространстве и нивелировать влияние удаленности отдельных пользователей на скорость их работы с документами.

Все документы компании располагаются в системе электронного документооборота в виде иерархии представлений документов или в отдельных базах данных[54].

Формироваться папки могут по хронологическому, алфавитному, номинальному или корреспондентскому признакам.

В папку помещается не сам документ, а ссылка на него, поэтому он может быть отнесен к нескольким папкам, обеспечивая различные варианты классификации одного и того же документа в зависимости от потребностей пользователя.

Такие электронные библиотеки обеспечивают централизованное хранение всех необходимых документов компании, удобство и оперативность доступа к ним. При этом каждый сотрудник "видит" именно те документы, которые нужны ему для работы. Как это возможно?[55]

Одной из главных задач специальной настраиваемой базы данных систем электронного документооборота является управление доступом пользователей к документам[56].

Такая база обычно содержит информацию о таких параметрах, как иерархия штатной структуры организации, которая состоит из штатных и структурных единиц, и функциональные роли[57].

В такой базе прописываются права на различные операции и доступ к документам штатной или структурной единицы или ее замещающего и функциональные роли, которые определяют набор доступных функций. Набор видов доступа варьируется от одной системы электронного документооборота к другой, но в целом можно сформировать такую классификацию доступа к документам:

- общий доступ, при котором документ доступен для ознакомления всем лицам;
- доступ по типу документа;
- регулируемый доступ, при котором документ доступен сотрудникам, имеющем на это право[58].

У сотрудников могут быть права:

- полный контроль над документом с возможностью создавать, редактировать и удалять;
- право доступа к регистрационно-контрольной карточке документа;
- право редактировать, но не уничтожать документ;
- право читать, но не редактировать документ;
- право оставлять комментарии к документу, но не создавать новые версии и не редактировать документ;
- полное отсутствие прав доступа к документу[59].

Настройка прав и ограничений доступа к документам может осуществляться как на уровне системы в отражающей организационную структуру компании базе, так и на уровне пользователя, который может сам определить список сотрудников, имеющих возможность просматривать документ, редактировать его и осуществлять другие действия[60] [2, 5, 10].

2.3 Антивирусная программа

Антивирусная программа является специализированной программой для обнаружения компьютерных вирусов и нежелательных программ как таковых и восстановления измененных такими программами файлов, а также для предотвращения заражения отдельных файлов или всей системы вредоносным кодом[61].

На данный момент антивирусное программное обеспечение разрабатывается, в основном, для операционных систем семейства Windows от компании Microsoft. Данная популярность вызвана большим количеством вредоносных программ именно под эту платформу, что, в свою очередь, вызвано большой популярностью этого семейства. В настоящий момент на рынок начинают выходить продукты для других операционных систем, таких как Linux и Mac OS X. Это вызвано началом распространения компьютерных вирусов и под эти платформы, хотя UNIX-подобные системы традиционно пользуются репутацией более устойчивых к воздействию вредоносных программ[62].

Пользователи операционных систем для мобильных устройств также подвержены риску заражения вредоносным программным обеспечением, поэтому некоторые разработчики антивирусных программ выпускают дополнительные версии продуктов для таких устройств.

Классифицировать антивирусные продукты можно сразу по нескольким признакам, таким, как: используемые технологии антивирусной защиты, функционал продуктов, целевые платформы[63].

По используемым технологиям защиты антивирусные продукты делятся на:

- классические антивирусные продукты, применяющие только сигнатурный метод детектирования;
- продукты проактивной антивирусной защиты, применяющие только проактивные технологии антивирусной защиты;
- комбинированные продукты, применяющие как сигнатурные методы защиты, так и проактивные[64].

По функционалу антивирусные продукты делятся на антивирусные продукты, обеспечивающие только антивирусную защиту, и комбинированные продукты, которые обеспечивают не только защиту от вредоносных программ, но и фильтрацию спама, шифрование и резервное копирование данных и другие функции[65].

