САНКТ-ПЕТЕРБУРГСКИЙ УНИВЕРСИТЕТ
МВД РОССИИ

КАЛИНИНГРАДСКИЙ ФИЛИАЛ

ГРИГОРЬЕВ А.Н., МУСКАТИНЬЕВ А.Ю.,
ИВАНОВ П.Ю.,

ОРГАНИЗАЦИЯ АНТИВИРУСНОЙ ЗАЩИТЫ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

УЧЕБНОЕ ПОСОБИЕ

КАЛИНИНГРАД
2016

УДК 004.056.5(075)
ББК Х.с51я73

Г83 Григорьев А.Н., Мускатиньев А.Ю., Иванов П.Ю. Организация антивирусной защиты автоматизированных информационных систем органов внутренних дел: учебное пособие. - Калининград: Калининградский филиал СПбУ МВД России, 2016. - 108 с.

Рецензенты:

- начальник тыла УМВД России по Калининградской области полковник внутренней службы А.Н. Салин;
- заместитель начальника ЦИТСиЗИ УМВД России по Калининградской области подполковник внутренней службы Ю.Ю. Безмельников.

Издание посвящено актуальным вопросам организации защиты автоматизированных информационных систем органов внутренних дел от воздействия вредоносных программ. В нем рассматриваются современные угрозы безопасности информационным системам, виды вредоносных программ и ответственность за их распространение, правовые основы обеспечения антивирусной защиты информационных систем МВД России, современные технологии антивирусной защиты, а также особенности организации подсистемы антивирусной защиты в ИСОД ОВД.

Пособие предназначено для курсантов, слушателей, преподавателей ведомственных образовательных организаций, а также сотрудников информационно-аналитических подразделений органов внутренних дел, подразделений технической защиты информации МВД России.

© Григорьев А.Н., Иванов П.Ю., Мускатиньев А.Ю., 2016.
© Калининградский филиал СПбУ МВД России, 2016.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ 4

1. СОВРЕМЕННЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫМ СИСТЕМАМ 6

2. ПОНЯТИЕ И ВИДЫ ВРЕДОНОСНЫХ ПРОГРАММ. ОТВЕТСТВЕННОСТЬ ЗА РАСПРОСТРАНЕНИЕ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ 18

3. ПРАВОВЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ АНТИВИРУСНОЙ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ МВД РОССИИ 38

4. СОВРЕМЕННЫЕ ТЕХНОЛОГИИ АНТИВИРУСНОЙ ЗАЩИТЫ, ОТЕЧЕСТВЕННЫЙ РЫНОК АНТИВИРУСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ 57

5. ЕДИНАЯ СИСТЕМА ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОГО ОБЕСПЕЧЕНИЯ МВД РОССИИ КАК ОБЪЕКТ АНТИВИРУСНОЙ БЕЗОПАСНОСТИ 70

6. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ПОДСИСТЕМЫ АНТИВИРУСНОЙ ЗАЩИТЫ В ИСОД ОВД 80

ЗАКЛЮЧЕНИЕ 90

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 93

ПРИЛОЖЕНИЕ 101

ВВЕДЕНИЕ

Анализ практики правоохранительной деятельности свидетельствует о том, что эта деятельность неразрывно связана с процессами глобальной информатизации всех сторон и аспектов жизнедеятельности современного общества, выражающейся, с одной стороны, в стремительном росте объема производимых и потребляемых информационных ресурсов, в том числе и открытых для общего доступа с использованием средств массовых коммуникаций, профессионализации преступного сообщества, вовлечении в преступную деятельность новейших информационных технологий, а с другой - в широком использовании современных информационных технологий и в деятельности органов внутренних дел.

Вместе с тем происходящие в современном обществе процессы глобальной информатизации определяют не только характер и глубину совершаемых преобразований, но и новые цели, задачи деятельности органов внутренних дел, обуславливаемые все возрастающей степенью «технизации» и интеллектуализации преступного сообщества, вовлечения в преступную деятельность новейших достижений науки и техники. Доступность и широкое использование информационных технологий является важнейшим фактором, создающим почву для качественной трансформации преступной деятельности, ее «виртуализации», перехода от традиционных иерархических к сетевым формам ее организации. Отмеченное предопределяет широкое использование в практике правоохранительной деятельности информационных систем, построенных на базе новых информационных технологий. В современных условиях эти технологии составляют ядро информационного обеспечения правоохранительной деятельности и являются неотъемлемой частью профессиональной деятельности сотрудника органов внутренних дел, поскольку информация является не только ее основой, но и связующим звеном со всей деятельностью гос-ударства по борьбе с преступностью.

Однако широкое использование в практике деятельности органов внутренних дел не только расширяет возможности правоохранительных органов по противодействию современной преступности, но и порождает целый ряд угроз в сфере обеспечения информационной безопасности правоохранительной деятельности. Как указал в своем выступлении на прошедшем 8 июля 2015 г. в г. Вологде совещании, посвященном вопросам противодействия угрозам в информационной сфере, Секретарь Совета Безопасности Российской Федерации Н.П. Патрушев: «...Специалисты отмечают замет-

ное увеличение числа компьютерных атак на информационно-телекоммуникационные сети и информационные системы органов государственной власти»[1]. О масштабах проблемы красноречиво свидетельствует и тот факт, что только в 2014 году Федеральной службой безопасности России было пресечено 74 миллиона кибератак на официальные сайты российских структур и государственных органов[2].

Вышеизложенное позволяет констатировать неуклонно возрастающий уровень опасности в сфере информационных технологий. По результатам опроса, проведенного специалистами Лаборатории Касперского, за последний год 96% отечественных компаний сталкивались с угрозами информационной безопасности[3]. Более того, более половины участников исследования отмечают ухудшение ситуации - возрастание количества кибератак, и лишь 8% констатируют снижение их количества.

Многие организации пострадали от киберпреступников: например, треть вирусных атак (а в российских компаниях - почти половина) закончилась потерей данных, при этом для 10% организаций это была важная для их деятельности информация.

В сложившихся условиях особую актуальность приобретает вопрос организации антивирусной защиты корпоративных информационных систем, в том числе и систем, используемых в деятельности органов внутренних дел.

Существует достаточно большое количество научных исследований, в которых рассматриваются различные вопросы обеспечения защиты информации в автоматизированных информационных системах, используемых в практической деятельности органов внутренних дел. Данным вопросам посвящены работы таких ученых, как К.К. Борзунов, В.А. Галатенко, А.Н. Григорьев, Л.А. Домбровская, В.Е. Кадулин, С.А. Клейменов, В.П. Мельников, А.С. Овчинский, А.И. Примакин, И.Н. Старостенко, Ю.Н. Сопильняк, В.В. Фадеева, С.М. Шапиро и др.

Вместе с тем анализ специальной литературы позволяет констатировать, что проблема организации антивирусной защиты ав-

[1] Патрушев рассказал о внедрении разведками вирусов в информационные системы госвласти [Электронный ресурс]. - Режим доступа: http://vz.ru/news/2015/7/8/755034.print.html.

[2] Путин: ФСБ в 2014 году пресекла деятельность 209 агентов иностранных спец-служб [Электронный ресурс]. - Режим доступа: http://vz.ru/news/2015/3/26/736531.html.

[3] Киберугрозы и информационная безопасность в корпоративном секторе: тенденции в мире и в России [Электронный ресурс]. - Режим доступа: http://www.kaspersky.ru/downloads/pdf/kaspersky_global_it_security_risks_survey.pdf.

томатизированных информационных систем органов внутренних дел является недостаточно изученной и нуждается в отдельной проработке. Наиболее актуальной задачей в этой сфере является разработка научно обоснованных подходов к построению подсистемы антивирусной безопасности как необходимой составляющей полноценной системы информационной безопасности в ИСОД ОВД, способной своевременно и эффективно противостоять вредоносному программному обеспечению. Указанные обстоятельства предопределили выбор темы исследования и ее актуальность.

1. СОВРЕМЕННЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫМ СИСТЕМАМ

Современное общество переживает сложные и порой весьма драматичные процессы модернизации и реформирования всех сфер общественной жизни, которая отличается высоким динамизмом и взаимозависимостью событий. Нередко решение этих поистине масштабных задач сопряжено с преодолением не только внутренних, но и внешних проблем, являющихся следствием глобализации всех сторон жизнедеятельности современного общества. По сути, человечество вступает в уникальную эпоху зарождения и развития гигантских по масштабам процессов и явлений в сфере экономики, культуры, геополитики, кардинальным образом меняющих облик современного общества и обуславливающих переход к качественно новой архитектуре мира.

Движущей силой глобализации современного мира выступают новые информационные технологии, которые «...начинают играть ведущую роль в современном обществе, уровень развития которого в значительной мере определяется степенью использования средств обработки информации (компьютеров, вычислительной техники, ксероксов, телефонов, программного обеспечения), плотностью потока изобретений новых продуктов и новых технологий с помощью компьютерных программ»[1].

Как отмечает И.В. Кондратьева, «...современное общество представляет собой комплекс активно развивающихся моделей коммуникаций, основанных на технических средствах связи, специфика новой эпохи характеризуется разработкой и внедрением новых

[1] Мамедов Э.Э.О. Роль информационных технологий в эпоху информационного общества на современном этапе // Вопросы новой экономики. 2008. № 1. С. 36.

методов обработки, передачи и хранения информации. Возможности информационно-коммуникационных технологий позволяют развивать возможности социального взаимодействия, что приводит к совершенствованию и увеличению скорости и качества передачи разнообразных информационных посланий на любые расстояния, что позволяет также связать в единую информационную сеть различные сегменты социального пространства. Такое многообразие форм информационного взаимодействия позволяет образовывать новые информационные центры, создавая границы, которые не совпадают с национально-государственными, а также способствуют образованию новой иерархической структуры. В результате таких изменений происходят преобразования в моделях социальной организации и сотрудничества»[1]. По мнению Н.Н. Калинкиной, «...дело идет к формированию в XXI веке единого мирового информационного пространства, которое будет основано на развитии глобальных информационно-телекоммуникационных систем, использовании унифицированных международных протоколов информационного обмена и методов удаленного доступа к базам данных и знаний различного назначения»[2].

Вместе с тем сегодня уже совершенно очевидно, что «...процесс глобальной информатизации развивается стремительно, лавинообразно и непредсказуемо, опережая теоретическое осмысление его последствий...»[3]. Как отмечает Р. Даль, «...мы едва лишь начали серьезно обдумывать открываемые ими *(информационно-коммуникационными технологиями - прим. авт.)* возможности и провели в ничтожных масштабах самые первые, робкие пробы»[4].

Одним из вызовов, который несет в себе глобальная информатизация современному обществу, является то обстоятельство, что переживаемая человечеством информационная революция не только ускоряет развитие цивилизации, но и порождает новые угрозы безопасности личности, общества и государства.

К числу таких угроз, без всякого сомнения, следует отнести такое явление, как криминализация современного информационного

---

[1] Кондратьева И.В. Трансформация информационно-коммуникационных технологий в условиях современного общества // Альманах современной науки и образования. 2009. № 7-2. С. 75.

[2] Калинкина Н.Н. Контуры формирования информационного общества в России: информатизация общества и развитие информационной инфраструктуры // Вестник Нижегородского университета им. Н.И. Лобачевского. 2010. № 3-2. С. 496.

[3] Мешкова Т.А. Социально-политические аспекты глобальной информатизации // Полит. исследования. 2002. № 6(71). С. 24-33.

[4] Даль Р. О демократии. М.: Аспект Пресс, 2000. С. 179.

пространства. В этой связи в выступлении Генерального секретаря ООН на десятом Конгрессе Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями (10-17 апреля 2000 г., Вена) отмечается, что глобальная информатизация «...создает условия для возникновения новых, более широких форм преступности. В результате изменений в структуре торговли, финансов, связи и информации, ... преступность уже не ограничивается национальными границами. Она становится все более трансграничной, а во многих случаях приобретает глобальный характер...»[1]. Таким образом, современные технологии дали толчок не только свободной торговле, глобализации и виртуализации экономической деятельности, но и стимулировали преступную деятельность[2].

В этой связи трудно не согласиться с утверждением Р.Г. Нургалиева о том, что «...современное общество, хотим мы того или нет, значительно зависит от компьютерных технологий. Вместе с тем технические инновации, внедряемые в киберпространство, значительно опережают их гуманитарное осмысление, что приводит к различным проблемам, препятствующим широкому бесконфликтному использованию возможностей новых технологий... Постоянно расширяющиеся возможности глобальных информационных телекоммуникационных сетей (ИТКС) обусловили повышенный интерес к ним со стороны организованной преступности, в том числе экстремистских и террористических организаций... Современные ИТКС характеризуются прежде всего значительным числом пользователей и предоставлением сервиса без закрепления de jure и de facto за пользователем абонентского терминала (чаще всего мобильного) и набора услуг. Криминалитет умело использует эти возможности для многократного усиления динамики и скрытности своей деятельности»[3].

Особую актуальность данный вопрос приобретает в связи с появлением и бурным развитием сетевых информационных технологий, в том числе с широким использованием в различных сферах человеческой деятельности возможностей глобальной электронной сети Интернет.

---

[1] Десятый Конгресс ООН по предупреждению преступности и обращению с правонарушителями Вена, 10-17 апреля 2000 г. Положение в мире в области преступности и уголовного правосудия. Доклад генерального секретаря A/CONF.187/5. С. 3.

[2] Григорьев А.Н. Безопасность в эпоху информатизации: новые угрозы и новые возможности // Материалы XIII Международной конференции «Информатизация и информационная безопасность правоохранительных органов». Москва, 25-26 июня 2004 г. М.: Академия управления МВД России, 2004. С. 26-31.

[3] Нургалиев Р.Г. Электронный патруль. В МВД создали систему защиты кибернетического пространства // Российская газета. 2009. 16 окт.

«Глобальная сеть Интернет открыла любому пользователю безграничный доступ к информационным ресурсам человечества, - пишут В.М. Трегубова, Т.А. Оводкова, А.Ф. Мялкина. - Не выходя из дома или из офиса можно получать интересующую информацию, дистанционно обучаться в учебных заведениях, совершать интернет-покупки, выбирать и бронировать отели, получать электронные государственные услуги, участвовать в форумах и конференциях, обмениваться мнениями с пользователями сети и многое, многое другое. Интернет создал для людей новые площадки для общения. С помощью социальных сетей мы можем найти одноклассников, разговаривать с друзьями и близкими, которые находятся на другом краю земли»[1].

В этой связи трудно не согласиться с мнением Д.А. Беляева, заметившего, что «если говорить о степени влияния Интернета на человечество, то экономический (финансовый) эффект от его использования вряд ли можно посчитать. В то же время организационная и социальная эффективность очевидна. Интернет является и управленческим инструментом, и социальным помощником. Но самый большой эффект, который ... не поддается никакой количественной оценке, заключается в том, что он кардинально изменил мировоззрение поколения людей XXI века. Интернет сейчас больше, чем некая информационная технология. Он является не только высокоэффективным инструментом решения наших стратегических и повседневных задач. Интернет фактически реализует идею Вернадского о ноосфере и сам постепенно становится ею»[2].

И действительно, Интернет настолько прочно вошел в нашу жизнь, что ограничение доступа к этой сети рассматривается в современном обществе как нарушение прав человека[3]. В этой связи не удивительно, что именно с появлением данной сети эксперты связывают процессы коренной трансформации современной преступности[4].

---

[1] Трегубова В.М., Оводкова Т.А., Мялкина А.Ф. Глобальная сеть в России: проблемы и перспективы // Социально-экономические явления и процессы. 2014. № 4(62). С. 101.

[2] Беляев Д.А. Интернет как основа информационного общества // Сборники конференций НИЦ Социосфера. 2011. № 1. С. 10.

[3] Доступ в Интернет приравняли к базовым правам человека [Электронный ресурс]. - Режим доступа: http://www.km.ru/v-mire/2011/06/07/oon/

[4] См.: Григорьев А.Н., Мешков В.М. Некоторые аспекты формирования научных основ расследования преступлений, сопряженных с использованием средств компьютерной техники // Библиотека криминалиста. Научный журнал. 2013. № 5. С. 256-264; Зяблов Д.Н. Использование интернета террористическими организациями в современном мире // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. 2011. № 4-3. С. 42-45.

Работы по созданию сети Интернет начались в далеком 1969 году. Именно в этом году - 2 января 1969 года - был дан старт проекту разработки сети Агентства перспективных исследований ARPA (Advances Research Projects Agency), получившей название ARPANET. В рамках реализации данного проекта были заложены технологические основы сети, которые позволили 2 сентября 1969 года впервые в истории осуществить по телефонной линии связь между двумя компьютерами, установленными в разных городах США. Именно этот день и считается официальным «днем рождения» сети Интернет.

В настоящее время глобальная (общемировая) сеть Интернет представляет собой совокупность неопределенного множества самых различных ЭВМ и их сетей, работающих по согласованным правилам - протоколам.

В 1985 году в Интернете было около двух тысяч компьютеров. Современная же статистика сети выглядит следующим образом.

Согласно результатам проведенных исследований по состоянию на июнь 2014 года интернет-аудитория составляет 3.053.749.340 человек. Общая картина распределения пользователей Интернет по регионам мира выглядит следующим образом[1]:

Таблица 1

Распределение пользователей сети Интернет по регионам мира					
Регионы и группы стран	Численность населения (млн. чел)	Численность пользователей сети Интернет (млн. чел)			Рост за период с 2000 по 2014 г.г. (в %)
		31.12.00	31.06.14	в % к населению	
Африка	1125	4	297	26,5	6.498,6
Азия	3996	114	1386	34,7	1.112,7
Европа	825	105	582	70,5	454,2
Средний Восток	231	3	111	48,3	3.303,8
Северная Америка	353	108	310	87,7	187,1
Латинская Америка/страны Карибского бассейна	612	18	320	52,3	1.672,7

[1] См.: World Internet Users and Population Stats [Электронный ресурс]. - Режим доступа: http://www.internetworldstats.com/stats.htm.

Океания/ Австралия	36	7	26	72,9	251,6
ВСЕГО	7182	360	3035	42,3	741,0

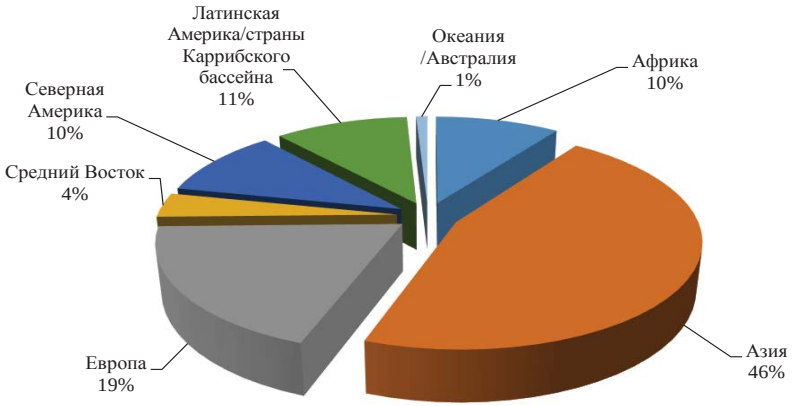

Рис. 1.1. Распределение пользователей сети Интернет по регионам мира

Как можно заметить из приведенных выше данных, численность пользователей сети Интернет за последние 14 лет выросла в 8,5 раз. При этом больше всего в процентном отношении пользователей в Северной Америке, Океании/Австралии и Европе.

Говоря о России, следует отметить, что, начиная с 1994 года, в стране наблюдается устойчивый рост числа активных пользователей сети. По данным Министерства связи и массовых коммуникаций Российской Федерации, по состоянию на октябрь 2014 года количество интернет-пользователей в России составляет 66% общего населения страны. Ежедневно выходят в сеть 53,6 млн взрослых россиян.

С конца 80-х годов прошлого века Интернет стремительно завоевывал популярность в мире, предоставляя все новые, более совершенные средства коммуникации, совместной работы, передачи информации. Совершенный технологический прорыв привел к появлению подлинно глобальной сети, доступной большинству населения самых разных стран мира.

Вместе с тем те очевидные преимущества, которые несет в себе Интернет, могут быть использованы и используются в преступной деятельности. В настоящее время Интернет привлекает

пристальное внимание различного рода преступных групп в первую очередь легкостью доступа, отсутствием прямого правительственного контроля, анонимностью а также удаленным доступом к огромной аудитории пользователей[1].

Указанные обстоятельства обуславливают резкую переориентацию региональных организованных преступных формирований на использование современных Интернет-технологий при совершении преступлений различного характера. Помимо всего, сейчас имеет смысл говорить не только об организованности криминального Интернет-сообщества, но и о повышении его влияния практически на все информационные процессы и явления, происходящие в глобальной сети и реальном мире[2]. О масштабах угрозы красноречиво свидетельствует хотя бы тот факт, что, по оценкам экспертов МВД России, ежесекундно жертвами киберпреступников становятся 12 человек в мире[3]. При этом прослеживается четкая тенденция вытеснения с криминального рынка преступников-одиночек. На смену им приходят хорошо организованные и разветвленные группы, объединяющие людей из разных регионов России или стран мира.

Таким образом, повсеместное использование сетевых технологий значительно повышает риски возникновения угроз личной и корпоративной информации. Как отмечает А.В. Шляпкин, «...в настоящее время киберпреступники используют различные виды сетевых атак, которые стремятся проникать в корпоративные и локальные сети с целью нарушения конфиденциальности, целостности и доступности информационных ресурсов, перехвата управления сетью или подавления информационного обмена путем резкого повышения коэффициента рабочей загрузки серверов сети»[4].

---

[1] См.: Глухарев Д.С. Противодействие экстремизму в современном медиапространстве // Вестник Южно-Уральского государственного университета. Серия: Социально-гуманитарные науки. 2012. № 10(269). С. 135-137.

[2] Гуров А.И: Угрозы национальной безопасности Российской Федерации и их уголовно-правовое регулирование // Уголовное право в XXI веке: материалы международной научной конференции, состоявшейся на юридическом факультете МГУ им. М.В. Ломоносова (31 мая - 1 июня 2001 г.). М., 2002. С. 14.

[3] По оценкам экспертов ежесекундно жертвами киберпреступников становятся 12 человек в мире [Электронный ресурс]. - Режим доступа: http://mvd.ru/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii/Publikacii_i_vistuplenija/item/1951798.

[4] Шляпкин А.В. Методы и средства противодействия атакам на компьютерные сети // Информационные системы и технологии: управление и безопасность. 2014. № 3. С. 325.

Существенно возрастает и ущерб, причиняемый российскому обществу киберпреступностью. Так, по оценкам аналитиков компании Group-IB, объем рынка киберпреступности в Российской Федерации в 2014 г. составил 2,5 млрд дол.[1] При этом среднегодовой ущерб от киберпреступлений в России достиг 3,3 млн долларов для организации. По данным исследования 2014 Cost of Cyber Crime Study, проведенного компанией Ponemon Institute при поддержке HP Enterprise Security, средний годовой убыток каждой организации из числа участвовавших в опросе составил 12,7 млн долларов, что на 96% больше аналогичного показателя, зарегистрированного пять лет назад. Выяснилось также, что в среднем время, уходящее на устранение последствий кибератаки, за тот же период выросло на 33%, а ущерб от одной атаки превысил 1,6 млн долларов[2].

В этой связи представляется вполне закономерным то, что в отчете о наиболее опасных угрозах для мировой экономики, подготовленном экспертами на Всемирном экономическом форуме в Давосе, киберугрозам отведено «почетное» четвертое место, после опасений по поводу неравенства доходов и бюджетных диспропорций, а также увеличения объемов выбросов в атмосферу парниковых газов[3].

Еще одной тревожной тенденцией в сфере кибербезопасности является рост количества атак на российские информационные ресурсы, активизация деятельности иностранных разведок по внедрению в информационные системы органов государственной власти Российской Федерации своих программных средств.

