32.9
П-57

Партыка Т.Л. Попов И.И.

Информационная безопасность

Т. Л. Партыка, И. И. Попов

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

3-е издание, переработанное и дополненное

Допущено Министерством образования Российской Федерации в качестве учебного пособия для студентов учреждений среднего профессионального образования, обучающихся по специальностям информатики и вычислительной техники

ФОРУМ
МОСКВА
2010

УДК 002.56(075.032)
ББК 32.973я723
П57

Рецензенты:
доцент кафедры «Проектирование автоматизированных информационных систем» РЭА им. Г. В. Плеханова, канд. физ.-мат. наук *Б. В. Евтеев*;
директор Института компьютерных технологий МЭСИ,
зав. кафедрой «Общая теория систем и системного анализа»,
доктор экон. наук, профессор *А. А. Емельянов*;
председатели предметных (цикловых) комиссий Математического колледжа *В. П. Агальцов, В. А. Макунин*

Партыка Т. Л., Попов И. И.
П57 Информационная безопасность : учебное пособие / Т. Л. Партыка, И. И. Попов. — 3-е изд., перераб. и доп. — М. : ФОРУМ, 2010. — 432 с. : ил. — (Профессиональное образование).

ISBN 978-5-91134-246-3

Рассмотрены вопросы информационной безопасности и защиты данных, в том числе в информационно-вычислительных системах и сетях. Дано введение в общие проблемы безопасности, определены роль и место информационной безопасности в системе обеспечения национальной безопасности государства. Рассмотрены проблемы защиты информации в автоматизированных системах обработки данных, криптографические методы защиты информации, вопросы защиты информации в персональных компьютерах, компьютерные вирусы и антивирусные программы, а также проблемы защиты информации в сетях ЭВМ и организации комплексных систем технического обеспечения безопасности.

Для учащихся техникумов, колледжей, а также студентов вузов.

УДК 002.56(075.032)
ББК 32.973я723

ISBN 978-5-91134-246-3

© Партыка Т. Л., Попов И. И., 2007, 2008
© Издательство «ФОРУМ», 2007, 2008

Введение

Современное развитие мировой экономики характеризуется все большей зависимостью рынка от значительного объема информационных потоков. Несмотря на все возрастающие усилия по созданию технологий защиты данных, их уязвимость не только не уменьшается, но и постоянно возрастает. Поэтому актуальность проблем, связанных с защитой потоков данных и обеспечением информационной безопасности их обработки и передачи, все более усиливается.

Проблема защиты информации является многоплановой и комплексной и охватывает ряд важных задач. Например, конфиденциальность данных, которая обеспечивается применением различных криптографических методов и средств (шифрование закрывает данные от посторонних лиц, а также решает задачу их целостности); идентификация пользователя на основе анализа кодов, используемых им для подтверждения своих прав на доступ в систему (сеть), на работу с данными и на их изменение (обеспечивается введением соответствующих паролей, анализом электронной подписи). Перечень аналогичных задач, решаемых для обеспечения информационной безопасности и защиты информации в современных системах обработки и передачи данных, может быть продолжен.

Интенсивное развитие современных информационных технологий, и в особенности сетевых технологий, для этого создает все предпосылки. Сюда необходимо также отнести бурное развитие в настоящее время технических и программных средств обеспечения информационных технологий, обусловленное прогрессом, происшедшим в области микроэлектронной технологии, и появлением новых мультипроцессорных систем обработки данных. В результате расширились функциональные возможности и повысился «интеллект» средств обработки и передачи данных, а также технических средств, применяемых для защиты информации. При решении перечисленных выше задач обяза-

тельным является комплексный подход, требующий необходимого сочетания применяемых законодательных, организационных и программно-технических мер.

Изменения, происходящие в экономической жизни России, — создание финансово-кредитной системы, предприятий различных форм собственности и т. п. — оказывают существенное влияние на вопросы защиты информации. Долгое время в СССР существовала только одна форма собственности — государственная, поэтому информация и секреты на предприятиях были тоже только государственными и охранялись мощными спецслужбами.

Проблемы информационной безопасности постоянно усугубляются процессами проникновения во все сферы общества технических средств обработки и передачи данных и, прежде всего, вычислительных систем. Это дает основание рассмотреть проблему компьютерного права, одним из основных аспектов которой являются так называемые компьютерные посягательства. Об актуальности проблемы свидетельствует обширный перечень возможных способов компьютерных преступлений.

Объектами посягательств могут быть как сами технические средства (компьютеры и периферийные устройства), так и программное обеспечение и базы данных, для которых технические средства являются ресурсом.

В этом смысле компьютер может выступать и как предмет посягательств, и как инструмент их реализации. Если рассматривать раздельно эти роли компьютера, то термин «компьютерное преступление» как юридическая категория не имеет особого смысла. Если компьютер — только объект посягательства, то квалификация правонарушения может быть произведена по существующим нормам права. Если же — только инструмент, то достаточен только такой признак, как «применение технических средств». Возможно объединение указанных понятий, когда компьютер одновременно и инструмент, и предмет. В частности, к этой ситуации относится факт хищения машинной информации. Если хищение информации связано с потерей материальных и финансовых ценностей, то этот факт можно квалифицировать как преступление. Также, если с данным фактом связываются нарушения интересов национальной безопасности, авторского права, то уголовная ответственность прямо предусмотрена законами РФ.

Каждый сбой работы компьютерной сети — это не только «моральный» ущерб для работников предприятия и сетевых адми-

нистраторов. По мере развития технологий электронных платежей, «безбумажного» документооборота серьезный сбой локальных сетей может полностью парализовать работу целых корпораций и банков, что приводит к ощутимым материальным потерям. Не случайно, что защита данных в компьютерных сетях становится одной из самых острых проблем в современной информатике. На сегодняшний день сформулировано три базовых принципа, которые должна обеспечивать информационная безопасность:

- *целостность данных* — защита от сбоев, ведущих к потере информации, а также защита от неавторизованного создания или уничтожения данных;
- *конфиденциальность* информации;
- *доступность* информации для всех авторизованных пользователей.

Следует отметить, что отдельные сферы деятельности (банковские и финансовые институты, информационные сети, системы государственного управления, оборонные и специальные структуры) требуют специальных мер безопасности и предъявляют повышенные требования к надежности функционирования информационных систем в соответствии с характером и важностью решаемых ими задач.

При разработке компьютерных систем, выход из строя или ошибки в работе которых могут привести к тяжелым последствиям, вопросы компьютерной безопасности становятся первоочередными. Известно много мер, направленных на обеспечение компьютерной безопасности, основными среди них являются *технические*, *организационные* и *правовые*.

К техническим мерам необходимо отнести защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку оборудования обнаружения и тушения пожара и оборудования обнаружения утечек воды, принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

К организационным мерам относятся охрана вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра после выхо-

да его из строя, организация обслуживания вычислительного центра посторонней организацией или лицами, не заинтересованными в сокрытии фактов нарушения работы центра, универсальная эффективность средств защиты для всех пользователей — потенциальных нарушителей (включая высшее руководство), возложение ответственности на лиц, которые должны обеспечить безопасность центра, выбор места расположения центра и т. п.

К правовым мерам следует отнести разработку норм, устанавливающих ответственность за компьютерные преступления, предусматривающих защиту авторских прав программистов, а также совершенствование уголовного и гражданского законодательства, процесса судопроизводства. К правовым мерам относятся и вопросы общественного контроля за разработчиками компьютерных систем и принятие международных договоров, регламентирующих эту деятельность в той степени, в какой они влияют или могут повлиять на военные, экономические и социальные аспекты жизни стран, заключающих соглашение.

Концентрация информации в компьютерах — аналогично концентрации наличных денег в банках — заставляет все более усиливать контроль в целях защиты информации. Юридические вопросы, служебная тайна, национальная безопасность — все эти соображения требуют усиления внутреннего контроля в коммерческих и правительственных организациях. Работы в этом направлении привели к появлению новой дисциплины: информационная безопасность. Специалист в области защиты информации отвечает за разработку, реализацию и эксплуатацию системы обеспечения целостности, пригодности и конфиденциальности накопленной в организации информации. В его функции входит обеспечение физической (технические средства, линии связи и удаленные компьютеры) и логической (данные, прикладные программы, операционная система) защиты информационных ресурсов.

Сложность создания системы защиты информации определяется тем, что данные могут быть похищены из компьютера и одновременно оставаться на месте; ценность данных для нарушителя может заключаться только в обладании ими, а не в уничтожении или изменении.

Обеспечение безопасности информации — дорогое дело, и не только из-за затрат на закупку или установку средств защиты, но также из-за того, что трудно квалифицированно определить

границы разумной безопасности и обеспечить соответствующее поддержание системы в работоспособном состоянии.

Средства защиты информации нельзя проектировать, покупать или устанавливать до тех пор, пока не произведен соответствующий анализ. Анализ риска должен дать объективную оценку многих факторов (подверженности к появлению нарушения работы системы, вероятности появления нарушения работы, ущерба от коммерческих потерь, снижения коэффициента готовности системы, общественных отношений, юридических проблем) и предоставить информацию для определения подходящих типов и уровней безопасности. Коммерческие организации все в большей степени переносят критическую корпоративную информацию с больших вычислительных систем в среду открытых систем и встречаются с новыми и сложными проблемами при реализации и эксплуатации систем безопасности. Сегодня все больше организаций разворачивают мощные распределенные базы данных и приложения архитектуры «клиент—сервер» для управления коммерческими данными. При увеличении степени распределенности возрастает также и риск неавторизованного доступа к данным и их искажения.

Шифрование данных традиционно использовалось правительственными и оборонными ведомствами, но в связи с необходимостью защиты коммерческой тайны частные компании тоже начинают использовать возможности, предоставляемые шифрованием для обеспечения конфиденциальности информации.

Следует подчеркнуть, что никакие аппаратные, программные и любые другие решения не смогут гарантировать абсолютную надежность и безопасность данных в компьютерных системах. В то же время свести риск потерь к минимуму возможно, но лишь при комплексном подходе к вопросам безопасности.

В первой главе настоящего учебного пособия рассмотрены общие проблемы безопасности. Дается определение предмета и структура национальной безопасности, ее составляющие и история вопроса. Анализируется информационная безопасность и ее место в системе национальной безопасности, определяются жизненно важные интересы в информационной сфере и угрозы для них. Рассмотрены вопросы информационной войны, информационного оружия, принципы, основные задачи и функции обеспечения информационной безопасности, функции государственной системы по обеспечению информационной безопасности, отечественные и зарубежные стандарты в области информацион-

ной безопасности. Значительное внимание уделяется также правовым вопросам информационной безопасности.

Во второй главе рассматриваются общие вопросы защиты информации в автоматизированных системах обработки данных (АСОД), предмет и объекты защиты информации, задачи защиты информации в АСОД. Рассмотрены типы преднамеренных угроз безопасности и методы защиты информации в АСОД. Рассмотрены методы и средства подтверждения подлинности пользователей и разграничения их доступа к компьютерным ресурсам, контроля доступа к аппаратуре, использования простых и динамически изменяющихся паролей, методы модификации схемы простых паролей, функциональные методы.

В третьей главе излагаются проблемы криптографической защиты информации — криптология и основные этапы ее развития, методы криптографического закрытия, подстановки и перестановки, одноалфавитные и многоалфавитные системы. Рассматриваются системы одноразового использования, системы шифрования Вижинера, шифрование методом гаммирования, шифрование с помощью аналитических преобразований. Рассматриваются кодирование и рассечение-разнесение данных. Дается понятие систем с открытым ключом, электронной цифровой подписи. Кратко описаны криптографические стандарты DES и ГОСТ 28147—89.

Глава четвертая посвящена проблематике защиты информации в персональных компьютерах (ПК) — особенности защиты и угрозы информации в ПК. Рассмотрены проблемы обеспечения целостности информации в ПК, опознавания (аутентификации) пользователей и используемых компонентов обработки информации, разграничения доступа к элементам защищаемой информации, криптографическое закрытие защищаемой информации. Рассматриваются некоторые конкретные системы защиты в среде MS-DOS и в средах Windows. Кратко описана задача защиты ПК от вредоносных закладок (разрушающих программных средств), приведена классификация закладок и даны общие их характеристики.

В пятой главе более подробно рассмотрены разрушающие программные средства класса компьютерных вирусов и методы борьбы с ними. Даются определение и классификация компьютерных вирусов, приводятся примеры их «функционирования», признаки проявления вируса в ПК. Рассмотрены методы защиты и классы антивирусных программ. Подробно рассмотрены воз-

можности наиболее популярных антивирусных программ — Антивирус Касперского; антивирус-ревизор диска ADinf для Windows. Описаны основные режимы работы — проверки дисков, построения таблиц, поиска стелс-вирусов, просмотра истории изменений, просмотра результатов. Кратко охарактеризованы известные программы Dr.Web и Symantec Antivirus.

Шестая глава посвящена вопросам защиты информации в сетях ЭВМ. Рассмотрены разновидности ВС по топологии (конфигурации), сетевые операционные системы (ОС), межсетевое взаимодействие, структура прикладного программного обеспечения в локальных вычислительных сетях (ЛВС). Рассмотрены цели, функции и задачи защиты информации в сетях ЭВМ, понятие сервисов безопасности, а также архитектура механизмов защиты информации в сетях ЭВМ, методы цифровой подписи данных, передаваемых в сети. Приводится пример системы защиты локальной вычислительной сети, кратко рассмотрены принципы функционирования межсетевых экранов (FireWall) и прокси- (Proxy-) серверов. Рассмотрены примеры систем активного аудита в информационных сетях.

В седьмой главе рассматриваются технические средства и вопросы комплексного обеспечения защиты каналов утечки информации. Характеризуются технические средства защиты, механические системы защиты, системы оповещения, системы опознавания, оборонительные системы, охранное освещение. Приводится пример комплекса физической защиты. Рассмотрены средства контроля доступа, замки, автоматизированные системы контроля доступа, биометрические системы идентификации и т. д. Даются краткие эксплуатационные характеристики ряда технических средств защиты.

Учебное пособие базируется на материалах, накопленных авторами в процессе практической, исследовательской, а также преподавательской (МИФИ, МИСИ, МГУ, РГГУ, РЭА им. Г. В. Плеханова) деятельности. Авторы выражают благодарность коллегам, принявшим участие в обсуждении материала: Н. В. Максимову, А. Г. Романенко (РГГУ), К.И. Курбакову (РЭА им. Г. В. Плеханова), П. Б. Храмцову (РНИЦ «Курчатовский институт»), рецензентам, а также студентам РЭА им. Г. В. Плеханова и РГГУ за предоставленные иллюстративные материалы.

Глава 1
ОБЩИЕ ПРОБЛЕМЫ БЕЗОПАСНОСТИ. РОЛЬ И МЕСТО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основанием для определения содержания национальной безопасности, в рамках классических традиций и имеющейся мировой практики, является наличие сформулированных *национальных интересов* — осознанных потребностей нации в самосохранении и развитии [21].

Под *интересом* понимается причина действий индивидов, социальных общностей (класса, нации, профессиональной группы), определяющих их социальное поведение.

Интересы различают:

а) по степени общности (индивидуальные, групповые, общественные);

б) направленности (экономические, политические, духовные);

в) степени осознанности (реализующиеся стихийно или на основе программы);

г) возможности осуществления (реальные и мнимые);

д) отношению к объективной тенденции общественного развития (прогрессивные, реакционные, консервативные);

е) срокам реализации (долгосрочные, среднесрочные, краткосрочные);

ж) характеру субъекта (классовые, национальные, профессиональные).

1.1. Национальные интересы и безопасность

Предпосылкой идеи национальных интересов стало обособление племенных, а затем государственных и национальных общностей, породившее стереотипы сознания в делении «мы — они», «наше — не наше».

Но ее современное понимание начало формироваться лишь на рубеже XVIII и XIX столетий. Особое значение в этом плане имело становление институтов гражданского общества и демократических механизмов, способствующих выявлению народной (национальной) воли и ее определяющему воздействию на политику государств. Выработанные европейской цивилизацией, концепции национальных интересов как совокупности общих интересов граждан национального государства и национальной безопасности, как системы государственной защиты этих интересов, личности, собственности основываются на реально существующем в развитых странах гражданском обществе. Признанные к концу XX в. практически во всем мире демократические институты обеспечивают приближение к такому порядку, при котором народ если и не полновластно распоряжается своей судьбой, то, по крайней мере, не целиком лишен такой возможности.

История вопроса

В дореволюционной России концепция национальных интересов имела форму утверждения монархического строя. Тогда сущность государства определялась формулой «самодержавие — православие — народность». После Октябрьской революции 1917 г. концепция национальных интересов оказалась невостребованной уже из-за ориентации на интернационализм. Таким образом, можно считать, что к моменту распада СССР в 1991 г. в России отсутствовала целостная концепция национальных интересов и их защиты.

В идеологии Советского государства доминирующее положение среди всех интересов занимали классовые интересы, что мотивировалось известным положением марксистско-ленинской философии об объяснении всех интересов, исходя из классовых: «люди всегда были и всегда будут глупенькими жертвами обмана и самообмана в политике, пока не научатся за любыми нравственными, религиозными, политическими, социальными фразами, заявлениями, обещаниями разыскивать интересы тех или иных классов». Следует отметить, что даже с появлением таких понятий, как «новая социальная и интернациональная общность людей — советский народ», национальные интересы как общенародные интересы не были определены, хотя это логично бы вытекало из изначального понимания «интереса» (нужды, потреб-

ности) и «нации» (от *лат.* natio — народ). Предполагалось, что «после полной победы коммунизма всестороннее сближение наций приведет к постепенному исчезновению национальных различий».

Нация понималась только исходя из значения в узком смысле, как «исторически сложившаяся форма общности людей, которая приходит на смену народности», и рассматривалась лишь как составная часть народа наряду с народностями. Вместо национальных интересов руководством правящей партии и страны на этапе горбачевской перестройки были предложены «общечеловеческие ценности» в качестве главного национального приоритета.

Центральной проблемой в определении национальных интересов является установление их объектного состава. Характерно, что в отличие от английского языка, допускающего употребление понятия Nation в качестве синонима понятия State, в русском языке два эти понятия — нация и государство — четко различаются. И многие теоретики при определении понятия национальных интересов исходили из потребностей страны, но в дальнейшем понимали под национальными интересами наиболее существенные потребности российского общества и государства, удовлетворение которых обеспечивает их существование и развитие и которые поэтому являются важнейшими целями внутренней и внешней политики. В то же время в этом понятии национальных интересов отсутствуют потребности личности как основа интересов человека. Следует признать, что это достаточно распространенная ошибка, когда забывают включать этот элемент в структуру национальных интересов. Производным такого подхода является понимание национальной безопасности как совокупности только государственной и общественной безопасности.

Таким образом, исходя из предложенных определений и классификации интересов, национальный интерес возникает только тогда, когда его субъектом выступает нация, что не равнозначно общенародному интересу. Поэтому необходимо рассматривать понятие «нация» в широком смысле как равнозначное «народу», а национальные интересы определять исходя из степени их общности. Некоторые ученые предлагают решение этой проблемы за счет введения понятия «общенациональные интересы».

Существует различие между государственными и общественными потребностями людей, влияющими на формирование на-

циональных интересов. Повсюду в мире, в том числе в странах, обладающих многовековыми демократическими традициями, существует бóльшая или меньшая степень расхождения между тем, как понимают национальные интересы «элита» и «простой народ», правящие круги и оппозиция. У бюрократического аппарата, составляющего костяк государственного механизма, имеются собственные интересы, далеко не всегда совпадающие с потребностями общества и интересами граждан. В России больше, чем где-либо, государственный интерес издавна доминировал над общественным, первое место среди приоритетов однозначно отдавалось могуществу российской державы, а не благосостоянию ее граждан. Такой подход сохранялся и в советское время. Демократические реформы 80—90-х годов, положив начало формированию гражданского общества, создали предпосылки для того, чтобы в понимании национальных интересов, а значит, в формулировании задач внутренней и внешней политики, достигался разумный баланс между непосредственно «державными» и общественными потребностями, принимались во внимание интересы различных социальных групп, частные интересы и права граждан в их совокупности.

Во второй половине 1990-х годов было проведено множество исследований, конференций, семинаров, слушаний, итогом которых стали проекты, программы и концепции по этой теме. Среди них можно выделить проект «Политика национальной безопасности Российской Федерации» (1996—2000), подготовленный в Российском научном фонде. В научном докладе, подводящем итоги исследований, авторы проекта предложили решение на основе своего понимания общенациональной идеи, национальных интересов, ценности, целей и приоритетов. В качестве общенациональной идеи предложено считать «возрождение российского государства, обустройство России, живущей в согласии с собой и с окружающим ее миром», высшим национальным интересом и социальным идеалом России — «обеспечение развития человека, устойчивого роста уровня его жизни и благополучия на основе соблюдения его прав и свобод», которые в свою очередь названы «высшей ценностью», как общенациональная цель — обеспечить «достойный уровень и качество жизни каждого», как главный приоритет государства — развитие его граждан. Как видно даже из этого перечисления, главной особенностью проекта является заявленный приоритет интересов человека перед общественными и государственными.

В то же время авторы другого проекта концепции обеспечения безопасности личности, общества, государства считают, что «определение общенациональных интересов России должно основываться на признании жизненно важных интересов личности, общества и государства в их динамике и необходимости их реализации на сбалансированной основе» [21].

К числу нерешенных пока проблем следует отнести и соотношение интересов по срокам их реализации (долгосрочные, среднесрочные, краткосрочные) — об актуальности этой проблемы говорит то обстоятельство, что пока ни один из заявленных национальных интересов в современной России не реализован в установленные сроки; и отношение интереса к информации, о чем писал еще К. Маркс: «идея неизменно посрамляла себя, как только она отделялась от интереса» и на что указывает само понятие «интерес» во втором его значении — желании вникнуть в суть, узнать, понять, т. е. здесь требует осмысления возможность использования организующей (внешней) информации как средства организации социальных систем.

К важным проблемам относится *соотношение национальных интересов и национальной безопасности.* С одной стороны, безопасность понимается как защищенность самих национальных интересов. С другой стороны, безопасность сама может быть определена как наиболее важный национальный интерес, поскольку обеспечение безопасности — непременное условие выживания страны, без этого невозможно достижение любых других целей. В то же время в условиях кризисного характера развития общественных процессов в нашей стране существует реальная опасность слияния предметов национальных интересов и собственно национальной безопасности. В результате возникла тенденция включать в это понятие едва ли не всю проблематику жизни и деятельности современного общества.

Национальные интересы и безопасность России

Формирование системы взглядов и подходов по определению государственной политики национальной безопасности в условиях становления новой государственности России началось при следующих исходных условиях, предопределивших как особенности, так и трудности этого процесса.

В национальном отношении Россия представляет собой уникальную общность. С одной стороны, ее можно считать мононациональной, поскольку более $^4/_5$ населения — русские. С другой, в ней насчитывается более 100 народностей, проживающих в основном компактно на своих исторических землях и сохранивших, несмотря на мощное притяжение русского языка и культуры, свои языки, культуру, обычаи, традиции, сознание самобытности. Многие народности сохранили собственную субгосударственность или приобрели различные формы политической автономии в составе России. При доминирующей роли православного христианства около 20 % населения исповедуют ислам, существуют крупные общины приверженцев буддизма, иудаизма, т. е. практически всех основных конфессий.

Таким образом, несмотря на, безусловно, ведущую и интегрирующую роль русского народа, Россия не стала «нацией-государством» как некоторые развитые страны мира. У русского и других народов, населяющих нашу страну, есть свои специфические потребности, которые должны быть согласованы и учтены во внутренней (особенно национальной) и внешней политике Российского государства. В силу этих обстоятельств существует точка зрения, что общие интересы России как целостного социально-политического образования выражают интересы всех россиян, которые и должны быть положены в основу национальных интересов государства.

Особенностью современной России является и переходное состояние российского общества. Концептуализация национальных интересов и национальной безопасности России в условиях только еще начавшегося и встречающего все нарастающие осложнения процесса перехода от системы распределения материальных и трудовых ресурсов к рыночной системе обмена в условиях начала становления гражданского общества требует неординарных подходов. Демократические реформы далеки от завершения. Все еще остро стоит проблема перехода от сверхцентрализованной к рыночной экономике, к интегрированию в международные экономические структуры. Череда лет реформ, местами разрушив, а местами основательно подорвав господствовавшую в течение семидесяти лет систему ценностей, не построила на ее месте иной. Безбрежный плюрализм, близкий к анархии, до крайности затруднил достижения общественного согласия по ключевым вопросам, а значит, и четкое формулирование национальных интересов. Разработке целостной доктрины

национальной безопасности серьезно препятствовало отсутствие политического согласия между элитами общества по базовым концептуальным вопросам в этой сфере. В то же время концепция национальных интересов могла бы выполнить функцию консолидации общества вокруг базовых ценностей, которые разделяло бы подавляющее большинство граждан, несмотря на имеющиеся между ними идейные, социальные, национальные и конфессиональные различия.

При определении национальных интересов и национальной безопасности России учитывают следующие предпосылки:

а) объективную слабость России, перешедшей в состав «средних держав»;

б) потерю стратегического интереса Запада к России, обусловленную как слабостью, так и «замкнутостью на себе» развитых стран Европы. Достаточно ясно, что финансовые ограничения, отсутствие серьезных иностранных инвестиций и в то же время высокая ресурсная самообеспеченность диктуют необходимость возврата к традиционной для России континентальной стратегии, частичный отказ от навязанного коммунистическим мессианством и случайностями истории глобального вовлечения России в дела всего мира.

Если ценностные ориентации выступают как категории устойчивые, определяющие, то национальные интересы и национальные цели — как категории подвижные, изменчивые, что обусловлено конкретными геополитическими и стратегическими условиями, внутренней и международной ситуацией, характером имеющихся и зарождающихся противоречий и порождаемыми ими угрозами национальной безопасности в конкретно-исторической обстановке.

Ряд теоретиков считают, что основной национальный интерес, стоящий перед современной Россией, заключается в воссоздании самобытного, уникального многонационального, демократического государственного образования на собственной цивилизационной основе, способного вобрать в себя достижения иных цивилизаций, но не подменить ими свою самобытность. При этом интеграцию России в международное сообщество следует рассматривать, прежде всего, как средство обеспечения национальных интересов, так как превращение интеграции в самоцель (и это показал короткий исторический опыт новой России) сопряжено с отказом от основных ценностных ориентаций рос-

сийской цивилизации, с потерей экономической и политической независимости.

Российские ученые по итогам проведенного в 1995—97-х годах исследования, исходя из ценностных ориентаций и национальных целей, пришли к следующим определениям.

Под национальными интересами следует понимать «осознанные и официально выраженные (на уровне закона, государственной доктрины, государственной политики) потребности страны, соотнесенные с основными ценностными ориентациями российской цивилизации», под национальными целями — «сформулированные в соответствии с национальными интересами властью и принятые народом установки на достижение будущего состояния общества, государства и личности, при котором единственным и высшим критерием оценки деятельности государства и власти может и должно быть благополучие народа».

В Концепции национальной безопасности РФ (от 10 января 2000 г.) на основе и с учетом результатов проведенных исследований существенно дополнены и конкретизированы положения, ранее закрепленные в Законе РФ «О безопасности» (1992), что предопределяет необходимость их последующего подтверждения в новом Федеральном законе «О национальной безопасности». Приведем краткий сравнительный анализ этих отличий и изменений, поскольку они касаются как обеспечения безопасности, так и отношений, возникающих при этом.

Если в Законе шла речь только о *жизненно важных интересах*, как совокупности потребностей, удовлетворение которых надежно обеспечивают существование и возможности прогрессивного развития личности, общества и государства, то в Концепции введено понятие *национальных интересов* как совокупности сбалансированных интересов личности, общества и государства. При этом ограничен (хотя и условно) перечень областей, национальные интересы в которых определяют предмет национальной безопасности: в экономической, социальной, внутриполитической, международной, информационной сферах, в области военной (оборонной), пограничной и экологической безопасности.

Интересы личности определены в Концепции как полное обеспечение конституционных прав и свобод, личной безопасности, повышения качества и уровня жизни, физического, духовного и интеллектуального развития. *Интересы общества* состоят в

упрочении демократии, создании правового, социального государства, достижении и поддержании общественного согласия, духовном обновлении России. *Интересы государства* состоят в незыблемости конституционного строя, суверенитета и территориальной целостности России, в политической, экономической и социальной стабильности, в безусловном обеспечении законности и поддержании правопорядка, в развитии международного сотрудничества.

В Концепции предложен и несколько иной субъектный состав национальной безопасности и ее обеспечения. Если в соответствии с Законом *систему безопасности* образуют органы законодательной, исполнительной и судебной властей, государственные, общественные и иные организации, объединения, граждане, принимающие участие в обеспечении безопасности, то в Концепции основу системы обеспечения национальной безопасности РФ составляют органы, силы и средства обеспечения национальной безопасности, осуществляющие меры политического, правового, организационного, экономического, военного и иного характера, направленные на обеспечение безопасности личности, общества и государства. В другом положении Концепции указывается, что национальные интересы России носят долгосрочный характер и обеспечиваются институтами государственной власти во взаимодействии с общественными организациями, т. е. здесь граждане выступают лишь как объект безопасности, а участие общества ограничено лишь общественными организациями.

Кроме того, существенно скорректированы основные задачи по обеспечению национальной безопасности РФ, а также направления деятельности и полномочия государственных органов по формированию и реализации политики обеспечения национальной безопасности (Президент РФ, Федеральное Собрание РФ, Правительство РФ, Совет Безопасности РФ, федеральные органы исполнительной власти и органы исполнительной власти субъектов РФ). Приведем лишь некоторые из них, имеющие прямое отношение к теме информационной безопасности:

- своевременное выявление и нейтрализация внешних и внутренних угроз национальной безопасности Российской Федерации;
- преодоление научно-технической и технологической зависимости Российской Федерации от внешних источников;

- обеспечение личной безопасности граждан Российской Федерации, их конституционных прав и свобод;
- обеспечение полноты и совершенствование законодательства Российской Федерации при обеспечении приоритета федерального законодательства;
- принятие эффективных мер по пресечению разведывательной и подрывной деятельности иностранных государств против Российской Федерации;
- разработка организационных и правовых механизмов защиты государственной целостности, единства правового пространства и национальных интересов России;
- выработка и реализация региональной политики, обеспечивающей оптимальный баланс федеральных и региональных интересов;
- совершенствование механизма предупреждения возникновения политических партий и общественных объединений, преследующих сепаратистские и антиконституционные цели, и пресечения их деятельности.

Национальная безопасность, ее определения

В недавнем прошлом под безопасностью понимали защищенность страны от нападения извне, шпионажа, покушения на государственный и общественный строй. До последнего времени само понятие безопасности было слабо разработано, так как исследователи мало внимания уделяли методологическим проблемам безопасности как определенного социального явления, что объяснялось, в свою очередь, закрытостью темы для ученых, когда обращение ученых к этим проблемам считалось деянием просто опасным. В универсальных энциклопедических изданиях, включая Новый иллюстрированный энциклопедический словарь научного издательства БРЭ (1999), это понятие отсутствует. В Большой советской энциклопедии раскрывается лишь понятие «безопасность международная», которое трактуется как «состояние экономических, политических и других отношений между государствами, утверждающее мирное сосуществование государств на началах равноправия, национальную независимость и самостоятельность народов, а также их свободное развитие на демократической основе». Этим понятие «безопас-

ность» сводилось только к противодействию внешним опасностям и угрозам, утверждая тем самым официальную позицию того времени об отсутствии внутренних угроз для безопасности страны.

В восьмитомной Советской военной энциклопедии и в Военном энциклопедическом словаре, изданных в 1970—80-е годы, дается лишь трактовка сугубо прикладных военно-технических видов безопасности: «безопасность полетов», «безопасность плавания», «безопасное удаление», «безопасный временно́й интервал» и т. д. Применение общих понятий «безопасность», «военная безопасность», «безопасность внешняя и внутренняя» почти исключалось, так как было принято считать более точным понятие «оборона», «защита государства» [21].

В. Даль указывал, что безопасность есть отсутствие опасности, сохранность, надежность. По С. Ожегову, безопасность — это «состояние, при котором не угрожает опасность, есть защита от опасности». Сегодня появилось множество других определений безопасности, авторы которых исходят из разных критериев. Иногда полагают, что «безопасность есть состояние, тенденции развития (в том числе латентные) и условия жизнедеятельности социума, его структур, институтов и установлений, при которых обеспечивается сохранение их качественной определенности с объективно обусловленными инновациями, и свободное, соответствующее собственной природе и ею определяемое функционирование».

Столь широкое определение безопасности как состояния или тенденций развития не раскрывает ее специфики как социального явления. Кроме того, если безопасность призвана ограничивать прогресс инновациями в рамках какой-то одной качественной определенности, то она может стать фактором застоя, консерватизма и регресса. Система безопасности не только не должна препятствовать ни количественным (эволюционным), ни качественным (революционным) изменениям (если они объективно назрели), но, напротив, способствовать преодолению без ущерба для общества и граждан устаревших форм жизни. При этом раскрытие понятия «безопасность» через термины «защита», «защищенность», «защитить» суживает его смысл. Защитить — значит, оборонять, закрывать, загораживать что-либо; это вещь, предмет, явление, скрывающие, охраняющие, ограждающие кого или что-либо, наконец, просто щит в прямом и переносном смысле. Примерно в таком смысле трактуется это сло-

во в энциклопедических словарях нашего времени. При этом приуменьшаются, и даже игнорируются, важнейшие свойства и функции безопасности — снижать, ослаблять, устранять и предупреждать опасности и угрозы. Таким образом, смысл слова «защищать» отражает одну из важнейших функций безопасности, но не исчерпывает их.

Представители Института социально-политических исследований РАН считают, что безопасность есть деятельность людей, общества, государства, мирового сообщества народов по выявлению (изучению), предупреждению, ослаблению, устранению (ликвидации) и отражению опасностей и угроз, способных погубить их, лишить фундаментальных материальных и духовных ценностей, нанести неприемлемый (недопустимый объективно и субъективно) ущерб, закрыть путь для выживания и развития.

Другие исследователи рассматривают безопасность страны не как состояние, а как ее системное свойство, позволяющее развиваться и процветать в условиях конфликтов, неопределенности и рисков на основе самоорганизации и управления, и предлагают включить в структуру безопасности страны социальную безопасность (в том числе государственную, национальную), безопасность культуры (в том числе интеллектуальную и информационную), политическую, военную, экономическую, экологическую безопасность и др.

В начале 1990-х годов комиссией союзного парламента, созданной для проработки вопросов по совершенствованию системы безопасности страны, были определены необходимые задачи государственных структур по выработке и реализации такой политики национальной безопасности, которая учитывала бы:

- интересы личности, общества и государства;
- угрозы, оценку возможностей парирования угроз и защиты интересов;
- задачи, функции, структуры и органы, меры противодействия;
- доктрину, концепцию национальной безопасности, концепцию информационной безопасности.

Комиссия пришла к выводу, что общенациональная безопасность реализуется в двух измерениях: общественном и государственном, и подразделяется на внутреннюю и внешнюю в зависимости от источников угроз, опасностей и рисков для жизненно важных интересов. Первоосновой безопас-

ности является *безопасность личности*, что предопределяет *безопасность гражданского общества* и *легитимность государства*.

Для обеспечения национальной безопасности необходима система, включающая совокупность законодательных актов и созданных на их основе структур и механизмов взаимодействия по защите интересов субъектов правоотношений. При этом устойчивость системы должна основываться на общенациональном согласии. Одной из основных составляющих системы обеспечения национальной безопасности была названа информационная безопасность. В качестве условий реализации указанных алгоритмов и задач построения безопасного гражданского общества в информационной сфере были предложены: переход от идеологизированного общества к информационному, научное прогнозирование и моделирование решения возникающих проблем на альтернативной основе, законодательное регулирование и защита информационной деятельности при обеспечении достоверности, открытости и свободы информации, освобождение сознания людей от стереотипов тоталитаризма и прекращение психологической войны политического руководства против народа в любых формах ее проявления.

Известна формула безопасности, закрепленная с 1992 г. в Законе РФ «О безопасности» как «состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз». Исходя из этого, к основным объектам безопасности относятся:

- личность (ее права и свободы);
- общество (его материальные и духовные ценности);
- государство (его конституционный строй, суверенитет и территориальная целостность).

Одновременно с этим государство, организации и граждане относятся и к основным субъектам обеспечения безопасности. Главную роль из них в этом играет государство, которое в соответствии с действующим законодательством должно обеспечивать безопасность каждого гражданина, а также социальную и правовую защиту гражданам и организациям, оказывающим содействие в обеспечении безопасности в соответствии с законом. В то же время закрепленные в этом законе положения нельзя назвать полными и достаточными, так как они не раскрывают механизмов определения интересов, их соотношения и реализации, что обусловлено рядом нерешенных проблем, в том числе методологического порядка.

Таким образом, *национальная безопасность включает в себя три составляющие: государственную безопасность, общественную безопасность и безопасность человека (личную безопасность).* Если первая прямо связана с противодействием угрозам, независимости и территориальной целостности страны, оборонному потенциалу, конституционному строю и связана с защитой институтов, обеспечивающих безопасность этих ценностей, то вторая отражает потребность защиты общественного порядка, собственности во всех ее формах, безопасности личности; третья же характеризует защищенность интересов, прав и свобод человека. Взаимозависимость этих трех составляющих национальной безопасности очевидна [21].

Отсюда возникает следующая проблема в определении национальных интересов — установление соотношения интересов личности, общества и государства. Ослабление любой из этих составляющих — ущерб для страны в целом и для конкретной личности, в частности, но и перекос в определении приоритетов также не менее опасен. Превращение, например, в 1930-е годы государственной безопасности в абсолютную величину (тождественно равную национальной безопасности) привело страну к террору, к массовому уничтожению граждан, подавлению общества и личности, оценке их интересов лишь через призму интересов государства.

Государственная безопасность в те времена следовала политической формуле: народ и общество для государства. В конце 1980-х — начале 1990-х годов объявленный приоритет общественной безопасности, обусловленный приоритетом целей и задач построения гражданского общества, сопровождался разрушением структуры органов государственной безопасности, что (осознанно или неосознанно) оправдывалось стремлением утвердить принцип правового государства: государство для личности и общества.

Если проанализировать эволюцию подхода к решению этого вопроса, то можно выделить три основных принципа в установлении соотношения интересов личности, общества и государства: приоритет интересов — паритет интересов — баланс интересов. Очевидно, более предпочтительным является принцип баланса интересов как принцип, позволяющий наиболее полно учитывать интересы каждого субъекта в конкретных исторических и иных условиях обстановки.

Уровни обеспечения национальной безопасности

Предметная область безопасности определяется следующими первоочередными интересами и целями:

- достижения политической стабильности (управляемости, поддержания порядка, необходимого для нормального функционирования всех общественных и государственных институтов, защиты конституционной законности, прав и свобод граждан);
- обеспечения целостности государства (такой его структуры и политического режима, которые исключают угрозу распада под воздействием внутренних противоречий);
- обороны (защиты независимости и территориальной целостности страны от вооруженной агрессии извне);
- техноэкологической безопасности (предупреждения техногенных катастроф, преодоления последствий стихийных бедствий);
- экономической безопасности (обеспечения экономической самостоятельности страны как условия выживания и развития народа);
- выбора внешнеполитических приоритетов (способствующих созданию максимально благоприятной для России международной среды).

Указанные цели могут быть распределены по уровням, которые определяются в соответствии с общим принципом взаимосвязи личности, общества и государства [21].

На личностном уровне — это надежная защита личной и имущественной безопасности; обеспечение научно обоснованного и гарантированного государством минимума материальных и экологических условий существования при тенденции к их улучшению; реальное обеспечение конституционных прав и свобод личности.

На уровне гражданского общества — преодоление конфронтационности в обществе, достижение и поддержание национального согласия по жизненно важным проблемам политического, экономического, социального, этнонационального развития страны; выход из кризисной демографической и экологической ситуации и обеспечение здоровья населения; ускорение процессов формирования институтов самоорганизации гражданского общества; повышение созидательной активности населения; преодоление экономического кризиса и обеспечение поступательного эконо-

мического развития на началах рыночной экономики; формирование политической и правовой культуры населения, соответствующей принципам гражданского общества; обеспечение признанных международным правом интересов и прав граждан России, проживающих в зарубежных странах; обеспечение экономических, социальных, политических, информационных условий всестороннего развития личности.

На государственном уровне — неуклонное обеспечение суверенитета и территориальной целостности России; обеспечение социально-политической и экономической стабильности страны; защита и обеспечение законных прав, свобод и интересов гражданина; совершенствование федеративного государственного устройства: повышение эффективности защиты конституционного строя, правопорядка, борьбы с организованной преступностью и коррупцией; развитие эффективной системы международных связей на основе партнерства и сотрудничества; создание надежного оборонного потенциала, способного к отражению любой внешней агрессии; развитие всесторонних взаимовыгодных связей со странами СНГ, участие в развитии интеграционных процессов между ними на взаимной основе. Если раньше угрозы имели внешний и военный характер, когда невоенные и военные средства практически невозможно было применять в комплексе, то сейчас в условиях взаимозависимого мира и новых технологий угроза национальной безопасности носит, как правило, комплексный характер. В одних случаях силовое воздействие может включать военный компонент (Ирак, Босния), в других — обходиться практически без его применения (Куба, Ливия, Иран). Наиболее яркий пример тому — поражение СССР в «холодной войне» и его устранение с мировой арены без применения военных мер.

В соответствии с перечисленными уровнями в системе обеспечения национальной безопасности современной России реально действуют несколько групп субъектов:

1. Государство, осуществляющее функции в этой области через органы законодательной, исполнительной, судебной власти, органы прокурорского надзора, через систему правоохранительных органов и специальные службы (в настоящее время здесь можно выделить такие первоочередные проблемы, как разделение полномочий между субъектами обеспечения безопасности «по вертикали»: РФ — субъект РФ — муниципалитеты и координация действий субъектов «по горизонтали»).

2. Общество (в лице негосударственных организаций, представленных частными охранными и детективными предприятиями и организациями, службами безопасности, фондами, научными, информационно-аналитическими центрами и иными структурами — с одной стороны, и криминальные структуры (другая часть общества), создающие «крыши» для борющихся за раздел сфер влияния и захвата собственности мафиозных кругов — с другой).

3. Граждане, вынужденные заниматься самозащитой своих прав и законных интересов от посягательств представителей как криминальных, так, порой, и государственных структур.

Требует дальнейшего совершенствования организация взаимодействия между первым и вторым уровнем — государственной и негосударственной системами обеспечения безопасности, и определение степени и правил участия граждан в обеспечении национальной безопасности, их взаимодействия с государством и обществом. Сегодня государство в лице своих органов рассматривает человека, в основном, как объект своей деятельности и весьма слабо оценивает его как субъекта отношений в сфере общественной и личной безопасности, что может привести к негативным последствиям.

Может наступить отторжение органов общественной безопасности от государства, при слабой осознанности своей зависимости от общества, появляется тенденция превращения этих органов в самодовлеющую силу, концентрирующую свое внимание на чисто профессиональных аспектах деятельности, а долг перед обществом все меньше осознается как основа жизнедеятельности самой системы, в конечном счете, происходит пренебрежение судьбой личности как объекта отношений уже и в сфере общественной безопасности.

Личность, ощущая свое бессилие и незащищенность, ищет иные пути самозащиты (железные двери и домофоны в квартирах, приемы самозащиты и телохранители, оружие и помощь представителей криминального мира и т. п.). В результате система государственной и общественной безопасности начинает рассматриваться личностью либо с равнодушием, либо как враждебная сила. В обществе постепенно под воздействием явлений социального и духовного характера, пренебрежения жизнью и безопасностью личности начинает утверждаться культ жестокости и насилия.

Основные угрозы безопасности России

Сегодня, по оценке ученых из Отделения экономики РАН, можно смоделировать несколько сценариев существенного подрыва безопасности России в результате враждебных действий (без применения военных средств):

Дезорганизация национальной экономики — вплоть до ее банкротства (в результате проведения целенаправленных и масштабных спекуляций на рынке ценных бумаг либо массированного предъявления платежных требований, которые РФ как страна-должник окажется не в состоянии выполнить, с последующим арестом зарубежного имущества и замораживанием банковских счетов и прочими негативными последствиями).

Экономическая блокада, или «мягкое эмбарго» (в форме интенсивной, целенаправленной конкуренции).

Продовольственная уязвимость. Россия рискует перейти в импорте продуктов питания «красную» черту: критический для продовольственной независимости страны уровень порядка 30 %, в то время как в ряде промышленных областей доля зарубежного импорта составляет до 60 %. К этому сценарию примыкает проблема биологической деградации населения вследствие последовательного ухудшения структуры питания и качества продуктов массового потребления.

Технологическая блокада. Россия пока остается страной с образованным населением и высокотехнологичным потенциалом. Однако за последние годы уровень образованности и научно-технический потенциал существенно понизились. За десятилетие (1991—2001) финансирование науки сократилось в 15 раз, численность научных сотрудников — в 5 раз, а финансирование такой специфической научно-технологической среды как наукограды — приблизительно в 100 раз. Имело место также существенное сокращение доли расходов на НИОКР в резко уменьшившемся российском оборонном бюджете. При этом утрата научно-технического потенциала может носить необратимый характер.

Вместе с тем уже сейчас стала актуальной проблема *информационно-коммуникационной безопасности*, например, от целенаправленной компьютерной агрессии либо «ползучей» утраты действенного контроля над национальными информационными и коммуникационными ресурсами. Существует не только вероятность деградации российской экономики до уровня природно-сырьевого анклава мирового хозяйства, но и возможная пер-

спектива поэтапного выведения страны из мировой торговли ресурсами.

Угроза дезинтеграции российского пространства как по этническому признаку, так и в результате «естественного сепаратизма». Например, существует возможность отпадения Дальнего Востока путем постепенного разрыва связей (при сохранении нынешнего состояния экономики) или стремительного отделения вследствие коллапса транспортной либо энергетической системы.

Угроза криминализации общества — утрата государством контроля над экономической и финансовой деятельностью. По различным оценкам, криминальными группировками в той или иной форме контролируется 60—80 % коммерческих и банковских структур. Проявлением этой угрозы является и крупномасштабная коррупция во всех эшелонах власти.

В целом, по оценке российских ученых, в настоящее время критические отметки по более чем десяти предельным показателям опасных социальных процессов, принятые в развитых странах, в России перекрываются в 1,5—3 раза. В то же время такие оценки «катастрофичности» российской практики в очередной раз ставят вопрос об ответственности не только руководителей страны, политиков, но и науки и ее представителей за результаты такой деятельности.

По мнению ряда отечественных ученых, в XXI в. человека (в отношениях с властью) и западную цивилизацию ожидают серьезные испытания. Иранская революция 1980 г. и распад СССР в 1991 г. — суть лишь первые признаки того, что мировая система вступает в период кризиса. Пока выбиваются слабые звенья, но придет черед и сильных, а затем и целого блока звеньев — западной цивилизации с характерным для нее типом отношений человека и власти. Уже сейчас следует готовиться к этому и прогнозировать возможные варианты. Исключительно полезен в этом отношении анализ отечественной истории XIX—XX вв.

В России и СССР за этот период времени уже проиграно (промоделировано) столько вариантов отношений «человек—власть», что можно в какой-то степени говорить о двух последних веках русской истории как о «воспоминании о будущем мира». Достаточно вспомнить, что Россия только в последнем столетии пережила три социальных взрыва, два из которых потрясли до основания государство и общество. Наверное, прав П. Я. Чаадаев, говоривший о том, что призвание России — пре-

поднести миру какой-то важный урок. Урок преподнесен. Теперь в осмыслении новой ситуации перехода от стереотипов прежних интересов и угроз в практике важно максимально сократить дистанцию хаотичных, неорганизованных либо по инерции идущих социальных процессов как у нас в стране, так и за рубежом.

По оценке известного «американиста» А. И. Уткина, российская политика США формируется сегодня в столкновении трех концепций: примата идеологии (борьба с коммунизмом), примата геополитики (борьба с Россией как сверхдержавой и нежелание восстановления ее мощи), примата постепенного вовлечения (примирение) [21].