По целевым платформам антивирусные продукты делятся на:

- антивирусные продукты для операционных систем семейства Windows;
- антивирусные продукты для операционных систем семейства *NIX, к которому относятся операционные системы Linux, BSD и другие подобные;
- антивирусные продукты для операционных систем семейства MacOS;
- антивирусные продукты для мобильных платформ Windows Phone 7, Windows Mobile, BlackBerry, Android, iOS, Symbian и других подобных.

Антивирусные продукты для корпоративных пользователей можно также классифицировать по объектам защиты:

- антивирусные продукты для защиты рабочих станций;
- антивирусные продукты для защиты терминальных и файловых серверов;
- антивирусные продукты для защиты Интернет и почтовых шлюзов;
- антивирусные продукты для защиты серверов виртуализации;
- антивирусные продукты для других объектов защиты[66] [1, 2, 5, 8].

По итогам данной главы можно сказать, что существует множество способов защиты информации в различных сферах. Разнообразие информации порождает разнообразие методов взлома, что ведет к увеличению количества мер защиты.

Заключение

В ходе данной работы были рассмотрены понятия антивируса, проведена классификация антивирусного и другого защитного программного обеспечения. Также в работе были изучены понятия основных видов угроз безопасности при работе в сети Интернет, таких как кибервандализм, хакерские атаки, фишинг, кибервымогательство, перехват по беспроводным сетям и спаминг. По каждой из угроз приведен определенный перечень мер, помогающий устранить или избежать угрозы сетевой безопасности.

При анализе основных видов угроз был сформирован перечень необходимых типов программ, поддерживающих безопасность. Такими программами являются межсетевые экраны, антивирусы, программы для борьбы со шпионскими и рекламными программами, программы для блокирования рекламы, контентные фильтры и системы комплексной защиты.

В целом, по итогам работы можно сказать, что любой начинающий пользователь сети Интернет, не использующий специфические сервисы сомнительного качества, может с высокой степенью безопасности использовать все возможности сети при условии соблюдения всех правил, указанных в данной работе.

Помимо всего прочего, необходимо отметить, что сетевые угрозы постоянно развиваются, ввиду чего пользователю необходимо осуществлять самостоятельное слежение за тенденциями в сетевой безопасности и своевременно осуществлять установку специализированных программ, использующих современные методы защиты.

Несмотря на широкую распространенность антивирусных программ, угрозы и количество вирусов продолжают увеличиваться. Чтобы справиться с ними, необходимо создавать более универсальные и качественно-новые антивирусные программы, которые будут включать в себя все положительные качества своих предшественников. К сожалению, на данный момент не существует антивирусной программы, гарантирующей 100% защиту от всех разновидностей вирусов, но некоторые фирмы, такие как Лаборатория Касперского, на сегодняшний день вплотную приблизились к результату.

Защищенность от вирусов также зависит от грамотности пользователя. Применение вкупе всех видов защит позволит достигнуть высокой безопасности

компьютера, и соответственно, информации.

Список используемой литературы

1. Галатенко В. А. О каналах скрытых, потайных, побочных. И не только / В. А. Галатенко // Информационный бюллетень JET INFO, 2012 – №4. – С. 16-22.
2. Гафнер В. В. Информационная безопасность: учеб. пособие / В. В. Гафнер. — Ростов на Дону: Феникс, 2010. — 324 с.
3. Доля А. Защита конфиденциальных данных на ноутбуках и КПК / А. Доля // "Экспресс Электроника", 2013 - №6. – С. 33-42.
4. Заика А. Компьютерная безопасность / А. Заика. – М.: Рипол Классик, 2013. – 160 с.
5. Климентьев А. Компьютерные вирусы и антивирусы. Взгляд программиста / А. Климентьев. – М.: ДМК Пресс, 2013 – 656 с.
6. Леонов В. Как ломаются беспроводные сети / Василий Леонов // Тестовая лаборатория Ferra, 2015 – №1. – С. 5-18.
7. Лукацкий А. Предотвращение сетевых атак: технологии и решения / А. Лукацкий // "Экспресс Электроника", 2014 - №3. – С. 12-21.
8. Малюк А. А. Теория защиты информации / А. А. Малюк. — М.: Горячая линия - Телеком, 2012. — 184 с.
9. Патий Е. Безопасность в сетях хранения данных /Евгений Патий // "Экспресс-Электроника", 2012 – №2. – С. 32-46.
10. Чернов В. Н. Системы электронного документооборота / В. Н. Чернов. – М: РАГС, 2009. – 84 с.
11. Щеглов А. Защита информации в корпоративных приложениях. Частные решения / А. Щеглов, А. Оголюк. // "Экспресс Электроника", 2014 - №4. – С. 55-67.

