ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный университет путей сообщения Императора Николая II»
МГУПС (МИИТ)

Р Е Ф Е Р А Т

по дисциплине:
«Использование информационных технологий при решении исследовательских задач»

на тему: «Информационная безопасность и роль антивирусных программ»

Выполнил: аспирант 1 года обучения
кафедра «Гражданское право и гражданский процесс»
специальность 12.00.03
Галицкая Анастасия Александровна
Проверил: Беспалько Сергей Валерьевич

Москва 2017

Содержание

Введение……...3

1. Понятие информационного общества и взгляды различных ученых на понятие «информационная безопасность»……...4

2. Компьютерные вирусы и антивирусные программы……..12

Заключение……20

Список использованной литературы……..22

Введение

При работе с современным персональным компьютером пользователя (а особенно начинающего) может подстерегать множество неприятностей: потеря данных, зависание системы, выход из строя отдельных частей компьютера и другие. Одной из причин этих проблем наряду с ошибками в программном обеспечении и неумелыми действиями самого оператора ПЭВМ могут быть проникшие в систему компьютерные вирусы.

Вирусы – едва ли не главные враги компьютера. Эти программы подобно биологическим вирусам размножаются, записываясь в системные области диска или приписываясь к файлам, и производят различные нежелательные действия, которые, зачастую, имеют катастрофические последствия. Еще два года назад казалось, что со владычеством вирусов покончено – со смертью DOS и DOS-совместимых программ неминуемо должны были исчезнуть и паразитирующие на них вирусы. Сегодня самой распространенной группой вирусов стали макровирусы, заражающие не программы, а документы, созданные в Microsoft Word и Microsoft Excel.

Путей распространения вирусов существует множество. Вирус может попасть на компьютер пользователя вместе с дискетой, пиратским компакт-диском или с сообщением электронной почты. Чтобы не стать жертвой этой напасти, каждому пользователю следует хорошо знать принципы защиты от компьютерных вирусов. Ведь нет никакой надежды на то, что с приходом нового тысячелетия вирусы исчезнут. Так же как и нет надежды справиться с ними окончательно в какие-то обозримые сроки, так как таланту авторов антивирусных программ противостоит фантазия компьютерных графоманов.

С давних времён известно, что к любому яду рано или поздно можно найти противоядие. Таким противоядием в компьютерном мире стали программы, называемые антивирусными.

1. Понятие информационного общества и взгляды различных ученых на понятие «информационная безопасность»

Информационное общество, то есть общество, в котором информационные процессы осуществляются главным образом на основе использования информационно коммуникационных технологий, а информационные ресурсы доступны всем слоям населения, переживает один из самых активных этапов своего развития. А значит, актуально все, что связано с понятием безопасности в информационном обществе и в условиях формирования электронного правительстве.

Появление и научное закрепление дефиниции «информационная безопасность» непосредственно связано с осмыслением феномена информатизации и изучением содержания процесса формирования информационного общества. Данной проблеме посвящены работы зарубежных теоретиков Д. Белла, Э. Тоффлера, Т. Стоуньера, А. Турена, У. Дайзарда, М. Кастельса, К.Кояма, Е.Масуда[1].

Представляет научный интерес вопрос анализа, наряду с правовым аспектом, подходов философов, политологов, социологов, исследователей технических наук к определению понятия «информационная безопасность». Остановимся на некоторых из них.

Подход философов[2] основывается на выделении трех составляющих информационной безопасности:

1 Иноземцев В.Л. За пределами экономического общества. Постиндустриальные теории и постэкономические тенденции в современном мире. – М.: Наука, 1998; MasudaY. The information societyas Post – industrialSociety.Tokyo, 1981; NeisitF/ Magatrends: The New Derection Transforming Ourhites; КастельсМ. Информационнаяэпоха: экономика, обществоикультура. – М.: ГУВШЭ, 2000;BellD. TheSocialFrameworkoftheInformationSociety/ Oxf. – 1980; Коваленко В.И. Критика новейших буржуазных концепций государственно-монополистического капитализма.— М.: Прогресс, 1987;Новая технократическая волна на Западе. – М.: Прогресс, 1986; Тоффлер Э. Третья волна. – М..: Изд-во «Аст», 1999; Уэбстер Ф. Теории информационного общества. – М.: Аспект - пресс, 2004.

