Интернет-журнал «Науковедение» ISSN 2223-5167 https://naukovedenie.ru/

Том 9, №5 (2017) https://naukovedenie.ru/vol9-5.php

URL статьи: https://naukovedenie.ru/PDF/72TVN517.pdf

Статья опубликована 30.10.2017

Ссылка для цитирования этой статьи:
Рудниченко А.К., Колесникова Д.С., Верещагина Е.А. Защита от вредоносного программного обеспечения, представляющего собой комплекс легитимных программных продуктов // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 9, №5 (2017) https://naukovedenie.ru/PDF/72TVN517.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ.

УДК 004.056.53

Рудниченко Алексей Константинович
ФГАУО ВО «Дальневосточный федеральный университет», Россия, Владивосток[1]
Магистрант
E-mail: rudnichenko_ak@dvfu.ru
РИНЦ: http://elibrary.ru/author_profile.asp?id=936050

Колесникова Дарья Сергеевна
ФГАУО ВО «Дальневосточный федеральный университет», Россия, Владивосток
Магистрант
E-mail: kolesnikova_dse@dvfu.ru
РИНЦ: http://elibrary.ru/author_profile.asp?id=936048

Верещагина Елена Александровна
ФГАУО ВО «Дальневосточный федеральный университет», Россия, Владивосток
Доцент кафедры «Информационной безопасности»
Кандидат технических наук
E-mail: everesh@mail.ru
РИНЦ: http://elibrary.ru/author_profile.asp?id=287436

Защита от вредоносного программного обеспечения, представляющего собой комплекс легитимных программных продуктов

Аннотация. Информация, обрабатываемая на предприятиях, весьма разнообразна и ее неправомерное использование может нанести серьезный ущерб, как экономический, так и ущерб потери репутации среди клиентов и конкурентов. С учетом того, что она содержится на компьютерах и подвергается автоматизированной обработке – риск потерь увеличивается. Информация, которая содержит сведения о том, каким образом может работать база данных или просто ее содержимое, является крайне ценной для организации и ее раскрытие будет на руку конкурентам.

В данной статье представлен пример разработки вредоносного программного обеспечения для несанкционированного доступа с помощью легитимных средств. Выработаны рекомендации по защите информационной системы предприятия от представленного вредоносного программного обеспечения, так как современное антивирусное программное

[1] 690922, Россия, Приморский край, г. Владивосток, Аякс-10, корпус D

обеспечение в целом не может гарантировать защищенность операционной системы Windows от вредоносных программ.

Целью исследований являлась выработка доступных и эффективных мер по защите от легитимного программного обеспечения как метода получения несанкционированного доступа к информации. Также было необходимо проанализировать процесс его разработки. В результате выполнения предложенных мер внедрение вредоносного программного обеспечения в информационную систему извне сводится к минимуму.

Ключевые слова: легитимное программное обеспечение; вредоносное программное обеспечение; вирус; защита от вирусов; джойнер; самораспаковывающиеся архив; антивирусная защита; средства защиты информации от несанкционированного доступа; сегментирование информационной системы; персональный межсетевой экран

Введение

В настоящее время уже в любой области деятельности так или иначе задействованы компьютеры и иные информационные технологии. Темпы информатизации общества превышают темпы развития других отраслей. В связи с этим, находятся люди, которые используют инновации не для благих целей. Безопасность – одна из самых серьезных задач, с которой сталкиваются предприятия, специалисты по защите информации постоянно принимают необходимые меры защиты для того, чтобы обезопасить информацию. Так как уже сейчас информация имеет намного большую ценность, чем ранее, то с каждым днем появляются новые способы кражи, изменения, уничтожения информации или прекращения работы информационной системы.

Один из видов проникновения в информационную систему, где обрабатывается конфиденциальная информация – программный. Злоумышленник внедряет вредоносную программу на предприятие, после чего он имеет полный или частичный (зависит от ранее поставленных целей) доступ к важной информации в информационной системе.

Средства антивирусной защиты, которые необходимо устанавливать на предприятии для того, чтобы препятствовать появлению вредоносных программ, не всегда помогает. Существует ряд вполне законных (легитимных) программ, имеющих в себе сомнительный функционал, который можно применить для получения несанкционированного доступа. Данное ПО (программное обеспечение), несмотря на его возможности, либо состоит в «белых» списках антивирусных программ, либо изначально не вызывает подозрения у них. Именно из такого программного обеспечения злоумышленник может собрать программу, которая по итогу будет иметь свойства вредоносной.

В связи с этим, вопрос о защите информационной системы от такого рода вредоносного программного обеспечения до сих пор открыт, даже при существовании хорошей, на первый взгляд, антивирусной защиты.

1. Использование вредоносного легитимного программного обеспечения для несанкционированного доступа с точки зрения злоумышленника

Легитимное программное обеспечение (легитимное ПО) – программное обеспечение, которое разрабатывается и распространяется легально и может использоваться в повседневной работе для выполнения определенных задач. Примеры: программы с функционалом родительского контроля, удаленного администрирования, средства защиты информации для

предотвращения утечек, Microsoft Word – OLE-интерфейс (object linking and embedding) [9], Punto Switcher.

Легитимное программное обеспечение, которое используется для НСД (несанкционированного доступа) в информационную систему, называется *вредоносным легитимным программным обеспечением*.

Для разработки вредоносной программы из легитимных средств необходимо определить цели, преследуемые злоумышленником, и задачи, как путь достижения поставленных целей.

Цели и задачи будущей вредоносной программы

Целью разработки вредоносной программы является слежение за пользователем (жертвой) и получение впоследствии информации, с помощью которой возможно получить доступ к необходимым данным. В течении долгосрочной слежки за пользователем можно узнать многое: его персональные данные, коды доступа на различных сайтах, образ жизни в целом (в частности, интервалы времени, когда жертва не бывает дома). К определенным данным могут относиться, например, аккаунты в социальных сетях, которые в будущем могут быть исследованы для получения более точной информации о жертве или проданы третьим лицам с целью заработка.

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных). Что может относиться к персональным данным:

- Ф. И. О. и адрес проживания;
- сведения о заработной плате, паспортные данные, номер ИНН и СНИЛС;
- информация о расовой и национальной принадлежности, частной жизни, состоянии здоровья и т. д.

Персональные данные могут быть представлены и другими реквизитами. Данной информации абсолютно достаточно для того, чтобы составить полную картину о жизни человека для последующих манипуляций.