Мы же, считает он, «живем сейчас в мире обратного движения маятника — от "планетарного гуманизма" к осознанию мирового эгоизма, тщетности примиренческих потуг, наивности самовнушенных верований, железобетона национальных интересов, своекорыстия внешнего мира. Россия достаточно быстро обнаружила, что коммунизм не был единственной преградой на пути сближения ее с Западом. Православие, коллективизм, иная трудовая этика, отсутствие организации, иной исторический опыт, отличный от западного менталитет, различие взглядов элиты и народных масс — все это и многое другое смутило даже стопроцентных западников, увидевших трудности построения рационального капитализма в "нерациональном" обществе, свободного рынка в атмосфере вакуума власти и очага трудолюбия в условиях отторжения конкурентной этики».

1.2. Информационная безопасность

Следующие факторы, наряду с задачами построения гражданского общества в Российской Федерации как информационного общества с возрастанием роли информационных ресурсов и технологий в развитии граждан, общества и государства в XXI в., выводят вопросы *информационной безопасности* на первый план в системе обеспечения национальной безопасности:

- национальные интересы, угрозы им и обеспечение защиты от этих угроз выражаются, реализуются и осуществляются через *информацию* и *информационную* сферу;

- человек и его права, *информация и информационные системы* и права на них — это основные объекты не только информационной безопасности, но и основные элементы всех объектов безопасности во всех ее областях;
- решение задач национальной безопасности связано с использованием *информационного подхода* как основного научно-практического метода;
- проблема национальной безопасности имеет ярко выраженный *информационный характер.*

Укрепление информационной безопасности названо в концепции национальной безопасности Российской Федерации в числе важнейших долгосрочных задач. Роль информационной безопасности и ее место в системе национальной безопасности страны определяются также тем, что государственная информационная политика тесно взаимодействует с государственной политикой обеспечения национальной безопасности страны через систему информационной безопасности, где последняя выступает важным связующим звеном всех основных компонентов государственной политики в единое целое.

Государственная информационная политика (ГИП) представляет собой совокупность целей, отражающих национальные интересы России в информационной сфере, стратегических направлений их достижения (задач) и систему мер их реализующих, она является важной составной частью внешней и внутренней политики государства и охватывает все сферы жизнедеятельности общества.

В рамках такой политики должны быть заложены основы для решения таких крупных задач, как формирование единого информационного пространства России и ее вхождение в мировое информационное пространство, обеспечение информационной безопасности личности, общества и государства, формирование демократически ориентированного массового сознания, становление отрасли информационных услуг, расширение правового поля регулирования общественных отношений, в том числе связанных с получением, распространением и использованием информации.

В целом, сегодня сложились две тенденции в органах государственной власти в определении понятия и структуры информационной безопасности. Представители *гуманитарного направления* связывают информационную безопасность только с институтом тайны. Представители *силовых структур* предлагают

распространить сферу информационной безопасности практически на все вопросы и отношения в информационной сфере, по сути, отождествляя информационную безопасность с информационной сферой. Эти два взаимоисключающих подхода порождают путаницу, причем не только в журнальных статьях, но даже в законодательных актах. Истина, как всегда, лежит посередине.

Под информационной безопасностью (ИБ) понимается состояние защищенности национальных интересов страны (жизненно важных интересов личности, общества и государства на сбалансированной основе) в информационной сфере от внутренних и внешних угроз. Это соответствует логике Закона РФ «О безопасности» и содержанию Концепции национальной безопасности [21].

Перечислим основные составляющие и аспекты информационной безопасности (которые не следует отождествлять с ИБ в целом):

- *защита информации* (в смысле охраны персональных данных, государственной и служебной тайны и других видов информации ограниченного распространения); иногда ошибочно, скорее по инерции, отождествляют два разных понятия — защиту информации и информационную безопасность, хотя это сегодня совсем не одно и то же;
- *компьютерная безопасность или безопасность данных* — набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных в компьютерных сетях, меры по защите информации от неавторизованного доступа, разрушения модификации, раскрытия и задержек в доступе, при этом используется термин *«критические данные»*, под которыми понимают данные, требующие защиты из-за вероятности нанесения (риска) ущерба и его величины в том случае, если произойдет случайное или умышленное раскрытие, изменение или разрушение данных. Целью является обезопасить систему, защитить и гарантировать точность и целостность информации, минимизировать разрушения, которые могут иметь место, если информация будет модифицирована или разрушена. При этом достигаются следующие цели: конфиденциальность критической информации, целостность информации и связанных с ней процессов (создания, ввода, обработки и вывода); доступность информации, когда она нужна; учет всех процессов, связанных с информацией;

- *защищенность информации и поддерживающей инфраструктуры* от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры;
- *защищенность потребностей граждан*, отдельных групп и социальных слоев, массовых объединений людей и населения в целом в качественной (ценной) информации, необходимой для их жизнедеятельности (функционирования), образования и развития, т. е. информационно-психологическая удовлетворенность потребностей граждан и защищенность от негативных (преднамеренных и случайных) информационно-психологических и информационно-технических воздействий.

Жизненно важные интересы в информационной сфере и угрозы жизненно важным интересам в информационной сфере

По общей направленности угрозы информационной безопасности Российской Федерации подразделяются на:

- угрозы конституционным правам и свободам граждан в области духовной жизни и информационной деятельности, духовному возрождению России;
- угрозы развитию отечественной индустрии средств информатизации, телекоммуникаций и связи, обеспечению потребностей внутреннего рынка, выходу ее продукции на мировые рынки, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
- угрозы безопасности информационных ресурсов, нормальному функционированию информационных и телекоммуникационных систем как развернутых, так и создаваемых на территории России.

В Концепции национальной безопасности особое значение для обеспечения национальной безопасности Российской Федерации придается использованию возможностей разведки и контрразведки в целях своевременного обнаружения угроз и определения их источников.

По уровням угрозы ИБ могут быть классифицированы следующим образом:

а) для личности:

- нарушение конституционных прав и свобод граждан на поиск, получение, передачу, производство и распространение объективной информации;
- лишение права граждан на неприкосновенность частной жизни;
- нарушение права граждан на защиту своего здоровья от неосознаваемой человеком вредной информации;
- посягательства на объекты интеллектуальной собственности;

б) для общества:

- препятствия в построении информационного общества;
- лишение права на духовное обновление общества, сохранение его нравственных ценностей, утверждение в обществе идеалов высокой нравственности, патриотизма и гуманизма, развитие многовековых духовных традиций Отечества, пропаганду национального, культурного наследия, норм морали и общественной нравственности;
- манипулирование массовым сознанием;
- создание атмосферы, препятствующей приоритетному развитию современных телекоммуникационных технологий, сохранению и развитию отечественного научного и производственного потенциала;

в) для государства:

противодействие:

- защите интересов личности и общества;
- построению правового государства;
- формированию институтов общественного контроля за органами государственной власти;
- формированию системы подготовки, принятия и реализации решений органами государственной власти, обеспечивающей баланс интересов личности, общества и государства;
- защите государственных информационных систем и государственных информационных ресурсов;
- защите единого информационного пространства страны.

По происхождению основные угрозы жизненно важным интересам личности, общества и государства в информационной сфере включают:

а) внутренние:

- отставание России от ведущих стран мира по уровню информатизации;
- ослабление роли русского языка как государственного языка Российской Федерации;
- размывание единого правового пространства страны вследствие принятия субъектами Российской Федерации нормативных правовых актов, противоречащих Конституции Российской Федерации и федеральному законодательству;
- разрушение единого информационного и духовного пространства России, активизация различного рода религиозных сект, наносящих значительный ущерб духовной жизни общества, представляющих прямую опасность для жизни и здоровья граждан;
- отсутствие четко сформулированной информационной политики, отвечающей национальным целям, ценностям и интересам;

б) внешние:

- целенаправленное вмешательство и проникновение в деятельность и развитие информационных систем Российской Федерации;
- стремление сократить использование русского языка как средства общения за пределами России;
- попытки не допустить участия России на равноправной основе в международном информационном обмене;
- подготовка к информационным войнам и использование информационного оружия.

Информационная война

В Концепции национальной безопасности РФ отмечено усиление угроз безопасности Российской Федерации в информационной сфере и стремление ряда стран к доминированию в мировом информационном пространстве, вытеснению России с внешнего и внутреннего информационного рынка, а также сделан вывод

о том, что «серьезную опасность представляет разработка рядом государств концепции *информационных войн*, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушения нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов или получения несанкционированного доступа к ним».

С учетом того, что угроза ведения информационной войны и применения информационного оружия носит многоплановый и актуальный характер, рассмотрим подробнее содержание этой угрозы и особенности ее реализации.

Информационное противоборство присутствовало практически во всех войнах в таких основных формах, как ведение разведки и противодействие ей, распространение дезинформации, слухов и борьба с ними (в том числе с помощью цензуры) и т. п. С появлением новых информационных технологий и организацией международного информационного обмена на новом уровне информационная составляющая в стратегии обеспечения национальной безопасности, по оценкам Совета Безопасности Российской Федерации, руководителей российских спецслужб и Минобороны России, вышла на первый план. По данным различных источников, за последние 15 лет расходы на приобретение средств информационной борьбы увеличились в США в 4 раза и занимают сейчас там первое место среди всех программ по вооружению. В интересах обеспечения информационной безопасности США Пентагон выделяет ежегодно более 90 млн долл. для проведения экспериментальных исследований по ряду направлений, в том числе по созданию новых технологий распознавания образов, формированию электронного образа боевого пространства, автоматическому поиску, сбору и обработки информации с помощью спутников. Информационное противоборство в ходе ведения обычной войны начало переходить на новую, более высокую стадию — информационной войны.

Термин «информационная война» (далее — ИВ) появился в середине 80-х годов в связи с новыми задачами Вооруженных сил США после окончания «холодной войны» (разработка группы военных теоретиков США в составе Г. Экклз, Г. Саммерз и других); начал активно употребляться после проведения операции «Буря в пустыне» в 1991 г., когда новые информационные технологии впервые были использованы как средства ведения войны; официально впервые закреплен в директиве Министерства обо-

роны США от 21 декабря 1992 г. В военных кругах США под информационной войной понимаются действия, предпринимаемые для достижения информационного превосходства в поддержке национальной военной стратегии посредством воздействия на информацию и информационные системы противника, при одновременном обеспечении безопасности и защиты собственной информации и информационных систем.

К особенностям информационной войны можно отнести следующие:

- информационная война охватывает в качестве самостоятельных объектов все виды информации и информационных систем, отделяя информацию от среды использования;
- объекты могут выступать и как оружие, и как объект защиты;
- информационная война расширяет территорию и пространство ведения войн, ведется как при объявлении войны, так и в кризисных ситуациях в различных сферах жизнедеятельности;
- информационная война ведется как специализированными военными, так и гражданскими структурами.

Концепция ИВ, по оценкам российских спецслужб, предусматривает:

- подавление (в военное время) элементов инфраструктуры государственного и военного управления (поражение центров командования и управления);
- электромагнитное воздействие на элементы информационных и телекоммуникационных систем (радиоэлектронная борьба);
- получение разведывательной информации путем перехвата и дешифрования информационных потоков, передаваемых по каналам связи, а также по побочным излучениям и за счет специально внедренных в помещения, и технические средства электронных устройств перехвата информации (радиоэлектронная разведка);
- осуществление несанкционированного доступа к информационным ресурсам (путем использования программно-аппаратных средств прорыва систем защиты информационных и телекоммуникационных систем противника) с последующим их искажением, уничтожением или хищением либо нарушением нормального функционирования этих систем («хакерная война»);

- формирование и массовое распространение по информационным каналам противника или глобальным сетям дезинформации или тенденциозной информации для воздействия на оценки, намерения и ориентацию населения и лиц, принимающих решения (психологическая война);
- получение интересующей информации путем перехвата и обработки открытой информации, передаваемой по незащищенным каналам связи, циркулирующей в информационных системах, а также публикуемой в средствах массовой информации.

Оценка основных направлений ведения информационной войны подтверждается выделением в программах Университета национальной обороны США таких форм ИВ, как радиоэлектронная борьба (РЭБ), война с использованием средств разведки, психологическая война, борьба с хакерами, кибернетическая война.

В целях реализации этой концепции (как в наступательном, так и в оборонительном плане) в США проведены и осуществляются следующие основные мероприятия.

1. Создана объединенная (Министерством обороны и ЦРУ) комиссия по безопасности, которая с июня 1993 г. по февраль 1994 г. исследовала эту проблематику и пришла к выводу, что вторжение в информационные системы и сети — это важнейшая угроза безопасности в XXI веке, что сети передачи данных превращаются в поле битвы будущего. Информационное оружие, стратегию и тактику применения которого еще предстоит тщательно разработать, будет использоваться с «электронными скоростями» при обороне и нападении. Информационные технологии позволят обеспечить разрешение геополитических кризисов, не производя ни одного выстрела. Политика обеспечения национальной безопасности и процедура ее реализации должны быть направлены на защиту возможностей по ведению информационных войн и на создание всех необходимых условий для воспрещения противоборствующим США государствам вести такие войны.

2. Начата разработка стратегии подготовки и ведения ИВ. Во всех видах Вооруженных сил США созданы специализированные центры по ведению ИВ: Центр информационных боевых действий ВВС США — AFIWC (расположен в шт. Техас на базе ВВС Келли); Служба наземных информационных боевых дейст-

вий Армии США — LIWA (расположена в шт. Вирджиния в форте Белвуар).

При этом в Пентагоне каждый из видов войск имеет свою рабочую группу по этой проблематике. В уставах Вооруженных сил США и нормативных документах изложены принципы и способы ведения ИВ.

3. Во всех видах Вооруженных сил США созданы спецподразделения ведения ИВ и введены специальные должности офицеров. Во всех военных учебных заведениях введены спецкурсы по ИВ и идет подготовка специалистов по ведению ИВ (в 1995 г. состоялся первый выпуск).

4. В Вооруженных силах США проводятся учения и штабные игры по этой проблематике (опыт учений 1994—1995 гг. обобщен в Пентагоне). Во время практических боевых действий за пределами США отрабатываются конкретные операции ИВ с применением информоружия.

5. Проведено пять международных конференций по ИВ под эгидой правительства США.

6. Принимаются меры по ежегодному совершенствованию национальной информационной инфраструктуры, где, по оценкам представителей правительства США, циркулирует до 80 процентов конфиденциальной информации, в том числе особо важной.

Администрация Клинтона в феврале 1998 г. приняла решение о развертывании проекта по созданию новой сети Internet (Next Generation Internet) на территории США с новыми качественными характеристиками.

7. Ежегодно увеличиваются ассигнования на разработку новых видов информационного оружия (в Министерстве обороны, Агентстве национальной безопасности, ЦРУ США) и оснащение им национальных структур в объеме, превышающем, по оценкам экспертов, уровень затрат на ракетно-ядерные и космические программы 1994 г.

Информационное превосходство в обычных и информационных войнах

Американские аналитики утверждают, что преобразование вооруженных сил с целью достижения всеобъемлющего военного господства во многом зависит от информационного превос-

ходства как основного фактора, определяющего успех этого преобразования, и от способности к внедрению инноваций.

Информационное превосходство — возможность сбора, обработки и распространения непрерывного потока информации при воспрещении использования (получения) информации противником. Информационное превосходство достигается в небоевой обстановке или в обстановке, в которой еще нет четко обозначившихся противников, в то время, когда свои войска получают информацию, необходимую им для выполнения оперативных задач. Аналитики рассматривают информационное превосходство как новый уровень боеготовности, необходимость в котором возникла за последнее время. Расстановка таких акцентов не бывает случайной. Безусловно, активная позиция Соединенных Штатов в международной политике породила ситуацию, в которой американская система безопасности не может четко ответить на вопросы: «кто?», «когда?» и «как?». В США теперь знают, что им приходится ожидать удара отовсюду, ведь у многих стран мира (в том числе и у союзников по НАТО) есть серьезные противоречия с ними.

Пентагон в условиях стремительного развития информационных возможностей отдает себе отчет, что «информационное превосходство» обозначает состояние дисбаланса в пользу одной из сторон, которое должно завоевываться и поддерживаться с помощью специальных операций. О важности информационного направления говорит тот факт, что в ноябре 2001 г. стало известно о создании в Министерстве обороны США *Управления стратегического влияния* (УСВ) (Office of Strategic Influence), которое предназначено не только для ведения информационных войн против враждебных стран, но и решает те же задачи относительно союзных США стран на Ближнем Востоке, в Азии и Западной Европе.

Об Управлении стратегического влияния до сих пор известно крайне мало. Его бюджет, сформированный из дополнительных 10 млрд долл., утвержденный Конгрессом в октябре 2001 г. для чрезвычайных нужд Пентагона, не раскрывается. Новое управление возглавил бригадный генерал ВВС США Симон Уорден (Simon P. Worden). Известно, что УСВ разрабатывает планы тайных операций с использованием иностранных СМИ и Internet. Управление «собирает в министерстве обороны все инструменты влияния на иностранные аудитории», — заявил на одной из конференций заместитель начальника управления по оперативной

работе Томас Тиммс (Thomas A. Timmes), бывший армейский полковник и специалист по психологическим операциям.

В помощь новому управлению Пентагон нанял Rendon Group, международную консалтинговую фирму со штаб-квартирой в Вашингтоне, во главе которой стоит Джон Рендон (John W. Rendon), бывший помощник по проведению избирательной кампании президента Джимми Картера. Эта фирма, которой платят 100 тыс. долл. в месяц, проделала большую работу в интересах ЦРУ США, королевской семьи Кувейта и Иракского национального конгресса — оппозиционной группировки. Сотрудники Rendon Group сообщали, что по условиям их контракта с Пентагоном они не имеют права говорить об их работе на это ведомство.

Принятая в США концепция защиты от нападения с любого направления означает способность объединенных сил защитить свой личный состав, боевые и материально-технические средства, необходимые для выполнения поставленных задач. Такой вид защиты должен быть достигнут выбором и применением «многослойных» активных и пассивных мер защиты в воздушном, наземном, космическом и информационном пространствах в любых видах военных действий.

Как видим, во всех разделах рассматриваемой концепции, во всех намеченных элементах преобразования ВС США, во всех их боевых возможностях выделен один из самых мощных факторов влияния — информация. Подтверждается старая истина: кто владеет информацией, тот владеет миром. Информационное превосходство обеспечивает быстродействие и возможность маневра. Но информационную работу нельзя рассматривать только как составляющую различных направлений военной сферы. Информационная работа — большая самостоятельная область деятельности. Американцы уделяют огромное внимание информационным операциям, под которыми подразумевают мероприятия, осуществляемые с целью воздействия на содержание информации и работу информационных систем противника при одновременной защите своей информации и своих информационных систем.

Сегодня информационные операции играют существенную роль в достижении военного превосходства. Американцы в своей концепции ставят вопрос об усилении работы по объединению информационных операций как самостоятельного вида боевых действий с другими операциями вооруженных сил — от физиче-

ского устранения до психологической операции против систем защиты компьютерных сетей. В этом контексте отдельно рассматривается проблема оценки военного ущерба, нанесенного противнику информационными операциями, что является довольно трудной задачей. Но руководство Пентагона намерено тщательно исследовать этот вопрос в ходе учений и экспериментов, в том числе, очевидно, и в «полевых условиях».

Более того, рассматривая информационные операции как перспективный самостоятельный вид боевых действий (за счет которого с учетом совершенствования военной доктрины в Пентагоне и рассчитывают в будущем добиваться решающих результатов), командование ВС США предполагает введение в виды вооруженных сил соответствующих формирований, укомплектованных специалистами, получившими специальную подготовку.

Необходимость развития информационных технологий, повышения форм и методов самой информационной работы и так никогда не ставилась под сомнение, но наступило время, когда и Минобороны РФ, ГРУ, а также другие специальные ведомства должны более внимательно взглянуть на это направление работы, перейти на качественно новый уровень в этой сфере деятельности.

Информационное оружие

Информационное оружие, как и информационное противоборство, по мере развития общества и информационных технологий претерпевало изменения.

Информационное оружие (далее — ИО) — это средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним законных пользователей, дезорганизации работы технических средств, вывода из строя телекоммуникационных сетей, компьютерных систем, всех средств высокотехнологического обеспечения жизни общества и функционирования государства.

Информационное оружие от обычных средств поражения отличает:

- скрытность — возможность достигать цели без видимой подготовки и объявления войны;

- масштабность — возможность наносить невосполнимый ущерб, не признавая национальных границ и суверенитета, без ограничения пространства во всех сферах жизнедеятельности человека;
- универсальность — возможность многовариантного использования как военных, так и гражданских структур страны нападения против военных и гражданских объектов страны поражения.

По оценкам экспертов, сфера применения ИО включает как военную, так и экономическую, банковскую, социальную и иные области потенциального противника в целях:

- дезорганизации деятельности управленческих структур, транспортных потоков и средств коммуникации;
- блокирования деятельности отдельных предприятий и банков, а также базовых отраслей промышленности путем нарушения многозвенных технологических связей и системы взаиморасчетов, посредством осуществления валютно-финансовых махинаций и т. п.;
- инициирования крупных техногенных катастроф на территории противника в результате нарушения штатного управления технологическими процессами и объектами, имеющими дело с большими количествами опасных веществ и высокими концентрациями энергии;
- массового распространения и внедрения в сознание людей определенных представлений, привычек и поведенческих стереотипов;
- вызова недовольства или паники среди населения, а также провоцирования деструктивных действий различных социальных групп.

При этом в качестве основных объектов применения ИО как в мирное, так и в военное время выступают:

- компьютерные и коммуникационные системы, используемые государственными организациями при выполнении своих управленческих функций;
- военная информационная инфраструктура, решающая задачи управления войсками и боевыми средствами, сбора и обработки информации в интересах вооруженных сил;
- информационные и управленческие структуры банков, транспортных и промышленных предприятий;
- средства массовой информации, в первую очередь электронные (радио, телевидение и т. д.).

По области применения информационное оружие подразделяется на ИО военного и невоенного назначения.

ИО, применение которого возможно в условиях открытой войны (радиоэлектронное подавление), включает в себя средства, обеспечивающие:

- поражение объектов противника обычными боеприпасами по целеуказаниям собственных средств радио и радиотехнической разведки и частичным самонаведением на конечном участке траектории;
- поражение высокоточными боеприпасами нового поколения, интеллектуальными боеприпасами с самостоятельным поиском цели и самонаведением на ее уязвимые элементы;
- радиолокационное подавление средств связи маскирующими помехами;
- создание имитирующих помех, затрудняющих вхождение в связь, синхронизацию в каналах передачи данных, инициирующих функций переспроса и дублирования сообщений;
- подавление с помощью средств силовой радиоэлектронной борьбы (РЭБ) (посредством мощного электромагнитного излучения, создающего подавляющие помехи за счет паразитных каналов приема);
- выведение из строя радиоэлектронных компонентов за счет воздействия больших уровней электромагнитных или ионизирующих излучений;
- силовое воздействие импульсом высокого напряжения через сеть питания;
- нарушение свойств среды распространения радиоволн (например, срыв КВ-радиосвязи за счет модификации параметров ионосферы);
- воздействие на ЭВМ с помощью специальных методов систем связи;
- генерацию естественной речи конкретного человека.

Особую опасность ИО представляет для информационных компьютерных систем органов государственной власти, управления войсками и оружием, финансами и банками, экономикой страны, а также для людей при информационно-психологическом (психофизическом) воздействии на них с целью изменения и управления их индивидуальным и коллективным поведением.

При этом, по своей результативности информационное оружие сопоставимо с оружием массового поражения.

К информационному оружию, применение которого возможно как в военное, так и в мирное время, могут быть отнесены средства поражения информационных компьютерных систем и средства поражения людей (их психики).

Возможность применения этих и других видов информационного оружия в условиях открытости и роста международного информационного обмена определяет необходимость и особенности защиты человека, общества, государства и информационных систем от его воздействия. По оценке руководителей ФАПСИ, «информационное оружие» сейчас является одной из основных угроз информационной безопасности государства».

Особенностью информационного оружия является то, что оно воздействует на мозг человека, разрушает способы и формы идентификации личности по отношению к фиксированным общностям, трансформирует матрицу памяти индивида, создавая личность с заранее заданными параметрами (типом сознания, искусственными потребностями, формами самоопределения и т. д.), удовлетворяющими требования агрессора, выводит из строя системы управления государства-противника и его вооруженных сил. Доказано, что наибольшие потери вооруженные силы несут от воздействия поражающих элементов ИО, действующих на системы управления и психику человека.

В последние годы ведущими организациями-разработчиками в России интенсивно ведутся НИР по созданию новых средств защиты от информационного оружия. Однако в связи с широтой научных исследований, относящихся к различным сферам жизнедеятельности человека, актуальным становится снижение стоимости разработки средств защиты в условиях ограниченности финансов.

Организация защиты от такого оружия предполагает выполнение ряда условий.

Во-первых, наличие разработанной базовой концепции «информационного оружия», позволяющей определить те психофизиологические и социокультурные средства и механизмы, которые необходимы для защиты российского социума, государства и личности на основе рассмотрения общества как организованной, автономной и самоуправляемой системы с вписанным в нее менталитетом и набором социокультурных традиций.

Во-вторых, создание классификации основных способов и форм поражения и разрушения органов управления государства и сознания индивида в информационной войне с учетом особен-

ностей цивилизационно-культурного контекста. Эта классификация позволит на основе особенностей российской цивилизации выработать психологические, культурные и концептуальные установки, образующие систему защитных фильтров от дезорганизации противником общественного и индивидуального сознания путем размывания «смыслов» российской культуры, подмены значений в системе принятых ценностей, стирания различий между добром и злом, истиной и заблуждением, прекрасным и безобразным и пр.

В-третьих, определение механизмов воздействия так называемых «программных закладок» (речи в речи, изображения в изображении) с использованием компьютеров и других аудиовизуальных средств на нейрофизиологический субстрат психического мира человека, нейролингвистического программирования, действующего на левое и правое полушария человеческого мозга, и разработка мероприятий, направленных на защиту индивида от поражающего воздействия этих «программных закладок» на матрицу памяти и психику индивида.

В-четвертых, теоретическое моделирование спектра вариантов и методов применения «информационного оружия» и разработка прогноза его развития в связи с обычным военным оружием и выработка соответствующих средств защиты.

Одним из средств защиты национальной безопасности России является подготовка к возможному нанесению ответного или превентивного массированного удара по мировому кибернетическому пространству, воплощенному в Internet и объединяющему десятки миллионов пользователей во всем мире, и прежде всего, в потенциальных странах-агрессорах.

Принципы, основные задачи и функции обеспечения информационной безопасности

Принципы. Поскольку информационная безопасность, как было сказано выше, должна быть связующим звеном между политикой национальной безопасности и информационной политикой страны, то логично было бы проводить ее по единым принципам, общим и для национальной безопасности, и для информационной политики. В то же время, если сопоставить принципы обеспечения национальной безопасности, закрепленные в

Законе РФ «О безопасности» и в Концепции национальной безопасности, с принципами государственной информационной политики (ГИП), изложенными в парламентском варианте Концепции ГИП, то прямо они не совпадают друг с другом, а в ряде случаев взаимопротиворечивы по своему содержанию (например, баланс интересов — равенство, государственные интересы — социальная ориентация).

Так, в новой Концепции национальной безопасности по ряду принципов, закрепленных в Законе, раскрыто их содержание (приведено в скобках):

- законность (соблюдение Конституции Российской Федерации, законодательства Российской Федерации и норм международного права при осуществлении деятельности по обеспечению национальной безопасности);
- соблюдение баланса жизненно важных интересов личности, общества и государства (единство, взаимосвязь и сбалансированность всех видов безопасности, гибкое изменение их приоритетности в зависимости от ситуации);
- не допускается ограничение прав и свобод граждан, за исключением случаев, прямо предусмотренных законом (уважение прав и свобод человека);

Ряд принципов не нашел отражения в Концепции, хотя закреплен в Законе (взаимная ответственность личности, общества и государства по обеспечению безопасности; интеграция с международными системами безопасности);

Добавлены новые принципы обеспечения безопасности (приоритет политических и экономических мер обеспечения национальной безопасности с опорой на военный потенциал России; сочетание централизованного управления силами и средствами обеспечения безопасности с передачей в соответствии с федеративным устройством России части полномочий в этой области органам государственной власти субъектов Российской Федерации и органам местного самоуправления).

Авторы Концепции ГИП исходят же из того, что государственная информационная политика должна опираться на следующие базовые принципы:

- открытости политики (все основные мероприятия информационной политики открыто обсуждаются обществом и государство учитывает общественное мнение);
- равенства интересов (политика в равной степени учитывает интересы всех участников информационной деятельности

вне зависимости от их положения в обществе, формы собственности и государственной принадлежности);
- системности (при реализации принятых решений по изменению состояния одного из объектов регулирования должны учитываться его последствия для состояния других и всех в совокупности);
- приоритетности отечественного производителя (при равных условиях приоритет отдается конкурентоспособному отечественному производителю информационно-коммуникационных средств, продуктов и услуг);
- социальной ориентации (основные мероприятия ГИП должны быть направлены на обеспечение социальных интересов граждан России);
- государственной поддержки (мероприятия информационной политики, направленные на информационное развитие социальной сферы финансируются преимущественно государством);
- приоритетности права (развитие и применение правовых и экономических методов имеет приоритет перед любыми формами административных решений проблем информационной сферы).

Таким образом, можно сделать вывод, что необходима как взаимная корректировка принципов обеспечения национальной безопасности и реализации информационной политики, так и учет ряда приведенных принципов ГИП при обеспечении информационной безопасности. Исходя из этого к принципам обеспечения информационной безопасности можно отнести:

- законность (соблюдение норм международного права, Конституции Российской Федерации и законодательства Российской Федерации при осуществлении деятельности по обеспечению информационной безопасности);
- сбалансированность (соблюдение баланса интересов субъектов, их взаимная ответственность);
- системность;
- открытость;
- реальность выдвигаемых задач (с учетом имеющихся ресурсов, сил и средств);
- сочетание централизованного управления силами и средствами обеспечения безопасности с передачей в соответствии с федеральным устройством России части полномочий в этой области органам государственной власти субъектов

Российской Федерации и органам местного самоуправления;
- интеграцию с международными системами обеспечения информационной безопасности.

Аналогичный подход, по-видимому, необходимо применить и при определении задач и функций обеспечения информационной безопасности, учитывая при этом результаты сравнительного и системного анализа других нормативных документов и разработок по этим вопросам.

Основные задачи в сфере обеспечения информационной безопасности. К основным задачам в сфере обеспечения информационной безопасности относятся:

- формирование и реализация единой государственной политики по обеспечению защиты национальных интересов от угроз в информационной сфере, реализации конституционных прав и свобод граждан на информационную деятельность;
- совершенствование законодательства Российской Федерации в сфере обеспечения информационной безопасности;
- определение полномочий органов государственной власти Российской Федерации, субъектов Российской Федерации и органов местного самоуправления в сфере обеспечения информационной безопасности;
- координация деятельности органов государственной власти по обеспечению информационной безопасности;
- создание условий для успешного развития негосударственного компонента в сфере обеспечения информационной безопасности, осуществления эффективного гражданского контроля за деятельностью органов государственной власти;
- совершенствование и защита отечественной информационной инфраструктуры, ускорение развития новых информационных технологий и их широкое распространение, унификация средств поиска, сбора, хранения, обработки и анализа информации с учетом вхождения России в глобальную информационную инфраструктуру;
- развитие стандартизации информационных систем на базе общепризнанных международных стандартов и их внедрение для всех видов информационных систем;
- развитие отечественной индустрии телекоммуникационных и информационных средств, их приоритетное по сравне-

нию с зарубежными аналогами распространение на внутреннем рынке;
- защита государственных информационных ресурсов, прежде всего в федеральных органах государственной власти, на предприятиях оборонного комплекса;
- духовное возрождение России; обеспечение сохранности и защиты культурного и исторического наследия (в том числе музейных, архивных, библиотечных фондов, основных историко-культурных объектов);
- сохранение традиционных духовных ценностей при важнейшей роли Русской православной церкви и церквей других конфессий;
- пропаганда средствами массовой информации элементов национальных культур народов России, духовно-нравственных, исторических традиций, норм общественной жизни и передового опыта подобной пропагандистской деятельности;
- повышение роли русского языка как государственного языка и языка межгосударственного общения народов России и государств — участников СНГ;
- создание оптимальных социально-экономических условий для осуществления важнейших видов творческой деятельности и функционирования учреждений культуры;
- противодействие угрозе развязывания противоборства в информационной сфере;
- организация международного сотрудничества по обеспечению информационной безопасности при интеграции России в мировое информационное пространство.

Функции государственной системы по обеспечению информационной безопасности. Для реализации указанных задач государственной системой обеспечения информационной безопасности должны осуществляться следующие функции [21]:

- оценка состояния информационной безопасности в стране, определение приоритетов по интересам в информационной сфере и установление их баланса в конкретных условиях;
- выявление и учет источников внутренних и внешних угроз, проведение их мониторинга и классификации;
- определение основных направлений предотвращения угроз или минимизации ущерба от их реализации;
- организация исследований в сфере обеспечения информационной безопасности;

- разработка и принятие законов и иных нормативных правовых актов;
- разработка федеральных целевых и ведомственных программ обеспечения информационной безопасности, координация работ по их реализации;
- организация единой системы лицензирования, сертификации, экспертизы и контроля в этой сфере;
- страхование информационных рисков;
- подготовка специалистов по обеспечению информационной безопасности, в том числе из работников правоохранительных и судебных органов;
- информирование общественности о реальной ситуации в сфере обеспечения информационной безопасности и работе государственных органов в этой сфере;
- изучение практики обеспечения информационной безопасности, обобщение и пропаганда передового опыта такой работы в регионах;
- правовая защита прав и интересов граждан, интересов общества и государства в сфере информационной безопасности;
- организация обучения способам и методам самозащиты физических лиц от основных угроз в информационной сфере;
- содействие разработке и принятию норм международного права в сфере обеспечения информационной безопасности;
- установление стандартов и нормативов в сфере обеспечения информационной безопасности.

Поскольку от эффективности выполнения последней указанной функции во многом напрямую зависят сроки и возможности организации системы обеспечения информационной безопасности, то рассмотрим ее содержание подробнее.

Отечественные и зарубежные стандарты в области информационной безопасности

В Российской Федерации сейчас насчитывается более 22 тысяч действующих стандартов. Стандартизация начинается с основополагающего стандарта, устанавливающего общие положения. На сегодняшний день такого стандарта в области информационной безопасности нет. Девять ГОСТов: ГОСТ 28147—89,

ГОСТ Р 34.10—94, ГОСТ Р 34.11—94, ГОСТ 29. 339—92, ГОСТ Р 50752—95, ГОСТ РВ 50170—92, ГОСТ Р 50600—93, ГОСТ Р 50739—95, ГОСТ Р 50922—96 относятся к различным группам по классификатору стандартов и, к сожалению, не являются функционально полными ни по одному из направлений защиты информации. Кроме того, есть семейства родственных стандартов, имеющих отношение к области защиты информации:

- системы тревожной сигнализации, комплектуемые извещателями различного принципа действия, — 12 ГОСТов;
- информационные технологии (сертификация систем телекоммуникации, программных и аппаратных средств, аттестационное тестирование взаимосвязи открытых систем, аттестация баз данных и т. д.) — около 200 ГОСТов;
- системы качества (в том числе стандарты серии 9000, введенные в действие на территории РФ) — больше 100 ГОСТов.

Значительная часть стандартов на методы контроля и испытаний (около 60 %) может быть признана не соответствующей требованию Закона РФ «Об обеспечении единства измерений», как правило, в части погрешностей измерений. Отсутствуют стандарты в сфере информационно-психологической безопасности.

Таким образом, очевидно, что работа над объектами стандартизации в сфере информационной безопасности только разворачивается. Для этого крайне важен международный опыт. В 1983 г. Агентство компьютерной безопасности Министерства обороны США опубликовало отчет, названный TSEC (Критерии Оценки Защищенности Надежных Систем) или Оранжевая книга (по цвету переплета), где были определены 7 уровней безопасности (A1 — гарантированная защита; B1, B2, B3 — полное управление доступом; C1, C2 — избирательное управление доступом; D — минимальная безопасность) для оценки защиты конфиденциальных данных в многопользовательских компьютерных системах. Для оценки компьютерных систем Министерства обороны США Национальный Центр компьютерной безопасности МО США выпустил инструкции NCSC-TG-005 и NCSC-TG-011, известные как Красная книга (по цвету пепреплета). В качестве ответа Агентство информационной безопасности ФРГ подготовило Green Book (Зеленая книга), где рассмотрены в комплексе требования к доступности, целостности и конфиденциальности информации как в государственном, так и в частном секторе.

В 1990 г. Зеленая книга была одобрена ФРГ, Великобританией, Францией и Голландией и направлена в ЕС, где на ее основе была подготовлена ITSEC (Критерии Оценки Защищенности Информационных Технологий) или Белая книга как европейский стандарт, определяющий критерии, требования и процедуры для создания безопасных информационных систем, имеющий две схемы оценки: по эффективности (от E1 до E6) и по функциональности (доступность, целостность системы, целостность данных, конфиденциальность информации и передача данных). С учетом интеграции России в общеевропейские структуры рассмотрим подробнее положения европейского стандарта.

В Белой книге названы основные компоненты критериев безопасности ITSEC:

1. Информационная безопасность.
2. Безопасность системы.
3. Безопасность продукта.
4. Угроза безопасности.
5. Набор функций безопасности.
6. Гарантированность безопасности.
7. Общая оценка безопасности.
8. Классы безопасности.

Согласно европейским критериям ITSEC, информационная безопасность включает в себя шесть основных элементов ее детализации:

1. Конфиденциальность информации (защита от несанкционированного получения информации).

2. Целостность информации (защита от несанкционированного изменения информации).

3. Доступность информации (защита от несанкционированного или случайного удержания информации и ресурсов системы).

4. Цели безопасности (зачем нужны функции информационной безопасности).

5. Спецификация функций безопасности:

- идентификация и аутентификация (понимается не только традиционная проверка подлинности пользователя, но и функции для регистрации новых пользователей и удаления старых, а также функции для изменения и проверки аутентификационной информации, в том числе средств контроля целостности и функции для ограничения количества повторных попыток аутентификации);

- управление доступом (в том числе функции безопасности, которые обеспечивают: временное ограничение доступа к совместно используемым объектам с целью поддержания целостности этих объектов; управление распространением прав доступа; контроль за получением информации путем логического вывода и агрегирования данных);
- подотчетность (протоколирование);
- аудит (независимый контроль);
- повторное использование объектов;
- точность информации (поддержка определенного соответствия между разными частями данных (точность связей) и обеспечение неизменности данных при передаче между процессами (точность коммуникации));
- надежность обслуживания (функции обеспечения, когда действия, критичные по времени, будут выполнены именно тогда, когда нужно; некритичные действия нельзя перенести в разряд критичных; авторизованные пользователи за разумное время получат запрашиваемые ресурсы; функции обнаружения и нейтрализации ошибок; функции планирования для обеспечения коммуникационной безопасности, т. е. безопасности данных, передаваемых по каналам связи);
- обмен данными.

6. Описание механизмов безопасности.

В Белой книге декларируется разница между «системой» и «продуктом». Под «системой» понимается конкретная аппаратно-программная конфигурация, созданная с вполне определенными целями и работающая в известном окружении, а под «продуктом» — аппаратно-программный пакет, который можно купить и по своему усмотрению вставить в ту или иную «систему». Для объединения критериев оценки «системы» и «продукта» в ITSEC вводится единый термин — «объект» оценки. Каждая «система» и/или «продукт» предъявляют свои требования к обеспечению конфиденциальности, целостности и доступности информации. Для их реализации необходим и соответствующий набор функций безопасности, таких, как идентификация и аутентификация, управление доступом, восстановление после сбоев, подотчетность, аудит, правила повторного использования объектов доступа, точность информации, надежность обслуживания, обмен данными. Например, для реализации функций идентифи-

кации и аутентификации могут использоваться такие механизмы, как специальный сервер «KERBEROS», а для защиты компьютерных сетей — фильтрующие маршрутизаторы, сетевые анализаторы протоколов (экраны) типа Firewall/Plus, Firewall/1, пакеты фильтрующих программ и т. д.

Чтобы «объект» оценки можно было признать надежным, необходима определенная степень уверенности, которая декларируется как гарантированность безопасности, включающая в себя два компонента — эффективность и корректность механизмов безопасности (средств защиты). В некоторых источниках гарантированность также называют адекватностью средств защиты.

При проверке эффективности анализируется соответствие между задачами безопасности по конфиденциальности, целостности, доступности информации и реализованным набором функций безопасности — их функциональной полнотой и согласованностью, простотой использования, а также возможными последствиями использования злоумышленниками слабых мест защиты. Кроме того, в понятие эффективности включается и способность механизмов защиты противостоять прямым атакам, которая называется мощностью механизмов защиты. По ITSEC декларируются три степени мощности (базовая, средняя, высокая). При проверке корректности анализируются правильность и надежность реализации функций безопасности. По ITSEC декларируются семь уровней корректности — от E0 до E6.

Общая оценка безопасности системы по ITSEC состоит из двух компонентов — оценки уровня гарантированной эффективности механизмов (средств) безопасности и оценки уровня их гарантированной корректности. Безопасность системы в целом оценивается отдельно для «систем» и «продуктов». Защищенность их не может быть выше мощности самого слабого из критически важных механизмов безопасности (средств защиты).

В европейских критериях устанавливаются 10 классов безопасности (F-C1, F-C2, F-B1, F-B2, F-B3, F-IN, F-AV, F-D1, F-DC, F-DX). Первые пять из них аналогичны классам C1, C2, B1, B2, B3 американских критериев TCSEC. Класс F-IN предназначен для систем с высокими потребностями к обеспечению целостности, что типично для СУБД, и различает виды доступа: чтение, запись, добавление, удаление, создание, переименование и выделение объектов. Класс F-AV предназначен для систем с высокими требованиями к обеспечению их работоспособности

за счет противодействия угрозам отказа в обслуживании (существенно для систем управления технологическими процессами). Класс F-DI ориентирован на системы с повышенными требованиями к целостности данных, которые передаются по каналам связи. Класс F-DC характеризуется повышенными требованиями к конфиденциальности информации, а класс F-DX предназначен для систем с повышенными требованиями одновременно по классам F-DI и F-DC.

Канада разработала CTCPEC, и США, наконец, разработали новые Федеральные Критерии (Federal Criteria). Так как эти критерии являются несовместимыми между собой, было принято решение попытаться гармонизировать (объединить) все эти критерии в новый набор критериев оценки защищенности, названный Common Criteria (CC). Общие критерии дают набор критериев по оценке защищенности и устанавливают:

- требования к функциональным возможностям и гарантиям;
- семь уровней доверия (Уровни Гарантий при Оценке), которые может запросить пользователь (уровень EAL1 обеспечивает лишь небольшое доверие к корректности системы, а уровень EAL7 дает очень высокие гарантии);
- два понятия: Профиль Защиты (PP) и Цель безопасности (ST).

Одним из отечественных аналогов перечисленных стандартов является Руководящий документ Гостехкомиссии РФ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требований по защите информации».

Комплексность защиты информации достигается за счет использования унифицированного алгоритмического обеспечения для средств криптографической защиты в соответствии с российскими государственными стандартами:

- ГОСТ 28147—89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»;
- ГОСТ Р 34. 10—94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма»;
- ГОСТ Р 34. 11—94 «Информационная технология. Криптографическая защита информации. Функция хэширования»;

- ГОСТ Р 50739—95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования».

Поскольку деятельность любой организации подвержена множеству рисков, в том числе вследствие использования информационных технологий, то относительно недавно появилась новая функция — управление рисками, которая включает в себя два вида деятельности: оценку (измерение) рисков и выбор эффективных и экономичных защитных регуляторов. Процесс управления рисками можно подразделить на следующие этапы:

1. Выбор анализируемых объектов и степени детальности их рассмотрения.
2. Выбор методологии оценки рисков.
3. Идентификация активов.
4. Анализ угроз и их последствий, определение слабостей в защите.
5. Оценка рисков.
6. Выбор защитных мер.
7. Реализация и проверка выбранных мер.
8. Оценка остаточного риска.

Правовое регулирование этих отношений возможно и необходимо, прежде всего, через страхование информационных рисков.

Проблема обеспечения безопасности носит комплексный характер. Для ее решения необходимо сочетание как правовых мер, так и организационных (например, в компьютерных информационных системах на управленческом уровне руководство каждой организации должно выработать политику безопасности, определяющую общее направление работ, и выделить на эти цели соответствующие ресурсы) и программно-технических (идентификация и аутентификация; управление доступом; протоколирование и аудит; криптография; экранирование).

1.3. Защита информации (ЗИ)

Защита информации — комплекс мероприятий, направленных на обеспечение важнейших аспектов информационной безопасности (целостности, доступности и, если нужно, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных) [1].

Система называется безопасной, если она, используя соответствующие аппаратные и программные средства, управляет доступом к информации так, что только должным образом авторизованные лица или же действующие от их имени процессы получают право читать, писать, создавать и удалять информацию.

Очевидно, что абсолютно безопасных систем нет, и здесь речь идет о надежной системе в смысле «система, которой можно доверять» (как можно доверять человеку). Система считается надежной, если она с использованием достаточных аппаратных и программных средств обеспечивает одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа.

Основными критериями оценки надежности являются политика безопасности и гарантированность.

Политика безопасности, являясь активным компонентом защиты (включает в себя анализ возможных угроз и выбор соответствующих мер противодействия), отображает тот набор законов, правил и норм поведения, которым пользуется конкретная организация при обработке, защите и распространении информации.

Выбор конкретных механизмов обеспечения безопасности системы производится в соответствии со сформулированной политикой безопасности.

Гарантированность, являясь пассивным элементом защиты, отображает меру доверия, которое может быть оказано архитектуре и реализации системы (другими словами, показывает, насколько корректно выбраны механизмы, обеспечивающие безопасность системы).

В надежной системе должны регистрироваться все происходящие события, касающиеся безопасности (должен использоваться механизм подотчетности протоколирования, дополняющийся анализом запомненной информации, т. е. аудитом).

При оценке степени гарантированности, с которой систему можно считать надежной, центральное место занимает достоверная (надежная) вычислительная база. Достоверная (доверенная) вычислительная база (ДВБ или TCB — Trusted Computer Base) представляет собой полную совокупность защитных механизмов компьютерной системы, которая используется для претворения в жизнь соответствующей политики безопасности.

Надежность ДВБ зависит исключительно от ее реализации и корректности введенных данных (например, данных о благонадежности пользователей, определяемых администрацией).

Граница ДВБ образует периметр безопасности. Компоненты ДВБ, находящиеся внутри этой границы, должны быть надежными (следовательно, для оценки надежности компьютерной системы достаточно рассмотреть только ее ДВБ). От компонентов, находящихся вне периметра безопасности, вообще говоря, не требуется надежности. Однако это не должно влиять на безопасность системы. Так как сейчас широко применяются распределенные системы обработки данных, то под «периметром безопасности» понимается граница владений определенной организации, в подчинении которой находится эта система. Тогда по аналогии то, что находится внутри этой границы, считается надежным. Посредством шлюзовой системы, которая способна противостоять потенциально ненадежному, а может быть даже и враждебному окружению, осуществляется связь через эту границу.

Контроль допустимости выполнения субъектами определенных операций над объектами, т. е. функции мониторинга, выполняется достоверной вычислительной базой. При каждом обращении пользователя к программам или данным монитор проверяет допустимость данного обращения (согласованность действия конкретного пользователя со списком разрешенных для него действий). Реализация монитора обращений называется ядром безопасности, на базе которой строятся все защитные механизмы системы. Ядро безопасности должно гарантировать собственную неизменность.

Основные предметные направления ЗИ

Основные предметные направления ЗИ — охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности [21].