2 Атаманов Г.А. Информационная безопасность: сущность и содержание // Бизнес и безопасность в России. – 2007. – № 47. – С. 108.

1. удовлетворение информационных потребностей субъектов;

2. обеспечение безопасности информации;

3. обеспечение защиты субъектов.

Таким образом, в сущностном плане, информационная безопасность, согласно философского подхода, есть такое состояние объекта, при котором состояние информационной среды, в которой он находится, позволяет ему сохранять способность и возможность принимать и реализовывать решения сообразно своим целям, направленным на прогрессивное развитие. Это означает, что информационная безопасность может достигаться как в результате проведения мероприятий, направленных на поддержание информационной среды в безопасном для объекта защиты состоянии, защиту объекта от деструктивного воздействия,так и путем укрепления иммунитета и развития способности объекта уклоняться от деструктивного информационного воздействия (в т.ч. за счет предвидения их возможности).

Следовательно, задача обеспечения информационной безопасности государства состоит в том, чтобы создать такие условия функционирования информационной инфраструктуры(главным элементом которой является не компьютер, а человек), при которых отдельные граждане, коллективы, органы власти могли бы принимать управленческие решения и добиваться их реализации сообразно целям, направленным на прогрессивное развитие всего общества.

Политический анализ проблематики информационной безопасности - сегодня один из наиболее активных и указывает, прежде всего, на растущую необходимость объединения усилий частного сектора, политических институтов и правоохранительных структур, экспертно-аналитических сообществ в поиске способов противостояния многообразным угрозам в данной области.Политологами, в частности, высказывается мнение[3], согласно которому Россия всё ещё стоит на перепутье, и задача государственной

3 Ковалева Е. В. Обеспечение транспарентности органов местного самоуправления современной России в процессе информатизации политического управления. Автореф. дис. …канд. полит.наук: 23.00.02. Саратов, 2010

политики в области безопасности РФ состоит не только в том, чтобы защитить граждан и общество от этих угроз, но и реализовать эту политику в таких формах и методах которые, в свою очередь, не поставили бы под угрозу выбранный демократический вектор развития. Адекватная запросам времени политика в области безопасности должна опираться на приоритеты взаимовыгодного сотрудничества и развития гражданской инициативы, при руководящей и направляющей роли государства. Сегодня сложились все предпосылки к тому, чтобы стратегии социального партнерства и гражданского участия заняли достойное место в процессах выработки и реализации комплексной политики информационной безопасности.

Характерной чертой политической науки стало признание необходимости привлечения к обеспечению информационной безопасности не только институтов федеральной государственной власти, но и структур государственного управления субъектов Федерации[4].

Технический подход основывается, прежде всего, на проблеме разработки требований безопасности сайтов, включающих защиту серверов, лицензирование, сертификацию и аттестацию объектов информатизации, применение криптографических механизмов при передаче данных по каналам связи, использование методов идентификации и аутентификации пользователей на сайте[5]. Кроме того, подчеркивается, что системная работа в сфере правового обеспечения информационной безопасности требует научного обоснования дальнейшей разработки таких нормативных актов, в которых бы в полной мере были учтены международные принципы и нормы, направленные на укрепление международной информационной безопасности и вместе с тем максимально учитывались национальные интересы[6].

4 Кафтанчиков Д.П. Информационная безопасность Российской Федерации: современное состояние и приоритеты обеспечения. Автореф. дис. …канд. полит.наук: 23.00.02. Орел, 2009

5 Проценко Е.А. Модель и метод анализа эффективности систем защиты информации сайтов органов власти Российской Федерации. Автореф. дис. …канд. технич. наук: 05.13.19. Санкт-Петербург, 2008.

6 Крылов Г.О. Международный опыт правового регулирования информационной безопасности и его применение в Российской Федерации. Автореф. дис. …канд. юрид.

Социологи развивают понятие информационной безопасности в рамках одного из направлений социологии – социологии информатики, тем самым взаимосвязывая социологический и информационный подходы[7].

