Министерство образования Республики Беларусь

Учреждение образования
«Гомельский государственный технический
университет имени П. О. Сухого»

Кафедра «Промышленная электроника»

Е. А. Храбров

ОСНОВНЫЕ ЗАЩИТЫ ИНФОРМАЦИИ

ПОСОБИЕ
по одноименному курсу для студентов специальности
1-36 04 02 «Промышленная электроника»
дневной и заочной форм обучения
В 2 частях
Часть 1

Электронный аналог печатного издания

Гомель 2009

УДК 004.056.5(075.8)
ББК 32.973-018.2я73
Х88

Рекомендовано к изданию научно-методическим советом факультета автоматизированных и информационных систем ГГТУ им. П. О. Сухого
(*протокол № 10 от 30.06.2008 г.*)

Рецензент: зав. каф. «Математика и информационные технологии» Гомельского филиала «Международного института трудовыхи социальных отношений» канд. техн. наук, доц. *В. П. Кудин*;
канд. техн. наук доц. каф. «Автоматизированный электропривод» ГГТУ им. П. О. Сухого *М. Н. Погуляев*

Храбров, Е. А.

Х88 Основы защиты информации : пособие по одноим. курсу для студентов специальности 1-36 04 02 «Промышленная электроника» днев. и заоч. форм обучения. В 2 ч. Ч. 1 / Е. А. Храбров. – Гомель : ГГТУ им. П. О. Сухого, 2009. – 52 с. – Систем. требования: PC не ниже Intel Celeron 300 МГц ; 32 Mb RAM ; свободное место на HDD 16 Mb ; Windows 98 и выше ; Adobe Acrobat Reader. – Режим доступа: http://lib.gstu.local. – Загл. с титул. экрана.

ISBN 978-985-420-866-4.

Рассмотрены основы правовых и организационных методов защиты информации, основы криптоанализа данных; приведены краткие технические характеристики некоторых устройств, предназначенных для защиты информации.

Для студентов специальности 1-36 04 02 «Промышленная электроника» дневной и заочной форм обучения.

УДК 004.056.5(075.8)
ББК 32.973-018.2я73

ISBN 978-985-420-866-4

ВВЕДЕНИЕ

Учебным планом подготовки по специальности 1-36 04 02 «Промышленная электроника» установлена дисциплина «Основы защиты информации».

Целью учебной дисциплины является подготовка студентов по основным направлениям современной теории кодирования и защиты информации в системах различного назначения от случайных и преднамеренных воздействий, приводящих к искажению, уничтожению или утечке информации, а также навязыванию ложной информации или ложных режимов работы; привитие навыков самостоятельного проектирования новой техники, обеспечивающей защиту информации.

В результате изучения дисциплины обучаемый должен:

знать:

– основы правового и нормативного обеспечения защиты информации;

– организационные и технические методы защиты информации;

– активные и пассивные мероприятия по защите информации и средства их реализации;

– основы криптологии;

– технические каналы утечки информации, их обнаружение и обеспечение информационной безопасности;

уметь:

– проводить анализ вероятных угроз информационной безопасности для заданных объектов;

– определять возможные каналы утечки информации;

– обоснованно выбирать методы и средства блокирования каналов утечки информации;

– качественно оценивать алгоритмы, реализующие криптографическую защиту информации, процедуры аутентификации и контроля целостности;

– разрабатывать рекомендации по защите объектов различного типа от несанкционированного доступа.

1. Системная и правовая методология защиты информации

Основные понятия и терминология, классификация угроз информационной безопасности, классификация методов защиты информации, организационные методы защиты информации: государствен-

ное регулирование в области защиты информации рассмотрены в [1], [2], [3]. Указ Президента Республики Беларусь 20.04.2007 № 195 касается вопросов обеспечения защиты государственных секретов.

Проектом закона Республики Беларусь «Об информации, информатизации и защите информации» регулируются общественные отношения, возникающие при: реализации права на осуществление поиска, передачу, получение, хранение, обработку, использование, распространение и (или) предоставление информации, в том числе информационных ресурсов (далее, если не определено иное, – информация); создании и использовании информационных технологий, информационных систем и информационных сетей (далее – информационные технологии, системы и сети); оказании информационных услуг; организации и обеспечении защиты информации.

В этом проекте закона приведены следующие основные термины и их определения:

– *база данных* – совокупность структурированной и взаимосвязанной информации, организованной по определенным правилам на материальных носителях;

– *банк данных* – организационно-техническая система, включающая одну или несколько баз данных и систему управления ими;

– *владелец программно-технических средств*, *информационных систем и сетей* – государственный орган (организация), гражданин, индивидуальный предприниматель или юридическое лицо, осуществляющие владение и пользование программно-техническими средствами, информационными системами и сетями и реализующие полномочия распоряжения в пределах, установленных законом или договором;

– *государственная информационная система* – информационная система, создаваемая и (или) приобретаемая за счет средств республиканского или местных бюджетов, государственных внебюджетных фондов, а также средств государственных юридических лиц;

– *государственные информационные ресурсы* – информационные ресурсы, создаваемые и (или) приобретаемые за счет средств республиканского или местных бюджетов, государственных внебюджетных фондов, а также средств государственных юридических лиц;

– *документированная информация* (*документ*) – информация, зафиксированная на материальном носителе с реквизитами, позволяющими ее идентифицировать;

– *доменное имя* – символьное (буквенно-цифровое) обозначение, сформулированное в соответствии с правилами адресации информа-

ционной сети, которому назначается определенный сетевой адрес или группа адресов;

– *доступ к информации* – возможность получения информации, в том числе информационных ресурсов, и ее (их) использования;

– *защита информации* – комплекс правовых, организационных и технических мер, направленных на обеспечение целостности (неизменности), конфиденциальности, доступности и сохранности информации от неправомерного (несанкционированного) доступа, уничтожения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении защищаемой информации;

– *информатизация* – организационный, социально-экономический и научно-технический процесс создания и развития единого информационного пространства Республики Беларусь как совокупности взаимосвязанных информационных ресурсов, информационных систем и информационных сетей, обеспечивающих условия для реализации информационных отношений;

– *информация* – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их предоставления;

– *информация*, *распространение и* (*или*) *предоставление которой ограничено*, – информация, доступ к которой ограничен законодательством Республики Беларусь либо ее обладателем в соответствии с законодательными актами Республики Беларусь;

– *информация*, *распространение и* (*или*) *предоставление которой запрещено*, – информация, доступ к которой запрещен законодательством Республики Беларусь либо ее обладателем в соответствии с законодательными актами Республики Беларусь;

– *информационная система* – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и комплекса программно-технических средств;

– *информационная система ограниченного доступа* – информационная система, содержащая информацию, распространение и (или) предоставление которой ограничено;

– *информационная сеть* – комплекс программно-технических средств, предназначенный для передачи информации по сетям электросвязи и обеспечения доступа к информации;

– *информационная услуга* – деятельность по осуществлению поиска, получения, хранения, обработки, распространения и (или) предоставления информации;

– *информационные ресурсы* – отдельные документы и отдельные массивы документов, документы и массивы документов в ин-

формационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);

– *информационный посредник* – гражданин, индивидуальный предприниматель или юридическое лицо, предоставляющие информационные услуги обладателям и (или) пользователям информации;

– *информационные отношения* – отношения, возникающие в процессе сбора, осуществления поиска, передачи, получения, хранения, обработки, накопления, использования, распространения и (или) предоставления информации, а также ее защиты с использованием информационных технологий, систем и сетей;

– *информационные технологии* – совокупность процессов, методов осуществления поиска, передачи, получения, хранения, обработки, использования, распространения и (или) предоставления информации;

– *комплекс программно-технических средств* – совокупность программных и технических средств, обеспечивающих осуществление информационных процессов;

– *конфиденциальность информации* – требование не допускать предоставление и (или) распространение информации без согласия ее обладателя или иного основания, предусмотренного законодательными актами Республики Беларусь;

– *негосударственная информационная система* – информационная система, создаваемая и (или) приобретаемая за счет средств граждан и (или) негосударственных юридических лиц;

– *негосударственные информационные ресурсы* – информационные ресурсы, формирование и использование которых осуществляется гражданами и (или) негосударственными юридическими лицами;

– *обладатель информации*, *информационных технологий* – государственный орган (организация), гражданин или юридическое лицо, создавший (создавшее) информацию или получивший (получившее) предусмотренные настоящим Законом права обладателя информации на основании акта законодательства Республики Беларусь или договора;

– *общедоступная информация* – информация, распространение и (или) предоставление которой не ограничено;

– *общедоступная информационная система* – информационная система, содержащая информационные ресурсы, которые предоставляются и (или) распространяются их обладателем без указания условий их использования, а также информационные ресурсы, распространение и (или) предоставление которых является свободным и не зависит от формы и способа их распространения и (или) предоставления;

– *оператор информационной системы* – юридическое лицо, индивидуальный предприниматель, осуществляющие эксплуатацию информационной системы;

– *официальный сайт государственного органа* (*организации*) – сайт, содержащий информацию о государственном органе (организации) и созданный по его (ее) решению;

– *персональные данные* – совокупность документированной информации о гражданине, позволяющей его идентифицировать;

– *предоставление информации* – действия, направленные на ознакомление с информацией определенного круга лиц;

– *пользователь информации*, *информационных систем и сетей* – государственный орган (организация), гражданин, индивидуальный предприниматель или юридическое лицо, получившие доступ к информации, информационным системам и сетям в порядке, установленном законодательством Республики Беларусь либо по договору сторон, реализующие в соответствии с настоящим Законом и иными актами законодательства Республики Беларусь право на получение и использование информации, информационных систем и сетей;

– *профессиональная тайна* – информация о третьих лицах, полученная гражданами при исполнении их профессиональных (трудовых, служебных) обязанностей;

– *публичная информация* – информация о деятельности государственных органов (организаций), юридических лицах, а также о принимаемых ими решениях, которую они обязаны распространять и (или) предоставлять в случаях и в порядке, установленных законодательством Республики Беларусь;

– *распространение информации* – действия, направленные на ознакомление с информацией неопределенного круга лиц;

– *собственник программно-технических средств*, *информационных систем и сетей* – государственный орган (организация), гражданин или юридическое лицо, реализующие права владения, пользования и распоряжения информационными системами и сетями;

– *сайт* – информационный ресурс, размещенный в информационной сети, по определенному сетевому адресу в совокупности с исключительным правом на использование доменного имени, баз данных и компьютерных программ, посредством которых обеспечивается доступ к такому информационному ресурсу;

– *сетевой адрес* – адрес нахождения информации в информационной сети;

– *сеть Интернет* – глобальная (международная) информационная сеть общего пользования;

– *техническая защита информации* – обеспечение защиты информации, содержащей сведения, составляющие государственные секреты или иные сведения, охраняемые в соответствии с законодательством Республики Беларусь, от утечки по техническим каналам, несанкционированных и непреднамеренных воздействий;

– *электронное сообщение* – текстовая, графическая, аудиовизуальная или иная информация, предназначенная для передачи и получения в электронном виде в информационных системах.