Как отметил в своем выступлении на заседании Совета Безопасности Президент Российской Федерации В.В. Путин, «...надежная работа информационных ресурсов, систем управления и связи имеет исключительное значение для обороноспособности страны, для устойчивого развития экономики и социальной сферы, для защиты суверенитета России в самом широком смысле этого слова... Вместе с тем наши соответствующие ведомства фиксируют постоянный рост компьютерных атак на российские информационные ресурсы. Должен сказать, что за последнее время ... количество атак увеличилось в разы... При этом методы, средства и тактика прове-

[1] Тенденции развития преступности в области высоких технологий 2014 [Электронный ресурс]. - Режим доступа: http://report2014.group-ib.ru/.
[2] Воронина Ю. Наперегонки с хакерами [Электронный ресурс]. - Режим доступа: http://www.rg.ru/2014/10/28/ubytok-ot-hackerov.html.
[3] Киберугрозы занимают четвертое место среди самых опасных угроз для мировой экономики [Электронный ресурс]. - Режим доступа: http://www.iso27000.ru/novosti-i-sobytiya/kiberugrozy-zanimayut-chetvertoe-mesto-sredi-samyh-opasnyh-ugroz-dlya-mirovoi-ekonomiki.

дения подобных атак совершенствуются, а их интенсивность прямо зависит от текущей международной обстановки»[1].

Так, в 2014 году специалистами компании Symantec был детектирован компьютерный вирус Regin, направленный против промышленных объектов России и Саудовской Аравии - более половины атак этого червя были зафиксированы в этих двух странах. Основное назначение червя - слежка за крупными корпорациями, операторами связи, научными лабораториями и правительственными организациями. «Данный вирус действительно очень опасен. Regin обладает возможностью таргетированно заражать целые корпоративные сети для перехвата управления на всех возможных уровнях, - полагает Костин Раю, руководитель центра глобальных исследований и анализа угроз «Лаборатории Касперского». - Вредоносная программа ворует конфиденциальную информацию и обладает способностью осуществлять разнообразные сценарии и виды атак ... в вопросе гибкости, организации кода, применения техник скрытия своего присутствия и реализации модульной системы Regin является на данный момент самой сложной и изощренной вредоносной платформой, которую мы когда-либо изучали»[2].

Данную проблему затронул в своем докладе на прошедшем 8 июля 2015 г. в г. Вологде совещании, посвященном вопросам противодействия угрозам в информационной сфере, и Секретарь Совета Безопасности Российской Федерации Н.П. Патрушев: «...Специалисты отмечают заметное увеличение числа компьютерных атак на информационно-телекоммуникационные сети и информационные системы органов государственной власти. Отмечается наличие в информационных системах программных средств и иностранных технических разведок. Это требует совершенствования системы защиты информации»[3]. По его словам, фиксируются «...факты нарушения обязательных требований по защите служебной информации в органах государственной власти субъектов России и органах местного самоуправления». При этом, как указал Н.П. Патрушев, к наиболее распространенным видам нарушений относятся: под-

[1] Владимир Путин провел заседание Совета Безопасности, посвященное вопросам противодействия угрозам национальной безопасности в информационной сфере [Электронный ресурс]. - Режим доступа: http://kremlin.ru/events/president/news/46709.

[2] Атака под цифровым флагом. Regin и другие знаменитые вирусы [Электронный ресурс]. - Режим доступа: http://www.aif.ru/techno/web/1388672.

[3] Патрушев рассказал о внедрении разведками вирусов в информационные системы госвласти [Электронный ресурс]. - Режим доступа: http://vz.ru/news/2015/7/8/755034.print.html.

ключение официальных информационных систем государственных органов к интернету, а также использование в органах государственной власти информационных систем, не прошедших аттестацию по требованиям ФСТЭК.

О масштабах проблемы красноречиво свидетельствует и тот факт, что только в 2014 году Федеральной службой безопасности России было пресечено 74 миллиона кибератак на официальные сайты российских структур и государственных органов[1].

Вышеизложенное позволяет констатировать неуклонно возрастающий уровень опасности в сфере информационных технологий. По результатам опроса, проведенного специалистами Лаборатории Касперского, за последний год 96% отечественных компаний сталкивались с угрозами информационной безопасности[2]. Более того, более половины участников исследования отмечают ухудшение ситуации - возрастание количества кибератак, и лишь 8% констатируют снижение их количества.

Многие организации пострадали от киберпреступников: например, треть вирусных атак (а в российских компаниях - почти половина) закончилась потерей данных, при этом для 10% организаций это была важная для их деятельности информация.

Результаты проведенного исследования свидетельствуют о том, что наибольшую опасность для корпоративных информационных систем представляет вредоносное программное обеспечение (компьютерные вирусы, шпионское программы и др.). Второе место - спам, на третьем - фишинговые атаки. За ними идут сбои, вызванные проникновением в корпоративную сеть, и DDoS-атаки (рис. 1.2).

Результаты исследования показывают, что представители отечественных компаний хорошо осведомлены об уровне опасности, однако степень защищенности организаций от киберугроз оставляет желать лучшего: некоторые компании плохо защищены, в ряде организаций выбранные меры защиты не соответствуют характеру опасности и серьезности возможных последствий для их деятельности.

Самые популярные меры, применяемые для защиты от киберугроз в компаниях в мире и в России, - антивирусная защита, кли-

[1] Путин: ФСБ в 2014 году пресекла деятельность 209 агентов иностранных спецслужб [Электронный ресурс]. - Режим доступа: http://vz.ru/news/2015/3/26/736531.html.

[2] Киберугрозы и информационная безопасность в корпоративном секторе: тенденции в мире и в России [Электронный ресурс]. - Режим доступа: http://www.kaspersky.ru/downloads/pdf/kaspersky_global_it_security_risks_survey.pdf.

ентские межсетевые экраны, установка обновлений (в том числе и устраняющих уязвимости в программном обеспечении) и резервное копирование данных. Тем не менее, 31% компаний в России не полностью внедрили антивирусную защиту (для сравнения - в Великобритании и США антивирусная защита внедрена в 92% и 82% компаний соответственно). Одна российская компания из ста не имеет вообще никакой защиты (а в мире - 3% организаций).

Рис. 1.2. Основные угрозы информационной безопасности корпоративных информационных систем

Таким образом, следует констатировать, что риски, связанные с воздействием на корпоративные информационные системы различного рода вредоносного программного обеспечения, являются одной из наиболее актуальных угроз в сфере информационной безопасности, о чем со всей очевидностью свидетельствуют и данные статистики: ведущими разработчиками антивирусного программного обеспечения в 2014 году было заблокировано 6167233068 вредоносных атак на компьютеры и мобильные устройства пользователей, зафиксировано 123054503 совершенно уникальных вредоносных объектов, не встречавшихся ранее[1]. В России с веб-атаками

[1] Гарнаева М., Чебышев В., Макрушин Д., Унучек Р., Иванов А. Kaspersky Security Bulletin 2014. Основная статистика за 2014 год [Электронный ресурс]. - Режим доступа: https://securelist.ru/analysis/ksb/24580/kaspersky-security-bulletin-2014-osnovnaya-statistika-za-2014-god/ (дата обращения: 17.04.2015).

столкнулся каждый второй пользователь (53,7%)[1]. При этом большинством экспертов в сфере IT-технологий прогнозируется увеличение в течение ближайших нескольких лет числа атак на информационные системы, связанных с использованием вирусов, червей и других вредоносных программ.

Понимание той опасности, которую представляет вредоносное программное обеспечение, обусловило криминализацию в отечественном уголовном законодательстве деяний, связанных с созданием, распространением и использованием вредоносных компьютерных программ. Рассмотрим соответствующие положения Уголовного кодекса Российской Федерации подробнее.

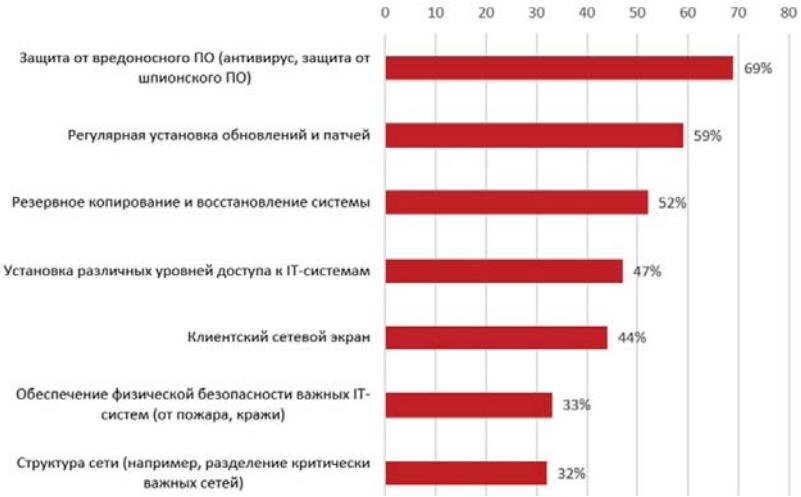

Рис. 1.3. Наиболее широко применяемые в России меры по обеспечению информационной безопасности

[1] Кривенцов П.А. Латентная преступность в России: криминологическое исследование: дисс. ... канд. юрид. наук. М., 2014.

2. ПОНЯТИЕ И ВИДЫ ВРЕДОНОСНЫХ ПРОГРАММ. ОТВЕТСТВЕННОСТЬ ЗА РАСПРОСТРАНЕНИЕ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Признавая ту опасность, которую несет создание и использование вредоносного программного обеспечения, в Уголовный кодекс Российской Федерации, вступивший в силу в 1997 году, была введена статья 273, предусматривающая ответственность за создание, использование и распространение вредоносных программ для ЭВМ.

Следует отметить, что появление в отечественном уголовном законодательстве данной статьи в полной мере отражало не только потребности практики по противодействию компьютерной преступности, но и зарубежный опыт борьбы с подобного рода угрозами[1].

Так, например, Уголовный кодекс Франции, вступивший в силу 1 марта 1993 года, содержит две статьи, касающиеся киберпреступлений: статья 186 и статья 323.

Статья 186-1 содержит положения об уголовной ответственности за неправомочный перехват данных в телекоммуникационных системах. Часть 1 статьи 323 предусматривает уголовную ответственность за неправомерный доступ к автоматизированной системе обработки данных или части этой системы, если в результате доступа были уничтожены или изменены данные, содержащиеся в системе, или нарушено, или изменено функционирование системы. Ответственность по данной статье может наступить за создание вредоносных программ, попытку вторжения в системы, незаконный доступ к данным, незаконный доступ к системам связи.

Уголовный кодекс Германии имеет множество различных статей, в соответствии с которыми можно привлечь к ответственности за компьютерные преступления, в том числе и статью 303, предусматривающую уголовную ответственность за совершение таких преступлений, как DNS-атаки (компьютерный саботаж) и создание вредоносных программ.

Ответственность за создание вредоносных программ и компьютерный саботаж предусмотрена статьями 523, 528, 559 УК Бельгии. Незаконная модификация компьютерной информации в преступных целях может преследоваться в зависимости от характера

[1] Быков В.М., Черкасов В.Н. Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы: монография. М.: Юрлитинформ, 2015.

преступления в соответствии со статьей 134 УК Бельгии (общие нормы о подлоге), статьей 461 (кража), статьей 496 (мошенничество).

По мере развития компьютерной техники и отечественного уголовного законодательства диспозиция статьи 273 УК РФ претерпевала незначительные изменения, пока Федеральным законом от 7 декабря 2011 г. № 420-ФЗ не были внесены изменения в текст статьи, сформировавшие ее в том виде, в котором она существует и в настоящий момент: «Создание, использование и распространение вредоносных компьютерных программ».

Часть 1 статьи 273 УК РФ предусматривает уголовную ответственность за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. Совершение указанных деяний наказываются ограничением свободы на срок до четырех лет либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

Те же деяния, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового (ч. 2 ст. 273 УК РФ).

В случае, если указанные выше деяния повлекли тяжкие последствия или создали угрозу их наступления, лица, их совершившие, могут быть лишены свободы на срок до семи лет (ч. 3 ст. 273 УК РФ).

Как можно заметить, в соответствии со ст. 15 УК РФ преступления, связанные с созданием и распространением вредоносных компьютерных программ, предусмотренные ч. 1 и ч. 2 ст. 273 УК РФ,

относятся к преступлениям средней тяжести, а предусмотренные ч. 3 ст. 273 УК РФ - к категории тяжких преступлений. И это представляется вполне закономерным. Использование передовых технологий в преступной деятельности, проявление сотен тысяч вредоносных объектов каждый день, а также низкий уровень образованности населения в сфере информационных технологий свидетельствует о том, что реальное количество таких преступлений многократно больше официально зарегистрированных. Таким образом, создание и распространение вредоносных компьютерных программ является серьезной угрозой для общественной безопасности и порядка.

В целях более полного уяснения сущности понятия «вредоносное программное обеспечение» представляется необходимым обратиться к рассмотрению основного понятийного аппарата, определяющего его содержание.

Одним из таких ключевых понятий является понятие компьютерной техники.

Здесь, прежде всего, необходимо отметить, что и в научной литературе, и в обиходе для обозначения подобного рода устройств используются два, весьма близких по содержанию, термина: «электронная вычислительная машина (ЭВМ)» и «компьютер». Несмотря на кажущуюся синонимичность, в содержании данных понятий есть определенные различия.

Как известно, в своем развитии средства вычислительной техники прошли долгий путь развития, в котором выделяют несколько этапов[1].

Первый этап - домеханический - характеризуется использованием для счета различных приспособлений, подручных средств, которые отличались простотой изготовления и помогали человеку облегчить выполнение некоторых арифметических операций.

Древнейшим счетным инструментом, который сама природа предоставила в распоряжение человека, была его собственная рука. Наши предки умели подсчитывать число членов своей семьи, количество принадлежащих им животных и вещей, отгибая пять пальцев каждой руки.

На смену пальцам пришли камешки (либо палочки), которые позднее помещались в контейнеры для удобства счета. Так в V веке до н.э. в Греции и Египте получил распространение абак. Происхождение слова «абак» доподлинно не установлено. Согласно одной из распространенных версий, оно означает «дощечка, покрытая пылью». Самый примитивный абак, действительно, представлял из

[1] Пригоров К.Ф. История развития ЭВМ. Концепции и этапы. М.: Лаборатория Книги, 2008.

себя такую дощечку. На ней острой палочкой проводили линии, и в получившихся колонках размещались камешки или палочки по позиционному принципу. Это значит, что были колонки единиц, десятков, сотен и так далее. До нашего времени дошел бронзовый римский абак, на котором камешки передвигались в вертикально прорезанных желобках. Внизу помещались камешки для счета до пяти, а в верхней части имелось отделение для камешка, соответствующего пятерке.

Подобные вычислительные инструменты распространялись и развивались по всему миру. Например, китайский вариант абака назывался суанпан, а японский - соробан. Потомком абака можно назвать и русские счеты, которые появились в стране на рубеже XVI-XVII веков и успешно использовались вплоть до конца прошлого века.

Второй этап - механический - начинается в далеком 1962 году, когда выдающимся французским ученым Блезом Паскалем была создана первая суммирующая машина, представляющая собой небольшой латунный ящик размером 36х13х8 см, содержащий внутри множество связанных между собой шестеренок и имеющий несколько наборных колесиков с делениями от 0 до 9, при помощи которых осуществлялось управление - ввод чисел для операций над ними и отображение результатов операций в окошках. В честь своего создателя машина получила название «Паскалина» или, как ее еще называют, «Паскалево колесо»[1].

Принцип связанных колес, заложенный Паскалем, почти на три столетия стал основой для создания последующих модификаций вычислительных устройств. В 1673 г. великий математик Готфрид Лейбниц, развив идею Паскаля, создал механический арифмометр, на котором можно было выполнять все четыре арифметические операции с многозначными числами.

Венцом развития вычислительной техники в рамках данного этапа считается проект разностной машины Чарльза Бэббиджа, который, несмотря на то, что так и не был реализован при жизни изобретателя, послужил основой для появления тех компьютеров, с которыми мы в настоящее время имеем дело каждый день. Именно Бэббиджу принадлежит идея о разработке полностью автоматической машины с программным управлением, то есть машины, которая могла бы работать по заранее заданной программе, без вмешательства человека.

Третий этапа - электронно-вычислительный - связан с бурным развитием радиоэлектроники в первой половине XX века. Ос-

[1] Частиков А.П. Архитекторы компьютерного мира. СПб: БВХ-Петербург, 2002.

новываясь на концептуальных идеях об устройстве вычислительной машины Чарльза Бэббиджа в 1946 году группой специалистов под руководством Джона Мочли и Преспера Экерта в США была сконструирована вычислительная машина на основе электронных ламп. Она получила название ENIAC *(сокр. от Electronical Numerical Integrator and Calculator - Электронный числовой интегратор и вычислитель)* и представляла собой первый электронный цифровой компьютер общего назначения, который можно было перепрограммировать для решения широкого спектра задач[1].

На смену электронным лампам пришли транзисторы, появились большие и сверхбольшие интегральные схемы. Это привело к появлению новых моделей, модификаций ЭВМ, которые, постепенно уменьшаясь в размерах, приобретали по своему функциональному назначению все более универсальный характер[2].

Знаковым событием стала разработка в 1976 году Стивом Джобсом и Стивом Возняком персонального компьютера Apple I - одного из первых подобного рода устройств, которое было рассчитано на широкий круг пользователей и продавалось в готовом виде, в отличие от аналогичных разработок, присутствовавших в то время на рынке. Востребованность данной идеи со стороны покупателей, а также то, что к производству персональных компьютеров подключились такие гиганты компьютерной индустрии, как фирма IBM, привели к тому, что компьютер из весьма сложного и специфичного устройства, доступного лишь ученым и большим корпорациям, превратился в необходимый элемент жизни каждого человека.

Таким образом, можно сделать вывод, что с содержательной точки зрения под компьютером *(от англ. computer - «вычислитель»)* в широком смысле можно понимать любое устройство или систему, способные производить вычисления[3]. Он охватывает все виды вычислительных машин от аналоговых до цифровых. Электронная вычислительная машина (ЭВМ) - это лишь один из способов реализации компьютера. Это машина, построенная с использованием в качестве функциональных элементов электронных устройств вместо механических. Данный термин употреблялся, в основном, для отличия ЭВМ от исторического предшественника - механической вычислительной машины.

---

[1] Баин А.М. История развития компьютерной техники: учебное пособие. М.: МИЭТ, 2013.
[2] Конев Ф.Б. История развития компьютерной техники и информационных технологий: учебное пособие. М.: Изд-во МГОУ, 2010.
[3] Сало И.А. О понятии «ЭВМ» применительно к статье 272 УК РФ // Криминалистъ. 2011. № 8. С. 34-37.

Таким образом, под компьютером следует понимать не только электронно-вычислительную машину, но и спецвычислитель или вообще техническое устройство, способное выполнять действия по хранению, записи, обработке, воспроизведению или передаче информации.

Однако в настоящее время появилось достаточно много новых электронных устройств, которые достаточно далеки от нашего традиционного представления о средствах компьютерной техники. Это различного рода смартфоны, планшеты, электронные книги и т.д. В этой связи полагаем, что современный компьютер необходимо рассматривать как комплекс аппаратно-программных средств, включающий[1]:

• процессор (или другое электронное устройство), выполняющий функции преобразования информации, представленной в машинном виде, и реализующий одно или несколько действий (программу) по обработке информации;

• устройство хранения управляющих программ и(или) данных, необходимых для реализации процессором его целевых функций;

• оборудование (приспособление), позволяющее каким-либо образом изменять или перезаписывать управляющие программы и(или) данные, необходимые для реализации процессором его целевых функций;

• совокупность программных средств, используемых для управления функционированием вычислительного устройства.

Таким образом, средства компьютерной техники - это комплексное понятие, описывающее весь спектр производимых компьютерных систем, от небольшого наладонника до сверхмощного суперкомпьютера. При этом понятие компьютерной техники вбирает в себя не только аппаратное, но также и программное обеспечение, устанавливаемых на данных типах устройств, обеспечивающее поддержку выполнения их базовых функций. Практически, сами устройства и работающие на них программы рассматриваются в рамках него, как составляющие единого аппаратно-программного комплекса.

В действующем законодательстве под программой для ЭВМ понимается «...представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в

[1] Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: автореф. ... д-ра юрид. наук. Воронеж, 2001. С. 16.

ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения» (с. 1261 Гражданского кодекса Российской Федерации).

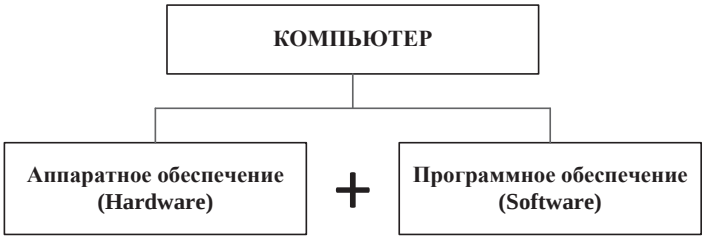

Рис. 2.1. Компьютер как аппаратно-программный комплекс

Совокупность установленных на компьютере программ и необходимых для ее эксплуатации документов составляют программное обеспечение компьютера[1], которое условно делится на две большие группы: системное (предназначенное для обеспечения работоспособности компьютера) и прикладное (предназначенное для решения конкретных задач).

Если пользователю требуется выполнить какую-то работу на компьютере, то он должен выбрать подходящую для этих целей программу и инициализировать ее выполнение. Таким образом, программное обеспечение компьютера является средством решения различных задач пользователя. Здесь термин «задача» понимается в самом широком смысле и обозначает любую информационную потребность пользователя, которую можно удовлетворить с помощью компьютера: создать текстовый документ, нарисовать иллюстрацию, выполнить вычисления, получить справку, принять и отправить электронную почту и т.д.

Очевидно, что, исходя даже из названия, вредоносные программы имеют совершенно иное назначение - не только затруднить, но и сделать невозможной работу пользователя за компьютером, нанести ему вред.

Следует отметить, что в настоящее время единого подхода к определению содержания понятия «вредоносная программа» в теории и практике не сложилось.

Так, в информатике можно считать общепризнанным следующее определение вредоносной программы: это любое программное обеспечение, предназначенное для получения несанкциони-

[1] Технология разработки программного обеспечения / Л.Г. Гагарина и др. М.: Форум, 2013. С. 27.

рованного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранящейся на ЭВМ, с целью несанкционированного владельцем использования ресурсов ЭВМ или причинения вреда (нанесения ущерба) владельцу информации, и(или) владельцу ЭВМ, и(или) владельцу сети ЭВМ, путем копирования, искажения, удаления или подмены информации[1].

Весьма схожее определение вредоносной программы содержится и в Национальном стандарте Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»: «Вредоносная программа: программа, предназначенная для осуществления несанкционированного доступа к информации и(или) воздействия на информацию или ресурсы информационной системы»[2].

В Национальном стандарте РФ ГОСТ Р ИСО/МЭК 27033-1-2011 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции» под вредоносной программой понимается «...вредоносное программное средство, специально разработанное для повреждения или разрушения системы посредством нарушения ее конфиденциальности, целостности и(или) доступности»[3].

Корпорация Microsoft трактует термин «вредоносная программа» следующим образом: «Вредоносная программа *(malware)* - обычно используемое как общепринятый термин для обозначения любого программного обеспечения, специально созданного для того, чтобы причинять ущерб отдельному компьютеру, серверу, или компьютерной сети, независимо от того, является ли оно вирусом, шпионской программой и т.д.»[4].

Исследуя данный вопрос, П.Б. Хорев пришел к выводу, что вредоносная программа - это некоторая самостоятельная програм-

---

[1] Вредоносная программа [Электронный ресурс]. - Режим доступа: http://ru.wikipedia.org/wiki/.

[2] Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»: приказ Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст. [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[3] Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27033-1-2011 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 1 декабря 2011 г. № 683-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[4] Вредоносное программное обеспечение [Электронный ресурс]. - Режим доступа: http://dic.academic.ru/dic.nsf/ruwiki/853615.

ма (набор инструкций), которая способна выполнять любое непустое подмножество функций[1]:

1) скрыть признаки своего присутствия в программной среде компьютера;

2) обладать способностью к самодублированию, ассоциированию себя с другими программами и(или) переносу своих фрагментов в иные области оперативной или внешней памяти;

3) разрушать (искажать произвольным образом) код программ в оперативной памяти;

4) выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирование, блокирование, уничтожение и проч.);

5) сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);

6) искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

Е.А. Маслакова говорит о вредоносной компьютерной программе как о специально созданной или модифицированной компьютерной программе, способной совершать действия, приводящие к несанкционированному собственником информационной системы уничтожению, блокированию, модификации либо копированию информации, хранящейся в компьютере, компьютерной системе, сети или на машинных носителях[2].