Задачи вредоносного программного обеспечения строятся из целей [2], то есть потребностей, которым должна удовлетворять программа, а именно:

- доступ к компьютеру жертвы должен осуществляться в любое время по желанию злоумышленника;
- возможность как просмотра удаленного компьютера, так и управления им;
- сохранение всех текстов, набираемых на клавиатуре (для последующего изымания паролей из них);
- возможность записи экрана или постоянного снимка экрана с интервалами (для случаев, когда у злоумышленника нет возможности контролировать жертву, а потребность в этом имеется);
- все действия вредоносной программы должны быть невидимы для обычного пользователя.

План разработки вредоносной программы на примере

Для того, чтобы выработать меры по защите от вредоносного легитимного программного обеспечения, необходимо проанализировать процесс разработки соответствующей вредоносной программы, а также действия злоумышленника на конкретном примере.

Исходя из целей и задач, которые были предъявлены к вредоносной программе разрабатывается соответствующий план. План разработки содержит все этапы создания итогового вредоносного комплекса, который впоследствии готов к внедрению (рисунок 1).

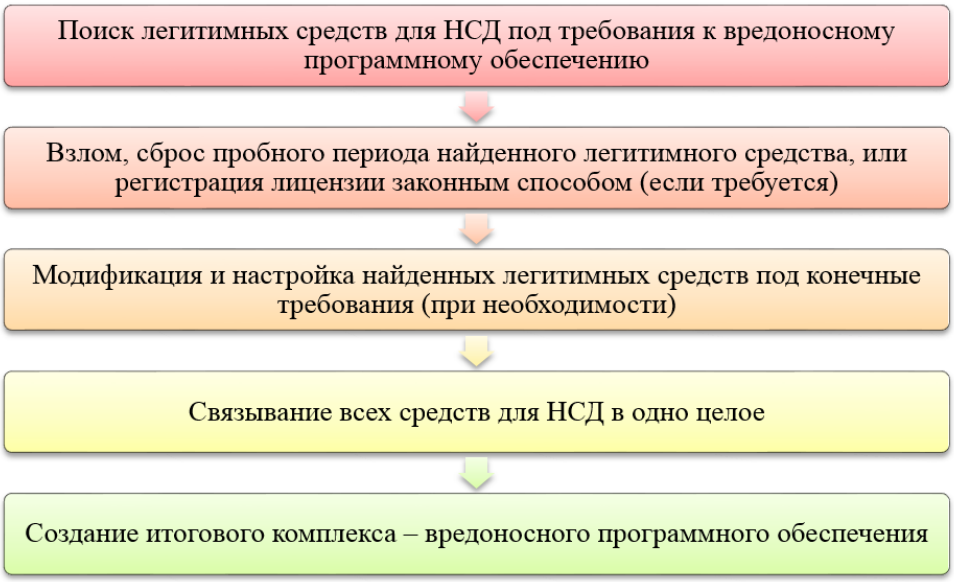


Рисунок 1. *Этапы создания вредоносного комплекса (разработано авторами)*

Поиск легитимных средств для НСД под требования к вредоносному программному обеспечению. Данный этап в себя включает изучение имеющихся программ на рынке программного обеспечения, которые полностью или частично удовлетворяют задачам будущего вредоносного ПО.

Если найденные программы имеют пробный период или требуют покупки, то злоумышленник прибегает к взлому, либо сбросу пробной периода. В крайнем случае, когда это сделать не удается, то происходит регистрация лицензии законным способом.

Зачастую бывает, что найденные средства не полностью удовлетворяют задачам вредоносного ПО и желанию злоумышленника. В таких случаях имеющееся программное обеспечение модифицируют и настраивают, если есть такая возможность.

После того, как все части будущего вредоносного ПО подготовлены, требуется соединить их в один файл. Шанс запуска одного файла больше, чем шанс запуска нескольких файлов.

Создание итогового комплекса – вредоносного программного обеспечения – осуществляется чаще всего вместе с предыдущим этапом. На данном этапе прописываются правила запуска будущего файла, значок итогового файла, а также действия после запуска.

Поиск легитимных средств для НСД

При поиске легитимных средств для НСД злоумышленник, как правило, учитывает факт срабатывания антивирусов на них. Даже на стандартное программное обеспечение у

антивируса может быть ложное срабатывание. Поэтому уточняется, как те или иные антивирусные средства «реагируют» на файл, который в будущем злоумышленник будет использовать.

VirusTotal (virustotal.com) – бесплатная служба, осуществляющая анализ подозрительных файлов и ссылок (URL) на предмет выявления вирусов, червей, троянов и всевозможных вредоносных программ.

Результаты проверок файлов сервисом не зависят от какого-то одного производителя антивирусов. В VirusTotal используется несколько десятков антивирусных систем, что может позволить делать более надежные выводы об опасности файла, по сравнению с каким-то одним продуктом, выявлять ложные срабатывания какого-то одного антивируса, либо, наоборот, несрабатывания на свежую угрозу, возможно, уже внесенную другими производителями в свои базы.

Исходя из задач, злоумышленнику необходимо найти легитимный продукт для удаленного управления персональным компьютером. Также, он должен состоять доверительных списках, чтобы в дальнейшем со стороны антивирусных программ не возникало проблем. Стоит отметить, что программа для удаленного доступа по своей сути не является вредоносной, поэтому злоумышленники берут практически любую подобную программу, которая удовлетворяет условиям.

В качестве программного обеспечения, которое осуществляет удаленное управление компьютера, будет использоваться RMS (Remote Manipulator System) от компании «TektonIT».

Remote Manipulator System – это продукт для управления удаленным рабочим столом, предоставляющий простой и безопасный доступ к ПК (персональному компьютеру) в любой точке земного шара.

RMS состоит из двух основных модулей:

- модуль управления «Клиент»;
- удаленный модуль «Хост».

Модуль «Клиент» предназначен для подсоединения к удаленным рабочим станциям, на которых установлен «Хост». Клиент предоставляет удобный интерфейс для управления списком соединений, построения карты сети, поиска удаленных рабочих станций и управления ими в различных режимах.

«Хост» должен быть установлен на каждой удаленной рабочей станции, к которой нужно получить доступ. Этот модуль позволяет удаленно управлять компьютером, на котором он установлен. Возможна удаленная установка клиентских модулей, также имеется конфигуратор дистрибутива хоста.

Каждое легитимное средство необходимо проверить в системе VirusTotal, чтобы удостовериться, что антивирусные программы не имеют ложного срабатывания на подобранное программное обеспечение. Отчет сервиса VirusTotal последней версии RMS (модуль «Клиент») представлены на рисунке 2.