В данном проекте определены также объекты и субъекты информационных отношений, виды информации и порядок ее предоставления и распространения, а также вопросы защиты информации.

2. Виды умышленных угроз безопасности информации и борьба с ними

Пассивные угрозы направлены в основном на несанкционированное использование информационных ресурсов информационных систем (ИС), не оказывая при этом влияния на ее функционирование. Например, несанкционированный доступ к базам данных, прослушивание каналов связи и т. д.

Активные угрозы имеют целью нарушение нормального функционирования ИС путем целенаправленного воздействия на ее компоненты. К активным угрозам относятся, например, вывод из строя компьютера или его операционной системы, разрушение ПО компьютеров, нарушение работы линий связи и т. д. Источником активных угроз могут быть действия взломщиков, вредоносные программы и т. п.

Умышленные угрозы подразделяются также на *внутренние* (возникающие внутри управляемой организации) и *внешние.*

Внутренние угрозы чаще всего определяются социальной напряженностью и тяжелым моральным климатом.

Внешние угрозы могут определяться злонамеренными действиями конкурентов, экономическими условиями и другими причинами (например, стихийными бедствиями). По данным зарубежных источников, получил широкое распространение *промышленный шпионаж* – это наносящие ущерб владельцу коммерческой тайны незаконные сбор, присвоение и передача сведений, составляющих коммерческую тайну, лицом, не уполномоченным на это ее владельцем.

К основным угрозам безопасности информации и нормального функционирования информационных систем (ИС) относятся:

– утечка конфиденциальной информации;

– компрометация информации;

– несанкционированное использование информационных ресурсов;

– ошибочное использование информационных ресурсов;

– несанкционированный обмен информацией между абонентами;

– отказ от информации;

– нарушение информационного обслуживания;

– незаконное использование привилегий.

Утечка конфиденциальной информации – это бесконтрольный выход конфиденциальной информации за пределы ИС или круга лиц, которым она была доверена по службе или стала известна в процессе работы. Эта утечка может быть следствием:

– разглашения конфиденциальной информации;

– ухода информации по различным, главным образом техническим, каналам;

– несанкционированного доступа к конфиденциальной информации различными способами.

Разглашение информации ее владельцем или обладателем есть умышленные или неосторожные действия должностных лиц и пользователей, которым соответствующие сведения в установленном порядке были доверены по службе или по работе, приведшие к ознакомлению с ним лиц, не допущенных к этим сведениям.

Возможен *бесконтрольный уход конфиденциальной информации* по визуально-оптическим, акустическим, электромагнитным и другим каналам.

Несанкционированный доступ – это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым сведениям.

Наиболее распространенными путями несанкционированного доступа к информации являются:

– перехват электронных излучений;

– принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции несущей;

– применение подслушивающих устройств (закладок);

– дистанционное фотографирование;

– перехват акустических излучений и восстановление текста принтера;

– копирование носителей информации с преодолением мер защиты;

– маскировка под зарегистрированного пользователя;

– маскировка под запросы системы;

– использование программных ловушек;

– использование недостатков языков программирования и операционных систем;

– незаконное подключение к аппаратуре и линиям связи специально разработанных аппаратных средств, обеспечивающих доступ информации;

– злоумышленный вывод из строя механизмов защиты;

– расшифровка специальными программами зашифрованной информации;

– информационные инфекции.

Перечисленные пути несанкционированного доступа требуют достаточно больших технических знаний и соответствующих аппаратных или программных разработок со стороны взломщика. Например, используются технические каналы утечки – это физические пути от источника конфиденциальной информации к злоумышленнику, посредством которых возможно получение охраняемых сведений. Причиной возникновения каналов утечки являются конструктивные и технологические несовершенства схемных решений либо эксплуатационный износ элементов. Все это позволяет взломщикам создавать действующие на определенных физических принципах преобразователи, образующие присущий этим принципам канал передачи информации – канал утечки.

Однако есть и достаточно примитивные пути несанкционированного доступа:

– хищение носителей информации и документальных отходов;

– инициативное сотрудничество;

– склонение к сотрудничеству со стороны взломщика;

– выпытывание;

– подслушивание;

– наблюдение и другие пути.

Любые способы утечки конфиденциальной информации могут привести к значительному материальному и моральному ущербу как для организации, где функционирует ИС, так и для ее пользователей.

Существует и постоянно разрабатывается огромное множество вредоносных программ, цель которых – порча информации в БД и ПО

компьютеров. Большое число разновидностей этих программ не позволяет разработать постоянных и надежных средств защиты против них.

Вредоносные программы классифицируются следующим образом: *Логические бомбы*, как вытекает из названия, используются для искажения или уничтожения информации, реже с их помощью совершаются кража или мошенничество. Манипуляциями с логическими бомбами обычно занимаются чем-то недовольные служащие, собирающиеся покинуть данную организацию, но это могут быть и консультанты, служащие с определенными политическими убеждениями и т. п.

Реальный пример логической бомбы: программист, предвидя свое увольнение, вносит в программу расчета заработной платы определенные изменения, которые начинают действовать, когда его фамилия исчезнет из набора данных о персонале фирмы.

Троянский конь – программа, выполняющая в дополнение к основным, т. е. запроектированным и документированным действиям, действия дополнительные, не описанные в документации. Аналогия с древнегреческим троянским конем оправдана – и в том, и в другом случае не вызывающей подозрения оболочке таится угроза. Троянский конь представляет собой дополнительный блок команд, тем или иным образом вставленный в исходную безвредную программу, которая затем передается (дарится, продается, подменяется) пользователям ИС. Этот блок команд может срабатывать при наступлении некоторого условия (даты, времени, по команде извне и т. д.). Запустивший такую программу подвергает опасности как свои файлы, так и всю ИС в целом. Троянский конь действует обычно в рамках полномочий одного пользователя, но в интересах другого пользователя или вообще постороннего человека, личность которого установить порой невозможно.

Вирус – программа, которая может заражать другие программы путем включения в них модифицированной копии, обладающей способностью к дальнейшему размножению.

Считается, что вирус характеризуется двумя основными особенностями:

1) способностью к саморазмножению;

2) способностью к вмешательству в вычислительный процесс (т. е. к получению возможности управления).

Наличие этих свойств, как видим, является аналогом паразитирования в живой природе, которое свойственно биологическим вирусам. В последние годы проблема борьбы с вирусами стала весьма актуальной, поэтому очень многие занимаются ею. Используются

различные организационные меры, новые антивирусные программы, ведется пропаганда всех этих мер. В последнее время удавалось более или менее ограничить масштабы заражений и разрушений. Однако, как и в живой природе, полный успех в этой борьбе не достигнут.

Червь – программа, распространяющаяся через сеть и не оставляющая своей копии на магнитном носителе. Червь использует механизмы поддержки сети для определения узла, который может быть заражен. Затем с помощью тех же механизмов передает свое тело или его часть на этот узел и либо активизируется, либо ждет для этого подходящих условий. Наилучший способ защиты от червя – принятие мер предосторожности против несанкционированного доступа к сети.

Захватчик паролей – это программы, специально предназначенные для воровства паролей. При попытке обращения пользователя к терминалу системы на экран выводится информация, необходимая для окончания сеанса работы. Пытаясь организовать вход, пользователь вводит имя и пароль, которые пересылаются владельцу программы-захватчика, после чего выводится сообщение об ошибке, а ввод и управление возвращаются к операционной системе. Пользователь, думающий, что допустил ошибку при наборе пароля, повторяет вход и получает доступ *к* системе. Однако его имя и пароль уже известны владельцу программы-захватчика. Перехват пароля возможен и другими способами. Для предотвращения этой угрозы перед входом в систему необходимо убедиться, что вы вводите имя и пароль именно системной программе ввода, а не какой-нибудь другой. Кроме того, необходимо неукоснительно придерживаться правил использования паролей и работы с системой. Большинство нарушений происходит не из-за хитроумных атак, а из-за элементарной небрежности. Соблюдение специально разработанных правил использования паролей – необходимое условие надежной защиты.

Несанкционированное использование информационных ресурсов, с одной стороны, является последствиями ее утечки и средством ее компрометации. С другой стороны, оно имеет самостоятельное значение, так как может нанести большой ущерб управляемой системе (вплоть до полного выхода ИТ из строя) или ее абонентам.

Ошибочное использование информационных ресурсов, будучи санкционированным, тем не менее может привести к разрушению, утечке или компрометации указанных ресурсов. Данная угроза чаще всего является следствием ошибок, имеющихся в ПО ИТ.

Несанкционированный обмен информацией между абонентами может привести к получению одним из них сведений, доступ к которым ему запрещен. Последствия – те же, что и при несанкционированном доступе.

Методы и средства защиты информации

Создание систем информационной безопасности (СИБ) в ИС и ИТ основывается на следующих принципах:

Системный подход к построению системы защиты, означающий оптимальное сочетание взаимосвязанных организационных, программных, аппаратных, физических и других свойств, подтвержденных практикой создания отечественных и зарубежных систем защиты и применяемых на всех этапах технологического цикла обработки информации.

Принцип непрерывного развития системы. Этот принцип, являющийся одним из основополагающих для компьютерных информационных систем, еще более актуален для СИБ. Способы реализации угроз информации в ИТ непрерывно совершенствуются, а потому обеспечение безопасности ИС не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования СИБ, непрерывном контроле, выявлении ее узких и слабых мест, потенциальных каналов утечки информации и новых способов несанкционированного доступа,

Обеспечение надежности системы защиты, т. е. невозможность снижения уровня надежности при возникновении в системе сбоев, отказов, преднамеренных действий взломщика или непреднамеренных ошибок пользователей и обслуживающего персонала.

Обеспечение контроля за функционированием системы защиты, т. е. создание средств и методов контроля работоспособности механизмов защиты.

Обеспечение всевозможных средств борьбы с вредоносными программами.

Обеспечение экономической целесообразности использования системы защиты, что выражается в превышении возможного ущерба ИС и ИТ от реализации угроз над стоимостью разработки и эксплуатации СИБ.

В результате решения проблем безопасности информации современные ИС и ИТ должны обладать следующими основными признаками:

– наличием информации различной степени конфиденциальности;

– обеспечением криптографической защиты информации различной степени конфиденциальности при передаче данных;

– обязательным управлением потоками информации, как в локальных сетях, так и при передаче по каналам связи на далекие расстояния;

– наличием механизма регистрации и учета попыток несанкционированного доступа, событий в ИС и документов, выводимых на печать;

– обязательным обеспечением целостности программного обеспечения и информации в ИТ;

– наличием средств восстановления системы защиты информации;

– обязательным учетом магнитных носителей;

– наличием физической охраны средств вычислительной техники и магнитных носителей;

– наличием специальной службы информационной безопасности системы.

3. Методы и средства обеспечения безопасности информации

Препятствие – метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т. д.).