Среди юристов также пока не выработано единого подхода к определению понятия «информационной безопасности».

«Информационная безопасность является важнейшей составляющей национальной безопасности в целом…В структуре информационного права проблема обеспечения информационной безопасности является одним из институтов. Суть этого института информационного права состоит в осуществлении правовых, организационных, технических мер, обеспечивающих безопасное состояние всех составляющих информационно-коммуникационного комплекса государства, отдельных организаций и каждого человека»[8].

По мнению В.Н. Лопатина[9] объективно категория «информационная безопасность» возникла с появлением средств информационных коммуникаций между людьми, а также с осознанием человеком наличия у людей и их сообществ интересов, которым может быть нанесен ущерб путем воздействия на средства информационных коммуникаций, наличие и развитие которых обеспечивает информационный обмен между всеми элементами социума. Выделяя отдельно информационно-психологическую безопасность, В.Н. Лопатин трактует ее как «состояние защищенности жизненно важных интересов личности, общества и государства от воздействия вредной информации»[10].

наук: 05.13.19. Москва, 2007.

7Шемякин В.П. Информационная безопасность в современных российских условиях: Социолого-управленческие аспекты. Автореф. дис. …канд. социол. наук: 22.00.08. Москва, 2004

8Бачило И.Л. Информационное право: Учеб. Для вузов. М.: Высшее образование; Юрайт-Издат, 2009. С. 398.

9

10 Лопатин В.Н. Информационное право: Учебник. СПб: Юридический центр Пресс, 2005. С. 474.

Законопроектом № 99114515-2, вносимом на рассмотрение Государственной Думы Российской Федерации депутатами Государственной Думы В.Н. Лопатиным, П.Т. Бурдуковым, С.В. Степашиным в 1999 году, предлагаемое понятие информационно-психологической безопасности определялось как состояние защищенности, отдельных лиц и (или) групп лиц от негативных информационно-психологических воздействий и связанных с этим иных жизненно важных интересов личности, общества и государства в информационной сфере[11].

Через более чем пятнадцать лет один из авторов указанного законопроекта В.Н. Лопатин продолжает отмечать, приводя в пример так называемый «закон информационного опережения (решение проблем информационного взаимодействия должно опережать по времени каждый очередной шаг в других сферах социальной деятельности) следует признать резкое возрастание роли информационной безопасности, необходимость обеспечения которой в рамках информатизации будет в дальнейшем только нарастать»[12].

А. А. Стрельцов понятие «обеспечение информационной безопасности» раскрывает как «сложное явление, включающее объект безопасности, образуемый совокупностью информационных потребностей государства и его деятельности по удовлетворению этих потребностей, угроз объекту безопасности, деятельности государства по противодействию угрозам, а также субъектов этого противодействия»[13].

В свою очередь Т.А. Полякова информационную безопасность рассматривает как состояние защищенности национальных интересов

11 Проект Федерального закона № 99114515-2 «Об информационно-психологической безопасности» (ред., внесенная в ГД ФС РФ, текст по состоянию на 03.12.1999).

12 Лопатин В.Н. Актуальные проблемы реализации и защиты прав Российской Федерации при построении электронного государства // Актуальные проблемы обеспечения национальных интересов Российской Федерации в информационной сфере: доклады исообщения на научно-практической конференции, г. Москва, 8 сентября 2015 года/ под общей редакцией д.ю.н., проф. Н.Н. Куняева. – М.: МФЮА, 2015. – С. 92.

13 Стрельцов А.А. Содержание понятия «обеспечение информационной безопасности» // Информационное общество. 2001. вып. 4. С. 16.

Российской Федерации в информационной сфере, состоящих из совокупности сбалансированных интересов личности, общества и государства, от внутренних и внешних угроз, что соответствует принципу обеспечения национальной безопасности в информационной сфере, определенному в Стратегии развития информационного общества в Российской Федерации.[14]

В целом государственная политика в области обеспечения безопасности, согласно ст. 4 Федерального закона Российской Федерации от 28 декабря 2010 г. № 390-ФЗ «О безопасности»[15] является частью внутренней и внешней политики Российской Федерации и представляет собой совокупность скоординированных и объединенных единым замыслом политических, организационных, социально-экономических, военных, правовых, информационных, специальных и иных мер.