Автор акцентирует внимание на том, что вредоносная программа должна выполнять операции автономно, без санкционирования и(или) уведомления собственника компьютера, когда такие операции могут нанести вред последнему, тем самым дополняя положение ст. 273 УК РФ: добросовестный пользователь компьютера не может влиять на функционирование таких программ, что и определяет их как вредоносных. Однако, как правильно замечает М.М. Менжега, несанкционированными могут быть действия многих легальных программ, потому как запрос программами санкци-

[1] Хорев П.Б. Программно-аппаратная защита информации: учебное пособие. - 2-е изд., испр. и доп. М.: Форум, 2015. С. 79-80.

[2] Маслакова Е.А. Анализ объективной стороны преступления, связанного с незаконным оборотом вредоносных компьютерных программ // Известия Тульского государственного университета. Экономические и юридические науки. 2008. № 1. С. 228.

онирования на выполнение каждой операции существенно затруднил бы работу пользователя с компьютером[1].

Подводя итог сказанному, представляется согласиться с мнением В.М. Быкова и В.Н. Черкасова, согласно которому, для того, чтобы программа считалась вредоносной, она должна соответствовать следующим трем критериям[2]:

1. Уничтожение информации или нарушение работы всей системы. Однако осуществление лицом только взлома защиты от копирования еще нельзя оценивать как создание вредоносной программы.

2. Несанкционированная работа. Программа же форматирования диска, входящая в комплект любой ОС, сама по себе еще не является вредоносной, так как ее запуск санкционируется пользователем.

3. Заведомая вредоносность программы. Явной целью ее создания является несанкционированное уничтожение информации. Программы, содержащие в себе различные ошибки, могут быть оценены как нарушение прав потребителей или как преступная халатность, но не как создание вредоносной программы.

Более четкие критерии, по которым программные продукты (модули) могут быть отнесены к категории вредоносных программ, до настоящего времени нигде четко не оговорены. Для того, чтобы утверждение о вредоносности программы было обоснованным и имело бы юридические последствия, необходимо проведение программно-технической экспертизы.

По мере нарастания темпов развития компьютерных технологий каждый год появляются тысячи новейших вредоносных программ, не имевших аналогов ранее либо коренным образом изменившихся. Но у значительного большинства таких программ в сущности можно выделить нечто общее, объединяющее их в определенный вид.

Одно из мнений таково, что производить классификацию вредоносных компьютерных программ следует по способу их действия. Так, Н.Г. Шурухнов предлагает распределять вредоносные программы на резидентные (или те, которые при заражении компьютера оставляют в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к

---

[1] Менжега М.М. Методика расследования создания и использования вредоносных программ для ЭВМ. М.: Юрлитинформ, 2009. С. 49.

[2] Быков В.М., Черкасов В.Н. Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы: монография. М.: Юрлитинформ, 2015. С. 163.

объектам заражения (файлам, загрузочным секторам дисков и т.п.) и внедряется в них) и на нерезидентные (которые не заражают память компьютера и являются активными только во время их непосредственной работы)[1].

Н.Н. Федотов, в свою очередь, распределяет вредоносные программы с позиции их предназначения: троянские программы (для создания сетей, которые используются при рассылке спама, DoS-атак, организации фишерских сайтов), черви и троянцы (для похищения персональных данных), вредоносные программы, скрытно внедряющиеся на персональный компьютер (показывающие пользователю несанкционированную рекламу), руткиты, логические бомбы (предназначенные для автоматического уничтожения всей чувствительной информации на компьютере) и «ransomware» (подвид троянских программ, которые после скрытного внедрения на компьютер жертвы шифруют файлы, содержащие пользовательскую информацию, после чего предъявляют требования об уплате выкупа за возможность восстановления файлов пользователя)[2].

В.Ф. Шаньгин разделяет вредоносные программы в соответствии со способами распространения и вредоносной нагрузки на четыре основных типа: компьютерные вирусы, черви, трояны и другие программы[3]. Данная классификация типична и встречается у множества авторов, таких как М.М. Менжега, В.И. Ярочкин, В.Б. Вехов, В.А. Мазуров и другие.

ЗАО «Лаборатория Касперского», крупнейший отечественный разработчик систем защиты от киберугроз, входящий в четверку ведущих мировых производителей антивирусного программного обеспечения[4], из года в год анализирует новейшие виды компьютерных угроз. На основании полученных данных Лабораторией разработана собственная классификация вредоносных компьютерных программ.

Условно специалисты Лаборатории Касперского подразделяют вредоносные программы на следующие основные группы:

- компьютерные вирусы;
- черви;

[1] Криминалистика: учебное пособие / Шурухнов Н.Г. М.: Эксмо, 2009. С. 332.
[2] Федотов Н.Н. Форензика - компьютерная криминалистика. М.: OneBook.ru, 2012. С. 68.
[3] Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. М.: Форум, 2012. С. 502.
[4] Кашин С. Вирусные нолики // Коммерсантъ. Секрет Фирмы. 2013. № 10. С. 74.

• трояны;

• другие вредоносные программы.

Компьютерные вирусы. Компьютерный вирус - это своеобразное явление, возникшее в процессе развития компьютерной техники и информационных технологий. Термин «компьютерный вирус» впервые употребил сотрудник Университета Южной Калифорнии Фред Коэн в 1984 г. на 7-й конференции по безопасности информации, проходившей в США. Этим термином был назван вредоносный фрагмент программного кода: «Компьютерный вирус - это программа, которая может заражать другие программы, модифицируя их посредством включения в них своей, возможно измененной копии, причем последняя сохраняет способность к дальнейшему размножению». Ключевыми понятиями в этом определении являются способность вируса к саморазмножению и способность к модификации вычислительного процесса. Указанные свойства компьютерного вируса аналогичны паразитированию биологического вируса в живой природе. С тех пор острота проблемы вирусов многократно возросла - к концу XX в. в мире насчитывалось более 14300 модификаций вирусов.

В настоящее время компьютерным вирусом принято называть программу, способную создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия (Государственный стандарт РФ ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство»).

Жизненный цикл любого компьютерного вируса можно разделить на четыре этапа:

• проникновение на чужой компьютер;

• активация;

• поиск объектов для заражения;

• подготовка и внедрение копий.

Путями проникновения вируса могут служить как мобильные носители, так и сетевые соединения фактически всех каналов, по которым можно скопировать файл. Однако, в отличие от червей, вирусы не используют сетевые ресурсы. Заражение вирусом возможно, только если пользователь сам каким-либо образом его активировал, например скопировал или получил по почте зараженный файл и сам его запустил или просто открыл.

После проникновения следует активация вируса. Это может происходить разными путями, и в зависимости от выбранного метода вирусы делятся на такие виды:

- *загрузочные вирусы* заражают загрузочные сектора жестких дисков и мобильных носителей;

- *файловые вирусы* заражают файлы.

Дополнительным признаком отличия вирусов от других вредоносных программ служит их привязанность к операционной системе или программной оболочке, для которой каждый конкретный вирус был написан. Так, вирус для Microsoft Windows не будет работать и заражать файлы на компьютере с другой установленной операционной системой, например UNIX.

При подготовке своих копий вирусы могут применять для маскировки разные технологии:

- шифрование - в этом случае вирус состоит из двух частей: сам вирус и шифратор;

- метаморфизм - при применении этого метода вирусные копии создаются путем замены некоторых команд на аналогичные, перестановки местами частей кода, вставки между ними дополнительных, обычно ничего не делающих команд.

Соответственно, в зависимости от используемых методов маскировки вирусы можно делить на шифрованные, метаморфные и полиморфные, использующие комбинацию двух типов маскировки.

Сетевые черви. В отличие от вирусов, сетевые черви - это вполне самостоятельные вредоносные программы. Главной их особенностью также является способность к саморазмножению, однако при этом они способны к самостоятельному распространению с использованием сетевых каналов.

В зависимости от способа проникновения в систему черви делятся на следующие типы:

• *сетевые черви* - используют для распространения локальные сети и Интернет;

• *почтовые черви* - распространяются с помощью почтовых программ;

• *IM-черви* - используют программы обмена сообщениями IM (Instant Messenger) в режиме реального времени;

• *IRC-черви* - распространяются через чаты IRC (Internet Relay Chat);

• *P2P-черви* - распространяются при помощи пиринговых файлообменных сетей P2P (Peer-to-Peer - равный с равным).

После проникновения на компьютер червь должен активироваться - иными словами, запуститься. По методу активации все черви можно разделить на две большие группы: на тех, которые требуют активного участия пользователя, и тех, кто его не требует.

Отличительная особенность червей из первой группы - это использование обманных методов. Например, получатель инфицированного файла вводится в заблуждение текстом полученного письма и добровольно открывает вложение с почтовым червем, тем самым его активируя. Черви из второй группы используют ошибки в настройке или бреши в системе безопасности операционной системы. В последнее время наметилась тенденция к совмещению этих двух технологий. Такие черви наиболее опасны и часто вызывают глобальные эпидемии.

Сетевые черви могут кооперироваться с вирусами - такая пара способна самостоятельно распространяться по сети (благодаря червю) и в то же время заражать ресурсы компьютера (функции вируса).

Троянские программы. Троянская программа (программа класса «троянский конь» или просто троян) имеет только одно назначение - нанести ущерб целевому компьютеру путем выполнения не санкционированных пользователем действий: кражи, порчи или удаления конфиденциальных данных, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях.

В отличие от вирусов и червей, трояны сами не размножаются. Жизненный цикл троянов состоит всего из трех этапов:

- проникновение в систему;
- активация;
- выполнение вредоносных действий.

Некоторые трояны способны к самостоятельному преодолению систем защиты компьютерной системы с целью проникновения в нее. В этом случае обычно применяется маскировка, когда троян выдает себя за полезное приложение, которое пользователь самостоятельно копирует себе на диск (например, загружает из Интернета) и запускает. При этом программа действительно может быть полезна, но наряду с основными функциями она может выполнять действия, свойственные трояну.

Однако в большинстве случаев трояны проникают на компьютеры вместе с вирусом либо червем, то есть такие трояны можно рассматривать как дополнительную вредоносную нагрузку, но не как самостоятельную программу.

После проникновения на компьютер трояну необходима активация, и здесь он похож на червя: либо требует активных действий от пользователя, либо через уязвимости в программном обеспечении самостоятельно заражает систему.

Поскольку цель троянов - это выполнение несанкционированных действий, они классифицируются по типу вредоносной нагрузки:

• *похитители паролей* предназначены для кражи паролей путем поиска на зараженном компьютере специальных файлов, которые их содержат;

• *утилиты скрытого удаленного управления* - это трояны, которые обеспечивают несанкционированный удаленный контроль над инфицированным компьютером. Обычно это возможность скрыто загружать, отсылать, запускать или уничтожать файлы. Такие трояны могут быть использованы как для получения конфиденциальной информации, так и для запуска вирусов, уничтожения данных;

• *логические бомбы* характеризуются способностью при срабатывании заложенных в них условий (в конкретный день, время суток, в ответ на определенное действие пользователя или команды извне) выполнять какое-либо действие, например, удаление файлов;

• *клавиатурные шпионы*, постоянно находясь в оперативной памяти, записывают все данные, поступающие от клавиатуры, с целью последующей их передачи своему автору;

• *анонимные SMTP- и прокси-серверы* - такие трояны на зараженном компьютере организуют несанкционированную отправку электронной почты, что часто используется для рассылки спама;

• *утилиты дозвона* в скрытом от пользователя режиме инициируют подключение к платным сервисам Интернета;

• *модификаторы настроек браузера* меняют стартовую страницу в браузере, страницу поиска или еще какие-либо настройки, открывают дополнительные окна, имитируют нажатия на рекламные баннеры и т.п.

Отдельно отметим, что существуют программы из класса троянов, которые наносят вред другим, удаленным компьютерам и сетям, при этом не нарушая работоспособности инфицированного компьютера. Яркие представители этой группы - организаторы DDoS-атак.

Другие вредоносные программы и нежелательная корреспонденция. Кроме вирусов, червей и троянов существует еще много других вредоносных программ и нежелательной корреспонденции. Среди них можно выделить следующие группы:

• *шпионское ПО (Spyware)* - опасные для пользователя программы, предназначенные для слежения за системой и отсылки собранной информации третьей стороне - создателю или заказчику такой программы. Среди заказчиков шпионского ПО спамеры, маркетинговые агентства, преступные группировки. Шпионские программы интересуются системными данными, типом браузера, посещаемыми веб-узлами, иногда и содержимым файлов на жестком диске компьютера-жертвы. Такие программы тайно закачива-

ются на компьютер вместе с каким-нибудь бесплатным софтом или при просмотре определенным образом сконструированных HTML-страниц и всплывающих рекламных окон и самоустанавливаются без информирования об этом пользователя. Побочные эффекты от присутствия шпионского ПО на компьютер - нестабильная работа браузера и замедление производительности системы;

• *условно опасные программы*, о которых нельзя однозначно сказать, что они вредоносны. Такие программы обычно становятся опасными только при определенных условиях или действиях пользователя. К ним относятся:

- *апплеты (applet)* - прикладные программы, небольшие Java-приложения, встраиваемые в HTML-страницы. По своей сути эти программы не вредоносные, но могут использоваться в злонамеренных целях. Особенно апплеты опасны для любителей онлайновых игр, так как в них апплеты Java требуются обязательно. Апплеты, как и шпионское ПО, могут использоваться для отправки собранной на компьютере информации третьей стороне;

- *рекламные утилиты (adware)* - условно-бесплатные программы, которые в качестве платы за свое использование демонстрируют пользователю рекламу, чаще всего в виде графических баннеров. После официальной оплаты и регистрации обычно показ рекламы заканчивается и программы начинают работать в обычном режиме. Проблема рекламных утилит кроется в механизмах, которые используются для загрузки рекламы на компьютер. Кроме того, что для этих целей часто используются программы сторонних и не всегда проверенных производителей, даже после регистрации такие модули могут автоматически не удаляться и продолжать свою работу и скрытом режиме;

- *riskware* - вполне легальные программы, которые сами по себе неопасны, но обладают функционалом, позволяющим злоумышленнику использовать их с вредоносными целями. К riskware относятся обычные утилиты удаленного управления, которыми часто пользуются администраторы больших сетей, клиенты IRC, программы для загрузки файлов из Интернета, утилиты восстановления забытых паролей и др.;

• *хакерские утилиты* - к этому виду программ относятся программы сокрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов), автоматизации создания сетевых червей, компьютерных вирусов и троянских программ (конструкторы вирусов), наборы программ, которые используют хакеры для скрытного взятия под контроль взломанной системы (RootKit), и другие подобные утилиты. Такие специфические программы обычно используют только хакеры;

• *мистификации* - программы, которые намеренно вводят пользователя в заблуждение путем показа уведомлений, например, о форматировании диска или обнаружении вирусов, хотя на самом деле ничего не происходит. Текст таких сообщений зависит от фантазии автора программы;

• *спам* - нежелательная почтовая корреспонденция рекламного характера, загружающая трафик и отнимающая время у пользователей.

ВИДЫ ВРЕДОНОСНЫХ ПРОГРАММ

Компьютерный вирус – программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия

Червь – программа, распространяющая свои копии по локальным и/или глобальным сетям с целью: проникновения на удаленные компьютеры; запуска своей копии на удаленном компьютере; дальнейшего распространения на другие компьютеры в сети.

Троянская программа – программа, кажущаяся полезной или безвредной, но содержащая скрытый код, предназначенный для использования уязвимости или нанесения ущерба компьютеру, на котором эта программа выполняется.

Другие вредоносные программы и нежелательная корреспонденция:
– *шпионское ПО (Spyware)* – опасные для пользователя программы, предназначенные для слежения за системой и отсылки собранной информации третьей стороне – создателю или заказчику такой программы;
– *условно опасные программы* – это программы, в том числе и легально разработанные, которые в определенных случаях могут представлять особую опасность для пользователей компьютеров (действуя так же, как шпионское программное обеспечение);
– *хакерские утилиты* – к этому виду программ относятся программы сокрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов), наборы программ, которые используют хакеры для скрытного взятия под контроль взломанной системы (RootKit), и другие подобные утилиты;
– *мистификации* – программы, которые намеренно вводят пользователя в заблуждение путем показа уведомлений, например, о форматировании диска или обнаружении вирусов, хотя на самом деле ничего не происходит;
– *спам* – нежелательная почтовая корреспонденция рекламного характера, загружающая трафик и отнимающая время у пользователей.

Рис. 2.2. Виды вредоносных программ

По оценкам экспертов[1], среди источников проникновения вредоносных программ на компьютер наиболее опасными являются:

- Интернет;
- электронная почта;
- уязвимости в программном обеспечении;
- внешние носители информации;
- пользователи.

Интернет.

Глобальная информационная сеть является основным источником распространения любого рода вредоносных программ. Достаточно сказать, что лишь в 2014 году решениями «Лаборатории Касперского» было отражено 1432660467 атак, проводившихся с интернет-ресурсов, размещенных в разных странах мира.

При использовании сети Интернет зловредное программное обеспечение может попасть на компьютер при следующих действиях пользователя:

- При посещении сайта, содержащего зловредный код. Примером могут являться drive-by атаки, которые осуществляются в два этапа. Сначала пользователя заманивают на сайт, содержащий код, который перенаправляет запрос на сторонний сервер, на котором хранится эксплойт (программа, использующая уязвимости в программном обеспечении и применяемая для проведения атаки на вычислительную систему). Как только операционная система жертвы определена, начинает действовать/активируется соответствующий эксплойт из набора. В случае успешной атаки на компьютере незаметно для пользователя устанавливается троянская программа, что предоставляет злоумышленникам полный контроль над зараженным компьютером.
- При скачивании с сайтов зловредного программного обеспечения, маскирующегося под кейгены, крэки, патчи и т.д.
- При скачивании через peer-to-peer сеть (например, торренты).

Электронная почта.

Почтовые сообщения, поступающие в почтовый ящик пользователя и хранящиеся в почтовых базах, могут содержать в себе вирусы. Вредоносные программы могут находиться как во вложении письма, так и в его теле. При открытии письма, при сохранении на диск вложенного в письмо файла вы можете заразить данные на компьютере. Также почтовая корреспонденция может стать источником еще двух угроз: спама и фишинга. Если спам влечет за со-

[1] Лаборатория Касперского. О вирусах: Основные источники проникновения угроз на компьютер [Электронный ресурс]. - Режим доступа: http://support.kaspersky.ru/ viruses#block2.

бой в основном потерю времени, то целью фишинг-писем является конфиденциальная информация пользователя компьютера.

Уязвимости в программном обеспечении.

Так называемые «дыры» (эксплойты) в программном обеспечении являются основным источником хакерских атак. Уязвимости позволяют получить хакеру удаленный доступ к компьютеру, а, следовательно, к хранящимся на нем данным, к ресурсам локальной сети, к другим источникам информации.

Внешние носители информации.

В настоящее время для передачи информации по-прежнему широко используются съемные диски, карты расширения памяти (флеш), а также сетевые папки. Запуская какой-либо файл, расположенный на внешнем носителе, можно заразить вирусом хранящиеся на компьютере данные, распространить вирус на другие диски компьютера, сети.

Пользователи.

Нередко сами пользователи сами устанавливают безобидные на первый взгляд программы, заражая таким образом свой компьютер. Этот метод называется социальной инженерией. С помощью него создатели вредоносных программ могут убедить излишне доверчивого пользователя запустить инфицированный файл или открыть ссылку на зараженный веб-сайт. Такие методы используются во многих почтовых червях, а также других типах вредоносных программ.

В качестве примера можно привести червь LoveLetter, который в 2000 году вызвал перегрузку почтовых серверов многих компаний. Пользователи получили по электронной почте сообщение с приглашением открыть вложенное любовное письмо. Когда они открывали вложенный файл, червь рассылал себя по всем контактам из адресной книги жертвы. Этот червь до сих пор считается одним из самых разрушительных с точки зрения нанесенного им финансового ущерба.

Таким образом, несложно заметить, что наибольшие риски, с точки зрения обеспечения информационной безопасности корпоративных систем, несет в себе онлайн активность сотрудников. Ее наиболее опасные виды в рассматриваемом контексте приведены в таблице 2 .

Таблица 2

Наиболее опасные виды онлайн-активности сотрудников с точки зрения информационной безопасности

Вид активности/ Приложение	В целом	США	Россия	Китай
Общий доступ к файлам/P2P	55%	62%	50%	44%
Социальные сети	35%	44%	52%	26%
Загрузка файлов, передача файлов, FTP-сервисы	34%	33%	44%	28%
Доступ к веб-сайтам	32%	35%	42%	29%
Личная электронная почта/веб-почта	31%	36%	22%	28%
Службы мгновенного обмена сообщениями	23%	20%	19%	36%
Онлайн-игры	21%	19%	16%	21%
Потоковое видео/ Интернет-ТВ	13%	8%	12%	21%
Сетевой подход в маркетинге	11%	5%	4%	24%
Голосовая связь по IP-протоколу (VoIP)	10%	5%	9%	17%

Противодействие угрозам воздействия на компьютерные системы вредоносного программного обеспечения подразумевает принятие целого комплекса мер организационного, технического и программного характера. Однако основой построения подобного рода системы обеспечения антивирусной безопасности выступают различные правовые нормы, определяющие состав этой системы и предъявляемые к ней требования.

3. ПРАВОВЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ АНТИВИРУСНОЙ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ МВД РОССИИ

Одной из важнейших составляющих деятельности по защите компьютерной информации является деятельность уполномоченных органов власти и управления по формированию, применению и охране социальных норм регулирования общественных отношений, которые позволяют противодействовать угрозам в информационной сфере.

Выделяются два основных типа норм: технические и социальные.

Технические нормы определяют порядок взаимодействия человека с окружающей средой, осуществления деятельности по созданию материальных благ, пользованию орудиями труда, и, в частности, использования средств и систем информатизации, телекоммуникации и связи. Современную систему технических норм составляют правила использования современных информационных технологий, правила защиты информации и информационных систем от несанкционированного доступа, правила пользования средствами автоматизации управления и обработки информации. Следование этим правилам способствует более производительной и эффективной работе, предупреждает нанесение ущерба таким объектам национальных интересов, как информация и информационно-телекоммуникационные системы, а также производственный травматизм и профессиональные заболевания.

Социальные нормы регулируют поведение индивидов и подразделяются на поддерживаемые силами социальной общности без участия государства и поддерживаемые с использованием государственного принуждения. Первые включают прежде всего мораль, обычаи и традиции, корпоративные и религиозные нормы.

Важной составляющей социального регулирования деятельности по обеспечению защиты компьютерной информации является правовое регулирование общественных отношений, связанных с противодействием угрозам безопасности компьютерной информации, которое заключается в установлении определенных правовых норм, их применении и охране норм от нарушения с использованием государственного принуждения. Правовое регулирование отношений в целях обеспечения безопасности компьютерной информации осуществляется в рамках правовой деятельности государства, в структуре которой выделяются: законодательная (правотворческая), правоприменительная и судебная деятельность.

Законодательная деятельность заключается в подготовке, принятии и издании законодательными органами нормативных правовых актов, регулирующих отношения в области удовлетворения национальных интересов в информационной сфере, а также создающих условия для предотвращения реализации угроз информационной безопасности или минимизации их воздействия на защищаемые общественные отношения. Эта деятельность направлена на создание правовой основы выполнения государственными органами задач по противодействию угрозам, установление таких правил реализации общественных отношений в рассматриваемой области, при которых ни внешние, ни внутренние угрозы не оказывают на эти отношения существенного негативного воздействия. Совокупность нормативных правовых актов, являющихся источниками права в данной сфере, составляют основу законодательства в области обеспечения информационной безопасности. Оно призвано реализовать социальное назначение права в достижении целей противодействия угрозам безопасности объектов национальных интересов в информационной сфере.

Правоприменительная деятельность представляет собой основанное на законодательстве оперативное, повседневное выполнение органами исполнительной власти (государственного управления) возложенных на них функций в области обеспечения информационной безопасности. Эта деятельность заключается в следующем:

• подготовка, принятие и исполнение решений органов исполнительной власти по осуществлению конкретных мероприятий по противодействию угрозам информационной безопасности;

• координация деятельности органов в системе исполнительной власти в процессе подготовки и реализации конкретных мероприятий;

• организационные, регистрационные и иные формы осуществления правоприменительной практики в рассматриваемой области;

• консультативная и информационная деятельность органов исполнительной власти, направленная на создание условий для эффективного выполнения возложенных на эти органы задач;

• учетные, аналитические, прогнозные и программные формы работы, являющиеся, на наш взгляд, разновидностью информационной деятельности, административные договоры;

• взаимодействие органов исполнительной власти с органами других ветвей государственной власти в целях согласования усилий по противодействию угрозам;

• информационное обеспечение деятельности субъектов противодействия угрозам информационной безопасности в системе исполнительной власти;

• государственный контроль за законностью деятельности субъектов правового регулирования в рассматриваемой области.