Государственная тайна — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Сведения могут считаться государственной тайной (могут быть засекречены), если они отвечают следующим требованиям:

- соответствуют перечню сведений, составляющих государственную тайну, не входят в перечень сведений, не подлежащих засекречиванию, и отвечают законодательству РФ о государственной тайне (принцип законности);
- целесообразность засекречивания конкретных сведений установлена путем экспертной оценки вероятных экономических и иных последствий, возможности нанесения ущерба безопасности РФ, исходя из баланса жизненно важных интересов государства, общества и личности (принцип обоснованности);
- ограничения на распространение этих сведений и на доступ к ним установлены с момента их получения (разработки) или заблаговременно (принцип своевременности);
- компетентные органы и их должностные лица приняли в отношении конкретных сведений решение об отнесении их к государственной тайне и засекречивании и установили в отношении них соответствующий режим правовой охраны и защиты (принцип обязательной защиты).

Коммерческая тайна исстари охранялась при содействии государства. Примером этого утверждения могут служить многочисленные факты ограничения доступа иностранцев в страну (в Китае — для защиты секретов производства фарфора), в отдельные отрасли экономики или на конкретные производства. В России к коммерческой тайне относили промысловую тайну, но затем она была ликвидирована как правовой институт в начале 30-х годов и в связи с огосударствлением отраслей экономики защищалась как государственная и служебная тайна. Сейчас начался обратный процесс.

Информация может составлять коммерческую тайну, если она отвечает следующим требованиям (критерии правовой охраны):

- имеет действительную или потенциальную коммерческую ценность в силу ее неизвестности третьим лицам;
- не подпадает под перечень сведений, доступ к которым не может быть ограничен, и перечень сведений, отнесенных к государственной тайне;
- к ней нет свободного доступа на законном основании;
- обладатель информации принимает меры к охране ее конфиденциальности.

К коммерческой тайне не может быть отнесена информация:

- содержащаяся в учредительных документах;
- содержащаяся в документах, дающих право заниматься предпринимательской деятельностью (регистрационные удостоверения, лицензии и т. д.);
- содержащаяся в годовых отчетах, бухгалтерских балансах, формах государственных статистических наблюдений и других формах годовой бухгалтерской отчетности, включая аудиторские заключения, а также в иных, связанных с исчислением и уплатой налогов и других обязательных платежей;
- содержащая сведения об оплачиваемой деятельности государственных служащих, о задолженностях работодателей по выплате заработной платы и другим выплатам социального характера, о численности и кадровом составе работающих;
- содержащаяся в годовых отчетах фондов об использовании имущества;
- подлежащая раскрытию эмитентом ценных бумаг, профессиональным участником рынка ценных бумаг и владельцем ценных бумаг в соответствии с законодательством Российской Федерации о ценных бумагах;
- связанная с соблюдением экологического и антимонопольного законодательства, обеспечением безопасных условий труда, реализацией продукции, причиняющей вред здоровью населения, другими нарушениями законодательства Российской Федерации, законодательства субъектов Российской Федерации, а также содержащая данные о размерах причиненных при этом убытков;
- о деятельности благотворительных организаций и иных некоммерческих организаций, не связанной с предпринимательской деятельностью;
- о наличии свободных рабочих мест;
- о хранении, использовании или перемещении материалов и использовании технологий, представляющих опасность для жизни и здоровья граждан или окружающей среды;
- о реализации государственной программы приватизации и об условиях приватизации конкретных объектов;
- о размерах имущества и вложенных средствах при приватизации;
- о ликвидации юридического лица и о порядке и сроке подачи заявлений или требований его кредиторами;

- для которой определены ограничения по установлению режима коммерческой тайны в соответствии с федеральными законами и принятыми в целях их реализации подзаконными актами.

Основными субъектами права на коммерческую тайну являются обладатели коммерческой тайны, их правопреемники.

Обладатели коммерческой тайны — физические (независимо от гражданства) и юридические (коммерческие и некоммерческие организации) лица, занимающиеся предпринимательской деятельностью и имеющие монопольное право на информацию, составляющую для них коммерческую тайну.

При этом под предпринимательством понимается «самостоятельная, осуществляемая на свой риск деятельность, направленная на систематическое получение прибыли от пользования имуществом, продажи товаров, выполнения работ или оказания услуг лицами, зарегистрированными в этом качестве в установленном законом порядке» (статья 2 Гражданского кодекса Российской Федерации).

Правопреемники — физические и юридические лица, которым в силу служебного положения, по договору или на ином законном основании (в том числе по наследству) известна информация, составляющая коммерческую тайну другого лица.

Банковская тайна — защищаемые банками и иными кредитными организациями сведения о банковских операциях по счетам и сделкам в интересах клиентов, счетах и вкладах своих клиентов и корреспондентов, а также сведения о клиентах и корреспондентах, разглашение которых может нарушить право последних на неприкосновенность частной жизни.

К основным объектам банковской тайны относятся следующие:

1. Тайна банковского счета — сведения о счетах клиентов и корреспондентов и действиях с ними в кредитной организации (о расчетном, текущем, бюджетном, депозитном, валютном, корреспондентском и тому подобных счетах, об открытии, закрытии, переводе, переоформлении счетов и т. д.).

2. Тайна операций по банковскому счету — сведения о принятии и зачислении поступающих на счет клиента денежных средств, о выполнении его распоряжений по перечислению и выдаче соответствующих сумм со счета, а также проведении других операций и сделок по банковскому счету, предусмотренных договором банковского счета или законом.

3. Тайна банковского вклада — сведения обо всех видах вкладов клиента в кредитной организации.

4. Тайна частной жизни клиента или корреспондента — сведения, составляющие личную, семейную тайну и охраняемые законом как персональные данные этого клиента или корреспондента.

Профессиональная тайна — защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, распространение которой может нанести ущерб правам и законным интересам другого лица (доверителя), доверившего эти сведения, и не являющаяся государственной или коммерческой тайной.

Информация может считаться профессиональной тайной, если она отвечает следующим требованиям (критериям охраноспособности права):

- доверена или стала известна лицу лишь в силу исполнения им своих профессиональных обязанностей;
- лицо, которому доверена информация, не состоит на государственной или муниципальной службе (в противном случае информация считается служебной тайной);
- запрет на распространение доверенной или ставшей известной информации, которое может нанести ущерб правам и законным интересам доверителя, установлен федеральным законом;
- информация не относится к сведениям, составляющим государственную и коммерческую тайну.

В соответствии с этими критериями можно выделить следующие объекты профессиональной тайны:

Врачебная тайна — информация, содержащая:

- результаты обследования лица, вступающего в брак;
- сведения о факте обращения за медицинской помощью, о состоянии здоровья, диагнозе заболевания и иные сведения, полученные при обследовании и лечении гражданина;
- сведения о проведенных искусственном оплодотворении и имплантации эмбриона, а также о личности донора;
- сведения о доноре и реципиенте при трансплантации органов и (или) тканей человека;

- сведения о наличии психического расстройства, фактах обращения за психиатрической помощью и лечении в учреждении, оказывающем такую помощь, а также иные сведения о состоянии психического здоровья гражданина;
- иные сведения в медицинских документах гражданина.

Тайна связи — тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.

Нотариальная тайна — сведения, доверенные нотариусу в связи с совершением нотариальных действий.

Адвокатская тайна — сведения, сообщенные адвокату гражданином в связи с оказанием ему юридической помощи.

Тайна усыновления — сведения об усыновлении ребенка, доверенные на законном основании иным лицам, кроме судей, вынесших решение об усыновлении, и должностных лиц, осуществляющих государственную регистрацию этого усыновления.

Тайна страхования — сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц, полученные страховщиком в результате своей профессиональной деятельности.

Тайна исповеди — сведения, доверенные гражданином священнослужителю на исповеди.

Служебная тайна — защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости.

Служебная тайна является видом конфиденциальной информации, и право на служебную тайну выступает самостоятельным объектом права. Для осуществления ее правовой охраны и защиты необходим специальный Федеральный закон «О служебной тайне».

Информация может считаться служебной тайной, если она отвечает следующим требованиям (критериям охраноспособности права):

- отнесена федеральным законом к служебной информации о деятельности государственных органов, доступ к которой ограничен по закону или в силу служебной необходимости (собственная служебная тайна);

- является охраноспособной конфиденциальной информацией («чужой тайной») другого лица (коммерческая тайна, банковская тайна, тайна частной жизни, профессиональная тайна);
- не является государственной тайной и не подпадает под перечень сведений, доступ к которым не может быть ограничен;
- получена представителем государственного органа и органа местного самоуправления только в силу исполнения обязанностей по службе в случаях и порядке, установленных федеральным законом.

Информация, не отвечающая этим требованиям, не может считаться служебной тайной и не подлежит правовой охране. В действующем законодательстве приводится перечень сведений, которые не могут быть отнесены к служебной информации ограниченного распространения:

- акты законодательства, устанавливающие правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;
- сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах, экологическая, гидрометеорологическая, гидрогеологическая, демографическая, санитарно-эпидемиологическая и другая информация, необходимая для обеспечения безопасного существования населенных пунктов, граждан и населения в целом, а также производственных объектов;
- описание структуры органа исполнительной власти, его функций, направлений и форм деятельности, а также его адрес;
- порядок рассмотрения и разрешения заявлений, в том числе юридических лиц, рассмотренных в установленном порядке;
- сведения об исполнении бюджета и использовании других государственных ресурсов, о состоянии экономики и потребностей населения;
- документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах организаций, необходимые для реализации прав, свобод и обязанностей граждан.

Таким образом, к основным объектам служебной тайны можно отнести такие виды информации, как:

1) служебная информация о деятельности федеральных государственных органов, доступ к которой ограничен федеральным законом в целях защиты государственных интересов: военная тайна; тайна следствия (данные предварительного расследования либо следствия); судебная тайна (тайна совещания судей, содержание дискуссий и результатов голосования закрытого совещания Конституционного суда Российской Федерации, материалы закрытого судебного заседания, тайна совещания присяжных заседателей или в силу служебной необходимости, порядок выработки и принятия решения, организация внутренней работы и т. д.);

2) охраноспособная конфиденциальная информация, ставшая известной в силу исполнения служебных обязанностей должностным лицам государственных органов и органов местного самоуправления: коммерческая тайна, банковская тайна, профессиональная тайна, а также конфиденциальная информация о частной жизни лица.

Особенность правоотношений в этой области состоит в том, что если во втором случае государственные органы и их должностные лица обязаны обеспечить (гарантировать) сохранность «чужой» тайны, ставшей известной им по службе, в объеме сведений, переданных ее владельцем, то в первом случае они самостоятельно в соответствии с законом определяют объем своей служебной тайны и режим ее защиты.

Охрана персональных данных. В Европе для охраны и защиты права на неприкосновенность частной жизни в условиях автоматизированной обработки личных данных о гражданах более 25 лет назад был введен особый институт правовой охраны личности — институт защиты персональных данных. Более чем в 20 европейских государствах приняты национальные законы о персональных данных, в ряде стран введены независимые уполномоченные по защите персональных данных, во всех странах Европейского Союза с 1998 г. создана единая унифицированная система защиты персональных данных, в том числе в секторе телекоммуникаций.

Федеральный закон «Об информации, информатизации и защите информации» [28] вводит понятие «персональные данные» (статья 2); относит персональные данные к конфиденциальной информации и устанавливает, что перечни персональных дан-

ных должны быть закреплены федеральным законом (статья 11); требует, чтобы деятельность негосударственных организаций и частных лиц по обработке и предоставлению персональных данных, равно как и по проектированию, производству средств защиты информации и обработки персональных данных, обязательно лицензировалась в порядке, установленном Правительством Российской Федерации (статьи 11, 19); декларирует, что персональные данные должны защищаться, а режим защиты в отношении персональных данных устанавливается федеральным законом (статья 21). Кодекс РФ об административных правонарушениях в статье 13.11 устанавливает ответственность за нарушение порядка сбора, хранения и распространение информации о гражданах [29].

Объектом правоотношений здесь выступает право на персональные данные — информация (зафиксированная на любом материальном носителе) о конкретном человеке, которая отождествлена или может быть отождествлена с ним.

К персональным данным могут быть отнесены сведения, использование которых без согласия субъекта персональных данных может нанести вред его чести, достоинству, деловой репутации, доброму имени, иным нематериальным благам и имущественным интересам:

- биографические и опознавательные данные (в том числе об обстоятельствах рождения, усыновления, развода);
- личные характеристики (в том числе о личных привычках и наклонностях);
- сведения о семейном положении (в том числе о семейных отношениях);
- сведения об имущественном, финансовом положении (кроме случаев, прямо установленных в законе);
- о состоянии здоровья.

Субъектами права здесь выступают:

- субъекты персональных данных — лица, к которым относятся соответствующие данные, и их наследники;
- держатели персональных данных — органы государственной власти и органы местного самоуправления, юридические и физические лица, осуществляющие на законных основаниях сбор, хранение, передачу, уточнение, блокирование, обезличивание, уничтожение персональных данных (баз персональных данных).

Персональные данные и работа с ними должны соответствовать следующим требованиям:

1. Персональные данные должны быть получены и обработаны законным образом на основании действующего законодательства.

2. Персональные данные включаются в базы персональных данных на основании свободного согласия субъекта, выраженного в письменной форме, за исключением случаев, прямо установленных в законе.

3. Персональные данные должны накапливаться для точно определенных и законных целей, не использоваться в противоречии с этими целями и не быть избыточными по отношению к ним. Не допускается объединение баз персональных данных, собранных держателями в разных целях, для автоматизированной обработки информации.

4. Персональные данные, предоставляемые держателем, должны быть точными и в случае необходимости обновляться.

5. Персональные данные должны храниться не дольше, чем этого требует цель, для которой они накапливаются, и подлежать уничтожению по достижении этой цели или по миновании надобности.

6. Персональные данные охраняются в режиме конфиденциальной информации, исключающем их случайное или несанкционированное разрушение или случайную их утрату, а равно несанкционированный доступ к данным, их изменение, блокирование или передачу.

7. Для лиц, занимающих высшие государственные должности, и кандидатов на эти должности может быть установлен специальный правовой режим для их персональных данных, обеспечивающий открытость только общественно значимых данных.

Охрана интеллектуальной собственности. К числу основных объектов интеллектуальной собственности отнесены:

- произведения науки, литературы и искусства;
- результаты исполнительской деятельности артистов, режиссеров, дирижеров;
- сложные результаты творчества;
- звукозаписи и записи изображения;
- передача радио- и телевизионных сигналов;
- изобретения;
- полезные модели;
- промышленные образцы;

- профессиональные секреты (ноу-хау);
- селекционные достижения;
- фирменные наименования и коммерческие обозначения правообладателя;
- товарные знаки и знаки обслуживания;
- наименования мест происхождения товаров;
- другие результаты интеллектуальной деятельности и средства индивидуализации, на которые в соответствии с законом могут признаваться или закрепляться исключительные права.

Правовые основы защиты информации

В целях охраны и защиты *прав и свобод в информационной сфере* Конституция РФ устанавливает гарантии, обязанности, механизмы защиты и ответственности. К основным конституционным гарантиям относятся:

- признание прав и свобод человека и гражданина неотчуждаемыми (статья 17), равными (статья 19), непосредственно действующими (статья 18) согласно общепризнанным принципам и нормам международного права и защищаемыми государством (статья 45);
- законы подлежат официальному опубликованию. Неопубликованные законы не применяются. Любые нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, не могут применяться, если они не опубликованы официально для всеобщего сведения (часть 3 статьи 15);
- права и свободы «определяют смысл, содержание и применение законов, деятельность законодательной и исполнительной власти, местного самоуправления и обеспечиваются правосудием» (статья 18);
- органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечивать каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом (часть 2 статьи 24);
- механизмы защиты наряду с государственной защитой предусматривают право каждого на самозащиту «всеми спосо-

бами, не запрещенными законом» (часть 2 статьи 45), судебную защиту (части 1 и 2 статьи 46), международно-правовую защиту (часть 3 статьи 46);

- сокрытие должностными лицами фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, влечет за собой ответственность в соответствии с федеральным законом (часть 3 статьи 41).

Важной сферой безопасности информации является защита прав собственности на нее. Информация (несмотря на ряд существенных особенностей) должна рассматриваться законом как объект права собственности. В первой части Гражданского кодекса РФ (ст. 128), принятого Государственной Думой (21.10.94 г.), впервые в России информация определена в качестве объекта права (рис. 1.1 и 1.2).

Федеральным законом «Об информации, информатизации и защите информации» от 20.02.95 года определено, что информационные ресурсы, т. е. отдельные документы или массивы документов, в том числе и в информационных системах, являясь объектами отношений физических, юридических лиц и государ-

Рис. 1.1. Информация как объект права собственности

Рис. 1.2. Право владения, пользования и распоряжения информацией

ства, подлежат обязательному учету и защите как материальное имущество собственника.

Источники права на доступ к информации

Наряду с нормами Конституции РФ источниками права о доступе к информации являются:

- законы (Основы законодательства РФ о культуре, Основы законодательства РФ об Архивном фонде и архивах; Федеральные законы «Об информации, информатизации и защите информации», «О порядке опубликования и вступления в силу Федеральных конституционных законов, федеральных законов, актов палат Федерального Собрания», «О библиотечном деле», «Об участии в международном информационном обмене» и др.);
- подзаконные нормативные акты (указы Президента РФ, постановления Правительства РФ);

- международные правовые акты, международные договоры и соглашения;
- судебная практика.

Федеральный закон «Об информации, информатизации и защите информации» для реализации права на доступ к информации провозглашает следующие дополнительные государственные гарантии.

1. Органы государственной власти и органы местного самоуправления создают доступные для каждого информационные ресурсы по вопросам деятельности этих органов и подведомственных им организаций, а также в пределах своей компетенции осуществляют массовое информационное обеспечение пользователей по вопросам прав, свобод и обязанностей граждан, их безопасности и другим вопросам, представляющим общественный интерес (пункт 1 статьи 13). При этом для формирования таких ресурсов закон предусматривает, что граждане, органы государственной власти, органы местного самоуправления и общественные объединения обязаны представлять документированную информацию органам и организациям, ответственным за формирование и использование государственных информационных ресурсов. Перечни представляемой в обязательном порядке документированной информации и перечни органов и организаций, ответственных за сбор и обработку федеральных информационных ресурсов, должно утверждать Правительство РФ (пункт 1 статьи 8). Оно же должно установить перечень информационных услуг (бесплатных или с частичной оплатой для пользователя) с компенсацией затрат из средств государственного бюджета (пункт 4 статьи 13).

2. Граждане, органы государственной власти, органы местного самоуправления, организации и общественные объединения обладают равными правами на доступ к государственным информационным ресурсам и не обязаны обосновывать перед владельцем этих ресурсов необходимость получения запрашиваемой ими информации. Исключение составляет информация с ограниченным доступом (пункт 1 статьи 12). При этом декларируется, что доступ физических и юридических лиц к государственным информационным ресурсам является основой осуществления общественного контроля за деятельностью органов государственной власти, органов местного самоуправления, общественных, политических и иных организаций, а также за состоянием экономики, экологии и других сфер общественной жизни.

3. Органы государственной власти и организации, ответственные за формирование и использование информационных ресурсов, обеспечивают условия для оперативного и полного предоставления пользователю документированной информации в соответствии с обязанностями, установленными уставами (положениями) этих органов и организаций (пункт 4 статьи 12). При этом перечни информации и информационных услуг, сведения о порядке и условиях доступа к информационным ресурсам должны предоставляться пользователям бесплатно (пункт 3 статьи 12).

4. Граждане и организации имеют право на доступ к документированной информации о них, на уточнение этой информации в целях обеспечения ее полноты и достоверности, имеют право знать, кто и в каких целях использует или использовал эту информацию. Ограничение доступа граждан и организаций к информации о них допустимо лишь на основаниях, предусмотренных федеральными законами (пункт 1 статьи 14). Владелец документированной информации о гражданах обязан предоставить информацию бесплатно по требованию тех лиц, которых она касается. Ограничения возможны лишь в случаях, предусмотренных законодательством РФ (пункт 2 статьи 14).

5. Информация, полученная на законных основаниях из государственных информационных ресурсов гражданами и организациями, может быть использована ими для создания производной информации в целях ее коммерческого распространения с обязательной ссылкой на источник информации (пункт 2 статьи 12).

6. Отказ в доступе к открытой информации или предоставление пользователям заведомо недостоверной информации могут быть обжалованы в судебном порядке. Неисполнение или ненадлежащее исполнение обязательств по договору поставки, купли-продажи, по другим формам обмена информационными ресурсами между организациями рассматривается арбитражным судом. Во всех случаях лица, которым отказано в доступе к информации, и лица, получившие недостоверную информацию, имеют право на возмещение понесенного ими ущерба (пункт 1 статьи 24).

7. Руководители, другие служащие органов государственной власти, организаций, виновные в незаконном ограничении доступа к информации и нарушении режима защиты информации, несут ответственность в соответствии с уголовным, гражданским законодательством и Кодексом об административных правонарушениях Российской Федерации (статьи 5.29, 13.12) [29].

Уровни доступа к информации с точки зрения законодательства

Вся информация с точки зрения права делится на несколько основных сегментов:

Информация без ограничения права доступа. К такого рода информации, например, относится:

- информация общего пользования, предоставляемая пользователям бесплатно;
- информация о состоянии окружающей природной среды, ее загрязнении — сведения (данные), полученные в результате мониторинга окружающей природной среды, ее загрязнения (Федеральный закон от 2 мая 1997 г. № 76-ФЗ «Об уничтожении химического оружия»);
- информация в области работ по хранению, перевозке, уничтожению химического оружия — сведения о состоянии здоровья граждан и объектов окружающей среды в районах размещения объектов по хранению химического оружия и объектов по уничтожению химического оружия, мероприятиях по обеспечению химической, санитарно-гигиенической, экологической и пожарной безопасности при проведении работ по хранению, перевозке и уничтожению химического оружия, а также о мерах по предотвращению возникновения чрезвычайных ситуаций и ликвидации их последствий при выполнении указанных работ, предоставляемые по запросам граждан и юридических лиц, в том числе общественных объединений (Федеральный закон от 2 мая 1997 г. № 76-ФЗ «Об уничтожении химического оружия», статья 1.2).

Информация, содержащая сведения об обстоятельствах и фактах, представляющих угрозу жизни, здоровью граждан, не подлежит засекречиванию, не может быть отнесена к тайне.

Информация с ограниченным доступом — государственная тайна, служебная тайна, коммерческая тайна, банковская тайна, профессиональная тайна и персональные данные как институт охраны права неприкосновенности частной жизни.

Информация, распространение которой наносит вред интересам общества, законным интересам и правам граждан, — порнография; информация, разжигающая национальную, расовую и другую рознь; пропаганда и призывы к войне, ложная реклама,

реклама со скрытыми вставками и т. п. — так называемая «вредная» информация.

Объекты интеллектуальной собственности (то, что не может быть отнесено к информации с ограниченным доступом, но охраняется особым порядком через институты интеллектуальной собственности — авторское право, патентное право, средства индивидуализации и т. п. Исключение составляют ноу-хау, которые охраняются в режиме коммерческой тайны).

Иная общедоступная информация, в которой эксперты выделяют более 20 видов открытой общедоступной информации.

К ограничениям и запретам следует отнести следующие перечни:

1. Перечень оснований для ограничения информационных прав:

- защита основ конституционного строя;
- защита нравственности, здоровья, прав, законных интересов других лиц;
- обеспечение обороны страны и безопасности государства;
- обеспечение общественного спокойствия в целях предотвращения беспорядков и борьбы с преступностью;
- предотвращение разглашения конфиденциальной информации;
- обеспечение авторитета и беспристрастности правосудия;
- условия чрезвычайного положения, установленные по закону (на определенный период).

2. Перечень случаев прямого ограничения информационных прав:

- использование прав в целях насильственного изменения конституционного строя;
- пропаганда социальной ненависти, социального, расового, национального, религиозного, языкового превосходства, насилия и войны;
- нарушение права на неприкосновенность частной жизни (на личную, семейную тайну), неприкосновенность жилища, права на уважение и защиту чести, достоинства и репутации, тайны переписки, телефонных переговоров, телеграфных и иных сообщений;
- нарушение права на государственную, служебную, профессиональную, коммерческую и банковскую тайну;
- право на отказ от свидетельствования против себя самого, своего супруга и близких родственников.

3. Перечень видов информации с ограниченным доступом:
   - государственная тайна;
   - служебная тайна;
   - коммерческая тайна;
   - банковская тайна;
   - профессиональная тайна;
   - персональные данные.

4. Перечень сведений, доступ к которым не может быть ограничен.

Для реализации права на информацию в Конституции РФ заложены основания, по которым доступ к отдельным видам информации не подлежит какому-либо ограничению, например в статье 42 закреплено право на достоверную информацию о состоянии окружающей среды, которое не может быть ограничено. В случае возникновения угрозы жизни и здоровью людей должностные лица обязаны информировать население о ней под страхом привлечения к ответственности (часть 3 статьи 41).

В ряде законов, устанавливающих ограничения доступа к информации, также вводится перечень сведений, доступ к которым не может быть ограничен. Так, в статье 7 Закона РФ «О государственной тайне» перечислены сведения, не подлежащие засекречиванию. В пункте 3 статьи 10 Федерального закона «Об информации, информатизации и защите информации» приведен перечень документов, доступ к которым запрещено ограничивать. В Закон РФ «О коммерческой тайне» планируется также включить перечень сведений, которые нельзя отнести к коммерческой тайне. В Федеральном законе «О благотворительной деятельности и благотворительных организациях» (пункт 7 статьи 19), в свою очередь, определен перечень сведений, которые не могут составлять коммерческую тайну.

К механизмам доступа к открытой информации можно отнести:

- структурирование открытой информации по уровням доступа — подлежащей обязательному опубликованию в средствах массовой информации, предоставлению по запросу каждого гражданина, обязательному предоставлению по запросу отдельных категорий граждан;
- структурирование органов государственной власти и местного самоуправления, чьи должностные лица обязаны предоставлять информацию (пример — государственная система научно-технической информации, положение о которой

утверждено постановлением Правительства РФ от 24 июля 1997 года № 950);

- установление обязанности должностных лиц на основании документов предоставлять по запросам граждан информацию, доступ к которой не ограничен законом;
- публикацию в общедоступных изданиях документированной информации, подлежащей обязательному распространению, всех перечней по установлению ограничений и запретов в информационной сфере, перечня органов государственной власти и местного самоуправления (с указанием их функций и адресов);
- создание общедоступных баз данных в органах государственной власти и местного самоуправления, в том числе на общедоступных серверах с указанием в средствах массовой информации их адресов и порядка получения информации;
- порядок предоставления информации, предусматривающий сроки, объем и форму предоставления информации в зависимости от правового статуса организации, в адрес которой направлен запрос;
- установление источников финансирования и покрытия расходов, связанных с предоставлением информации, — в соответствии с нормой Гражданского кодекса РФ (пункт 2 статьи 779) предоставление информации отнесено к обязательствам о возмездном оказании услуг.

Важное значение для реализации информационных прав граждан на доступ к информации имеет Послание Президента РФ Федеральному Собранию РФ от 17 февраля 1998 года, где в целях обеспечения информационной открытости государственной власти гражданскому обществу определены следующие задачи:

- радикальное обновление функций, методов, критериев деятельности существующих информационных служб органов исполнительной власти;
- сужение области ведомственных тайн;
- уточнение с помощью общественных организаций гарантий предоставления общественно значимой официальной информации;
- обучение государственных служащих практической работе в условиях информационной открытости;
- установление каналов двусторонней связи государственных органов с общественными организациями, занимающими-

ся аналогичными проблемами (экологическими, социальными и др.).

Виды доступа к информации. Доступ к информации также важно четко разграничить в зависимости от вида информации и вида субъекта, реализующего свое право на доступ к информации. Исходя из этого, различаются следующие виды доступа:

1. Обязательное доведение.
2. Свободный доступ.
3. Предоставление информации по запросу юридических лиц.
4. Предоставление информации по запросу физических лиц.

Например, доступ к информации через обязательное ее доведение (на примере законодательной деятельности) должен быть обеспечен после принятия закона и подписания его Президентом РФ, поскольку законы должны быть опубликованы и вступают в силу только в случае их обязательного опубликования.

Наряду с этим обязательному доведению подлежит информация об обстоятельствах и фактах по угрозе общественной безопасности, здоровью и жизни граждан, о реквизитах организаций, предоставляющих информацию, о реестрах официальных документов, которые также подлежат обязательному доведению.

Свободный доступ — это ситуация, когда, например, на сервере соответствующего субъекта органа власти в электронном виде выставляется информация о законопроекте. Правомочия на свободный доступ к информации в данном случае могут реализоваться через обязанность государства создать условия, при которых лицо, заинтересованное в получении информации, могло получить к ней доступ по своему желанию. В перечень таких условий могут входить — накопление информации и поддержание ее в актуальном состоянии, систематизация информации и т. п. В то же время условия свободного доступа, включая адрес нахождения информации, должны быть широко известны, и здесь применимо уже правомочие обязательного доведения.

Различаются четыре основных вида отношений, которые могут возникать между субъектами по степени ограничения доступа:

- лиц (как физических, так и юридических) по отношению к государству;
- государства по отношению к лицам (как физическим, так и юридическим);

- физических лиц по отношению к организациям (юридическим лицам);
- юридических лиц по отношению к физическим лицам.

Например, при запросе *лиц в органы государственной власти* и органы местного самоуправления ограничение права на доступ к информации связано только с государственной тайной, служебной тайной и персональными данными, потому что коммерческой тайны, банковской тайны, профессиональной тайны в органах государственной власти и органах местного самоуправления, по определению, быть не может.

Что касается государственных предприятий, которые, казалось бы, представляют государство, то в данной ситуации они являются коммерческими структурами с государственным видом собственности, в которых может иметь место коммерческая тайна.

При запросах *государства по отношению к физическим и юридическим* лицам (что регламентируется нормами Законов РФ «О государственной службе», «О воинской обязанности и военной службе», «Об обороне», «О милиции» и т. п.) в качестве основания для ограничения права доступа к информации могут выступать персональные данные, коммерческая тайна, банковская тайна и профессиональная тайна.

При реализации права *физических лиц на доступ к информации у юридических* лиц в качестве основания для ограничения права доступа к информации могут выступать профессиональная тайна, коммерческая тайна, банковская тайна. При запросе юридических лиц к физическим лицам основанием для ограничения права могут выступать персональные данные.

При реализации права на доступ к информации важно обеспечить, чтобы получаемая информация была достоверной, полной и ее подлинность при дальнейшем использовании не вызывала ни у кого сомнения. В связи с возрастающим объемом хранения и использования информации, в том числе ограниченного доступа, в электронном виде все чаще применяется понятие «электронного документа». В то же время проблема сохранения электронных документов от уничтожения, копирования, модификации, подделки требует для своего разрешения специфических средств и методов защиты (формирование корпоративных сетей, техническая защита сетей, криптографическая защита и т. д.).

Ответственность за нарушение законодательства в информационной сфере

За непредоставление информации гражданам, палатам Федерального Собрания РФ и Счетной палате РФ (статьи 140 и 287), а также за сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей (статья 237), в Уголовном кодексе РФ (от 13.06.1996 г.) предусмотрена ответственность.

Ответственность в действующем законодательстве оговорена в случае неправомерного засекречивания, нарушения требований по составу предоставляемых сведений, неопубликования сведений, нарушения права граждан на бесплатное получение информации, сокрытие (непредоставление) сведений об обстоятельствах, создающих опасность для жизни или здоровья людей, несвоевременное предоставление сведений, сокрытие информации, сообщение ложных (недостоверных) сведений, ограничение права на предоставление информации, искажение сведений, нарушение свободного международного информационного обмена.

Защита права на доступ к информации может осуществляться:

- в форме, находящейся за пределами юрисдикции (самозащита своих прав и законных интересов);
- в юрисдикционной форме (в административном или в судебном порядке).

В *административном* порядке — через подачу жалобы лицом, чьи права нарушены, на должностное лицо (орган) в вышестоящую инстанцию, специальный орган — Судебную палату по информационным спорам при Президенте РФ.

В *судебном* порядке — лицо может выбрать любой способ защиты нарушенных прав через подачу иска (жалобы) для рассмотрения в гражданском, административном или уголовном судопроизводстве.

При рассмотрении иска в гражданском судопроизводстве потерпевший вправе использовать основные способы защиты гражданских прав, предусмотренных в статье 12 Гражданского кодекса РФ (от 30.11.1996 г.), в том числе требовать:

- признания права;
- прекращения действий, нарушающих право или создающих угрозу его нарушения;

- признания недействительным акта государственного органа или органа местного самоуправления;
- восстановления права;
- возмещения убытков;
- компенсации морального ущерба.

Случаи возможной административной ответственности при нарушении права на доступ к объективной информации достаточно многочисленны.

Так, в Кодексе РФ об административных правонарушениях (от 30.12.2001 г.) [29] предусматривается административная ответственность за следующие нарушения:

- нарушение права граждан на ознакомление со списком избирателей (статья 5.1);
- изготовление или распространение анонимных агитационных материалов (статья 5.12);
- умышленное уничтожение, повреждение агитационных печатных материалов (статья 5.14);
- непредоставление или неопубликование отчетов о расходовании средств на подготовку и проведение выборов (референдума) (статья 5.17);
- непредоставление либо неопубликование сведений об итогах голосования или о результатах выборов (статья 5.25);
- невыполнение обязанностей по регистрации в судовых документах операций с вредными веществами и смесями (статья 8.16);
- изготовление или эксплуатацию технических средств, не соответствующих государственным стандартам или нормам на допускаемые уровни радиопомех (статья 13.8);
- непредоставление сведений федеральному антимонопольному органу (статья 19.8);
- непредоставление информации для составления списков присяжных заседателей (статья 17.6);
- невыполнение законных требований прокурора (в том числе на предоставление информации) (статья 17.7);
- несообщение сведений о гражданах, состоящих или обязанных состоять на воинском учете (статья 21.4);
- нарушение порядка и сроков предоставления сведений о несовершеннолетних, нуждающихся в передаче на воспитание, и др. (статья 5.36).
- нарушение порядка предоставления обязательного экземпляра документов и др. (статья 13.23);

- отказ в предоставлении гражданину информации (статья 5.39);
- злоупотребление свободой массовой информации (статья 13.15);
- воспрепятствование распространению продукции средства массовой информации (статья 13.16);
- воспрепятствование приему радио- и телепрограмм (статья 13.18);
- нарушение правил распространения обязательных сообщений (статья 13.17). Уголовная ответственность в этой сфере предусмотрена в Уголовном кодексе РФ (от 13.06.1996 г.) в следующих статьях:
  - статья 140 — отказ в предоставлении гражданину информации;
  - статья 237 — сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей;
  - статья 287 — отказ в предоставлении информации Федеральному Собранию РФ или Счетной палате РФ.

Контрольные вопросы

1. Что такое национальные интересы? Какие другие виды интересов вам известны?
2. В чем могут заключаться национальные интересы России?
3. В чем заключается национальная безопасность, ее определения?
4. Что такое уровни обеспечения национальной безопасности?
5. В чем состоят основные угрозы безопасности России?
6. Какие имеются основные направления обеспечения безопасности и какова их взаимосвязь с информационной безопасностью?
7. Что такое информационная безопасность, каковы ее основные аспекты?
8. В чем заключаются жизненно важные интересы в информационной сфере и угрозы жизненно важным интересам в информационной сфере?
9. Укажите основные законы, относящиеся к организации и функционированию системы информационной безопасности и защиты информации.
10. Назовите основные факторы, создающие возможность применения информационного оружия против РФ.
11. Какие основные мероприятия проводятся в государственных структурах для обеспечения информационной безопасности?
12. Что такое информационная война и информационное превосходство?

13. Что такое информационное оружие, каковы его разновидности?
14. Каковы принципы, основные задачи и функции обеспечения информационной безопасности?
15. В чем заключаются функции государственной системы по обеспечению информационной безопасности?
16. Каковы основные отечественные и зарубежные стандарты в области информационной безопасности?
17. Какая система называется безопасной и какая надежной?
18. Что такое политика безопасности?
19. Каковы основные предметные направления ЗИ?
20. Что такое государственная тайна?
21. Что называется коммерческой тайной?
22. Что такое служебная тайна?
23. Что представляет профессиональная тайна?
24. Что такое персональные данные?
25. Каковы источники права на доступ к информации?
26. Каковы уровни доступа к информации с точки зрения законодательства?
27. Что такое информация ограниченного распространения?
28. Каковы виды доступа к информации?
29. В чем может заключаться ответственность за нарушение законодательства в информационной сфере?

Глава 2
ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОБРАБОТКИ ДАННЫХ

Под защитой информации в АСОД понимается регулярное использование в них средств и методов, принятие мер и осуществление мероприятий с целью системного обеспечения требуемой надежности информации, хранимой и обрабатываемой с использованием средств АСОД [1, 9, 10].

2.1. Предмет и объекты защиты информации в автоматизированных системах обработки данных (АСОД)

Надежность информации

Под надежностью информации в АСОД понимается интегральный показатель, характеризующий качество информации с точки зрения:

- физической целостности, т. е. отсутствия искажений или уничтожения элементов этой информации;
- доверия к информации, т. е. уверенности в отсутствии в ней подмены (несанкционированной модификации) ее элементов при сохранении целостности;
- безопасности информации, т. е. отсутствия несанкционированного получения ее лицами или процессами, не имеющими на это соответствующих полномочий;
- уверенности в том, что переданные (проданные) владельцем программы или элементы баз (массивов) данных не будут размножаться (копироваться, тиражироваться) и использоваться без его санкции.

На основе интегрального критерия надежности активно развивается концепция интегральной информационной безопасности (рис. 2.1).

Рис. 2.1. Интегральная информационная безопасность

Под интегральной информационной безопасностью понимается комплексная совокупность мер по защите информации в ходе всего непрерывного процесса подготовки, обработки, хранения и передачи информации (меры защиты действуют непрерывно в течение всего защищаемого периода)

Вторая цель защиты — это предупреждение несанкционированной модификации информации — в значительной мере является некоторой комбинацией первой и третьей целей. В самом деле, несанкционированная модификация может быть или случайной или злоумышленной.

Случайная модификация может являться следствием искажения некоторой информации вследствие ошибки людей, искажения адреса записи информации из-за сбоя ЭВМ и т. п. Злоумышленная же модификация является результатом злоумышленных действий людей.

Под системной защитой информации понимается защита:

- во всех структурных элементах АСОД;
- на всех участках и технологических маршрутах автоматизированной обработки информации;
- при всех режимах функционирования АСОД;
- на всех этапах жизненного цикла АСОД;
- с учетом взаимодействия АСОД с внешней средой.

В автоматизированных системах обработки данных информация имеет свой жизненный цикл. Полученная информация в начале оценивается на достоверность и полезность. Остальные этапы жизненного цикла информации иллюстрируются на рис. 2.2. На каждом этапе жизненного цикла информация, с точки зрения ее защиты, оценивается по-разному.

Рис. 2.2. Жизненный цикл информации в АСОД

При выборе или разработке методов защиты информации, а также при их внедрении существенную роль играют: формы машинного представления информации; используемые способы физического представления информации; структуры данных; используемые физические носители сообщений и т. д. [1].

Основными видами информации, подлежащими защите, в общем случае могут быть (рис. 2.3):

1) исходные данные, т. е. данные, поступившие в АСОД на хранение и обработку от пользователей, абонентов и взаимодействующих систем;

2) производные данные, т. е. данные, полученные в АСОД в процессе обработки исходных и производных данных;

3) нормативно-справочные, служебные и вспомогательные данные, включая и данные системы защиты;

4) программы, используемые для обработки данных, организации и обеспечения функционирования АСОД, включая и программы системы защиты информации;

Рис. 2.3. Элементы информационной базы АСОД

5) алгоритмы, на основе которых разрабатывались программы (если они находятся на объектах, входящих в состав АСОД);

6) методы и модели, на основе которых разрабатывались алгоритмы (если они находятся на объектах, входящих в состав АСОД);

7) постановки задач, на основе которых разрабатывались методы, модели, алгоритмы и программы (если они находятся на объектах, входящих в состав АСОД);

8) техническая, технологическая и другая документация, находящаяся на объектах АСОД.

Уязвимость информации

Уязвимость информации необходимо оценивать в процессах разработки и внедрения АСОД, функционирования АСОД на технологических участках автоматизированной обработки информации, функционирования АСОД независимо от процессов обработки информации. Уязвимость информации в процессе разработки и внедрения АСОД обусловливается уязвимостью создаваемых компонентов системы и создаваемых баз данных. Особое значение на данной стадии имеет минимизация уязвимости программного обеспечения, поскольку от этого существенно зависит общая уязвимость информации в АСОД.

Условия автоматизированной обработки информации характеризуются главным образом совокупностью следующих параметров: структурой АСОД, которой определяется состав подлежащих защите объектов и элементов; наличием и количеством дестабилизирующих факторов, потенциально возможных в структурных компонентах АСОД; количеством и категориями лиц, которые могут быть потенциальными нарушителями статуса защищаемой системы.

Уязвимость информации в процессе функционирования АСОД независимо от процесса обработки информации обусловливается тем, что современные АСОД представляют собою организационную структуру с высокой концентрацией информации, которая может быть объектом случайных или злоумышленных воздействий даже в том случае, если автоматизированная обработка ее не осуществляется.

Поскольку воздействие на информацию различных факторов в значительной мере является случайным, то в качестве количе-

ственной меры уязвимости информации наиболее целесообразно принять вероятность нарушения ее защищаемых характеристик при тех условиях сбора, обработки и хранения, которые имеют место в АСОД, а также потенциально возможные размеры (математическое ожидание) возможного ущерба защищенности информации.

2.2. Элементы и объекты защиты в АСОД

Под объектом защиты будем понимать такой структурный компонент АСОД, в котором находится или может находиться подлежащая защите информация. С точки зрения развиваемых здесь подходов к защите информации объект защиты должен отвечать следующим условиям:

1) принадлежать к одному и тому же организационному компоненту АСОД;

2) участвовать в осуществлении одних и тех же функций, связанных с автоматизированной отработкой информации в АСОД;

3) быть локализованным с точки зрения территориального расположения АСОД. Формирования, удовлетворяющие перечисленным условиям, будем называть типовыми структурными компонентами (ТСК) АСОД. Таким образом, в качестве объектов защиты выступают ТСК АСОД.

Под элементом защиты будем понимать ту находящуюся в АСОД совокупность данных, которая может содержать подлежащие защите сведения. Элементы защиты выделяются по следующим условиям:

1) нахождения в одном и том же объекте защиты;

2) локализуемости с точки зрения носителя информации;

3) однородности в смысле воздействия дестабилизирующих факторов.

Чтобы соответствовать приведенным выше требованиям и условиям, принципы формирования перечней объектов и элементов защиты информации должны быть следующими:

1) унифицированность;

2) охват всех потенциально возможных структур АСОД;

3) минимизация состава.

Основным методом формирования перечней объектов и элементов защиты является структурно-логический анализ потенциально возможных архитектур АСОД и технологических схем автоматизированной обработки информации.

Основные элементы АСОД и типовые структурные компоненты

Основными элементами АСОД и типовыми структурными компонентми являются (рис. 2.4):

- *аппаратные средства ЭВМ* (основные устройства: память, процессор, управляющее устройство, устройства ввода, устройства вывода);

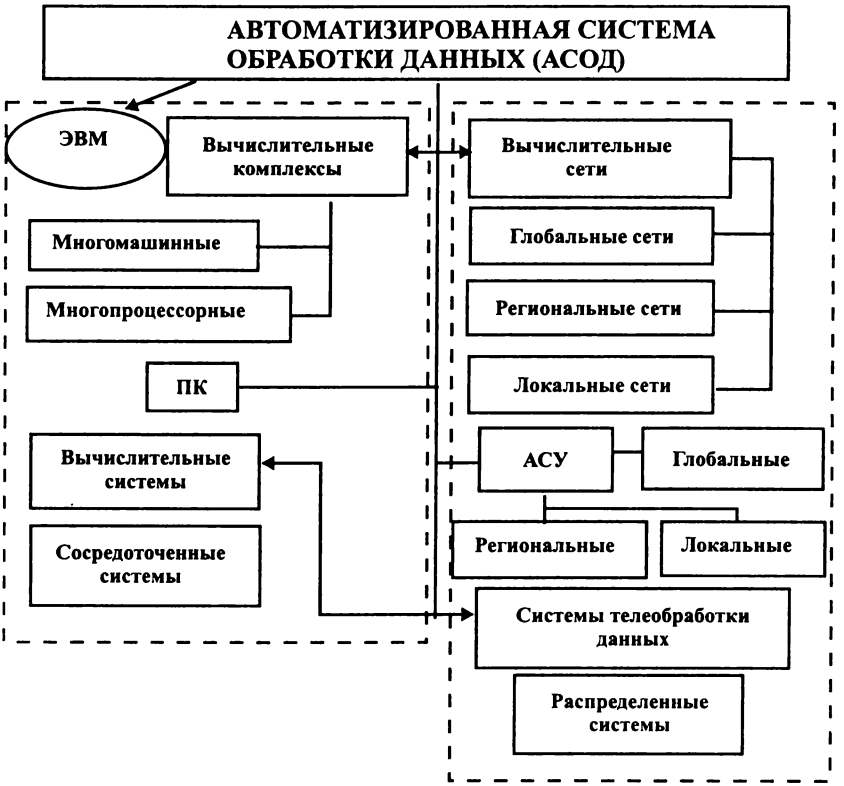


Рис. 2.4. Основные элементы, объекты защиты в АСОД и типовые структурные компоненты системы

- *система программного обеспечения ЭВМ* (операционная система, комплекс программ технического обслуживания, пакеты прикладных программ).

Аппаратные средства ЭВМ и система ее программного обеспечения образуют одномашинную систему обработки данных.

Для повышения надежности и производительности несколько ЭВМ связываются между собой, образуя многомашинный вычислительный комплекс (ВК). Если ВК состоит из двух машин, то связь чаще всего осуществляется через адаптер, который обеспечивает обмен данными каналами ввода-вывода машин и передачу сигналов прерывания;

- *ВК*, состоящий из нескольких процессоров с общей оперативной памятью и периферийными устройствами, образует многопроцессорный ВК (все процессоры имеют доступ ко всему объему данных). В таких ВК процессоры, модули оперативной памяти и каналы ввода-вывода, к которым подключены периферийные устройства, объединяются в единый комплекс с помощью средств коммутации, обеспечивающих доступ каждого процессора к любому модулю оперативной памяти и каналу ввода-вывода, а также возможность передачи данных между последними;
- *многомашинные и многопроцессорные* ВК, являющиеся базовыми средствами для создания систем обмена данными различного назначения. Поэтому в состав ВК принято включать только аппаратные средства и общесистемное программное обеспечение (но не прикладное программное обеспечение, связанное с конкретной областью применения ВК);
- *вычислительная система (ВС)* — система обработки данных, включающая в себя аппаратные средства и программное обеспечение, ориентированное на решение определенной совокупности задач. Если ВС имеет средства гибкого приспособления к структуре реализуемого алгоритма (за счет изменения конфигурации системы), то она называется адаптируемой ВС или системой с динамической структурой. За счет адаптации достигается высокая производительность в широком классе задач и обеспечивается устойчивость системы к отказам;
- *системы телеобработки данных*, которые используются для получения данных из удаленных ЭВМ или ВК. Пользователи (абоненты) взаимодействуют с системой посредством терминалов;

- *каналы*, через которые передаются блоки данных (собственно данные и служебная информация).

С ростом масштабов применения средств автоматизированной обработки данных и необходимостью обмена информацией на расстоянии стало целесообразным объединение сосредоточенных систем обработки данных в вычислительные сети (использование территориально-распределенными пользователями программного обеспечения и информационных баз, возможностью организации «распределенной обработки» данных и др.);

- *сеть передачи данных (СПД)*, которая образует каналы связи и узлы (центры) коммутации, в которых связанные процессоры управляют выбором маршрутов передачи данных в сети.

По функциональному назначению различают [1]:

- информационные сети (оказывающие пользователям в основном информационные услуги);
- вычислительные сети (решающие в основном задачи с обменом данными и программными средствами между ЭВМ сети);
- смешанные сети — информационно-вычислительные сети;
- *локальные вычислительные сети (ЛВС)* и персональные ЭВМ (ПЭВМ). В настоящее время они очень распространены. Все новые разработки АСОД в основном ведутся на их основе. Однако с точки зрения безопасности информации идеи и принципы ее ввода-вывода, хранения, обработки и передачи изменились не настолько, чтобы это принципиально повлияло на возможные каналы несанкционированного преднамеренного доступа к информации и концепцию ее защиты. Произошли лишь пространственные перемещения средств централизованной обработки информации, увеличились ее объемы и усложнилась техника ее обработки. С этих позиций ПЭВМ можно рассматривать как миниатюрный комплекс средств автоматизации с централизованной обработкой данных, который в своем составе содержит те же самые средства ввода-вывода, хранения и обработки информации.