На протяжении нескольких лет только Доктрина информационной безопасности определяла исследуемую дефиницию: информационная безопасность – это состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства[16].

В то же время, необходимо отметить тенденцию принимаемых и разрабатываемых актов, регламентирующих вопросы безопасности, к выделению личности в качестве субъекта информационных отношений и ее интересов в информационной сфере – в качестве приоритетных. Это становится очевидным при анализе норм Стратегии национальной

14 Полякова Т.А. Правовое обеспечение информационной безопасности при построении информационного общества в России. Автореф. дис. …докт. юрид. наук: 12.00.14. Москва, 2008

15Российская газета. № 5374. 29.12.2010.

16Доктрина информационной безопасности Российской Федерации (утверждена Президентом РФ 09.09.2000 г. № Пр-1895) // Парламентская газета. 2000. № 187. 30 сентября.

безопасности Российской Федерации[17] и новой Доктрины информационной безопасности Российской Федерации[18].

Д.А. Ловцов, пытаясь дать свое определение понятию, отмечает, что «под информационной безопасностью в науке понимается свойство субъекта или объекта, характеризующее степень (уровень) защищенности его потребностей в качественной (ценной) информации, необходимой ему для нормального (устойчивого) функционирования (жизнедеятельности) и развития (обучения). К сожалению, в законодательстве пока закреплено лингвистически некорректное определение через состояние (мгновенная характеристика объекта, обеспечивающая определение его свойств в конкретный момент времени и определяемая входными управляющими и возмущающими воздействиями и начальными условиями функционирования) защищенности, то есть одно-единственное - идеальное, а значит, практически недостижимое состояние»[19]. С этим мнением следует согласиться.

Сравнение базового понятия «информационная безопасность» в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента 5 декабря 2016 года[20], и в утратившей силу[21] приводит к ряду неоднозначных размышлений. Прежде всего, «новое» определение стало более развернутым. Напомним, что в утратившей силу Доктрине под информационной безопасностью понималось «состояние защищенности ее национальных интересов в информационной сфере,

17Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru. 31.12.2015.

18Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru. 06.12.2016.

19Ловцов Д.А. Лингвистическое обеспечение правового регулирования информационных отношений в инфосфере // Информационное право. 2015. № 2. С. 8 - 13.

20Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru. 06.12.2016.

21Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895) // Российская газета. № 187. 28.09.2000 (утратила силу).

определяющихся совокупностью сбалансированных интересов личности, общества и государства». Содержание понятия в новой редакции определено как «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства». Как положительное, нельзя не отметить, что нынешняя редакция понятия более осмысленна с точки зрения его не только статических характеристик, но также и динамических, однако «утерянное» указание на значение сбалансированности интересов личности, общества и государства вряд ли следует признать оправданным.

2. Компьютерные вирусы и антивирусные программы

Борьбой с компьютерными вирусами профессионально занимаются тысячи специалистов в десятках компаний. Компьютерные вирусы были и остаются одной из наиболее распространенных причин потери

информации. Известны случаи, когда вирусы блокировали работу организаций и предприятий.

Более того, был зафиксирован случай, когда компьютерный вирус стал причиной гибели человека – в одном из госпиталей Нидерландов пациент получил летальную дозу морфия по той причине, что компьютер был заражен вирусом и выдавал неверную информацию.

Несмотря на огромные усилия конкурирующих между собой антивирусных фирм, убытки, приносимые компьютерными вирусами, не падают и достигают астрономических величин в сотни миллионов долларов ежегодно. Эти оценки явно занижены, поскольку известно становится лишь о части подобных инцидентов. При этом следует иметь в виду, что антивирусные программы и «железо» не дают полной гарантии защиты от вирусов.

Что же это такое? 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 с целью нарушения работы программно-аппаратных комплексов, удаления файлов, приведения в негодность структур размещения данных, блокирования работы пользователей или же приведения в негодность аппаратных комплексов компьютера.