Судебная деятельность охватывает реализацию функции государства по обеспечению правосудия в процессе выполнения задач противодействия угрозам безопасности информации. Эта деятельность является неотъемлемой составляющей обеспечения информационной безопасности, так как позволяет каждому реализовать свое конституционное право на объективное рассмотрение всех обстоятельств, связанных с применением к нему мер государственного принуждения.

Как известно, обеспечение защиты компьютерной информации осуществляется посредством целой совокупности правовых, организационных и технических средств. Правовые средства по существу являются центральным элементом обеспечения безопасности компьютерной информации, поскольку в определяющей степени именно они регламентируют возможность применения других средств защиты, как технических, так и организационных.

Правовую основу защиты информации в корпоративных информационных системах, в том числе и в информационных системах МВД России, составляют положения действующего законодательства Российской Федерации, а также рекомендации международных стандартов. Основные требования российского законодательства, касающегося вопросов защиты компьютерной информации, изложены в общем виде в федеральных законах и уточнены в документах Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности, государственных стандартах, а также других документах.

Международные стандарты позволяют дополнить отечественное законодательство в тех областях, которые не затрагиваются российскими нормативно-правовыми документами. Примерами таких областей является аудит информационной безопасности, интеграция различных средств обеспечения безопасности, управление системами защиты и др. В настоящее время наибольшее распространение в России получили следующие международные стандарты:

ISO/IEC 17799 - международный стандарт, включающий в себя передовой опыт в области информационной безопасности. Первоначально он был разработан в ответ на требование со стороны промышленности по созданию общей структуры, позволяющей

фирмам разрабатывать, внедрять и измерять эффективную практику управления безопасностью и обеспечивать доверие к торговле между фирмами. По своей сути он является сводом правил для качественного управления информационной безопасностью. Данный стандарт может применяться ко всей информации независимо от вида носителей, на которых она хранится и передается, или места ее размещения.

CobiT - подход к управлению информационными технологиями, созданный Ассоциацией контроля и аудита систем (Information Systems Audit and Control Association - ISACA) и Институтом руководства ИТ (IT Governance Institute - ITGI) в 1992 году. Он предоставляет менеджерам, аудиторам и ИТ пользователям набор утвержденных метрик, процессов и лучших практик с целью помочь им в извлечении максимальной выгоды от использования информационных технологий и для разработки соответствующего руководства и контроля ИТ в компании. По своему содержанию COBIT является синтезом четырех десятков международных стандартов в области управления ИТ, аудита, контроля и информационной безопасности. Его основной стратегической задачей является ликвидация разрыва между руководством организации с их видением бизнес целей и ИТ департаментом, осуществляющим поддержку информационной инфраструктуры.

ITIL (Information Technology Infrastructure Library) - библиотека наиболее эффективных методов организации и управления для компаний, ведущих свою деятельность в области информационных технологий, а также для компаний, организаций и учреждений, желающих построить эффективный процесс управления и взаимодействия как внутри компании, так и с внешними поставщиками и потребителями ее услуг. Она содержит обобщенное описание удачных управленческих решений, лучших из применяемых на практике способов организации работы IT-подразделений разных предприятий или обособленных IT компаний по всему миру, предоставляющих услуги в области информационных технологий. ITIL, по сути, представляет собой набор публикаций, содержащих рекомендации по предоставлению качественных услуг, а также процессов и компонентов, необходимых для их поддержки. Основная цель ITIL - продвижение современных знаний и обмен опытом в области.

OCTAVE - методология оценки критичных угроз, активов и уязвимостей (Operationally Critical Threat, Asset, and Vulnerability Evaluation), разработанная в Институте программной инженерии при Университете Карнеги-Меллона (США). Данный метод предусматривает активное вовлечение владельцев информации в процесс

определения критичных информационных активов и ассоциированных с ними рисков[1].

Ключевые элементы OCTAVE:

• идентификация критичных информационных активов;

• идентификация угроз для критичных информационных активов;

• определение уязвимостей, ассоциированных с критичными информационными активами;

• оценка рисков, связанных с критичными информационными активами.

OCTAVE предусматривает высокую степень гибкости, достигаемую путем выбора критериев, которые предприятие может использовать при адаптации методологии под собственные нужды.

В отличие от положений российского законодательства, требования международных стандартов носят рекомендательный характер.

Условно всю совокупность правовых актов по рассматриваемой проблематике можно разделить на три основные группы:

1) законодательные акты, указы и распоряжения Президента России, постановления Правительства Российской Федерации;

2) ведомственные правовые акты в области защиты компьютерной информации, а также российские и международные стандарты;

3) локальные правовые акты, действующие в конкретной организации (приказы, распоряжения и другие документы по вопросам защиты компьютерной информации).

Одним из основополагающих программных документов в сфере обеспечения защиты информации, информационной безопасности является Доктрина информационной безопасности Российской Федерации (утв. Президентом Российской Федерации от 9 сентября 2000 г. № Пр-1895).

Доктрина представляет собой документ, который содержит совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации и служит основой для:

• формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;

• подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;

[1] Пастоев А. Методологии управления ИТ-рисками // Открытые системы. 2006- № 8.

• разработки целевых программ обеспечения информационной безопасности Российской Федерации.

Особая значимость этого документа заключается в том, что в нем на основе развернутого анализа современного состояния безопасности личности, общества и государства определены цели, задачи и ключевые проблемы обеспечения информационной безопасности. В Доктрине выделяется четыре основные составляющие национальных интересов Российской Федерации в информационной сфере.

Первая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Вторая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Третья составляющая национальных интересов Российской Федерации в информационной сфере включает в себя развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

Четвертая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа,

обеспечение безопасности информационных и телекоммуникационных систем как уже развернутых, так и создаваемых на территории России.

Крайне важным с методологической точки зрения представляется выделение в Доктрине угроз информационной безопасности Российской Федерации. По своей общей направленности эти угрозы подразделены на следующие виды:

• угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;

• угрозы информационному обеспечению государственной политики Российской Федерации;

• угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

• угрозы безопасности информационных и телекоммуникационных средств и систем как уже развернутых, так и создаваемых на территории России.

В контексте настоящего исследования наибольший интерес представляет последняя группа угроз, которая включает в себя угрозы, связанные с:

• противоправным сбором и использованием информации;

• нарушением технологии обработки информации;

• внедрением в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;

• разработкой и распространением программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;

• уничтожением, повреждением, радиоэлектронным подавлением или разрушением средств и систем обработки информации, телекоммуникации и связи;

• воздействием на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;

• компрометацией ключей и средств криптографической защиты информации;

• утечкой информации по техническим каналам;

• внедрением электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;

• уничтожением, повреждением, разрушением или хищением машинных и других носителей информации;

• перехватом информации в сетях передачи данных и на линиях связи, дешифрованием этой информации и навязыванием ложной информации;

• использованием несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;

• несанкционированным доступом к информации, находящейся в банках и базах данных;

• нарушением законных ограничений на распространение информации.

Как можно заметить, угрозы, связанные с проявлениями воздействия на информационные системы вредоносных компьютерных программ, отнесены Доктриной к числу наиболее актуальных угроз информационной безопасности Российской Федерации. В этой связи представляется вполне закономерным, что к наиболее важным объектам обеспечения информационной безопасности в правоохранительной сфере Доктриной отнесены:

• информационные ресурсы федеральных органов исполнительной власти, реализующих правоохранительные функции, судебных органов, их информационно-вычислительных центров, научно-исследовательских учреждений и учебных заведений, содержащие специальные сведения и оперативные данные служебного характера;

• информационно-вычислительные центры, их информационное, техническое, программное и нормативное обеспечение;

• информационная инфраструктура (информационно-вычислительные сети, пункты управления, узлы и линии связи).

Помимо отмеченного, в Доктрине определяются методы обеспечения информационной безопасности Российской Федерации в различных сферах общественной жизни, которые подразделяются на: правовые, организационно-технические и экономические.

В качестве ключевых методов обеспечения защиты информационных систем и сетей от воздействия вредоносных программ

можно выделить такие организационно-технические мероприятия, как:

• разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;

• создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;

• выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации.

Таким образом, Доктрина информационной безопасности Российской Федерации недвусмысленным образом указывает, что информационная безопасность является составной частью системы национальной безопасности и относится к жизненно важным сферам обеспечения интересов личности, общества и государства. Исходя из целей настоящего исследования значимым является то, что опасность создания, использования и распространения вредоносных программ признается Доктриной в качестве одной из наиболее актуальных угроз для ключевых информационных сетей и систем, в том числе и в правоохранительной сфере.

Следует отметить, что в принятых спустя тринадцать лет Основах государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом Российской Федерации В. Путиным 24 июля 2013 г., № Пр-1753) создание, использование и распространение вредоносных компьютерных программ отнесено к основным угрозам не только национальной, но и международной информационной безопасности[1].

Последнее представляется вполне оправданным, учитывая сложившиеся тенденции в данной сфере. Как заметил по этому

[1] Основах государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом Российской Федерации В. Путиным 24 июля 2013 г., № Пр-1753) [Электронный ресурс]. - Режим доступа: http://www.scrf.gov.ru/documents/6/114.html.

поводу генеральный директор компании Kraftway А.Ю. Кравцов, «...в настоящее время не только совершаются преступления в информационном пространстве, но и создаются кибервойска. Атаки на информационные, телекоммуникационные системы становятся целью не только злоумышленников и хакеров. Многие государства всерьез рассматривают и создают подразделения, которые занимаются противодействием и нападением в этой области. Это понятно, поскольку, парализовав любую информационную систему, можно парализовать процессы, которые происходят в стране».

В целях противодействия подобного рода угрозам в Российской Федерации должна быть создана государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Указом Президента Российской Федерации от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» определены основные задачи этой системы:

а) прогнозирование ситуации в области обеспечения информационной безопасности Российской Федерации;

б) обеспечение взаимодействия владельцев информационных ресурсов Российской Федерации, операторов связи, иных субъектов, осуществляющих лицензируемую деятельность в области защиты информации, при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак;

в) осуществление контроля степени защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак;

г) установление причин компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации.

В более развернутом виде контуры рассматриваемой системы представлены в Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, утвержденной Президентом Российской Федерации 12 декабря 2014 г. № К 1274.

Согласно положениям данной концепции, основным назначением системы является обеспечение защищенности информационных ресурсов Российской Федерации от компьютерных атак и штатного функционирования данных ресурсов в условиях возникновения компьютерных инцидентов, вызванных компьютерными

атаками. Для выполнения основных задач, определенных в Указе Президента Российской Федерации от 15 января 2013 г. №31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», система осуществляет реализацию целого ряда функций, в том числе:

• выявление признаков проведения компьютерных атак, определение их источников, методов, способов и средств осуществления и направленности, а также разработка методов и средств обнаружения, предупреждения и ликвидации последствий компьютерных атак;

• осуществление мероприятий по оперативному реагированию на компьютерные атаки и вызванные ими компьютерные инциденты, а также по ликвидации последствий данных компьютерных инцидентов в информационных ресурсах Российской Федерации;

• выявление, сбор и анализ сведений об уязвимостях программного обеспечения и оборудования;

• совершенствование оперативно-тактического взаимодействия сил и средств обнаружения, предупреждения и ликвидации последствий компьютерных атак;

• организация и осуществление антивирусной защиты;

Основной организационно-технической составляющей системы являются центры обнаружения, предупреждения и ликвидации последствий компьютерных атак. К их основным задачам относятся:

• обнаружение, предупреждение и ликвидация последствий компьютерных атак, направленных на контролируемые информационные ресурсы;

• проведение мероприятий по оценке степени защищенности контролируемых информационных ресурсов;

• проведение мероприятий по установлению причин компьютерных инцидентов, вызванных компьютерными атаками на контролируемые информационные ресурсы;

• сбор и анализ данных о состоянии информационной безопасности в контролируемых информационных ресурсах;

• осуществление взаимодействия между центрами;

• информирование заинтересованных лиц и субъектов системы по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак.

В своей совокупности центры подразделяются на главный центр системы, а также региональные, территориальные, ведом-

ственные и корпоративные центры. Главный и региональный центры создаются силами ФСБ России, ведомственные центры создаются заинтересованными органами государственной власти. Корпоративные центры могут создаваться госкорпорациями, операторами связи и другими организациями, имеющими лицензии в области защиты информации.

Отмеченное позволяет заключить, что соответствующий центр, одной из задач которого является организация и осуществление антивирусной защиты ведомственных информационных ресурсов, должен быть создан и в системе МВД России.

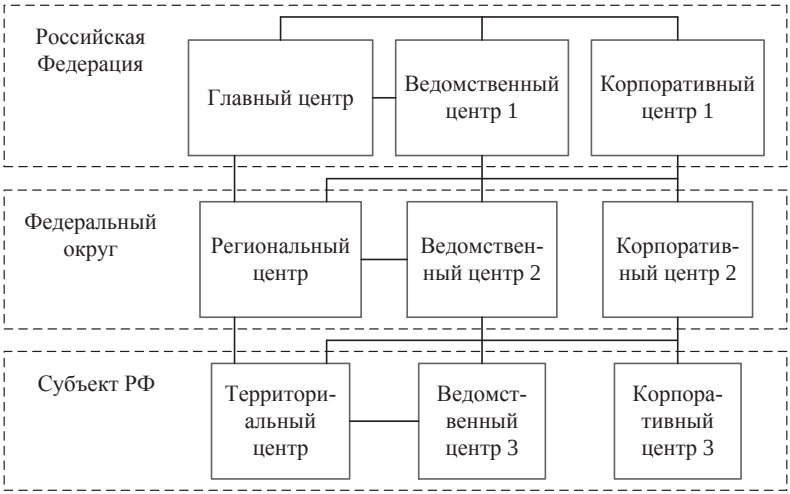

Рис. 3.1. Структура центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

Ключевые положения рассмотренных правовых актов применительно к специфике деятельности органов внутренних дел нашли свое отражение в таком программном документе, как Концепция обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года (утв. приказом МВД России от 14 марта 2012 г. № 169).

Данная концепция определяет комплекс мер, направленных на обеспечение защиты информации, информационных ресурсов и информационных систем органов внутренних дел Российской Федерации от специальных программно-технических воздействий, средств технических разведок, несанкционированного доступа, а также утечки информации по техническим каналам.

Констатируя значительный объем работы, проделанной в сфере обеспечения безопасности ведомственных информационных ресурсов и информационных систем, разработчики концепции выделяют следующие основные задачи обеспечения информационной безопасности органов внутренних дел:

• совершенствование правовых, научно-практических, нормативно-технических, организационно-методических и иных основ информационной безопасности ОВД;

• реализация комплекса организационных (режимных) и технических мероприятий, направленных на обеспечение защиты информации, информационных ресурсов и информационных систем ОВД от утечки, хищения, утраты, несанкционированного доступа, уничтожения, искажения, модификации, подделки, копирования, блокирования;

• создание и развитие системы информационной безопасности ОВД с учетом реализации «облачной архитектуры»;

• формирование и совершенствование системы мониторинга состояния информационной безопасности ОВД;

• организация и совершенствование профессиональной подготовки и переподготовки сотрудников органов внутренних дел в области обеспечения информационной безопасности.

Решение поставленных задач предполагает осуществление целого комплекса мероприятий, в том числе:

• разработка новых и совершенствование существующих способов, методов и средств выявления, оценки, прогнозирования, нейтрализации и ликвидации угроз информационной безопасности ОВД;

• организация технической защиты информации, программных, программно-технических и технических средств защиты, в том числе криптографической;

• обеспечение информационной безопасности при межведомственном информационном взаимодействии с федеральными органами государственной власти;

• разработка и совершенствование защищенных информационных технологий и информационно-телекоммуникационных систем ОВД;

• организация защиты информации в единой информационной системе централизованной обработки данных от несанкционированного доступа к обрабатываемой информации и воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи.

Таким образом, анализ концептуальных документов в сфере обеспечения информационной безопасности позволяет сделать вывод о том, что на государственном уровне сложилось четкое понимание той угрозы, которое несет в себе вредоносное программное обеспечения для безопасности информационных систем, используемых как в сфере государственного управления, так и корпоративного сектора. При этом государством не только декларируется потенциальная опасность, но и определяется целый комплекс мер по обеспечению противодействия современным киберугрозам.

Правовой основой реализации этих мероприятий, равно как и деятельности по обеспечению антивирусной защиты ведомственных информационных ресурсов Министерства внутренних дел Российской Федерации в целом, выступают, прежде всего, положения Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Данный закон приводит понятийный аппарат и механизмы регулирования в соответствие с практикой применения информационных технологий, определяет правовой статус различных категорий информации, закрепляет положения в области создания и эксплуатации информационных систем, общие требования к использованию информационно-телекоммуникационных сетей, а также принципы регулирования общественных отношений, связанных с использованием информации.

Практическая деятельность органов внутренних дел по решению стоящих перед ними задач характеризуется широким использованием самой разнообразной информации, которая по режиму доступа к ней может быть подразделена на две основные группы: общедоступную и информацию с ограниченным доступом (ст. 5 закона). К последней относятся[1]:

1) сведения, составляющие государственную тайну;

2) сведения о фактах, событиях и обстоятельствах частной жиз-ни гражданина, позволяющие идентифицировать его личность (персональные данные);

3) сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» и другими нормативными правовыми актами Российской Федерации;

[1] Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера».

4) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским Кодексом Российской Федерации и федеральными законами (служебная тайна);

5) сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телефонных или иных сообщений и т.д.);

6) сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским Кодексом Российской Федерации и федеральными законами (коммерческая тайна).

Используемая в деятельности органов внутренних дел информация хранится и обрабатывается с помощью различных информационных систем. Как совершенно верно отмечает Т.К. Шогенов[1], в настоящее время «...неотъемлемым условием информационного обеспечения деятельности подразделений, служб, организаций и учреждений Министерства внутренних дел Российской Федерации при реализации их функций является активное использование современных информационных технологий, программных и аппаратных средств, а также информационных систем на их основе. Значительное количество задач, в том числе принятие юридически значимых решений, подразумевает использование информационных систем, в которых осуществляется сбор, систематизация, уточнение, накопление, хранение и передача самой разнообразной информации».

В соответствии с положениями рассматриваемого закона, все информационные системы, рассматриваемые законодателем как совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств, подразделяются на три группы:

• государственные информационные системы - федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов;

• муниципальные информационные системы, созданные на основании решения органа местного самоуправления;

• иные информационные системы.

[1] Шогенов Т.К. Вопросы обеспечения безопасности персональных данных в информационных системах МВД России // Информационные технологии, связь и защита информации МВД России. М., 2012. С. 98.

Как представляется, информационные системы, используемые в практической деятельности подразделений Министерства внутренних дел для решения возложенных на них действующим законодательством задач, могут быть, с учетом положений постановления Правительства РФ от 6 июля 2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации», отнесены к классу государственных информационных систем, что возлагает на МВД России обязанность по защите содержащейся в подобного рода системах информации от неправомерных попыток доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий (п. 9 ст. 14).

При этом, согласно положениям п. 5 ст. 16 рассматриваемого закона, требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации. Федеральным органом исполнительной власти в области обеспечения безопасности является Федеральная служба безопасности, а федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации - Федеральная служба по техническому и экспортному контролю (ФСТЭК России).

Приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 утверждены Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.

Данный документ устанавливает требования к обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения или блокирования доступа к ней при обработке указанной информации в государственных информационных системах.

Как указывается в п. 12 данных требований, защита информации, содержащейся в информационной системе, является составной частью работ по созданию и эксплуатации информационной

системы и обеспечивается на всех стадиях (этапах) ее создания и в ходе эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в информационной системе. При этом организационные и технические меры защиты информации, реализуемые в информационной системе в рамках ее системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационной системы должны обеспечивать, помимо прочего, и антивирусную защиту информации (п. 20 требований).

В зависимости от значимости обрабатываемой в информационной системе информации в требованиях устанавливаются четыре класса защищенности информационной системы, определяющие уровни защищенности содержащейся в ней информации. Самый низкий класс - четвертый, самый высокий - первый.

Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы приведены в приложении № 2 рассматриваемого документа. Согласно требований данного приложения в системе любого класса защищенности должна быть реализована антивирусная защита информации и обновление базы данных признаков вредоносных компьютерных программ (вирусов).

Особое внимание в действующем законодательстве уделяется вопросам защиты сведений, составляющих государственную тайну, под которой в соответствии с п. 2 Закона РФ от 21 июля 1993 г. № 5485-I «О государственной тайне» понимаются «...защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации». Как можно заметить, данный вопрос особенно актуален для МВД России, поскольку оперативно-разыскная деятельность является одним из важнейших направлений деятельности органов внутренних дел по противодействию современной преступности.

Сведения, накапливаемые в рамках проведения оперативно-разыскных мероприятий, могут храниться в делах оперативного учета или создаваемых для этих целях информационных системах (п. 10 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»). В последнем случае, как уже отмечалось ранее, в отношении хранящейся в подобной системе информации должны применяться меры по ее защите. При этом,

согласно п. 28 Закона РФ от 21 июля 1993 г. № 5485-I «О государственной тайне», средства защиты информации, составляющей государственную тайну, должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Также следует отметить, что в соответствии с требованиями Указа Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» в случаях подключения информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей государственную или служебную тайны, к информационно-телекоммуникационным сетям международного информационного обмена, или если речь идет о защите общедоступной информации государственных органов, размещаемой в информационно-телекоммуникационных сетях международного информационного обмена, должны использоваться средства защиты информации, прошедшие в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и(или) получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю.

Порядок сертификации средств защиты информации, составляющей государственную тайну, установлен приказом Федеральной службы безопасности (ФСБ) РФ от 13 ноября 1999 г. № 564 «Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия».

Правовую основу сертификации средств защиты информации ФСТЭК России составляет «Положение о сертификации средств защиты информации по требованиям безопасности информации», утвержденное приказом Гостехкомиссии от 27.10.1995 № 119.

Также необходимо отметить, что, помимо отмеченного, при выборе конкретного программного решения в целях обеспечения антивирусной защиты информационной системы следует руководствоваться Требованиями к средствам антивирусной защиты, утвержденными приказом ФСТЭК России от 20 марта 2012 г. № 28[1].

[1] Информационное сообщение Федеральной службы по техническому и экспортному контролю от 30 июля 2012 г. № 240/24/3095 «Об утверждении Требований к средствам антивирусной защиты» [Электронный ресурс]. Доступ из справ.-правовой системы «Гарант».

Данные требования применяются к программным средствам, используемым в целях обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом.

Для дифференциации требований к функциям безопасности средств антивирусной защиты установлено шесть классов защиты средств антивирусной защиты. Самый низкий класс - шестой, самый высокий - первый.

Средства антивирусной защиты, соответствующие 6 классу защиты, применяются в информационных системах персональных данных 3 и 4 классов[1].

Средства антивирусной защиты, соответствующие 5 классу защиты, применяются в информационных системах персональных данных 2 класса.

Средства антивирусной защиты, соответствующие 4 классу защиты, применяются в государственных информационных системах, в которых обрабатывается информация ограниченного доступа, не содержащая сведения, составляющие государственную тайну, в информационных системах персональных данных 1 класса, а также в информационных системах общего пользования II класса[2].

Средства антивирусной защиты, соответствующие 3, 2 и 1 классам защиты, применяются в информационных системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.

Также выделяются следующие типы средств антивирусной защиты:

тип «А» - средства антивирусной защиты (компоненты средств антивирусной защиты), предназначенные для централизованного администрирования средствами антивирусной защиты, установленными на компонентах информационных систем (серверах, автоматизированных рабочих местах);

тип «Б» - средства антивирусной защиты (компоненты средств антивирусной защиты), предназначенные для применения на серверах информационных систем;

[1] Здесь и далее классы информационных систем персональных данных устанавливаются в соответствии с Порядком проведения классификации информационных систем персональных данных, утвержденным приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20.