Управление доступом – методы защиты информации регулированием использования всех ресурсов ИС и ИТ. Эти методы должны противостоять всем возможным путям несанкционированного доступа к информации. Управление доступом включает следующие функции защиты:

– идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);

– опознание (установление подлинности) объекта или субъекта по предъявленному им идентификатору;

– разрешение и создание условий работы в пределах установленного регламента;

– регистрацию (протоколирование) обращений к защищаемым ресурсам;

– реагирование (сигнализация, отключение, задержка работ, отказ в запросе и т. п.) при попытках несанкционированных действий.

Механизмы шифрования – криптографическое закрытие информации. Эти методы защиты все шире применяются как при обработке,

так и при хранении информации на магнитных носителях. При передаче информации по каналам связи большой протяженности этот метод является единственно надежным.

Противодействие атакам вредоносных программ предполагает комплекс разнообразных мер организационного характера и использование антивирусных программ.

Вся совокупность технических средств подразделяется на аппаратные и физические.

Аппаратные средства – устройства, встраиваемые непосредственно в вычислительную технику, или устройства, которые сопрягаются с ней по стандартному интерфейсу.

Физические средства включают различные инженерные устройства и сооружения, препятствующие физическому проникновению злоумышленников на объекты защиты и осуществляющие *защиту* персонала (личные средства безопасности), материальных средств и финансов, информации от противоправных действий. Примеры физических средств: замки на дверях, решетки на окнах, средства электронной охранной сигнализации и т. п.

Программные средства – это специальные программы и программные комплексы, предназначенные для защиты информации в ИС.

Из средств ПО системы защиты необходимо выделить еще программные средства, реализующие механизмы шифрования (криптографии). Криптография – это наука об обеспечении секретности и/или аутентичности (подлинности) передаваемых сообщений.

Организационные средства осуществляют своим комплексом регламентацию производственной деятельности в ИС и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становится невозможным или существенно затрудняется за счет проведения организационных мероприятий.

Законодательные средства защиты определяются законодательными актами страны, которыми регламентируются правила пользования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

Морально-этические средства защиты включают всевозможные нормы поведения, которые традиционно сложились ранее, складываются по мере распространения ИС в стране и в мире или специально разрабатываются. Морально-этические нормы могут быть неписаные (например, честность) либо оформленные в некий свод (устав) правил или предписаний. Эти нормы, как правило, не являются законода-

тельно утвержденными, но поскольку их несоблюдение приводит к падению престижа организации, они считаются обязательными для исполнения.

4. Криптография и криптоанализ

Криптография занимается поиском и исследованием математических методов преобразования информации.

Основные направления использования криптографических методов – передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.

Итак, криптография дает возможность преобразовать информацию таким образом, что ее прочтение (восстановление) возможно только при знании ключа.

В качестве информации, подлежащей шифрованию и дешифрованию, будут рассматриваться тексты, построенные на некотором алфавите. Под этими терминами понимается следующее:

Алфавит – конечное множество используемых для кодирования информации знаков.

Текст – упорядоченный набор из элементов алфавита.

В качестве примеров алфавитов, используемых в современных ИС можно привести следующие:

– алфавит Z33 – 32 буквы русского алфавита и пробел;

– алфавит Z256 – символы, входящие в стандартные коды ASCII и КОИ-8;

– бинарный алфавит – Z2 = {0,1};

– восьмеричный алфавит или шестнадцатеричный алфавит.

Шифрование – преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом.

Дешифрование – обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный.

Ключ – информация, необходимая для беспрепятственного шифрования и дешифрования текстов.

Криптографическая система представляет собой семейство T преобразований открытого текста. Члены этого семейства индексируются, или обозначаются символом k; параметр k является ключом. Пространство ключей K – это набор возможных значений

ключа. Обычно ключ представляет собой последовательный ряд букв алфавита.

Криптосистемы разделяются на *симметричные* и с *открытым ключом*.

В ***симметричных криптосистемах*** и для шифрования, и для дешифрования используется один и тот же ключ.

В системах с ***открытым ключом*** используются два ключа – открытый и закрытый, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Термины ***распределение ключей*** и ***управление ключами*** относятся к процессам системы обработки информации, содержанием которых является составление и распределение ключей между пользователями.

Электронной (цифровой) подписью называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

Криптостойкостью называется характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т. е. криптоанализу). Имеется несколько показателей криптостойкости, среди которых:

– количество всех возможных ключей;

– среднее время, необходимое для криптоанализа.

Преобразование Tk определяется соответствующим алгоритмом и значением параметра k. Эффективность шифрования с целью защиты информации зависит от сохранения тайны ключа и криптостойкости шифра.

4.1. Требования к криптосистемам

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т. д. Программная реализация более практична, допускает известную гибкость в использовании.

Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

– зашифрованное сообщение должно поддаваться чтению только при наличии ключа;

– число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста,

– должно быть не меньше общего числа возможных ключей;

– число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений);

– знание алгоритма шифрования не должно влиять на надежность защиты;

– незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа;

– структурные элементы алгоритма шифрования должны быть неизменными;

– дополнительные биты, вводимые в сообщение в процессе шифрования, должны быть полностью и надежно скрыты в шифрованном тексте;

– длина шифрованного текста должна быть равной длине исходного текста;

– не должно быть простых и легко устанавливаемых зависимостью между ключами, последовательно используемыми в процессе шифрования;

– любой ключ из множества возможных должен обеспечивать надежную защиту информации;

– алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

5. Кодирование

Естественные языки обладают большой избыточностью для экономии памяти, объем которой ограничен, имеет смысл ликвидировать избыточность текста или уплотнить текст.

Существуют несколько способов уплотнения текста.

1. *Переход от естественных обозначений к более компактным.* Этот способ применяется для сжатия записи дат, номеров изделий,

уличных адресов и т. д. Идея способа показана на примере сжатия записи даты. Обычно мы записываем дату в виде 10.05.01, что требует 6 байтов памяти ЭВМ. Однако ясно, что для представления дня достаточно 5 битов, месяца – 4, года – не более 7, т. е. вся дата может быть записана в 16 битах или в 2-х байтах.

2. *Подавление повторяющихся символов.* В различных информационных текстах часто встречаются цепочки повторяющихся символов, например, пробелы или нули в числовых полях. Если имеется группа повторяющихся символов длиной более 3, то ее длину можно сократить до трех символов. Сжатая таким образом группа повторяющихся символов представляет собой триграф S P N, в котором S – символ повторения; P – признак повторения; N – количество символов повторения, закодированных в триграфе. В других схемах подавления повторяющихся символов используют особенность кодов ДКОИ, КОИ-7, КОИ-8, заключающуюся в том, что большинство допустимых в них битовых комбинаций не используется для представления символьных данных.

3. *Кодирование часто используемых элементов данных.* Этот способ уплотнения данных также основан на употреблении неиспользуемых комбинаций кода ДКОИ. Для кодирования, например, имен людей можно использовать комбинации из двух байтов диграф PN, где P – признак кодирования имени, N – номер имени. Таким образом может быть закодировано 256 имен людей, чего обычно бывает достаточно в информационных системах. Другой способ основан на отыскании в текстах наиболее часто встречающихся сочетаний букв и даже слов и замене их на неиспользуемые байты кода ДКОИ.

4. *Посимвольное кодирование.* Семибитовые и восьмибитовые коды не обеспечивают достаточно компактного кодирования символьной информации. Более пригодными для этой цели являются 5-битовые коды, например, международный телеграфный код МГК-2. Перевод информации в код МГК-2 возможен с помощью программного перекодирования или с использованием специальных элементов на основе больших интегральных схем (БИС). Пропускная способность каналов связи при передаче алфавитно-цифровой информации в коде МГК-2 повышается по сравнению с использованием восьмибитовых кодов почти на 40 %.

5. *Коды переменной длины.* Коды с переменным числом битов на символ позволяют добиться еще более плотной упаковки данных. Метод заключается в том, что часто используемые символы кодируются

короткими кодами, а символы с низкой частотой использования – длинными кодами. Идея такого кодирования была впервые высказана Хаффманом, и соответствующий код называется кодом Хаффмана. Использование кодов Хаффмана позволяет достичь сокращения исходного текста почти на 80 %.

Использование различных методов уплотнения текстов кроме своего основного назначения – уменьшения информационной избыточности – обеспечивает определенную криптографическую обработку информации. Однако наибольшего эффекта можно достичь при совместном использовании как методов шифрования, так и методов кодирования информации.

Надежность защиты информации может быть оценена временем, которое требуется на расшифрование (разгадывание) информации и определение ключей.

Если информация зашифрована с помощью простой подстановки, то расшифровать ее можно было бы, определив частоты появления каждой буквы в шифрованном тексте и сравнив их с частотами букв русского алфавита. Таким образом определяется подстановочный алфавит и расшифровывается текст.

Кодирование текстовых данных

Если каждому символу алфавита сопоставить определенное целое число, то с помощью двоичного кода можно кодировать текстовую информацию. Восьми двоичных разрядов достаточно для кодирования 256 различных символов. Это хватит, чтобы выразить различными комбинациями восьми битов все символы английского и русского языков, как строчные, так и прописные, а также знаки препинания, символы основных арифметических действий и некоторые общепринятые специальные символы.

Технически это выглядит очень просто, однако всегда существовали достаточно веские организационные сложности. В первые годы развития вычислительной техники они были связаны с отсутствием необходимых стандартов, а в настоящее время вызваны, наоборот, изобилием одновременно действующих и противоречивых стандартов. Для того чтобы весь мир одинаково кодировал текстовые данные, нужны единые таблицы кодирования, а это пока невозможно из-за противоречий между символами национальных алфавитов, а также противоречий корпоративного характера.

Для английского языка, захватившего де-факто нишу международного средства общения, противоречия уже сняты. Институт стан-

дартизации США ввел в действие систему кодирования ASCII (American Standard Code for Information Interchange – стандартный код информационного обмена США). В системе ASCII закреплены две таблицы кодирования базовая и расширенная. Базовая таблица закрепляет значения кодов от 0 до 127, а расширенная относится к символам с номерами от 128 до 255.

Первые 32 кода базовой таблицы, начиная с нулевого, отданы производителям аппаратных средств. В этой области размещаются управляющие коды, которым не соответствуют никакие символы языков. Начиная с 32 по 127 код размещены коды символов английского алфавита, знаков препинания, арифметических действий и некоторых вспомогательных символов.

Кодировка символов русского языка, известная как кодировка Windows-1251, была введена «извне» – компанией Microsoft, но, учитывая широкое распространение операционных систем и других продуктов этой компании в России, она глубоко закрепилась и нашла широкое распространение.

Другая распространенная кодировка носит название КОИ-8 (код обмена информацией, восьмизначный) – ее происхождение относится к временам действия Совета Экономической Взаимопомощи государств Восточной Европы. Сегодня кодировка КОИ-8 имеет широкое распространение в компьютерных сетях на территории России и в российском секторе Интернета.

Международный стандарт, в котором предусмотрена кодировка символов русского языка, носит названия ISO (International Standard Organization – Международный институт стандартизации). На практике данная кодировка используется редко.