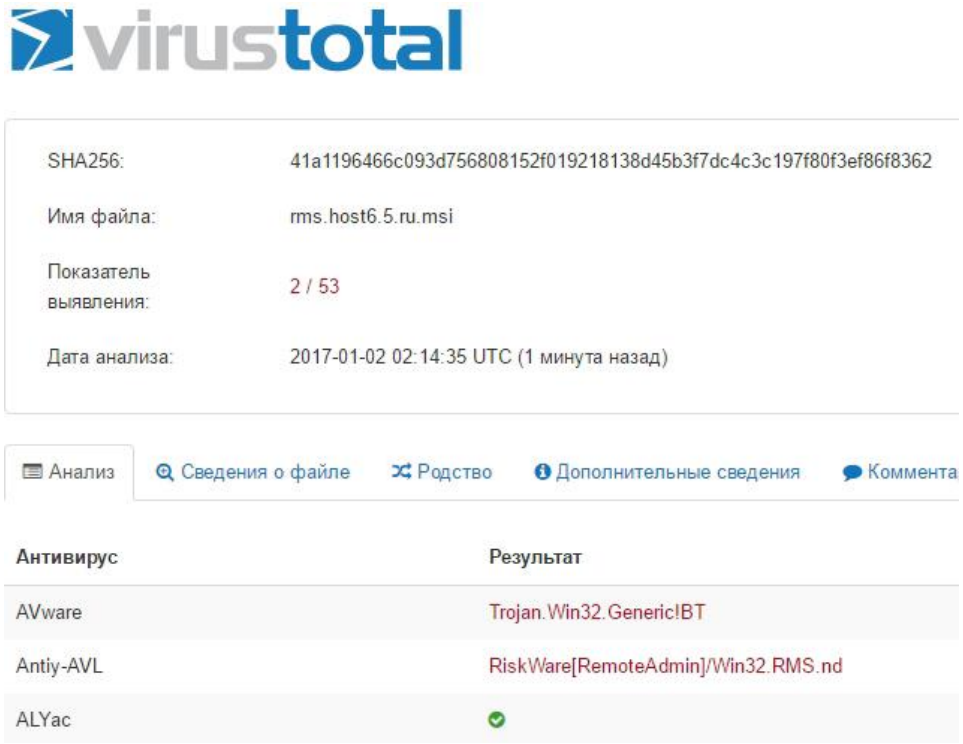
SHA256:	92528e91923c5e3bf066d96916545fdec44c536919da282eb41b4c5ebb23c1fe
Имя файла:	rms.viewer6.5.ru.msi
Показатель выявления:	4 / 54
Дата анализа:	2017-01-02 02:14:26 UTC (0 минут назад)

Анализ | Сведения о файле | Родство | Дополнительные сведения | Комментар

Антивирус	Результат
AVware	Trojan.Win32.Generic!BT
AegisLab	Remoteadmin.W32.Agent!c
Antiy-AVL	RiskWare[RemoteAdmin]/Win32.Agent
Kaspersky	not-a-virus:HEUR:RemoteAdmin.Win32.Agent.gen
ALYac	

Рисунок 2. *Отчет об анализе модуля RMS «Клиент» (разработано авторами)*

Отчет сервиса VirusTotal последней версии RMS (модуль «Хост») представлены на рисунке 3. Результаты именно этого модуля важнее всего, они повлияют на дальнейшее внедрение. Необходимо, чтобы как можно меньше антивирусных программ проявили бдительность по отношению к исследуемому файлу.



SHA256:	41a1196466c093d756808152f019218138d45b3f7dc4c3c197f80f3ef86f8362
Имя файла:	rms.host6.5.ru.msi
Показатель выявления:	2 / 53
Дата анализа:	2017-01-02 02:14:35 UTC (1 минута назад)

Анализ | Сведения о файле | Родство | Дополнительные сведения | Коммента

Антивирус	Результат
AVware	Trojan.Win32.Generic!BT
Antiy-AVL	RiskWare[RemoteAdmin]/Win32.RMS.nd
ALYac	

Рисунок 3. *Отчет об анализе модуля RMS «Хост» (разработано авторами)*

Из приведенных рисунков видно, что программное обеспечение удовлетворяет поставленным задачам, так как из 53 антивирусных программ всего 2 показали, что программное обеспечение является подозрительным. У модуля «Клиент» есть срабатывание от антивируса «Kaspersky». Так как внедряться жертве будет исключительно модуль «Хост», результаты сканирования модуля «Клиент» не играют особой роли, так как он будет установлен на компьютере злоумышленника.

Удовлетворяя указанные ранее задачи итогового вредоносного программного обеспечения, необходимо найти программу для записи текста с клавиатуры. В качестве ПО, выполняющего данную функцию, выступает Punto Switcher от компании «Яндекс».

Punto Switcher – программа для автоматического переключения между различными раскладками клавиатуры и бесплатна для некоммерческого использования. Основное назначение программы – увеличение продуктивности и удобства при работе с компьютером. Работает в фоновом режиме.

Среди стандартных возможностей программы (смена раскладки, замена сочетания клавиш для переключения языка, исправление опечаток, преобразования чисел в текст и пр.) существует функция ведения дневника – сохранение всех текстов, набираемых на клавиатуре. Данная возможность была модернизирована в новых версиях Punto Switcher (в версии 4.3.1 функция позволяет записывать текст от 2 слов и более) по причине нелегального его использования. В связи с этим злоумышленники используют старые версии этого ПО (например, 3.2.9.240), где такие ограничения отсутствуют.

Отчет проверки на сервисе VirusTotal представлен на рисунке 4.