ЛВС с позиций безопасности информации содержит те же, что и обычная сеть, комплексы средств автоматизации и каналы связи, применяются те же протоколы связи открытых систем (за исключением физического и канального уровней). Конечно, техническая реализация этих элементов другая;

- *АСУ*, отличающаяся от ВС наличием средств, решающих задачи управления каким-либо процессом (технологическими устройствами или производственными процессами — АСУ ТП и административно-организационными процессами — автоматизированная система организационного управления (АСОУ));
- *АСОУ* представляет собой сложный комплекс, состоящий из коллективов специалистов, автоматизированных и иных технических средств, математического, программного, информационного, лингвистического и правового обеспечения. Весь этот комплекс предназначен для сбора, обработки, хранения и передачи (выдачи) информации. Общая структура таких АСУ обычно соответствует иерархической структуре органов управления и принятым в них процессам управления.

При формировании перечня ТСК, которые принимаются в качестве объектов защиты, естественно, должны быть приняты во внимание все существующие формы и способы использования современной вычислительной техники. Данное обстоятельство является существенно важным, поскольку в связи с массовым распространением персональных ЭВМ резко расширилось многообразие форм и способов организации АСОД. Все это многообразие может быть охвачено следующим перечнем:

1) отдельно функционирующая ЭВМ;

2) стандартные модули обработки информации, т. е. ЭВМ (чаще всего ПЭВМ), осуществляющие строго определенную в функциональном отношении обработку информации;

3) локальные вычислительные центры (ВЦ), т. е. ВЦ, обеспечивающие автоматизированную обработку информации в интересах одного предприятия (учреждения);

4) вычислительные центры коллективного пользования (ВЦКП), представляющие собой высокоорганизованную совокупность различных средств, которые позволяют осуществлять автоматизированную обработку информации в интересах большого числа пользователей, независимо от их организационной принадлежности.

Все перечисленные организационные структуры использования вычислительной техники могут функционировать как автономно (т. е. независимо от других структур), так и в сопряжении между собой, причем сопряжение может быть организационным (обмен информацией осуществляется посредством промежуточ-

ного носителя) и техническим (информация из ЗУ одной машины пересылается непосредственно в ЗУ другой машины). С помощью средств сопряжения могут создаваться информационно-вычислительные системы и сети различной архитектуры и территориальной распределенности.

Исходя из современных возможностей реализации различных элементов АСОД, в полный перечень, очевидно, должны быть включены следующие ТСК:

- терминал пользователя непрограммируемый;
- терминал пользователя программируемый (ПЭВМ);
- терминал оператора ЭВМ;
- терминал прикладного программиста;
- терминал администратора баз данных;
- сетевое оборудование (каналы связи, разветвители, заглушки, коммутаторы, концентраторы);
- аппаратура связи типа модем;
- большая (мини-, супермини-) ЭВМ;
- электронно-вычислительный комплекс (ЭВК);
- зона внешних запоминающих устройств большой ЭВМ;
- диспетчерский пункт ВЦ;
- хранилище машинных носителей информации;
- хранилище документов;
- служебные помещения пользователей и персонала АСОД.

Дестабилизирующие факторы АСОД

Наиболее общим подходом является рассмотрение в качестве дестабилизирующих тех факторов, которые влияют на уязвимость информации в современных АСОД [10, 11].

Дестабилизирующими факторами являются такие процессы или события, которые могут появляться на каком-либо этапе функционирования АСОД и следствием которых могут быть нежелательные (в смысле защищенности) воздействия на информацию. Задача выявления множества дестабилизирующих факторов является одной из центральных в проблеме защиты информации, причем по вполне понятным причинам требование полноты ее решения является абсолютным. В то же время регулярные методы решения данной задачи практически отсутствуют. Поэтому к формированию множества дестабилизирующих факторов надо

подходить в максимальной степени системно. С этой целью прежде всего сформируем полный перечень возможных типов дестабилизирующих факторов и потенциально возможных источников их формирования.

В соответствии с архитектурой, технологией и условиями функционирования современных АСОД дестабилизирующими факторами являются: количественная недостаточность АСОД; качественная недостаточность элементов АСОД; отказы элементов АСОД; сбои элементов АСОД; ошибки элементов АСОД; стихийные бедствия; злоумышленные действия; побочные явления.

Названные типы дестабилизирующих факторов определяются следующим образом:

- *количественная недостаточность* — физическая нехватка одного или нескольких компонентов АСОД для обеспечения требуемой защищенности информации по рассматриваемым показателям;
- *качественная недостаточность* — несовершенство конструкции или организации одного или нескольких компонентов АСОД, в силу чего не обеспечивается требуемая защищенность информации;
- *отказ* — нарушение работоспособности какого-либо элемента АСОД, приводящее к невозможности выполнения им своих функций;
- *сбой* — временное нарушение работоспособности какого-либо элемента АСОД, следствием чего может быть неправильное выполнение им в этот момент своих функций;
- *ошибка* — неправильное (одноразовое или систематическое) выполнение элементом АСОД одной или нескольких функций, происходящее вследствие специфического (постоянного или временного) его состояния;
- *стихийное бедствие* — спонтанно возникающее неконтролируемое явление, проявляющееся как могущественная разрушительная сила;
- *злоумышленное действие* — действия людей, специально направленные на нарушение защищенности информации;
- *побочное явление* — явление, сопутствующее выполнению элементом АСОД своих основных функций, следствием которого может быть нарушение защищенности информации.

Источниками дестабилизирующих факторов, т. е. средой их проявления, могут быть как компоненты *АСОД*, так и внешняя среда; люди — отдельные лица или группы лиц, имеющие отно-

шение к функционированию АСОД и действия которых могут стать причиной нарушения защищенности информации; технические устройства — технические средства, используемые в АСОД; модели, алгоритмы и программы — математические и программные средства, используемые в АСОД; технология функционирования — совокупность средств, приемов, правил, мероприятий и соглашений, используемых в процессе обработки информации; внешняя среда — совокупность элементов, не входящих в состав АСОД, но которые могут оказывать влияние на защищенность информации в АСОД.

Причины нарушения целостности информации (ПНЦИ)

Под ПНЦИ понимаются такие дестабилизирующие факторы, следствием проявления которых может быть нарушение физической целостности информации, т. е. ее искажение или уничтожение.

Ниже перечислены группы причин нарушения целостности информации.

1. Нарушение функционирования элементов АСОД:
   - отказы/сбои/ошибки основной аппаратуры;
   - отказы/сбои/ошибки программ;
   - отказы/сбои/ошибки людей;
   - отказы/сбои/ошибки носителей информации;
   - отказы/сбои/ошибки систем питания;
   - отказы/сбои/ошибки систем обеспечения нормальных условий работы аппаратуры и персонала;
   - отказы/сбои/ошибки системы передачи данных;
   - отказы/сбои/ошибки вспомогательных материалов.
2. Стихийные бедствия:
   - пожар;
   - наводнение;
   - землетрясение;
   - ураган;
   - взрыв;
   - авария.
3. Злоумышленные действия:
   - запоминание информации;
   - копирование;

- хищение;
- подмена;
- подключение;
- поломка (повреждение);
- диверсия.

4. Другие факторы:
   - электромагнитные излучения устройств АСОД;
   - паразитные наводки;
   - внешние электромагнитные излучения;
   - вибрация;
   - внешние атмосферные условия.

Каналы несанкционированного получения информации в АСОД (КНПИ)

Под КНПИ понимаются такие дестабилизирующие факторы, следствием проявления которых может быть получение (или опасность получения) защищаемой информации лицами или процессами, не имеющими на это законных полномочий.

Перечни основных типов каналов несанкционированного доступа к информации выглядят следующим образом.

Каналы, проявляющиеся безотносительно к обработке информации и без доступа злоумышленника к элементам ЭВТ:

- хищение носителей информации на заводах, где производится ремонт ЭВТ;
- подслушивание разговоров лиц, имеющих отношение к АСОД;
- провоцирование на разговоры лиц, имеющих отношение к АСОД;
- использование злоумышленником визуальных средств;
- использование злоумышленником оптических средств;
- использование злоумышленником акустических средств.

Каналы, проявляющиеся в процессе обработки информации без доступа злоумышленника к элементам АСОД:

- электромагнитные излучения устройств отображения информации;
- электромагнитные излучения процессоров;
- электромагнитные излучения внешних запоминающих устройств;

- электромагнитные излучения аппаратуры связи;
- электромагнитные излучения линий связи;
- электромагнитные излучения вспомогательной аппаратуры;
- паразитные наводки в коммуникациях водоснабжения;
- паразитные наводки в системах канализации;
- паразитные наводки в сетях теплоснабжения;
- паразитные наводки в системах вентиляции;
- паразитные наводки в шинах заземления;
- паразитные наводки в цепях радиофикации;
- паразитные наводки в цепях телефонизации и диспетчерской связи;
- паразитные наводки в сетях питания по цепи 50 Гц;
- подключение генераторов помех;
- подключение регистрирующей аппаратуры;
- осмотр отходов производства, попадающих за пределы контролируемой зоны.

Каналы, проявляющиеся безотносительно к обработке информации с доступом злоумышленника к элементам АСОД, но без изменения последних:

- копирование бланков с исходными данными;
- копирование магнитных носителей;
- копирование с устройств отображения;
- копирование выходных документов;
- копирование других документов;
- хищение производственных отходов.

Каналы, проявляющиеся в процессе обработки информации с доступом злоумышленника к элементам АСОД, но без изменения последних:

- запоминание информации на бланках с исходными данными;
- запоминание информации с устройств наглядного отображения;
- запоминание информации на выходных документах;
- запоминание служебных данных;
- копирование (фотографирование) информации в процессе обработки;
- изготовление дубликатов массивов и выходных документов;
- копирование распечатки массивов;
- использование программных ловушек;
- маскировка под зарегистрированного пользователя;
- использование недостатков систем программирования;

- использование недостатков операционных систем;
- использование пораженности программного обеспечения «вирусом».

Каналы, проявляющиеся безотносительно к обработке информации с доступом злоумышленника к элементам ЭВТ с изменением последних:

- подмена/хищение бланков;
- подмена/хищение магнитных носителей;
- подмена/хищение выходных документов;
- подмена/хищение аппаратуры;
- подмена элементов программ;
- подмена элементов баз данных;
- подмена/хищение других документов;
- включение в программы блоков типа «троянский конь», «бомба» и т. п.;
- чтение остаточной информации в ЗУ после выполнения санкционированных запросов.

Каналы, проявляющиеся в процессе обработки информации с доступом злоумышленника к объектам ЭВТ с изменением элементов ЭВТ:

- незаконное подключение к аппаратуре;
- незаконное подключение к линиям связи;
- снятие информации на шинах питания устройств отображения;
- снятие информации на шинах питания процессоров;
- снятие информации на шинах питания аппаратуры связи;
- снятие информации на шинах питания линий связи;
- снятие информации на шинах питания печатающих устройств;
- снятие информации на шинах питания внешних запоминающих устройств;
- снятие информации на шинах питания вспомогательной аппаратуры.

Под угрозой информации в АСОД понимают меру возможности возникновения на каком-либо этапе жизнедеятельности системы такого явления или события, следствием которого могут быть нежелательные воздействия на информацию: нарушение (или опасность нарушения) физической целостности, несанкционированная модификация (или угроза такой модификации) информации, несанкционированное получение (или угроза такого получения) информации, несанкционированное размно-

жение информации. Оценка угроз, естественно, должна заключаться в определении значений тех показателей, которые необходимы для решения всех задач, связанных с построением и эксплуатацией механизмов защиты информации.

Преднамеренные угрозы безопасности АСОД

Рассмотрим кратко преднамеренные угрозы безопасности АСОД. Реализация угрозы будет называться *атакой*. Классификацию угроз безопасности будем производить по следующим признакам (рис. 2.5).

По цели реализации угрозы:

- нарушение конфиденциальности информации (информация в АСОД имеет большую ценность для ее владельца). Ее несанкционированное использование другими лицами наносит значительный ущерб интересам владельца;
- нарушение целостности информации (полная или частичная дезинформация — ценная информация может быть утрачена или обесценена путем ее несанкционированного удаления или модификации). Ущерб может быть намного больше, чем при нарушении конфиденциальности;
- частичное или полное нарушение работоспособности АСОД (нарушение доступности, так как диапазон услуг, предоставляемых современными АСОД, весьма широк, отказ в обслуживании может существенно повлиять на работу пользователя).

По принципу воздействия на АСОД:

- с использованием стандартных каналов доступа субъекта системы (пользователя, процесса) к объекту (файлу данных, каналу связи и т. д.). Под доступом понимается воздействие субъекта (выполнение некоторой операции) на объект, приводящее к возникновению информационного потока от объекта к субъекту. При этом происходит взаимодействие субъекта и объекта и, следовательно, изменяется состояние объекта;
- с использованием *скрытых каналов*. Под скрытым каналом понимается путь передачи информации, позволяющий двум взаимодействующим процессам обмениваться информацией таким образом, который нарушает системную политику безопасности. При этом используются лишь побоч-

Рис. 2.5. Угрозы безопасности АСОД (начало)

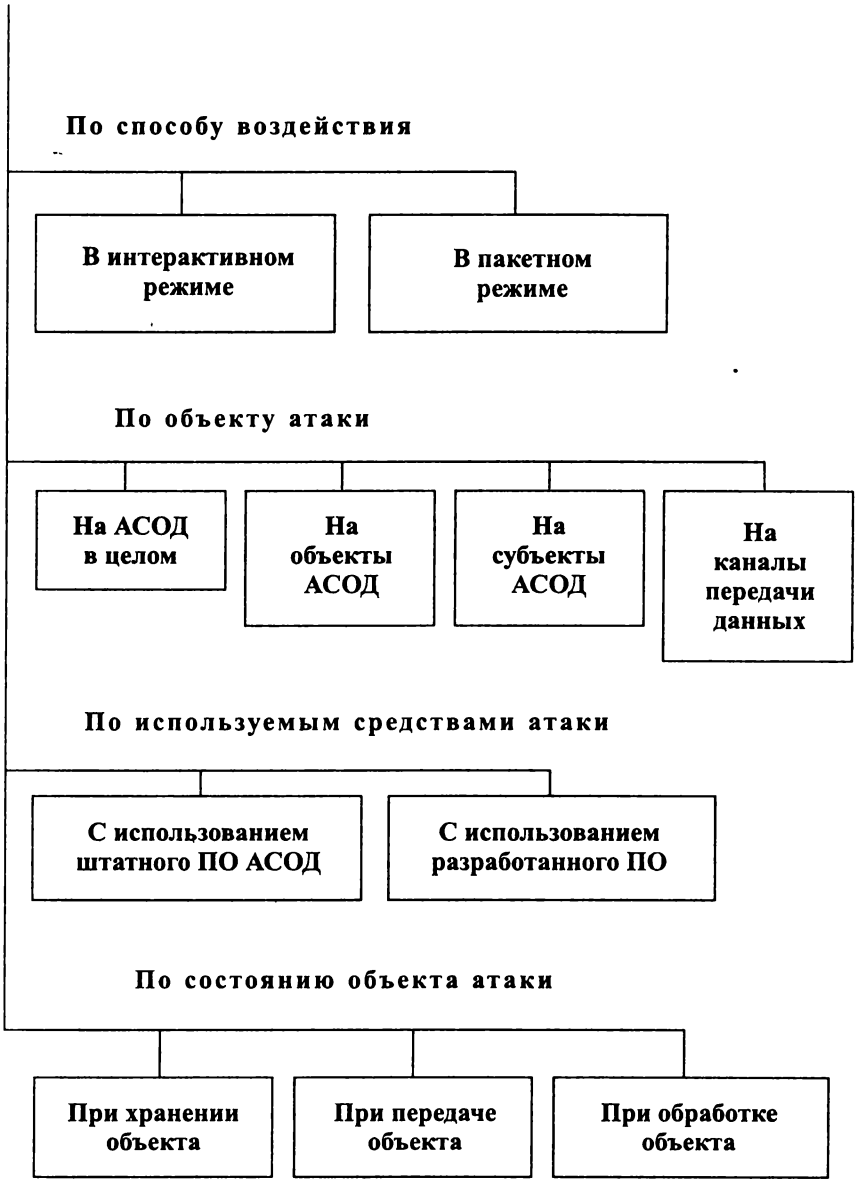


Рис. 2.5. Угрозы безопасности АСОД (окончание)

ные эффекты от взаимодействия двух субъектов, что не оказывает влияния на состояние системы. Здесь воздействие организовывать относительно трудно, принцип отличается меньшей информативностью и сложностью обнаружения и устранения. Эти каналы бывают двух типов:

— *скрытые каналы с памятью* (позволяющие произвести чтение или запись информации другого процесса непосредственно или с помощью промежуточных объектов для хранения информации — временная память);

— *скрытые временные каналы* (один процесс может получать информацию о действиях другого процесса, используя интервалы между какими-либо событиями — например, интервал времени между началом и концом процесса ввода-вывода дает информацию о размере вводимой или выводимой информации).

По характеру воздействия на АСОД:

- активное воздействие (всегда связано с выполнением пользователем каких-либо действий, выходящих за рамки его обязанностей и нарушающих существующую политику безопасности — доступ к определенным наборам данных, программам, вскрытие пароля и т. д.). В результате изменяется состояние системы (осуществляется с использованием доступа и/или с использованием доступа и скрытых каналов);
- пассивное воздействие (осуществляется путем наблюдения каких-либо побочных эффектов и их анализа — например, подслушивание линии связи между двумя узлами сети). При этом всегда нарушается только конфиденциальность информации (так как при нем никаких действий с объектами и субъектами не производится) и состояние системы не изменяется.

По причине появления используемой ошибки защиты. Реализация какой-либо угрозы становится возможной, если в системе имеется ошибка или брешь в защите. Ошибка может быть обусловлена одной из следующих причин:

- неадекватность политики безопасности реальной АСОД (разработанная для данной системы политика безопасности настолько не отражает реальные аспекты обработки информации, что становится возможным использование этого несоответствия для выполнения несанкционированных действий). Модель никогда не может точно соответст-

вовать реальной системе, но в одних случаях это не может приводить к нарушениям, а в других — может. Даже такие действия нельзя назвать несанкционированными, поскольку защита от них не предусмотрена политикой безопасности и система защиты в принципе не способна их предотвратить (необходимо разработать новую политику безопасности);

- ошибки административного управления, под которыми понимается некорректная реализация или поддержка принятой политики безопасности в данной системе (например, неправильное определение прав доступа к определенным наборам данных);
- ошибки в алгоритмах программ, в связях между ними и т. д., которые возникают на этапе проектирования программных продуктов и благодаря которым их можно использовать совсем не так, как описано в документации (например, ошибка в программе аутентификации пользователя системой дает возможность с помощью отдельных действий пользователю войти в систему без пароля);
- ошибки реализации программ (ошибки кодирования), связей между ними и т. д., которые возникают на этапе реализации или отладки. Они могут служить источником недокументированных свойств (например, люки, которые обнаружить труднее всего).

По способу активного воздействия на объект атаки:

- непосредственное воздействие на объект атаки, в том числе с использованием привилегий (например, непосредственный доступ к набору данных, программе, службе, каналу связи и т. д.), воспользовавшись какой-либо ошибкой (нужно применить контроль доступа);
- воздействие на систему разрешений, в том числе с захватом привилегий (здесь несанкционированные действия выполняются относительно прав пользователей, а сам доступ к объекту потом осуществляется законным образом — например, захват привилегий);
- опосредованное воздействие через других пользователей, в том числе:
  - — «маскарад», пользователь присваивает себе каким-либо образом полномочия другого, выдавая себя за него;
  - — «использование вслепую» (один пользователь заставляет другого выполнить необходимые действия, которые для

системы защиты не выглядят несанкционированными, — для этой угрозы может использоваться *вирус*, который выполняет необходимые действия и сообщает тому, кто его внедрил о результате). Для предотвращения подобных действий требуется постоянный контроль за работой АСОД в целом и со стороны пользователей за своими наборами данных.

По способу воздействия на АСОД:

- в интерактивном режиме (например, атака на систему с помощью интерпретатора команд — воздействие оказывается более длительным по времени и может быть обнаружено, но является более гибким);
- в пакетном режиме (например, с помощью вирусов действие является кратковременным, трудно диагностируемым, более опасным, но требует большой предварительной подготовки, так как необходимо предусмотреть все возможные последствия вмешательства).

По объекту атаки:

- АСОД в целом (для этого используются «маскарад», перехват или подделка пароля, взлом или доступ к АСОД через сеть);
- объекты АСОД (программы в оперативной памяти или на внешних носителях, сами устройства системы, каналы передачи данных и т. д. — получение доступа к содержимому носителей информации или нарушение их функциональности);
- субъекты АСОД — процессы и подпроцессы пользователей (цели: приостановка; изменение привилегий или характеристик; использование злоумышленником привилегий или характеристик и т. д.);
- каналы передачи данных — передаваемые по каналу связи пакеты данных и сами каналы (нарушение конфиденциальности, подмена или модификация сообщений, нарушение целостности информации, изменение топологии и характеристик сети, нарушение доступности сети и т. д.).

По используемым средствам атаки:

- использование стандартного программного обеспечения (ПО);
- использование специально разработанных программ (поэтому в защищенных системах рекомендуется не допускать

добавление программ в АСОД без разрешения администратора безопасности системы).

По состоянию объекта атаки:

- хранения (диск или другой вид носителя информации находится в пассивном состоянии — воздействие осуществляется с использованием доступа);
- передачи по линиям связи между узлами сети или внутри узла;
- обработки (объектом атаки является процесс пользователя).

2.3. Функции и задачи защиты информации

С целью противостояния угрозам и дестабилизирующим факторам необходимо реализовать совокупность *функций и задач* защиты информации.

Функции непосредственной защиты информации

Множество функций непосредственной защиты информации может быть представлено так:

- предупреждение возникновения условий, благоприятствующих порождению дестабилизирующих факторов;
- предупреждение непосредственного проявления дестабилизирующих факторов;
- обнаружение проявившихся дестабилизирующих факторов;
- предупреждение воздействия на информацию дестабилизирующих факторов:
  - — проявившихся и обнаруженных;
  - — проявившихся, но необнаруженных;
- обнаружение воздействия дестабилизирующих факторов на защищаемую информацию;
- локализация воздействия дестабилизирующих факторов на информацию:
  - — обнаруженного воздействия;
  - — необнаруженного;
- ликвидация последствий локализованного воздействия на информацию:
  - — обнаруженного;
  - — необнаруженного воздействия.

Общее содержание перечисленных функций в общем виде представлено ниже.

Предупреждение возникновения условий, благоприятствующих порождению (возникновению) дестабилизирующих факторов. Главной целью данной функции является способствование такому построению архитектуры АСОД, технологических схем автоматизированной обработки информации и их обеспечению, чтобы свести к минимуму саму возможность появления дестабилизирующих факторов во всех потенциально возможных условиях функционирования АСОД. Иными словами — преследуется упреждающая цель.

Предупреждение непосредственного проявления дестабилизирующих факторов в конкретных условиях функционирования АСОД. Выделением данной функции также преследуется цель упреждения возникновения дестабилизирующих факторов, однако в отличие от предыдущей функции, осуществляемой с целью общего предупреждения, мероприятия функции 2 предполагается осуществлять для предупреждения проявления дестабилизирующих факторов в конкретных условиях жизнедеятельности АСОД.

Обнаружение проявившихся дестабилизирующих факторов. Предполагается осуществление таких мероприятий, в результате которых проявившиеся дестабилизирующие факторы (или реальная угроза их проявления) будут обнаружены еще до того, как они окажут воздействие на защищаемую информацию. Иными словами, это функция непрерывного слежения за дестабилизирующими факторами.

Предупреждение воздействия дестабилизирующих факторов на защищаемую информацию. Само название функции говорит о ее содержании: мероприятия, осуществляемые в рамках данной функции, преследуют цель не допустить нежелательного воздействия дестабилизирующих факторов на защищаемую информацию даже в том случае, если они реально проявились, т. е. данная функция является естественным продолжением предыдущей. Однако осуществление предыдущей функции может быть как успешным (проявление дестабилизирующих факторов будет обнаружено), так и неуспешным (проявление дестабилизирующих факторов не будет обнаружено). С целью же создания условий для надежной защиты информации в рамках данной функции, вообще говоря, должны быть предусмотрены мероприятия по предупреждению воздействия дестабилизирующих факторов на

информацию в любых условиях. С учетом этого обстоятельства функцию предупреждения воздействия целесообразно разделить на две составные: предупреждение воздействия на информацию проявившихся и обнаруженных дестабилизирующих факторов и предупреждение воздействия на информацию проявившихся, но необнаруженных дестабилизирующих факторов.

Обнаружение воздействия дестабилизирующих факторов на защищаемую информацию. Нетрудно видеть, что основное содержание мероприятий данной функции аналогично содержанию мероприятий функции 3 с той разницей, что если функция 3 есть функция слежения за дестабилизирующими факторами, то рассматриваемая функция есть функция слежения за компонентами защищаемой информации с целью своевременного обнаружения фактов воздействия на них дестабилизирующих факторов. При этом под своевременным понимается такое обнаружение, при котором сохраняются реальные возможности локализации воздействия на информацию, т. е. предупреждения распространения его в нежелательных размерах.

Локализация воздействия дестабилизирующих факторов на информацию. Являясь логическим продолжением предыдущей, данная функция предусмотрена с целью недопущения распространения воздействия на информацию за пределы максимально допустимых размеров. Но в рамках данной функции должны быть предусмотрены мероприятия как на случай успешного осуществления функции 5 (воздействие дестабилизирующих факторов на информацию обнаружено), так и на случай неуспешного ее осуществления (указанное воздействие не обнаружено). Тогда аналогично функции 4 рассматриваемую функцию также целесообразно разделить на две составные: локализацию обнаруженного воздействия дестабилизирующих факторов на информацию и локализацию необнаруженного воздействия.

Ликвидация последствий воздействия дестабилизирующих факторов на защищаемую информацию. Под ликвидацией последствий понимается проведение таких мероприятии относительно локализованного воздействия дестабилизирующих факторов на информацию, в результате которых дальнейшая обработка информации может осуществляться без учета имевшего место воздействия. Иными словами, удается восстановить то состояние защищаемой информации, которое имело место до воздействия дестабилизирующих факторов. Совершенно очевидно, что механизмы, с помощью которых могут быть ликвидированы послед-

ствия воздействия, в общем случае будут различными для случаев локализации обнаруженного и необнаруженного воздействия. Тогда аналогично предыдущему эту функцию целесообразно представить в виде двух составных: ликвидация последствий обнаруженного и локализованного воздействия дестабилизирующих факторов на защищаемую информацию и ликвидация последствий локализованного, но необнаруженного воздействия на информацию.

Механизмы защиты

Общая классификационная структура задач включает следующие группы. *Первый вид задач* — собственно механизмы защиты.

Введение избыточности элементов системы. Под избыточностью понимается включение в состав элементов системы дополнительных компонентов сверх минимума, который необходим для выполнения ими всего множества своих функций. Избыточные элементы функционируют одновременно с основными, что позволяет создавать системы, устойчивые относительно внешних и внутренних дестабилизирующих воздействий. Различают избыточность организационную (т. е. введение дополнительной численности людей), аппаратурную (введение дополнительных технических устройств), программно-алгоритмическую (введение дополнительных алгоритмов и программ), информационную (создание дополнительных информационных массивов), временную (выделение дополнительного времени для проведения обработки информации) и т. п.

Резервирование элементов системы. Резервирование, как разновидность задач защиты информации, в некотором смысле противоположно введению избыточности: вместо введения в активную работу дополнительных элементов, наоборот, часть элементов выводится из работы и держится в резерве на случай непредвиденных ситуаций. Резервироваться могут практически все элементы АСОД, причем различают два основных вида резервирования, которые получили названия горячего и холодного. Горячим называется такое резервирование, когда выводимые в резерв элементы находятся в рабочем состоянии и способны включаться в работу сразу, т. е. без проведения дополнительных операций включения и подготовки к работе; холодным — когда резервные элементы находятся в таком состоянии, что для пере-

вода в рабочее состояние требуются дополнительные операции (процедуры).

Регулирование доступа к элементам системы. Регулирование доступа, по определению, заключается в том, что доступ на территорию (в помещение, к техническим средствам, программам, массивам (базам) данных и т. п.) будет предоставлен лишь при условии предъявления некоторой заранее обусловленной идентифицирующей информации.

Регулирование использования элементов системы. Регулирование использования, по определению, заключается в том, что осуществление запрашиваемых процедур (операций) производится лишь при условии предъявления некоторых заранее обусловленных полномочий.

Маскировка информации. Заключается в том, что защищаемые данные преобразуются или маскируются иным способом таким образом, что преобразованные данные в явном виде могут быть доступными лишь при предъявлении некоторой специальной информации, называемой ключом преобразования.

Контроль элементов системы. Данный класс задач предполагает целый ряд проверок: соответствия элементов системы заданному их составу, текущего состояния элементов системы, работоспособности элементов системы, правильности функционирования элементов системы, состояния существенно значимых параметров внешней среды и т. п.

Регистрация сведений. Под регистрацией как классом задач защиты информации понимается фиксация всех тех сведений о фактах, событиях и ситуациях, которые возникают в процессе функционирования АСОД, знание которых необходимо для эффективной защиты информации.

Уничтожение информации. Под уничтожением как классом задач защиты информации понимается осуществление процедур своевременного уничтожения (или полного вывода из системы обработки) тех элементов информации (или других компонентов системы), которые больше не нужны для функционирования АСОД и дальнейшее нахождение которых в АСОД может отрицательно сказаться на защищенности информации. Наиболее типичной процедурой данного класса является уничтожение так называемой остаточной информации, т. е. информации, остающейся на регистрах, полях оперативного ЗУ и других устройствах после решения соответствующей задачи обработки данных в АСОД. Ненужной может оказаться информация на отдельных

носителях (МЛ, МД), некоторые программные модули, контрольные распечатки, выданные документы и т. п.

Сигнализация. Одним из важнейших положений концептуального подхода к защите информации является активность защиты, что обеспечивается созданием функционально самостоятельной системы защиты и осуществлением регулярного управления ее функционированием. Во всякой же системе управления непременно должна быть обратная связь, по которой будет поступать информация (сигналы) о состоянии управляемых объектов и процессов. Процедуры генерирования, передачи и отображения (выдачи) этих сигналов и составляют содержание рассматриваемого класса задач.

Реагирование. Вторым важнейшим признаком активности системы защиты является наличие возможностей реагирования на проявление дестабилизирующих факторов с целью предотвращения или по крайней мере снижения степени воздействия их на информацию. Характерным примером такого реагирования может служить противодействие попыткам несанкционированного получения информации злоумышленником.

Управление механизмами защиты

Рассмотрим теперь общее содержание выделенных классов задач второго вида, т. е. задач управления механизмами защиты.

Планирование защиты представляет собой процесс выработки наиболее рациональной (оптимальной) программы предстоящей деятельности. В общем случае различают долгосрочное (перспективное), среднесрочное и текущее планирование.

Оперативно-диспетчерское управление защитой информации — это организованное реагирование на непредвиденные ситуации, которые возникают в процессе функционирования управляемых объектов или процессов.

Календарно-плановое руководство защитой. Основное содержание данной функции управления заключается в регулярном сборе информации о ходе выполнения планов защиты и изменении условий защиты, анализе этой информации и выработке решений о корректировке планов защиты.

Обеспечение повседневной деятельности всех подразделений и отдельных должностных лиц, имеющих непосредственное отношение к защите информации. Основными решаемыми задачами

в этом случае являются планирование, организация, оценка текущей деятельности, сбор, накопление и обработка информации, относящейся к защите, принятие текущих решений и некоторые другие. Особенно важной является задача аналитико-синтетической обработки всей накопленной информации, относящейся к защите информации.

2.4. Методы и системы защиты информации

Рассмотренные функции и задачи защиты информации определяют состав и структуру методов и систем защиты. Здесь рассматриваются основные принципы и понятия, касающиеся методов и систем защиты информации; более подробные сведения о защите информации в компьютерных сетях, персональных ЭВМ и антивирусных системах рассмотрены в главах 4, 5, 6.

Перечень основных методов защиты информации приведен на рис. 2.6, 2.7.

Одним из основных видов угроз *целостности и конфиденциальности информации*, а также работоспособности вычислительных систем являются преднамеренные угрозы, реализация кото-

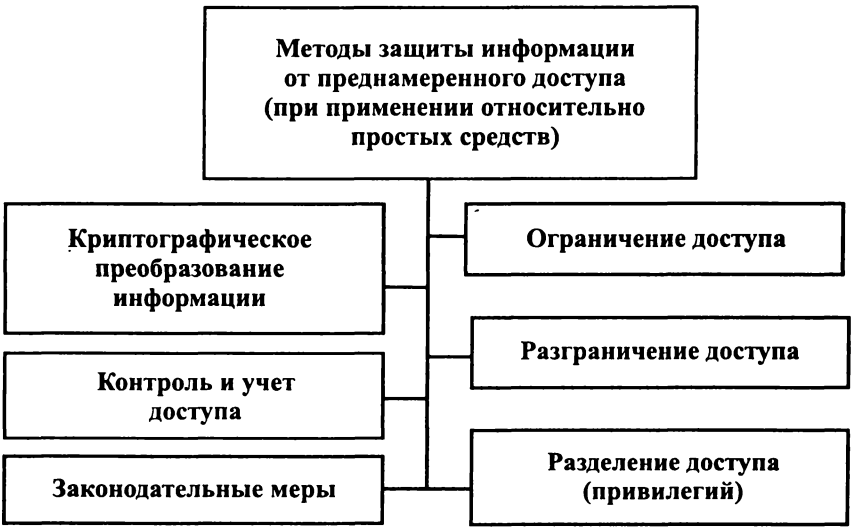


Рис. 2.6. Методы защиты информации от преднамеренного доступа (при применении простых средств хранения и обработки информации)

Рис. 2.7. Основные методы защиты информации в вычислительных системах

рых заранее планируется злоумышленником для нанесения вреда. Этот вид угроз по субъекту непосредственной реализации можно разделить на две группы [1]:

- угрозы, реализация которых выполняется при постоянном участии человека;
- угрозы, реализация которых после разработки злоумышленником соответствующих компьютерных программ выполняется этими программами без непосредственного участия человека.

Первый тип угроз называют угрозами несанкционированных действий со стороны людей, а второй — со стороны программ, созданных людьми.

Задачи по защите от реализации угроз каждого из данных типов одинаковы:

- преградить несанкционированный доступ к ресурсам вычислительных систем;
- сделать невозможным несанкционированное использование компьютерных ресурсов, если доступ к ним все-таки осуществлен;
- своевременно обнаружить факт несанкционированных действий и устранить причины, а также последствия их

реализации. Способы же решения перечисленных задач по защите от несанкционированных действий со стороны людей и компьютерных программ существенно отличаются друг от друга.

Основные функции системы защиты по преграждению несанкционированного доступа людей к ресурсам вычислительных систем заключаются прежде всего в *идентификации и подтверждении подлинности пользователей* при доступе в вычислительную систему, а также разграничении их доступа к компьютерным ресурсам.

Важную роль играет также функция *корректного завершения сеанса* работы пользователей, предотвращающая возможность реализации угрозы маскировки под санкционированного пользователя вычислительной системы. Обычное завершение сеанса работы должно обязательно проводиться каждым пользователем по окончании его работы. Принудительное же завершение сеанса работы или блокировка устройств ввода-вывода должны выполняться по истечении для пользователя заданного времени отсутствия признаков активности.

Невозможность несанкционированного использования информационных ресурсов вычислительной системы, если доступ к ним все-таки осуществлен, достигается прежде всего защитой хранящихся в памяти компьютера данных и программ от исследования и копирования.

Защита информации от исследования и копирования предполагает криптографическое закрытие защищаемых от хищения данных, выполняемое путем их зашифровки. Кроме того, должно быть предусмотрено уничтожение остаточной информации, а также аварийное уничтожение данных. *Зашифровка информации* делает невозможным ее использование без предварительного расшифровывания, осуществимого только при наличии пароля (ключа шифрования). *Уничтожение остаточных данных* в рабочих областях оперативной и внешней памяти предотвращает возможность их последующего несанкционированного использования. Аварийное уничтожение защищаемой от хищения информации необходимо при обнаружении для этой информации неотвратимой опасности несанкционированного доступа, например при возникновении отказа в системе защиты.

Защита программ от копирования предотвращает возможность выполнения несанкционированно скопированной программы на другом компьютере. *Защита программ от исследова-*

ния позволяет защитить от исследования алгоритмические и другие детали реализации программы.

Своевременное обнаружение фактов несанкционированных действий пользователей основано на выполнении таких функций, как периодический контроль целостности информации, регистрация, сигнализация, а также контроль правильности функционирования системы защиты.

Периодический контроль целостности конфиденциальной информации позволяет своевременно обнаружить попытки подлога и потери данных, а системной — внедрение программных закладок и компьютерных вирусов.

Для своевременного обнаружения фактов несанкционированных действий регистрация предполагает фиксацию и накопление сведений о всех запросах, содержащих обращения к защищаемым компьютерным ресурсам, включая доступ в вычислительную систему и завершение сеанса работы пользователей. Сигнализация в этом случае состоит в своевременном уведомлении соответствующих компонентов системы защиты и службы безопасности об обнаруженных несанкционированных действиях. Без эффективной реализации функций контроля правильности функционирования системы защиты невозможно достигнуть высокой эффективности функционирования не только подсистемы обнаружения несанкционированных действий пользователей, но и системы защиты в целом

Подтверждение подлинности пользователей и разграничение их доступа к компьютерным ресурсам

Системой защиты по отношению к любому пользователю с целью обеспечения безопасности обработки и хранения информации должны быть предусмотрены следующие этапы допуска в вычислительную систему:

1) идентификация;

2) установление подлинности (аутентификация);

3) определение полномочий для последующего контроля и разграничения доступа к компьютерным ресурсам.

Данные этапы должны выполняться и при подключении к вычислительной системе (ВС) таких устройств, как удаленные рабочие станции и терминалы.

Идентификация необходима для указания компьютерной системе уникального идентификатора обращающегося к ней пользователя с целью последующего выполнения следующих защитных функций:

- установления подлинности и определения полномочий пользователя при его допуске в компьютерную систему;
- контроля установленных полномочий и регистрации заданных действий пользователя в процессе сеанса работы после его допуска в ВС;
- учета обращений к компьютерной системе. Сам идентификатор может представлять собой последовательность любых символов и должен быть заранее зарегистрирован в системе администратором службы безопасности.

Контроль доступа к аппаратуре. Внутренний монтаж аппаратуры, технологические органы и пульты управления должны быть закрыты физически и на них установлены соответствующие датчики. При вскрытии аппаратуры оповещающие сигналы должны поступать на центральный пульт сигнализации. С позиций НСД контроль вскрытия аппаратуры срабатывает тогда, когда возникает одна из следующих ситуаций.

- изменение внутренних схем;
- подключение постороннего устройства;
- использование технологических пультов и органов управления для изменения алгоритма функционирования системы;
- загрузка посторонних программ и внесения «вирусов» в систему;
- доступ посторонних лиц к терминалам.

В процессе регистрации администратором в базу эталонных данных системы защиты для каждого пользователя заносятся следующие элементы данных:

- фамилия, имя, отчество и, при необходимости, другие характеристики пользователя;
- уникальный идентификатор пользователя;
- имя процедуры установления подлинности;
- используемая для подтверждения подлинности эталонная информация, например пароль;
- ограничения на используемую эталонную информацию, например минимальное и максимальное время, в течение которого указанный пароль будет считаться действительным;

- полномочия пользователя по доступу к компьютерным ресурсам.

Процесс установления подлинности, называемый еще *аутентификацией*, заключается в проверке, является ли пользователь, пытающийся осуществить доступ в ВС, тем, за кого он себя выдает.

Общая схема идентификации и установления подлинности пользователя при его доступе в компьютерную систему представлена на рис. 2.8.

Если в процессе аутентификации подлинность пользователя установлена, то система защиты должна определить его полно-

Рис. 2.8. Блок-схема общего алгоритма идентификации и установления подлинности пользователя

мочия по использованию ресурсов ВС для последующего контроля установленных полномочий.

Основными и наиболее часто применяемыми методами установления подлинности пользователей являются методы, основанные на использовании *паролей*. Под паролем при этом понимается некоторая последовательность символов, сохраняемая в секрете и предъявляемая при обращении к компьютерной системе. Ввод пароля, как правило, выполняют с клавиатуры.

Эффективность парольных методов может быть значительно повышена путем записи в зашифрованном виде длинных и нетривиальных паролей на информационные носители, например дискеты, магнитные карты, носители данных в микросхемах и т. д. В этом случае компьютерная система должна включать специальные устройства и обслуживающие их драйверы для считывания паролей с этих информационных носителей, а служба безопасности должна располагать средствами для формирования носителей с парольными данными.

Для особо надежного опознавания могут применяться и методы, основанные на использовании технических средств определения сугубо индивидуальных характеристик человека (голоса, отпечатков пальцев, структуры зрачка и т. д.). Однако такие средства требуют значительных затрат и поэтому используются редко.

Существующие парольные методы проверки подлинности пользователей при входе в ВС можно разделить на две группы:

- методы проверки подлинности на основе простого пароля;
- методы проверки подлинности на основе динамически изменяющегося пароля.

Пароль подтверждения подлинности пользователя при использовании простого пароля не изменяется от сеанса к сеансу в течении установленного администратором службы безопасности времени его существования (действительности).

При использовании динамически изменяющегося пароля пароль пользователя для каждого нового сеанса работы или нового периода действия одного пароля изменяется по правилам, зависящим от используемого метода.

Использование простого пароля. Процедура опознавания с использованием простого пароля может быть представлена в виде следующей последовательности действий [18]:

- пользователь посылает запрос на доступ к компьютерной системе и вводит свой идентификатор;

- система запрашивает пароль;
- пользователь вводит пароль;
- система сравнивает полученный пароль с паролем пользователя, хранящимся в базе эталонных данных системы защиты, и разрешает доступ, если пароли совпадают; в противном случае пользователь к ресурсам компьютерной системы не допускается.

Поскольку пользователь может допустить ошибку при вводе пароля, то системой должно быть предусмотрено допустимое количество повторений для ввода пароля.

В базе эталонных данных пароли, как и другую информацию, никогда не следует хранить в явной форме, а только зашифрованными. При этом можно использовать метод как обратимого, так и необратимого шифрования.

Согласно методу *обратимого шифрования* эталонный пароль при занесении в базу эталонных данных зашифровывается по ключу, совпадающему с этим эталонным паролем, а введенный после идентификации пароль пользователя для сравнения с эталонным также зашифровывается по ключу, совпадающему с этим введенным паролем. Таким образом, при сравнении эталонный и введенный пароли находятся в зашифрованном виде и будут совпадать только в том случае, если исходный введенный пароль совпадет с исходным эталонным. При несовпадении исходного введенного пароля с исходным эталонным исходный введенный пароль будет зашифрован по-другому, так как ключ шифрования отличается от ключа, которым зашифрован эталонный пароль, и после зашифровки не совпадет с зашифрованным эталонным паролем.

Для обеспечения возможности контроля правильности ввода пароля при использовании необратимого шифрования на винчестер записывается таблица преобразованных паролей. Для их преобразования используется односторонняя криптографическая функция $y = F(x)$, обладающая следующим свойством: для данного аргумента x значение $F(x)$ вычисляется легко, а по данному y вычислительно сложно найти значение аргумента x, соответствующего данному y. В таблице паролей хранятся значения односторонних функций, для которых пароли берутся в качестве аргументов. При вводе пароля система защиты легко вычисляет значение функции от пароля текущего пользователя и сравнивает со значением, приведенным в таблице для пользователя с выбранным идентификатором. Нарушитель, захвативший компью-

тер, может прочитать таблицу значений функций паролей, однако вычисление пароля практически не реализуемо.

При работе с паролями должна предусматриваться и такая мера, как недопустимость их распечатки или вывода на экраны мониторов. Поэтому система защиты должна обеспечивать ввод пользователями запрошенных у них паролей без отображения этих паролей на мониторах.

Можно выделить следующие основные способы повышения стойкости системы защиты на этапе аутентификации:

- повышение степени нетривиальности пароля;
- увеличение длины последовательности символов пароля;
- увеличение времени задержки между разрешенными попытками повторного ввода неправильно введенного пароля;
- повышение ограничений на минимальное и максимальное время действительности пароля.

Чем *нетривиальнее пароль*, тем сложнее его запомнить. Плохо запоминаемый пароль может быть записан на листе бумаги, что повышает риск его раскрытия. Выходом здесь является использование определенного числа незаписываемых на бумаге пробелов или других символов в начале, внутри, а также в конце последовательности основных символов пароля. Кроме того, отдельные символы пароля могут набираться на другом регистре (например, вместо строчных быть прописными или наоборот), что также не должно отражаться на листе бумаги. В этом случае незаконно полученный лист бумаги с основными символами пароля не будет достаточным условием раскрытия пароля целиком.

Вероятность подбора пароля уменьшается также при увеличении его длины и времени задержки между разрешенными попытками повторного ввода неправильно введенного пароля. Ожидаемое время раскрытия пароля $T_р$ (в днях) можно вычислить на основе следующей приближенной формулы:

$$T_р \approx (AS \times t_п)/2,$$

где A — число символов в алфавите, используемом для набора символов пароля;

S — длина пароля в символах, включая пробелы и другие служебные символы;

$t_п$ — время ввода пароля в секундах с учетом времени задержки между разрешенными попытками повторного ввода неправильно введенного пароля.

Например, если $A = 26$ символов (учтены только буквы английского алфавита), $t_п = 2$ с, а $S = 6$ символов, то ожидаемое время раскрытия $T_р$ приблизительно равно одному году. Если в данном примере после каждой неудачной попытки ввода пароля предусмотреть временную задержку в 10 с, то ожидаемое время раскрытия увеличится в 5 раз.

Из приведенной выше формулы становится понятно, что повышения стойкости системы защиты на этапе аутентификации можно достигнуть и увеличением числа символов алфавита, используемого для набора символов пароля. Такое увеличение можно обеспечить путем использования нескольких регистров (режимов ввода) клавиатуры для набора символов пароля, например путем использования строчных и прописных латинских символов, а также строчных и прописных символов кириллицы.

Для исключения необходимости запоминания пользователями длинных и нетривиальных паролей в системе защиты может быть предусмотрена возможность записи паролей в зашифрованном виде на информационные носители, например дискеты, магнитные карты, носители данных в микросхемах и т. д., а также считывания паролей с этих информационных носителей. Такая возможность позволяет повысить безопасность за счет значительного увеличения длины паролей, записываемых на носители информации. Однако при этом администрации службы безопасности следует приложить максимум усилий для разъяснения пользователям ВС о необходимости тщательной сохранности носителей информации с их паролями.

На степень информационной безопасности при использовании простого парольного метода проверки подлинности пользователей большое влияние оказывают *ограничения на минимальное и максимальное время действительности каждого пароля.* Чем чаще меняется пароль, тем обеспечивается большая безопасность.

Минимальное время действительности пароля задает время, в течение которого пароль менять нельзя, а максимальное — время, по истечении которого пароль будет недействительным. Соответственно, пароль должен быть заменен в промежутке между минимальным и максимальным временем его существования. Поэтому понятно, что более частая смена пароля обеспечивается при уменьшении минимального и максимального времени его действительности.

Рис. 2.9. Некоторые методы, применяемые для установления подлинности различных объектов

Минимальное и максимальное времена действительности пароля задаются для каждого пользователя администратором службы безопасности, который должен постоянно контролировать своевременность смены паролей пользователей.

Использование динамически изменяющегося пароля. Методы проверки подлинности на основе динамически изменяющегося пароля обеспечивают большую безопасность, так как частота смены паролей в них максимальна — пароль для каждого пользователя меняется ежедневно или через несколько дней. При этом каждый следующий пароль по отношению к предыдущему изменяется по правилам, зависящим от используемого метода проверки подлинности.