Универсальная система кодирования текстовых данных

Если проанализировать организационные трудности, связанные с созданием единой системы кодирования текстовых данных, то можно прийти к выводу, что они вызваны ограниченным набором кодов (256). В то же время, очевидно, что, если кодировать символы не восьмиразрядными двоичными числами, а числами с большим разрядом то и диапазон возможных значений кодов станет намного больше. Такая система, основанная на 16-разрядном кодировании символов, получила название универсальной – UNICODE. Шестнадцать разрядов позволяют обеспечить уникальные коды для 65 536 различных символов – этого поля вполне достаточно для размещения в одной таблице символов большинства языков планеты.

Несмотря на тривиальную очевидность такого подхода, простой механический переход на данную систему долгое время сдерживался из-за недостатков ресурсов средств вычислительной техники (в системе кодирования UNICODE все текстовые документы становятся автоматически вдвое длиннее). Во второй половине 90-х годов технические средства достигли необходимого уровня обеспечения ресурсами, и сегодня мы наблюдаем постепенный перевод документов и программных средств на универсальную систему кодирования.

Кодирование графических данных

Если рассмотреть с помощью увеличительного стекла черно-белое графическое изображение, напечатанное в газете или книге, то можно увидеть, что оно состоит из мельчайших точек, образующих характерный узор, называемый растром. Поскольку линейные координаты и индивидуальные свойства каждой точки (яркость) можно выразить с помощью целых чисел, то можно сказать, что растровое кодирование позволяет использовать двоичный код для представления графических данных. Общепринятым на сегодняшний день считается представление черно-белых иллюстраций в виде комбинации точек с 256 градациями серого цвета, и, таким образом, для кодирования яркости любой точки обычно достаточно восьмиразрядного двоичного числа.

Для кодирования цветных графических изображений применяется принцип декомпозиции произвольного цвета на основные составляющие. В качестве таких составляющих используют три основные цвета: красный (Red), зеленый (Green) и синий (Blue). На практике считается, что любой цвет, видимый человеческим глазом, можно получить путем механического смешения этих трех основных цветов. Такая система кодирования получила названия RGB по первым буквам основных цветов.

Режим представления цветной графики с использованием 24 двоичных разрядов называется полноцветным (True Color).

Каждому из основных цветов можно поставить в соответствие дополнительный цвет, т. е. цвет, дополняющий основной цвет до белого. Нетрудно заметить, что для любого из основных цветов дополнительным будет цвет, образованный суммой пары остальных основных цветов. Соответственно дополнительными цветами являются: голубой (Cyan), пурпурный (Magenta) и желтый (Yellow). Принцип декомпозиции произвольного цвета на составляющие компоненты

можно применять не только для основных цветов, но и для дополнительных, т. е. любой цвет можно представить в виде суммы голубой, пурпурной и желтой составляющей. Такой метод кодирования цвета принят в полиграфии, но в полиграфии используется еще и четвертая краска – черная (Black). Поэтому данная система кодирования обозначается четырьмя буквами CMYK (черный цвет обозначается буквой К, потому, что буква В уже занята синим цветом), и для представления цветной графики в этой системе надо иметь 32 двоичных разряда. Такой режим также называется полноцветным.

Если уменьшить количество двоичных разрядов, используемых для кодирования цвета каждой точки, то можно сократить объем данных, но при этом диапазон кодируемых цветов заметно сокращается. Кодирование цветной графики 16-разрядными двоичными числами называется режимом High Color.

При кодировании информации о цвете с помощью восьми бит данных можно передать только 256 оттенков. Такой метод кодирования цвета называется индексным.

Кодирование звуковой информации

Приемы и методы работы со звуковой информацией пришли в вычислительную технику наиболее поздно. К тому же, в отличие от числовых, текстовых и графических данных, у звукозаписей не было столь же длительной и проверенной истории кодирования. В итоге методы кодирования звуковой информации двоичным кодом далеки от стандартизации. Множество отдельных компаний разработали свои корпоративные стандарты, но среди них можно выделить два основных направления.

1. Метод FM (Frequency Modulation) основан та том, что теоретически любой сложный звук можно разложить на последовательность простейших гармонических сигналов разных частот, каждый из которых представляет собой правильную синусоиду, а, следовательно, может быть описан числовыми параметрами, т. е. кодом. В природе звуковые сигналы имеют непрерывный спектр, т. е. являются аналоговыми. Их разложение в гармонические ряды и представление в виде дискретных цифровых сигналов выполняют специальный устройства – аналогово-цифровые преобразователи (АЦП). Обратное преобразование для воспроизведения звука, закодированного числовым кодом, выполняют цифро-аналоговые преобразователи (ЦАП). При таких преобразованиях неизбежны потери информации, связан-

ные с методом кодирования, поэтому качество звукозаписи обычно получается не вполне удовлетворительным и соответствует качеству звучания простейших электромузыкальных инструментов с окрасом, характерным для электронной музыки. В то же время данный метод копирования обеспечивает весьма компактный код, поэтому он нашел применение еще в те годы, когда ресурсы средств вычислительной техники были явно недостаточны.

2. Метод таблично-волнового (Wave-Table) синтеза лучше соответствует современному уровню развития техники. В заранее подготовленных таблицах хранятся образцы звуков для множества различных музыкальных инструментах. В технике такие образцы называют сэмплами. Числовые коды выражают тип инструмента, номер его модели, высоту тона, продолжительность и интенсивность звука, динамику его изменения, некоторые параметры среды, в которой происходит звучание, а также прочие параметры, характеризующие особенности звучания. Поскольку в качестве образцов исполняются реальные звуки, то его качество получается очень высоким и приближается к качеству звучания реальных музыкальных инструментов.

6. Программные средства защиты информации

Программными называются средства защиты данных, функционирующие в составе программного обеспечения. Среди них можно выделить и подробнее рассмотреть следующие:

– средства архивации данных;
– антивирусные программы;
– криптографические средства;
– средства идентификации и аутентификации пользователей;
– средства управления доступом;
– протоколирование и аудит.

Как примеры комбинаций вышеперечисленных мер можно привести:

– защиту баз данных;
– защиту информации при работе в компьютерных сетях.

Средства архивации информации

Иногда резервные копии информации приходится выполнять при общей ограниченности ресурсов размещения данных, например, владельцам персональных компьютеров. В этих случаях используют программную архивацию. Архивация это слияние нескольких файлов

и даже каталогов в единый файл – архив, одновременно с сокращением общего объема исходных файлов путем устранения избыточности, но без потерь информации, т. е. с возможностью точного восстановления исходных файлов. Действие большинства средств архивации основано на использовании алгоритмов сжатия, предложенных в 80-х гг. Абрахамом Лемпелем и Якобом Зивом. Наиболее известны и популярны следующие архивные форматы:

– ZIP, ARJ для операционных систем DOS и Windows.

– TAR для операционной системы Unix.

– межплатформный формат JAR (Java ARchive).

– RAR (все время растет популярность этого нового формата, так как разработаны программы, позволяющие использовать его в операционных системах DOS, Windows и Unix).

Пользователю следует лишь выбрать для себя подходящую программу, обеспечивающую работу с выбранным форматом, путем оценки ее характеристик – быстродействия, степени сжатия, совместимости с большим количеством форматов, удобности интерфейса, выбора операционной системы и т. д. Список таких программ очень велик – PKZIP, PKUNZIP, ARJ, RAR, WinZip, WinArj, ZipMagic, WinRar и много других. Большинство из этих программ не надо специально покупать, так как они предлагаются как программы условно-бесплатные (Shareware) или свободного распространения (Freeware). Также очень важно установить постоянный график проведения таких работ по архивации данных или выполнять их после большого обновления данных.

7. Антивирусные программы

Это программы, разработанные для защиты информации от вирусов. Неискушенные пользователи обычно считают, что компьютерный вирус – это специально написанная небольшая по размерам программа, которая может «приписывать» себя к другим программам (т. е. «заражать» их), а также выполнять нежелательные различные действия на компьютере. Специалисты по компьютерной вирусологии определяют, что ОБЯЗАТЕЛЬНЫМ (НЕОБХОДИМЫМ) СВОЙСТВОМ КОМПЬЮТЕРНОГО ВИРУСА является возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению. Следует

отметить, что это условие не является достаточным, т. е. окончательным. Вот почему точного определения вируса нет до сих пор, и вряд ли оно появится в обозримом будущем. Следовательно, нет точно определенного закона, по которому «хорошие» файлы можно отличить от «вирусов». Более того, иногда даже для конкретного файла довольно сложно определить, является он вирусом или нет.

7.1. Классификация компьютерных вирусов

Вирусы можно разделить на классы по следующим основным признакам:

– деструктивные возможности;

– особенности алгоритма работы;

– среда обитания.

По деструктивным возможностям вирусы можно разделить на:

– безвредные, т. е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);

– неопасные, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и прочими эффектами;

– опасные вирусы, которые могут привести к серьезным сбоям в работе компьютера;

– очень опасные, в алгоритм работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти.

Особенности алгоритма работы вирусов можно охарактеризовать следующими свойствами:

– резидентность;

– использование стелс-алгоритмов;

– самошифрование и полиморфичность.

Резидентные вирусы

Под термином «резидентность» (DOS'овский термин TSR – Terminate and Stay Resident) понимается способность вирусов оставлять свои копии в системной памяти, перехватывать некоторые события (например, обращения к файлам или дискам) и вызывать при этом процедуры заражения обнаруженных объектов (файлов и секторов). Таким образом, резидентные вирусы активны не только в момент работы зараженной программы, но и после того, как программа закон-

чила свою работу. Резидентные копии таких вирусов остаются жизнеспособными вплоть до очередной перезагрузки, даже если на диске уничтожены все зараженные файлы. Часто от таких вирусов невозможно избавиться восстановлением всех копий файлов с дистрибутивных дисков или backup-копий. Резидентная копия вируса остается активной и заражает вновь создаваемые файлы. То же верно и для загрузочных вирусов – форматирование диска при наличии в памяти резидентного вируса не всегда вылечивает диск, поскольку многие резидентные вирусы заражает диск повторно после того, как он отформатирован.

Нерезидентные вирусы

Нерезидентные вирусы, напротив, активны довольно непродолжительное время – только в момент запуска зараженной программы. Для своего распространения они ищут на диске незараженные файлы и записываются в них. После того, как код вируса передает управление программе-носителю, влияние вируса на работу операционной системы сводится к нулю вплоть до очередного запуска какой-либо зараженной программы. Поэтому файлы, зараженные нерезидентными вирусами значительно проще удалить с диска и при этом не позволить вирусу заразить их повторно.

Стелс-вирусы

Стелс-вирусы теми или иными способами скрывают факт своего присутствия в системе.