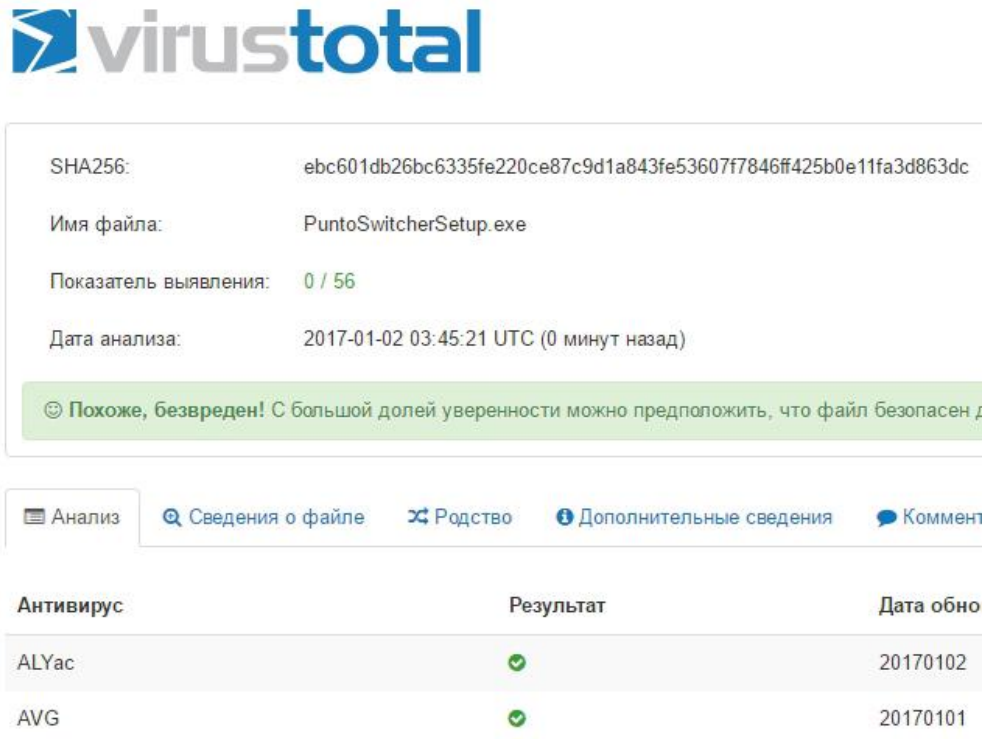


Рисунок 4. *Отчет об анализе дистрибутива Punto Switcher (разработано авторами)*

Из приведенного рисунка видно, что программное обеспечение удовлетворяет поставленным задачам, так как из 56 антивирусных программ ни одна не показала, что программное обеспечение является подозрительным.

Создание итогового комплекса – вредоносного программного обеспечения

Для внедрения вредоносной программы на компьютер жертвы она должна быть сосредоточена в одном исполняемом файле. Таким образом, повышается шанс запуска программного обеспечения из неизвестного источника.

Для того, чтобы удовлетворить данному требованию, злоумышленники используют джойнеры. *Джойнер (joiner)* – программа, которая позволяет «склеивать» вредоносное программное обеспечение с любым файлом в конечный формат «.exe» [10]. Таким образом, несколько легитимных средств возможно соединить в одно целое.

Самым простым джойнером является любой архиватор (например, WinRAR). Архиваторы имеют возможность создания самораспаковывающихся архивов SFX (self-extracting archive), которые имеют расширение «.exe».

Итоговый SFX архив представлен на рисунке 5, где:

- «css.exe» – программа Punto Switcher;
- «go.exe» – программа Remote Manipulator System;
- «prog.exe» – программа, под которую маскируется вредоносное программное обеспечение;
- «start.exe» – файл запуска цепочки указанных программ.

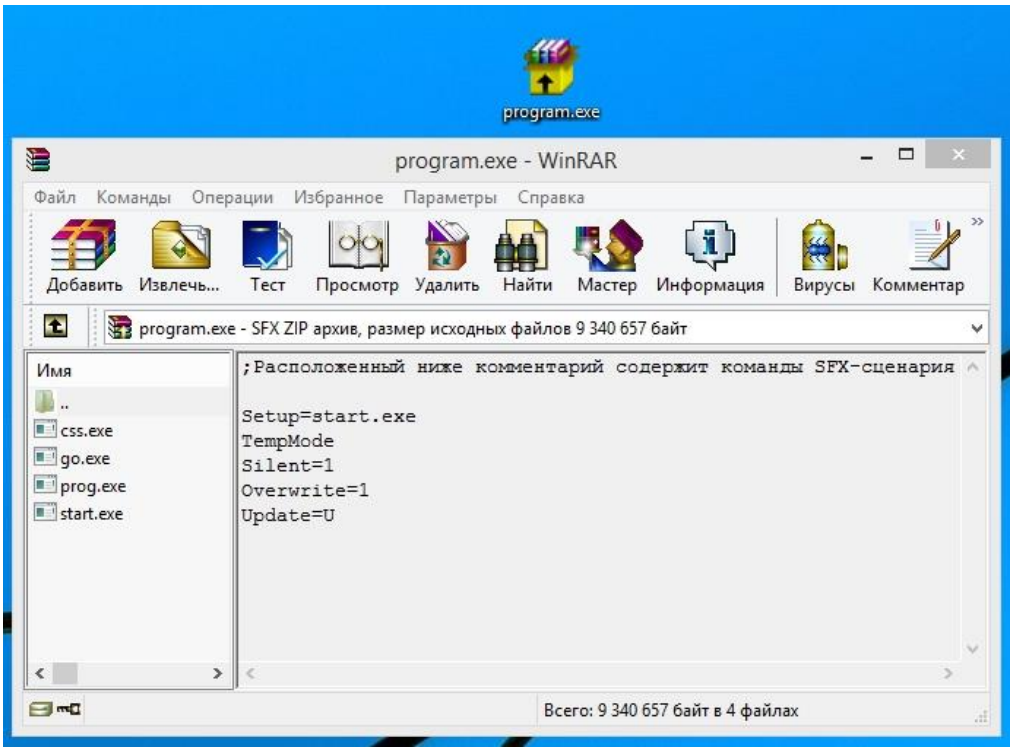


Рисунок 5. *Демонстрация итогового SFX архива (разработано авторами)*

2. Методика защиты от вредоносного легитимного ПО для НСД на предприятии

На основе проведенных исследований представлена методика защиты информации от вредоносного легитимного ПО для НСД на предприятии. Она включает в себя комплекс мер двух типов [3]:

- организационные;

- технические.

Как правило, организационные меры представляют собой основную деятельность по обеспечению физической защиты (например, доступ к помещениям), разработке организационно-распорядительной документации и проведению мероприятий по обучению сотрудников.

Технические меры включают в себя предотвращение утечки и определение возможности получения несанкционированного доступа с помощью программных и аппаратных средств.

Общий список мер, предлагаемых в методике представлен на рисунке 6.

Рисунок 6. *Классификация мер по защите от вредоносного легитимного ПО (разработано авторами)*

Повышение осведомленности персонала в области информационной безопасности

Под организационными мерами понимается повышение осведомленности персонала организации в области информационной безопасности [6]. Таким образом, удастся снизить шанс возникновения преднамеренных или непреднамеренных действий работника, результатом которых может быть отказ в обслуживании части информационной системы, утечка важной конфиденциальной информации или нарушение доступа к ресурсам.

Повышение осведомленности персонала в области информационной безопасности требует разработки следующей документации:

- программа повышения осведомленности и плана ее реализации;
- политика обучения и повышения осведомленности персонала в области информационной безопасности;
- методика оценки уровня осведомленности персонала в области информационной безопасности.

Обучение и повышение осведомленности персонала в области информационной безопасности можно проводить в различных формах:

- очное обучение;
- дистанционное обучение (электронные курсы, вебинары);
- самостоятельное изучение выданных курсов.