Существуют следующие методы парольной защиты, основанные на использовании динамически изменяющегося пароля:

- методы модификации схемы простых паролей;
- метод «запрос—ответ»;
- функциональные методы.

Наиболее эффективными из данных методов, как станет понятно далее, являются функциональные методы.

Методы модификации схемы простых паролей. К методам модификации схемы простых паролей относят случайную выборку символов пароля и одноразовое использование паролей.

При использовании первого метода каждому пользователю выделяется достаточно длинный пароль, причем каждый раз для опознавания используется не весь пароль, а только его некоторая часть. В процессе проверки подлинности система запрашивает у пользователя группу символов под заданным порядковым номерам. Количество символов и их порядковые номера для запроса определяются с помощью датчика псевдослучайных чисел.

При одноразовом использовании паролей каждому пользователю выделяется список паролей. В процессе запроса номер пароля, который необходимо ввести, выбирается последовательно по списку или по схеме случайной выборки.

Недостатком методов модификации схемы простых паролей является необходимость запоминания пользователями длинных паролей или их списков. Запись же паролей на бумагу или в записные книжки приводит к появлению риска потери или хищения носителей информации с записанными на них паролями.

Существует множество методов, применяемых для идентификации и установления подлинности различных объектов.

Методы идентификации и установления подлинности субъектов и различных объектов

При обмене информацией рекомендуется в любом случае предусмотреть взаимную проверку подлинности полномочий объекта или субъекта. Если обмен информацией производится по сети, то эта процедура должна выполняться обязательно. Для этого необходимо, чтобы каждому из объектов и субъектов присваивалось уникальное имя. Каждый из объектов (субъектов) должен хранить в своей памяти (недоступной для посторонних лиц) тот список, в котором находятся имена объектов (субъек-

тов), с которыми будут производиться процессы обмена защищаемыми данными (рис. 2.10).

Метод «запрос—ответ». При использовании метода «запрос—ответ» в ВС заблаговременно создается и особо защищается массив вопросов, включающий в себя как вопросы общего характера, так и персональные вопросы, относящиеся к конкретному пользователю, например вопросы, касающиеся известных только пользователю случаев из его жизни.

Для подтверждения подлинности пользователя система последовательно задает ему ряд случайно выбранных вопросов, на которые он должен дать ответ. Опознание считается положительным, если пользователь правильно ответил на все вопросы.

Рис. 2.10. Идентификация и установление подлинности субъекта (объекта)

Основным требованием к вопросам в данном методе аутентификации является уникальность, подразумевающая, что правильные ответы на вопросы знают только пользователи, для которых эти вопросы предназначены.

Функциональные методы. Среди функциональных методов наиболее распространенными является метод функционального преобразования пароля, а также метод «рукопожатия» [18].

Метод функционального преобразования основан на использовании некоторой функции F, которая должна удовлетворять следующим требованиям:

- для заданного числа или слова X легко вычислить $Y = F(X)$;
- зная X и Y, сложно или невозможно определить функцию $Y = F(X)$.

Необходимым условием выполнения данных требований является наличие в функции $F(X)$ динамически изменяющихся параметров, например текущих даты, времени, номера дня недели или возраста пользователя.

Пользователю сообщается:

- исходный пароль — слово или число X, например число 31;
- функция $F(X)$, например $Y = (X \bmod 100) \cdot D + W$, где $(X \bmod 100)$ — операция взятия остатка от целочисленного деления X на 100; D — текущий номер дня недели, а W — текущий номер недели в текущем месяце;
- периодичность смены пароля, например каждый день, каждые три дня или каждую неделю.

Паролями пользователя для последовательности установленных периодов действия одного пароля будут соответственно X, $F(X)$, $F(F(X))$, $F(F(F(X)))$ и т. д., т. е. для i-го периода действия одного пароля паролем пользователя будет $F^{i-1}(X)$. Поэтому для того чтобы вычислить очередной пароль по истечении периода действия используемого пароля, пользователю не нужно помнить начальный (исходный) пароль, важно лишь не забыть функцию парольного преобразования и пароль, используемый до настоящего момента времени.

С целью достижения высокого уровня безопасности функция преобразования пароля, задаваемая для каждого пользователя, должна периодически меняться, например каждый месяц. При замене функции целесообразно устанавливать и новый исходный пароль.

Согласно методу «рукопожатия» существует функция F, известная только пользователю и ВС. Данная функция должна удовлетворять тем же требованиям, которые определены для функции, используемой в методе функционального преобразования.

При входе пользователя в ВС системой защиты генерируется случайное число или случайная последовательность символов X и вычисляется функция $F(X)$, заданная для данного пользователя.

Далее X выводится пользователю, который должен вычислить $F'(X)$ и ввести полученное значение в систему. Значения $F(X)$ и $F'(X)$ сравниваются системой и если они совпадают, то пользователь получает доступ в ВС.

Например, в ВС генерируется и выдается пользователю случайное число, состоящее из семи цифр. Для дезориентации злоумышленника в любое место числа может быть вставлена десятичная точка. В качестве функции F принимается: Y = (<сумма 1-й, 2-й и 5-й цифр числа>)^2 – <сумма 3-й, 4-й, 6-й и 7-й цифр числа> + <сумма цифр текущего времени в часах>.

Для высокой безопасности функцию «рукопожатий» целесообразно циклически менять через определенные интервалы времени, например устанавливать разные функции для четных и нечетных чисел месяца.

Достоинством метода «рукопожатия» является то, что никакой конфиденциальной информации между пользователем и ВС не передается. По этой причине эффективность данного метода особенно велика при его применении в вычислительных сетях для подтверждения подлинности пользователей, пытающихся осуществить доступ к серверам или центральным ЭВМ.

В некоторых случаях может оказаться необходимым пользователю проверить подлинность той ВС, к которой он хочет осуществить доступ. Необходимость во взаимной проверке может понадобиться и когда два пользователя ВС хотят связаться друг с другом по линии связи. Методы простых паролей, а также методы модификации схем простых паролей в этом случае не подходят. Наиболее подходящим здесь является метод «рукопожатия». При его использовании ни один из участников сеанса связи не будет получать никакой секретной информации.

Идентификация и установление подлинности технических средств. Здесь широко используются пароли как для идентификации и установления подлинности терминала (с которого поль-

зователь входит в систему), так и для обратного установления подлинности ЭВМ по отношению к пользователю.

Идентификация и установление подлинности документов. Подлинность документов необходимо рассматривать со следующих позиций:

- документ сформирован непосредственно на этой ВС (на ее аппаратуре документирования);
- документ получен с удаленных объектов.

В первом случае подлинность документа гарантируется средствами защиты информации от НСД и применением криптографического преобразования информации. Информация закрывается кодом пароля (он известен передающему лицу и получателю).

Во втором случае также широко используются методы криптографического преобразования информации (если документы относительно долго хранились в памяти ВС или же транспортировались по неохраняемой территории).

Идентификация и установление подлинности информации на средствах ее отображения и печати. Методы определения подлинности информации на средствах ее отображения тесно связаны с методами определения подлинности документов, которые являются носителями соответствующей информации. Поэтому все соображения по отношению к методам определения подлинности документов также относятся и к методам установления подлинности информации, содержащейся на средствах ее отображения. Здесь также широко используются различные методы криптографического преобразования информации.

Своевременное обнаружение несанкционированных действий пользователей. Своевременное обнаружение фактов несанкционированных действий пользователей основано на выполнении следующих функций:

- периодический контроль целостности информации;
- регистрация и сигнализация;
- контроль правильности функционирования системы защиты.

Периодический контроль целостности конфиденциальной информации позволяет своевременно обнаружить попытки подлога и потери данных, а системной — внедрение программных закладок и компьютерных вирусов.

Регистрация для своевременного обнаружения фактов несанкционированных действий пользователей предполагает фик-

сацию и накопление сведений о всех запросах, содержащих обращения к защищаемым компьютерным ресурсам, включая доступ в вычислительную систему и завершение сеанса работы пользователей. Сигнализация же в этом случае состоит в своевременном уведомлении соответствующих компонентов системы защиты и администрации об обнаруженных несанкционированных действиях.

Без эффективной реализации функций контроля правильности функционирования системы защиты невозможно достигнуть высокой эффективности функционирования не только подсистемы обнаружения несанкционированных действий пользователей, но и системы защиты в целом.

Общие сведения о контроле информационной целостности

Под контролем целостности данных, хранимых в вычислительной системе или передаваемых по каналам связи, понимается обнаружение их любых случайных или несанкционированных изменений.

Периодическому контролю на целостность должна подвергаться вся конфиденциальная и системная информация, хранящаяся в вычислительной системе.

Периодичность контроля целостности хранящейся в вычислительной системе конфиденциальной и системной информации не должна быть реже ежедневной. Поэтому программы контроля информационной целостности целесообразно активизировать в процессе загрузки операционной системы.

Передаваемая по каналам связи информация должна подвергаться контролю на целостность после каждого приема этой информации получателем.

Контроль информационной целостности реализуется на основе предварительного определения характеристики целостной (эталонной) информации, называемой эталонной характеристикой или эталонным кодом обнаружения модификаций. Для высокой эффективности использования эта эталонная характеристика должна быть по объему значительно меньше контролируемой информации и ее значение должно зависеть от содержимого и очередности всех двоичных блоков защищаемых от модификации данных. В зарубежной литературе эталонную характеристи-

ку обнаружения модификаций называют MAC-кодом (message authentication code).

В процессе непосредственного контроля информационной целостности выполняются следующие действия:

- для контролируемой информации определяется текущая характеристика обнаружения модификаций по тому же способу, по которому формировалась эталонная характеристика;
- текущая и эталонная характеристики обнаружения модификаций сравниваются и если они совпадают, то считается, что контролируемая на целостность информация не подвергалась изменению.

Для объективности заключения об информационной целостности по совпадению текущей и эталонной характеристик обнаружения модификаций необходимо, чтобы метод, используемый для формирования этих характеристик, обеспечивал чрезвычайно малую вероятность изменения данных, при которых их текущая и эталонная характеристики совпадают.

Эталонная характеристика обнаружения модификаций должна храниться или передаваться вместе с контролируемыми на целостность данными, для которых эта характеристика сформирована.

Способы определения модификаций информации.

Определение случайных модификаций. Для определения случайных модификаций информации ее эталонная характеристика может быть открытой для доступа. В этом случае формирование характеристики обнаружения модификаций может осуществляться в соответствии со схемой последовательного контрольного суммирования по операции исключающего ИЛИ (XOR) двоичных блоков, составляющих контролируемую на целостность информацию.

Определение преднамеренных модификаций. Для определения не только случайных, но и преднамеренных модификаций информации ее эталонная характеристика должна защищаться криптографическими методами или формироваться на основе криптографических преобразований. Рассмотрим два наиболее часто используемых метода формирования характеристики обнаружения модификаций на основе криптографических преобразований:

- метод шифрования в режиме объединения;
- метод вычисления хэш-функции.

При доступе к зашифрованному информационному объекту выполняются следующие действия:

1) после ввода ключа этот объект расшифровывается;

2) для определения его целостности вычисляется по описанному способу текущая характеристика обнаружения модификаций;

3) полученная текущая характеристика обнаружения модификаций сравнивается с эталонной, хранящейся вместе с зашифрованным информационным объектом, и при их совпадении выдается сообщение, что контролируемая на целостность информация не подвергалась изменению.

После расшифровывания информационного объекта при непосредственном контроле информационной целостности вычисленное текущее значение хэш-функции сравнивается с эталонным, хранящимся вместе с зашифрованными данными.

Стойкость данной схемы основана на стойкости блочного шифра, для которого по известным входному и выходному сообщениям нельзя вычислить ключ. Если бы ключ можно было бы вычислить, то хэш-функция не обладала бы необходимой стойкостью, т. е. допускала бы модифицирование информации без изменения значения хэш-функции.

Практическая реализация контроля целостности. Подсистема контроля информационной целостности является неотъемлемым компонентом любой специализированной системы защиты информации. Данная подсистема должна обеспечивать периодический контроль целостности не только конфиденциальных данных, но и всей системной информации, задающей требуемые режимы и параметры функционирования компьютера. Это позволяет своевременно обнаруживать как попытки подлога и потери конфиденциальной информации, так и внедрение несанкционированных программ (программных закладок и компьютерных вирусов).

Таким образом, функции по контролю информационной целостности наряду с проверкой целостности конфиденциальной информации обеспечивают своевременное обнаружение отклонений текущего состояния рабочей среды компьютера от эталонного. По этой причине подсистему контроля информационной целостности часто называют подсистемой обеспечения эталонного состояния рабочей среды вычислительной системы.

Наиболее надежные системы защиты, например, система «Кобра», обеспечивают не только своевременное обнаружение

отклонений текущего состояния рабочей среды компьютера от эталонного, но и автоматическое восстановление ее основных компонентов (содержимого CMOS-памяти, главной загрузочной записи винчестера, включая его таблицу разделов, загрузчика ОС, файлов CONFIG.SYS, AUTOEXEC.BAT и т. д.).

Для контроля информационной целостности также можно использовать антивирусные программы, называемые «ревизорами». Однако перед выбором ревизора следует выяснить, обеспечивает ли он выполнение функций по контролю целостности файлов данных, так как основное назначение ревизоров — контроль целостности программ.

Организация контроля. При установке и использовании программных средств контроля информационной целостности должны быть выполнены следующие этапы:

1. Проведены тщательный анализ всех файлов конфигурирования и настройка на отсутствие вызовов несанкционированных программ. При обнаружении такие вызовы следует удалить, а также установить и устранить причину их появления.

2. Проведен тщательный анализ вычислительной системы на наличие вирусов и осуществлено полное обезвреживание обнаруженных вирусных программ с помощью обновленной версии транзитного сканера. Для большей эффективности процессов поиска и обезвреживания вирусов целесообразно независимое применение нескольких различных сканеров.

3. Установлены требуемые режимы и параметры рабочей среды компьютера.

4. Сформированы с помощью специализированной программы, например ревизора, следующие эталонные характеристики рабочей среды компьютера:

- содержимое загрузочных секторов жестких дисков;
- содержимое CMOS-памяти;
- контрольные суммы содержимого файлов конфигурирования и настройки, например файлов AUTOEXEC.BAT, CONFIG.SYS, MNI для MS-DOS/Windows 3.XX, а также SYSTEM.DAT и USER.DAT для Windows;
- контрольные суммы или описания структуры содержимого оперативной памяти компьютера;
- информация о количестве и расположении сбойных кластеров жестких дисков (некоторые вирусы размещают свои тела в свободных кластерах, помечаемых затем этими вирусами как сбойные);

- контрольные суммы содержимого файлов с программами, а также их системные характеристики: пути, даты и времена создания, длины, значения атрибутов, а при необходимости, и адреса физического расположения;
- контрольные суммы и системные характеристики файлов с конфиденциальными данными.

5. Осуществлялась периодическая проверка специализированной программой, например ревизором, соответствия реальных характеристик элементов компьютерной системы их эталонным характеристикам, которые эти элементы имели при целостном (эталонном) состоянии. В зависимости от возможностей специализированной программы контроля могут использоваться следующие виды периодических проверок:

- строго периодическая, например ежедневная, при которой проверяются все элементы компьютера, для которых созданы эталонные характеристики;
- в режиме реального времени, при которой осуществляется проверка контролируемых элементов только при попытке их использования, например при попытке запуска программ и открытия документов.

При обновлении контролируемых на целостность информационных объектов, например при изменении файлов конфигурирования и настройки, должны быть изменены и их эталонные характеристики.

Для файлов с конфиденциальными данными эталонные характеристики следует формировать после каждого обновления или создания этих файлов. Для высокой безопасности непосредственный контроль целостности файлов с информацией повышенного уровня секретности целесообразно выполнять не только ежедневно, но и перед доступом к этим файлам.

В случае обнаружения несоответствия реальных характеристик эталонным перед принятием мер необходимо выяснить причину этого несоответствия. Возможны следующие причины:

- после обновления элементов, для которых формировались эталонные характеристики, не была обновлена эталонная информация;
- произошло повреждение контролируемых элементов данных из-за сбоев или отказов программно-аппаратных средств;
- произошла несанкционированная модификация информационных файлов;
- произошло заражение программ компьютерным вирусом.

Особенности использования программ непосредственного контроля. Программы, предназначенные для непосредственного контроля соответствия текущих характеристик элементов данных их эталонным характеристикам могут функционировать транзитно и резидентно.

Транзитные программы контроля загружаются в оперативную память только для выполнения проверок. Резидентные же программы после запуска остаются в оперативной памяти и проверяют контролируемые элементы компьютера при возникновении с ними определенных событий (открытие документов, запуск и модификация программ, копирование, создание, переименование файлов и т. д.). Наибольшая результативность контроля информационной целостности достигается при совместном использовании транзитного и резидентного средства, когда осуществляется не только строго периодическая, например ежедневная проверка, но и динамический контроль элементов данных на соответствие эталонным характеристикам. При этом следует учитывать, что использование резидентной программы контроля приводит к снижению быстродействия функционирования компьютера.

Для транзитной программы контроля должны быть предусмотрены следующие режимы работы:

- первый запуск для формирования эталонных характеристик подлежащих контролю информационных объектов компьютера после поиска и обезвреживания вирусов транзитным сканером и тщательной проверки файлов конфигурирования на отсутствие вызовов программных закладок;
- ежедневный запуск в процессе загрузки операционной системы для проверки всех контролируемых информационных объектов (в оперативной памяти, а также на всех логических дисках) и по мере необходимости для формирования эталонных характеристик созданных или обновленных файлов с конфиденциальной и системной информацией;
- запуск по мере необходимости для формирования эталонных характеристик программ, поступающих извне, после проверки их транзитным сканером.

Для активизации строго периодического запуска транзитной программы контроля может использоваться резидентная программа-планировщик.

Запуск резидентной программы контроля для ее постоянного нахождения в оперативной памяти должен осуществляться в процессе загрузки операционной системы.

Недостатком программ контроля информационной целостности является настойчивость и требовательность по отношению к пользователям, так как пользователями или администраторами не всегда вовремя обновляются эталонные данные. Но этот недостаток с лихвой компенсируется значительным повышением степени защищенности от подлога и потери данных, а также внедрением программных закладок и компьютерных вирусов.

Регистрация действий пользователей. Подсистема регистрации представляет собой совокупность средств, используемых для регулярного сбора, фиксации и выдачи по запросам сведений о всех обращениях к защищаемым компьютерным ресурсам, а также доступе в вычислительную систему и выходе из нее.

Для защиты от сбоев и отказов регистрируются также сведения о всех действиях пользователей и программ по модификации данных на внешних информационных носителях.

Основной формой регистрации является программное ведение специальных регистрационных журналов, представляющих собой файлы на внешних носителях информации.

При регистрации сведений по обращению к вычислительной системе и ее ресурсам рекомендуется фиксировать:

- время поступления запроса;
- идентификатор пользователя, от имени которого выдан запрос;
- идентификатор компьютера (терминала), с которого поступил запрос;
- содержание сообщения в составе запроса;
- реквизиты защиты (полномочия пользователей, пароли, коды, ключи и др.), используемые при выполнении запроса;
- время окончания использования ресурса.

Имея такие сведения, в любой момент можно получить статистические данные относительно компьютеров (терминалов), пользователей и программ, запрашивающих доступ, а также сведения о результатах выполнения запросов и характере использования запрашиваемых ресурсов.

При регистрации всех действий пользователей и программ по модификации данных на внешних информационных носителях следует фиксировать все изменения как системной, так и несистемной информации между непротиворечивыми состояниями файловой структуры и содержимого файлов. Это обеспечивает поддержание логической целостности данных на основе возможности их восстановления при возникновении сбоев и от-

казов программно-аппаратных средств вычислительной системы. Например, если при перемещении файла отказ произойдет между стадиями обновления информации в системной области и области данных диска, то возникшее противоречивое состояние файловой структуры без зарегистрированной информации по модификации данных можно будет устранить только отменой сделанных действий, что не позволит полностью восстановить перемещаемый файл.

Регистрационные журналы способствуют решению следующих задач:

- регулирования использования средств защиты в процессе функционирования вычислительной системы;
- фиксации всех нарушений правил обращения к защищаемым ресурсам;
- наблюдения за использованием реквизитов защиты (полномочий пользователей, паролей, ключей и т. д.);
- восстановления информации и работоспособности вычислительной системы после возникновения сбоев и отказов программно-аппаратных средств;
- анализа процесса поддержания безопасности информации и процесса ее обработки с целью совершенствования системы защиты;
- настройки компонентов системы защиты и других компонентов вычислительной системы, особенно библиотек программ и элементов баз данных в соответствии с частотой их использования. Сам факт ведения регистрационных журналов в вычислительной системе оказывает психологическое воздействие на потенциальных нарушителей, удерживая их от злоумышленных действий.

В общем случае подсистема сигнализации предназначена для выполнения следующих функций:

- своевременного уведомления специалистов службы безопасности вычислительной системы (ВС) о несанкционированных действиях пользователей и программ, нарушении работоспособности системы защиты, а также возникновении сбоев и отказов в работе программно-аппаратных средств;
- предупреждения пользователей ВС о необходимости соблюдения предосторожностей при работе с секретными данными.

Первый вид сигнализации осуществляется путем формирования и выдачи службе безопасности ВС специальных сигналов при обнаружении несанкционированных действий пользователей и программ, нарушении работоспособности системы защиты, а также возникновении сбоев и отказов в работе программно-аппаратных средств. Содержание такого сигнала должно включать:

- информацию о самом факте наступления соответствующего события;
- сообщение о месте, времени и характере события;
- информацию о пользователях, программах или устройствах, связанных с возникновением отслеживаемого события.

Сообщение сигнала, выводимое на печать или экран терминала, должно программно регистрироваться в специальном журнале учета и может сопровождаться звуковым и световым сопровождением.

Для пресечения злоумышленных действий важное значение имеет выигрыш во времени, необходимый для принятия соответствующих мер.

В то же время злоумышленник может почувствовать, что его несанкционированные действия обнаружены, и, прекратив эти действия, попытаться их скрыть. Если же в целях конспирации принимаемых мер не реагировать на злоумышленные действия, то может произойти утечка информации или злоумышленник попытается нарушить работоспособность системы.

В качестве выхода из такой ситуации предлагается создавать специальные программы, осуществляющие имитацию нормальной работы с нарушителем, предоставляя этим самым необходимое время для его задержания. В процессе имитации могут выполняться следующие действия:

- увеличение количества вопросов, задаваемых подозреваемому в диалоговом режиме при выполнении запроса;
- искусственная задержка времени перед каждым вопросом, задаваемым подозреваемому;
- указания повторить запуск, мотивируя это тем, что произошел программно-аппаратный сбой;
- выдача подозреваемому сообщения о том, что его запрос принят и поставлен в очередь.

Основными требованиями к таким программам имитации являются обеспечение требуемого времени работы с нарушителем, закрытие доступа к секретным сведениям закрытия и средствам поддержания работоспособности ВС, а также естествен-

ность. Последнее требование предполагает, что все задаваемые подозреваемому вопросы должны быть естественными и обычными в практике работы данной ВС.

Предупреждение пользователей о необходимости соблюдать предосторожности при работе с секретными данными осуществляется путем автоматического формирования и присвоения специального признака (грифа секретности) всем выдаваемым на печать или устройства отображения страницам документов (форм), содержащих защищаемую информацию. При этом, если в защищаемом документе (форме) используется несколько элементов данных с разными уровнями секретности, то гриф секретности документа (формы) определяется по максимальному уровню.

Важную роль играет также сигнализация, проводимая с помощью пользователей вычислительной системы. Для реализации данной сигнализации необходимо сообщение каждому пользователю после успешного подтверждения его подлинности при входе в компьютерную систему следующих сведений:

- даты и времени начала и окончания его последнего сеанса работы;
- количества неуспешных попыток установления сеанса работы при регистрации с его идентификатором со времени окончания его последнего сеанса работы, а также даты и времени совершения каждой из этих попыток.

Сведения о последнем сеансе работы, который пользователь не проводил, позволяют установить факт имевшего место несанкционированного сеанса работы, в процессе которого злоумышленник, узнав или подобрав пароль, маскировался под данного пользователя. В этом случае пользователю необходимо немедленно сообщить об этом факте службе безопасности, сменить пароль, а также выяснить и по возможности устранить причины и последствия случившегося несанкционированного действия.

Сведения об имевших место неуспешных попытках установления сеанса работы при регистрации с идентификатором пользователя со времени окончания его последнего сеанса работы дают возможность своевременно узнать о том, что кто-то пытается осуществить несанкционированный доступ, маскируясь под данного пользователя. В этом случае пользователю также следует сообщить об обнаруженных попытках несанкционированных действий службе безопасности и при необходимости принять меры для усиления защиты.

Контроль правильности функционирования системы защиты

Независимо от мощности системы защиты невозможно достигнуть своевременного обнаружения несанкционированных действий пользователей и высокой информационной безопасности в целом без эффективной реализации функций контроля правильности работы защитных подсистем.

Для комплексного контроля правильности функционирования системы защиты должна быть предусмотрена реализация следующих базовых функций:

- периодического контроля правильности функционирования защитных подсистем;
- контроля корректности модификации параметров настроек системы защиты;
- постоянной регистрации данных о функционировании системы защиты и их анализа;
- уведомления ответственных лиц при нарушении правильности работы защитных средств.

Периодический контроль правильности функционирования защитных подсистем предполагает периодическое выполнение следующих действий:

- проверки наличия требуемых резидентных компонентов системы защиты в оперативной памяти компьютера;
- контроля всех программ системы защиты, находящихся во внешней и оперативной памяти, на соответствие эталонным характеристикам (контрольным суммам);
- проверки корректности параметров настройки функционирования системы защиты, располагаемых как в оперативной, так и во внешней памяти;
- контроля корректности эталонной информации (идентификаторов, паролей, ключей шифрования и т. д.).

При проверке корректности модификации параметров настроек системы защиты подсистема контроля не должна допустить установку параметров, противоречащих политике безопасности, принятой в организации.

Регистрация данных о функционировании системы защиты предполагает фиксацию и накопление информации о следующих действиях:

- действиях всех подсистем защиты;
- действиях всех администраторов и пользователей других категорий по использованию защитных средств.

Кроме регистрации данных о функционировании системы защиты, должен быть обеспечен и периодический анализ накопленной информации. Основной задачей такого анализа является своевременное определение недопустимых действий, а также прогнозирование степени безопасности информации и процесса ее обработки в вычислительной системе.

Для возможности и результативности периодического анализа предварительно должны быть определены принципы, описывающие политику работы системы защиты:

- в работе системы защиты допустимо все, что не запрещено;
- в работе системы защиты запрещено все, что явно недопустимо.

Более высокий уровень контроля и безопасности обеспечивает второй принцип, так как на практике не всегда удается полностью учесть все действия, которые запрещены. Надежнее определить все действия, которые разрешены, и запретить все остальные.

При обнаружении подсистемой контроля любых нарушений в правильности функционирования подсистемы защиты должно быть выполнено немедленное уведомление соответствующей службы безопасности.

Только системный подход к организации и реализации контроля правильности функционирования всех защитных средств позволит достигнуть уровня безопасности, на который ориентирована используемая система защиты информации.

Контрольные вопросы

1. В чем состоит предмет и объекты защиты информации в автоматизированных системах обработки данных (АСОД)?
2. Что такое надежность информации?
3. В чем заключается уязвимость информации?
4. Что представляют собой элементы и объекты защиты в АСОД?
5. Дайте определение и перечислите основные дестабилизирующие факторы АСОД.
6. Каковы причины нарушения целостности информации? Сгруппируйте их.
7. Перечислите каналы несанкционированного получения информации в АСОД.
8. Назовите преднамеренные угрозы безопасности АСОД.
9. В чем состоят функции непосредственной защиты информации?

10. Назовите основные задачи защиты информации.
11. Каковы методы подтверждения подлинности пользователей и разграничения их доступа к компьютерным ресурсам? Назовите цели и методы контроля доступа к аппаратуре.
12. Какие разновидности методов использования паролей вам известны?
13. Перечислите методы идентификации и установления подлинности субъектов и различных объектов.
14. Каковы методы своевременного обнаружения несанкционированных действий пользователей?
15. В чем состоят задачи контроля информационной целостности?
16. Перечислите способы определения модификаций информации.
17. Назовите методы регистрации действий пользователей.
18. Перечислите цели и задачи контроля правильности функционирования системы защиты.
19. Каковы методы защиты информации от преднамеренного доступа при использовании простых средств хранения и обработки информации?
20. Что значит разграничение и контроль доступа к информации?
21. Объясните сущность метода разделения привилегий доступа.
22. Из чего состоит комплекс средств автоматизации и как организуется его обслуживание?
23. Что понимается под идентификацией и установлением подлинности субъекта (объекта)?
24. В чем заключается суть идентификации и установления подлинности технических средств?
25. В чем суть идентификации и установления подлинности документов?
26. В чем заключается суть идентификации и установления подлинности информации на средствах отображения и печати?
27. Объясните суть комплексного подхода к организации систем защиты.
28. Какие имеются методы и средства защиты информации от случайных воздействий?
29. Какие методы функционального контроля вычислительных систем вы знаете?

Глава 3
КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом, волновала человеческий ум с давних времен. История криптографии — ровесница истории человеческого языка. Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные. Священные книги Древнего Египта, Древней Индии тому примеры.

Криптографическое закрытие является специфическим способом защиты информации, оно имеет многовековую историю развития и применения. Поэтому у специалистов не возникало сомнений в том, что эти средства могут эффективно использоваться также и для защиты информации в АСОД, вследствие этого им уделялось и продолжает уделяться большое внимание. Достаточно сказать, что в США еще в 1978 г. утвержден и рекомендован для широкого применения национальный стандарт (DES) криптографического закрытия информации. Подобный стандарт в 1989 г. (ГОСТ 28147—89) утвержден и у нас в стране. Интенсивно ведутся исследования с целью разработки высокостойких и гибких методов криптографического закрытия информации. Более того, сформировалось самостоятельное научное направление — криптология, изучающая и разрабатывающая научно-методологические основы, способы, методы и средства криптографического преобразования информации.

3.1. Криптология и основные этапы ее развития

Можно выделить следующие три периода развития криптологии [9, 11]. Первый период — эра донаучной криптологии, являвшейся ремеслом — уделом узкого круга искусных умельцев. На-

чалом второго периода можно считать 1949 г., когда появилась работа К. Шеннона «Теория связи в секретных системах», в которой проведено фундаментальное научное исследование шифров и важнейших вопросов их стойкости. Благодаря этому труду криптология оформилась как прикладная математическая дисциплина. И наконец, начало третьему периоду было положено появлением в 1976 г. работы У. Диффи, М. Хеллмана «Новые направления в криптографии», в которой было показано, что секретная связь возможна без предварительной передачи секретного ключа. Так началось и продолжается до настоящего времени развитие наряду с обычной классической криптографией и криптографии с открытым ключом.

Еще несколько веков назад само применение письменности можно было рассматривать как способ закрытия информации, так как владение письменностью было уделом немногих.

XX в. до н. э. При раскопках в Месопотамии был найден один из самых древних шифротекстов. Он был написан клинописью на глиняной табличке и содержал рецепт глазури для покрытия гончарных изделий, что, по-видимому, было коммерческой тайной. Известны древнеегипетские религиозные тексты и медицинские рецепты.

Середина IX в. до н. э. Именно в это время, как сообщает Плутарх, использовалось шифрующее устройство — скиталь, которое реализовывало так называемый шифр перестановки. При шифровании слова писались на узкую ленту, намотанную на цилиндр, вдоль образующей этого цилиндра (скиталя). После этого лента разматывалась и на ней оставались переставленные буквы открытого текста. Неизвестным параметром-ключом в данном случае служил диаметр этого цилиндра. Известен и метод дешифрования такого шифротекста, предложенный Аристотелем, который наматывал ленту на конус, и то место, где появлялось читаемое слово или его часть, определяло неизвестный диаметр цилиндра.

56 г. н. э. Во время войны с галлами Ю. Цезарь использует другую разновидность шифра — шифр замены. Под алфавитом открытого текста писался тот же алфавит со сдвигом (у Цезаря на три позиции) по циклу. При шифровании буквы открытого текста у верхнего алфавита заменялись на буквы нижнего алфавита. Хотя этот шифр был известен до Ю. Цезаря, тем не менее он был назван его именем.

Другим более сложным шифром замены является греческий шифр — квадрат Полибия. Алфавит записывается в виде квадратной таблицы. При шифровании буквы открытого текста заменялись на пару чисел — номера столбца и строки этой буквы в таблице. При произвольном расписывании алфавита по таблице и шифровании такой таблицей короткого сообщения этот шифр является стойким даже по современным понятиям. Идея была реализована в более сложных шифрах, применявшихся во время Первой мировой войны.

Крах Римской империи в V в. н. э. сопровождался закатом искусства и наук, в том числе и криптографии. Церковь в те времена преследовала тайнопись, которую она считала чернокнижием и колдовством. Сокрытие мыслей за шифрами не позволяло церкви контролировать эти мысли.

Р. Бэкон (1214—1294) — францисканский монах и философ — описал семь систем секретного письма. Большинство шифров в те времена применялись для закрытия научных записей.

Вторая половина XV в. Леон Баттиста Альберта, архитектор и математик, работал в Ватикане, автор книги о шифрах, где описал шифр замены на основе двух концентрических кругов, по периферии которых были нанесены на одном круге — алфавит открытого текста, а на другом — алфавит шифротекста. Важно, что шифроалфавит был непоследовательным и мог быть смещен на любое количество шагов. Именно Альберта впервые применил для дешифрования свойство неравномерности встречаемости различных букв в языке. Он впервые также предложил для повышения стойкости применять повторное шифрование с помощью разных шифросистем.

Известен факт, когда король Франции Франциск I в 1546 г. издал указ, запрещающий подданным использование шифров. Хотя шифры того времени были исключительно простыми, они считались нераскрываемыми.

Иоганн Тритемий (1462—1516) — монах-бенедиктинец, живший в Германии. Написал один из первых учебников по криптографии. Предложил оригинальный шифр многозначной замены под названием «Ave Maria». Каждая буква открытого текста имела не одну замену, а несколько, по выбору шифровальщика. Причем буквы заменялись буквами или словами так, что получался некоторый псевдооткрытый текст, тем самым скрывался сам факт передачи секретного сообщения. Разновидность шифра

многозначной замены применяется до сих пор, например в архиваторе ARJ.

Джироламо Кардано (1506—1576) — итальянский математик, механик, врач — изобрел систему шифрования, так называемую решетку Кардано, на основе которой, например, был создан один из наиболее стойких военно-морских шифров Великобритании во время Второй мировой войны. В куске картона с размеченной решеткой определенным образом прорезались отверстия, нумерованные в произвольном порядке. Чтобы получить шифротекст, нужно положить этот кусок картона на бумагу и начинать вписывать в отверстия буквы в выбранном порядке. Затем после поворота решетки на 90° процедура повторялась. Скрытие легко достигается, если эти промежутки достаточно велики, а слова языка имеют небольшую длину, как, например, в английском языке. Решетка Кардано — это пример шифра перестановки.

XVI в. Шифры замены получили развитие в работах итальянца Джованни Батиста Порты (математик) и француза Блеза де Вижинера (дипломат).

Система Вижинера в том или ином виде используется до настоящего времени, поэтому ниже она будет рассмотрена достаточно детально.

XVII в. Кардинал Ришелье (министр при короле Франции Людовике XIII) создал первую в мире шифрслужбу.

Лорд Френсис Бэкон (1562—1626) был первым, кто обозначил буквы 5-значным двоичным кодом: A = 00001, B = 00010, ... и т. д. Правда, Бэкон никак не обрабатывал этот код, поэтому такое закрытие было совсем нестойким. Просто интересно, что через три века этот принцип был положен в основу электрической и электронной связи. Тут уместно вспомнить коды Морзе, Бодо, международный телеграфный код № 2 (МККТТ-2), код ASCII, также представляющие собой простую замену.

В XVII же веке были изобретены так называемые словарные шифры. При шифровании буквы открытого текста обозначались двумя числами — номером строки и номером буквы в строке на определенной странице какой-нибудь выбранной распространенной книги. Эта система является довольно стойкой, но неудобной. К тому же книга может попасть в руки противника.

К. Гаусс (1777—1855) — великий математик, тоже не обошел своим вниманием криптологию. Он создал шифр, который ошибочно считал нераскрываемым. При его создании использовался

интересный прием — рандомизация (от *random* — случайный) открытого текста. Открытый текст можно преобразовать в другой текст, содержащий символы большего алфавита, путем замены часто встречающихся букв случайными символами из соответствующих определенных им групп. В получающемся тексте все символы большого алфавита встречаются с примерно одинаковой частотой. Зашифрованный таким образом текст противостоит методам раскрытия на основе анализа частот появления отдельных символов. После расшифровывания законный получатель легко снимает рандомизацию. Такие шифры называют «шифрами с многократной подстановкой» или «равночастотными шифрами». Ниже будет приведен пример такого шифра.

Как известно, до недавнего времени криптографические средства использовались преимущественно (если не всецело) для сохранения государственной тайны, поэтому сами средства разрабатывались специальными органами, причем использовались криптосистемы очень высокой стойкости, что, естественно, сопряжено было с большими затратами. Однако, поскольку сфера защиты информации в настоящее время резко расширяется, становится весьма целесообразным системный анализ криптографических средств с учетом возможности и целесообразности их широкого применения для сохранения различных видов секретов и в различных условиях. Кроме того, в последние годы интенсивно разрабатываются новые способы криптографического преобразования данных, которые могут найти более широкое по сравнению с традиционным применение.

Криптографические методы защиты информации в автоматизированных системах могут применяться как для защиты информации, обрабатываемой в ЭВМ или хранящейся в различного типа ЗУ, так и для закрытия информации, передаваемой между различными элементами системы по линиям связи. Криптографическое преобразование как метод предупреждения несанкционированного доступа к информации имеет многовековую историю. В настоящее время разработано большое количество различных методов шифрования, созданы теоретические и практические основы их применения. Подавляющее число этих методов может быть успешно использовано и для закрытия информации.

Почему проблема использования криптографических методов в информационных системах (ИС) стала в настоящий момент особо актуальна?

С одной стороны, расширилось использование компьютерных сетей, в частности глобальной сети Internet, по которым передаются большие объемы информации государственного, военного, коммерческого и частного характера, не допускающего возможность доступа к ней посторонних лиц.

С другой стороны, появление новых мощных компьютеров, технологий сетевых и нейронных вычислений сделало возможным дискредитацию криптографических систем, еще недавно считавшихся практически нераскрываемыми.

Проблемой защиты информации путем ее преобразования занимается криптология (*kryptos* — тайный, *logos* — наука). Криптология разделяется на два направления — *криптографию* и *криптоанализ*. Цели этих направлений прямо противоположны.

Криптография занимается поиском и исследованием математических методов преобразования информации.

Сфера интересов *криптоанализа* — исследование возможности расшифровывания информации без знания ключей.

Современная криптография включает в себя четыре крупных раздела:

1. Симметричные криптосистемы.
2. Криптосистемы с открытым ключом.
3. Системы электронной подписи.
4. Управление ключами.

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.

Криптографические методы защиты информации в автоматизированных системах могут применяться как для защиты информации, обрабатываемой в ЭВМ или хранящейся в различного типа ЗУ, так и для закрытия информации, передаваемой между различными элементами системы по линиям связи. Криптографическое преобразование как метод предупреждения несанкционированного доступа к информации имеет многовековую историю. В настоящее время разработано большое количество различных методов шифрования, созданы теоретические и практические основы их применения. Подавляющее число этих методов может быть успешно использовано и для закрытия информации.

3.2. Методы криптографического преобразования данных

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

Перечислим вначале некоторые основные понятия и определения.

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 Z_{33} — 32 буквы русского алфавита и пробел;
- алфавит Z_{256} — символы, входящие в стандартные коды ASCII и КОИ-8;
- бинарный алфавит — $Z_2 = \{0,1\}$;
- восьмеричный 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*.

Рис. 3.1. Процедура шифрования файлов

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

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 зависимостей 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.

Рассмотрим классификацию методов криптографического закрытия [9, 10, 11].

1. Шифрование
   1.1. Замена (подстановка)
      1.1.1. Простая (одноалфавитная)
      1.1.2. Многоалфавитная одноконтурная обыкновенная
      1.1.3. Многоалфавитная одноконтурная монофоническая
      1.1.4. Многоалфавитная многоконтурная
   1.2. Перестановка
      1.2.1. Простая
      1.2.2. Усложненная по таблице
      1.2.3. Усложненная по маршрутам
   1.3. Аналитическое преобразование
      1.3.1. С использованием алгебры матриц
      1.3.2. По особым зависимостям

1.4. Гаммирование
1.4.1. С конечной короткой гаммой
1.4.2. С конечной длинной гаммой
1.4.3. С бесконечной гаммой
1.5. Комбинированные методы
1.5.1. Замена и перестановка
1.5.2. Замена и гаммирование
1.5.3. Перестановка и гаммирование
1.5.4. Гаммирование и гаммирование
2. Кодирование
2.1. Смысловое
2.1.1. По специальным таблицам (словарям)
2.2. Символьное
2.2.1. По кодовому алфавиту
3. Другие виды
3.1. Рассечение-разнесение
3.1.1. Смысловое
3.1.2. Механическое
3.2. Сжатие-расширение

Под *шифрованием* понимается такой вид криптографического закрытия, при котором преобразованию подвергается каждый символ защищаемого сообщения. Все известные способы шифрования можно разбить на пять групп: подстановка (замена), перестановка, аналитическое преобразование, гаммирование и комбинированное шифрование. Каждый из этих способов может иметь несколько разновидностей.

Под *кодированием* понимается такой вид криптографического закрытия, при котором некоторые элементы защищаемых данных (это не обязательно отдельные символы) заменяются заранее выбранными кодами (цифровыми, буквенными, буквенно-цифровыми сочетаниями и т. п.). Этот метод имеет две разновидности: смысловое и символьное кодирование. При смысловом кодировании кодируемые элементы имеют вполне определенный смысл (слова, предложения, группы предложений). При символьном кодировании кодируется каждый символ защищаемого сообщения. Символьное кодирование по существу совпадает с шифрованием заменой.

Многоалфавитная подстановка — наиболее простой вид преобразований, заключающийся в замене символов исходного тек-

ста на другие (того же алфавита) по более или менее сложному правилу. Для обеспечения высокой криптостойкости требуется использование больших ключей.

Перестановки — несложный метод криптографического преобразования. Используется, как правило, в сочетании с другими методами.

Гаммирование — этот метод заключается в наложении на исходный текст некоторой псевдослучайной последовательности, генерируемой на основе ключа.

Блочные шифры представляют собой последовательность (с возможным повторением и чередованием) основных методов преобразования, применяемую к блоку (части) шифруемого текста. Блочные шифры на практике встречаются чаще, чем «чистые» преобразования того или иного класса в силу их более высокой криптостойкости. Российский и американский стандарты шифрования основаны именно на этом классе шифров.

К отдельным видам криптографического закрытия отнесены методы *рассечения-разнесения и сжатия данных.* Рассечение-разнесение заключается в том, что массив защищаемых данных делится (рассекается) на такие элементы, каждый из которых в отдельности не позволяет раскрыть содержание защищаемой информации. Выделенные таким образом элементы данных разносятся по разным зонам ЗУ или располагаются на различных носителях. Сжатие данных представляет собой замену часто встречающихся одинаковых строк данных или последовательностей одинаковых символов некоторыми заранее выбранными символами.

Кратко рассмотрим основные методы криптографического закрытия информации.

Шифрование

Шифрование заменой (подстановка). В этом наиболее простом методе символы шифруемого текста заменяются другими символами, взятыми из *одного (одно- или моноалфавитная подстановка)* или *нескольких (много- или полиалфавитная подстановка)* алфавитов.

Самой простой разновидностью является прямая (простая) замена, когда буквы шифруемого сообщения заменяются други-

ми буквами того же самого или некоторого другого алфавита. Таблица замены может иметь следующий вид — табл. 3.1.

Таблица 3.1. **Таблица простой замены**

Исходные символы шифруемого текста	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Заменяющие символы	S	P	X	L	R	Z	I	M	A	Y	E	D	W	T	B	G	V	N	J	O	C	F	H	Q	U	K

Используя эту таблицу, зашифруем текст: IN THIS BOOK THE READER WILL FIND A COMPREHENSIVE SURVEY... Получим следующее зашифрованное сообщение: AT OMIY PBBE OMR NRSIRN FADD ZAIL S XBWGNRMRTJAFR JCNFRU... Однако такой шифр имеет низкую стойкость, так как зашифрованный текст имеет те же статистические характеристики, что и исходный. Например, текст на английском языке содержит символы со следующими частотами появления (в порядке убывания): E — 0,13, T — 0,105, A — 0,081, O — 0,079 и т. д. В зашифрованном тексте наибольшие частоты появления в порядке убывания имеют буквы R — 0,12, O — 0,09, A и N по 0,07.

Естественно предположить, что символом *R* зашифрована буква *E*, символом *O* — буква *T* и т. д. Это действительно соответствует таблице замены. Дальнейшая расшифровка не составляет труда. Эти методы дешифровки хорошо известны из классической литературы (см., например, Артур Конан Дойль — «Пляшущие человечки», или Алан Эдгар По — «Золотой жук»).

Если бы объем зашифрованного текста был намного больше, чем в рассмотренном примере, то частоты появления букв в зашифрованном тексте были бы еще ближе к частотам появления букв в английском алфавите и расшифровка была бы еще проще. Поэтому простую замену используют редко и лишь в тех случаях, когда шифруемый текст короток.

Для повышения стойкости шифра используют *полиалфавитные подстановки*, в которых для замены символов исходного текста используются символы нескольких алфавитов. Известно несколько разновидностей полиалфавитной подстановки, наиболее известными из которых являются одно- (обыкновенная и монофоническая) и многоконтурная.

При *полиалфавитной одноконтурной* обыкновенной подстановке для замены символов исходного текста используется несколько алфавитов, причем смена алфавитов осуществляется по-

следовательно и циклически, т. е. первый символ заменяется соответствующим символом первого алфавита, второй — символом второго алфавита и т. д. до тех пор, пока не будут использованы все выбранные алфавиты. После этого использование алфавитов повторяется.

Схема шифрования Вижинера. Таблица Вижинера представляет собой квадратную матрицу с n^2 элементами, где n — число символов используемого алфавита. На рис. 3.2 показана таблица Вижинера для кириллицы. Каждая строка получена циклическим сдвигом алфавита на символ. Для шифрования выбирается буквенный ключ, в соответствии с которым формируется рабочая матрица шифрования.

а	б	в	г	д	е	ж	з	и	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я
б	в	г	д	е	ж	з	и	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а
в	г	д	е	ж	з	и	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б
г	д	е	ж	з	и	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в
д	е	ж	э	и	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г
е	ж	з	и	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д
ж	з	и	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е
з	и	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж
и	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з
и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и
к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	и
л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	и	к
м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	и	к	л
н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	с	ж	з	и	и	к	л	м
о	л	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	и	к	л	м	н
п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	с	ж	з	и	и	к	л	м	н	о
р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	и	к	л	м	н	о	п
с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	и	к	л	м	н	о	п	р
т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	и	к	л	м	н	о	п	р	с
у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	с	ж	з	н	и	к	л	м	и	о	п	р	с	т
ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	и	к	л	м	н	о	п	р	с	т	у
х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	и	к	л	м	н	о	п	р	с	т	у	ф
ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	и	к	л	м	н	о	п	р	с	т	у	ф	х
ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	и	к	л	м	в	о	п	р	с	т	у	ф	х	ц
ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч
щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш
ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь
ы	э	ю	я	а	б	в	г	д	с	ж	з	и	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ
э	ю	я	а	б	в	г	д	е	ж	з	и	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы
ю	я	а	б	в	г	д	е	ж	з	и	и	к	л	м	н	о	л	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э
я	а	б	в	г	д	с	ж	з	и	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ь	ы	э	ю

Рис. 3.2. Таблица Вижинера для русского алфавита

Осуществляется это следующим образом. Из полной таблицы выбирается первая строка и те строки, первые буквы которых соответствуют буквам ключа. Первой размещается первая строка, а под нею — строки, соответствующие буквам ключа в порядке следования этих букв в ключе. Пример такой рабочей матрицы для ключа САЛЬЕРИ приведен в средней части рис. 3.3.