Компьютерные вирусы прошли длительную эволюционную линию, приспосабливаясь к изменчивому миру операционных систем и защитных механизмов. Вирусы получили повсеместное распространение, освоив не только MS DOS, Windows, Linux/BSD, но и мобильные платформы.[22]

Три аксиомы о компьютерных вирусах:

− во-первых, вирусы не возникают сами собой – их создают программисты-хакеры и рассылают по сети передачи данных или подкидывают на компьютеры через съёмные носители данных;

22 Собейкис, В.Г. Азбука хакера. Компьютерная вирусология. - М.: Майор, 2006. – 122 с.

− во-вторых, вирус не может сам собой появиться на вашем компьютере;

− в-третьих, компьютерные вирусы заражают только компьютер и ничего больше, поэтому не надо бояться – через клавиатуру и мышь они не передаются.

В настоящее время известно более 70 000 программных вирусов,их можно классифицировать по следующим признакам:

- среде обитания;
- способу заражения;
- особенностям алгоритма;
- деструктивным возможностям.

В зависимости от среды обитания вирусы делятся на файловые, сетевые, загрузочные и макровирусы. Файловые вирусы внедряются чаще всего в исполняемые модули, то есть в файлы, имеющие расширения COM и EXE. Файловые вирусы могут внедряться и в другие типы файлов, но, как правило, в таком виде они никогда не получают управление и, следовательно, теряют способность к размножению.

Сетевые вирусы распространяются, как следует из названия, по различным сетям. Загрузочные вирусы внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Record). Макровирусы внедряются в форматы файлов, используемые наиболее популярными редакторами, такими как Microsoft Word или Microsoft Excel.

По способу заражения вирусы делятся на резидентные и нерезидентные. Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть

до выключения или перезагрузки компьютера. Нерезидентные вирусы не заражают память компьютера и являются активными лишь ограниченное время.

По особенностям алгоритма вирусы трудно классифицировать из-за большого разнообразия. В связи с методом противостояния защитным механизмам можно выделить несколько основных типов.

Стелс-вирус (англ. stealthvirus – вирус-невидимка) – вирус, полностью или частично скрывающий свое присутствие в системе путем перехвата обращений к операционной системе, осуществляющих чтение, запись, чтение дополнительной информации о зараженных объектах (загрузочных секторах, элементах файловой системы, памяти).

Для скрытия своего кода они используют в основном два способа. Суть первого заключается в том, что вирус автоматически перехватывает команды, которые направлены на чтение-запись зараженного сектора, и моментально подставляет вместо него какой-то незараженный файл. Благодаря таким действиям вирус становится практически невидимым для антивирусных программ (которые не могут лечить оперативную память).

Второй способ разработан с целью борьбы с антивирусами, которые поддерживают специальные команды чтения секторов напрямую через отдельные порты контроллера жесткого диска. Во время запуска программы (антивируса, к примеру) такие вирусы восстанавливают ранее зараженные сектора жесткого диска, а после окончания ее работы опять восстанавливают зараженное состояние.

Загрузочный вирус перехватывает функцию ОС, предназначенную для посекторного доступа к дискам, с целью «показать» пользователю или программе-антивирусу оригинальное содержимое сектора до заражения.[23]

Файловые стелс-вирусы, которые используют такой способ скрытия своей активности, в большинстве случаев очень громоздки. Это связано

23 Климентьев К. Е. Компьютерные вирусы и антивирусы, взгляд программиста. – М.: ДМК- Пресс, 2015. –309 с.

с тем, что им необходимо перехватывать огромное количество DOS-функций работы с приложениями и файлами. К ним относятся: чтение/запись, открытие/закрытие, запуск, поиск, переименование и так далее.

Файловый вирус перехватывает функции чтения/установки позиции в файле, чтения/записи в файл, чтения каталога и так далее, чтобы скрыть увеличение размера зараженных программ; перехватывает функции чтения/записи/отображения файла в память, чтобы скрыть факт изменения файла.