Стоит отметить, что самостоятельное обучение с помощью выданных на руки сотрудникам материалов является самым неэффективным, так как не дает должного результата. Для регулярного обучения и повышения осведомленности работников очное обучение также невыгодно, так как отрыв сотрудников от основной деятельности негативно влияет на рабочий процесс предприятия. Поэтому важно отнестись к составлению плана по обучению с должным вниманием. Эффективной является дистанционная форма обучения по электронным курсам или онлайн-конференциям с возможностью его промежуточного и итогового контроля и оценки.

Наиболее выгодным и эффективным является комплексный подход к обучению и повышению осведомленности персонала в области информационной безопасности. В таком случае возможно параллельно проводить занятия сразу на нескольких уровнях комбинируя различные формы:

- очное обучение посредством инструктажа по обеспечению информационной безопасности;
- информационные рассылки персоналу с освещением актуальных вопросов информационной безопасности, важных для сотрудников изменений в законодательстве;
- консультации по вопросам информационной безопасности в форме свободной беседы на совещаниях.

Оценка уровня осведомленности персонала необходима не только для анализа полученных сотрудниками знаний и умений, но и для оформления отчетности об усвоении сотрудниками материала. Также составляется лист ознакомления с материалами, выданными при инструктаже.

В предлагаемой методике технические меры защиты от вредоносного легитимного программного обеспечения представляют собой следующие программные и технические решения:

- антивирусная защита;
- средства защиты информации от несанкционированного доступа (СЗИ от НСД);
- сегментирование информационной системы;
- персональный межсетевой экран.

Не все представленные меры способны полностью решить проблемы защиты от вредоносного легитимного ПО. Это возможно только при совокупном их использовании.

Антивирусная защита

Программа антивирусной защиты – программное обеспечение, нацеленное на защиту от вредоносных программ.

Существует две основных группы методов обнаружения вредоносного ПО:

- сигнатурные методы – методы обнаружения, основанные на сравнении файла с известными образцами, находящимися в базе сигнатур (базе данных известных вредоносных программ);
- эвристические методы – методы обнаружения, основанные на предположении, что сканируемый файл может быть заражен.

Рассматривая проблему вредоносного легитимного программного обеспечения, можно сделать вывод, что антивирусная защита, на первый взгляд, не способна обнаружить ПО такого типа. Но существует ряд случаев, когда антивирусы могут составить конкуренцию.

Поведение вредоносного легитимного программного обеспечения является вполне законным, поэтому эвристические методы с большой долей вероятности не дадут результатов. Методы эвристического сканирования не обеспечивают какой-либо гарантированной защиты от новых, отсутствующих в базе сигнатур вредоносных программ. А чрезмерная чувствительность и подозрительность эвристического анализатора может вызвать большое количество ложных срабатываний.

Также, на сегодняшний день существует множество простых способов обмана эвристического анализатора. Как правило, прежде чем распространять вредоносную программу, ее разработчики исследуют существующие распространенные антивирусные продукты, избегая ее детектирование на вредоносном файле при эвристическом сканировании.

В случае, если вредоносная программа распространяется уже довольно долгое время, не меняя содержимого файла, то сигнатурные методы обнаружения вредоносного ПО в этом случае помогут, так как многие антивирусные компании по запросам физических лиц и корпоративных пользователей вносят информацию о программе в свои базы сигнатур, которые работают по принципу «черного» списка. Одним из важных свойств сигнатурного анализа является точное определение типа вируса.

Таким образом, программы антивирусной защиты частично могут решить проблему вредоносного легитимного программного обеспечения. Установка антивируса – одна из первых и самых важных мер по борьбе с вредоносными программами [11]. В этом случае тоже нельзя исключать его полезность, но в случае с легитимным ПО антивирус начнет его детектировать не сразу, что является серьезной угрозой для информационной системы.

Средства защиты информации от несанкционированного доступа

СЗИ от НСД (средства защиты информации от несанкционированного доступа – программные, технические или программно-технические средства, предназначенные для предотвращения или существенного затруднения несанкционированного доступа к информации.

Наиболее распространенные программные СЗИ от НСД и их последние версии [8]:

- Secret Net 7.6;
- Dallas Lock 8.0-К и Dallas Lock 8.0-С.

Основные защитные функции, реализуемые различными программными средствами защиты информации от НСД:

- контроль входа пользователей в систему;
- разграничение доступа пользователей к устройствам компьютера;

- разграничение доступа пользователей к конфиденциальным данным;
- создание для пользователей замкнутой программной среды;
- контроль потоков конфиденциальной информации;
- контроль вывода конфиденциальных данных на печать;
- контроль целостности защищаемых ресурсов;
- контроль аппаратной конфигурации компьютера;
- безвозвратное уничтожение содержимого файлов при их удалении;
- регистрация событий безопасности;
- сбор и хранение журналов.

СЗИ от НСД позволяет запретить запуск программ, которые определил администратор (внес их в «черный» список). Данный функционал позволяет защитить информационную систему от таких угроз, как несанкционированное повышенных прав с помощью прикладного или системного программного обеспечения или запуск нежелательных программ, которые можно найти в публичном доступе.

Средства защиты информации от несанкционированного доступа позволяют создать ЗПС (замкнутую программную среду) – режим, в котором пользователь может запускать только те программы, которые определены администратором (внесены в «белый» список СЗИ). Данный функционал позволяет защититься от практически любого вредоносного программного обеспечения, легитимного в частности.

Зачастую это возможно исключительно на государственных предприятиях, где рабочий процесс строго регламентирован. В коммерческих организациях иначе, поэтому данная мера защиты от вредоносного легитимного ПО может нарушить рабочий процесс или внести явные неудобства в него. Исходя из этого, необходимо внимательно составить «белый» список программ для того, чтобы в дальнейшем сотрудники не ощущали дискомфорт в работе.

Для корректной настройки замкнутой программной среды необходимо выполнить несколько шагов. Рассмотрим их на примере СЗИ от НСД Dallas Lock:

1) войти в систему от лица пользователя, права которого в будущем будут ограничены;
2) установить на компьютер сотрудника пакет прикладных программ, необходимый исключительно для рабочего процесса и выполнения должностных обязанностей;
3) сменить пользователя и войти под учетной записью администратора безопасности. Запустить оболочку администратора. Создать специальную группу, например, «ZPS-gr», и включить пользователя с ограниченными правами (например, «zps») в группу «ZPS-gr»;
4) для группы «ZPS-gr» в глобальных настройках запретить запуск всех программ (вкладка «Контроль ресурсов» => «Глобальные» => «Параметры ФС по умолчанию»);
5) в дескрипторе «Параметры ФС по умолчанию» включить полный аудит отказов;
6) настроить неактивный режим работы Dallas Lock (Основное меню => «Настройка режимов работы» => «Настроить неактивный режим»). В окне настройки необходимо включить «мягкий режим» контроля доступа. Дополнительно желательно очистить (архивировать) журнал ресурсов;

7) перезагрузить компьютер и осуществить вход в операционную систему под учетной записью пользователя «zps». Далее запустить все то программное обеспечение, с которым пользователь будет иметь право работать;

8) сменить пользователя и войти под учетной записью администратора безопасности. Запустить оболочку администратора. Открыть журнал ресурсов;

9) используя фильтр, найти все ресурсы с результатом «ошибка». Каждому из них в свойстве «Права для файлов» назначить дискреционные права для группы «ZPS-gr» – «только чтение»;

10) отключить «мягкий режим» и по необходимости отключить ранее выставленный «аудит доступа».