1. Лукацкий А. Предотвращение сетевых атак: технологии и решения / А. Лукацкий // "Экспресс Электроника", 2014 - №3. – С. 12. ↑

2. Леонов В. Как ломаются беспроводные сети / Василий Леонов // Тестовая лаборатория Ferra, 2015 – №1. – С. 5. ↑

3. Патий Е. Безопасность в сетях хранения данных /Евгений Патий // "Экспресс-Электроника", 2012 – №2. – С. 32. ↑

4. Леонов В. Как ломаются беспроводные сети / Василий Леонов // Тестовая лаборатория Ferra, 2015 – №1. – С. 6. ↑

5. Щеглов А. Защита информации в корпоративных приложениях. Частные решения / А. Щеглов, А. Оголюк. // "Экспресс Электроника", 2014 - №4. – С. 55. ↑

6. Леонов В. Как ломаются беспроводные сети / Василий Леонов // Тестовая лаборатория Ferra, 2015 – №1. – С. 7. ↑

7. Щеглов А. Защита информации в корпоративных приложениях. Частные решения / А. Щеглов, А. Оголюк. // "Экспресс Электроника", 2014 - №4. – С. 56. ↑

8. Доля А. Защита конфиденциальных данных на ноутбуках и КПК / А. Доля // "Экспресс Электроника", 2013 - №6. – С. 35. ↑

9. Галатенко В. А. О каналах скрытых, потайных, побочных. И не только / В. А. Галатенко // Информационный бюллетень JET INFO, 2012 – №4. – С. 16. ↑

10. Климентьев А. Компьютерные вирусы и антивирусы. Взгляд программиста / А. Климентьев. – М.: ДМК Пресс, 2013 – С. 258. ↑

11. Леонов В. Как ломаются беспроводные сети / Василий Леонов // Тестовая лаборатория Ferra, 2015 – №1. – С. 7. ↑

12. Щеглов А. Защита информации в корпоративных приложениях. Частные решения / А. Щеглов, А. Оголюк. // "Экспресс Электроника", 2014 - №4. – С. 57. ↑

13. Малюк А. А. Теория защиты информации / А. А. Малюк. — М.: Горячая линия - Телеком, 2012. — С. 95. ↑

14. Щеглов А. Защита информации в корпоративных приложениях. Частные решения / А. Щеглов, А. Оголюк. // "Экспресс Электроника", 2014 - №4. – С. 58. ↑

15. Леонов В. Как ломаются беспроводные сети / Василий Леонов // Тестовая лаборатория Ferra, 2015 – №1. – С. 9. ↑

16. Щеглов А. Защита информации в корпоративных приложениях. Частные решения / А. Щеглов, А. Оголюк. // "Экспресс Электроника", 2014 - №4. – С. 60. ↑

17. Леонов В. Как ломаются беспроводные сети / Василий Леонов // Тестовая лаборатория Ferra, 2015 – №1. – С. 11. ↑

18. Галатенко В. А. О каналах скрытых, потайных, побочных. И не только / В. А. Галатенко // Информационный бюллетень JET INFO, 2012 – №4. – С. 12. ↑