Процесс шифрования выглядит следующим образом: 1) под каждой буквой шифруемого текста записываются буквы ключа. Ключ при этом повторяется необходимое число раз; 2) каждая буква шифруемого текста заменяется по подматрице буквами, находящимися на пересечении линий, соединяющих буквы шифруемого текста в первой строке подматрицы и находящихся под ними букв ключа; 3) полученный текст может разбиваться на группы по несколько знаков. Пусть, например, требуется зашифровать сообщение: МАКСИМАЛЬНО ДОПУСТИМОЙ ЦЕНОЙ ЯВЛЯЕТСЯ ПЯТЬСОТ РУБ. ЗА ШТУКУ. В соответствии с первым правилом записываем под буквами шифруемого текста буквы ключа. Получаем:

МАКСИМАЛЬНО ДОПУСТИМОЙ ЦЕНОЙ ЯВЛЯЕТСЯ ПЯТЬСОТ РУБ. ЗА ШТУКУ
САЛЬЕРИСАЛЬ ЕРИСАЛЬЕРИ САЛЬЕ РИСАЛЬЕР ИСАЛЬЕР ИСА ЛЬ ЕРИСА

Дальше осуществляется непосредственное шифрование в соответствии со вторым правилом, а именно: берем первую букву шифруемого текста (М) и соответствующую ей букву ключа (С); по букве шифруемого текста (М) входим в рабочую матрицу шифрования и выбираем под ней букву, расположенную в строке, соответствующей букве ключа (С), — в нашем примере такой буквой является Э; выбранную таким образом букву помещаем в шифрованный текст. Эта процедура циклически повторяется до зашифровывания всего текста.

На рис. 3.3 представлена схема шифрования. Эксперименты показали, что при использовании такого метода статистические характеристики исходного текста практически не проявляются в зашифрованном сообщении. Нетрудно видеть, что замена по таблице Вижинера эквивалентна простой замене с циклическим изменением алфавита, т. е. здесь мы имеем полиалфавитную подстановку, причем число используемых алфавитов определяется числом букв в слове ключа. Поэтому стойкость такой замены определяется произведением стойкости прямой замены на число используемых алфавитов, т. е. на число букв в ключе.

Исходный текст — **максимально допустимой ценой является пятьсот...**

а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я
с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р
а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я
л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к
ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь
е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д
р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п	р
и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з

Шифротекст — эахмныиын пифгцчичио жнюоф...

Рис. 3.3. Последовательность шифрования по таблице Вижинера с использованием ключа «Сальери»

Расшифровка текста производится в следующей последовательности: 1) над буквами зашифрованного текста последовательно надписываются буквы ключа, причем ключ повторяется необходимое число раз; 2) в строке подматрицы Вижинера, соответствующей букве ключа, отыскивается буква, соответствующая знаку зашифрованного текста. Находящаяся под ней буква первой строки подматрицы и будет буквой исходного текста; 3) полученный текст группируется в слова по смыслу.

На рис. 3.4 данная процедура представлена в наглядном виде.

Исходный текст — **максимально...**

а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я
с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р
а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я
л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к
ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь
е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д
р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п	р
и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з

Ключ: **сальерисальерисальерисальери**

Шифротекст — **эахмныиын пифгцчичио жнюоф...**

Рис. 3.4. Порядок расшифровки по таблице Вижинера

Нетрудно видеть, что процедуры как прямого, так и обратного преобразований являются строго формальными, что позволяет реализовать их алгоритмически. Более того, обе процедуры легко реализуются по одному и тому же алгоритму.

Одним из недостатков шифрования по таблице Вижинера является то, что при небольшой длине ключа надежность шиф-

рования остается невысокой, а формирование длинных ключей сопряжено с трудностями.

Нецелесообразно выбирать ключ с повторяющимися буквами, так как при этом стойкость шифра не возрастает. В то же время ключ должен легко запоминаться, чтобы его можно было не записывать. Последовательность же букв, не имеющую смысла, запомнить трудно.

С целью повышения стойкости шифрования можно использовать усовершенствованные варианты таблицы Вижинера. Приведем некоторые из них: 1) во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке; 2) в качестве ключа используются случайные последовательности чисел. Из таблицы Вижинера выбираются десять произвольных строк, которые кодируются натуральными числами от 0 до 10. Эти строки используются в соответствии с чередованием цифр в выбранном ключе. Известны и другие модификации метода.

Вариант системы подстановок Вижинера при $m = 2$ называется системой Вернама (1917 год). В то время ключ $k = (k_0, k_1, \ldots, k_к - 1)$ записывался на бумажной ленте. Каждая буква исходного текста переводилась с использованием *кода Бодо* в пятибитовый символ. К исходному тексту Бодо добавлялся ключ (по модулю 2). Старинный телетайп фирмы AT&T со считывающим устройством Вернама и оборудованием для шифрования использовался корпусом связи армии США.

Монофоническая замена. Частным случаем рассмотренной полиалфавитной замены является так называемая монофоническая замена. Особенность этого метода состоит в том, что количество и состав алфавитов выбираются таким образом, чтобы частоты появления всех символов в зашифрованном тексте были одинаковыми. При таком положении затрудняется криптоанализ зашифрованного текста с помощью его статистической обработки. Выравнивание частот появления символов достигается за счет того, что для часто встречающихся символов исходного текста предусматривается использование большего числа заменяющих элементов, чем для редко встречающихся. Пример монофонического шифра для английского алфавита показан на рис. 3.5. Шифрование осуществляется так же, как и при простой замене (т. е. по шифрующему алфавиту № 1), с той лишь разницей, что после шифрования каждого знака соответствующий ему столбец алфавитов циклически сдвигается вверх на

	Алфавит открытого текста																									
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Алфавит шифротекста	f	N	Q	.	G	т	D	,	A	e	L	-	R	(	C	x	I	Z	V	--	W	S	h	u	K	t
	*	N	Q	b	+	[	D	p	)	e	L	O	R	y	/	x	I	=	$	j	W	S	h	u	K	t
	k	N	Q	i	]	W	D	r	q	e	L	и	R	(	#	x	I	a	d	:	W	S	h	u	K	t
	f	N	Q	.	I	т	D	,	A	e	L	A.	R	y	п	x	I	Z	V	C	W	S	h	u	K	t
	*	N	Q	b	G	[	D	p	)	e	L	O	R	(	C	x	I	=	$	--	W	S	h	u	K	t
	R	N	Q	i	+	W	D	r	q	e	L	и	R	y	/	x	I	a	d	j	W	S	h	u	K	t
	f	N	Q	.	]	т	D	,	A	e	L	A.	R	(	#	x	I	Z	V	:	W	S	h	u	K	t
	*	N	Q	b	I	[	D	p	)	e	L	O	R	y	п	x	I	=	$	C	W	S	h	u	K	t
	k	N	Q	i	G	W	D	r	q	e	L	и	R	(	c	x	I	a	d	--	W	S	h	u	K	t
	f	N	Q	.	+	т	D	,	A	e	L	O	R	y	/	x	I	Z	V	j	W	S	h	u	K	t
	*	N	Q	b	]	[	D	p	)	e	L	A	R	(	#	x	I	=	$	:	W	S	h	u	K	t
	k	N	Q	i	I	W	D	r	q	e	L	и	R	y	п	x	I	a	d	C	W	S	h	u	K	t

Рис. 3.5. Монофонический шифр для английского алфавита

одну позицию. Таким образом, столбцы алфавита как бы образуют независимые друг от друга кольца, поворачиваемые вверх на один знак каждый раз после шифрования соответствующего знака. В качества примера зашифруем монофоническим шифром тот же текст, который шифровался простой заменой:

IN THIS BOOK THE READER WILL FIND A COMPREHENSIVE SURVEY...

Шифрованный текст имеет вид:

A(-,) VNG/LjpGZ+F.=hg...

Если подсчитать частоты появления символов, то легко видеть, что даже на таком коротком образце текста они в значительной мере выровнены. При увеличении объема текста частоты появления символов будут еще более выравниваться.

Полиалфавитная многоконтурная замена заключается в том, что для шифрования используется циклически несколько наборов (контуров) алфавитов, причем каждый контур в общем случае имеет свой индивидуальный период применения. Этот период исчисляется, как правило, количеством знаков, после зашифровки которых меняется контур алфавитов. Частным случаем многоконтурной полиалфавитной подстановки является замена по таблице Вижинера, если для шифрования используется несколько ключей, каждый из которых имеет свой период применения.

Общий принцип шифрования подстановкой может быть представлен следующей формулой:

$$R_i = S_i + w \bmod (k - 1),$$

где R_i — символ зашифрованного текста;

S_i — символ исходного текста;

w — целое число в диапазоне 0—(k – 1);

k — число символов используемого алфавита.

Если w фиксировано, то формула описывает моноалфавитную подстановку, если w выбирается из последовательности w_1, w_2, ... w_n, то получается полиалфавитная подстановка с периодом n.

Если в полиалфавитной подстановке $n > m$ (где m — число знаков шифруемого текста) и любая последовательность w_1, w_2, ... w_n используется только один раз, то такой шифр является теоретически нераскрываемым, если, конечно, злоумышленник не имеет доступа к исходному тексту. Такой шифр получил название шифра Вермэна.

Шифрование методом перестановки. Этот метод заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов. Рассмотрим некоторые наиболее часто встречающиеся разновидности этого метода, которые могут быть использованы в автоматизированных системах.

Самая простая перестановка — написать исходный текст задом наперед и одновременно разбить шифрограмму на пятерки букв. Например, из фразы

ПУСТЬ БУДЕТ ТАК, КАК МЫ ХОТЕЛИ.

получится такой шифротекст:

ИЛЕТО ХЫМКА ККАТТ ЕДУБЬ ТСУП

В последней группе (пятерке) не хватает одной буквы. Значит, прежде чем шифровать исходное выражение, следует его дополнить незначащей буквой (например, О) до числа, кратного пяти:

ПУСТЬ-БУДЕТ-ТАККА-КМЫХО-ТЕЛИО.

Тогда шифрограмма, несмотря на столь незначительное изменение, будет выглядеть по-другому:

ОИЛЕТ ОХЫМК АККАТ ТЕДУБ ЬТСУП

Кажется, ничего сложного, но при расшифровке возникнут серьезные проблемы.

Во время Гражданской войны в США в ходу был такой шифр: исходную фразу писали в несколько строк. Например, по

пятнадцать букв в каждой (с заполнением последней строки незначащими буквами).

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
П	У	С	Т	Ь	Б	У	Д	Е	Т	Т	А	К	К	А
К	М	Ы	Х	О	Т	Е	Л	И	К	Л	М	Н	О	П

После этого вертикальные столбцы по порядку писали в строку с разбивкой на пятерки букв:

ПКУМС ЫТХЬО БТУЕД ЛЕИТК ТЛАМК НКОАП

Вариант этого шифра: сначала исходную фразу записать в столбики:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
П	С	Ь	У	Е	Т	К	А	М	Х	Т	Л	А	В	Д
У	Т	Б	Д	Т	А	К	К	Ы	О	Е	И	Б	Г	Е

Потом разбить строки на пятерки букв:

ПСЬУЕ ТКАМХ ТЛАВД УТБДТ АККЫО ЕИБГЕ

Если строки укоротить, а количество строк увеличить, то получится прямоугольник-решетка, в который можно записывать исходный текст. Но тут уже требуются предварительные договоренности между адресатом и отправителем посланий, поскольку сама решетка может быть различной длины-высоты, записывать в нее можно по строкам, по столбцам, по спирали туда или по спирали обратно, можно писать и по диагоналям, а для шифрования можно брать тоже различные направления. В общем, здесь масса вариантов.

Для примера возьмем решетку 6×6 (причем количество строк может увеличиваться или уменьшаться в зависимости от длины исходного сообщения) и заполним ее по строкам:

П	У	С	Т	Ь	Б
У	Д	Е	Т	Т	А
К	К	А	К	М	Ы
Х	О	Т	Е	Л	И
А	Б	В	Г	Д	Е
М	Л	К	И	З	Ж

Если шифровать по стрелкам (диагоналям) сверху вниз с левого верхнего угла, то в итоге получится такая шифрограмма:

П УУ СДК ТЕКХ ЬТАОА БТКТБМ АМЕВЛ ЫЛГК ИДИ ЕЗ Ж

Для окончательного оформления шифротекст может быть разбит на группы по 6 символов:

ПУУСДК ТЕКХЬТ АОАБТК ТБМАМЕ ВЛЫЛГК ИДИЕЗЖ

Весьма часто используют перестановки с ключом. Тогда правила заполнения решетки и шифрования из нее упрощаются, становятся стандартными. Единственное, что надо помнить и знать, — это ключ, которым может быть любое слово, например РАДИАТОР. В соответствии с расположением букв в алфавите буква А получает номер 1, вторая буква А — 2, следующая по алфавиту буква Д — 3, потом И — 4, О — 5, первая буква Р — 6, вторая Р — 7 и буква Т — 8.

Заполняем решетку:

Р	А	Д	И	А	Т	О	Р
6	1	3	4	2	8	5	7
П	У	С	Т	Ь	Б	У	Д
Е	Т	Т	А	К	К	А	К
М	Ы	Х	О	Т	Е	Л	И
О							

Записываем столбики в соответствии с номерами букв ключа:

УТЫ ЬКТ СТХ ТАО УАЛ ПЕМО ДКИ БКЕ

Затем последовательность опять разбивается на пятерки:

УТЫЬК ТСТХТ АОУАЛ ПЕМОД КИБКЕ

Таким шифром простой перестановки колонок пользовались немецкие секретные агенты во время Второй мировой войны. В качестве ключа они использовали первые буквы строк на определенной странице какой-нибудь обыкновенной книги.

Развитием этого шифра является шифр перестановки колонок с пропусками, которые располагаются в решетке тоже в со-

ответствии с ключом (в нашем случае через 6-1-3-4-2-8-5-7 ... символов):

Р	А	Д	И	А	Т	О	Р
6	1	3	4	2	8	5	7
П	У	С	Т	Ь	Б	=	У
=	Д	Е	Т	=	Т	А	К
К	=	Х	О	=	Т	Е	Л
И	К	Л	М	=	О	П	Р

Шифрограмма будет такой:

УДК Ь СЕХЛ ТТОМ АЕП ПКИ УКЛР БТТО

Из рассмотренных примеров очевидно, что все процедуры шифрования и расшифровки по методу перестановок являются в достаточной степени формальными и могут быть реализованы алгоритмически.

Шифрование методом гаммирования. Суть этого метода состоит в том, что символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, которая называется гаммой. Иногда такой метод представляют как наложение гаммы на исходный текст, поэтому он получил название гаммирование.

Процедуру наложения гаммы на исходный текст можно осуществить двумя способами. При первом способе символы исходного текста и гаммы заменяются цифровыми эквивалентами, которые затем складываются по модулю k, где k — число символов в алфавите, т. е.

$$R_i = (S_i + \mathrm{G}) \bmod (k - 1),$$

где R_i, S_i, G — символы соответственно зашифрованного, исходного текста и гаммы.

При втором методе символы исходного текста и гаммы представляются в виде двоичного кода, затем соответствующие разряды складываются по модулю 2. Вместо сложения по модулю 2 при гаммировании можно использовать и другие логические операции, например преобразование по правилу логической эквивалентности (рис. 3.6, *а*) или логической неэквивалентности (рис. 3.6, *б*).

Гамма	Текст 0	Текст 1
0	0	1
1	1	0

а

Гамма	Текст 0	Текст 1
0	1	0
1	0	1

б

Шифруемый текст	Б	У	Д	Ь ...	
	010010	100000	110010	100000	
Знаки гаммы	7	1	8	2 ...	
	000111	000001	001000	000010	
Шифрованный текст	010101	100001	111010	100010	

в

Рис. 3.6. Пример шифрования гаммированием

Такая замена равносильна введению еще одного ключа, которым является выбор правила формирования символов зашифрованного сообщения из символов исходного текста и гаммы.

Стойкость шифрования методом гаммирования определяется главным образом свойствами гаммы — длительностью периода и равномерностью статистических характеристик. Последнее свойство обеспечивает отсутствие закономерностей в появлении различных символов в пределах периода.

Обычно разделяют две разновидности гаммирования — с конечной и бесконечной гаммами. При хороших статистических свойствах гаммы стойкость шифрования определяется только длиной периода гаммы. При этом, если длина периода гаммы превышает длину шифруемого текста, то такой шифр теоретически является абсолютно стойким, т. е. его нельзя вскрыть с помощью статистической обработки зашифрованного текста. Это, однако, не означает, что дешифрование такого текста вообще невозможно: при наличии некоторой дополнительной информации исходный текст может быть частично или полностью восстановлен даже при использовании бесконечной гаммы.

В качестве гаммы может быть использована любая последовательность случайных символов, например последовательность цифр числа π, числа e (основание натурального логарифма) и т. п. При шифровании с помощью ЭВМ последовательность гаммы может формироваться с помощью датчика псевдослучайных чисел (ПСЧ). В настоящее время разработано несколько алгоритмов работы таких датчиков, которые обеспечивают удовлетворительные характеристики гаммы.

Шифрование с помощью аналитических преобразований. Достаточно надежное закрытие информации может быть обеспечено

при использовании для шифрования некоторых аналитических преобразований. Для этого можно использовать методы алгебры матриц, например умножение матрицы на вектор по правилу:

$$\overline{C} = A \times \overline{B}; \quad \sum_{j=1}^{N} a_{ij} b_j .$$

Если матрицу $A = (a_{ij})$ использовать в качестве ключа, а вместо компонента вектора $B = (b_j)$ подставить символы текста, то компоненты вектора $C = (c_j)$ будут представлять собой символы зашифрованного текста.

Приведем пример, взяв в качестве ключа квадратную матрицу третьего порядка

$$A = \begin{pmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{pmatrix}.$$

Заменим буквы алфавита цифрами, соответствующими их порядковому номеру в алфавите: А — 0, Б — 1, В — 2 и т. д. Тогда отрывку текста ВАТАЛА будет соответствовать последовательность **2**, **0**, **19**, **0**, **12**, **0**. По принятому алгоритму шифрования выполним необходимые действия:

$$\overline{C} = A \times \overline{B} = \begin{pmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{pmatrix} \times \begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix} = \begin{pmatrix} 85 \\ 54 \\ 25 \end{pmatrix};$$

$$\overline{C} = A \times \overline{B} = \begin{pmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{pmatrix} \times \begin{pmatrix} 0 \\ 12 \\ 0 \end{pmatrix} = \begin{pmatrix} 96 \\ 60 \\ 24 \end{pmatrix}.$$

При этом зашифрованный текст будет иметь вид: **85**, **54**, **25**, **96**, **60**, **24**.

Дешифрование осуществляется с использованием того же правила умножения матрицы на вектор, только в качестве ключа берется матрица, обратная той, с помощью которой осуществляется шифрование, а в качестве вектора-сомножителя — соответствующие фрагменты символов закрытого текста; тогда значе-

ниями вектора-результата будут цифровые эквиваленты знаков открытого текста.

Матрицей, обратной данной A, называется матрица A^{-1}, получающаяся из присоединенной матрицы делением всех ее элементов на определитель данной матрицы. В свою очередь ***присоединенной*** называется матрица, составленная из алгебраических дополнений A_{ij}, к элементам данной матрицы, которые вычисляются по формуле

$$A_{ij} = (-1)^{i+j}\,\Delta_{ij},$$

где Δ_{ij} — определитель матрицы, получаемой вычеркиванием i-й строки и j-го столбца исходной матрицы A.

Определителем матрицы называется алгебраическая сумма $n!$ членов (для определителя n-го порядка), составленная следующим образом: членами служат всевозможные произведения n элементов матрицы, взятых по одному в каждой строке и в каждом столбце, причем член суммы берется со знаком «+», если его индексы составляют четную подстановку, и со знаком «–» — в противоположном случае. Для матрицы третьего порядка, например, определитель вычисляется следующим образом:

$$\Delta = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31}.$$

Тогда процесс раскрытия выглядит так:

$$A^{-1} \times \overline{C} = \begin{pmatrix} 1 & -2 & 1 \\ -2 & 5 & -4 \\ 1 & -4 & 6 \end{pmatrix} \times \begin{pmatrix} 85 \\ 54 \\ 25 \end{pmatrix} = \begin{pmatrix} 1\cdot 85 - 2\cdot 54 + 1\cdot 25 \\ -2\cdot 85 + 5\cdot 54 - 4\cdot 25 \\ 1\cdot 85 - 4\cdot 54 + 6\cdot 25 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix};$$

$$A^{-1} \times \overline{C} = \begin{pmatrix} 1 & -2 & 1 \\ -2 & 5 & -4 \\ 1 & -4 & 6 \end{pmatrix} \times \begin{pmatrix} 96 \\ 60 \\ 24 \end{pmatrix} = \begin{pmatrix} 1\cdot 96 - 2\cdot 60 + 1\cdot 24 \\ -2\cdot 96 + 5\cdot 60 - 4\cdot 24 \\ 1\cdot 96 - 4\cdot 60 + 6\cdot 24 \end{pmatrix} = \begin{pmatrix} 0 \\ 12 \\ 0 \end{pmatrix}.$$

Таким образом, получена последовательность знаков раскрытого текста **3**, **0**, **19**, **0**, **12**, **0**, что соответствует исходному тексту. Этот метод шифрования является формальным, что позволяет легко реализовать его программными средствами.

Комбинированные методы шифрования. Одним из важнейших требований, предъявляемых к системе шифрования, является ее высокая стойкость. Однако повышение стойкости любого метода шифрования приводит, как правило, к существенному усложне-

нию самого процесса шифрования и увеличению затрат ресурсов (времени, аппаратных средств, уменьшению пропускной способности и т. п.).

Достаточно эффективным средством повышения стойкости шифрования является комбинированное использование нескольких различных способов шифрования, т. е. последовательное шифрование исходного текста с помощью двух или более методов.

Как показали исследования, стойкость комбинированного шифрования S_k не ниже произведения стойкостей используемых способов S_i, т. е.

$$S_k \geq \prod_i S_i.$$

Вообще говоря, комбинировать можно любые методы шифрования и в любом количестве, однако на практике наибольшее распространение получили следующие комбинации: 1) подстановка + гаммирование; 2) перестановка + гаммирование; 3) гаммирование + гаммирование; 4) подстановка + перестановка. Типичным примером комбинированного шифра является национальный стандарт США криптографического закрытия данных (DES).

Кодирование

Одним из средств криптографического закрытия информации, также имеющим длительную историю практического использования, является кодирование, под которым понимается замена элементов закрываемых данных некоторыми цифровыми, буквенными или комбинированными сочетаниями — кодами. Нетрудно заметить, что между кодированием информации и ее шифрованием подстановкой существует значительная аналогия. Однако между этими методами можно найти и различия.

При шифровании подстановкой заменяемыми единицами информации являются символы алфавита, и, следовательно, шифрованию могут подвергаться любые данные, для фиксирования которых используется данный алфавит. При кодировании замене подвергаются смысловые элементы информации, поэтому для каждого специального сообщения в общем случае необходимо использовать свою систему кодирования. Правда, в последнее время разработаны специальные коды, цель которых —

сократить объем информации при записи ее в ЗУ. Специфика этих кодов заключается в том, что для записи часто встречающихся символов используются короткие двоичные коды, а для записи редко встречающихся — длинные.

Примером такого кода для английского языка может служить код Хаффмана, показанный в табл. 3.2.

Таблица 3.2. **Коды Хаффмана**

A	1	1	1	1						
O	1	1	1	0						
N	1	1	0							
D	1	1	0	1	1					
P	1	1	0	1	0	1				
V	1	1	0	1	0	0	1			
K	1	1	0	1	0	0	0	1	1	
Q	1	1	0	1	0	0	0	1	0	1
Z	1	1	0	1	0	0	0	1	0	0
X	1	1	0	1	0	0	0	0	1	
J	1	1	0	1	0	0	0	0	0	
R	1	0	1	1						
I	1	0	1	0						
E	1	0	0							
S	0	1	1	0						
W	0	1	1	1	0	1				
B	0	1	1	1	0	0				
H	0	1	0	1						
F	0	1	0	0	1					
C	0	1	0	0	0					
M	0	0	0	1	1					
U	0	0	0	1	0					
G	0	0	0	0	1					
Y	0	0	0	0	0					

Такое кодирование имеет криптографическую стойкость на уровне шифрования простой заменой.

При смысловом кодировании основной кодируемой единицей является смысловой элемент текста. Для кодирования составляется специальная таблица кодов, содержащая перечень кодируемых элементов и соответствующих им кодов. Введем, например, следующую кодовую таблицу:

Автоматизированные системы управления	001
Автоматизация управления	002
Осуществляет	415
Позволяет	632

Тогда предложение «Автоматизированные системы управления позволяют осуществлять автоматизацию управления» после кодирования будет иметь вид: 001 632 415 002.

Другие виды криптографического закрытия информации

К ним относятся рассечение-разнесение и сжатие данных. Рассечение-разнесение данных состоит в том, что массив защищаемых данных рассекается на такие элементы, каждый из которых не позволяет раскрыть содержание защищаемой информации, и выделенные таким образом элементы размещаются в различных зонах ЗУ. Обратная процедура называется сборкой данных. Совершенно очевидно, что алгоритм разнесения и сборки данных должен тщательно охраняться.

Системы с открытым ключом

Как бы ни были сложны и надежны криптографические системы, их слабое место при практической реализации — проблема *распределения ключей*. Для того чтобы был возможен обмен конфиденциальной информацией между двумя субъектами ИС, ключ должен быть сгенерирован одним из них, а затем каким-то образом опять же в конфиденциальном порядке передан другому. То есть, в общем случае для передачи ключа опять же требуется использование какой-то криптосистемы.

Для решения этой проблемы на основе результатов, полученных классической и современной алгеброй, были предложены *системы с открытым ключом*.

Суть их состоит в том, что каждым адресатом ИС генерируются два ключа, связанные между собой по определенному правилу. Один ключ объявляется *открытым*, а другой *закрытым*. Открытый ключ публикуется и доступен любому, кто желает послать сообщение адресату. Секретный ключ сохраняется в тайне.

Исходный текст шифруется открытым ключом адресата и передается ему. Зашифрованный текст в принципе не может быть расшифрован тем же открытым ключом. Дешифрование сообщения возможно только с использованием закрытого ключа, который известен только самому адресату.

Криптографические системы с открытым ключом (рис. 3.7) используют так называемые *необратимые, или односторонние, функции*, которые обладают следующим свойством: при заданном значении x относительно просто вычислить значение $f(x)$, однако если $y = f(x)$, то нет простого пути для вычисления значения x.

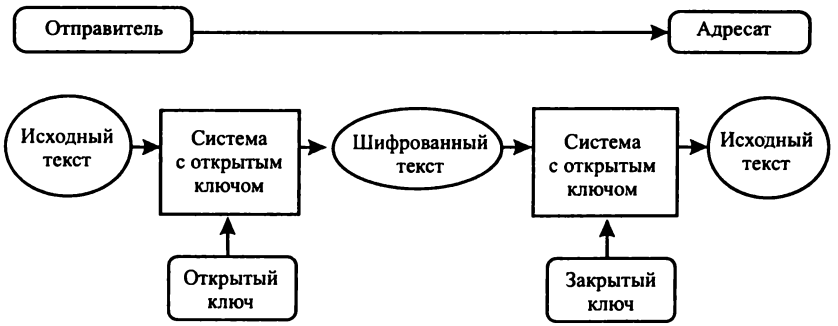


Рис. 3.7. Реализация процедуры шифрования с открытым ключом

Множество классов необратимых функций и порождает все разнообразие систем с открытым ключом. Однако не всякая необратимая функция годится для использования в реальных ИС.

В самом определении необратимости присутствует неопределенность. Под *необратимостью* понимается не теоретическая необратимость, а практическая невозможность вычислить обратное значение, используя современные вычислительные средства за обозримый интервал времени.

Поэтому, чтобы гарантировать надежную защиту информации, к системам с открытым ключом (СОК) предъявляются два важных и очевидных требования:

1. Преобразование исходного текста должно быть необратимым и исключать его восстановление на основе открытого ключа.

2. Определение закрытого ключа на основе открытого также должно быть невозможным при современном уровне технологии. При этом желательна точная нижняя оценка сложности (количества операций, необходимых для раскрытия шифра).

Алгоритмы шифрования с открытым ключом получили широкое распространение в современных информационных системах. Так, алгоритм RSA стал мировым стандартом де-факто для открытых систем и рекомендован МККТТ.

Вообще же, все предлагаемые сегодня криптосистемы с открытым ключом опираются на один из следующих типов необратимых преобразований:

- разложение больших чисел на простые множители;
- вычисление логарифма в конечном поле;
- вычисление корней алгебраических уравнений.

Здесь же следует отметить, что алгоритмы криптосистемы с открытым ключом (СОК) можно использовать в трех назначениях.

1. Как *самостоятельные средства защиты* передаваемых и хранимых данных.

2. Как *средства для распределения ключей*. Алгоритмы СОК более трудоемки, чем традиционные криптосистемы. Поэтому часто на практике рационально с помощью СОК распределять ключи, информационный объем которых незначителен. А потом с помощью обычных алгоритмов осуществлять обмен большими потоками данных.

3. *Средства аутентификации пользователей* (электронная подпись).

Несмотря на довольно большое число различных СОК, наиболее популярна криптосистема RSA, разработанная в 1977 г. и получившая название в честь ее создателей — Рона Ривеста, Ади Шамира и Леонарда Эйдельмана.

Они воспользовались тем фактом, что нахождение больших простых чисел в вычислительном отношении осуществляется легко, но разложение на множители произведения двух таких чисел практически невыполнимо. Доказано (теорема Рабина), что раскрытие шифра RSA эквивалентно такому разложению. Поэто-

му для любой длины ключа можно дать нижнюю оценку числа операций для раскрытия шифра, а с учетом производительности современных компьютеров оценить и необходимое на это время.

Возможность гарантированно оценить защищенность алгоритма RSA стала одной из причин популярности этой СОК на фоне десятков других схем. Поэтому алгоритм RSA используется в банковских компьютерных сетях, особенно для работы с удаленными клиентами (обслуживание кредитных карточек).

В настоящее время алгоритм RSA используется во многих стандартах, среди которых SSL, S-HHTP, S-MIME, S/WAN, STT и PCT.

Электронная цифровая подпись

Целью применения цифровой подписи является, во-первых, гарантированное подтверждение подлинности информации, содержащейся в конкретном электронном документе, и, во-вторых, иметь возможность неопровержимо доказать третьей стороне (арбитру, суду и т. д.), что документ составлен именно этим конкретным лицом, являющимся действительным автором данного документа. Для достижения указанной цели автор должен, используя свое секретное индивидуальное число (индивидуальный ключ, пароль и т. д.), определенным образом выполнять процесс «цифрового подписывания» документа. При таком подписывании каждый раз индивидуальный ключ соответствующим образом сворачивается (замешивается) с содержимым электронного документа. Полученное в результате такого сворачивания число (последовательность определенной длины цифровых разрядов) и является цифровой подписью автора под данным конкретным документом. Следовательно, процедуры подписывания и проверки цифровой подписи, в которых используется по одному ключу из пары ключей, должны быть известны, но при этом должна обеспечиваться гарантированная невозможность восстановления ключа подписывания по ключу проверки. Лучшим на сегодня из предложенных способов является использование таких процедур, чтобы практическое восстановление ключей подписи (закрытых ключей) по ключам проверки (открытым ключам) требовало бы решения известной, вычислительно сложной, задачи.

Коротко и просто эту задачу можно сформулировать следующим образом. Если известны три больших целых положительных числа A, B и X, то легко вычислить значение $C = A^X$ MOD B. При дискретном логарифмировании же требуется по заданным A, C и B таким, что $C = A^X$ MOD B, вычислить X (при правильном выборе больших целых чисел эта задача столь сложна, что практически невозможно восстановить X по числу C). Необходимо выбрать X в качестве индивидуального ключа подписывания, а C в качестве известного ключа проверки подписи.

Впервые идея цифровой подписи как законного средства подтверждения подлинности и авторства электронного документа была выдвинута в работе Диффи и Хеллмана в 1976 г.

Как известно, при передаче сообщения по линиям связи или хранении его в памяти должны быть обеспечены вместе или по отдельности следующие требования:

1. Соблюдение конфиденциальности сообщения — злоумышленник не должен иметь возможности узнать содержание передаваемого (или хранимого) сообщения.

2. Удостоверение в подлинности полученного (или считанного из памяти) сообщения, которое включает два понятия:

- целостность — сообщение должно быть защищено от случайного или умышленного изменения по пути его следования (или во время хранения в памяти);
- идентификацию отправителя (проверку авторства) — получатель должен иметь возможность проверить, кем отправлено (или составлено) сообщение.

Шифрование может обеспечить конфиденциальность, а в некоторых системах и целостность. Целостность сообщения проверяется вычислением некоторой контрольной функции от сообщения (некоего числа небольшой длины). Она должна с достаточно высокой степенью вероятности изменяться даже при малых изменениях самого сообщения. Называют и вычисляют контрольную функцию по-разному:

- код подлинности сообщения (Message Authentical Code — MAC);
- квадратичный конгруэнтный алгоритм (Quadratic Congruentical Manipulation Detection Code — QCMDC);
- Manipulation Detection Code (MDC);
- Message Digest Algorithm (MD5);
- контрольная сумма;
- символ контроля блока (Block Check Character — BCC);

- циклический избыточный код (ЦИК, Cyclic Redundance Check — CRC);
- хэш-функция (Hash);
- имитовставка по ГОСТ 28147—89;
- алгоритм с усечением до *n* битов (n-bit Algorithm with Truncation).

При вычислении контрольной функции может использоваться какой-либо алгоритм шифрования. Возможно шифрование и самой контрольной суммы.

В настоящее время широкое применение получила цифровая подпись (цифровое дополнение к передаваемому или же хранящемуся зашифрованному тексту, которое гарантирует целостность последней и позволяет проверить авторство). Известны модели цифровой подписи на основе алгоритмов симметричного шифрования. Однако при широком использовании криптографических систем с открытыми ключами целесообразно применить цифровую подпись, так как она при этом осуществляется более удобно.

Криптографические стандарты DES и ГОСТ 28147—89

Рассмотрим кратко алгоритмы блочного шифрования, принятые в качестве государственных стандартов шифрования данных в США и России.

В 1973 г. Национальное бюро стандартов США начало разработку программы по созданию стандарта шифрования данных на ЭВМ. Был объявлен конкурс среди фирм-разработчиков США, который выиграла фирма IBM, представившая в 1974 г. алгоритм шифрования, известный под названием DES (Data Encryption Standart).

В этом алгоритме входные 64-битовые векторы, называемые блоками открытого текста, преобразуются в выходные 64-битовые векторы, называемые блоками шифртекста, с помощью двоичного 56-битового ключа K. Число различных ключей DES-алгоритма равно $2^{56} > 7 \cdot 10^{16}$.

Алгоритм реализуется в последовательности 16 аналогичных циклов шифрования, где на i-м цикле используется цикловой ключ K_i, представляющий собой алгоритмически вырабатываемую выборку 48 битов из 56 битов ключа K_i, $i = 1, 2, ..., 16$.

Алгоритм обеспечивает высокую стойкость, однако недавние результаты показали, что современная технология позволяет создать вычислительное устройство стоимостью около 1 млн долларов США, способное вскрыть секретный ключ с помощью полного перебора в среднем за 3,5 часа.

Из-за небольшого размера ключа было принято решение использовать DES-алгоритм для закрытия коммерческой (несекретной) информации. Практическая реализация перебора всех ключей в данных условиях экономически нецелесообразна, так как затраты на реализацию перебора не соответствуют ценности информации, закрываемой шифром.

DES-алгоритм явился первым примером широкого производства и внедрения технических средств в области защиты информации. Национальное бюро стандартов США проводит проверку аппаратных реализаций DES-алгоритма, предложенных фирмами-разработчиками, на специальном тестирующем стенде. Только после положительных результатов проверки производитель получает от Национального бюро стандартов сертификат на право реализации своего продукта. К настоящему времени аттестовано несколько десятков изделий, выполненных на различной элементной базе.

Достигнута высокая скорость шифрования. По некоторым сообщениям, разработаны микросхемы, реализующие DES-алгоритм со скоростью 45 Мбит/с. Велика доступность этих изделий: стоимость некоторых аппаратных реализаций ниже 100 долл. США.

Основные области применения DES-алгоритма:

1) хранение данных в ЭВМ (шифрование файлов, паролей);

2) аутентификация сообщений (имея сообщение и контрольную группу, несложно убедиться в подлинности сообщения);

3) электронная система платежей (при операциях с широкой клиентурой и между банками);

4) электронный обмен коммерческой информацией (обмен данными между покупателем, продавцом и банкиром защищен от изменений и перехвата).

В 1989 г. в СССР был разработан блочный шифр для использования в качестве государственного стандарта шифрования данных. Разработка была принята и зарегистрирована как ГОСТ 28147—89. И хотя масштабы применения этого алгоритма шифрования до сих пор уточняются, начало его внедрению, в частности в банковской системе, уже положено. Алгоритм, судя по

публикациям, несколько медлителен, но обладает весьма высокой стойкостью.

Блок-схема алгоритма ГОСТ отличается от блок-схемы DES-алгоритма лишь отсутствием начальной перестановки и числом циклов шифрования (32 в ГОСТе против 16 в DES-алгоритме).

Ключ алгоритма ГОСТ — это массив, состоящий из 32-мерных векторов X_1, X_2, ... X_8. Цикловой ключ i-го цикла K_i равен Xs, где ряду значений i от 1 до 32 соответствует следующий ряд значений s:

1, 2, 3, 4, 5, 6, 7, 8, 1, 2, 3, 4, 5, 6, 7, 8, 1, 2, 3, 4, 5, 6, 7, 8, 8, 7, 6, 5, 4, 3, 2, 1.

В шифре ГОСТ используется 256-битовый ключ, и объем ключевого пространства составляет 2^{256}. Ни на одной из существующих в настоящее время или предполагаемых к реализации в недалеком будущем ЭВМ общего применения нельзя подобрать ключ за время, меньшее многих сотен лет. Российский стандарт проектировался с большим запасом, по стойкости он на много порядков превосходит американский стандарт DES с его реальным размером ключа в 56 бит и объемом ключевого пространства всего 2^{56}. В свете прогресса современных вычислительных средств этого явно недостаточно. В этой связи DES может представлять скорее исследовательский или научный, чем практический интерес.

Алгоритм расшифровки отличается от алгоритма зашифровки тем, что последовательность ключевых векторов используется в обратном порядке.

Расшифровка данных возможна только при наличии синхропосылки, которая в скрытом виде хранится в памяти ЭВМ или передается по каналам связи вместе с зашифрованными данными.

Важной составной частью шифросистемы является ключевая система шифра. Под ней обычно понимается описание всех видов ключей (долговременные, суточные, сеансовые и др.), используемых шифром, и алгоритмы их использования (протоколы шифрованной связи).

В электронных шифраторах в качестве ключей могут использоваться начальные состояния элементов памяти в схемах, реализующих алгоритм шифрования, функциональные элементы алгоритма шифрования. Ключ может состоять из нескольких ключевых составляющих различных типов: долговременных, сеансовых и т. д.

Одной из основных характеристик ключа является его размер, определяющий число всевозможных ключевых установок шифра. Если размер ключа недостаточно велик, то шифр может быть вскрыт простым перебором всех вариантов ключей. Если размер ключа чрезмерно велик, то это приводит к удорожанию изготовления ключей, усложнению процедуры установки ключа, понижению надежности работы шифрующего устройства и т. д. Таким образом, выбранный криптографом размер ключа — это всегда некий компромисс.

Заметим, что DES-алгоритм подвергался критике именно в связи с небольшим размером ключа, из-за этого многие криптологи пришли к мнению, что необходимым «запасом прочности» DES-алгоритм не обладает.

Другой важной характеристикой ключа является его случайность.

Наличие закономерностей в ключе приводит к неявному уменьшению его размера и, следовательно, к понижению криптографической стойкости шифра. Такого рода ослабление криптографических свойств шифра происходит, например, когда ключевое слово устанавливается по ассоциации с какими-либо именами, датами, терминами. Всякая логика в выборе ключа наносит ущерб криптографическим свойствам шифра.

Таким образом, требование случайности ключей выступает как одно из основных при их изготовлении.

Для изготовления ключей могут использоваться физические датчики и псевдослучайные генераторы со сложным законом образования ключа. Использование хорошего физического датчика более привлекательно с точки зрения обеспечения случайности ключей, но является, как правило, более дорогим и менее производительным способом. Псевдослучайные генераторы более дешевы и производительны, но привносят некоторые зависимости если не в отдельные ключи, то в совокупности ключей, что также нежелательно.

Важной частью практической работы с ключами является обеспечение секретности ключа. К основным мерам по защите ключей относятся следующие:

1) ограничение круга лиц, допущенных к работе с ключами;

2) регламентация рассылки, хранения и уничтожения ключей;

3) регламентация порядка смены ключей;

4) применение технических мер защиты ключевой информации от несанкционированного доступа.

Важной составляющей защиты информации являются протоколы связи, определяющие порядок вхождения в связь, зашифровки и передачи информации. Протокол связи должен быть построен с учетом следующих обстоятельств:

1) протокол должен защищать открытый текст и ключ от несанкционированного доступа на всех этапах передачи информации от источника к получателю сообщений;

2) протокол не должен допускать выхода в линии связи «лишней» информации, предоставляющей криптоаналитику противника дополнительные возможности дешифрования криптограмм.

Нетрудно видеть, что использование криптосистем с секретным ключом предполагает заблаговременные до сеансов связи договоренности между абонентами о сеансовых секретных ключах или их предварительную пересылку по защищенному каналу связи. К настоящему времени разработаны принципы так называемого открытого распределения ключей (ОРК) и открытого шифрования (ОШ), которые явились «новыми направлениями в криптографии», давшими начало криптографии с открытым ключом.

3.3. Проблемы реализации методов криптографической защиты в АСОД

Проблема реализации методов защиты информации имеет два аспекта [2]: разработку средств, реализующих криптографическое закрытие, и методику использования этих средств. Каждый из рассмотренных выше методов закрытия информации может быть реализован либо аппаратными, либо программными средствами. Возможность программной реализации обусловливается тем, что все методы криптографического закрытия формальны и могут быть представлены в виде конечной алгоритмической процедуры.

При аппаратной реализации все процедуры шифрования и дешифрования реализуются специальными электронными схемами. Обычно такие схемы выполняются в виде отдельных модулей, сопрягаемых с ЭВМ, терминалами пользователей, модемами связи, с другими элементами автоматизированных систем. Наибольшее распространение получили модули, реализующие комбинированные методы шифрования. При этом непременным компонентом всех аппаратно реализованных комбинаций шиф-

ров является гаммирование. Это объясняется, с одной стороны, достаточно высокой степенью закрытия с помощью гаммирования, а с другой — сравнительно простой схемой, реализующей этот метод. Обычно в качестве генератора гаммы применяют широко известный регистр сдвига с обратными (линейными или нелинейными) связями. Минимальный период порождаемой таким регистром последовательности составляет $2^N - 1$ двоичных знаков. Если, например, $N = 56$ (столько рабочих разрядов в регистре сдвига шифрующего аппарата для уже упоминавшегося DES), то $2^{56} - 1 = 10^{16}$. Если перебирать знаки этой гаммы со скоростью 1 млн знаков в секунду, то для перебора всех знаков одного периода потребуется не менее 3000 лет.

Для повышения качества генерируемой последовательности можно предусмотреть специальный блок управления работой регистра сдвига. Такое управление может заключаться, например, в том, что после зашифровки определенного объема исходного текста содержимое регистра сдвига циклически изменяется (например, сдвигается на несколько тактов). Дальнейшего повышения качества генерируемой гаммы можно достичь, если использовать три регистра сдвига, два из которых являются рабочими, а третий — управляющим. На каждом такте работы в качестве знака гаммы принимается выходной сигнал первого или второго регистра, причем выбор определяется значением выходного сигнала третьего регистра (0 — выбор первого регистра, 1 — выбор второго регистра).

Еще одна возможность улучшения криптографических свойств гаммы заключается в использовании нелинейных обратных связей. При этом улучшение достигается не за счет увеличения длины гаммы, а за счет усложнения закона ее формирования, что существенно усложняет криптоанализ. Показано, что N регистров сдвига с нелинейными обратными связями обеспечивают такую же стойкость шифра, что и 2^N регистров с линейными связями.

Технические средства криптографии

К настоящему времени разработано значительное число шифровальных аппаратов, различающихся и алгоритмом работы, и методом формирования гаммы. Рассмотрим некоторые из них (см. также гл. 7).

Например, фирмой AEG-Telefunken разработана система Telekrypt, реализующая шифрование гаммированием. Формирование гаммы осуществляется с помощью специальной процедуры с использованием двух ключей — основного, определяемого пользователем, и дополнительного, определяемого системой. Основной ключ может принимать 10^{30} различных значений, он вводится в систему с помощью специальной карты. Дополнительный ключ выбирается системой случайно, он передается на шифроаппарат получателя сообщения в начале каждого нового сообщения. Благодаря наличию дополнительного ключа появляется возможность применения двухкаскадного ключа с варьируемой периодичностью изменения. С использованием одного и того же основного ключа можно в таком случае передавать бо́льший объем информации при обеспечении требуемой надежности закрытия информации.

Шифровальное устройство Telekrypt выполнено на интегральных схемах. Для предотвращения выдачи в линию открытого исходного текста предусмотрено специальное устройство контроля. Максимальная скорость формирования гаммы достигает 10 Кбит/с.

Американская фирма Cryptex разработала устройство шифрования данных для вычислительной системы TRS-80. Устройство размером с пачку сигарет подключается к задней панели ЭВМ или шине интерфейса.

В этом устройстве применен алгоритм шифрования, который существенно отличается от DES. Хотя структура алгоритма держится в секрете, его разработчики утверждают, что достигнутая ими стойкость шифрования превышает стойкость DES. Повышения стойкости удалось добиться за счет увеличения длины исходного ключа, используемого для формирования гаммы. Ключ состоит из 10 символов кода ASCII. В двоичном исчислении длина кода равна 80 битам, что значительно превышает длину ключа DES. За счет дополнительного усложнения алгоритма (ветвление кода и задержка в использовании формируемой гаммы) удается увеличить объем пространства ключей до 2^{350} двоичных знаков. Максимальная скорость шифрования до 15 тыс. символов в минуту. Устройство имеет усиленный корпус и защиту от воздействия внешних электромагнитных полей.

Основным достоинством программных методов реализации криптографической защиты является их гибкость, т. е. возможность быстрого изменения алгоритма шифрования. При этом

можно предварительно создать пакет шифрования, содержащий программы для различных методов шифрования или их комбинаций. Смена программ будет производиться оперативно в процессе функционирования системы.

Программные средства

Основным недостатком программной реализации криптографических методов является существенно меньшее быстродействие. Например, при аппаратной реализации национального стандарта время на обработку одного блока составляет примерно 5 мкс, при программной реализации на большой ЭВМ — 100 мкс, а на специализированной мини-ЭВМ это время составляет примерно 50 мкс. Поэтому при больших объемах защищаемой информации аппаратные методы представляются более предпочтительными. Программные методы, кроме того, могут быть реализованы только при наличии в составе аппаратуры мощного процессора, тогда как шифрующие аппараты с помощью стандартных интерфейсов могут подключаться практически к любым подсистемам автоматизированных систем.

По способу использования средств закрытия информации обычно различают потоковое и блочное шифрование. При потоковом шифровании каждый символ исходного текста преобразуется независимо от других. Поэтому такое шифрование может осуществляться одновременно с передачей данных по каналу связи. При блочном шифровании одновременно преобразуется некоторый блок символов закрываемого исходного текста, причем преобразование символов в пределах блока является взаимозависимым. Может существовать зависимость и между преобразованиями символов в некоторых смежных блоках.