Следует помнить, что не для всех приложений является достаточным просто их запуск. Некоторые сложные приложения при своем запуске загружают не все исполняемые модули, а только необходимые, остальные модули они подгружают динамически, в процессе работы. Поэтому после запуска приложения лучше выполнить все основные действия приложения для будущей работы.

Необходимо отметить, что вероятна ситуация, когда не все нужные для работы пользователя исполняемые файлы занеслись в список. Так как некоторые приложения вызывают какие-либо другие исполняемые файлы только при активизации определенных функций. Если после включения замкнутой программной среды у пользователя какое-либо приложение стало работать неправильно – это можно сразу же увидеть в журнале доступа к ресурсам. В таком случае, для дополнительных исполняемых файлов необходимо добавить аналогичное право на исполнение («только чтение»).

В результате создания замкнутой программной среды полностью исключается случайное внедрение вредоносных программ от лица сотрудников. Таким образом, пользователь может запускать только те программы, которые разрешены администратором безопасности.

Сегментирование информационной системы

Данный метод нейтрализации угрозы вредоносного легитимного программного обеспечения подразумевает под собой разделение общей сети предприятия на два сегмента [12]:

- сегмент, имеющий доступ к внутренней сети организации и не имеющий доступа в сеть Интернет;
- сегмент, имеющий доступ к сети Интернет и не имеющий доступа к внутренней сети организации.

Благодаря сегментированию информационной системы можно получить полностью защищенную внутреннюю сеть предприятия и при необходимости доступ в сеть «Интернет» для решения задач во время рабочего процесса.

Сегментирование возможно организовать несколькими способами:

- установка двух компьютеров пользователям, которым необходимо работать как во внутренней сети предприятия, так и в интернете;
- создание «абонентского пункта» – отдельного помещения с компьютерами (или терминальными машинами) для взаимодействия с сетью Интернет;

- установка сервера на базе Windows с доступом в интернет и предоставление доступа по Remote Desktop Protocol (RDP) с компьютеров сотрудников.

Вне зависимости от способов сегментирования рекомендуется использовать технологии аппаратного межсетевого экранирования, что даст возможность эффективно разграничить части сети. Каждый способ данной методики имеет свои плюсы и минусы. Необходимо рассмотреть их особенности подробнее.

При *установке двух компьютеров* сотрудникам, которым необходимо работать как во внутренней сети предприятия, так и в интернете, есть ряд особенностей:

- два компьютера на одном рабочем столе существенно занимают место;
- нет необходимости отлучаться от места работы для доступа в сеть Интернет;
- с экономической точки зрения данное решение является дорогостоящим для реализации.

В данном случае схема сети при сегментировании представлена рисунке 7. На рисунке АРМ (автоматизированное рабочее место) – это программно-технический комплекс для автоматизации деятельности (например, обработки персональных данных).

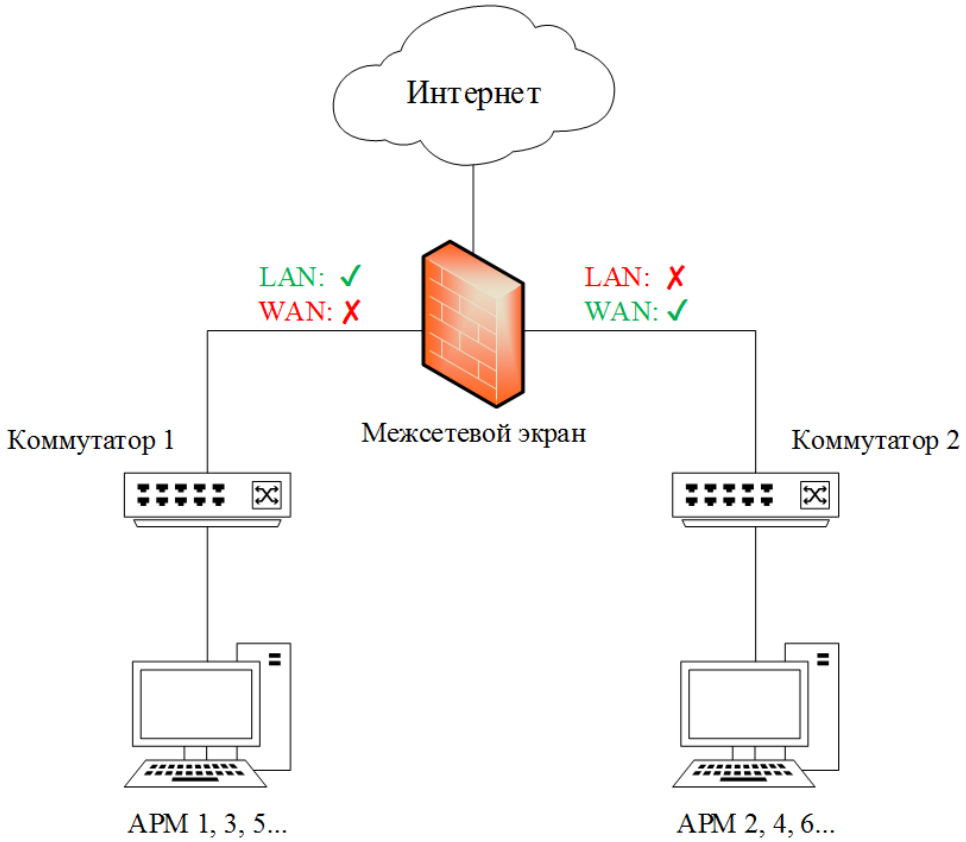


Рисунок 7. *Схема сети при сегментировании (установка двух компьютеров) (разработано авторами)*

На данной схеме WAN – это доступ в глобальную сеть «Интернет», а LAN – доступ к локальной сети предприятия (другим рабочим станциям, которые находятся в организации). Коммутаторы предназначены исключительно для соединения нескольких узлов (рабочих станций) компьютерной сети в пределах одного сегмента сети. Межсетевое экранирование позволяет разделить общую сеть на два сегмента при помощи программных настроек в нем.

Также межсетевой экран на данной схеме выполняет основные функции маршрутизатора, поэтому он тут отсутствует.