19. Малюк А. А. Теория защиты информации / А. А. Малюк. — М.: Горячая линия - Телеком, 2012. — С. 109. ↑

20. Доля А. Защита конфиденциальных данных на ноутбуках и КПК / А. Доля // "Экспресс Электроника", 2013 - №6. – С. 33. ↑

21. Леонов В. Как ломаются беспроводные сети / Василий Леонов // Тестовая лаборатория Ferra, 2015 – №1. – С. 11. ↑

22. Доля А. Защита конфиденциальных данных на ноутбуках и КПК / А. Доля // "Экспресс Электроника", 2013 - №6. – С. 39. ↑

23. Лукацкий А. Предотвращение сетевых атак: технологии и решения / А. Лукацкий // "Экспресс Электроника", 2014 - №3. – С. 18. ↑

24. Малюк А. А. Теория защиты информации / А. А. Малюк. — М.: Горячая линия - Телеком, 2012. — С. 94. ↑

25. Галатенко В. А. О каналах скрытых, потайных, побочных. И не только / В. А. Галатенко // Информационный бюллетень JET INFO, 2012 – №4. – С. 20. ↑

26. Доля А. Защита конфиденциальных данных на ноутбуках и КПК / А. Доля // "Экспресс Электроника", 2013 - №6. – С. 40. ↑

27. Малюк А. А. Теория защиты информации / А. А. Малюк. — М.: Горячая линия - Телеком, 2012. — С. 99. ↑

28. Леонов В. Как ломаются беспроводные сети / Василий Леонов // Тестовая лаборатория Ferra, 2015 – №1. – С. 14. ↑

29. Малюк А. А. Теория защиты информации / А. А. Малюк. — М.: Горячая линия - Телеком, 2012. — С. 111. ↑

30. Лукацкий А. Предотвращение сетевых атак: технологии и решения / А. Лукацкий // "Экспресс Электроника", 2014 - №3. – С. 19. ↑

31. Патий Е. Безопасность в сетях хранения данных /Евгений Патий // "Экспресс-Электроника", 2012 – №2. – С. 44. ↑

32. Доля А. Защита конфиденциальных данных на ноутбуках и КПК / А. Доля // "Экспресс Электроника", 2013 - №6. – С. 39. ↑

33. Леонов В. Как ломаются беспроводные сети / Василий Леонов // Тестовая лаборатория Ferra, 2015 – №1. – С. 12. ↑

34. Лукацкий А. Предотвращение сетевых атак: технологии и решения / А. Лукацкий // "Экспресс Электроника", 2014 - №3. – С. 15. ↑

35. Патий Е. Безопасность в сетях хранения данных /Евгений Патий // "Экспресс-Электроника", 2012 – №2. – С. 41. ↑

36. Лукацкий А. Предотвращение сетевых атак: технологии и решения / А. Лукацкий // "Экспресс Электроника", 2014 - №3. – С. 19. ↑

37. Леонов В. Как ломаются беспроводные сети / Василий Леонов // Тестовая лаборатория Ferra, 2015 – №1. – С. 16. ↑

38. Щеглов А. Защита информации в корпоративных приложениях. Частные решения / А. Щеглов, А. Оголюк. // "Экспресс Электроника", 2014 - №4. – С. 55-67. ↑

39. Лукацкий А. Предотвращение сетевых атак: технологии и решения / А. Лукацкий // "Экспресс Электроника", 2014 - №3. – С. 21. ↑

40. Климентьев А. Компьютерные вирусы и антивирусы. Взгляд программиста / А. Климентьев. – М.: ДМК Пресс, 2013 – С. 263. ↑

41. Заика А. Компьютерная безопасность / А. Заика. – М.: Рипол Классик, 2013. – С. 103. ↑

42. Патий Е. Безопасность в сетях хранения данных /Евгений Патий // "Экспресс-Электроника", 2012 – №2. – С. 41. ↑