Проблема управления ключами

Большие трудности возникают при формировании механизма распределения ключей криптографического преобразования. Одним из принципов, которого придерживаются многие специалисты в области криптографии, является несекретность используемого способа закрытия. Предполагается, что необходимая надежность закрытия полностью обеспечивается за счет сохране-

ния в тайне ключей. Именно этим объясняется то, что алгоритм и архитектура аппаратной реализации DES были широко опубликованы в печати. Отсюда с однозначностью вытекает принципиальная важность формирования ключей, распределения их и доставки в пункты пользования. Существенными аспектами этой проблемы являются следующие соображения:

- ключи должны выбираться случайно, чтобы исключалась возможность их отгадывания на основе каких-либо ассоциаций;
- выбранные ключи должны распределяться таким образом, чтобы не было закономерностей в изменении ключей от пользователя к пользователю;
- механизм распределения ключей должен обеспечивать тайну ключей на всех этапах функционирования системы. Ключи должны передаваться по линиям связи и храниться в системе обработки только в защищенном виде;
- должна быть предусмотрена достаточно частая смена ключей, причем частота их изменения должна определяться двумя факторами: временем действия и объемом закрытой с их использованием информации.

Если система криптографического закрытия информации разработана правильно, то доступ злоумышленников к информации невозможен. Однако любое отступление от правил использования реквизитов защиты может явиться причиной утечки информации. Поэтому соблюдение этих правил является непременным условием надежной защиты информации.

Очень сложной является проблема распределения ключей в сети с большим числом пользователей. Суть проблемы состоит в том, чтобы в случае необходимости обеспечить секретную связь между любыми двумя пользователями, и только эти пользователи должны знать ключ, используемый для шифрования сообщений. Эту задачу можно решить, предоставив каждому из пользователей по $m - 1$ ключу, т. е. по одному ключу для связи с каждым из остальных пользователей. При этом необходимо распределить $m(m - 1)$ пар ключей, что представляется невыполнимой на практике задачей. Применение другого метода требует от пользователей доверия к сети. При этом каждому пользователю нужно запомнить только один ключ. Этим ключом шифруются сообщения, которые передаются к одному из узлов сети. Там оно перешифровывается и передается к следующему узлу. Этот процесс продолжается до тех пор, пока сообщение не поступит

в точку назначения. Так как при таком подходе для разрушения секретности в сети достаточно разрушить защиту лишь в одном узле, то авторы не настаивают на использовании этого метода. Они предлагают два дополнительных подхода, которые позволяют разрешить возникающие проблемы.

При первом подходе требуется, чтобы небольшое число k узлов сети функционировало в качестве узлов распределителей ключей. Каждый пользователь запоминает k ключей, каждый из которых должен применяться при связи с определенным узлом. Когда два пользователя захотят установить между собой связь, они соединяются со всеми узлами и получают случайные ключи от каждого из узлов. Затем пользователь объединяет эти ключи с помощью операции «исключающее ИЛИ» и использует результат в качестве действительного ключа для шифрования любых сообщений. Преимуществом такого подхода является уменьшение распределяемого числа ключей. Кроме того, для разрушения секретности в такой сети нужно разрушить секретность во всех узлах-распределителях ключей в сети.

При использовании второго подхода допускается, чтобы некоторые ключи были известны. При этом пользователь имеет два ключа — А и Б, ключ А используется для шифрования сообщений самого пользователя, а Б — для расшифровки сообщений, поступающих к пользователю. Необходимым условием при этом является выполнение следующих требований: пары А—Б должны формироваться с помощью простых методов, при этом, однако, вычисление ключа Б по ключу А должно представлять собой невыполнимую задачу. Ключ А является общим, так как он используется всеми пользователями системы для передачи сообщений к данному пользователю. Так как ключи А и Б связаны между собой, то требование невозможности восстановления А и Б является совершенно обязательным.

Задача управления большим числом ключей является очень важной при использовании любого метода шифрования. Известен метод, который применим для обеспечения секретности связи в системе с единственной центральной ЭВМ и большим числом терминалов.

Предположим, что каждый терминал имеет единственный главный терминальный ключ, известный на терминале и в центральной ЭВМ. В этой ЭВМ ключ может быть защищен с помощью главного ключа ЭВМ, который недоступен для любой программы пользователя. Для любого интервала работы централь-

ная ЭВМ генерирует интервальный ключ, который передается на терминал после зашифровывания с помощью главного ключа терминала. После расшифровки интервального ключа с помощью своего главного ключа терминал использует его в течение всего интервала работы с центральной ЭВМ.

Таким образом, используемые в системе ключи подразделяются на ключи для шифрования данных и ключи для шифрования ключей. Последние должны быть очень устойчивыми, поэтому для их генерации рекомендуется использовать случайные процессы. Ключи для шифрования данных используются в значительно большем количестве и сменяются значительно чаще. Поэтому их можно формировать с помощью некоторого детерминированного процесса или устройства.

Характеристики криптографических средств защиты

Важнейшей характеристикой криптографического закрытия информации является его стойкость [8, 11]. Под этим понимается тот минимальный объем зашифрованного текста, статистическим анализом которого можно вскрыть исходный текст. Таким образом, по стойкости шифра можно определить предельно допустимый объем информации, зашифровываемой при использовании одного ключа.

При выборе криптографического алгоритма для использования в конкретной разработке его стойкость, т. е. устойчивость к попыткам противоположной стороны его раскрыть, является одним из определяющих факторов. Вопрос о стойкости шифра при ближайшем рассмотрении сводится к двум взаимосвязанным вопросам:

- можно ли вообще раскрыть данный шифр;
- если да, то насколько это трудно сделать практически.

Шифры, которые вообще невозможно раскрыть, называются абсолютно или теоретически стойкими. Существование подобных шифров доказывается теоремой Шеннона, однако ценой этой стойкости является необходимость использования для шифрования каждого сообщения ключа, не меньшего по размеру самого сообщения. Во всех случаях, за исключением ряда особых, эта цена чрезмерна, поэтому на практике в основном используются шифры, не обладающие абсолютной стойкостью. Таким об-

разом, наиболее употребительные схемы шифрования могут быть раскрыты за конечное время или, что точнее, за конечное число шагов, каждый из которых является некоторой операцией над числами. Для таких схем важнейшее значение имеет понятие практической стойкости, выражающее практическую трудность их раскрытия. Количественной мерой этой трудности может служить число элементарных арифметических и логических операций, которые необходимо выполнить, чтобы раскрыть шифр, т. е. чтобы для заданного шифротекста с вероятностью, не меньшей заданной величины, определить соответствующий открытый текст. При этом в дополнение к дешифруемому массиву данных криптоаналитик может располагать блоками открытых данных и соответствующих им зашифрованных данных или даже иметь возможность получить для любых выбранных им открытых данных соответствующие зашифрованные данные. В зависимости от перечисленных и многих других неуказанных условий различают отдельные виды криптоанализа.

Все современные криптосистемы построены по принципу Кирхгофа, т. е. секретность зашифрованных сообщений определяется секретностью ключа. Это значит, что даже если сам алгоритм шифрования известен криптоаналитику, тот тем не менее не в состоянии расшифровать сообщение, если не располагает соответствующим ключом. Все классические блочные шифры, в том числе DES и ГОСТ, соответствуют этому принципу и спроектированы таким образом, чтобы не было пути вскрыть их более эффективным способом, чем полным перебором по всему ключевому пространству, т. е. по всем возможным значениям ключа. Ясно, что стойкость таких шифров определяется размером используемого в них ключа.

Приведем оценки стойкости рассмотренных выше методов шифрования. Моноалфавитная подстановка является наименее стойким шифром, так как при ее использовании сохраняются все статистические закономерности исходного текста. Уже при длине зашифрованного текста в 20—30 символов указанные закономерности проявляются в такой степени, что, как правило, позволяют вскрыть исходный текст. Поэтому такое шифрование считается пригодным только для закрытия паролей, коротких сигнальных сообщений и отдельных знаков.

Стойкость простой полиалфавитной подстановки (из подобных систем нами была рассмотрена подстановка по таблице Вижинера) оценивается значением 20^n, где n — число различных

алфавитов, используемых для замены. При использовании таблицы Вижинера число различных алфавитов определяется числом букв в ключевом слове. Усложнение полиалфавитной подстановки существенно повышает ее стойкость. Монофоническая подстановка может быть весьма стойкой (и даже теоретически нераскрываемой), однако строго монофоническую подстановку, в которой все символы имеют равные вероятности появления, реализовать на практике трудно, а любые отклонения от монофоничности снижают реальную стойкость шифра.

Стойкость простой перестановки однозначно определяется размерами используемой матрицы. Например, при использовании матрицы 16×16 число возможных перестановок достигает $1{,}4 \times 10^{26}$. Такое число вариантов невозможно перебрать даже с использованием современных ЭВМ. Стойкость усложненных перестановок может быть выше. Однако следует иметь в виду, что при шифровании перестановкой полностью сохраняются вероятностные характеристики исходного текста, что облегчает криптоанализ.

Стойкость гаммирования однозначно определяется длиной периода гаммы. В настоящее время реальным становится применение бесконечной гаммы, при использовании которой теоретическая стойкость зашифрованного текста также будет бесконечной.

Можно отметить, что для надежного закрытия больших массивов информации наиболее пригодны гаммирование и усложненные перестановки и подстановки.

При использовании комбинированных методов шифрования стойкость шифра равна произведению стойкостей отдельных методов. Поэтому комбинированное шифрование является наиболее надежным способом криптографического закрытия. Именно такой метод был положен в основу работы всех известных в настоящее время шифрующих аппаратов (в том числе и аппарата, реализующего DES).

Рассмотренные значения стойкости шифров являются потенциальными величинами. Они могут быть реализованы при строгом соблюдении правил использования криптографических средств защиты. Основными из этих правил являются: сохранение в тайне ключей, исключение дублирования и достаточно частая смена ключей. Остановимся на двух последних правилах. Под дублированием здесь понимается повторное шифрование одного и того же отрывка текста с использованием тех же клю-

чей (например, если при первом шифровании имел место сбой). Нарушение этого правила резко снижает надежность шифрования, так как исходный текст может быть восстановлен с помощью статистического анализа двух вариантов текста.

Важнейшим правилом использования криптографических средств является достаточно частая смена ключей. Причем эту частоту можно определять и исходя из длительности использования ключа, и объема зашифрованного текста. При этом смена ключей по временному графику является защитной мерой против возможного их хищения, а смена после шифрования определенного объема текста — от раскрытия шифра статистическими методами.

До сих пор мы предполагали, что злоумышленник не обладает никакой другой информацией, кроме отрезка зашифрованного текста. Однако для крупных современных систем коллективного пользования, для которых более характерно территориальное распределение отдельных элементов, злоумышленнику может стать доступной и дополнительная информация, которая может существенно облегчить криптоанализ.

На практике, например, может встретиться ситуация, когда злоумышленник имеет возможность направить в систему ряд специально подобранных сообщений и получить их от системы в зашифрованном виде. Особенно опасна такая ситуация при использовании перестановок. При использовании полиалфавитных подстановок это облегчает определение количества используемых алфавитов, а при использовании гаммирования — закономерности формирования гаммы. Более того, если злоумышленнику удается полностью перехватить зашифрованное сообщение, то он может попытаться получить «куски» шифрованного и соответствующего исходного текстов, предполагая наличие в сообщении служебных слов: адреса отправителя, даты, времени, грифа секретности и т. п. Все это может быть использовано при криптоанализе зашифрованного текста.

Оценим далее некоторые технико-экономические показатели криптографических средств.

Расходы на программную реализацию криптографических методов защиты определяются сложностью алгоритмов прямого и обратного преобразований. Оценка затрат на эти цели производится по тем же методикам, что и оценка затрат на другие компоненты программного обеспечения. При этом, однако, надо иметь в виду, что для подавляющего большинства методов

закрытия прямое и обратное преобразования осуществляются по одному и тому же алгоритму.

Расходы на аппаратную реализацию могут быть оценены приближенно стоимостью шифрующей аппаратуры. По данным зарубежной печати, такие аппараты в настоящее время поступают на коммерческий рынок. Выпускаются и поступают в продажу, например, шифрующие аппараты, реализующие DES.

Одной из наиболее важных технико-экономических характеристик систем криптографического закрытия является трудоемкость метода шифрования, которую можно выразить числом элементарных операций, необходимых для шифрования одного символа исходного текста.

При шифровании подстановкой необходимо выполнить выбор алфавита и поиск необходимого символа в этом алфавите. При полиалфавитной подстановке дополнительно необходимо выполнить выбор очередного алфавита. Основными процедурами, выполняемыми при перестановке, являются выбор знаков исходного текста, определение места записи и запись в поле шифрованного текста. Трудоемкость аналитического преобразования определяется сложностью используемого преобразования. Если, например, используется правило перемножения матрицы и вектора, то для шифрования одного символа необходимо осуществить m умножений и $m - 1$ сложений, где m — размерность матрицы.

При шифровании гаммированием основная трудоемкость связана с формированием гаммы. Если, например, для этой цели применен линейный рекуррентный генератор, реализующий алгоритм вида $t_{i+1} = (at_i + c) \bmod m$, где a и c — константы, то нетрудно заметить, что для формирования каждого знака гаммы необходимо выполнить не менее трех операций.

Таким образом, наиболее трудоемкими являются аналитические преобразования, затем по мере снижения трудоемкости следует гаммирование, перестановки и замены.

Задания для дешифровки текстов, зашифрованных методами перестановки

1. Изречение немецкого философа Фридриха Ницше:
   ОЬТСО НЙАЧУ ЛСВТЯ РЕВЕН ИЛЕТИ ДЕБОП
2. Изречение немецкого ученого-гуманиста Эразма Роттердамского:
   ЙЫТЫР КСТНА ЛАТЕН ТЕАДЗ ОСИИЦ АТУПЕ РОООО

3. Изречение чешского писателя Карела Чапека:

   ЕЛЙГС АМОЛТ ЕМИЬР УНСЕО ЕАПОМ МОООП МОЖОЕ ОЕКШО ШРАОЬ АЙОСЙ ДОДНДР ОЕЕУО

4. Высказывание польского писателя-фантаста Станислава Лема:

   ТОУМА МЕЖЕЧ ЫАООО ОММГЗ ЕСНМЕ ДЕООО ЧЫАОД НЛОТМ УМООО ТДЕРО ЕОЧОМ МОООО

5. Изречение датского ученого-физика Нильса Бора:

   ТПРРО УСЕБД ООДИН ОБЖВЛ ООЕЕУ ИОЧОЕ НАДТО ЩНЬЕУ ОТДБУ

6. Изречение французского философа Жана-Поля Сартра:

   ИНККО ОТСОЧ ЯЧПОТ ЕАРЕЯ ОЛНЕА АЕМТК ОНСТШ

7. Высказывание американского писателя Джона Стейнбека:

   АРЕНО ЫЕТМО ЕЖОИБ ЕДДЖЙ ЯПТВС ОДОКМ ПСИОЖ ОЙЛГО ОИЕНТ

Контрольные вопросы

1. Что такое криптология?
2. Что такое ключ?
3. Определите понятие «криптологический алгоритм».
4. Какие функции выполняет криптологический протокол?
5. Что из себя представляет криптосистема?
6. Дайте определение стойкости криптосистемы.
7. Какие основные типы криптосистем вы знаете?
8. Дайте общее определение цифровой подписи.
9. Объясните суть преобразований — перестановка и замена.
10. Приведите пример табличной перестановки с использованием ключевого слова.
11. Что из себя представляет система шифрования с использованием таблицы Вижинера?
12. Что из себя представляет система шифрования Вернама? Укажите ее особенности.
13. Что из себя представляет симметричная криптографическая система?
14. Что из себя представляет блочная симметричная криптографическая система?
15. Объясните, что такое композиционный блочный шифр и итерационный блочный шифр.
16. Объясните суть алгоритма DES и укажите на его особенности.
17. В каких режимах может работать алгоритм DES?
18. Дайте описание отечественного алгоритма криптографического преобразования данных (ГОСТ 28147—90) и его отличительных особенностей.

19. Какие режимы имеет отечественный алгоритм криптографического преобразования данных (ГОСТ 28147—90)?
20. Чем отличаются поточные симметричные криптографические системы?
21. Какими характеристиками оценивается стойкость криптографических систем?
22. Что подразумевается под понятием «вычислительная сложность алгоритма»?
23. Для каких целей применяются случайные последовательности и простые числа в криптографии?
24. Чем характеризуются односторонние функции с секретом?
25. Чем характеризуется криптографическая система с открытым ключом?
26. В чем заключается суть электронной цифровой подписи?
27. Как проверяется целостность сообщения?

Глава 4
ЗАЩИТА ИНФОРМАЦИИ В ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРАХ

Персональные компьютеры (ПК) обладают всеми свойствами ЭВМ других классов, поэтому фактически все проблемы защиты информации в построенных на их основе системах и подходы к защите аналогичны рассмотренным выше. Однако персональным компьютерам присущ ряд таких свойств, которые, с одной стороны, благоприятствуют защите, а с другой — затрудняют ее и усложняют.

4.1. Особенности защиты информации в персональных ЭВМ

К основным из указанных свойств относятся:

- малые габариты и вес, что делает их не просто транспортабельными, а легко переносимыми;
- наличие встроенного внутреннего запоминающего устройства (ЗУ) большого объема, сохраняющего записанные данные после выключения питания;
- наличие сменного ЗУ большого объема и малых габаритов;
- наличие устройств сопряжения с каналами связи и широкое распространение технологий и программ дистанционного доступа;
- оснащенность программным обеспечением с широкими функциональными возможностями;
- массовость производства и распространения;
- относительно низкая стоимость.

Перечисленные и некоторые другие особенности создали объективные предпосылки для массового распространения ПК

практически во всех сферах деятельности современного общества, резкого повышения интенсивности циркуляции информации, децентрализации процессов ее хранения и обработки, существенного изменения структуры и содержания информационных технологий.

С точки зрения общих подходов к защите особенно существенными являются две особенности ПК. Как известно, в АСОД, базирующихся на больших ЭВМ, наряду с защитой информации непосредственно в ЭВМ такое же решающее (если не большее) значение имеет общая организация защиты: организация и обеспечение технологических процессов циркуляции и обработки потоков информации; охрана территории, зданий и помещений; подбор, обучение и организация работы персонала и т. п. В АСОД с большими ЭВМ основные вопросы защиты, как правило, решают подготовленные специалисты-профессионалы в данной области. Для персональных же ЭВМ, во-первых, вопросы общей организации защиты могут быть решены физической изоляцией (например, размещением ПК в отдельной комнате, закрываемой на замок), поэтому превалирующую роль играет внутренняя защита, во-вторых, в большинстве случаев заботу о защите информации должны проявлять сами пользователи, которые не только не являются профессионалами в области защиты, но нередко вообще имеют лишь навыки непосредственного решения ограниченного набора задач. Этими особенностями и обусловлена необходимость самостоятельного рассмотрения вопросов защиты информации в персональных ЭВМ с акцентированием внимания именно на внутренней защите.

Угрозы информации в персональных ЭВМ

Применительно к защите информации в ПК справедливо практически все сказанное ранее относительно защиты ее в АСОД вообще. Естественно, это относится и к вопросу об угрозах информации [18]. Однако специфические особенности архитектурного построения и способов использования ПК позволяют конкретизировать значительную часть угроз (каналов утечки) информации. Характерные для ПК каналы принято классифицировать по типу средств, которые используются в целях несанкционированного получения по ним информации,

причем выделяются три типа средств: человек, аппаратура, программа.

Группу каналов, в которых основным средством несанкционированного получения информации является человек, составляют:

- хищение носителей информации (магнитных дисков и дискет, распечаток и т. д.);
- чтение или фотографирование информации с экрана;
- чтение или фотографирование информации с распечаток.

В группе каналов, основным средством использования которых служит аппаратура, выделяют:

- подключение к устройствам ПК специальной аппаратуры, с помощью которой можно уничтожать или регистрировать защищаемую информацию;
- регистрацию с помощью специальных средств электромагнитных излучений устройств ПК в процессе обработки защищаемой информации.

Группу каналов, основное средство использования которых — программы, образуют:

- программный несанкционированный доступ к информации;
- уничтожение (искажение) или регистрация защищаемой информации с помощью программных закладок или ловушек;
- чтение остаточной информации из ОЗУ;
- программное копирование информации с магнитных носителей.

Как известно, современные ЭВМ могут работать как локально (изолированно), так и в сопряжении с другими ЭВМ, причем как в пределах одной АСОД, так и в сопряженном режиме с другими АСОД. По способу реализации сопряжение может быть организационным (посредством машинных носителей) и техническим (посредством автоматизированного канала связи).

Тогда полный базовый перечень тех участков (мест), в которых могут находиться защищаемые данные, может быть представлен в следующем виде: системная плата ПК; накопители на гибких магнитных дисках (НГМД) или CD/DVD; НЖМД (несменяемый накопитель на магнитном диске); монитор (дисплей); печатающее устройство; каналы связи. Защите подлежат данные, связанные с каждым из перечисленных мест.

Носители информации могут быть персонального, группового и общего использования.

Для разработки мероприятий защиты информации необходимы следующие исходные характеристики элементов защиты:

- возможные объемы находящейся в них информации;
- возможная продолжительность пребывания информации;
- возможные угрозы информации;
- возможные средства защиты.

Как и для объектов защиты, значения этих характеристик для всех элементов защиты целесообразно свести в специальный каталог.

В соответствии с изложенным каждый пользователь ПК может применительно к своим условиям составить перечень потенциально возможных угроз его информации и на этой основе целенаправленно решать вопросы надежной ее защиты.

На формирование множества возможных подходов к защите информации в ПК и выбор наиболее целесообразного из них в конкретных ситуациях определяющее влияние оказывают следующие факторы:

- цели защиты;
- потенциально возможные способы защиты;
- имеющиеся средства защиты.

Цели защиты

Основные цели защиты информации включают как минимум следующий перечень:

- обеспечение физической и логической целостности данных;
- предупреждение несанкционированной модификации данных;
- предупреждение несанкционированного копирования/получения информации.

Обеспечение целостности информации в ПК. Актуальность данного вида защиты информации в ПК носит общий характер независимо от того, какая информация обрабатывается, поэтому знания и навыки обеспечения целостности необходимы всем пользователям ПК.

Прежде всего, следует знать и помнить, что нарушения целостности информации в ПК, как и в любой другой автоматизированной системе, могут быть случайными и преднамеренными. Основными разновидностями случайных угроз являются отказы, сбои, ошибки, стихийные бедствия и побочные явления, а кон-

кретными источниками их проявления — технические средства, программы и пользователи. С учетом современного состояния технических и программных средств ПК, а также способов и средств их использования к наиболее реальным угрозам целостности информации случайного характера следует отнести ошибки пользователей. Основными из этих ошибок являются неправильные обращения к серийным компонентам программного обеспечения.

Гораздо большую опасность целостности информации в ПК представляют преднамеренные угрозы, создаваемые людьми в злоумышленных целях. Такая угроза может быть непосредственной, если злоумышленник получает доступ к ПК, и опосредованной, когда угроза создается с помощью промежуточного носителя, чаще всего с помощью дискеты. Из преднамеренных угроз наибольшее распространение получили так называемые разрушающие программные средства (РПС): электронные вирусы, черви, троянские кони и др. Они же представляют и наибольшую опасность целостности информации в ПК.

Обеспечение физической целостности. Физическая целостность информации в ПК зависит от целостности самого ПК, целостности дисков и дискет, целостности информации на дисках, дискетах и полях оперативной памяти. В широком спектре угроз целостности информации в ПК следует обратить особое внимание на угрозы, связанные с недостаточной квалификацией большого числа владельцев ПК. В этом плане особо опасной представляется возможность уничтожения или искажения данных на жестком диске (винчестере), на котором могут накапливаться очень большие объемы данных, самим пользователем.

Предупреждение несанкционированной модификации. Весьма опасной разновидностью несанкционированной модификации информации в ПК является действие вредоносных программ (компьютерных вирусов), которые могут разрушать или уничтожать программы или массивы данных. Данная опасность приобретает актуальность в связи с тем, что среди владельцев ПК общепринятой является практика обмена дискетами (а также CD/DVD). Получаемый сменный носитель может содержать весьма неприятный сюрприз.

Предупреждение несанкционированного получения информации, находящейся в ПК. Данная цель защиты приобретает особую актуальность в тех случаях, когда хранимая или обрабатываемая

информация содержит тайну того или иного характера (государственную, коммерческую и т. п.). Возможности несанкционированного получения информации в современных ПК очень широки и разнообразны, поэтому данный вид защиты требует серьезного внимания.

Предупреждение несанкционированного копирования информации. Актуальность данной разновидности защиты определяется следующими тремя обстоятельствами:

- накопленные массивы информации все больше становятся товаром;
- все более широкое распространение получает торговля компьютерными программами;
- накопители на гибких МД и оптические дисководы с перезаписью создают весьма благоприятные условия для широкомасштабного копирования информации ПК.

Защита от копирования заключается в предупреждении возможностей несанкционированного снятия копии с информации, находящейся в ОЗУ ЭВМ или на МД (гибком или жестком), в целях злоумышленного ее использования. Нетрудно видеть, что данная защита может быть представлена составной частью защиты от несанкционированного получения информации. Выделение же ее в самостоятельный вид защиты обусловлено, главным образом, стремлением защитить авторские и коммерческие интересы разработчиков и собственников программ для ПК. Как известно, программы для ЭВМ законодательно признаны интеллектуальной собственностью, и уже вполне сформировался рынок их распространения на коммерческой основе. В условиях рыночных отношений это с неизбежностью привело к так называемому программному пиратству, т. е. к злоумышленному присвоению чужих программ, причем, как в целях присвоения авторства, так и в целях наживы.

Защищаемые программы для ПК могут находиться в ОЗУ, на ГМД и на ЖМД (бумажные носители здесь не рассматриваются, поскольку их защита должна осуществляться традиционными способами и методами). Защита программ, находящихся в ОЗУ и на ЖМД, ничем не отличается от рассмотренной выше защиты от НСД. Поэтому здесь основное внимание сосредоточено на защите от копирования ГМД (дискет), поскольку эта разновидность пиратства получила достаточно широкое распространение, а защита от него носит сугубо специфический характер.

Под системой защиты программы от копирования понимается система, которая обеспечивает выполнение ею своих функций только при опознании некоторого уникального, не поддающегося копированию элемента, называемого ключевым. В качестве ключевого элемента могут выступать дискета, определенная часть аппаратуры ПК или специальное устройство, подключаемое к ПК.

Основные функции, которые выполняют системы защиты программы от копирования, заключаются в следующем:

- идентификация (т. е. присвоение индивидуального трудноподделываемого отличительного признака) той среды (дискеты или ПК), из которой будет запускаться защищаемая программа;
- аутентификация (опознавание) той среды, из которой поступает запрос на копирование защищаемой программы;
- регистрация санкционированного копирования;
- реагирование на попытки несанкционированного копирования;
- противодействие изучению алгоритмов работы системы защиты.

Для идентификации дискет (CD/DVD) распространение получили два способа: нанесение повреждения на часть поверхности и нестандартное форматирование дискеты. Одним из достаточно надежных методов идентификации по первому способу считается создание так называемой лазерной дыры, заключающееся в прожигании дискеты в некотором месте лазерным лучом. Доказано, что создание в дискете-копии такой же метки и в том же самом месте, что и на дискете-оригинале, весьма сложно. Второй способ идентификации защищаемой дискеты заключается в осуществлении некопируемого ее форматирования. Способ достаточно надежный, однако задача нахождения некопируемого формата носит эмпирический характер, и ее решение возможно лишь при детальном знании всех тонкостей процессов функционирования контроллера. К настоящему времени разработан ряд методов реализации данного способа идентификации: нарушение последовательности секторов на дорожке дискеты, изменение межсекторной дистанции, форматирование с кодом длины 0 или 1, контроль длины дорожки, прерывание операции и выключение мотора и др.

Реагирование на попытки несанкционированного копирования дискеты может быть различным: отказ в исполнении запро-

са, предупреждение злоумышленника о более серьезных санкциях, уничтожение защищаемой программы (после первой попытки или после нескольких попыток) и т. п.

Последняя из перечисленных выше функций системы защиты от копирования — противодействие изучению алгоритмов работы системы защиты — предусмотрена для того, чтобы воспрепятствовать злоумышленнику в изучении структуры и содержания реализованной на дискете системы защиты в целях ее преодоления (нейтрализации). Важность данной функции определяется тем, что квалифицированный системный программист, в общем случае, может определить (восстановить) логику работы любого модуля всей системы защиты и найти способы ее преодоления.

Изучение логики работы программы может осуществляться двумя способами: дисассемблированием (преобразованием выполняемого программного модуля в листинг исходного текста) и трассировкой программы (выполнением ее в такой среде, которая позволяет осуществлять доступ к регистрам и областям памяти, останов исполнения программы по некоторым адресам и т. п.). Отсюда следует, что основное содержание рассматриваемой функции должно заключаться в создании надежных препятствий на пути дисассемблирования и трассировки программных модулей системы защиты. К настоящему времени разработано значительное число программных систем защиты дискет от копирования.

4.2. Защита ПК от несанкционированного доступа

Как показывает практика, несанкционированный доступ (НСД) представляет одну из наиболее серьезных угроз для злоумышленного завладения защищаемой информацией в современных АСОД. Как ни покажется странным, но для ПК опасность данной угрозы по сравнению с большими ЭВМ повышается, этому способствуют следующие объективно существующие обстоятельства:

- подавляющая часть ПК располагается непосредственно в рабочих комнатах специалистов, что создает благоприятные условия для доступа к ним посторонних лиц;

- многие ПК служат коллективным средством обработки информации, что обезличивает ответственность, в том числе и за защиту информации;
- современные ПК оснащены несъемными накопителями на ЖМД большой емкости, причем информация на них сохраняется даже в обесточенном состоянии;
- накопители на ГМД (CD/DVD) производятся в таком массовом количестве, что уже используются для распространения информации так же, как и бумажные носители;
- первоначально ПК создавались именно как персональное средство автоматизации обработки информации, а потому и не оснащались специально средствами защиты от НСД.

В силу сказанного те пользователи, которые желают сохранить конфиденциальность своей информации, должны особенно позаботиться об оснащении используемой ПК высокоэффективными средствами защиты от НСД.

Основные механизмы защиты ПК от НСД могут быть представлены следующим перечнем:

- физическая защита ПК и носителей информации;
- опознавание (аутентификация) пользователей и используемых компонентов обработки информации;
- разграничение доступа к элементам защищаемой информации;
- криптографическое закрытие защищаемой информации, хранимой на носителях (архивация данных);
- криптографическое закрытие защищаемой информации в процессе непосредственной ее обработки;
- регистрация всех обращений к защищаемой информации.

Ниже излагаются общее содержание и способы использования перечисленных механизмов.

Физическая защита ПК и носителей информации

Содержание физической защиты общеизвестно, поэтому детально обсуждать ее здесь нет необходимости. Заметим только, что ПК лучше размещать в надежно запираемом помещении, причем, в рабочее время помещение должно быть закрыто или ПК должен быть под наблюдением законного пользователя. При обработке закрытой информации в помещении могут находиться

только лица, допущенные к обрабатываемой информации. В целях повышения надежности физической защиты в нерабочее время ПК следует хранить в опечатанном сейфе.

Опознавание (аутентификация) пользователей и используемых компонентов обработки информации

В концептуальном плане решение данной задачи принципиально не отличается от аналогичной задачи, решаемой в любой АСОД: система защиты должна надежно определять законность каждого обращения к ресурсам, а законный пользователь должен иметь возможность убедиться, что ему предоставляются именно те компоненты (аппаратура, программы, массивы данных), которые ему необходимы.

Для опознавания пользователей к настоящему времени разработаны и нашли практическое применение следующие способы:

- с использованием простого пароля;
- в диалоговом режиме с использованием нескольких паролей и/или персональной информации пользователей;
- по индивидуальным особенностям и физиологическим характеристикам человека (отпечатки пальцев, геометрия руки, голос, персональная роспись, структура сетчатки глаза, фотография и некоторые другие);
- с использованием радиокодовых устройств;
- с использованием электронных карточек.

Рассмотрим коротко перечисленные способы.

Распознавание по простому паролю заключается в том, что каждому зарегистрированному пользователю выдается персональный пароль, который он должен держать втайне и вводить в ЗУ ЭВМ при каждом обращении к ней. Специальная программа сравнивает введенный пароль с эталоном, хранящимся в ЗУ ЭВМ, и при совпадении паролей запрос пользователя принимается к исполнению. Простота способа очевидна, но очевидны и явные недостатки: пароль может быть утерян или подобран перебором возможных комбинаций, а искусный злоумышленник может проникнуть в ту область ЗУ, в которой хранятся эталонные пароли. Попытки преодолеть указанные недостатки, естественно, ведут к усложнению способа.

Опознавание в диалоговом режиме может быть осуществлено по следующей схеме. В файлах механизмов защиты заблаговре-

менно создаются записи, содержащие персонифицирующие пользователя данные (дата рождения, рост, вес, имена и даты рождения родных и близких и т. п.) или достаточно большой и упорядоченный набор паролей. При обращении пользователя программа механизма защиты предлагает пользователю назвать некоторые данные из имеющейся записи, которые сравниваются с данными, хранящимися в файле. По результатам сравнения принимается решение о допуске. Для повышения надежности опознавания запрашиваемые у пользователя данные могут выбираться каждый раз разные. Достоинства и недостатки данного способа очевидны.

Опознавание по индивидуальным особенностям и физиологическим характеристикам может быть весьма надежным, но для его реализации необходима специальная аппаратура для съема и ввода соответствующих параметров и достаточно сложные программы их обработки и сравнения с эталоном. Все это в настоящее время вполне разрешимо, однако сопряжено с удорожанием и усложнением аппаратуры и программ ПК. В силу сказанного данный способ применительно к ПК пока не получил сколько-нибудь значительного распространения. Заманчивым по сравнительной простоте и доступности может оказаться опознавание пользователя по параметрам его работы с клавиатурой ПК (скорость набора текста, интервалы между нажатием клавиш и др.), которые тоже носят сугубо индивидуальный характер.

Опознавание посредством радиокодовых устройств, как это следует из самого названия, заключается в том, что изготавливаются специальные устройства, каждое из которых может генерировать радиосигналы, имеющие индивидуальные характеристики. ПК оснащается программно-аппаратными средствами приема (например, при приближении устройства к экрану дисплея), регистрации и обработки генерируемых сигналов. Каждому зарегистрированному пользователю выдается такое устройство, а его параметры заносятся в ЗУ механизмов защиты. Надежность опознавания по данному способу может быть высокой, однако такие устройства персонифицируют владельца, а не персону, поэтому похищение устройства дает злоумышленнику реальные шансы несанкционированного доступа.

Опознавание по идентификационным карточкам заключается в том, что изготавливаются специальные карточки, на которые наносятся данные, персонифицирующие пользователя: персональный идентификационный номер, специальный шифр или

код и т. п. Эти данные на карточку заносятся в зашифрованном виде, причем ключ шифрования может быть дополнительным идентифицирующим параметром, поскольку он может быть известен только пользователю, вводится им каждый раз при обращении к системе и уничтожается сразу же после использования. Опознавание по карточкам может быть очень надежным, однако для его реализации необходимы предприятия-изготовители карточек, а ПК должна быть оснащена устройством считывания данных с карточки. Поскольку все это сопряжено со значительными дополнительными расходами, то данный способ опознавания оказывается эффективным при его использовании в больших территориально распределенных сетях, где он в последнее время находит все большее применение, особенно в автоматизированных банковских системах.

Для опознавания компонентов обработки данных, т. е. ЭВМ, ОС, программ функциональной обработки, массивов данных (такое опознавание особенно актуально при работе в сети ЭВМ) используются следующие средства:

- специальные аппаратные блоки-приставки (для опознавания ЭВМ, терминалов, внешних устройств);
- специальные программы, реализующие процедуру «запрос—ответ»;
- контрольные суммы (для опознавания программ и массивов данных).

Опознавание с помощью блоков-приставок заключается в том, что технические средства оснащаются специальными устройствами, генерирующими индивидуальные сигналы. В целях предупреждения перехвата этих сигналов и последующего их злоумышленного использования они могут передаваться в зашифрованном виде, причем периодически может меняться не только ключ шифрования, но и используемый способ (алгоритм) криптографического преобразования.

Программное опознавание по процедуре «запрос—ответ» заключается в том, что в ЗУ опознающего и опознаваемого объектов заблаговременно вносятся достаточно развитые массивы идентифицируемых данных. Тогда опознающий объект в диалоговом режиме запрашивает те или иные данные из массива опознаваемого объекта и сравнивает их с соответствующими данными своего массива. Опять-таки в целях предупреждения перехвата и злоумышленного использования передаваемых идентифицирующих данных может осуществляться их криптографическое закрытие.

Опознавание по контрольной сумме заключается в том, что для программ и массивов данных заблаговременно вычисляются их контрольные суммы (или другие величины, зависящие от содержания опознаваемых объектов). Дальнейшая процедура опознавания очевидна.

Разграничение доступа к элементам защищаемой информации

Разграничение доступа заключается в том, чтобы каждому зарегистрированному пользователю предоставить возможности беспрепятственного доступа к информации в пределах его полномочий и исключить возможности превышения своих полномочий. В этих целях разработаны и реализованы на практике методы и средства разграничения доступа к устройствам ЭВМ, к программам обработки информации, к полям (областям ЗУ) и к массивам (базам) данных. Само разграничение может осуществляться несколькими способами, а именно:

- по уровням (кольцам) секретности;
- специальным спискам;
- так называемым матрицам полномочий;
- специальным мандатам.

Приведем краткую характеристику перечисленных способов.

Разграничение доступа по уровням (кольцам) секретности заключается в том, что защищаемые данные распределяются по массивам (базам) таким образом, чтобы в каждом массиве (каждой базе) содержались данные одного уровня секретности (например, только с грифом «конфиденциально» или только «секретно», или только «совершенно секретно», или каким-либо другим). Каждому зарегистрированному пользователю предоставляется вполне определенный уровень допуска (например, «секретно», «совершенно секретно» и т. п.). Тогда пользователю разрешается доступ к массиву (базе) своего уровня и массивам (базам) низших уровней и запрещается доступ к массивам (базам) более высоких уровней.

Разграничение доступа по специальным спискам заключается в том, что для каждого элемента защищаемых данных (файла, базы, программы) составляется список всех тех пользователей, которым предоставлено право доступа к соответствующему элементу, или, наоборот, для каждого зарегистрированного пользователя составляется список тех элементов защищаемых данных, к которым ему предоставлено право доступа.

Разграничение доступа по матрицам полномочий предполагает формирование двумерной матрицы, по строкам которой содержатся идентификаторы зарегистрированных пользователей, а по столбцам — идентификаторы защищаемых элементов данных. Элементы матрицы содержат информацию об уровне полномочий соответствующего пользователя относительно соответствующего элемента (табл. 4.1). Например, при размерах элементов матрицы в 2 бита их содержание может быть следующим: 00 — доступ запрещен, 01 — разрешено только чтение, 10 — разрешена только запись, 11 — разрешены и чтение, и запись.

Таблица 4.1. **Пример матрицы полномочий**

Пользователи	Ресурсы		
	Каталог d:\work	Каталог d:\book	Каталог d:\test
YM07	10	01	10
YK16	10	10	00
ZN21	00	10	01
.....	.....	.....	.....
HY12	10	00	00

Недостатком метода разграничения доступа на основе матрицы полномочий является то, что с увеличением масштаба ВС данная матрица может оказаться слишком громоздкой. Преодолеть данный недостаток можно путем применения следующих рекомендаций по сжатию матрицы установления полномочий:

- объединение пользователей, имеющих идентичные полномочия в группы;
- объединение ресурсов, полномочия на доступ к которым совпадают;
- комбинирование метода разграничения доступа на основе матрицы полномочий с методом разграничения по уровням секретности.

Разграничение доступа по мандатам есть способ разового разрешения на допуск к защищаемому элементу данных. Заключается он в том, *что* каждому защищаемому элементу присваивается персональная уникальная метка, после этого доступ к этому элементу будет разрешен только тому пользователю, который в своем запросе предъявит метку элемента (мандат), которую ему может выдать администратор защиты или владелец элемента.

Криптографическое закрытие защищаемой информации, хранимой на носителях (архивация данных)

Данный механизм, как следует из самого названия, предназначается для обеспечения защиты информации, которая подлежит продолжительному хранению на машинных носителях. Но при разработке методов его реализации имелась в виду и еще одна весьма важная цель — уменьшение объемов ЗУ, занимаемых хранимой информацией. Указанные цели и выступают в качестве основных критериев при поиске оптимальных вариантов решения задачи архивации данных.

Для предупреждения несанкционированного доступа к хранимой информации могут и должны использоваться все три рассмотренных выше механизма. Но особенно эффективными являются методы криптографического преобразования информации, поэтому они составляют основу практически всех известных механизмов архивации. Уменьшение объемов ЗУ достигается применением так называемых методов сжатия данных, сущность которых заключается в использовании таких систем кодирования архивируемых данных, которые при сохранении содержания информации требуют меньшего объема памяти носителя. Но тогда естественной представляется идея выбора такого способа кодирования, который удовлетворял бы обоим требованиям: обеспечивал бы уменьшение объема ЗУ и обладал бы требуемой надежностью криптографической защиты.

Классическим примером такого способа кодирования может служить достаточно известный код Хаффмана, суть которого заключается в том, что для кодирования часто встречающихся символов (букв) используются более короткие кодовые комбинации, чем для кодирования редко встречающихся. Нетрудно видеть, что если таблицу кодирования держать в секрете, то закодированный таким образом текст будет не только короче исходного, но и недоступен для чтения посторонними лицами.

Криптографическое закрытие защищаемой информации в процессе непосредственной ее обработки. Назначение указанного метода очевидно, а целесообразность применения определяется возможностями несанкционированного доступа к защищаемой информации в процессе непосредственной обработки. Если же обработка информации осуществляется в сетевой среде, то без применения криптографических средств надежное предотвраще-

ние несанкционированного доступа к ней практически не может быть обеспечено. Этим и обусловлено то достаточно большое внимание, которое уделяется разработке криптографических средств, ориентированных на применение в ПК.

Для иллюстрации приведем краткое описание одной из серий криптографических устройств, получившей название «Криптон».

Криптон — это ряд выполненных в виде одноплатных устройств программно-аппаратных комплексов, обеспечивающих шифрование и дешифрование информации в ЭВМ и в информационно-вычислительных сетях. Устройства содержат датчики случайных чисел для генерации ключей и узлы шифрования, реализованные аппаратно в специализированных однокристальных микроЭВМ. Открытый интерфейс позволяет внедрять устройства Криптон в любые системы и дополнять программным обеспечением специального назначения.

Устройства Криптон позволяют осуществлять:

- шифрование и дешифрование файлов, групп файлов и разделов дисков;
- разграничение и контроль доступа к компьютеру;
- защиту информации, передаваемой по открытым каналам связи и сетям межмашинного обмена;
- электронную подпись документов;
- прозрачное шифрование жестких и гибких дисков.

Для криптографического преобразования защищаемых данных использован алгоритм отечественного стандарта ГОСТ 28147—89. Длина ключа — 256 бит, причем предусмотрено 7 типов ключевых систем, любую из которых пользователь может выбрать по своему усмотрению. Конкретные ключи в пределах выбранного типа ключевой системы пользователь может изготовить самостоятельно или заказать в специализированном центре.

На базе устройств Криптон разработана и серийно выпускается система Криптон-ИК, обеспечивающая дополнительно к перечисленным выше функциям также чтение, запись и защиту данных, хранящихся на так называемых интеллектуальных идентификационных карточках, получающих в последнее время широкое применение как в виде дебетно/кредитных карточек при безналичных расчетах, так и в виде средства хранения прав доступа, ключей шифрования и другой конфиденциальной информации.

Регистрация всех обращений к защищаемой информации и исключение несанкционированного доступа

Регистрация обращений к защищаемой информации ПК позволяет решать ряд важных задач, способствующих существенному повышению эффективности защиты, поэтому оно непременно присутствует во всех системах защиты информации.

Основные задачи, при решении которых заметную роль играет регистрация обращений, могут быть представлены следующим перечнем:

- контроль использования защищаемой информации;
- выявление попыток несанкционированного доступа к защищаемой информации;
- накопление статистических данных о функционировании систем защиты.

Вообще говоря, регистрация обращений может быть осуществлена серийными средствами операционных систем ПК. Однако учитывая специфичность и избирательность необходимой регистрации в системах защиты, разработчики этих систем предпочитают создавать свои версии программ регистрации.

Проведенное рассмотрение вопросов предупреждения несанкционированного доступа достаточно убедительно показывает, что они, во-первых, составляют основу систем защиты информации в ПК, а во-вторых, что их реализация сопряжена с решением широкого спектра разноплановых задач. Теоретические исследования и практический опыт показали, что наиболее эффективным способом их решения является создание комплексных систем защиты ПК от несанкционированного доступа.

Для защиты от несанкционированного входа в персональную компьютерную систему могут использоваться как общесистемные, так и специализированные программные средства защиты.

К общесистемным средствам относится утилита Setup, входящая в состав BIOS и предназначенная для настроек аппаратных параметров компьютера. Для реализации рассматриваемого вида защиты необходимо с помощью данной утилиты установить следующие параметры загрузки компьютера:

- порядок загрузки операционной системы (ОС), задающий первичную загрузку с жесткого диска (устройство `c:`);
- запрос пароля перед загрузкой операционной системы. Установка первичной загрузки с жесткого диска необходима

для предотвращения возможности загрузки ОС с дискеты или компакт-диска, так как некоторые устаревшие версии BIOS позволяют осуществить загрузку с дискеты без запроса пароля. Если используемая версия BIOS при установленном пароле загрузки обеспечивает запрос пароля и при загрузке с дискеты, что, как правило, реализовано во всех современных версиях базовой системы ввода-вывода, то изменять порядок загрузки для защиты от несанкционированного входа в компьютерную систему нет необходимости.

Запуск утилиты Setup выполняется, как правило, нажатиями клавиши <Del> после активизации процесса загрузки операционной системы, т. е. после включения компьютера или перезапуска после нажатия кнопки <Reset> в процессе сеанса работы пользователя,

После запуска утилиты необходимо войти в пункт меню BIOS Features Setup (Advanced CMOS Setup) и с помощью клавиш <PgUp> и <PgDn> установить следующие переключатели:

- Boot Sequence (System Boot Up Sequence) — в положение C, A или C, CDROM, A;
- Security Option (Password Checking Options) — в положение System.

Далее следует задать пароль входа в систему с помощью пункта меню Password Setting (Change Password), а потом сохранить сделанные изменения и выйти из утилиты с помощью пункта меню Save & Exit Setup. После указанных действий загрузка компьютера будет выполняться только после ввода установленного пароля.

При необходимости изменения пароля следует активизировать утилиту Setup, изменить пароль с помощью пункта меню Password Setting (Change Password), а потом сохранить сделанные изменения и выйти из утилиты с помощью пункта меню Save & Exit Setup.

Недостатком реализации защиты от несанкционированной загрузки компьютера с помощью утилиты BIOS Setup является то, что установленная с помощью данной утилиты защита может быть преодолена путем принудительного обнуления содержимого энергонезависимой памяти компьютера (CMOS-памяти) после вскрытия его корпуса. Кроме того, BIOS некоторых производителей предусматривают «широко известные в узких кругах» фабричные пароли по умолчанию, позволяющие обойти пароли, установленные пользователем в Password Setting.

Защита от несанкционированного доступа к компьютеру при его оставлении без завершения сеанса работы

В ряде случаев в процессе работы пользователя за компьютером может возникнуть необходимость кратковременно оставить компьютер без присмотра, не завершая при этом сеанс работы (не выключая компьютер). При отсутствии пользователя ничто не мешает осуществлению несанкционированного доступа к компьютерной системе, так как процесс подтверждения подлинности уже выполнен санкционированным пользователем, оставившим компьютер.

Для предотвращения такой ситуации перед оставлением компьютера необходимо либо завершить сеанс работы, либо заблокировать клавиатуру, «мышь» и экран до активизации процесса подтверждения подлинности. Кроме того, должна быть предусмотрена возможность автоматического блокирования клавиатуры, «мыши» и экрана по истечении заданного времени бездействия пользователя. Это обеспечит защиту, если при оставлении компьютера пользователь забудет завершить сеанс работы или принудительно заблокировать клавиатуру, «мышь» и экран.