Использование стелс-алгоритмов позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным стелс-алгоритмом является перехват запросов ОС на чтение/запись зараженных объектов. Стелс-вирусы при этом либо временно лечат их, либо «подставляют» вместо себя незараженные участки информации. В случае макро-вирусов наиболее популярный способ – запрет вызовов меню просмотра макросов. Известны стелс-вирусы всех типов, за исключением Windows-вирусов – загрузочные вирусы, файловые DOS-вирусы и даже макро-вирусы. Появление стелс-вирусов, заражающих файлы Windows, является скорее всего делом времени.

Полиморфик-вирусы

Самошифрование и полиморфичность используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру детектирования вируса. Полиморфик – вирусы (polymorphic) –

это достаточно трудно обнаружимые вирусы, не имеющие сигнатур, т. е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфик-вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

К полиморфик-вирусам относятся те из них, детектирование которых невозможно (или крайне затруднительно) осуществить при помощи так называемых вирусных масок – участков постоянного кода, специфичных для конкретного вируса. Достигается это двумя основными способами – шифрованием основного кода вируса с непостоянным ключем и случайным набором команд расшифровщика или изменением самого выполняемого кода вируса. Полиморфизм различной степени сложности встречается в вирусах всех типов – от загрузочных и файловых DOS-вирусов до Windows-вирусов.

По среде обитания вирусы можно разделить на:

– файловые;
– загрузочные;
– макровирусы;
– сетевые.

Файловые вирусы

Файловые вирусы либо различными способами внедряются в выполняемые файлы (наиболее распространенный тип вирусов), либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы).

Внедрение файлового вируса возможно практически во все исполняемые файлы всех популярных ОС. На сегодняшний день известны вирусы, поражающие все типы выполняемых объектов стандартной DOS: командные файлы (BAT), загружаемые драйверы (SYS, в том числе специальные файлы IO.SYS и MSDOS.SYS) и выполняемые двоичные файлы (EXE, COM). Существуют вирусы, поражающие исполняемые файлы других операционных систем – Windows 3.x, Windows95/NT, OS/2, Macintosh, UNIX, включая VxD-драйвера Windows 3.x и Windows95.

Существуют вирусы, заражающие файлы, которые содержат исходные тексты программ, библиотечные или объектные модули. Возможна запись вируса и в файлы данных, но это случается либо в результате ошибки вируса, либо при проявлении его агрессивных свойств. Макро-вирусы также записывают свой код в файлы данных –

документы или электронные таблицы, – однако эти вирусы настолько специфичны, что вынесены в отдельную группу.

Загрузочные вирусы

Загрузочные вирусы заражают загрузочный (boot) сектор флоппи-диска и boot-сектор или Master Boot Record (MBR) винчестера. Принцип действия загрузочных вирусов основан на алгоритмах запуска операционной системы при включении или перезагрузке компьютера – после необходимых тестов установленного оборудования (памяти, дисков и т. д.) программа системной загрузки считывает первый физический сектор загрузочного диска (A:, C: или CD-ROM в зависимости от параметров, установленных в BIOS Setup) и передает на него управление.

В случае дискеты или компакт-диска управление получает boot-сектор, который анализирует таблицу параметров диска (BPB – BIOS Parameter Block), высчитывает адреса системных файлов операционной системы, считывает их в память и запускает на выполнение. Системными файлами обычно являются MSDOS.SYS и IO.SYS, либо IBMDOS.COM и IBMBIO.COM, либо других в зависимости от установленной версии DOS, Windows или других операционных систем. Если же на загрузочном диске отсутствуют файлы операционной системы, программа, расположенная в boot-секторе диска выдает сообщение об ошибке и предлагает заменить загрузочный диск.

В случае винчестера управление получает программа, расположенная в MBR винчестера. Эта программа анализирует таблицу разбиения диска (Disk Partition Table), вычисляет адрес активного boot-сектора (обычно этим сектором является boot-сектор диска C:), загружает его в память и передает на него управление. Получив управление, активный boot-сектор винчестера проделывает те же действия, что и boot-сектор дискеты.

При заражении дисков загрузочные вирусы «подставляют» свой код вместо какой-либо программы, получающей управление при загрузке системы. Принцип заражения, таким образом, одинаков во всех описанных выше способах: вирус «заставляет» систему при ее перезапуске считать в память и отдать управление не оригинальному коду загрузчика, но коду вируса.

Заражение дискет производится единственным известным способом – вирус записывает свой код вместо оригинального кода boot-сектора дискеты. Винчестер заражается тремя возможными способа-

ми – вирус записывается либо вместо кода MBR, либо вместо кода boot-сектора загрузочного диска (обычно диска C:), либо модифицирует адрес активного boot-сектора в Disk Partition Table, расположенной в MBR винчестера.

Макро-вирусы

Макро-вирусы заражают файлы-документы и электронные таблицы нескольких популярных редакторов. Макро-вирусы (macro viruses) являются программами на языках (макро-языках), встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т. д.). Для своего размножения такие вирусы используют возможности макро-языков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие. Наибольшее распространение получили макро-вирусы для Microsoft Word, Excel и Office97. Существуют также макро-вирусы, заражающие документы Ami Pro и базы данных Microsoft Access.

Сетевые вирусы

К сетевым относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. «Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла. Пример сетевых вирусов – так называемые IRC-черви.

IRC (Internet Relay Chat) – это специальный протокол, разработанный для коммуникации пользователей Интернет в реальном времени. Этот протокол предоставляет им возможность Итернет-«разговора» при помощи специально разработанного программного обеспечения. Помимо посещения общих конференций пользователи IRC имеют возможность общаться один на один с любым другим пользователем. Кроме этого существует довольно большое количество IRC-команд, при помощи которых пользователь может получить информацию о других пользователях и каналах, изменять некоторые установки IRC-клиента и прочее. Существует также возможность передавать и принимать файлы – именно на этой возможности и базируются IRC-черви. Как оказалось, мощная и разветвленная система

команд IRC-клиентов позволяет на основе их скриптов создавать компьютерные вирусы, передающие свой код на компьютеры пользователей сетей IRC, так называемые «IRC-черви».

Принцип действия таких IRC-червей примерно одинаков. При помощи IRC-команд файл сценария работы (скрипт) автоматически посылается с зараженного компьютера каждому вновь присоединившемуся к каналу пользователю. Присланный файл-сценарий замещает стандартный и при следующем сеансе работы уже вновь зараженный клиент будет рассылать червя. Некоторые IRC-черви также содержат троянский компонент: по заданным ключевым словам производят разрушительные действия на пораженных компьютерах. Например, червь «pIRCH.Events» по определенной команде стирает все файлы на диске пользователя.

Существует большое количество сочетаний – например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные сектора дисков. Такие вирусы, как правило, имеют довольно сложный алгоритм работы, часто применяют оригинальные методы проникновения в систему, используют стелс и полиморфик-технологии. Другой пример такого сочетания – сетевой макро-вирус, который не только заражает редактируемые документы, но и рассылает свои копии по электронной почте.

7.2. Методы обнаружения и удаления компьютерных вирусов

Способы противодействия компьютерным вирусам можно разделить на несколько групп: профилактика вирусного заражения и уменьшение предполагаемого ущерба от такого заражения; методика использования антивирусных программ, в том числе обезвреживание и удаление известного вируса; способы обнаружения и удаления неизвестного вируса.

7.3. Профилактика заражения компьютера

Одним из основных методов борьбы с вирусами является, как и в медицине, своевременная профилактика. Компьютерная профилактика предполагает соблюдение небольшого числа правил, которое позволяет значительно снизить вероятность заражения вирусом и потери каких-либо данных.

Для того чтобы определить основные правила компьютерной гигиены, необходимо выяснить основные пути проникновения вируса в компьютер и компьютерные сети.

Основным источником вирусов на сегодняшний день является глобальная сеть Internet. Наибольшее число заражений вирусом происходит при обмене письмами в форматах Word/Office97. Пользователь зараженного макро-вирусом редактора, сам того не подозревая, рассылает зараженные письма адресатам, которые, в свою очередь, отправляют новые зараженные письма и т. д. Выводы – следует избегать контактов с подозрительными источниками информации и пользоваться только законными (лицензионными) программными продуктами. К сожалению, в нашей стране это не всегда возможно.

7.4. Восстановление пораженных объектов

В большинстве случаев заражения вирусом процедура восстановления зараженных файлов и дисков сводится к запуску подходящего антивируса, способного обезвредить систему. Если же вирус неизвестен ни одному антивирусу, то достаточно отослать зараженный файл фирмам-производителям антивирусов и через некоторое время (обычно – несколько дней или недель) получить лекарство-»апдейт» против вируса. Если же время не ждет, то обезвреживание вируса придется произвести самостоятельно. Для большинства пользователей необходимо иметь резервные копии своей информации.

7.5. Классификация антивирусных программ

Наиболее эффективны в борьбе с компьютерными вирусами антивирусные программы. Однако сразу хотелось бы отметить, что не существует антивирусов, гарантирующих стопроцентную защиту от вирусов, и заявления о существовании таких систем можно расценить как либо недобросовестную рекламу, либо непрофессионализм. Таких систем не существует, поскольку на любой алгоритм антивируса всегда можно предложить контр-алгоритм вируса, невидимого для этого антивируса (обратное, к счастью, тоже верно: на любой алгоритм вируса всегда можно создать антивирус).

Самыми популярными и эффективными антивирусными программами являются антивирусные сканеры (другие названия: фаг, полифаг, программа-доктор). Следом за ними по эффективности и популярности следуют CRC-сканеры (также: ревизор, checksumer, integrity checker). Часто оба приведенных метода объединяются в од-

ну универсальную антивирусную программу, что значительно повышает ее мощность. Применяются также различного типа блокировщики и иммунизаторы.

Сканеры

Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются так называемые «маски». Маской вируса является некоторая постоянная последовательность кода, специфичная для этого конкретного вируса. Если вирус не содержит постоянной маски, или длина этой маски недостаточно велика, то используются другие методы. Примером такого метода является алгоритмический язык, описывающий все возможные варианты кода, которые могут встретиться при заражении подобного типа вирусом. Такой подход используется некоторыми антивирусами для детектирования полиморфик-вирусов.

Сканеры также можно разделить на две категории – «универсальные» и «специализированные». Универсальные сканеры рассчитаны на поиск и обезвреживание всех типов вирусов вне зависимости от операционной системы, на работу в которой рассчитан сканер. Специализированные сканеры предназначены для обезвреживания ограниченного числа вирусов или только одного их класса, например, макро-вирусов. Специализированные сканеры, рассчитанные только на макро-вирусы, часто оказываются наиболее удобным и надежным решением для защиты систем документооборота в средах MS Word и MS Excel.

Сканеры также делятся на «резидентные» (мониторы, сторожа), производящие сканирование «на-лету», и «нерезидентные», обеспечивающие проверку системы только по запросу. Как правило, «резидентные» сканеры обеспечивают более надежную защиту системы, поскольку они немедленно реагируют на появление вируса, в то время как «нерезидентный» сканер способен опознать вирус только во время своего очередного запуска. С другой стороны резидентный сканер может несколько замедлить работу компьютера в том числе и из-за возможных ложных срабатываний.