[2] Устанавливается в соответствии с Требованиями о защите информации, содержащейся в информационных системах общего пользования, утвержденными приказом ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

тип «В» - средства антивирусной защиты (компоненты средств антивирусной защиты), предназначенные для применения на автоматизированных рабочих местах информационных систем;

тип «Г» - средства антивирусной защиты (компоненты средств антивирусной защиты), предназначенные для применения на автономных автоматизированных рабочих местах.

При этом средства антивирусной защиты типа «А» не применяются в информационных системах самостоятельно и предназначены для использования только совместно со средствами антивирусной защиты типов «Б» и(или) «В».

Рассмотрев правовые основы построения системы антивирусной защиты информационных систем, остановимся на технологиях работы современных антивирусов и анализе отечественного рынка антивирусного программного обеспечения.

4. СОВРЕМЕННЫЕ ТЕХНОЛОГИИ АНТИВИРУСНОЙ ЗАЩИТЫ, ОТЕЧЕСТВЕННЫЙ РЫНОК АНТИВИРУСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Самыми эффективными средствами защиты от вирусов являются специальные программы, способные распознавать и обезвреживать вирусы в файлах, письмах и других объектах. Такие программы называются антивирусами, и для того, чтобы построить действительно надежную антивирусную защиту, использовать их нужно обязательно.

В современных антивирусных продуктах используется два основных подхода к обнаружению вредоносных программ: сигнатурный и проактивный/эвристический.

Сигнатурные методы - это точные методы обнаружения вирусов, основанные на сравнении файла с известными образцами вирусов.

Проактивные/эвристические методы - приблизительные методы обнаружения, которые позволяют с определенной вероятностью предположить, что файл заражен.

Термин «сигнатура» происходит от английского слова *signature*, означающего «подпись», или же в переносном смысле «характерная черта, нечто идентифицирующее».

Сигнатурный анализ заключается в выявлении характерных идентифицирующих черт каждого вируса и поиска вирусов путем сравнения файлов с выявленными чертами.

Сигнатурой вируса будет считаться совокупность черт, позволяющих однозначно идентифицировать наличие вируса в файле (включая случаи, когда файл целиком является вирусом). Все вместе сигнатуры известных вирусов составляют антивирусную базу.

Эта технология предполагает непрерывное отслеживание новых экземпляров вредоносных программ, их описание и включение в базу сигнатур. Задачу выделения сигнатур, как правило, решают люди - эксперты в области компьютерной вирусологии, способные выделить код вируса из кода программы и сформулировать его характерные черты в форме, наиболее удобной для поиска. В наиболее простых случаях могут применяться специальные автоматизированные средства выделения сигнатур, например для несложных по структуре троянов или червей, которые не заражают другие программы, а целиком являются вредоносными программами.

Практически в каждой компании, выпускающей антивирусы, есть своя группа экспертов, проводящая анализ новых вирусов и пополняющая антивирусную базу новыми сигнатурами. По этой причине антивирусные базы в разных антивирусах различаются. Тем не менее между антивирусными компаниями существует договоренность об обмене образцами вирусов, а значит, рано или поздно сигнатура нового вируса попадает в антивирусные базы практически всех антивирусов. Лучшим же антивирусом будет тот, для которого сигнатура нового вируса была выпущена раньше всех.

Часто для обнаружения семейства похожих вирусов используется одна сигнатура, и поэтому количество сигнатур не всегда равно количеству обнаруживаемых вирусов. Соотношение количества сигнатур и числа известных вирусов для каждой антивирусной базы свое. Если же учесть, что антивирусные компании обмениваются образцами вирусов, можно с высокой долей уверенности считать, что антивирусные базы наиболее известных антивирусов эквивалентны.

Важное дополнительное свойство сигнатур - точное и гарантированное определение типа вируса. Это свойство позволяет занести в базу не только сами сигнатуры, но и способы лечения вируса.

Главные критерии эффективности сигнатурного метода - это скорость реакции на новые угрозы, частота обновлений, максимальное число обнаруженных угроз.

Главный недостаток сигнатурного метода - задержка при реакции на новые угрозы. Для получения сигнатуры необходимо иметь образец вируса. Создать его сигнатуру невозможно, пока вирус не попал на анализ к экспертам. Поэтому сигнатуры всегда появляются только через некоторое время после появления ново-

го вируса. С момента появления вируса в сети Интернет до выпуска первых сигнатур обычно проходит несколько часов, и все это время вирус способен заражать компьютеры почти беспрепятственно. Именно поэтому традиционный сигнатурный метод непригоден для оперативной зашиты от вновь появляющихся вирусов.

Этот недостаток традиционного сигнатурного анализа позволяет преодолеть проактивная антивирусная защита.

Проактивные методы обнаружения вирусов получают все большее распространение. В принципе, использование этой технологии позволяет обнаруживать еще неизвестные вредоносные программы. Существует несколько подходов к проактивной защите.

Рассмотрим два наиболее популярных подхода: эвристические анализаторы и поведенческие блокираторы.

Эвристические анализаторы.

Слово «эвристика» происходит от греческого глагола «находил»». Суть эвристических методов состоит в том, что решение проблемы основывается на некоторых правдоподобных предположениях, а не на строгих выводах из имеющихся фактов и предпосылок. Такое определение звучит достаточно туманно, поэтому эвристический метод поясним далее на примерах.

Если сигнатурный метод основан на выделении характерных признаков вируса и поиске этих признаков в проверяемых файлах, то эвристический анализ основывается на предположении (весьма правдоподобном), что новые вирусы часто оказываются похожи на какие-либо из уже известных. Такое предположение оправдывается наличием в антивирусных базах сигнатур для определения не одного, а сразу нескольких вирусов. Этот эвристический метод часто называют поиском вирусов, похожих на известные, или статическим анализом.

Эвристический анализатор (эвристик) - это программа, которая анализирует программный код проверяемого объекта и по косвенным признакам определяет, является ли объект вредоносным. Работа эвристического анализатора, как правило, начинается с поиска в программном коде подозрительных признаков (команд), характерных для вредоносных программ.

Например, многие вредоносные коды ищут исполняемые программы, открывают найденные файлы и изменяют их. Эвристический анализатор просматривает код приложения и, встретив подозрительную команду, увеличивает некий «счетчик подозрительности» для данного приложения. Если после просмотра всего кода значение счетчика превышает заданное пороговое значение, то объект признается подозрительным.

Первые эвристические анализаторы появились в антивирусных продуктах довольно давно, и на сегодняшний день более или менее совершенные эвристики реализованы во всех антивирусных решениях.

Достоинствами статического анализа являются простота реализации, высокая скорость работы, возможность обнаружения новых, неизвестных вирусов еще до того, как для них будут выделены сигнатуры.

Однако уровень обнаружения новых вредоносных кодов остается довольно низким, а вероятность ложных срабатываний - высокой. Поэтому в современных антивирусах статический анализ используется в сочетании с динамическим.

Идея такого комбинированного подхода состоит в том, чтобы до того, как приложение будет запущено на компьютере пользователя, эмулировать его запуск в безопасном виртуальном окружении, которое называется также буфером эмуляции или «песочницей».

Динамический эвристический анализатор читает часть кода приложения в буфер эмуляции антивируса и с помощью специальных приемов эмулирует его исполнение. Если в процессе этого псевдоисполнения обнаруживаются какие-либо подозрительные действия, объект признается вредоносным и его запуск на компьютере пользователя блокируется.

В отличие от статического метода, динамический более требователен к ресурсам компьютера, так как для анализа приходится использовать безопасное виртуальное пространство, а запуск приложения на компьютере пользователя откладывается на время анализа. Однако и уровень обнаружения вредителей у динамического метода значительно выше, чем у статического, а вероятность ложных срабатывании существенно меньше.

Недостатки эвристических анализаторов:

- невозможность лечения в силу потенциальных ложных срабатываний и возможного неточного определения типа вируса: попытка лечения может привести к большим потерям информации, чем из-за самого вируса, а это недопустимо;

- низкая эффективность против принципиально новых типов вирусов.

Поведенческие блокираторы.

Поведенческий блокиратор - это программа, которая анализирует поведение запущенного приложения и блокирует любые опасные действия.

К основным вредоносным действиям относят:

• удаление файла;

• запись в файл;
• запись и определенные области системного реестра;
• открытие порта на прослушивание;
• перехват данных, вводимых с клавиатуры;
• рассылка писем и др.

Выполнение каждого такого действия по отдельности не дает повода считать программу вредоносной. Но если программа последовательно выполняет несколько таких действий, например перехватывает данные, вводимые с клавиатуры, и с определенной частотой пересылает их на какой-то адрес в Интернете, значит, эта программа по меньшей мере подозрительна.

В отличие от эвристических анализаторов, где подозрительные действия отслеживаются в режиме эмуляции (динамический эвристик), поведенческие блокираторы работают в реальных условиях.

Принцип действия первых поведенческих блокираторов был прост. При обнаружении потенциально опасного действия задавался вопрос пользователю: разрешить или запретить это действие. Во многих случаях такой подход работал, но «подозрительные» действия производили и легитимные программы (вплоть до операционной системы). Поэтому, если пользователь не обладал должной квалификацией, вопросы антивируса вызывали непонимание.

Современные поведенческие блокираторы анализируют уже не отдельные действия, а последовательность операций. Другими словами, заключение об опасности того или иного приложения выносится па основе более сложного анализа. Таким образом, удается значительно сократить количество запросов к пользователю и повысить надежность детектирования.

Современные поведенческие блокираторы способны контролировать широкий спектр событий, происходящих в системе. Это прежде всего контроль опасной активности (анализ поведения всех процессов, запущенных в системе, сохранение всех изменений, производимых в файловой системе и реестре).

При выполнении некоторым приложением набора подозрительных действий выдается предупреждение пользователю об опасности данного процесса. Помимо этого, блокиратор позволяет перехватить все возможности внедрения программного кода в чужие процессы. Вдобавок блокиратор способен обнаружить руткиты, то есть программы, которые скрывают от пользователя работу вредоносного кода с файлами, папками и ключами реестра, а также прячут запущенные программы, системные службы, драйверы и сетевые соединения.

Особо стоит выделить такую функциональность поведенческих блокираторов, как контроль целостности приложений и системного реестра Microsoft Windows. В последнем случае блокиратор контролирует изменения ключей реестра и позволяет задавать правила доступа к ним для различных приложений. Все вместе это позволяет осуществить откат изменений после определения опасной активности в системе. Таким образом, можно восстанавливать систему даже после вредоносных действий неизвестных программ, вернув ее к незараженному состоянию.

В качестве примера эффективного поведенческого блокиратора нового поколения можно привести модуль проактивной защиты (Proactive Defence Module), реализованный в продуктах «Лаборатории Касперского». Данный модуль включает в себя все перечисленные выше возможности и, что особенно важно, хорошую систему информирования пользователя о том, в чем реально состоит опасность тех или иных подозрительных действий. Любой поведенческий блокиратор на определенном этапе требует вмешательства пользователя, что предполагает наличие у последнего определенной квалификации. На практике пользователь часто не обладает необходимыми знаниями, поэтому информационная поддержка - фактически поддержка принятия решений - является обязательным атрибутом современных антивирусных решений.

Поведенческий блокиратор может предотвратить распространение как известного, так и неизвестного (написанного после создания блокиратора) вируса, что является неоспоримым достоинством такого подхода к защите.

Недостатком поведенческих блокираторов остается срабатывание на действия ряда легитимных программ. Для принятия окончательного решения о вредоносности приложения требуется вмешательство пользователя, что предполагает наличие у него достаточной квалификации.

Для оптимальной антивирусной защиты необходимо сочетание проактивных и сигнатурных подходов. Максимального уровня обнаружения угроз можно достигнуть, только комбинируя эти методы. Примером успешного сочетания проактивных и сигнатурных методов может служить технология ThreatSense компании Eset.

ThreatSense - это сбалансированная технология, позволяющая комбинировать эвристический анализатор и поведенческий блокиратор с сигнатурным методом. Эта технология обеспечивает обнаружение не только известных, но и новых угроз, не снижая при этом скорости работы используемой системы.

Практически любая антивирусная программа объединяет в разных пропорциях все технологии и методы защиты от вирусов, созданные к сегодняшнему дню.

Также весьма надежным методом зашиты от вирусов является использование аппаратно-программных антивирусных средств. В настоящее время для зашиты ПЭВМ используются специальные контроллеры и их программное обеспечение. Контроллер устанавливается в разъем расширения и имеет доступ к обшей шине. Это позволяет ему контролировать все обращения к дисковой системе. В программном обеспечении контроллера запоминаются области на дисках, изменение которых в обычных режимах работы не допускается. Таким образом можно установить защиту на изменение главной загрузочной записи, загрузочных секторов, файлов конфигурации, исполняемых файлов и др. Примером аппаратно-программной зашиты от вирусов может служить комплекс Sheriff, Dr.Web Office Shield.

В настоящее время на отечественном рынке присутствует достаточно большое количество как российских, так и зарубежных продуктов обеспечения антивирусной защиты информационных систем. По оценкам экспертов, в 2014 году выручка от продажи антивирусных программ составила 12 миллиардов рублей, в 2013 году - 11,9 млрд.[1] При этом аналитиками ожидается увеличение продаж за счет вытеснения российскими продуктами западных аналогов.

По данным компании IDC, специализирующейся на исследованиях рынка IT-технологий, крупнейшим производителем решений для защиты конечных устройств в пользовательском и корпоративном сегментах в России является «Лаборатория Касперского», в активе которой значится 55,5% рынка. Продукты компании ESET занимают порядка 26% рынка, а вендоры Symantec, Dr. Web, TrendMicro и McAfee - около 20%[2].

Рассмотрим вкратце основные решения в области антивирусной защиты корпоративных информационных систем лидеров отечественного рынка: «Лаборатории Касперского» и компании ESET.

---

[1] Ситуация на рынке антивирусов в России [Электронный ресурс]. - Режим доступа: http://www.ecomyzone.com/?p=1616.

[2] Российский рынок антивирусов находится в стагнации [Электронный ресурс]. - Режим доступа: http://www.dailycomm.ru/m/29960/.

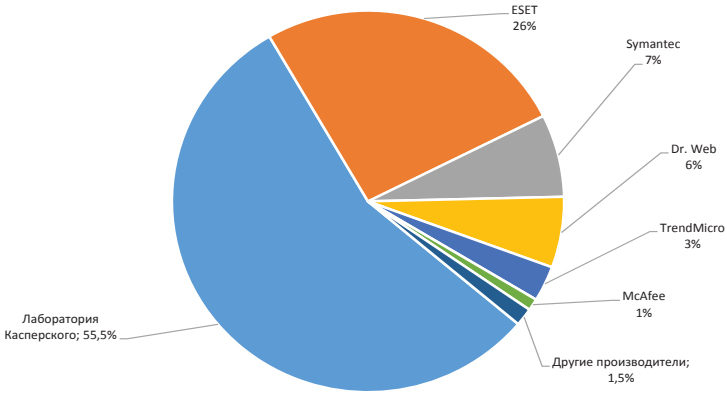

Рис. 4.1. Российский рынок антивирусного программного обеспечения

Лаборатория Касперского - самый популярный в России и крупнейший в Европе производитель систем защиты от вирусов, спама и хакерских атак. Компания входит в пятерку ведущих мировых производителей программных решений для обеспечения информационной безопасности.

«Лаборатория Касперского» выпускает широкий спектр решений для обеспечения надежной защиты от вирусов, спама и хакерских атак. Компания создает продукты как для домашних пользователей, так и для крупных корпораций.

В контексте настоящего исследования наибольший интерес представляет линейка «Kaspersky Security для бизнеса», позволяющая выбрать оптимальное решение для контроля рабочих мест (от рабочих станций до смартфонов и виртуальных машин), серверов и интернет-шлюзов и обеспечения их надежной защитой. Одно из основных преимуществ корпоративных продуктов «Лаборатории Касперского» - легкое централизованное администрирование при помощи инструмента Kaspersky Security Center, который обеспечивает эффективное управление антивирусной защитой вне зависимости от масштабов сети и типа используемых в ней платформ.

В общем виде линейка корпоративных решений «Лаборатории Касперского» может быть представлена следующим образом:

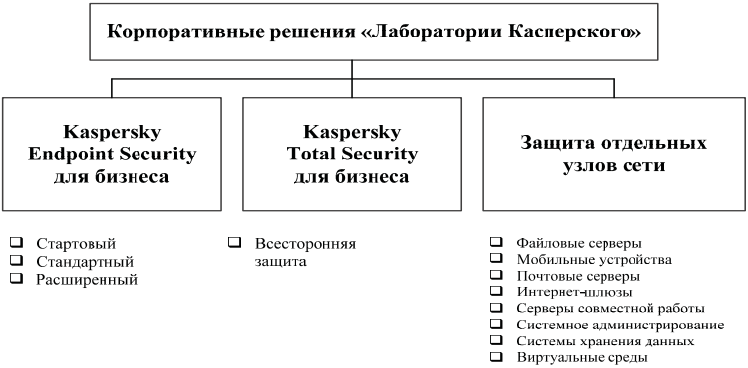

Рис. 4.2. Корпоративные решения «Лаборатории Касперского»

Продукты линейки Kaspersky Security для бизнеса обеспечивают антивирусную защиту, контроль использования устройств, приложений и веб-ресурсов, предоставляют инструменты шифрования и системного администрирования. В него также входят средства управления мобильными устройствами и создания политик безопасности. Управление защитой осуществляется из единого центра.

Технологии антивирусной защиты рабочих станций и сетевой экран образуют единый уровень защиты, формируя первый - СТАРТОВЫЙ - уровень защитного решения Kaspersky Endpoint Security для бизнеса СТАРТОВЫЙ, предлагаемого «Лабораторией Касперского».

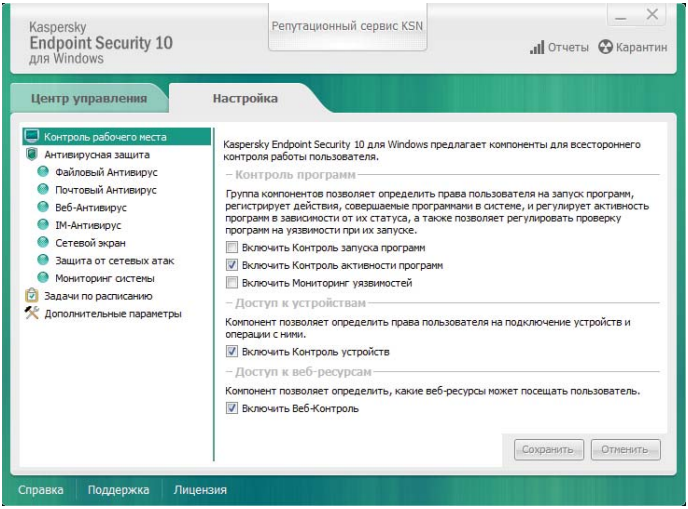

Рис. 4.3. Интерфейсное окно Kaspersky Endpoint Security 10

В СТАНДАРТНЫЙ уровень защиты, помимо возможностей СТАРТОВОГО уровня, в список защитных функций включены технологии контроля программ и белые списки, контроль устройств и веб-контроль. Кроме них в этот уровень входит защитное решение для мобильных устройств, состоящее из решения для защиты конечных точек и средства управления мобильными устройствами (смартфонами и планшетами) - Mobile Device Management (MDM).

Помимо возможностей, предусмотренных СТАНДАРТНЫМ уровнем защиты, в РАСШИРЕННЫЙ уровень включена технология шифрования данных, обеспечивающая возможность шифрования как отдельных файлов и папок, так и всего диска.

Еще одна новая функция в составе уровня РАСШИРЕННЫЙ, обеспечивающая более высокий уровень безопасности и эффективности IT-инфраструктуры - Kaspersky Systems Management.

Kaspersky Systems Management включает несколько функциональных модулей:

• развертывание операционных систем;

• удаленная установка программного обеспечения и устранение неполадок;

• поддержка Microsoft Wsus и Wake-on-lan;

• управление лицензиями;

• учет программного и аппаратного обеспечения;

• мониторинг уязвимостей;

• управление установкой исправлений;

• контроль доступа в сеть (Nac).

Все эти технологии составляют решение Kaspersky Endpoint Security для бизнеса РАСШИРЕННЫЙ.

И наконец, в максимальный уровень защиты - Kaspersky Total Security - добавлено разработанное «Лабораторией Касперского» решение для защиты серверов совместной работы, а также продукты компании для защиты почтовых серверов и интернет-шлюзов.

Как можно заметить, «Лаборатория Касперского» предлагает достаточно широкий спектр технологий, интегрированных в единое решение и основанных на единой технологической базе.

ESET. Компания ESET (Essential Security against Evolving Threats - эффективная защита от эволюционирующих угроз) является одним из мировых лидеров в области разработки антивирусного программного обеспечения и решений в области компьютерной безопасности для корпоративных и домашних пользователей. Штаб-квартиры ESET находятся в Братиславе (Словакия) и в Сан-Диего (США). Продукты и решения ESET NOD32 представлены более чем в 180 странах мира.

ESET стала одним из первых производителей антивирусного программного обеспечения, начавшим использовать проактивные методы обнаружения неизвестных сетевых угроз. В основе всех актуальных продуктов ESET лежит программная платформа, основным элементом которой является блок расширенной эвристики под названием ThreatSense.

Компания ESET в настоящий момент предлагает корпоративным пользователям несколько вариантов решений для защиты корпоративной IT-инфраструктуры, отличающихся лишь набором функциональных компонентов. Наиболее полным является NOD32 Secure Enterprise - кроссплатформенный комплекс решений для информационной защиты всех узлов корпоративной инфраструктуры: рабочих станций, мобильных устройств, файловых и почтовых серверов, а также HTTP- и FTP-шлюзов. Вся система безопасности централизованно управляется с помощью консоли ESET Remote Administrator.

Система лицензирования ESET дает возможность сформировать индивидуальный комплекс безопасности с учетом особенностей ИТ-инфраструктуры отдельной компании (использования определенных ОС, мобильных устройств, объема входящего трафика, требуемого уровня защиты и т.д.). Масштабируемость ESET NOD32 Secure Enterprise позволяет быстро развернуть и настроить эффективную систему безопасности в организациях любого размера - от небольших офисов с несколькими ПК до корпораций с десятками региональных представительств.

Программные компоненты ESET Endpoint Security и Endpoint Antivirus, входящие в состав NOD32 Secure Enterprise, защищают компьютеры сотрудников как от уже известных, так и от новых вредоносных программ, еще не внесенных в антивирусные базы.

Для защиты корпоративных мобильных устройств предназначены решения Endpoint Security для Android и Mobile Security. Они не только защищают устройства от мобильных угроз, но и позволяют администратору блокировать нежелательные SMS и MMS, а также (с помощью «черных» и «белых» списков) ограничивать как входящие, так и исходящие вызовы. При краже или потере мобильного устройства его местонахождение можно оперативно определить по GPS-координатам. Если вернуть устройство не удалось, все контакты, сообщения и другие хранящиеся на нем данные могут быть дистанционно удалены.

Для защиты файловых серверов компании, в зависимости от используемой платформы, предназначены ESET File Security для Microsoft Windows Server и ESET File Security для Linux/BSD/Solaris.

Эти решения были оптимизированы для работы в серверных средах, благодаря чему демонстрируют неизменной высокий уровень защиты без снижения производительности. Также стоит отметить режим многопоточного сканирования, который обеспечивает быструю работу при минимальной нагрузке на систему.

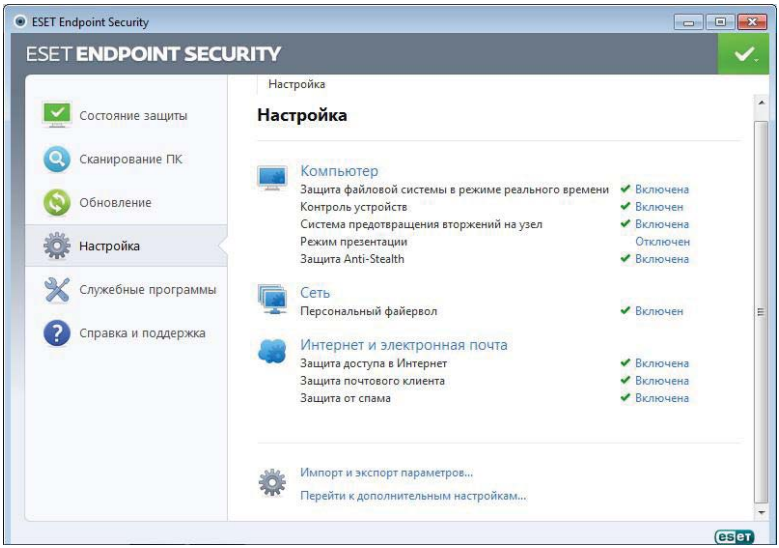

Рис. 4.4. Интерфейсное окно ESET Endpoint Security

Помимо этого, комплекс ESET NOD32 Secure Enterprise предлагает ряд решений для защиты почтовых серверов на всех возможных платформах. Они обнаруживают угрозы и вредоносные вложения в электронной почте, защищают корпоративную информацию, а также используют новейшую антиспам-технологию ESET для отсеивания нежелательных писем.