Последними по списку, но не по значению являются макровирусы. Реализация стелс-алгоритмов с использования макропрограмм является самой простой и одновременно многофункциональной задачей. Для маскировки вполне достаточно запретить вызов меню Tools/Macro или File/Templates. Зачастую вирус подменивает эти пункты из меню на зараженные макросы либо удаляет их вообще.

Стелс-вирусы могут быть обнаружены, если их сигнатура уже есть в антивирусной базе.

Полиморфик-вирусы. К полиморфик-вирусам относятся те из них, детектирование которых невозможно осуществить при помощи так называемых вирусных масок, или сигнатур – участков постоянного кода, специфичных для конкретного вируса. Достигается это двумя основными способами – шифрованием основного кода вируса с непостоянным ключом и случайным набором команд расшифровщика или изменением самого выполняемого кода вируса. Полиморфизм различной степени сложности встречается в вирусах всех типов – от загрузочных и файловых DOS-вирусов до Windows-вирусов и даже макровирусов. Этот вид компьютерных вирусов представляется на сегодняшний день наиболее опасным.

Такие вирусы не только шифруют свой код, используя различные пути шифрования, но и содержат код генерации шифровщика и расшифровщика, что отличает их от обычных шифровальных вирусов, которые также

могут шифровать участки своего кода, но имеют при этом постоянный код шифровальщика и расшифровщика. Все это делается ради затруднения анализа кода вируса.[24]

По деструктивным возможностям вирусы можно разделить на следующие виды:

- безвредные, то есть никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);

- неопасные, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах;

- опасные вирусы, которые могут привести к различным нарушениям в работе компьютера;

- очень опасные, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

Существуют различные виды антивирусных программ: программмы-детекторы, программы-доктора, программы-ревизоры, программы-фильтры и программы-вакцины.

Программы-детекторы обеспечивают поиск и обнаружение вирусов в оперативной памяти и на внешних носителях и при обнаружении выдают соответствующее сообщение. Различают детекторы универсальные и специализированные.

Универсальные детекторы в своей работе используют проверку неизменности файлов путем подсчета и сравнения с эталоном контрольной суммы. Недостаток универсальных детекторов связан с невозможностью определения причин искажения файлов.

24 Глушаков, С.В. Секреты хакера: защита и атака / С.В. Глушаков, Т.С. Хачиров, Р.О. Соболев. – 3-е изд. – Ростов н/Д.: Феникс; Харьков: Фолио, 2008. – 245-247 с.

Специализированные детекторы выполняют поиск известных вирусов по их повторяющемуся участку кода. Недостаток таких детекторов состоит в том, что они неспособны обнаруживать все известные вирусы.

Детектор, позволяющий обнаруживать несколько вирусов, называют полидетектором.

К недостаткам таких антивирусных программ можно отнести то, что они могут находить только те вирусы, которые известны разработчикам таких программ, а также они не могут "вылечить" повреждения, наносимые вирусами. Примерами таких программ служат Avast antivirus protection, drsolomon's antivirus toolkit и Norman virus control.[25]

Программы-доктора, в отличие от детекторов, не только находят зараженные вирусами файлы, но и "лечат" их, то есть удаляют из файла тело программы вируса, возвращая файлы в исходное состояние. В начале своей работы доктора ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к «лечению» файлов. Среди докторов выделяют полидокторов, то есть программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов.

Учитывая, что постоянно появляются новые вирусы, еще одним недостатком программ-детекторов и программ-докторов является то, что они быстро устаревают и требуется регулярное обновление их версий.

Программы-ревизоры относят к самым надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран монитора. Как правило, сравнение состояний производят сразу после загрузки операционной системы.

25 Домачев, А. Некоторые проблемы правового регулирования электронного документооборота в киберпространстве [Электронный ресурс] / А. Домачев. – Электрон. дан. – 2006. – Режим доступа: http://www.reestr-pki.ru/binaries/70/assoc-conv.doc.

При сравнении проверяются длина файла, контрольная сумма файла, дата и время модификации и некоторые другие параметры.

Программы-ревизоры имеют достаточно развитые алгоритмы, могут обнаружить стелс-вирусы и могут даже отличить изменения версии проверяемой программы от изменений, внесенных вирусом.