В рамках данного способа на оба компьютера, если необходимо, устанавливается СЗИ от НСД с целью запретить подключение съемных носителей, так как с их помощью можно перенести данные с одного компьютера на другой и произвести заражение компьютера, обрабатывающего конфиденциальную информацию. Запрет съемных носителей возможно сделать и штатными средствами Windows, но такое решение не дает гарантий, а также нет возможности проконтролировать данный запрет (просмотреть журнал безопасности).

При *создании «абонентского пункта»* – отдельного помещения с компьютерами (или терминальными машинами) для взаимодействия с сетью Интернет – характерны следующие особенности:

- необходимость иметь отдельное помещение;
- сотрудники должны отлучиться от своего места работы для доступа в сеть «Интернет»;
- с экономической точки зрения данное решение дешевле, чем сегментирование сети при помощи установки двух компьютеров сотрудникам.

Схема сети при данном способе сегментирования представлена на рисунке 8.

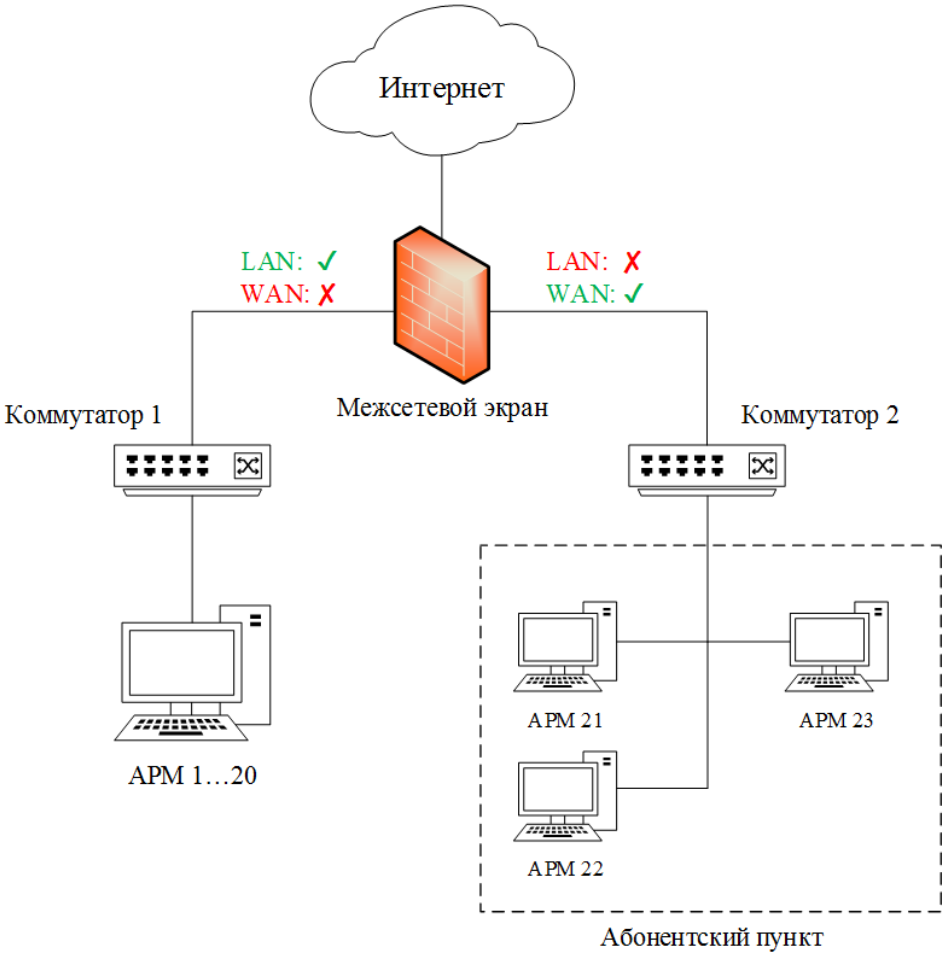


Рисунок 8. *Схема сети при сегментировании (создание «абонентского пункта») (разработано авторами)*

В рамках данного способа на все компьютеры ставится СЗИ от НСД с целью запретить подключение съемных носителей, как и в предыдущем методе. Аналогичным способом может являться установка компьютеров на базе операционной системы Linux, чтобы в дальнейшем использовать компьютер в виде терминала, где будут доступны пользователям исключительно необходимые программы (например, браузер). Так значительно дешевле.

При *установке сервера на базе Windows с доступом в интернет* и предоставление доступа по Remote Desktop Protocol (RDP) с компьютеров сотрудников есть свои особенности, характеризующие целесообразность данного метода:

- нет необходимости иметь отдельное помещение или занимать рабочее место сотрудника;
- сотрудникам нет необходимости покидать свое рабочее место;
- с экономической точки зрения данное решение может оказаться как и самым дешевым из всех представленных, так и дороже, чем создание «абонентского пункта».

RDP (Remote Desktop Protocol) – протокол, который используется для удаленного подключения пользователя к серверу.

Схема сети данного способа сегментирования изображена на рисунке 9.