43. Лукацкий А. Предотвращение сетевых атак: технологии и решения / А. Лукацкий // "Экспресс Электроника", 2014 - №3. – С. 20. ↑

44. Климентьев А. Компьютерные вирусы и антивирусы. Взгляд программиста / А. Климентьев. – М.: ДМК Пресс, 2013 – С. 375. ↑

45. Заика А. Компьютерная безопасность / А. Заика. – М.: Рипол Классик, 2013. – С. 129. ↑

46. Галатенко В. А. О каналах скрытых, потайных, побочных. И не только / В. А. Галатенко // Информационный бюллетень JET INFO, 2012 – №4. – С. 22. ↑

47. Леонов В. Как ломаются беспроводные сети / Василий Леонов // Тестовая лаборатория Ferra, 2015 – №1. – С. 18. ↑

48. Климентьев А. Компьютерные вирусы и антивирусы. Взгляд программиста / А. Климентьев. – М.: ДМК Пресс, 2013 – С. 206. ↑

49. Гафнер В. В. Информационная безопасность: учеб. пособие / В. В. Гафнер. — Ростов на Дону: Феникс, 2010. — С. 134. ↑

50. Климентьев А. Компьютерные вирусы и антивирусы. Взгляд программиста / А. Климентьев. – М.: ДМК Пресс, 2013 – С. 285. ↑

51. Климентьев А. Компьютерные вирусы и антивирусы. Взгляд программиста / А. Климентьев. – М.: ДМК Пресс, 2013 – С. 473. ↑

52. Гафнер В. В. Информационная безопасность: учеб. пособие / В. В. Гафнер. — Ростов на Дону: Феникс, 2010. — С. 28. ↑

53. Лукацкий А. Предотвращение сетевых атак: технологии и решения / А. Лукацкий // "Экспресс Электроника", 2014 - №3. – С. 21. ↑

54. Чернов В. Н. Системы электронного документооборота / В. Н. Чернов. – М: РАГС, 2009. – С. 38. ↑

55. Гафнер В. В. Информационная безопасность: учеб. пособие / В. В. Гафнер. — Ростов на Дону: Феникс, 2010. — С. 276. ↑

56. Климентьев А. Компьютерные вирусы и антивирусы. Взгляд программиста / А. Климентьев. – М.: ДМК Пресс, 2013 – С. 524. ↑

57. Гафнер В. В. Информационная безопасность: учеб. пособие / В. В. Гафнер. — Ростов на Дону: Феникс, 2010. — С. 127. ↑

58. Чернов В. Н. Системы электронного документооборота / В. Н. Чернов. – М: РАГС, 2009. – С. 27. ↑

59. Климентьев А. Компьютерные вирусы и антивирусы. Взгляд программиста / А. Климентьев. – М.: ДМК Пресс, 2013 – С. 385. ↑

60. Галатенко В. А. О каналах скрытых, потайных, побочных. И не только / В. А. Галатенко // Информационный бюллетень JET INFO, 2012 – №4. – С. 22. ↑

61. Гафнер В. В. Информационная безопасность: учеб. пособие / В. В. Гафнер. — Ростов на Дону: Феникс, 2010. — С. 296. ↑

62. Малюк А. А. Теория защиты информации / А. А. Малюк. — М.: Горячая линия - Телеком, 2012. — С. 92. ↑

63. Климентьев А. Компьютерные вирусы и антивирусы. Взгляд программиста / А. Климентьев. – М.: ДМК Пресс, 2013 – С. 375. ↑

64. Гафнер В. В. Информационная безопасность: учеб. пособие / В. В. Гафнер. — Ростов на Дону: Феникс, 2010. — С. 268. ↑

65. Галатенко В. А. О каналах скрытых, потайных, побочных. И не только / В. А. Галатенко // Информационный бюллетень JET INFO, 2012 – №4. – С. 22. ↑

66. Гафнер В. В. Информационная безопасность: учеб. пособие / В. В. Гафнер. — Ростов на Дону: Феникс, 2010. — С. 147. ↑