К достоинствам сканеров всех типов относится их универсальность, к недостаткам –относительно небольшую скорость поиска вирусов. Наиболее распространены в России следующие программы: AVP – Касперского, Dr.Weber – Данилова, Norton Antivirus фирмы Semantic.

CRC-сканеры

Принцип работы CRC-сканеров основан на подсчете CRC-сумм (контрольных сумм) для присутствующих на диске файлов/системных секторов. Эти CRC-суммы затем сохраняются в базе данных антивируса, как, впрочем, и некоторая другая информация: длины файлов, даты их последней модификации и т. д. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом.

CRC-сканеры, использующие анти-стелс алгоритмы, являются довольно сильным оружием против вирусов: практически 100 % вирусов оказываются обнаруженными почти сразу после их появления на компьютере. Однако у этого типа антивирусов есть врожденный недостаток, который заметно снижает их эффективность. Этот недостаток состоит в том, что CRC-сканеры не способны поймать вирус в момент его появления в системе, а делают это лишь через некоторое время, уже после того, как вирус разошелся по компьютеру. CRC-сканеры не могут определить вирус в новых файлах (в электронной почте, на дискетах, в файлах, восстанавливаемых из backup или при распаковке файлов из архива), поскольку в их базах данных отсутствует информация об этих файлах. Более того, периодически появляются вирусы, которые используют эту «слабость» CRC-сканеров, заражают только вновь создаваемые файлы и остаются, таким образом, невидимыми для них. Наиболее используемые в России программы подобного рода – ADINF и AVP Inspector.

Блокировщики

Антивирусные блокировщики – это резидентные программы, перехватывающие «вирусоопасные» ситуации и сообщающие об этом пользователю. К «вирусоопасным» относятся вызовы на открытие для записи в выполняемые файлы, запись в boot-сектора дисков или MBR винчестера, попытки программ остаться резидентно и т. д., т. е. вызовы, которые характерны для вирусов в моменты их размножения. Иногда некоторые функции блокировщиков реализованы в резидентных сканерах.

К достоинствам блокировщиков относится их способность обнаруживать и останавливать вирус на самой ранней стадии его раз-

множения, что, кстати, бывает очень полезно в случаях, когда давно известный вирус постоянно «выползает неизвестно откуда». К недостаткам относятся существование путей обхода защиты блокировщиков и большое количество ложных срабатываний, что, видимо, и послужило причиной для практически полного отказа пользователей от подобного рода антивирусных программ (например, неизвестно ни об одном блокировщике для Windows95/NT – нет спроса, нет и предложения).

Необходимо также отметить такое направление антивирусных средств, как антивирусные блокировщики, выполненные в виде аппаратных компонентов компьютера («железа»). Наиболее распространенной является встроенная в BIOS защита от записи в MBR винчестера. Однако, как и в случае с программными блокировщиками, такую защиту легко обойти прямой записью в порты контроллера диска, а запуск DOS-утилиты FDISK немедленно вызывает «ложное срабатывание» защиты.

Существует несколько более универсальных аппаратных блокировщиков, но к перечисленным выше недостаткам добавляются также проблемы совместимости со стандартными конфигурациями компьютеров и сложности при их установке и настройке. Все это делает аппаратные блокировщики крайне непопулярными на фоне остальных типов антивирусной защиты.

Иммунизаторы

Иммунизаторы – это программы записывающие в другие программы коды, сообщающие о заражении. Они обычно записывают эти коды в конец файлов (по принципу файлового вируса) и при запуске файла каждый раз проверяют его на изменение. Недостаток у них всего один, но он летален: абсолютная неспособность сообщить о заражении стелс-вирусом. Поэтому такие иммунизаторы, как и блокировщики, практически не используются в настоящее время. Кроме того многие программы, разработанные в последнее время, сами проверяют себя на целостность и могут принять внедренные в них коды за вирусы и отказаться работать.

7.6. Перспективы борьбы с вирусами

Вирусы успешно внедрились в повседневную компьютерную жизнь и покидать ее в обозримом будущем не собираются. Так кто же пишет вирусы? Основную их массу создают студенты и школьники,

которые только что изучили язык ассемблера, хотят попробовать свои силы, но не могут найти для них более достойного применения. Вторую группу составляют также молодые люди (чаще – студенты), которые еще не полностью овладели искусством программирования, но уже решили посвятить себя написанию и распространению вирусов. Единственная причина, толкающая подобных людей на написание вирусов, это комплекс неполноценности, который проявляет себя в компьютерном хулиганстве. Из-под пера подобных «умельцев» часто выходят либо многочисленные модификации «классических» вирусов, либо вирусы крайне примитивные и с большим числом ошибок. Став старше и опытнее, но так и не повзрослев, некоторые из подобных вирусописателей попадают в третью, наиболее опасную группу, которая создает и запускает в мир «профессиональные» вирусы. Однако другие профессионалы будут создавать и новые более совершенные антивирусные средства. Какой прогноз этого единоборства? Для того, чтобы ответить на этот вопрос следует определить, где и при каких условиях размножаются вирусы.

Основная питательная среда для массового распространения вируса в компьютере – это:

– слабая защищенность операционной системы (ОС);

– наличие разнообразной и довольно полной документации по ОС и «железу», используемой авторами вирусов;

– широкое распространение этой ОС и этого «железа».

Хотя следует отметить, что понятие операционной системы достаточно растяжимое. Например, для макро-вирусов операционной системой являются редакторы Word и Excel, поскольку именно редакторы, а не Windows предоставляют макро-вирусам (т. е. программам на бейсике) необходимые ресурсы и функции.

Чем больше в операционной системе присутствуют элементов защиты информации, тем труднее будет вирусу поразить объекты своего нападения, так как для этого потребуется (как минимум) взломать систему шифрования, паролей и привилегий. В результате работа, необходимая для написания вируса, окажется по силам только профессионалам высокого уровня. А у профессионалов, как представляется, уровень порядочности все-таки намного выше, чем в среде потребителей их продукции, и, следовательно, число созданных и запущенных в большую жизнь вирусов будет сокращаться.

Нужно четко представлять себе, что никакие аппаратные, программные и любые другие решения не смогут гарантировать абсо-

лютную надежность и безопасность данных в информационных системах. В то же время можно существенно уменьшить риск потерь при комплексном подходе к вопросам безопасности. Средства защиты информации нельзя проектировать, покупать или устанавливать до тех пор, пока специалистами не произведен соответствующий анализ. Анализ должен дать объективную оценку многих факторов (подверженность появлению нарушения работы, вероятность появления нарушения работы, ущерб от коммерческих потерь и др.) и предоставить информацию для определения подходящих средств защиты – административных, аппаратных, программных и прочих. На рынке защитных средств, присутствуют такие продукты как Кобра, Dallas Lock, Secret Net, Аккорд, Криптон и ряд других. Однако обеспечение безопасности информации – дорогое дело.

Большая концентрация защитных средств в информационной системе может привести не только к тому, что система окажется очень дорогостоящей и потому нерентабельной и неконкурентноспособной, но и к тому, что у нее произойдет существенное снижение коэффициента готовности. Например, если такие ресурсы системы, как время центрального процессора будут постоянно тратиться на работу антивирусных программ, шифрование, резервное архивирование, протоколирование и тому подобное, скорость работы пользователей в такой системе может упасть до нуля.

Поэтому главное при определении мер и принципов защиты информации это квалифицированно определить границы разумной безопасности и затрат на средства защиты с одной стороны и поддержания системы в работоспособном состоянии и приемлемого риска с другой.

8. Система обнаружения и подавления электронных средств перехвата информации

В течение последнего времени резко возрос уровень технического промышленного шпионажа. Многим фирмам и предприятиям все чаще и чаще приходится сталкиваться с проблемой утечки коммерчески важной и конфиденциальной информации. Известно, например, что японские компании, славящиеся своими технологическими разработками и умеющие их охранять, до 80 % новых идей получают за счет утечки информации в конкурирующих фирмах, а на контршпионаж западные фирмы тратят до 15–20 % чистой прибыли.

Существует множество способов несанкционированного доступа к источникам конфиденциальной информации, включая такие, как незаконное подключение, высокочастотное навязывание, установка радиозакладок, перехват электромагнитных излучений и другие. Наиболее распространенным методом получения информации частного и коммерческого характера является акустический перехват при помощи радиопередающих средств. К ним относятся широкая номенклатура радиомикрофонов, назначением которых является передача по радиоканалу акустической информации на объекте.

Поэтому, в связи с обилием подслушивающих электронных устройств, создание портативного бесконтактного подавителя является сегодня актуальной и своевременной задачей. В ходе проведения профилактических мероприятий встает задача быстрого обнаружения и уничтожения электронных устройств перехвата информации, что часто должно быть сделано без нарушения интерьера помещения.

С этой целью была разработана система обнаружения, перехвата и подавления электронных устройств несанкционированного съема информации.

Она состоит из антенного блока, приемного и подавляющего тракта и системы обработки сигналов для автоматизированного управления процессом.

Антенный тракт состоит из нескольких приемопередающих антенн, охватывающих весь возможный спектр частот работы радиозакладок (0,1–2000 МГц). Приемник-сканер сканирует частотный диапазон и останавливается, обнаружив несущую частоту сигнала. При помощи частотомера измеряются частоты и параметры обнаруженных сигналов. В зависимости от уровня сигнала имеется возможность возобновления сканирования. Все сигналы поступают на программно-автоматизированный комплекс для дальнейшей их обработки и анализа, на основе которого вырабатываются управляющие сигналы для тракта подавления.

Тракт подавления состоит из генератора импульсов с заданными характеристиками, преобразователя, на основе которого формируются параметры выходных сигналов, модулятора, смесителя. С выхода преобразователя сигналы по каналам передачи поступают на входы предварительных усилителей, проходят фильтрующие цепи, подаются на входы усилителей мощности и затем выводятся в приемно-подавительный антенный тракт.

В разработке заложена идея дистанционного нарушения структуры транзисторных переходов микрорадиопередатчиков, в основе которой лежит передача энергии от усилителя мощности и наведения ЭДС в выходных контурах радиозакладки с последующим пробоем коллекторного перехода выходного каскада маломощного транзистора. Также реализуется возможность нахождения резонансных частот работы радиозакладок, с дальнейшим пробоем и выведением из строя активных электронных компонентов, работающих на этих частотах.

Основная проблема бесконтактного подавления радиозакладок состоит в применении минимально необходимой для уничтожения мощности и минимального количества циклов проверки сканирование-подавление. Также важным является получение как можно более узкой диаграммы направленности передающей антенны при минимальных отражениях сигнала. Это связано с тем, что, во-первых, требуется оперативность и быстрота уничтожения подслушивающих устройств, и, во-вторых, необходимо исключить вероятность вывода из строя другой аудио-, видеотехники, бытовых радиоприемных устройств и другой аппаратуры.

Литература

1. О некоторых вопросах обеспечения защиты государственных секретов : Указ Президента Республики Беларусь № 195. – Режим доступа : htpp://www.kgb.by/okomitete.