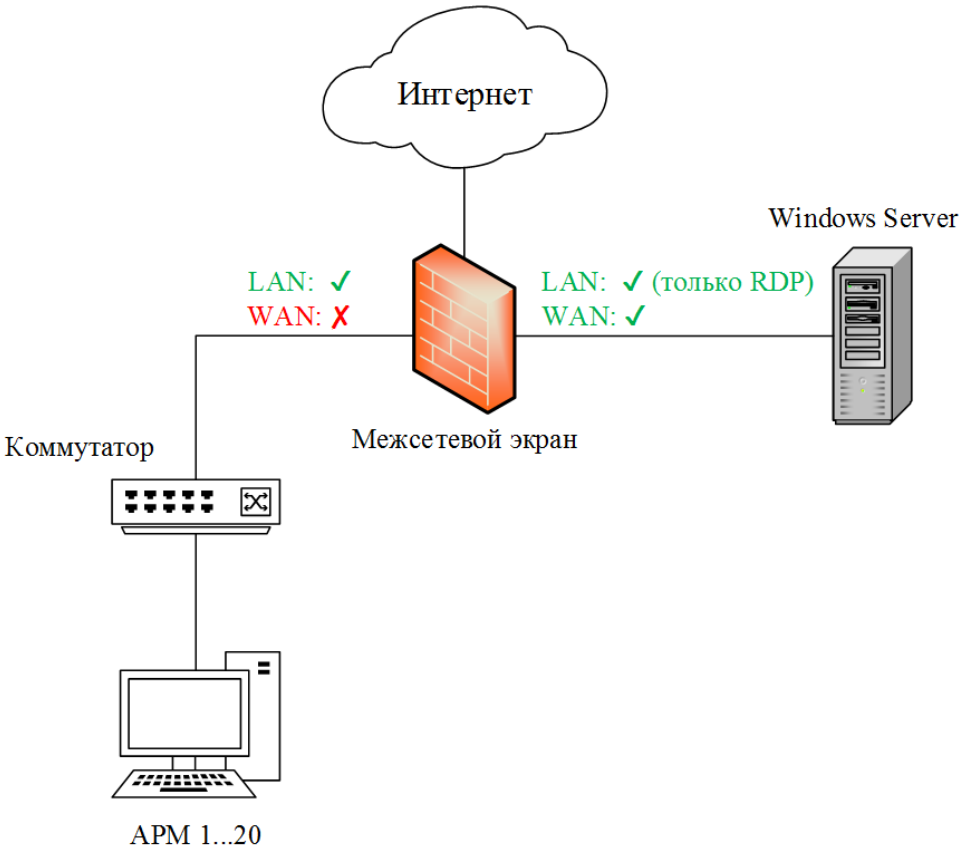


Рисунок 9. *Схема сети при сегментировании (установка сервера на базе Windows) (разработано авторами)*

В рамках данного способа нет необходимости ставить на сервер СЗИ от НСД. По желанию устанавливается на сервера для контроля входов и мониторинга доступа к ресурсам. Вариация данного метода позволяет сделать его одним из самых дешевых в реализации.

Также необходимо в настройках RDP соединения запретить использование общего буфера обмена, чтобы исключить копирование файла с сервера на компьютер сотрудника, который обрабатывает конфиденциальную информацию.

Таким образом, наиболее рациональным способом сегментирования информационной системы является установка сервера на базе Windows с доступом в интернет и предоставление доступа к серверу по RDP с компьютеров сотрудников.

Данный метод является одновременно одним из дешевых и наименее трудозатратным как для системного администратора, осуществляющего проектирование системы защиты информации, так и для сотрудников предприятия за счет экономии времени на перемещение до «абонентского пункта».

Персональный межсетевой экран

Персональный межсетевой экран – программное средство защиты информации, установленное на компьютере пользователя и предназначенное для фильтрации проходящего сетевого трафика исключительно для данного компьютера.

На данный момент разработчики известных средств защиты информации от несанкционированного доступа включают функционал межсетевого экранирования. Так, межсетевой экран является дополнительным модулем СЗИ Dallas Lock 8.0-К и Dallas Lock 8.0-С, а также входит в состав Secret Net Studio.

Учитывая, что для нейтрализации других угроз на предприятии зачастую необходима установка СЗИ от НСД, данный способ защиты от вредоносного легитимного программного обеспечения не является экономически затратным.

Метод защиты с помощью персонального межсетевого экрана сводится к работе межсетевого экранирования по принципу «белого» списка [4], то есть пропуская исключительно те соединения, которые разрешены. В рамках «белого» списка разрешаются основные ресурсы, связанные с рабочим процессом, и поисковые сервисы.

ЛИТЕРАТУРА

1. Александров А. А. Интегративная психотерапия. – СПб.: Питер, 2009. – 352 с.
2. Гинодман В. А., Обелец Н. В., Павлов А. А. От первых вирусов до целевых атак. – М.: МИФИ, 2014. – 96 с.
3. Грибунин В. Г., Чудовский В. В. Комплексная система защиты информации на предприятии. – Учебное пособие. – М.: Академия, 2009. – 416 с.
4. Духан Е. И., Синадский Н. И., Хорьков Д. А. Программно-аппаратные средства защиты компьютерной информации. – Екатеринбург: УрГУ, 2008. – 240 с.
5. Курилов Ф. М. Оптимизационный метод проведения сравнительного анализа средств защиты информации от несанкционированного доступа [Текст] // Технические науки: проблемы и перспективы: материалы III Междунар. науч. конф. (г. Санкт-Петербург, июль 2015 г.). – СПб.: Свое издательство, 2015. – С. 40-44.
6. Милославская Н. Г., Сенаторов М. Ю., Толстой А. И. Технические, организационные и кадровые аспекты управления информационной безопасностью. Учебное пособие для вузов. – 2-е изд., испр. – М.: Горячая линия-Телеком, 2014. – 214 с.
7. Платонов В. В. Программно-аппаратные средства защиты информации: учебник для студ. учреждений высш. проф. образования / В. В. Платонов. – М.: Издательский центр «Академия», 2013. – 336 с. – (Сер. Бакалавриат).
8. Рудниченко А. К. Опасность использования примитивных средств разграничения доступа Windows на предприятии. Средства защиты информации // Молодой ученый. – 2016. – №27. – С. 30-32.
9. Рудниченко А. К., Кошелев С. О. Использование OLE-объектов в документах Microsoft Word как средство распространения вредоносных программ. Методы защиты от них // Молодой ученый. – 2016. – №29. – С. 36-38.
10. Рудниченко А. К., Шаханова М. В. Актуальные способы внедрения компьютерных вирусов в информационные системы // Молодой ученый. – 2016. – №11. – С. 221-223.
11. Спицын В. Г. Информационная безопасность вычислительной техники. – Томск: Эль Контент, 2011. – 148 с.
12. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. – ИНФРА-М, 2011. – 416 с.

Rudnichenko Aleksey Konstantinovich
Far Eastern federal university, Russia, Vladivostok
E-mail: rudnichenko_ak@dvfu.ru

Kolesnikova Daria Sergeevna
Far Eastern federal university, Russia, Vladivostok
E-mail: kolesnikova_dse@dvfu.ru

Vereshchagina Elena Alexandrovna
Far Eastern federal university, Russia, Vladivostok
E-mail: everesh@mail.ru

Protection against malicious software, which is a complex of legitimate software products

Abstract. Information processed in organizations is very diverse and its illegitimate using can cause serious damage, both economic and damage to reputation loss among customers and competitors. Given that it is contained on computers and is subjected to automated processing – the risk of losses increases. Data that contains information about how the database can work or simply its content is extremely valuable to the organization and its disclosure will be beneficial to competitors.

This article presents an example of the development of malicious software for unauthorized access using legitimate means. The recommendations for protecting the information system of organization from the presented malicious software are developed, since modern anti-virus software as a whole can not guarantee the protection of the Windows operating system from malicious programs.

The aim of the research was to develop accessible and effective measures to protect against legitimate software as a method of obtaining unauthorized access to information. It was also necessary to analyze the process of its development. As a result of the proposed measures, the introduction of malicious software into the information system from the outside is minimized.

Keywords: legitimate software; malicious software; virus; virus protection; joiner; self-extracting archive; antivirus protection; means of protecting information from unauthorized access; segmentation of the information system; personal firewall