NOD32 Secure Enterprise также предлагает защиту на уровне HTTP- и FTP-шлюзов, что не только существенно повышает безопасность и управляемость системы, но и обеспечивает высокую скорость работы для многофункциональных систем с большим объемом входящего трафика.

Вся система безопасности управляется с помощью консоли ESET Remote Administrator. Этот гибкий инструмент позволяет централизованно разворачивать, настраивать и администрировать решения ESET NOD32 в корпоративных средах любой сложности и разветвленности, обеспечивая работу всех защитных механизмов на всех узлах корпоративной ИТ-инфраструктуры.

Рассмотрев лидеров отечественного рынка антивирусного программного обеспечения, нельзя не отметить и такое антивирусное решение, как ***Dr.Web Enterprise Security Suite***. Прежде всего, оно представляет несомненный интерес тем, что наряду с продукцией «Лаборатории Касперского» является полностью отечественным программным продуктом, что в современных условиях представляется крайне важным с учетом реализуемого в России курса на импортозамещение, в том числе и в сфере информационных технологий.

Dr.Web Enterprise Security Suite предназначен для организации и управления единой и надежной комплексной антивирусной защитой как внутренней сети компании, включая мобильные устройства, так и домашних компьютеров сотрудников.

Решение Dr.Web Enterprise Security Suite имеет архитектуру клиент-сервер. Клиентские компоненты комплекса устанавливаются на защищаемые рабочие станции и серверы. Dr.Web Сервер обеспечивает централизованное администрирование антивирусной и антиспам-защиты сети предприятия, включая развертывание, обновление вирусных баз и программных модулей компонентов, мониторинг состояния сети, извещения о вирусных событиях, сбор статистики.

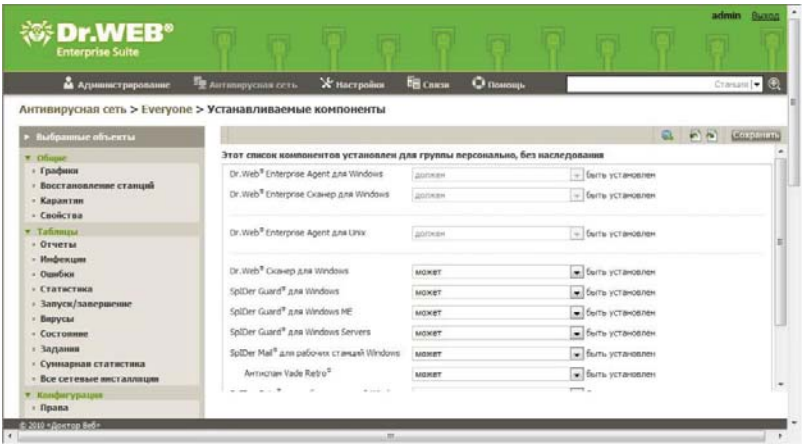

Рис. 4.5. Интерфейсное окно Dr.Web Enterprise Security Suite

Совокупность компьютеров, на которых установлены взаимодействующие компоненты Dr.Web ESS, объединяются под названием антивирусная сеть. Для развертывания антивирусной сети могут применяться преимущества технологии Active Directory, ис-

пользующейся в серверах под ОС Windows. Для связи Dr.Web Сервера с Dr.Web Агентами используются протоколы TCP/IP.

Особенностью Dr.Web Enterprise Suite является возможность управления им из любой точки мира, с любого компьютера, имеющего выход в Интернет, вне зависимости от используемой операционной системы. При этом для управления защитой не требуется устанавливать какое-либо дополнительное программное обеспечение.

Рассмотренные продукты не исчерпывают всего многообразия современного рынка антивирусного программного обеспечения. Однако выбор того или иного программного решения в каждом конкретном случае определяется, прежде всего, спецификой той информационной системы, защиту которой он должен обеспечивать. В этой связи представляется необходимым более подробно остановиться на особенностях Единой системы информационно-аналитического обеспечения МВД России как объекта антивирусной безопасности.

5. ЕДИНАЯ СИСТЕМА ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОГО ОБЕСПЕЧЕНИЯ МВД РОССИИ КАК ОБЪЕКТ АНТИВИРУСНОЙ БЕЗОПАСНОСТИ

Анализ практики правоохранительной деятельности свидетельствует о том, что эта деятельность неразрывно связана с процессами глобальной информатизации всех сторон и аспектов жизнедеятельности современного общества, выражающейся, с одной стороны, в стремительном росте объема производимых и потребляемых информационных ресурсов, в том числе и открытых для общего доступа с использованием средств массовых коммуникаций, профессионализации преступного сообщества, вовлечении в преступную деятельность новейших информационных технологий, а с другой - в широком использовании современных информационных технологий в оперативно-служебной деятельности органов внутренних дел. Знаковым событием в этой сфере стала разработка и внедрение Единой информационно-телекоммуникационной системы органов внутренних дел (ЕИТКС). С ее введением отдельные частные научные методики и методологии, информационные и инновационные системы в министерстве приобрели должную ценность, организационное единство и завершенность.

В марте 2012 года МВД России была разработана концепция создания единой системы информационно-аналитического обеспечения деятельности (ИСОД) МВД России. Создание ИСОД пришло на смену проекту по созданию единой информационно-телекоммуникационной системы (ЕИТКС) ОВД, которое велось с 2005 года. Важнейшей составной частью этой системы являлась телекоммуникационная подсистема, обеспечивающая информационное взаимодействие всех подразделений ОВД с другими правоохранительными органами и госорганами различных уровней.

Основной причиной принятия решения о создании ИСОД ОВД являлось отсутствие единых архитектурных решений и системного подхода к внедрению автоматизированных систем, то есть программные решения создавались независимо друг от друга, отдельно для каждого подразделения органов внутренних дел. На самом деле информация, которая требуется конкретному подразделению полиции, необходима и другим структурам. Вместе с тем получить ее быстро из различных систем на одно рабочее место довольно затруднительно из-за несовместимости форматов. Таким образом, чтобы сотрудники органов внутренних дел могли использовать разные системы необходимо устанавливать несколько компьютеров на одном рабочем месте. Следовательно, сегодня одной из первостепенных задач Департамента информационных технологий, связи и защиты информации является «связывание» между собой всех уже созданных информационных систем. Приведение к единой информационной платформе возможно либо за счет интеграции существующих систем, или замены программного обеспечения.

Другой не менее важной причиной является то, что системы создавались без учета современных тенденций, их использование предполагало установку программ непосредственно на рабочих местах пользователей и серверах локальных сетей, а также создание отдельных центров обработки данных на территориальном и региональном уровнях, что влекло за собой высокую стоимость обслуживания, низкую надежность и недостаточную производительность[1].

ИСОД ОВД представляет собой совокупность используемых в Министерстве автоматизированных систем обработки информации, программно-аппаратных комплексов и комплексов программно-технических средств, а также систем связи и передачи данных, необходимых для эффективного обеспечения служебной деятельности МВД России. В процессе создания Системы были решены

[1] Деятельность информационных служб МВД России / Н.В. Ходякова и др. Волгоград: ВА МВД России, 2012.

задачи автоматизации основных видов деятельности подразделений МВД России, организации централизованного хранения и обработки данных. Система должна стать единым источником информации для всех сотрудников подразделений МВД России, служить для организации электронного взаимодействия между ними, обеспечения разграниченного доступа к информационным ресурсам. Также ИСОД будет способствовать повышению эффективности принимаемых решений за счет улучшения качества подготавливаемых отчетов, основанных на актуальных и достоверных данных, обеспечения оперативного и своевременного анализа ключевых показателей деятельности МВД России. Таким образом, главный ожидаемый от создания ИСОД ОВД результат - более эффективное выполнение государственных функций и предоставление государственных услуг за счет снижения времени и трудоемкости операций по обработке информации, финансовых затрат на техническое сопровождение и обслуживание программно-технических комплексов за счет исключения необходимости замены используемых в настоящее время морально устаревших технических средств ввиду реализации технологии «облачных вычислений», способной динамически перераспределять нагрузку и обеспечивать требуемый уровень защиты, катастрофоустойчивости и доступности информации.

Основным элементом инфраструктуры ИСОД ОВД является ЕИС ЦОД, который создается на нескольких территориально удаленных площадках. Он предназначен для размещения централизованных информационных систем и сервисов МВД и предоставления доступа к ним с использованием облачных технологий.

За счет создания ЕИС ЦОД в МВД становится возможным унифицировать используемые в ведомстве программно-технические решения и привести архитектуру основных автоматизированных информационных систем в соответствие современным требованиям к доступности и надежности. Он должен обеспечить консолидацию разнородных данных, содержащихся в различных системах МВД и обеспечить единую точку доступа к ним для использования в оперативно-служебной деятельности МВД.

Прикладные сервисы обеспечения повседневной деятельности подразделений МВД России, реализуемые в рамках ИСОД, включают:

- сервис электронного документооборота (СЭД);
- сервис электронной почты (СЭП);
- ведомственный информационно-справочный портал (ВИСП);
- систему видеоконференцсвязи.

Прикладные сервисы обеспечения оперативно-служебной деятельности включают:

- информационно-поисковый сервис «Следопыт-М»;
- сервис обеспечения охраны общественного порядка (СООП);
- сервис обеспечения деятельности дежурных частей (СОДЧ);
- сервис обеспечения деятельности подразделений материально-технического обеспечения МВД (СОМТО);
- федеральную информационную систему ГИБДД (ГИБДД-М);
- сервис обеспечения экономической безопасности (СОЭБ);
- сервис НЦБ Интерпола (СОДИ);
- сервис экспертно-криминалистической деятельности (ЕАИС ЭКП);
- сервис обеспечения государственной защиты лиц (СУОГЗ);
- сервис оформления проезда сотрудников (СОПС);
- сервис ГУ собственной безопасности МВД (СОПД ГУСБ);
- сервис статистической отчетности (МОСТ);
- банк отпечатков пальцев (ЦИАДИС).

Подсистема поддержки взаимодействия с населением, а также межведомственного взаимодействия с целью предоставления госуслуг включает:

- сервис предоставления госуслуг (СПГУ);
- систему централизованного учета оружия (СЦУО);
- единый банк данных архивной информации (Ретроспектива);
- интегрированный банк данных.

Типизация объектов ИСОД ОВД определяется их функционированием на объектах четырех уровней управления системы ОВД:

• 1 уровень - МВД России;

• 2 уровень - ГУ МВД России по федеральным округам;

• 3 уровень - МВД, ГУВД, УМВД по субъектам Российской Федерации, УВДТ, ОВД на закрытых территориях и режимных объектах;

• 4 уровень - горрайлинорганы внутренних дел.

При этом выделяются стационарные и мобильные типы объектов ИСОД ОВД.

ИСОД ОВД должна взаимодействовать со следующими системами:

- системами ФМС России;
- системами ГКВВ МВД России;
- информационными системами других федеральных органов исполнительной власти (ФОИВ);

- Государственной информационной системой «Правоохранительный портал Российской Федерации» (ГИС ПП РФ);
- Системой удостоверяющих центров МВД России.

В состав ИСОД ОВД входят объекты информатизации следующих типов:

- центры обработки данных (ЦОД ИСОД ОВД);
- стационарные и мобильные объекты ОВД (объекты ОВД);
- интегрированная мультисервисная телекоммуникационная система (ИМТС).

Общая структурная схема ИСОД ОВД и ее взаимосвязи с другими системами представлена на рисунке 5.1.

Центры обработки данных ИСОД ОВД размещаются на 1 и 2 уровнях управления системы ОВД. На 1 уровне управления системы ОВД создаются центры обработки данных - основной (на площадке ФКУ НПО «СТиС» МВД России), резервный (на площадке ФГУП «Гознак»). В центры обработки данных переносятся банки данных ИСОД ОВД.

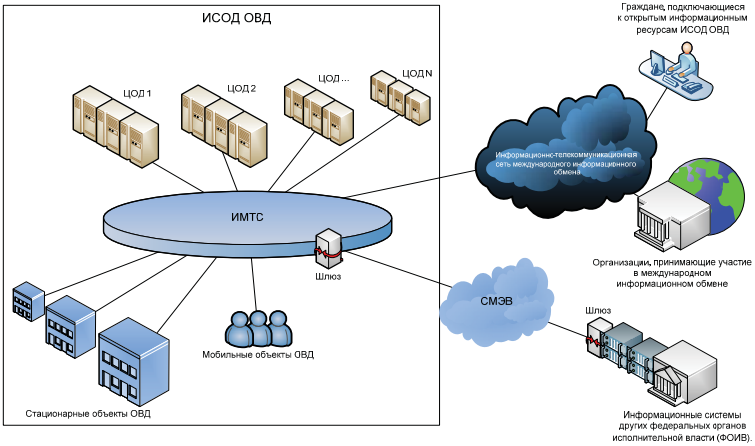

Рис. 5.1. Структурная схема ИСОД ОВД и ее взаимосвязи с другими системами

В состав ЦОД ИСОД ОВД входят следующие элементы:

- транзакционный сегмент;
- сегмент системы хранения данных;
- сегмент системы резервного копирования;
- сегмент сетевой подсистемы;
- сегмент защищенного узла подключения к телекоммуникационной системе;

- аналитический сегмент (для основного ЦОД на площадке ФКУ НПО «СТиС» МВД России);
- сегмент системы резервирования данных (для резервного ЦОД на площадке ФГУП «Гознак»);
- сегмент разработки и тестирования (для резервного ЦОД на площадке ФГУП «Гознак»);
- оборудование администрирования.

Стационарные и мобильные объекты ИСОД ОВД предназначены для обработки информации ИСОД ОВД конечными пользователями.

Стационарные объекты ОВД осуществляют межобъектовое взаимодействие и обмениваются информацией с центрами обработки данных используя проводные каналы связи ИМТС. Соединение стационарных объектов с ИМТС осуществляется через установленные на стационарных объектах ОВД телекоммуникационные узлы.

Мобильные объекты ОВД, которые подключаются к стационарным объектам ОВД 3 уровня управления, взаимодействуют с элементами ИСОД ОВД через беспроводные каналы связи. После установления соединения стационарные объекты ОВД 3 уровня управления, используя свои проводные каналы связи в ИМТС, обрабатывают запрос мобильного объекта ОВД или, при необходимости, передают его на объекты ОВД более высокого уровня.

Информационное взаимодействие между элементами ИСОД ОВД осуществляется через *интегрированную мультисервисную телекоммуникационную систему* (ИМТС). При этом каналы передачи данных между элементами ИСОД ОВД проходят за пределами контролируемых зон объектов информатизации.

ИМТС предназначена для обеспечения органов внутренних дел универсальной транспортной средой на базе единых технологий, схемных решений и наборов типовых программно-аппаратных средств.

Телекоммуникационные узлы ИМТС размещаются в каждом ЦОД ИСОД ОВД и на стационарных объектах ОВД, обеспечивая их взаимодействие.

ИМТС обеспечивает выполнение следующих функций:

- передачи данных;
- телефонной связи;
- телематических служб.

Телематические службы включают:

• службы электронных сообщений в части службы электронной почты (по протоколам SMTP, POP3, IMAP4);

• информационные службы в части службы доменных имен (по протоколу DNS), службы доступа к информационным ресурсам (по протоколам HTTP, FTP);

• службы голосовой связи;

• факсимильные службы;

• службы аудио/видеоконференции;

• службы доступа к информации, хранящейся в электронном виде.

Узлы ИМТС размещены на объектах ИСОД ОВД всех четырех уровней управления ОВД. В состав узла входит: коммутационное оборудование, средства защиты информации осуществляется через узлы ИМТС. При этом данные, поступающие в узел ИМТС, обрабатываются и передаются на объект (с объекта) через коммутационное оборудование. Общая структурная схема ИМТС представлена на рисунке 5.2.

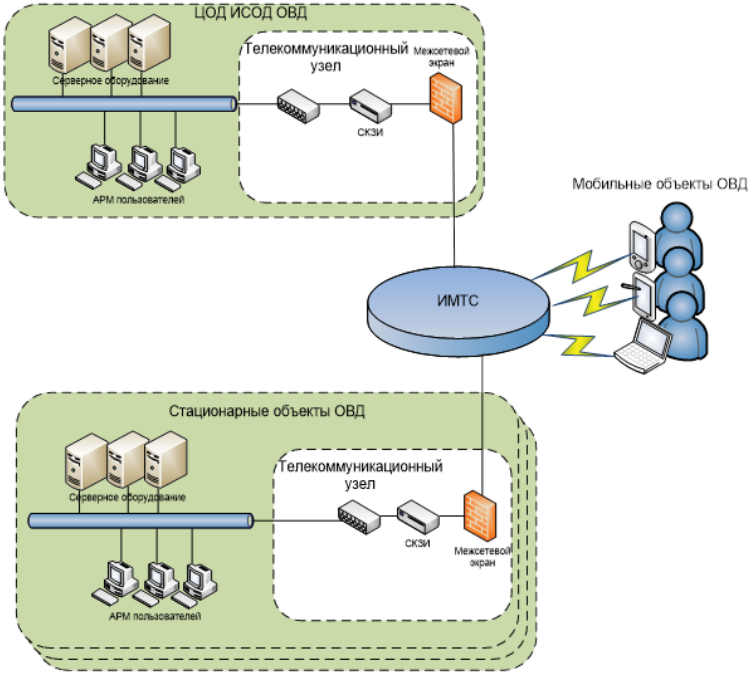

Рис. 5.2. Структурная схема ИМТС

Таким образом, практическая реализация проекта по созданию ИСОД позволяет пользователям этой системы получить:

- единый универсальный механизм доступа и санкционированного получения требуемой информации;
- возможность обеспечения доступа с любого объекта ОВД и любого рабочего места, включая мобильное;
- возможность формирования типовых и специальных запросов;
- возможность одновременного поиска по всем информационным ресурсам;
- существенное сокращение времени обработки запроса и получения информации;
- протоколирование действий.

Также необходимо указать, что реализация технических и технологических решений в рамках системы ИСОД ОВД, в отличие ЕИТКС ОВД, позволяет упростить организационную и техническую инфраструктуру обеспечения централизованного управления, непрерывной работоспособности и технического обслуживания информационно-аналитической системы. К тому же в тенденции устранения территориального разобщенности кроется серьезный экономический потенциал. УМВД России появляется возможность более рационально использовать имеющееся оборудование, осуществив централизацию серверного оборудования.

Основными целями обеспечения информационной безопасности ИСОД ОВД являются:

- предотвращение несанкционированного ознакомления с защищаемой информацией, а также несанкционированного уничтожения, искажения, разглашения, копирования и блокирования информации;
- обеспечение разграничения доступа к информационным ресурсам ИСОД ОВД;
- соблюдение правового режима использования массивов данных и программ обработки информации;
- сохранение возможности управления процессом обработки, хранения и использования информации в условиях несанкционированных воздействий на ИСОД ОВД;
- обеспечение защищенного обмена информацией внутри объектов информатизации и с внешними системами и пользователями.

Защите подлежит информация, обрабатываемая в ИСОД ОВД.

Состав защищаемой информации в ИСОД ОВД определяется Актами категорирования информации и включает в себя следующие типы:

- целевую информацию, включая информацию об объектах учета, информацию подсистемы электронного документооборота, сообщения ведомственной электронной почты;

- технологическую информацию, включая информацию о системе защиты информации.

Целевая информация содержит сведения, отнесенные к информации ограниченного доступа: служебная тайна, согласно Указу Президента Российской Федерации от 6 марта 1997 г. №188 «Об утверждении перечня сведений конфиденциального характера», и персональные данные, в соответствии с Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных».

Источники угроз безопасности информации могут носить как объективный, так и субъективный характер. Все источники угроз безопасности информации делятся на три основные группы:

- обусловленные стихийными факторами;

- обусловленные техническими факторами (техногенные источники угрозы);

- обусловленные действиями субъекта (антропогенные источники угроз).

Источником стихийных угроз является природная среда.

Техногенные источники угроз - источники, определяемые технократической деятельностью человека и развитием цивилизации. Технические средства, являющиеся источниками потенциальных угроз безопасности информации, также могут быть внешними:

- средства связи и передачи данных;

- сети электроснабжения;

- сети водоснабжения и канализации;

- транспорт и т.д.

и внутренними:

- технические средства обработки информации;

- вспомогательные средства (охраны, сигнализации, телефонии);

- другие технические средства, применяемые на объекте информатизации.

Антропогенными источниками угроз безопасности информации выступают субъекты, действия которых могут быть квалифицированы как умышленные или случайные нарушения.

В качестве внутреннего антропогенного источника угроз необходимо рассматривать субъекта, имеющего возможность физического или удаленного доступа к ресурсам ИСОД ОВД.

Угрозы информационной безопасности могут быть направлены и на самих пользователей систем ИСОД ОВД. Эти угрозы могут осуществляться методами подкупа, шантажа, принуждения.

Угрозы информационной безопасности могут быть реализованы нарушителями на разных (одном или нескольких) уровнях и взаимодействия открытых систем (ЭМВОС).

Все физические лица в качестве потенциальных нарушителей применительно к ресурсам ИСОД ОВД могут быть отнесены к следующим категориям:

1. Внешние нарушители (категория I) - лица, не имеющие права доступа в КЗ объектов ОВД, на которых размещаются объекты информатизации ИСОД ОВД.

Внешний нарушитель не имеет непосредственного доступа к ИСОД ОВД и его компонентам, находящимся в пределах контролируемой зоны объектов ОВД. Этот нарушитель может осуществлять атаки только из-за пределов контролируемой зоны объектов ОВД. Внешний нарушитель осуществляет создание способов и подготовку атак с привлечением специалистов, имеющих соответствующий опыт, в том числе в отношении СКЗИ.

Информация, обрабатываемая в ИСОД ОВД, для внешнего нарушителя с возможностями иностранной спецслужбы интереса не представляет.

2. Внутренние нарушители (категория II) - лица, имеющие право постоянного или разового доступа (пропуска) внутрь КЗ объектов ОВД, на которых размещаются объекты информатизации ИСОД ОВД.

Внутренний нарушитель скрывает свои несанкционированные действия от других сотрудников, самостоятельно осуществляет создание методов и средств реализации атак, а также самостоятельно реализует атаки. Внутренний нарушитель также может проводить атаку из-за пределов КЗ объектов ОВД.

6. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ПОДСИСТЕМЫ АНТИВИРУСНОЙ ЗАЩИТЫ В ИСОД ОВД

При проектировании подсистемы антивирусной системы защиты в рамках системы управления информационной безопасностью организации одной из проблем является адекватная оценка угроз, создаваемых различными источниками. Оценить вероятность реализации тех или иных угроз зачастую затруднительно ввиду отсутствия исходных данных и достоверной статистической информации.

Однако приведенные выше экспертные оценки позволяют сделать вывод о том, что для государственных информационных систем, систем правительственных учреждений, посольств, научно-исследовательских центров, военных организаций, компаний нефтегазового сектора и т.д. наиболее остро стоит угроза технических компьютерных разведок, целевых компьютерных атак со стороны иностранных государств и организованных преступных группировок - «кибернаемников», целью которых, чаще всего, является получение доступа к конфиденциальной информации, в том числе к интеллектуальной собственности, а также другой стратегически важной информации либо вывод из строя инфраструктуры.

Исходя из изложенного, можно предположить о применении направленного вектора атаки, именуемого комплексными долговременными угрозами (Advanced Persistent Threats) и позволяющего в некоторой степени обходить ограничение, связанное с непосредственным отсутствием доступа к глобальным информационным сетям.

Указанный вид компьютерных атак возможен в том числе в силу того, что современные информационные системы строятся таким образом, что успешная атака на второстепенный ресурс позволяет злоумышленнику преодолеть периметр защиты и атаковать информационную систему организации изнутри, встречая значительно меньше противодействия со стороны системы защиты. Это общая тенденция частного и государственного секторов: наличие даже одного уязвимого узла на периметре защиты либо внутри системы предоставляет нарушителю техническую возможность получить контроль над всеми информационными ресурсами организации.