Программы-фильтры, которые также называются программы-сторожа, представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться:

- попытки коррекции файлов с расширениями COM и EXE;
- изменение атрибутов файлов;
- прямая запись на диск по абсолютному адресу;
- запись в загрузочные сектора диска;
- загрузка резидентной программы.

При попытке какой-либо программы произвести указанные действия «сторож» посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Программы-фильтры весьма полезны, так как способны обнаружить вирус на самой ранней стадии его существования до размножения. Но недостаток в том, что лечить файлы и диски они не умеют. Для уничтожения вирусов требуется применить другие программы, например доктора.[26]

К недостаткам программ-сторожей еще можно отнести их «назойливость» (например, они постоянно выдают предупреждение о любой попытке копирования исполняемого файла), а также возможные конфликты с другим программным обеспечением.

Последний вид программ – это программы-вакцины, также их называют иммунизаторы. Это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-

26 Гульев И. Создаем вирус и антивирус. – М.: ДМК- Пресс,2013. –50 с.

доктора, «лечащие» этот вирус. Но вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. В настоящее время программы-вакцины имеют ограниченное применение. Еще одним существенным недостатком таких программ является их ограниченные возможности по предотвращению заражения от большого числа разнообразных вирусов.

Заключение

В заключении хотелось бы отметить, что современный век информационных технологий очень разнообразен. Каждый день появляются новые программы или обновления к уже существующим. И мало кто задумывался над вопросом безопасности данной программы, то есть о ее непосредственной безвредности. Потому что компьютер предмет первой необходимости, ему нужно уделять особое внимание и проявлять

надежную защиту, которую сможет обеспечить такая программа, как антивирус.

Антивирусная программа (антивирус) – это специализированная программа для защиты компьютера, а именно для обнаружения опасных деструктивных программ и предотвращения заражения, так называемым, вирусным атакам и эпидемиям.

С появлением многозадачной и разветвленной системой Windows и распространения интернета, требования к разработчикам стали существенно выше. То есть программе необходимо было производить проверку файлов очень быстро, что привело к резкому сокращению числа производителей, а также к существенному росту прибыли. Сегодня борьба с вредоносными программами также продолжается (более 60 компаний трудится над разработкой). И на данный момент самыми популярными из них остаются: Антивирус Касперского,Eset NOD32, Symantec Norton Anti - Virus, Dr.Web иAvast.

Вот уже на протяжении более двадцати лет, индустрия антивирусных программ заметно преобразилась. Появились более качественные утилиты, способные предотвращать практически любые вирусные угрозы. Но все же есть небольшая ложка дегтя в этой бочке меда, и существуют несколько заметных минусов, на которые пользователи постоянно выражают свое недовольствие. Первый и самый значимый фактор – это стоимость программы. Да, разработчики тоже как- то должны зарабатывать на хлеб, но ведь и не каждый пользователь может себе позволить ее приобрести. К примеру, цена за один год пользования Антивирусом Касперского колеблется в районе 1200 рублей. На второе место выходит требовательность к ресурсам. То есть может возникнуть проблема нехватки производительности компьютера. Следующим фактором является интерфейс. Необходимо его как можно больше минимизировать, ведь люди тянутся к простоте.

Ну и как же не затронуть вопрос «а что же ждет антивирусы в будущем?». По современным сведениям разработчики Израиля планируют отказаться от постоянного обновления программ. Суть которой состоит в том, чтобы искать вредоносные файлы и сверять их с кодом файлов своих баз данных. Также вскоре планируют снизить системное требование при применении кэширования проверенных файлов, что позволит использовать антивирусы на менее мощных процессорах. Еще одним нововведением стало добавление поддержки Unicode, которое сможет обеспечить полную совместимость с новыми версиями приложений.

Таким образом, можно надеяться, что вскоре появится такой антивирус, который сможет моментально анализировать и предотвращать любую вирусную угрозу.

Список использованной литературы

Нормативно-правовые акты

1. Федеральный закон Российской Федерации от 28 декабря 2010 г. № 390-ФЗ «О безопасности» // Российская газета. 2010. № 295.
2. Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru. 31.12.2015.

3. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru. 06.12.2016.
4. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru. 06.12.2016.
5. Проект Федерального закона № 99114515-2 «Об информационно-психологической безопасности» (ред., внесенная в ГД ФС РФ, текст по состоянию на 03.12.1999).
6. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895) // Российская газета. № 187. 28.09.2000 (утратила силу).

Список учебной и научной литературы

7. Атаманов Г.А. Информационная безопасность: сущность и содержание // Бизнес и безопасность в России. – 2007. – № 47. – 108-112 с.
8. Бачило И.Л. Информационное право: Учеб. Для вузов. М.: Высшее образование; Юрайт-Издат, 2009.- 515 с.
9. Глушаков, С.В. Секреты хакера: защита и атака / С.В. Глушаков, Т.С. Хачиров, Р.О. Соболев. – 3-е изд. – Ростов н/Д.: Феникс; Харьков: Фолио, 2008. – 414 с.
10. Гульев И. Создаем вирус и антивирус. – М.: ДМК- Пресс,2013. –50 с.
11. Иноземцев В.Л. За пределами экономического общества. Постиндустриальные теории и постэкономические тенденции в современном мире. – М.: Наука, 1998.
12. Кафтанчиков Д.П. Информационная безопасность Российской Федерации: современное состояние и приоритеты обеспечения. Автореф. дис. …канд. полит.наук: 23.00.02. Орел, 2009

13. Ковалева Е. В. Обеспечение транспарентности органов местного самоуправления современной России в процессе информатизации политического управления. Автореф. дис. …канд. полит.наук: 23.00.02. Саратов, 2010
14. Коваленко В.И. Критика новейших буржуазных концепций государственно-монополистического капитализма.— М.: Прогресс, 1987.
15. Крылов Г.О. Международный опыт правового регулирования информационной безопасности и его применение в Российской Федерации. Автореф. дис. …канд. юрид. наук: 05.13.19. Москва, 2007.
16. Ловцов Д.А. Лингвистическое обеспечение правового регулирования информационных отношений в инфосфере // Информационное право. 2015. № 2. С. 8 - 13.
17. Лопатин В.Н. Актуальные проблемы реализации и защиты прав Российской Федерации при построении электронного государства // Актуальные проблемы обеспечения национальных интересов Российской Федерации в информационной сфере: доклады исообщения на научно-практической конференции, г. Москва, 8 сентября 2015 года/ под общей редакцией д.ю.н., проф. Н.Н. Куняева. – М.: МФЮА, 2015. – 92-95 с.
18. Лопатин В.Н. Информационное право: Учебник. СПб: Юридический центр Пресс, 2005. 675 с.
19. Новая технократическая волна на Западе. – М.: Прогресс, 1986
20. Полякова Т.А. Правовое обеспечение информационной безопасности при построении информационного общества в России. Автореф. дис. …докт. юрид. наук: 12.00.14. Москва, 2008
21. Проценко Е.А. Модель и метод анализа эффективности систем защиты информации сайтов органов власти Российской Федерации. Автореф. дис. …канд. технич. наук: 05.13.19. Санкт-Петербург, 2008.

22. Собейкис, В.Г. Азбука хакера. Компьютерная вирусология. - М.: Майор, 2006. – 512 с.
23. Стрельцов А.А. Содержание понятия «обеспечение информационной безопасности» // Информационное общество. 2001. вып. 4. 14-17 с.
24. Тоффлер Э. Третья волна. – М..: Изд-во «Аст», 1999
25. Уэбстер Ф. Теории информационного общества. – М.: Аспект - пресс, 2004
26. Шемякин В.П. Информационная безопасность в современных российских условиях: Социолого-управленческие аспекты. Автореф. дис. …канд. социол. наук: 22.00.08. Москва, 2004

Электронные источники

27. Климентьев К. Е. Компьютерные вирусы и антивирусы, взгляд программиста. – М.: ДМК- Пресс, 2015. –309 с.
28. COMSS1[Электронный ресурс] // comss.ru http: // www.comss.info / Istorija _ zarozhdenija _ antivirusov