2. Об информации, информатизации и защите информации (проект) : Закон Республики Беларусь. – Режим доступа : htpp://www.pravo.by/webpra.

3. Об информации, информатизации и защите информации : Федерал. закон РФ. – Режим доступа : htpp://www.internet-law.ru.

4. Харкевич, А. А. Борьба с помехами / А. А. Харкевич. – Москва : Наука, 1979.

5. Конопелько, В. К. Помехоустойчивое кодирование в радиотехнических системах передачи информации : метод. пособие. В 5 ч. Ч. 4. Коды, исправляющие дефекты / В. К. Конопелько. – Минск : МРТИ, 1993.

6. Саломатин, С. Б. Защита информации в радиоэлектронных системах : учеб. пособие / С. Б. Саломатин. – Минск : БГУИР, 2002.

7. Грушо, А. А. Теоретические основы защиты информации / А. А. Грушо, Е. Е. Тимонина. – Москва : Изд-во агентства «Яхтсмен», 1996.

8. Питерсон, У. Коды, исправляющие ошибки / У. Питерсон, Э. Уэлдон ; пер. с англ. – Москва : Мир, 1976.

9. Герасименко, В. А. Защита информации в автоматизированных системах обработки данных. В 2 кн. Кн. 1, 2 / В. А. Герасименко. – Москва : Энергоатомиздат, 1994.

10. Гайкович, В. Безопасность электронных банковских систем / В. Гайкович, А. Першин. – Москва : Единая Европа, 1994.

11. Введение в криптографию / под общ. ред. В. В. Ященко. – 2-е изд. – Москва : МЦНМЩ «ЧеРо», 1999.

ПРИЛОЖЕНИЯ

Приложение 1

Компьютерная экспертиза

В. ПОГУЛЯЕВ,
начальник юридического управления
НП «Федерация правообладателей по коллективному управлению Авторскими правами при использовании Произведений в Интерактивном режиме»

Правонарушения, совершаемые с использованием компьютерной техники и телекоммуникационных сетей связи, характеризуются высокой ступенью латентности. Основной их отличительной чертой является то, что злоумышленник может совершать противоправные действия не покидая своих квартиры, дачи или офиса. Компьютерные преступления, в том числе хакерские «атаки» финансовых систем и крупных информационных порталов давно приобрели уже не только организованный, но и трансграничный характер. Универсальные возможности Интернет позволяют нарушителям из разных стран договориться и координировать свои деструктивные действия. Рост численности преступлений, совершаемых в сфере информационного обмена, их многочисленные разновидности и изощренность, способность нарушителей оперативно устранять следы своего вмешательства в нормальное течение информационных процессов – все это обуславливает необходимость в постоянном повышении квалификации, уровня знаний и подготовки правоведов и других специалистов, которые вынуждены противостоять хакерам и другим компьютерным злоумышленникам.

Компьютерная преступность, несмотря на свою «молодость» по отношению к другим более древним видам противоправных деяний, уже имеет свою многолетнюю историю и даже классификацию. Первые компьютерные преступления были зарегистрированы в конце 60-х г. прошлого века. Начиная с 90-х годов крупнейшие банки России уже вовсю подвергались хакерским «атакам». Кодификатор Генерального Секретариата Интерпола делит компьютерные преступления следующим образом: 1) QA – несанкционированный доступ и перехват (сюда входят: QAH – компьютерный абордаж; QAI – перехват; QAT – кража времени; QAZ – другие виды несанкционированного

доступа и перехвата); 2) QD – изменение компьютерных данных (QDL – логическая бомба; QDT – троянский конь; QDV – компьютерный вирус; QDW – компьютерный червь; QDZ – прочее); 3) QF – Компьютерное мошенничество (QFC – мошенничество с банкоматами; QFF – компьютерная подделка; QFG – мошенничество с игровыми автоматами; QFM – манипуляции с программами ввода-вывода; QFP – мошенничества с платежными средствами; QFT – телефонное мошенничество; QFZ – прочее); 4) QR – Незаконное копирование (QRG – компьютерные игры; QRS – другое программное обеспечение; QRT – топология полупроводниковых устройств; QRZ – другие виды незаконного копирования); 5) QS – Компьютерный саботаж (QSH – с аппаратным обеспечением; QSS – с программным обеспечением; QSZ – прочие виды саботажа); 6) QZ – Прочие компьютерные преступления (QZB – с использованием компьютерных досок объявлений; QZE – хищение информации, составляющей коммерческую тайну; QZS – передача информации, подлежащая судебному рассмотрению; QZZ – прочие компьютерные преступления).

Учитывая это, очевидно, что для раскрытия преступлений в сфере компьютерной информации, всестороннего и правильного рассмотрения дела в суде и вынесения обоснованного решения во многих случаях (а точнее – в большинстве) требуются специальные познания в области компьютерной техники. Изучение состояния компьютерной информации, изменений, которые она претерпела в тот или иной период времени, носителей, на которых эта информация содержится, программного и аппаратного обеспечения электронно-вычислительных машин, которые подверглись несанкционированному воздействию «извне», а также устройств, при помощи которых это воздействие предположительно осуществлялось – предмет особых исследований, именуемых в литературе компьютерной, компьютерно-технической, информационно-технической экспертизой. В настоящей работе в целях удобства и универсальности мы применяем термин «компьютерная экспертиза».

Указанная экспертиза в основном назначается по уголовным делам. Однако ее роль в гражданском и арбитражном процессе также представляется немаловажной. Назначается и проводится компьютерная экспертиза строго в соответствии с нормами УПК РФ, ГПК РФ и АПК РФ, а также Федеральным законом «О государственной судебно-экспертной деятельности в Российской Федерации» от 31 мая 2001 г. № 73-ФЗ. Прежде всего, эта строгость касается оснований и процедуры изъятия (ареста) средств компьютерной техники для проведения экспертизы. Любые на первый взгляд оперативные, а на деле безосно-

вательные или совершенные с превышением полномочий, действия правоохранительных органов или суда в данном случае могут повлечь не только нарушения прав собственности отдельных лиц, но и простой в экономической деятельности целой организации и, как следствие, – причинить значительные убытки. Отметим, что методика изъятия компьютерной техники была подробно описана в специальной литературе (см., например: Россинская, Е. Р. Судебная экспертиза в уголовном, гражданском, арбитражном процессе / Е. Р. Россинская. – Москва : Право и закон, 1996).

Нельзя не упомянуть о существовании еще одной процессуальной формы использования специальных познаний – привлечение **специалиста**. Специалист призван содействовать в обнаружении, закреплении и изъятии доказательств путем применения своих профессиональных знаний и навыков. Его участие очень важно на стадии проведения дознания и предварительного следствия. Кроме того, специалист нередко привлекается для выполнения работы, предшествующей экспертизе, по сути, обеспечивающих ее проведение. Например, не рекомендуется отключать, упаковывать и транспортировать компьютерную технику без рекомендаций специалиста. Иногда, когда компьютерную технику транспортировать вообще невозможно, специалист привлекается для копирования необходимой информации (однако в этом случае существует риск упустить важные детали, т. к. какую именно информацию копировать предстоит решать на месте), либо изъятия из компьютера «жесткого» диска и иных устройств, на которых может содержаться значимая для дела и экспертизы информация.

Перейдем к вопросам квалификации самих эксперта и специалиста. Как отмечалось в литературе, понятия «специалист по компьютерной технике» не существует[1], несмотря на широкое убеждение в противоположном. Каждый специалист в области информационных технологий (**IT**) имеет, как правило, четкую, а во многих случаях – достаточно узкую специализацию. Например, специалист по Windows (ходовые версии – 98, 2000, Millenium, NT, XP) зачастую не разбирается в Microsoft DOS (MS-DOS) и Unix. Поэтому к проведению работ по сбору, фиксированию, обработке доказательств, а также экспертизе по делам, связанным с правонарушениями в области компьютерной информации, необходимо привлекать профессионала в той или иной конкретной области IT.

[1]Курушин, В. Д. Компьютерные преступления и информационная безопасность / В. Д. Курушин, В. А. Минаев. – Москва : Новый Юрист, 1998. – С. 157.

Сказанное касается не только программистов, но и лиц, обслуживающих операционные системы, аппаратное обеспечение ЭВМ, средства связи. Вообще, специальные познания в сфере IT могут быть условно разделены на четыре сферы:

1. Информационные процессы.
2. Межкомпьютерное (сетевое) взаимодействие.
3. Программирование.
4. Автоматизация.

В связи с этим, во многих случаях существует необходимость в проведении комплексной экспертизы. Таковая, например, согласно ст. 82 ГПК РФ назначается судом в том случае, если установление обстоятельств по делу требует одновременного проведения исследований с использованием различных областей знания или с использованием различных научных направлений в пределах одной области знания. Вопросы, поставленные перед тем или иным экспертом не должны выходить за пределы его специальных познаний.

Компьютерная экспертиза может включать в себя исследования программного и аппаратного комплексов, сетей связи. В тех или иных случаях, комплексная компьютерная экспертиза может включать в себя элементы судебной автороведческой, судебной инженерно-технической, судебной психологической, различных судебно-экономических экспертиз.

Одной из наиболее сложных компьютерных экспертиз является компьютерно-сетевая (телематическая) экспертиза. Не менее трудоемкими являются и функции специалистов по сбору, фиксации доказательств и подготовке к данной экспертизе. Чтобы доказать факт злоумышленного проникновения из Интернет и выявить его источник необходимо провести подробное изучение всего программного обеспечения, содержащегося на компьютере – «жертве». Внимание специалистов, прежде всего, будет обращено на Интернет-браузеры, загрузочные компоненты Интернет-приложений и следы (последствия) работы с ними, кэш-память. Будут проанализированы настройки удаленного доступа (в том числе протокола TCP/IP и конфигурации DNS), имеющиеся на компьютере протоколы соединений. Решающее значение порой имеют оперативные эксперименты, проводимые с учетом положений Федерального закона «Об оперативно-розыскной деятельности». Например, преднамеренное «заражение» распространяемым по сети конкретным компьютерным «червем» или «троянцем», а затем слежение за его работой и выявление получателей передаваемой им информации с помощью специальных программных средств.

Для определения подозреваемого (или, по крайней мере, круга подозреваемых лиц) могут быть использованы средства интерактивного общения (чаты, ICQ и т. д.). Нередко хакеры охотно делятся своими «успехами» в кругу коллег. Поэтому, осуществив авторизацию на соответствующем хакерском форуме (чате) и используя особый NIC-name (псевдоним) вполне можно выяснить если не имя и конкретные координаты нарушителя, то какую-то более определенную информацию о нем (адрес личного сайта, электронной почты и т. д.). Такие действия правоохранительных органов по своему содержанию и смыслу подпадают еще под одно оперативно-розыскное мероприятие, предусмотренное ФЗ «Об оперативно-розыскной деятельности», – оперативное внедрение.