С целью недопущения воздействия вредоносного программного обеспечения на информационные системы, в том числе закрытые, необходимо выстраивать и поддерживать актуальную систему управления информационной безопасностью, способную противо-

стоять современным угрозам. Одним из элементов которой, безусловно, является подсистема антивирусной защиты.

Необходимым условием обеспечения эффективной антивирусной защиты корпоративной информационной системы является описание возможностей нарушителя посредством отображения угроз в модели нарушителя антивирусной безопасности.

Рассмотрим модель потенциального нарушителя, исходя из уровня квалификации нарушителя и степени преднамеренности выполняемых действий, оказываемых на защищаемый сегмент ИСОД ОВД.

№	Класс нарушителя	Степень преднамеренности действий нарушителя	Уровень квалификации нарушителя
1	Класс «Н-1»	Непреднамеренные действия	-
2	Класс «Н-2»	Преднамеренные действия	Низкий
3	Класс «Н-3»	Преднамеренные действия	Средний
4	Класс «Н-4»	Преднамеренные действия	Высокий

Нарушители, относящиеся к классу «Н-1», представляют собой рядовых сотрудников, в результате непреднамеренных действий которых может произойти инфицирование автоматизированной системы организации. Примерами таких действий являются скачивание из сети Интернет непроверенных файлов и запуск их на локальном компьютере.

Нарушители класса «Н-2» выполняют преднамеренные действия, однако для проведения вирусной атаки используются известные экземпляры вредоносного кода, а также опубликованные уязвимости программного обеспечения.

Класс нарушителей «Н-3» предполагает наличие у злоумышленника более высокого уровня квалификации, что дает ему возможность использовать вредоносный код, который может детектироваться не всеми антивирусными продуктами.

Нарушители класса «Н-4» являются наиболее опасными и обладают достаточной квалификацией для разработки вредоносного кода, который не обнаруживается антивирусными программными продуктами.

Необходимо отметить, что в рамках описанной модели предполагается, что нарушители «Н-2», «Н-3» и «Н-4» являются внешними по отношению к атакуемой организации и обладают минимумом информации об автоматизированной системе.

В целях защиты от нарушителей класса «Н-1» и «Н-2» достаточно использовать стандартное антивирусное программное обеспечение одного производителя, установив его на все рабочие станции и серверы в компании. Такой подход может применяться для небольших подразделений органов внутренних дел, где обрабатывается небольшой объем конфиденциальной информации.

Для защиты от нарушителя класса «Н-3» необходимо использовать многовендорный вариант антивирусной защиты, который предусматривает применение антивирусных ядер различных производителей. Это позволит существенно повысить вероятность обнаружения вируса за счет того, что каждый файл или почтовое сообщение будет проверяться различными ядрами.

Еще одним преимуществом использования многоядерных антивирусов является более высокая надёжность работы системы антивирусной защиты.

В качестве альтернативы использования нескольких продуктов различных производителей возможно применение программных комплексов, которые включают в себя несколько ядер с единой консолью управления.

Для защиты от нарушителей класса «Н-4» применение одних лишь антивирусных продуктов недостаточно, так как злоумышленники данной категории обладают возможностями создавать вредоносный код, который не обнаруживается антивирусами. Поэтому в дополнении к многовендорной антивирусной защите необходимо использовать подсистему сетевого экранирования, выявления и предотвращения атак, а также обнаружения уязвимостей. Применение данных подсистем позволит существенно снизить риск успешной реализации информационной атаки на информационные ресурсы, размещенные в ИСОД ОВД.

Подсистема сетевого экранирования предназначена для защиты рабочих станций пользователей от возможных сетевых вирусных атак посредством фильтрации потенциально опасных пакетов данных. Подсистема должна обеспечивать возможность фильтрации на канальном, сетевом, транспортном и прикладном уровнях стека TCP/IP. Как правило, данная подсистема реализуется на основе межсетевых и персональных сетевых экранов. При этом межсетевой экран устанавливается в точке подключения АС к сети Интернет, а персональные экраны размещаются на рабочих станциях пользователей.

Подсистема выявления и предотвращения атак предназначена для обнаружения несанкционированной вирусной активности посредством анализа пакетов данных, циркулирующих в АС, а также событий, регистрируемых на серверах и рабочих станциях пользователей. Подсистема дополняет функции межсетевых и персональных экранов за счет возможности более детального контекстного анализа содержимого передаваемых пакетов данных.

Подсистема выявления уязвимостей должна обеспечивать возможность обнаружения технологических и эксплуатационных уязвимостей АС посредством проведения сетевого сканирования. В качестве объектов сканирования могут выступать рабочие станции пользователей, серверы, а также коммуникационное оборудование. Для проведения сканирования могут использоваться как пассивные, так и активные методы сбора информации. По результатам работы подсистема должна генерировать детальный отчет, включающий в себя информацию об обнаруженных уязвимостях, а также рекомендации по их устранению. Совместно с подсистемой выявления уязвимостей в АС может использоваться система управления модулями обновлений общесистемного и прикладного программного обеспечения, установленного в АС. Совместное использование этих систем позволит автоматитировать процесс устранения выявленных уязвимостей путем установки необходимых обновлений на узлы АС (service pack, hotfix, patch и др.).

Подсистема управления антивирусной безопасностью, предназначенная для выполнения следующих функций:

- удаленной установки и деинсталляции антивирусных средств на серверах и рабочих станциях пользователей;
- удаленного управления параметрами работы подсистем защиты, входящих в состав комплексной системы антивирусной защиты;
- централизованного сбора и анализа информации, поступающей от других подсистем. Данная функция позволяет автоматизировать процесс обработки поступающих данных, а также повысить оперативность принятия решений по реагированию на выявленные инциденты, связанные с нарушением антивирусной безопасности.

Описанный выше подход к защите от нарушителей класса «Н-4» целесообразно применять в региональных сегментах ИСОД ОВД, ресурсы которых потенциально могут быть подвержены целевым атакам злоумышленников, реализуемых при помощи вредоносного кода.

Современная антивирусная защита, обеспечивающая безопасность в сложных распределенных информационных системах,

таких как ИСОД ОВД, требует своевременной реакции на возникающие угрозы со стороны вредоносного программного обеспечения. Помимо этого, указанная подсистема должна быть централизованно-управляемой и динамически подстраиваемой под требования и изменения, возникающие на всех этапах жизненного цикла ИСОД.

Согласно положений утвержденной в 2012 году «Базовой моде-ли нарушителя и модели угроз единой системы информационно-аналитического обеспечения деятельности МВД России» с учетом особенностей «облачной архитектуры», для использования в ИСОД ОВД средства антивирусной защиты должны быть сертифицированы в соответствии с утвержденными приказом ФСТЭК Росси от 20 марта 2012 г. № 28 Требованиями к средствам антивирусной защиты, соответствующими методическими документами ФСТЭК России - профилями защиты, правовыми актами ФСБ России.

Как уже отмечалось ранее, в соответствии с вышеупомянутыми Требованиями к средствам антивирусной защиты выделяют следующие типы средств антивирусной защиты:

- тип «А» - средства антивирусной защиты (компоненты средств антивирусной защиты), предназначенные для централизованного администрирования средствами антивирусной защиты, установленными на компонентах информационных систем (серверах, автоматизированных рабочих местах);
- тип «Б» - средства антивирусной защиты (компоненты средств антивирусной защиты), предназначенные для применения на серверах информационных систем;
- тип «В» - средства антивирусной защиты (компоненты средств антивирусной защиты), предназначенные для применения на автоматизированных рабочих местах информационных систем;
- тип «Г» - средства антивирусной защиты (компоненты средств антивирусной защиты), предназначенные для применения на автономных автоматизированных рабочих местах.

Средства антивирусной защиты типа «А» не применяются в информационных системах самостоятельно и предназначены для использования только совместно со средствами антивирусной защиты типов «Б» и(или) «В».

Примерная схема построения антивирусной защиты в информационной системе с применением средств антивирусной защиты разных типов приведена на рисунке 6.1.

Для дифференциации требований к функциям безопасности средств антивирусной защиты выделяются шесть классов защиты средств антивирусной защиты. Самый низкий класс - шестой, самый высокий - первый.

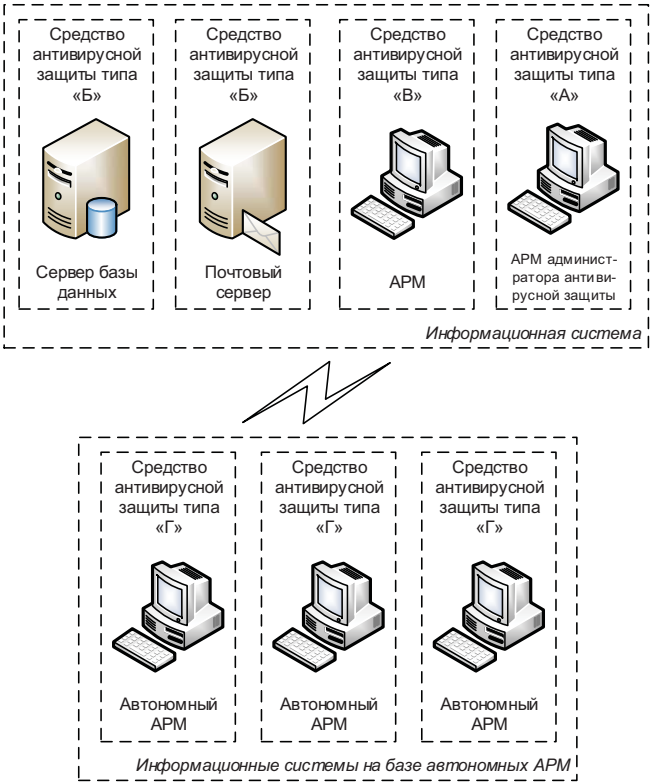

Рис. 6.1. Примерная схема построения антивирусной защиты в информационной системе с применением средств антивирусной защиты разных типов

Средства антивирусной защиты, соответствующие 6 классу защиты, применяются в информационных системах персональных данных 3 и 4 классов.

Средства антивирусной защиты, соответствующие 5 классу защиты, применяются в информационных системах персональных данных 2 класса.

Средства антивирусной защиты, соответствующие 4 классу защиты, применяются в государственных информационных системах, в которых обрабатывается информация ограниченного доступа, не содержащая сведения, составляющие государственную тайну, в информационных системах персональных данных 1 класса, а также в информационных системах общего пользования II класса.

Средства антивирусной защиты, соответствующие 3 классу защиты, применяются в информационных системах, в которых обрабатывается информация, содержащая секретные сведения.

Средства антивирусной защиты, соответствующие 2 классу защиты, применяются в информационных системах, в которых обрабатывается информация, содержащая совершенно секретные сведения.

Средства антивирусной защиты, соответствующие 1 классу защиты, применяются в информационных системах, в которых обрабатывается информация, содержащая сведения особой важности.

С учетом классификации средств антивирусной защиты, структуры ИСОД ОВД и циркулирующей в ней информации, наиболее походящими являются средства, соответствующие 4 классу защиты, применяемые в государственных информационных системах, в которых обрабатывается информация ограниченного доступа, не содержащая сведения, составляющие государственную тайну, в информационных системах персональных данных 1 класса, а также в информационных системах общего пользования II класса.

Проведенный анализ отечественного рынка антивирусных средств при построении подсистемы антивирусной безопасности ИСОД ОВД позволяет сделать выбор в пользу программных продуктов «Лаборатории Касперского», особо принимая во внимание и то обстоятельство, что номенклатура данной компании присутствует в Государственном оборонном заказе и предусматривает поставку средств антивирусной защиты для нужд ОВД.

Система антивирусной защиты «Kaspersky Endpoint Security 10 для Windows» имеет соответствующий сертификат соответствия ФСТЭК России и содержит эффективные инструменты контроля выполнения корпоративных политик безопасности на уровне использования программ, внешних устройств и веб-ресурсов. Эти инструменты снижают риск заражения корпоративной сети, позволяют повысить производительность труда и предотвратить утечку конфиденциальной информации.

Структурно подсистема антивирусной защиты в ИСОД ОВД, как представляется, должна носить централизованный характер. Иными словами, она должна предусматривать наличие единой консоли администрирования, позволяющей эффективно управлять различными аспектами безопасности IT-инфраструктуры. В качестве такого инструмента можно выделить Kaspersky Security Center.

Программа Kaspersky Security Center включает в себя следующие основные компоненты:

• Сервер администрирования. Осуществляет функции централизованного хранения информации об установленных в сети организации программах и управления ими.

• Агент администрирования. Осуществляет взаимодействие между Сервером администрирования и программами «Лаборатории Касперского», установленными на сетевом узле (рабочей станции или сервере). Этот компонент является единым для всех программ, разработанных для систем Microsoft Windows. Для программ «Лаборатории Касперского», разработанных для систем Novel и Unix, существуют отдельные версии Агента администрирования.

• Консоль администрирования. Предоставляет пользовательский интерфейс к административным службам Сервера и Агента. Консоль администрирования выполнена в виде компонента расширения к Microsoft Management Console (MMC). Консоль администрирования позволяет подключаться к удаленному Серверу администрирования через интернет.

• Сервер мобильных устройств. Предоставляет доступ к мобильным устройствам и позволяет управлять ими через Консоль администрирования. Сервер мобильных устройств получает информацию о мобильных устройствах и хранит их профили.

• Kaspersky Security Center Web Console. Предназначена для контроля состояния системы защиты сети организации-клиента, находящейся под управлением Kaspersky Security Center.

Инструмент управления антивирусной защитой Kaspersky Security Center позволяет удаленно устанавливать программные решения на рабочие станции и серверы, настраивать параметры защиты, управлять обновлениями ПО и антивирусных баз, контролировать статус защиты и оперативно реагировать на события. Такие инструменты, как централизованный поиск уязвимостей, поддержка виртуальных сред и иерархическое управление, делают управление системой защиты эффективным.

В единой консоли осуществляется управление безопасностью и защита от известного и нового вредоносного программного обеспечения, предотвращаются риски безопасности и уменьшаются издержки на подсистему антивирусной защиты. Общая схема управления посредством Kaspersky Security Center представлена на рисунке 6.2.

В соответствии с возможностями KSC, возможная структура построения подсистемы антивирусной защиты в ИСОД ОВД может выглядеть следующим образом рисунок 6.3.

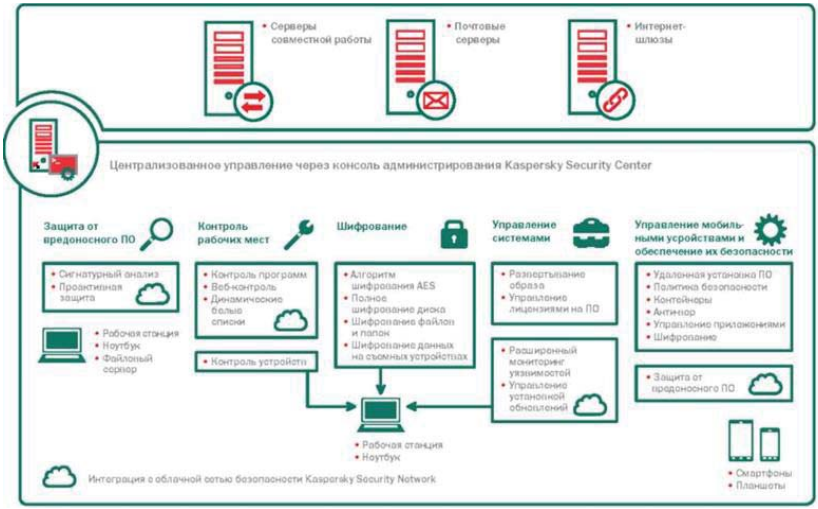

Рис. 6.2. Общая схема управления системой антивирусной защиты посредством Kaspersky Security Center

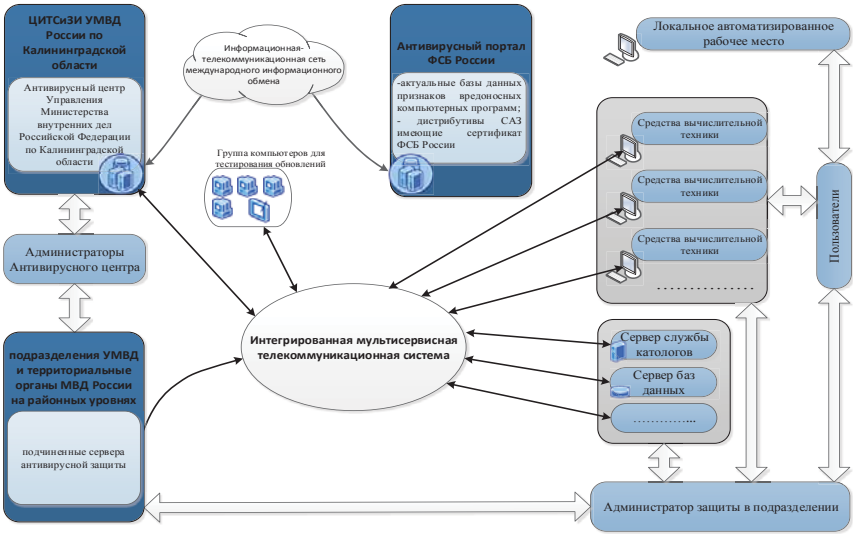

Рис. 6.3. Структура подсистемы антивирусной защиты в ИСОД ОВД

На 1-ом уровне, в соответствии с архитектурой ИСОД ОВД, располагается Антивирусный центр МВД России, который формирует основные политики безопасности, осуществляет распространение ключевых файлов и общее управление подсистемой антивирусной безопасности.

Одновременно с этим Антивирусный центр МВД России осуществляет формирование верифицированных вирусных баз обновления посредством Антивирусного центра ФСБ России и последующую их передачу на подчиненные антивирусные центры (2-ой и 3-ий уровень).

Указанные центры осуществляют общий контроль и управление на заданных уровнях.

Разработанное в рамках исследования Типовое положение о системе антивирусной защиты в региональном управлении Министерства внутренних дел Российской Федерации приведено в приложении к пособию.

Как представляется, описанная структура подсистемы антивирусной защиты в единой системе информационно-аналитического обеспечения деятельности МВД России способна обеспечить своевременную защиту от вирусных угроз, единый контроль и управление, успешную реакцию на возникающие инциденты. Однако для обеспечения заданного уровня информационный безопасности в ИСОД ОВД необходимо создание интегративной системы, объединяющей основные компоненты системы безопасности.

ЗАКЛЮЧЕНИЕ

Проведенное исследование позволило сделать ряд выводов и предложений, имеющих, на наш взгляд, научное и практическое значение для совершенствования деятельности информационно-аналитических подразделений органов внутренних дел, подразделений технической защиты информации МВД России при организации антивирусной защиты служебной информации, хранимой и обрабатываемой в автоматизированных информационных системах.

Данная тема имеет немаловажное значение для продолжения работ по дальнейшей информатизации деятельности органов внутренних дел. На сегодняшний день разработка, внедрение и защита автоматизированных информационных систем является одной из самых важных задач в области информационных технологий. Появляется потребность в использовании новейших технологий передачи информации. Интенсивное использование информационных технологий в настоящее время является фактором, определяющим эффективность деятельности органов внутренних дел по противодействию преступности.

Анализ современных угроз безопасности информационным системам со стороны вредоносного программного обеспечения позволил сделать вывод о том, что риски, связанные с воздействием на корпоративные информационные системы различного рода вредоносного программного обеспечения, являются одной из наиболее актуальных угроз в сфере информационной безопасности. Устоявшейся тенденцией можно считать неуклонный рост количества атак на российские информационные ресурсы, активизацию деятельности иностранных разведок по внедрению в информационные системы органов государственной власти Российской Федерации вредоносных программных средств.

В этой связи вполне закономерна криминализация подобного рода деяний российским уголовным законодательством. Уголовный кодекс Российской Федерации, вступивший в силу в 1997 году, содержит статью 273, предусматривающую ответственность за создание, использование и распространение вредоносных компьютерных программ. В качестве основных критериев отграничения вредоносных программ от другого программного обеспечения можно выделить следующие: уничтожение информации или нарушение работы всей системы; несанкционированная работа; заведомая вредоносность программы. Для того, чтобы утверждение о вредоносности программы было обоснованным и имело бы юридические

последствия, необходимо проведение программно-технической экспертизы.

Все множество вредоносных компьютерных программ условно подразделяется на следующие основные группы: компьютерные вирусы; черви; трояны; другие вредоносные программы. При этом, как показали результаты исследования, к наиболее опасным источникам проникновения этих программ в информационную систему следует отнести: Интернет; электронная почта; уязвимости в программном обеспечении; внешние носители информации; пользователи.

Противодействие угрозам воздействия на компьютерные системы вредоносного программного обеспечения подразумевает принятие целого комплекса мер организационного, технического и программного характера. Однако основой построения подобного рода системы обеспечения антивирусной безопасности выступают различные правовые нормы, определяющие состав этой системы и предъявляемые к ней требования.

Правовую основу защиты информации в корпоративных информационных системах, в том числе и в информационных системах МВД России, составляют положения действующего законодательства Российской Федерации, а также рекомендации международных стандартов. Основные требования российского законодательства, касающегося вопросов защиты компьютерной информации, изложены в общем виде в федеральных законах и уточнены в документах Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности, государственных стандартах, а также других документах.

Правовые нормы выступают своеобразным базисом построения системы антивирусной защиты автоматизированных информационных систем. В плане же практической реализации необходимым условием создания такой системы является использование специальных программ - антивирусов, способных распознавать и обезвреживать вирусы в различных информационных объектах.

Проведенный анализ технологий работы современных средств антивирусной защиты информации, представленных на отечественном рынке, позволил прийти к выводу о том, что в целях построения системы антивирусной защиты корпоративных информационных систем, в том числе и информационных систем органов внутренних дел, должны использоваться программные средства, реализующие как сигнатурные, так и проактивные/эвристические методы обнаружения вредоносных программ. Выбор конкретного

программного решения определяется прежде всего спецификой той информационной системы, защиту которой он должен обеспечивать - ИСОД ОВД.

ИСОД ОВД представляет собой совокупность используемых в Министерстве автоматизированных систем обработки информации, программно-аппаратных комплексов и комплексов программно-технических средств, а также систем связи и передачи данных, необходимых для эффективного обеспечения служебной деятельности МВД России.

Изучение функциональных и технологических характеристик ИСОД ОВД позволило сделать вывод о том, что для построения подсистемы антивирусной защиты наиболее походящими являются антивирусные средства, соответствующие 4 классу защиты, применяемые в государственных информационных системах, в которых обрабатывается информация ограниченного доступа, не содержащая сведения, составляющие государственную тайну, в информационных системах персональных данных 1 класса, а также в информационных системах общего пользования II класса.

Из присутствующих на отечественном рынке антивирусных средств наиболее оптимальных вариантом по соотношению цена/качество является система антивирусной защиты «Kaspersky Endpoint Security 10 для Windows», имеющая соответствующий сертификат ФСТЭК России.

Структурно подсистема антивирусной защиты в ИСОД ОВД должна носить централизованный характер. Иными словами, она должна предусматривать наличие единой консоли администрирования, позволяющей эффективно управлять различными аспектами безопасности IT-инфраструктуры. В качестве такого инструмента был определен Kaspersky Security Center, также сертифицированный ФСТЭК России.

Структурно подсистема антивирусной защиты в ИСОД ОВД должна включать несколько уровней.

На 1-ом уровне, в соответствии с архитектурой ИСОД ОВД, располагается Антивирусный центр МВД России, который формирует основные политики безопасности, осуществляет распространение ключевых файлов и общее управление подсистемой антивирусной безопасности. Одновременно с этим Антивирусный центр МВД России осуществляет формирование верифицированных вирусных баз обновления посредством Антивирусного центра ФСБ России и последующие их передачу на подчиненные антивирусные центры (2-ой и 3-ий уровень). Указанные центры осуществляют общий контроль и управление на заданных уровнях.

Данная структура подсистемы антивирусной защиты в единой системе информационно-аналитического обеспечения деятельности МВД России способна обеспечить своевременную защиту от вирусных угроз, единый контроль и управление, успешную реакцию на возникающие инциденты. Однако для обеспечения заданного уровня информационный безопасности в ИСОД ОВД необходимо создание интегративной системы, объединяющей основные компоненты системы безопасности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Конституция Российской Федерации (в ред. от 21 июля 2014 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

2. Уголовный кодекс Российской Федерации (в ред. от 30 марта 2015 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

3. Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне» (в ред. от 8 марта 2015 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

4. Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (в ред. от 21 декабря 2013 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

5. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» (в ред. от 31 декабря 2014 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

6. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (в ред. от 31 декабря 2014 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

7. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (в ред. от 21 июля 2014 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

8. Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» (в ред. от 30 апреля 2015 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

9. Указ Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникацион-

ных сетей международного информационного обмена» (в ред. от 25 июля 2014 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

10. Указ Президента Российской Федерации от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

11. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 9 сентября 2000 г. № Пр-1895) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

12. Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (утв. Президентом Российской Федерации 12 декабря 2014 г. № К 1274) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

13. Стратегия национальной безопасности Российской Федерации до 2020 года (утв. Указом Президента РФ от 12 мая 2009 г. № 537) (в ред. от 1 июля 2014 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

14. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом РФ 24 июля 2013 г. № ПР-1753) (в ред. от 1 июля 2014 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

15. Положение о сертификации средств защиты информации (утв. постановлением Правительства РФ от 26.06.95 года № 608 «О сертификации средств защиты информации») (в ред. от 21 апреля 2010 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

16. Положение о сертификации средств защиты информации по требованиям безопасности информации (введено в действие приказом Председателя Гостехкомиссии России от 27.10.1995 № 199) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

17. Положение о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну (утв. приказом ФСБ РФ от 13.11.1999 № 564) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

18. Приказ МВД России от 19 сентября 2006 г. № 734 «Об ут-

верждении правил предоставления доступа и использования ресурсов сети «Интернет» в системе МВД России» [Электронный ресурс]. Доступ из СТРАС «Юрист».

19. Приказ МВД России от 6 октября 2008 г. № 070 «Об утверждении временных Правил обеспечения информационной безопасности Единой информационно-телекоммуникационной системе органов внутренних дел» [Электронный ресурс]. Доступ из СТРАС «Юрист».

20. Приказ МВД России от 14 марта 2012 г. № 169 «Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года» [Электронный ресурс]. Доступ изСТРАС «Юрист».

21. Приказ МВД России от 16 января 2012 г. № 25 «Об утверждении Комплекса мер по обеспечению информационной безопасности и защиты данных информационных систем МВД России с учетом реализации «облачной архитектуры» [Электронный ресурс]. Доступ из СТРАС «Юрист».

22. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (утв. приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

23. Требования к средствам антивирусной защиты (утв. приказом ФСТЭК России от 20 марта 2012 г. № 28) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

24. Информационное сообщение Федеральной службы по техническому и экспортному контролю от 30 июля 2012 г. № 240/24/3095 «Об утверждении Требований к средствам антивирусной защиты» [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

25. Порядок проведения классификации информационных систем персональных данных (утв. приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

26. Требования о защите информации, содержащейся в информационных системах общего пользования (утв. приказом ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489) [Электрон-ный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

27. Национальный стандарт РФ ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» (утв. приказом

Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

28. Национальный стандарт РФ ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 374-ст) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

29. Государственный стандарт РФ ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство» (введен в действие постановлением Госстандарта РФ от 14 июля 1998 г. № 295) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

30. Аполлонский А.В., Домбровская Л.А., Примакин А.И., Смирнова О.Г., Основы информационной безопасности в ОВД: учебник для вузов. СПб.: СПбУ МВД РФ, 2010.

31. Атака под цифровым флагом. Regin и другие знаменитые вирусы [Электронный ресурс]. - Режим доступа: http://www.aif.ru/techno/web/1388672.

32. Баин А.М. История развития компьютерной техники: учебное пособие. М.: МИЭТ, 2013. 107 с.

33. Беляев Д.А. Интернет как основа информационного общества // Сборники конференций НИЦ Социосфера. 2011. № 1. С. 9-10.

34. Быков В.М., Черкасов В.Н. Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы: монография. М.: Юрлитинформ, 2015.

35. Быков В.М., Черкасов В.Н. Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы: монография. М.: Юрлитинформ, 2015. С. 163.

36. Владимир Путин провел заседание Совета Безопасности, посвященное вопросам противодействия угрозам национальной безопасности в информационной сфере [Электронный ресурс]. - Режим доступа: http://kremlin.ru/events/president/news/46709.

37. Воронина Ю. Наперегонки с хакерами [Электронный ресурс]. - Режим доступа: http://www.rg.ru/2014/10/28/ubytok-ot-hackerov.html.

38. Вредоносная программа [Электронный ресурс]. - Режим доступа: http://ru.wikipedia.org.

39. Гарнаева М., Чебышев В., Макрушин Д., Унучек Р., Ива-

нов A. Kaspersky Security Bulletin 2014. Основная статистика за 2014 год [Электронный ресурс]. - Режим доступа: https://securelist.ru/analysis/ksb/24580.

40. Глухарев Д.С. Противодействие экстремизму в современном медиапространстве // Вестник Южно-Уральского государственного университета. Серия: Социально-гуманитарные науки. 2012. № 10(269). С. 135-137.

41. Григорьев А.Н. Безопасность в эпоху информатизации: новые угрозы и новые возможности // Материалы XIII Международной конференции «Информатизация и информационная безопасность правоохранительных органов». Москва, 25-26 июня 2004 г. М.: Академия управления МВД России, 2004. С. 26-31.

42. Григорьев А.Н. Основы информационной безопасности в органах внутренних дел: учебное пособие. Калининград: Калининградский филиал СПбУ МВД России, 2014. 224 с.

43. Григорьев А.Н., Мешков В.М. Некоторые аспекты формирования научных основ расследования преступлений, сопряженных с использованием средств компьютерной техники // Библиотека криминалиста. Научный журнал. 2013. № 5. С. 256-264.

44. Григорьев А.Н., Фадеева В.В. Современные технологии защиты компьютерной информации: учебно-практическое пособие. Калининград: Калининградский ЮИ МВД России, 2011. 186 с.

45. Гуров А.И: Угрозы национальной безопасности Российской Федерации и их уголовно-правовое регулирование // Уголовное право в XXI веке: материалы международной научной конференции, состоявшейся на юридическом факультете МГУ им. М.В. Ломоносова (31 мая - 1 июня 2001 г.). М., 2002. С. 12-18.

46. Десятый Конгресс ООН по предупреждению преступности и обращению с правонарушителями. Вена, 10-17 апреля 2000 г. Положение в мире в области преступности и уголовного правосудия. Доклад генерального секретаря A/CONF.187/5.

47. Доступ в Интернет приравняли к базовым правам человека [Электронный ресурс]. - Режим доступа: http://www.km.ru/v-mire/2011/06/07/oon.

48. Защита информации в компьютерных системах / П.В. Костин и др. Н. Новгород: НА МВД России, 2013.

49. Зяблов Д.Н. Использование интернета террористическими организациями в современном мире // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. 2011. № 4-3. С. 42-45.

50. Калинкина Н.Н. Контуры формирования информационного общества в России: информатизация общества и развитие ин-

формационной инфраструктуры // Вестник Нижегородского университета им. Н.И. Лобачевского. 2010. № 3-2. С. 494-499.

51. Кашин С. Вирусные нолики // Коммерсантъ. Секрет Фирмы. 2013. № 10. С. 74.

52. Киберугрозы занимают четвертое место среди самых опасных угроз для мировой экономики [Электронный ресурс]. - Режим доступа: http://www.iso27000.ru/novosti-i-sobytiya.

53. Киберугрозы и информационная безопасность в корпоративном секторе: тенденции в мире и в России [Электронный ресурс]. - Режим доступа: http://www.kaspersky.ru/downloads/pdf/kaspersky_global _it_security_risks_survey.pdf.

54. Кондратьева И.В. Трансформация информационно-коммуникационных технологий в условиях современного общества // Альманах современной науки и образования. 2009. № 7-2. С. 75-77.

55. Конев Ф.Б. История развития компьютерной техники и информационных технологий: учебное пособие. М.: Изд-во МГОУ, 2010. 77 с.

56. Концептуальные основы обеспечения безопасности информации на объектах органов внутренних дел Российской Федерации. Домодедово: ВИПК МВД России, 2013 [Электронный ресурс]. - Режим доступа: http://10.5.0.15/onti/niokr/2013/vp/vp133820.htm.

57. Кривенцов, П.А. Латентная преступность в России: криминологическое исследование: дисс. ... канд. юрид. наук. М., 2014.

58. Лаборатория Касперского. О вирусах: Основные источники проникновения угроз на компьютер [Электронный ресурс]. - Режим доступа: http://support.kaspersky.ru/ viruses#block2.

59. Мамедов Э.Э.О. Роль информационных технологий в эпоху информационного общества на современном этапе // Вопросы новой экономики. 2008. № 1. С. 36-42.

60. Маслакова Е.А. Анализ объективной стороны преступления, связанного с незаконным оборотом вредоносных компьютерных программ // Известия Тульского государственного университета. Экономические и юридические науки. 2008. № 1. С. 226-229.

61. Менжега М.М. Методика расследования создания и использования вредоносных программ для ЭВМ. М.: Юрлитинформ, 2009. 178 с.

62. Мешкова Т.А. Социально-политические аспекты глобальной информатизации // Полит. исследования. 2002. № 6(71). С. 24-33.

63. Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: автореф. дисс. ... д-ра юрид. наук. Воронеж, 2001. 48 с.

64. Основы информационной безопасности в ОВД: курс лекций / А.И. Примакин и др. СПб.: СПбУ МВД России, 2009. 256 с.

65. Нургалиев Р.Г. Электронный патруль. В МВД создали систему защиты кибернетического пространства // Российская газета. 2009. 16 окт.

66. Пастоев А. Методологии управления ИТ-рисками // Открытые системы. 2006. № 8. С. 18-23.

67. Патрушев рассказал о внедрении разведками вирусов в информационные системы госвласти [Электронный ресурс]. - Режим доступа: http://vz.ru/news/2015/7/8/755034.print.html.

68. По оценкам экспертов ежесекундно жертвами киберпреступников становятся 12 человек в мире [Электронный ресурс]. - Режим доступа: http://mvd.ru/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii/Publikacii_i_vistuplenija/item/1951798.

69. Пригоров К.Ф. История развития ЭВМ. Концепции и этапы. М.: Лаборатория Книги, 2008. 227 с.

70. Путин: ФСБ в 2014 году пресекла деятельность 209 агентов иностранных спецслужб [Электронный ресурс]. - Режим доступа: http://vz.ru/news.

71. Российский рынок антивирусов находится в стагнации [Электронный ресурс]. - Режим доступа: http://www.dailycomm.ru.

72. Сало И.А. О понятии «ЭВМ» применительно к статье 272 УК РФ // Криминалистъ. 2011. № 8. С. 34-37.

73. Ситуация на рынке антивирусов в России [Электронный ресурс]. - Режим доступа: http://www.ecomyzone.com.

74. Старостенко И.Н., Сопильняк Ю.Н. Выявление и предупреждение угроз безопасности информационных ресурсов органов внутренних дел, связанных с внедрением и распространением вредоносного программного обеспечения. Краснодар: КрУ МВД России, 2012 [Электронный ресурс]. - Режим доступа: http://10.5.0.15/onti/niokr/2013/kr/kr132403.htm.

75. Тенденции развития преступности в области высоких технологий 2014 [Электронный ресурс]. - Режим доступа: http://report2014.group-ib.ru/.

76. Технология разработки программного обеспечения / Гагарина Л.Г. и др. М.; Форум, 2013. 399 с.

77. Трегубова В.М., Оводкова Т.А., Мялкина А.Ф. Глобальная сеть в России: проблемы и перспективы // Социально-экономические явления и процессы. 2014. № 4(62). С. 101-105.

78. Федотов Н.Н. Форензика - компьютерная криминалистика. М.: OneBook.ru, 2012. 418 с.

79. Хорев П.Б. Программно-аппаратная защита информации:

учебное пособие. - 2-е изд., испр. и доп. М.: Форум, 2015. 349 с.

80. Частиков А.П. Архитекторы компьютерного мира. СПб: БВХ-Петербург, 2002. 383 с.

81. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. М.: Форум, 2012. 415 с.

82. Шляпкин А.В. Методы и средства противодействия атакам на компьютерные сети // Информационные системы и технологии: управление и безопасность. 2014. № 3. С. 325-330.

83. Шогенов Т.К. Вопросы обеспечения безопасности персональных данных в информационных системах МВД России// Информационные технологии, связь и защита информации МВД России. М., 2012. С. 98-101.

84. World Internet Users and Population Stats [Электронный ресурс]. - Режим доступа: http://www.internetworldstats.com/stats.htm.

Приложение

ТИПОВОЕ ПОЛОЖЕНИЕ О СИСТЕМЕ АНТИВИРУСНОЙ ЗАЩИТЫ В РЕГИОНАЛЬНОМ УПРАВЛЕНИИ МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

I. Общие положения

1. Положение о системе антивирусной защиты в региональном Управлении Министерства внутренних дел Российской Федерации[1] (далее - Положение) разработано в соответствии с Федеральным законом от 07.02.2011 № 3-ФЗ «О полиции», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Доктриной информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации 09.09.2000 № 1895, Положением о государственной системе защиты информации в Российской Федерации от иностранной технической разведки и от ее утечки по техническим каналам, утвержденным постановлением Совета Министров - Правительства Российской Федерации от 15.09.1993 № 912-51, «Требованиями к средствам антивирусной защиты», утвержденных приказом ФСТЭК России от 20.03.2012 № 28.

2. Настоящее Положение определяет: организационную структуру системы антивирусной защиты в УМВД, единый порядок оснащения, интеграции и обновление средств и/или систем антивирусной защиты; порядок эксплуатации средств антивирусной защиты[2]; распределение обязанностей для подразделений системы УМВД и территориальных органов МВД России на районном уровне в области обеспечения антивирусной защиты.

3. САЗ являются элементом систем защиты информации информационных систем УМВД, функционирующих на базе СВТ, и применяются совместно с другими средствами защиты информации от несанкционированного доступа к информации, обрабатываемой в информационных системах.

4. Мероприятия по антивирусной защите являются составной частью комплекса мероприятий по защите информации в УМВД.

5. К использованию в информационных системах и автоматизированных рабочих местах УМВД, допускаются только лицензионные средства антивирусной защиты, сертифицированные ФСБ России или имеющие положительное заключение 8 Центра ФСБ России, имеющие сертификат ФСТЭК России с указанием соответствующего класса защиты.

6. САЗ должны обеспечивать нейтрализацию угроз безопасности информации, связанных с внедрением в информационные системы

[1] Далее - «УМВД».
[2] Далее - «САЗ».

из информационно-телекоммуникационных сетей, в том числе доступ к которым не ограничен определенным кругом лиц, и/или со съемных машинных носителей информации компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации (далее - вредоносные компьютерные программы (вирусы)).

7. Задачами системы антивирусной защиты являются:

- определение состава и регламента запуска средств антиви-русной защиты, регламента их ревизии и обновления базы данных признаков вредоносных компьютерных программ (вирусов);

- проведение профилактических работ с применением средств антивирусной защиты;

- непрерывное обеспечение защиты информации от действия вредоносных компьютерных программ (вирусов) на всех этапах эксплуатации информационных систем УМВД;

- осуществление мониторинга сетевой активности, в том числе мониторинга компьютерных атак.

8. Средства антивирусной защиты должны устанавливаться и эксплуатироваться на всех СВТ, участвующих в процессе обработки, передачи и хранения информации в ведомственных сетях УМВД.

9. Требования Положения обязательны для выполнения всеми должностными лицами и работниками подразделений системы УМВД, где используются автоматизированная обработка информации с применением средств вычислительной техники.

II. Состав и организационная структура системы антиви-русной защиты

10. Организационная структура системы антивирусной защиты в УМВД включает:

- ЦИТСиЗИ УМВД[1], на базе которого развернут и функционирует антивирусный центр УМВД;

- подразделения системы УМВД и территориальные органы МВД России на районном уровне, подчиненные УМВД , на базе которых функционируют подчиненные сервера антивирусной защиты;

- должностных лиц подразделения технической защиты информации ЦИТСиЗИ, назначенных администраторами антивирусного центра;

- должностные лица подразделений системы УМВД и территориальных органов, назначенных администраторами защиты в подразделении;

- должностные лица подразделений системы УМВД и территориальных органов - пользователей СВТ.

11. Техническая составляющая, системы антивирусной защиты в УМВД, включает:

[1] Далее - «ЦИТСиЗИ».

- различные сервера, обеспечивающие доступность информационных ресурсов УМВД;
- СВТ, подключенные к интегрированной мультисервисной телекоммуникационной сети ;
- группы СВТ, предназначенных для тестирования выходящих обновлений;
- локальные СВТ, не имеющие подключения к ИМТС.

12. ЦИТСиЗИ, осуществляет:
- планирование мероприятий по антивирусной защите информации;
- планирование оснащения подразделений УМВД САЗ;
- ежегодное продление лицензий САЗ, определение потребностей и обеспечение поставки новых лицензий САЗ;
- организацию контроля состояния антивирусной защиты в структурных подразделениях системы УМВД и территориальных органов;
- формирование единой антивирусной политики в УМВД;
- организацию проверок по фактам заражения компьютерными вирусами автоматизированных систем обработки информации, СВТ и т.д.;
- организацию проверок по фактам зарегистрированных сетевых атак на информационные системы, СВТ и т.д.;
- подготовку ежеквартального отчета по состоянию антивирусной защиты в УМВД.

13. Администраторами антивирусного центра УМВД, осуществляется:
- организация и сопровождение эксплуатации системы антивирусной зашиты;
- управление конфигурацией и логической структурой всего программного обеспечения системы антивирусной защиты;
- реализация установленной единой политики антивирусной защиты в УМВД;
- техническая поддержка администраторов защиты и пользователей подразделений системы УМВД и территориальных органов;
- организация методической и практической помощи администраторам защиты и пользователям подразделений системы УМВД и территориальных органов по установке, настойке и работе с САЗ;
- ежесуточное обновление баз данных признаков вредоносных компьютерных программ антивирусного центра;
- обеспечение своевременного удаленного обновления баз дан ных признаков вредоносных компьютерных программ и версий антивирусного программного обеспечения на СВТ, имеющих подключение к антивирусному центру УМВД;
- своевременная установка актуальных лицензионных ключей для серверов и рабочих станций, имеющих подключение к антивирусному центру УМВД;
- своевременная передача необходимого количества файлов-лицензий САЗ, в подразделения системы УМВД и территориальные органы, при отсутствии подключения СВТ к ИМТС;

- обеспечение контроля за состоянием САЗ в подразделениях УМВД и территориальных органов, средствами антивирусного центра;

- мониторинг сетевой активности, в том числе мониторинг компьютерных атак;

- своевременное блокирование СВТ, распространяющих вредоносное программного обеспечения и осуществляющих компьютерные атаки;

- выявление СВТ не имеющих установленных САЗ и подключенных к ИМТС;

- создание, соответствующих требованиям информационной безопасности, дистрибутивов антивирусных программ и обеспечение регламентированного доступа к ним.

14. Должностными лицами подразделений системы УМВД, назначенных администраторами защиты, начальниками структурных подразделений системы УМВД и территориальных органов, во взаимодействии с администраторами антивирусного центра УМВД, осуществляется:

- установка и настройка подчиненных серверов антивирусной защиты в соответствующих подразделениях системы УМВД и территориальных органах (при необходимости);

- установка на СВТ сотрудников системы УМВД и территориальных органов САЗ и осуществление их первичной настройки;

- контроль за состоянием автоматического обновления баз данных признаков вредоносных компьютерных программ на серверах и СВТ, эксплуатируемых в подразделениях системы УМВД и территориальных органах, и имеющих подключение к антивирусному центру УМВД;

- обновление баз данных признаков вредоносных компьютерных программ на локальных СВТ, эксплуатируемых в подразделениях системы УМВД и территориальных органах, не имеющих доступа к антивирусному центру УМВД, посредством ИМТС;

- обучение пользователей правилам работы с САЗ;

15. Пользователи, во взаимодействии с администраторами защиты, осуществляют контроль актуальности и обновление баз данных признаков вредоносных компьютерных программ САЗ на эксплуатируемых СВТ.

III. Обязанности должностных лиц подразделений УМВД и территориальных органов МВД России на районном уровне, подчиненных УМВД

16. Начальник отдела технической защиты информации ЦИТСиЗИ, осуществляет непосредственное руководство проведением работ по антивирусной защите в УМВД и несет персональную ответственность за организацию и контроль выполнения требований настоящего Положения.

17. Практическое выполнение мероприятий антивирусного контроля, управление и соблюдение требований настоящего Положения

осуществляют администраторы антивирусного центра УМВД, назначаемые соответствующим распоряжением, с обязательным отражением обязанностей в должностной инструкции.

18. Практическое выполнение мероприятий по организации антивирусной защиты в подразделениях УМВД и территориальных органах, осуществляет должностное лицо, назначенное распоряжением администратором защиты.

19. Администраторы защиты, в конкретном подразделении системы УМВД или территориальном органе, несут ответственность:

- за своевременную установку САЗ на СВТ, осуществляющие автоматизированную обработку информации, в подразделении;
- за соблюдение установленной политики антивирусной защиты информации в подразделении;
- за своевременное обновление лицензионных ключей САЗ в подразделении;
- за своевременное обновление антивирусных баз САЗ на СВТ.

20. Непосредственную ответственность за соблюдение установленных норм обеспечения антивирусной безопасности на своих рабочих местах несут пользователи.

IV. Порядок развертывания, применения и обновления баз данных признаков вредоносных компьютерных программ средств антивирусной защиты в подразделениях УМВД и территориальных органов МВД России на районном уровне.

21. САЗ устанавливаются на выделенный сервер или СВТ с техническими характеристиками, уровень которых не ниже требова-ний, указанных в программной и эксплуатационной документации на САЗ.

22. Созданные и вновь создаваемые серверы администрирования антивирусной защиты, подчиняются антивирусному центру. Согласование взаимодействия серверов администрирования с антивирусным центром, осуществляется при участии администраторов антивирусного центра

23. Администраторы антивирусного центра, формируют специальные инсталляционные пакеты, включающие в себя средства антивирусной защиты, настройки доступа к базам обновления, а также политики антивирусной безопасности. Данные пакеты располагаются на веб-портале ЦИТСиЗИ в сегменте ИМТС.

24. Администраторами антивирусного центра, оказывается техническая поддержка администраторам защиты и пользователям по вопросам установки, настройки и эксплуатации САЗ.

25. При необходимости устанавливать САЗ на большое количество локальных СВТ не имеющих подключения к ИМТС, администраторами центра организуется работа по передаче необходимого количество файлов лицензий, а также верифицированных дистрибутивов антивирусного программного обеспечения в соответствующие подразделение.

26. Продление лицензий САЗ, осуществляется автоматически при наличии подключения к антивирусному центру.

27. Передача полученных файлов-лицензий САЗ на объекты, не входящие в систему подразделений УМВД, запрещена.

28. Обновление СВТ и подчиненных серверов антивирусной защиты, осуществляется автоматически, по каналам ИМТС, не реже одного раза в сутки.

29. Обновление антивирусных баз САЗ на автоматизированных рабочих местах, установленных локально в структурных подразделениях УМВД и территориальных органах, производится не реже одного раза в неделю. Порядок получения и установки обновлений определяется Инструкцией.

30. Проверка СВТ на наличие вирусов, осуществляется не реже одного раза в неделю.

ГРИГОРЬЕВ А.Н.,
МУСКАТИНЬЕВ А.Ю., ИВАНОВ П.Ю.

ОРГАНИЗАЦИЯ АНТИВИРУСНОЙ ЗАЩИТЫ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

УЧЕБНОЕ ПОСОБИЕ

Корректор - Артамонова Е.В.
Технический редактор,
компьютерная верстка
оригинал-макета - Удальцова Е.В.

Сдано в набор - 11.05.2016. Подписано в печать - 24.05.2016.
Формат 60x90 1/16.
Тираж - 100 экз. Объем - 6,75 усл. п.л. Заказ № 245.

Научно-исследовательское и редакционно-издательское отделение
Калининградского филиала
Санкт-Петербургского университета МВД России.
Тираж изготовлен на участке оперативной полиграфии
Калининградского филиала
Санкт-Петербургского университета МВД России.
236006, г. Калининград, ул. Ген. Галицкого, 30.

© Калининградский филиал СПбУ МВД России, 2016.