Компьютерная экспертиза может проводиться экспертами государственных и негосударственных судебно-экспертных учреждений. Государственными судебно-экспертными учреждениями являются специализированные учреждения федеральных органов исполнительной власти, органов исполнительной власти субъектов РФ, созданные для обеспечения исполнения полномочий судов, судей, органов дознания, лиц, производящих дознание, следователей и прокуроров посредством организации и производства судебной экспертизы (ст. 11 указанного выше Федерального закона от 31 мая 2001 г. № 73-ФЗ). С 1996 г. экспертизы подобного рода на первых порах эпизодически, а затем и систематически начали выполняться в экспертно-криминалистических подразделениях органов внутренних дел и судебно-экспертных учреждениях Министерства юстиции России[2]. Экспертов-криминалистов в данной области сегодня готовят, в частности, Московская академия и Саратовский юридический институт МВД России.

В заключение отметим, что какими бы ни были процедуры определения достоверности доказательств, связанных с компьютерами, в дальнейшем суды будут требовать все более и более четких доказательств с целью обеспечения уверенности в том, что они получены надлежащим и правильным образом, а также тем, что сотрудники, представившие эти доказательства, имеют необходимую квалификацию для их исследования[3].

---

[2]Россинская, Е. Р. Судебная компьютерно-техническая экспертиза / Е. Р. Россинская, А. И. Усов. – Москва : Право и закон, 2001. – С. 11.

[3]Курушин, В. Д. Компьютерные преступления и информационная безопасность / В. Д. Курушин, В. А. Минаев. – Москва : Новый Юрист, 1998. – С. 156

Приложение 2

Криптопровайдер AVEST CSP

ЗАО АВЕСТ является разработчиком и правообладателем единственного на сегодняшний день в Республике Беларусь сертифицированного ГЦБИ криптопровайдера – AVEST CSP.

Криптопровайдер – независимый программный модуль, содержащий реализации низкоуровневых криптографических функций интерфейса Microsoft CryptoSPI – одного из стандартных интерфейсов расширения возможностей Microsoft CryptoAPI.

Microsoft CryptoAPI – развитая система криптографических библиотек, ставшая стандартом де-факто для разработки защищенных приложений на платформе Windows. Одним из важнейших преимуществ Microsoft Crypto API является принцип абстрагирования от специфики криптоалгоритмов, реализуемых в криптопровайдерах, что позволяет приложениям использовать высокоуровневые функции Crypto API (работа с цифровыми сертификатами и их хранилищами, сообщениями в формате PKCS#7, и т. д.) с любым набором криптоалгоритмов (например, криптопровайдер AVEST CSP предоставляет возможность работы с алгоритмами ГОСТ 28147-89, СТБ 1176.1-99, СТБ 1176.2-99, предусмотренными Законом РБ «Об электронном документе»).

В основе криптопровайдера AVEST CSP лежит библиотека криптографических преобразований AvCSPBase.DLL. Данная библиотека содержит высокоэффективную реализацию следующих алгоритмов:

– Симметричного шифрования (согласно стандарту ГОСТ 28147-89).

– Вычисления хэш-функции (согласно стандарту СТБ 1176.1-99).

– Выработки и проверки электронной цифровой подписи (согласно стандарту СТБ 1176.2-99).

– Процедуры выработки псевдослучайных последовательностей (согласно руководящему документу РД РБ 07040.1202-2003 «Банковские технологии. Процедура выработки псевдослучайных данных с использованием секретного параметра»).

– Процедуры выработки общего секретного ключа согласно проекту руководящего документа «Банковские технологии. Протоколы формирования общего ключа», разработанного ГЦБИ.

– Криптопровайдер AVEST CSP позволяет использовать вышеуказанные криптографические алгоритмы через программный интерфейс Microsoft Crypto API версий 1 и 2. Такой подход имеет следующие достоинства:

– Разработчики программных средств могут использовать криптографические функции, встроенные в операционные системы Microsoft Windows, используя для этого высокоуровневые (CryptoAPI 2) или низкоуровневые (CryptoAPI 1) функции или CAPI COM-интерфейс.

– Становится возможным использование перечисленных криптоалгоритмов в уже разработанных или разрабатываемых независимо от криптопровайдера Avest CSP Base продуктах, использующих Microsoft Crypto API.

– Автоматически (за счет использования CryptoAPI 2) обеспечивается поддержка международных форматов представления криптографических данных (сообщений, ключевой информации и т. д.). В частности, используемые форматы удовлетворяют рекомендациям X.509 и стандартам семейства PKCS (PKCS#7, PKCS#8, PKCS#10, PKCS#12).

Библиотека AvCSPBase.DLL удовлетворяет требованиям руководящего документа РД РБ 07040.1201-2003 «Банковские технологии. Средства выработки электронной цифровой подписи программные. Общие требования». Она разработана на основе программных модулей, имеющих экспертное заключение ГЦБИ.

В настоящее время криптопровайдер AVEST CSP поддерживает следующие носители для хранения личных ключей:

– Rainbow iKey™1000,
– Rainbow iKey™1032,
– RuToken,
– Dallas Semiconductor TouchMemory™,
– Aladdin eToken™ (R2/PRO),
– Смарт-карта ЦНИИС РБ.

Приложение 3

Система постановки виброакустических и акустических помех ЛГШ-401

Система постановки виброакустических и акустических помех ЛГШ-401 предназначена для противодействия специальным средствам несанкционированного съема информации, использующих в качестве канала утечки ограждающие конструкции помещения.

В первую очередь это электронные или акустические стетоскопы для прослушивания через потолки, полы и стены, проводные или радио-микрофоны, установленные на ограждающие конструкции или водопроводные и отопительные трубопроводы, а также лазерные или микроволновые системы съема информации через оконные проемы помещений.

ЛГШ-401 обеспечивает защиту путем постановки широкополосной виброакустической шумовой помехи на потенциально опасные конструкции помещений. Кроме того, предусмотрена возможность установки акустического излучателя для защиты воздуховодов и вентиляционных шахт.

В состав системы **ЛГШ-401** входят:

– генератор шума ЛГШv401;

– пьезоэлектрические вибропреобразователи ЛВП-А и/или ЛВП-Б (общим количеством до 16 штук);

– акустический излучатель.

Генератор шума **ЛГШ-401** представляет собой восьмиканальный цифровой генератор псевдослучайной последовательности импульсов тактовой частоты 5 кГц с кварцевой стабилизацией. Выходы генератора предназначены для подключения шестнадцати пьезоэлектрических вибропреобразователей (по два последовательно соединенных вибропреобразователя на каждый канал) и одного акустического преобразователя.

Отличительной особенностью **ЛГШ-401** является наличие системы контроля состояния подключенных вибропреобразователей. Она позволяет оперативно определять обрыв соединительных проводов или короткое замыкание для каждого из восьми каналов генератора с сигнализацией на светодиодных индикаторах. Предусмотрена возможность подключения дистанционного устройства управления устройством.

Вибропреобразователи предназначены для передачи генерируемой помехи на строительные, ограждающие и инженерные конструкции:

– ЛВП-А – для установки на стены, полы, потолки и трубопроводы;

– ЛВП-Б – для установки на стекло или раму каждого оконного проема.

Вибропреобразователи могут комплектоваться различными крепежными арматурами, в зависимости от места их установки.

Примечание. Базовый комплект поставки включает только генератор шума ЛГШ-401. Включение в комплект поставки необходимого количества вибропреобразователей, креплений к ним и акустического излучателя оговаривается отдельно. Гарантийный срок – 18 месяцев с даты приобретения.

Технические характеристики модели:

Количество виброакустических каналов 8

Количество вибропреобразователей, подключаемых к генератору при последовательном подключении двух вибропреобразователей на один выходной канал ……..16

Количество акустических каналов ……..……..1

Среднеквадратическое напряжение акустического канала на нагрузке 8 Ом ……не менее 8 В

Амплитуда напряжения виброакустического канала ……не менее 130 В

Диапазон регулирования выходного сигнала акустического канала ……не менее 40 дБ

Диапазон регулирования выходного сигнала виброакустического канала ……..не менее 6 дБ

Период повторения псевдослучайной последовательности ……...не менее 39 суток

Потребляемая мощность ……не более 20 Вт

Габаритные размеры генераторного блока ……...200×125×50 мм

Масса генераторного блока ……не более 1 кг

Приложение 4

Аппаратура обнаружения и подавления сотовых телефонов «МОСКИТ»

Москит-GSM

Миниатюрное устройство индикации включения мобильного телефона в режим передачи позволяет вовремя обнаружить работающий телефон

Технические характеристики:

Дальность определения мобильного телефона стандарта GSM 900/1800 МГц – не менее 2–3 м
Звуковая и светодиодная индикация работы телефона
Длительность непрерывной работы – не менее 300 часов
Конструктивное исполнение в виде брелка
Питание от стандартной батареи – 6 В (11А-С5)

Москит-плюс 1

Малогабаритное автономное устройство подавления мобильного телефона, включенного в режим передачи, позволяет предотвратить утечку информации

Технические характеристики:

Дальность определения мобильного телефона стандарта GSM 900/1800 МГц – не менее 2–3 м
Светодиодная индикация работы телефона
Длительность непрерывной работы – не менее 8 часов
Питание от батареи – 9 В (6PLF22)

Москит-плюс 2

Малогабаритное (с сетевым питанием) устройство подавления мобильного телефона, включенного в режим передачи, позволяет предотвратить утечку информации

Технические характеристики:

Дальность определения мобильного телефона стандарта GSM 900/1800 МГц – не менее 10–15 м
Светодиодная индикация работы телефона
Питание от сетевого адаптера
Возможность регулировки уровня помехи

Москит-плюс 3

Малогабаритное автоматическое устройство обнаружения и подавления мобильного телефона, включенного в режим передачи, позволяет предотвратить утечку информации

Технические характеристики:

Дальность определения мобильного телефона стандарта GSM 900/1800 МГц – не менее 10–15 м
Светодиодная индикация работы телефона
Питание от сети 220 В
Возможность регулировки уровня помехи и чувствительности приемника обнаружителя

Содержание

Учебное электронное издание комбинированного распространения

Учебное издание

Храбров Евгений Александрович

ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Пособие
по одноименному курсу для студентов специальности 1-36 04 02 «Промышленная электроника» дневной и заочной форм обучения
В 2 частях
Часть 1

Электронный аналог печатного издания

Редактор *Н. И. Жукова*
Компьютерная верстка *Н. Б. Козловская*

Подписано в печать 10.07.09.
Формат 60x84/16. Бумага офсетная. Гарнитура «Таймс».
Ризография. Усл. печ. л. 3,02. Уч.-изд. л. 3,2.
Изд. № 104.
E-mail: ic@gstu.gomel.by
http://www.gstu.gomel.by

Издатель и полиграфическое исполнение:
Издательский центр учреждения образования
«Гомельский государственный технический университет
имени П. О. Сухого».
ЛИ № 02330/0549424 от 08.04.2009 г.
246746, г. Гомель, пр. Октября, 48.