Особенности реализации уровня защиты от несанкционированного доступа к компьютеру при его оставлении без завершения сеанса работы для сред MS-DOS, Windows 3.xx и Windows 95/98/NT/2000/XP отличаются друг от друга.

При использовании общесистемных средств защиты в среде MS-DOS блокировка клавиатуры, экрана и «мыши» по тайм-ауту при отсутствии признаков активности пользователя не обеспечивается.

Недостатком хранителей экрана для защиты от несанкционированного доступа в средах Windows является отсутствие возможности принудительной блокировки клавиатуры, экрана и «мыши» без завершения сеанса работы,

В специализированных же системах защиты, например, в системе Кобра, обеспечивается как возможность блокировки клавиатуры, «мыши» и экрана компьютера по тайм-ауту, так и возможность принудительного блокирования компьютера на время его оставления без присмотра.

Защита в среде MS-DOS. Защиту от несанкционированного доступа к компьютеру при его оставлении без завершения сеанса работы в среде MS-DOS можно реализовать с помощью утилиты

Diskreet, входящей в состав пакета Norton Utility 7- или 8-й версий. Для этого необходимо выполнить следующие действия:

- подключить драйвер diskreet.sys, включив в файл Config.sys строку device = d:\path\diskreet.sys, где d и path — соответственно логический привод и путь файла diskreet.sys;
- перезагрузить ОС;
- запустить утилиту diskreet.exe;
- нажатием клавиши <F10> войти в меню, выбрать пункт Options и ввести команду Driver. Раскрыть список Hot key с помощью комбинации клавиш <Ctrl+!> и выбрать комбинацию клавиш для блокирования клавиатуры, «мыши» и экрана; установить нажатием клавиши пробела флажок Keyboard\Screen Lock и нажать OK;
- используя команду Master Password из пункта меню Options, ввести главный пароль и выйти из утилиты.

Выполнив перечисленные действия, можно будет блокировать экран, клавиатуру и «мышь», нажав установленную комбинацию клавиш. Для разблокирования следует ввести главный пароль и нажать клавишу <Enter>. Данный пароль необходимо будет вводить и после выдачи команды Driver в меню Options из среды утилиты Diskreet.

Для изменения главного пароля следует запустить утилиту Diskreet, ввести команду Master Password из пункта меню Options и далее определить новый пароль, введя предварительно старый. При забывании главного пароля единственным выходом из данного положения является удаление файла Diskreet.ini. Когда данный файл отсутствует, считается, что главный пароль не установлен.

Защита в средах Windows. Установка параметров защиты от несанкционированного доступа к компьютеру при его оставлении без завершения сеанса работы для операционной среды *Windows 95/98/NT/2000/XP* выполняется следующими действиями:

- активизация Панели Управления Windows (рис. 4.1) и запуск программного компонента Экран, предназначенного для настройки параметров экрана (рис. 4.2);
- активизация листа свойств Заставка (рис. 4.3) и выбор хранителя экрана;
- установка в поле Интервал требуемого времени бездействия пользователя, по истечении которого будет активизироваться хранитель экрана;

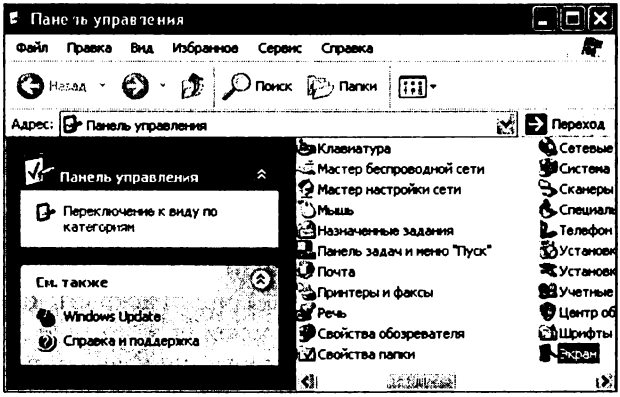


Рис. 4.1. Экран Панель управления Windows XP

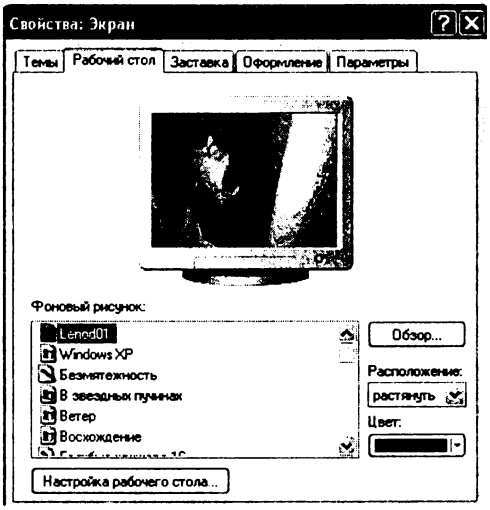


Рис. 4.2. Экран `Свойства экрана` `Панели управления` Windows XP

- установка флажка `Пароль`;
- определение пароля с помощью кнопки `Сменить`;
- подтверждение нажатием кнопки `OK` внесенных изменений и закрытие `Панели управления`.

После выполнения указанных настроек по истечении установленного времени бездействия пользователя будет активизирован хранитель экрана, который не позволит вернуться в систему без ввода заданного в `Панели управления` пароля. Измене-

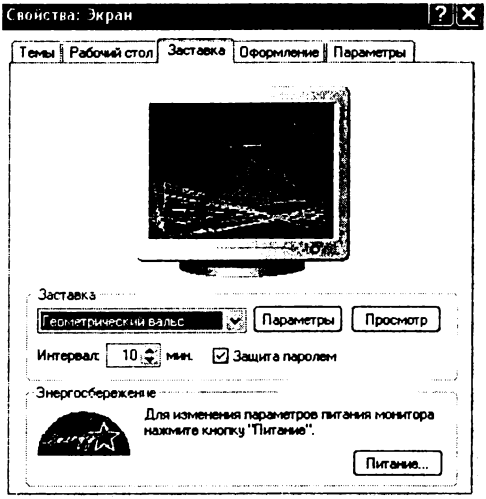


Рис. 4.3. Экран свойств Заставка

ние пароля возврата в систему осуществляется по аналогии с процессом его установки.

4.3. Вредоносные закладки в ПК и борьба с ними

К основным разновидностям вредоносного воздействия относятся воздействие на информацию (уничтожение, искажение, модификация) и воздействие на систему (вывод из строя, ложное инициирование действия, модификация содержания выполняемых функций, создание помех в работе). Англоязычное наименование этих феноменов — malware или badware (от инициативы Stopbadware.org) — говорит само за себя (буквально — «нехорошие изделия»). Stopbadware.org определяет приложение как «badware» (символизируется картинкой, приведенной в начале данного пункта), если оно:

- действует обманным путем или вызывает необратимые последствия;
- приводит к потенциально нежелательным результатам без того, чтобы:

  а) вначале информировать пользователя об этом понятно и доходчиво;

  б) затем получить его согласие.

Защита от злонамеренных (вредоносных) программных средств (ЗПС) для ПК имеет особое значение по ряду причин, а именно:

- актуальность для всех без исключения пользователей ПК независимо от того, конфиденциальная или открытая информация ими обрабатывается;
- заражение ЗПС представляет угрозу повышенной опасности для ПК, этому особенно способствует высокий динамизм обмена информацией как по каналам связи (в сетях ЭВМ), так и посредством гибких дисков;
- защита ПК от ЗПС требует особого профессионализма, поскольку многие из них носят специфический индивидуальный характер, а их нейтрализация и устранение сопряжено с программными манипуляциями нередко весьма сложного и даже искусного характера.

Классификация закладок и их общие характеристики

К сожалению, всеобъемлющая и научно обоснованная классификация закладок пока не разработана, что объясняется отчасти недостаточным объемом статистических данных, а отчасти тем, что работы по защите от закладок различных разновидностей ведутся изолированно. Исходя из целей защиты от вредоносного воздействия закладок, их целесообразно классифицировать по следующей совокупности критериев:

- характеру вредоносного воздействия на ПК;
- способу реализации;
- способу проникновения в ПК;
- способности к саморазмножению.

Основные значения *первого* критерия могут быть представлены в следующем виде:

- уничтожение или искажение программ и/или массивов данных;
- формирование каналов несанкционированного получения информации;
- вывод ПК из числа действующих, т. е. приведение его в такое состояние, при котором он не может осуществлять свои основные функции;
- инициирование выполнения предусмотренных в ПК функций (например, ложная подача команды на остановку про-

изводства в автоматизированных системах управления технологическими процессами);
- создание препятствий в выполнении функций ПК (например, блокировка отображения информации на экране дисплея, выдачи на печать и др.).

Возможные значения *второго* критерия (способ реализации) могут быть представлены следующим перечнем:
- аппаратный;
- программный;
- организационный.

Первые два способа реализации рассмотрены выше, они, вообще говоря, являются основными. Однако в общем случае можно предположить возможность создания также организационных закладок. Например, в инструкции об уничтожении информации, находящейся в ЭВМ, в злоумышленных целях можно предусмотреть преждевременное ее уничтожение или, наоборот, сохранение той информации, которую надлежало бы уничтожить. В инструкции по использованию криптографических средств злоумышленно можно внести такие положения, выполнение которых может дать криптоаналитику дополнительную информацию, облегчающую криптоанализ шифртекста. Нетрудно предположить возможность создания ряда других организационных закладок.

По способу проникновения в ПК (*третий* критерий классификации) закладки могут быть разделены на следующие группы:
- злоумышленно создаваемые в процессе производства аппаратуры ЭВТ и компонентов ее программного обеспечения;
- неосознанно вносимые персоналом или пользователями ПК в процессе ее функционирования;
- злоумышленно вносимые в процессе функционирования ПК;
- злоумышленно создаваемые в процессе ремонта аппаратуры или обновления ПК.

Наконец, по способности к размножению *(четвертый* критерий классификации) закладки естественным образом делятся на две разновидности:
- саморазмножающиеся;
- несаморазмножающиеся.

В табл. 4.2 приводится альтернативная классификация программных средств, опирающаяся на различные уровни нежела-

тельных последствий их функционирования и информированности пользователей об этих последствиях, позволяющая различать легитимные и вредоносные программы.

Таблица 4.2. **Матрица классов программных средств**

Осознание последствий пользователями	Негативные последствия работы программных средств		
	Незначительные	*Средние*	*Высокие*
Высокое	Легальные ПС[1]	Нежелательные ПС[2]	[illegible]
Среднее	«Полупрозрачные» ПС	«Непрощенные» ПС	[illegible]
Низкое	[illegible]	[illegible]	[illegible]

[1] Легальные ПС с низкими негативными последствиями и высокой информированностью пользователя.

[2] Шпионские программы со средней информированностью пользователя или средними негативными последствиями.

[3] Вредоносные программы с низкой информированностью пользователя или неприемлемыми последствиями.

Известные в настоящее время закладки осуществляются аппаратным или программным путем.

Аппаратные закладки могут быть осуществлены в процессе изготовления ПК, ее ремонта или проведения профилактических работ. Реальная угроза таких закладок создается массовым и практически неконтролируемым распространением ПК. Особая опасность аппаратных закладок заключается в том, что они могут длительное время не проявлять своих вредоносных воздействий, а затем начать их осуществление или по истечении определенного времени, или при наступлении некоторого состояния ПК (например, при заполнении данными жесткого магнитного диска до заданного уровня), или по специальной, подаваемой дистанционно команде. Заблаговременное обнаружение аппаратных закладок возможно только в условиях проверок с использованием специальных методов и средств.

Программные закладки с точки зрения массового пользователя представляются особо опасными в силу сравнительной (относительно аппаратных) простоты их осуществления, высо-

кой динамичности их распространения и повышенной трудности защиты от них. Так, если в итоге специальных проверок аппаратные закладки не были обнаружены или они были ликвидированы (нейтрализована возможность их действия), то с высокой степенью достоверности можно утверждать об их отсутствии в соответствующем ПК. Программные же закладки могут появиться в любое время, этому особенно способствуют следующие обстоятельства:

- массовый обмен информацией на сменных носителях (НГМД, CD/DVD);
- широкое распространение копий программ, приобретенных незаконным путем;
- возможности дистанционного воздействия на ПК, подключенные к сети;
- широкий и непрерывно растущий диапазон разновидностей закладок, что усложняет процессы их обнаружения и нейтрализации.

В силу изложенных причин защиту от программных закладок рассмотрим несколько детальней, выделив при этом следующие вопросы:

- классификация закладок и их характеристики;
- принципиальные подходы и общая схема защиты от закладок;
- методы и средства защиты;
- рекомендации пользователям ПК по защите от программных закладок.

Средства вторжения в частную жизнь

Это программы (privacy-invasive software), игнорирующие право пользователя на частную жизнь (или конфиденциальность) и часто преследующие негативные и/или коммерческие цели. В такой автоматизированной среде, как Internet, существует целый ряд угроз конфиденциальности, которые варьируются от систематической записи повседневных событий (например, какие Internet-сайты были посещены пользователем или какие товары приобретены в Internet-магазинах) до массового маркетинга на основе незаконно полученной персональной информации, а также распространения информации о смертоносных технологиях, которые могут использоваться, например, при терактах.

Сегодня в различных аспектах использования Internet могут возникать следующие ситуации нарушения конфиденциальности:

- программы-шпионы (spyware) — собирают и передают персональную информацию о пользователе, тайно загружаясь и выполняясь на его рабочей станции;
- программные закладки навязчивой рекламы (adware) — несанкционированно отображают рекламу и другое коммерческое содержание на ПК пользователей, зачастую основываясь на персональных данных пользователя, выкраденных программами-шпионами;
- системные мониторы (system monitors) — записывают и отслеживают различные действия, происходящие в компьютерной системе;
- перехватчики клавиатуры (keyloggers) — протоколируют работу пользователя на клавиатуре;
- саморазмножающиеся вредоносные программы (self-replicating malware), например, вирусы и черви, — загружаются и дезорганизуют работу систем и сетей;
- программы сбора данных (data-harvesting software), предназначенные для сбора почтовых адресов, стали обычным делом в Internet, в результате этого спам-сообщения по электронной почте с нежелательным коммерческим содержанием заполнили сети и компьютеры.

Может быть дано следующее определение ПС, нарушающих конфиденциальность:

- эти ПС игнорируют право пользователя на частную жизнь (т. е. нежелательны и не дают пользователю возможность установить, с какой целью и с какими последствиями данные персональной идентичности собираются, хранятся или обрабатываются);
- они распространяются (дистрибьютор часто анонимен, но обычно располагается в Internet-инфраструктуре) с определенными целями, зачастую коммерческого характера (т. е. как некий инструмент извлечения доходов, независимо от типа и качества), которые негативно сказываются на пользователях.

Программы-шпионы. Известен ряд определений этих типов ПС.

Например: любое программное обеспечение, которое использует соединение пользователя с Internet в фоновом режиме (или «backchannel») без его ведома и разрешения (2000 г., Стив Гибсон).

В Антишпионской коалиции (Anti-Spyware Coalition — ASC), которая состоит из заинтересованных общественных групп, торговых ассоциаций и разработчиков антишпионских программ, пришли к выводу, что термин «шпионские программы» следует использовать на различных уровнях абстракции.

В узком смысле шпионские программы — средства слежения (tracking software), помещенные на ПК пользователя без надлежащего его уведомления, согласия или контроля.

В более широком смысле, это программы, которые размещаются на ПК без согласия соответствующего пользователя и/или функционируют таким образом, чтобы мешать пользователю контролировать:

- существенные изменения, которые влияют на эффективность, неприкосновенность частной жизни, или системы безопасности;
- использование системных ресурсов (в том числе, какие программы установлены на компьютере);
- сбор, использование и распространение персональных данных или другой важной информации.

В наиболее широком смысле ASC предлагает использовать термин «программы-шпионы и другие потенциально нежелательные технологии» для любого программного обеспечения, которое может быть запущено на компьютерах пользователей без их информированного согласия.

Компьютерные наблюдения

Этот термин (computer surveillance) имеет двоякое толкование: во-первых, сюда относятся средства отслеживания (слежения, «трекинга», от англ. *tracking*) компьютерной активности, во-вторых — это средства «зомбирования» компьютера, превращения его в устройство наблюдения за пользователем.

«Трекинг» (tracking software) — программное обеспечение, которое осуществляет протоколирование активности пользователя без его ведома, например, какую почту он получил, какие Web-сайты посетил, какие символы ввел с клавиатуры и т. д.

Программа отслеживания, установленная на компьютере, может анализировать содержимое жесткого диска, собирать определенные данные, запоминать пароли и даже передавать эту информацию своему «шефу» через Internet. Наиболее распро-

страненными, безусловно, являются коммерческие шпионские программы, предназначенные для сбора маркетинговой информации. Однако такие программы не ограничиваются только сбором данных, они также могут производить более опасные действия, а именно — удаление или изменение данных.

Компьютеры представляют собой идеальные инструменты для организации подобного наблюдения, поскольку они могут выполнить какие-то действия без ведома и согласия их владельцев. Большинство компьютеров подключены к сетям и могут использоваться (после разрушения средств безопасности), чтобы получить доступ к любой конфиденциальной информации, которая может храниться на компьютере.

Известны, например, средства регистрации трафика данных между компьютером и сетью. В некоторых сетях данные отправляются только на ту машину, которой они предназначены, в то время как в других (например, Ethernet) передача транслируется на все связанные компьютеры, но обрабатываются данные только целевым компьютером. В последнем случае можно перехватывать трафик, просто используя другой компьютер в той же сети, без необходимости какого-либо программного обеспечения или оборудования на «поднадзорной» машине.

Известны также и устройства физического (аппаратного) наблюдения («жучки»). Относительно простым «жучком» является перехватчик клавиатуры, способный запоминать и передавать клавиатурные последовательности.

Более сложные (и более легко обнаруживаемые) устройства, имеющие доступ к окружающей информации могут также, в принципе, быть установлены внутри компьютера (или рядом). Их очевидным недостатком является необходимость физического присутствия злоумышленника при их установке в том месте, где находится компьютер, а это факт легко подпадает под множество законодательных определений преступных действий (известно, однако, что законодательство США, например, дает работодателям довольно широкие полномочия по использовании компьютеров для слежения за поведением работников).

Самый простой способ поместить программы слежения на компьютер заключается в том, чтобы проникнуть в помещение, где находится компьютер, и установить их с компакт-диска, дискеты или флэш-накопителя. Этот метод имеет недостатки, присущие аппаратным «жучкам», поскольку требует физического доступа к компьютеру.

Более сложный метод предполагает, чтобы пакет программного обеспечения слежения был установлен в качестве компьютерного вируса или «троянского коня». Эта тактика имеет то преимущество, что сразу несколько компьютеров будут «оборудованы для наблюдения». Тем не менее, если вирус будет распространяться, то он станет мишенью антивирусных программ, которые могут удалить ПО наблюдения с зараженных компьютеров.

Известно, что можно отслеживать операции компьютера на расстоянии, используя только оборудование, находящееся в открытой продаже, путем анализа излучения ЭЛТ-монитора. Известно, кроме того, что высокочастотный шум, излучаемый процессором, включает в себя информацию о выполняющихся командах. Более того, исследования фирмы IBM показали также, что для большинства компьютерных клавиатур каждая нажимаемая клавиша издает свой специфический звук/шум, и эти различия можно индивидуально идентифицировать при определенных условиях, и поэтому существует возможность записать и идентифицировать последовательности клавиатурных кодов без необходимости анализа работы компьютерных программ. Еще одним каналом отслеживания использования компьютера (работа с клавиатурой, отображение изображений и т. д.) являются видеокамеры, которые становятся достаточно компактными, чтобы быть легко скрытыми для обеспечения тайного наблюдения.

Беспроводная связь между компьютерами или между компонентами компьютера (например, клавиатуры, мыши, принтеры, модемы и т. д.) также создает проблемы безопасности. Некоторые беспроводные протоколы в своей основе уязвимы с точки зрения обеспечения безопасности (например, WEP, Bluetooth), поэтому при разработке новых беспроводных стандартов (обеспечивающих большую дальность и скорость передачи), требования к безопасности возрастают.

Радикальным, но чрезмерно дорогим средством защиты от дистанционного наблюдения на основе излучения мониторов или процессоров, является экранирование помещения («клетка Фарадея»), исключающее проникновение электромагнитных волн за пределы периметра. Более простым методом является применение специальных программных средств (например, в правительственных учреждениях США с этой целью используется продукт Tempest), фоновая работа которых маскирует естественный характер излучения компьютера.

HTTP cookies — небольшие текстовые файлы, протоколирующие состояния HTTP-обмена и активность браузера (поскольку протокол HTTP не предусматривает запоминания состояний сессии), также могут использоваться для отслеживания действий пользователя. Поэтому «антишпионские» программы» (например, AdAware, см. ниже) обычно воспринимают как закладки и либо удаляют, либо рекомендуют пользователю удалить их.

Простые cookies. Базовый метод распознавания пользователей на Web-сайте основан на идентификации по файлу cookie, относящемуся к этому сайту. Такая идентификация позволяет опознавать пользователя, возвращающегося на сайт, и связывать с ним данные, которые он ввел ранее. Обычно это удобно для потребителя, который сознательно соглашается предоставить сайту сведения о себе, рассматривая связанный с такими действиями риск как незначительный. Эта полезная функция позволяет немедленно обеспечить индивидуальное обслуживание, подобно тому, как делают продавцы книг или авиакомпании.

Простая идентификация на основе файла cookie редко рассматривается как разновидность шпионажа. Однако некоторые считают ее таковой из-за возможности опознавания пользователя и хранения на сайте связанных с ним данных.

Ассоциированные cookies. Многие специалисты считают, что реальная опасность шпионажа начинается при применении ассоциированных файлов cookies, которые повышают степень риска для пользователя и его подверженность посторонним воздействиям. Ассоциированные файлы cookie идентифицируют потребителя при посещении им любого сайта, входящего в определенную группу. Эти файлы следят за его деятельностью и сохраняют данные, собранные в ходе взаимодействия с каждым из сайтов-соучастников. Рекламные агентства заключают с сайтами-соучастниками соглашения о размещении ссылок на шпионские серверы, которые могут представлять собой обычные картинки или даже совершенно незаметные изображения размером в один пиксель. Эти ссылки заставляют браузер пользователя обращаться к шпионскому серверу, который, в свою очередь, пытается обнаружить на компьютере пользователя определенный файл cookie. Если такового найти не удается, создается новый файл, содержащий глобальный уникальный идентификатор GUID, который позволяет опознавать пользователя при посещении им любого сайта-соучастника.

Компьютерный червь

Компьютерный червь (computer worm) — саморазмножающаяся программа, использующая сеть для отправки своих копий на другие узлы (компьютерные терминалы сети), причем он может делать это без какого-либо вмешательства пользователей. В отличие от вируса червь не нуждается в присоединении к какой-либо другой программе. Черви почти всегда причиняют вред сети, хотя бы тем, что увеличивают трафик, тогда как вирусы обычно повреждают или изменяют файлы на компьютере-мишени.

Первоначально многие черви были созданы только для распространения по сети и не пытались воздействовать на системы, через которые они проходят. Однако в дальнейшем ситуация изменилась. Наиболее типичным является случай, когда червь проделывает «черный ход» (backdoor или бэкдор) с целью «зомбировать» зараженный компьютер, поставив его под контроль автора червя. Черви Sobig и Mydoom являются такими примерами. Созданный «черный ход» может быть использован другими вредоносными программами, в том числе червями. Примеры включают Doomjuice, который распространяется, используя черный ход, открытый червем Mydoom.

Большинство экспертов по безопасности считает всех червей вредоносными программами независимо от их действительного поведения и/или намерений их авторов.

Основным признаком, по которому типы червей различаются между собой, является способ распространения червя — каким способом он передает свою копию на удаленные компьютеры. Другими признаками различия червей между собой являются способы запуска копии червя на заражаемом компьютере, методы внедрения в систему, а также полиморфизм, «стелс» и прочие характеристики, присущие и другим типам вредоносного программного обеспечения (вирусам и троянским программам). Рассмотрим некоторые их разновидности.

Email-Worm — почтовые черви. К данной категории червей относятся те из них, которые для своего распространения используют электронную почту. При этом червь отсылает либо свою копию в виде вложения в электронное письмо, либо ссылку на свой файл, расположенный на каком-либо сетевом ресурсе (например, URL на зараженный файл, расположенный на взломанном или хакерском Web-сайте). В первом случае код червя

активизируется при открытии (запуске) зараженного вложения, во втором — при открытии ссылки на зараженный файл. В обоих случаях эффект одинаков — активизируется код червя.

Для отправки зараженных сообщений почтовые черви используют различные способы, например:

- прямое подключение к SMTP-серверу, применяя встроенную в код червя почтовую библиотеку;
- сервисы MS Outlook;
- функции Windows MAPI.

Различные методы используются почтовыми червями для поиска почтовых адресов, на которые будут рассылаться зараженные письма. Почтовые черви:

- рассылают свой код по всем адресам, обнаруженным в адресной книге MS Outlook;
- считывает адреса из адресной базы WAB;
- сканируют «подходящие» файлы на диске и выделяет в них строки, являющиеся адресами электронной почты;
- отсылают код по всем адресам, обнаруженным в письмах в почтовом ящике (при этом некоторые почтовые черви «отвечают» на обнаруженные в ящике письма).

Многие черви используют сразу несколько из перечисленных методов. Встречаются также и другие способы поиска адресов электронной почты.

IM-Worm — черви, использующие Internet-пейджеры. Известные компьютерные черви данного типа используют единственный способ распространения — рассылку на обнаруженные контакты (из списка контактов) сообщений, содержащих ссылки на файлы, расположенные на каком-либо Web-сервере. Данный прием практически полностью повторяет аналогичный способ рассылки, использующийся почтовыми червями.

IRC-Worm — черви в IRC-каналах. У данного типа червей, как и у почтовых червей, существует два способа распространения червя по IRC-каналам, повторяющих способы, описанные выше. Первый заключается в отсылке URL-ссылки на копию червя. Второй способ — отсылка зараженного файла какому-либо пользователю сети. При этом атакуемый пользователь должен подтвердить прием файла, затем сохранить его на диске и открыть (запустить на выполнение).

Net-Worm — прочие сетевые черви. Существуют прочие способы заражения удаленных компьютеров, например:

- копирование червя на сетевые ресурсы;

- проникновение червя на компьютер через уязвимости в операционных системах и приложениях;
- проникновение в сетевые ресурсы публичного использования;
- паразитирование на других вредоносных программах.

Первый способ заключается в том, что червь ищет удаленные компьютеры и копирует себя в каталоги, открытые на чтение и запись (если такие обнаружены). При этом черви данного типа или перебирают доступные сетевые каталоги, используя функции операционной системы, и/или случайным образом ищут компьютеры в глобальной сети, подключаются к ним и пытаются открыть их диски на полный доступ.

Для проникновения вторым способом черви ищут в сети компьютеры, на которых используется программное обеспечение, содержащее критические уязвимости. Для заражения уязвимых компьютеров червь посылает специально оформленный сетевой пакет или запрос (эксплойт уязвимости), в результате этого код (или часть кода) червя проникает на компьютер-жертву. Если сетевой пакет содержит только часть кода червя, он затем скачивает основной файл и запускает его на исполнение.

Отдельную категорию составляют черви, использующие для своего распространения Web- и FTP-серверы. Заражение происходит в два этапа. Сначала червь проникает в компьютер-сервер и необходимым образом модифицирует служебные файлы сервера (например, статические Web-страницы). Затем червь «ждет» посетителей, которые запрашивают информацию с зараженного сервера (например, открывают зараженную Web-страницу), и таким образом проникает на другие компьютеры в сети.

Существуют сетевые черви, паразитирующие на других червях и/или троянских программах удаленного администрирования (бэкдор). Данные черви используют тот факт, что многие бэкдоры позволяют по определенной команде скачивать указанный файл и запускать его на локальном диске. То же возможно с некоторыми червями, содержащими бэкдор-процедуры. Для заражения удаленных компьютеров данные черви ищут другие компьютеры в сети и посылают на них команду скачивания и запуска своей копии. Если атакуемый компьютер оказывается уже зараженным «подходящей» троянской программой, червь проникает в него и активизирует свою копию. Следует отметить, что многие компьютерные черви используют более одного способа

распространения своих копий по сетям, применяя два и более методов атаки удаленных компьютеров.

P2P-Worm — черви для файлообменных сетей. Механизм работы большинства подобных червей достаточно прост — для внедрения в P2P-сеть червю достаточно скопировать свой код в каталог обмена файлами, который обычно расположен на локальной машине. Всю остальную работу по распространению P2P-червя сеть берет на себя — при поиске файлов в сети она сообщит удаленным пользователям о данном файле и предоставит весь необходимый сервис для скачивания файла с зараженного компьютера.

Существуют более сложные P2P-черви, которые имитируют сетевой протокол конкретной файлообменной системы и на поисковые запросы отвечают положительно — при этом червь предлагает для скачивания свою копию.

Троянские программы

«Троянские кони» (Trojan horse) или просто «троянцы» (Trojans) представляют собой программы, реализующие, помимо функций, описанных в документации, и некоторые другие, связанные с нарушением безопасности и деструктивными действиями (обычно — уничтожение информации, перехват и передача информации, целенаправленная модификация кода программы, интересующей нарушителя). Отмечены случаи создания таких программ с целью облегчения распространения вирусов. Обычно они маскируются под игровые или развлекательные программы и наносят вред под красивые картинки или музыку. Рассмотрим некоторые классы «троянцев».

Backdoor — троянские программы этого класса являются утилитами удаленного администрирования компьютеров в сети. По своей функциональности они во многом напоминают различные системы администрирования, разрабатываемые и распространяемые фирмами-производителями программных продуктов. Единственная особенность, которая заставляет классифицировать их как вредные троянские программы — отсутствие предупреждения об инсталляции и запуске. При запуске «троянец» устанавливается в системе и затем следит за ней, и при этом пользователю не выдается никаких сообщений о действиях троянца в системе. Более того, ссылка на «троянца» может отсутствовать в списке активных приложений. В результате «поль-

зователь» этой троянской программы может и не знать о ее присутствии в системе, в то время как его компьютер открыт для удаленного управления.

Утилиты скрытого управления позволяют делать с компьютером все, что в них заложил автор — принимать или отправлять файлы, запускать и уничтожать их, выводить сообщения, стирать информацию, перезагружать компьютер и т. д. В результате эти троянцы могут быть использованы для обнаружения и передачи конфиденциальной информации, для запуска вирусов, уничтожения данных и т. п. — пораженные компьютеры оказываются открытыми для злоумышленных действий хакеров.

Таким образом, троянские программы данного типа являются одним из самых опасных видов вредоносного программного обеспечения, поскольку в них заложена возможность самых разнообразных злоумышленных действий, присущих другим видам троянских программ.

Отдельно следует отметить группу бэкдоров, способных распространяться по сети и внедряться в другие компьютеры, как это делают компьютерные черви. Отличает таких «троянцев» от червей тот факт, что они распространяются по сети не самопроизвольно (как черви), а только по специальной команде «хозяина», управляющего данной копией троянской программы.

Trojan-PSW (Password Stealing Ware) — воровство паролей. Данное семейство объединяют троянские программы, «ворующие» различную информацию с зараженного компьютера, обычно — системные пароли. При запуске PSW-троянцы ищут системные файлы, хранящие различную конфиденциальную информацию (обычно — номера телефонов и пароли доступа к Internet) и отсылают ее по указанному в коде «троянца» электронному адресу или адресам. Существуют PSW-троянцы, которые сообщают и другую информацию о зараженном компьютере, например, информацию о системе (размер памяти и дискового пространства, версия операционной системы), тип используемого почтового клиента, IP-адрес и т. п. Некоторые троянцы данного типа «воруют» регистрационную информацию к различному программному обеспечению, коды доступа к сетевым играм и пр.

Trojan-Clicker — Internet-кликеры. Семейство троянских программ, основная функция которых — организация несанкционированных обращений к Internet-ресурсам (обычно к Web-страницам). Достигается это либо посылкой соответствующих команд браузеру, либо заменой системных файлов, в которых

указаны «стандартные» адреса Internet-ресурсов (например, файл hosts в MS Windows).

У злоумышленника могут быть следующие цели для подобных действий:

- увеличение посещаемости каких-либо сайтов с целью увеличения показов рекламы;
- организация DoS-атаки (Denial of Service) на какой-либо сервер;
- привлечение потенциальных жертв для заражения вирусами или троянскими программами.

Trojan-Downloader — транспортировка других вредоносных программ. Троянские программы этого класса предназначены для загрузки и установки на компьютер-жертву новых версий вредоносных программ, установки «троянцев» или рекламных систем. Загруженные из Internet программы затем либо запускаются на выполнение, либо регистрируются «троянцем» на автозагрузку в соответствии с возможностями операционной системы. Данные действия при этом происходят без ведома пользователя.

Информация об именах и расположении загружаемых программ содержится в коде и данных троянца или скачивается троянцем с «управляющего» Internet-ресурса (обычно с Web-страницы).

Trojan-Dropper — инсталляторы прочих вредоносных программ. Троянские программы этого класса написаны в целях скрытой инсталляции других программ и практически всегда используются для «подсовывания» на компьютер-жертву вирусов или других троянских программ. Данные троянцы обычно без каких-либо сообщений (либо с ложными сообщениями об ошибке в архиве или неверной версии операционной системы) сбрасывают на диск в какой-либо каталог (в корневой диск `c:`, во временный каталог, в каталоги Windows) другие файлы и запускают их на выполнение.

Обычно структура таких программ следующая:

```
Основной код+ Файл 1+ Файл 2+...
```

`Основной код` выделяет из своего файла остальные компоненты (`Файл 1`, `Файл 2`, ...), записывает их на диск и запускает на выполнение. Обычно один (или более) компонентов являются троянскими программами, а как минимум один компонент является «обманкой» — программой-шуткой, игрой, картинкой

или чем-то подобным. «Обманка» должна отвлечь внимание пользователя и/или продемонстрировать то, что запускаемый файл действительно делает что-то «полезное», в то время как троянский компонент инсталлируется в систему.

В результате использования программ данного класса хакеры достигают двух целей:

- скрытая инсталляция троянских программ и/или вирусов;
- защита от антивирусных программ, поскольку не все из них в состоянии проверить все компоненты внутри файлов этого типа.

Trojan-Spy — шпионские программы. Данные троянцы осуществляют электронный шпионаж за пользователем зараженного компьютера — вводимая с клавиатуры информация, снимки экрана, список активных приложений и действия пользователя с ними сохраняются в какой-либо файл на диске и периодически отправляются злоумышленнику. Троянские программы этого типа часто используются для кражи информации пользователей различных систем онлайновых платежей и банковских систем.

ArcBomb — «бомбы» в архивах. Представляют собой архивы, специально оформленные таким образом, чтобы вызывать нештатное поведение архиваторов при попытке разархивировать данные — зависание или существенное замедление работы компьютера, или заполнение диска большим количеством «пустых» данных. Особенно опасны «архивные бомбы» для файловых и почтовых серверов, если на сервере используется какая-либо система автоматической обработки входящей информации — «архивная бомба» может полностью заблокировать работу сервера.

Встречаются три типа подобных «бомб»: некорректный заголовок архива, повторяющиеся данные и одинаковые файлы в архиве.

Некорректный заголовок архива или испорченные данные в архиве могут привести к сбою в работе конкретного архиватора или алгоритма разархивирования при разборе содержимого архива.

Значительных размеров файл, содержащий повторяющиеся данные, позволяет заархивировать такой файл в архив небольшого размера (например, 5 Гбайт данных упаковываются в 200 Кбайт `rar`- или в 480 Кбайт `zip`-архива).

Огромное количество одинаковых файлов в архиве также практически не сказывается на размере архива при использовании специальных методов (например, существуют приемы упа-

ковки 10^{100} одинаковых файлов в 30 Кбайт `rar`- или 230 Кбайт `zip`-архива).

Trojan-Notifier — оповещение об успешной атаке. Троянцы данного типа предназначены для сообщения своему «хозяину» о зараженном компьютере. При этом на адрес «хозяина» отправляется информация о компьютере, например IP-адрес компьютера, номер открытого порта, адрес электронной почты и т. п. Отсылка осуществляется различными способами: электронным письмом, специально оформленным обращением к Web-странице «хозяина», ICQ-сообщением. Данные троянские программы используются в многокомпонентных троянских наборах для извещения своего «хозяина» об успешной инсталляции троянских компонент в атакованную систему.

Прочие вредоносные программы

К прочим вредоносным относятся разнообразные программы, которые могут не представлять угрозы непосредственно компьютеру, на котором исполняются, а разработаны для организации DoS-атак на удаленные серверы, взлома других компьютеров и т. п.

DoS, DDoS — сетевые атаки. Программы данного типа реализуют атаки на удаленные серверы, посылая на них многочисленные запросы, что приводит к отказу в обслуживании (DoS, Denial of Service — отказ от обслуживания), если ресурсы атакуемого сервера недостаточны для обработки всех поступающих запросов.

DoS-программы реализуют атаку с одного компьютера с ведома пользователя. DDoS-программы (Distributed DoS) реализуют распределенные атаки с разных компьютеров, причем без ведома пользователя зараженного компьютера. Для этого DDoS-программа засылается любым способом на компьютер «жертв-посредников» и после запуска в зависимости от текущей даты или по команде от «хозяина» начинает DoS-атаку на указанный сервер в сети.

Некоторые компьютерные черви содержат в себе DoS-процедуры, атакующие сайты, которые по каким-либо причинам «невзлюбил» автор червя. Так, червь `Codered` 20 августа 2001 г. организовал успешную атаку на официальный сайт президента

США, а червь Mydoom.a 1 февраля 2004 г. «выключил» сайт SCO, производителя дистрибутивов UNIX.

Exploit, ***HackTool*** — взломщики удаленных компьютеров. Хакерские утилиты данного класса предназначены для проникновения в удаленные компьютеры с целью дальнейшего управления ими (используя методы троянских программ типа «backdoor») или для внедрения во взломанную систему других вредоносных программ.

Хакерские утилиты типа «exploit» при этом используют уязвимости в операционных системах или приложениях, установленных на атакуемом компьютере.

Flooder — «замусоривание» сети. Данные хакерские утилиты используются для «забивания мусором» (бесполезными сообщениями) каналов Internet — IRC-каналов, компьютерных пейджинговых сетей, электронной почты и т. д.

Nuker — фатальные сетевые атаки. Утилиты, отправляющие специально оформленные запросы на атакуемые компьютеры в сети, в результате этого атакуемая система прекращает работу. Используют уязвимости в программном обеспечении и операционных системах, в результате сетевой запрос специального вида вызывает критическую ошибку в атакуемом приложении.

Факторы уязвимости систем для вредоносных программ

Атакуемой «системой» могут быть различные объекты — отдельное приложение, ОС в целом, отдельный компьютер или сеть. Могут быть выделены следующие факторы уязвимости:

- гомогенность (однородность) систем;
- дефекты в системах;
- неподтвержденный запуск;
- сверхпривилегированные пользователи;
- сверхпривилегированный программный код.

Гомогенность (монокультурность) — случай, когда все компьютеры в сети используют одну и ту же ОС или одни и те же наборы приложений. В частности, ОС Microsoft Windows занимает такую большую долю рынка, что ориентируясь на нее, злоумышленник может подорвать большое количество систем. Поэтому одним из очевидных заслонов к беспрепятственному распространения ЗПС является изменение платформы — переход

на альтернативные средства (ОС Linux или хотя бы браузеры Opera или FireFox).

Дефекты — многие системы содержат ошибки, которыми могут воспользоваться вредоносные программы. Типичным примером является буферная недостаточность, когда небольшой объем буфера в ОП приводит к необходимости многократного перезаписывания данных, этим и может воспользоваться ЗПС, чтобы заставить систему выполнить свой код.

Запуск без подтверждения — код с дискеты, CD-ROM или USB-устройства может быть запущен без подтверждения пользователем (первоначально ПК всегда загружались с дискет и до недавнего времени НЖМД был первичным загрузочным устройством по умолчанию, поэтому зараженная дискета, оставленная в НЖМД имеет все шансы быть запущенной, и то же самое можно сказать о CD, поскольку BIOS довольно редко запрашивает подтверждение пользователем загрузки со сменных носителей).

Сверхпривилегии пользователей. В некоторых системах обычные пользователи имеют привилегии администратора, в том смысле, что они могут изменять внутреннюю структуру этой системы. Это, конечно, определяется конфигурацией, однако в системах Microsoft Windows конфигурация по умолчанию отличается тем, что здесь пользователь имеет сверхпривилегии. Это связано с принятым в Microsoft решении о приоритете совместимости с более старыми системами над безопасностью новых систем, поскольку типичные приложения были разработаны ранее в расчете на равные права всех пользователей. Эта точка зрения была пересмотрена при разработке Microsoft Windows Vista, и в результате многие существующие приложения, которые требуют более высоких привилегией, могут иметь проблемы совместимости с Vista. Механизм User Account Control, предусмотренный в этой ОС, пытается исправить ситуацию, создавая виртуальную среду для запуска привилегированных кодов, присущих старым приложениям.

Сверхпривилегированный код. Вредоносная программа, запущенная как привилегированный код, может воспользоваться этим для подрыва системы. Почти все сегодняшние популярные ОС, а также многие приложения разрешают программам слишком много привилегий, в том смысле что, когда пользователь запускает код, система приписывает ему все права этого пользователя. Это делает пользователей уязвимыми к вредоносным про-

граммам в виде вложений в электронную почту, которые могут быть или не быть скрытыми.

Учитывая такое положение дел, пользователям рекомендуется открывать только почтовые вложения из источников, которым они доверяют, и избегать кода, полученного от ненадежных источников. Кроме того, общим источником опасности для операционных систем является то, что драйверы внешних устройств обычно требуют повышенных привилегий, причем они поставляются все возрастающим количеством производителей аппаратного обеспечения, некоторые из которых могут оказаться ненадежными.

Проникновение шпионских программ.

Прикрепление программы-шпиона к полезному приложению, которое загружает пользователь. Она устанавливается вместе с этим приложением и ее действия остаются скрытыми. Шпионская программа может быть отдельным исполняемым файлом или входить в состав динамических библиотек DLL, к которым обращается основное приложение. Активируясь, программа-шпион самостоятельно настраивается таким образом, чтобы затем работать без ведома пользователя.

Любопытно, что в лицензионном соглашении конечного пользователя часто и не скрывается наличие программ-шпионов. Это соглашение обычно бывает длинным и утомительным для чтения, преднамеренно составляется так, чтобы в нем трудно было разобраться. Сообщается, например, что лицензионное соглашение по подозрительному продукту Claria на 43 % длиннее, чем конституция США. Такой документ может включать в себя неявное упоминание о программах-шпионах или ссылаться на другое соглашение, которое содержит описание таких программ. Некоторые компании, использующие подобные средства, вообще не утруждаются упомянуть об этом в своих соглашениях.

Предложение программой-шпионом услуг разного рода, например сохранения и восстановления паролей, учетных записей, адресов и номеров телефонов. Она может пообещать расширить возможности почтовых программ оформления сообщений или предложить новую форму панели инструментов. А вдобавок шпионская утилита установит дополнительное программное обеспечение, которое с полной свободой сможет работать в вашей системе. Как и при первом способе, пользователь получает доступ к приложению, которое способно предпринимать действия, остающиеся за пределами его понимания. В ряде

случаев, но далеко не всегда, это отражается в лицензионном соглашении, которое пользователь принимает при инсталляции.

Выполнение Java или ActiveX. Использование Web-приложений на базе Java или ActiveX — также распространенный способ транспортировки вредоносных программ. После активации апплет Java или код ActiveX может загрузить и вызвать программу-шпион. Предыдущие способы позволяют достичь того же результата, но в данном случае все действия совершаются полностью без ведома пользователя.

К признакам присутствия программы-шпиона можно отнести непонятную активность жесткого диска, повышенную загрузку центрального процессора, программные конфликты, которых ранее не наблюдалось, медленный отклик или отказ системы. К сожалению, те же самые признаки могут быть вызваны другими проблемами и сделать на их основании правильные выводы не так-то просто.

Предустановка. При покупке компьютера на нем устанавливается некоторый набор программ. Например, в системах Windows можно обнаружить многочисленные файлы cookies, установленные как часть Internet Explorer, которые могут использоваться программами слежения. Поэтому рекомендуется «вычистить» новую машину программами обнаружения/устранения закладок.

Средства борьбы с вирусами и другими вредоносными закладками

Принципиальные подходы и общая схема защиты от закладок. Основу защиты составляют следующие функции:

- создание таких условий, при которых дестабилизирующие факторы (ДФ) не могут появляться;
- предупреждение появления ДФ, даже если для этого имеются условия;
- обнаружение появления ДФ;
- предупреждение воздействия на информацию появившихся ДФ;
- обнаружение негативного воздействия ДФ на информацию;
- локализация негативного воздействия ДФ на информацию;
- ликвидация последствий воздействия ДФ.

Средства борьбы с вирусами и другими вредоносными закладками можно разделить на юридические, организационно-административные, аппаратные и программные.

Юридические средства сводятся к установлению ответственности за умышленное создание и распространение вирусов и других закладок в целях нанесения ущерба, хотя доказать авторство и умышленность создания таких программ довольно трудно.

Следует признать, что на Западе соответствующие правовые нормы разработаны гораздо лучше, чем в России. Назовем некоторые законы, применяемые в западных странах для борьбы с компьютерными преступлениями:

- Закон о поддельных средствах доступа, компьютерном мошенничестве и злоупотреблении (США);
- Федеральный закон о частной тайне (США);
- Закон о предупреждении экономических преступлений (Германия);
- Закон об авторском праве (Германия);
- Федеральный закон о защите данных (Германия);
- Закон об авторском праве и поправки к нему (Великобритания);
- Закон о защите данных (Великобритания);
- Закон об обработке данных, о файлах данных и личных свободах (Франция).

В ряде стран введены соответствующие статьи в уголовные кодексы. Перечисленные законы позволяют вести достаточно эффективную борьбу с изготовителями вредоносных программ. Например, еще в начале 1989 г. один американский студент был приговорен судом к трем месяцам тюремного заключения и штрафу в 270 тыс. долл. за разработку вируса, которым были выведены из строя шесть тысяч компьютеров МО США.

В Российской Федерации в последнее время также предпринимаются серьезные усилия по созданию юридической основы борьбы с рассматриваемыми угрозами. Так, в принятый недавно Уголовный кодекс Российской Федерации введены три статьи (272—274), по которым предусмотрена ответственность за компьютерные преступления, причем самое строгое наказание (от 3 до 7 лет тюремного заключения) предписывается статьей 273 — за создание, использование и распространение вредоносных программ.

Организационно-административная защита от вредоносных программ заключается в выработке и неукоснительном осущест-

влении организационных и организационно-технических мероприятий, направленных на предупреждение заражения компьютеров этими программами, обнаружение заражения, нейтрализацию негативного их воздействия и ликвидацию последствий. Названные мероприятия должны осуществляться как в организациях-разработчиках программных средств, так и в организациях, эксплуатирующих эти программы.

В организациях-разработчиках весьма целесообразно из состава высококвалифицированных программистов создавать специальные группы для выполнения следующих функций:

- проверки психологических особенностей сотрудников при приеме на работу;
- создания и поддержания в коллективах здорового морально-психологического климата;
- определения потенциально возможных источников вредоносных программ и выработки рекомендаций по их обходу;
- выявления и изучения всех нештатных ситуаций, возникающих при разработке программного обеспечения, документального оформления результатов анализа, и оповещения всех заинтересованных при выявлении опасностей;
- регулярного контроля состояния программного обеспечения и средств борьбы с вредоносными программами;
- возможно более быстрой ликвидации последствий произошедшей атаки вредоносных программ и изготовления соответствующих средств защиты;
- оказания методической помощи своим абонентам в организации необходимой защиты от вредоносных программ.

Из ***аппаратных средств защиты*** могут рекомендоваться следующие:

- форматирование диска (для винчестера — полное стирание и переразметка), перезагрузка операционной системы и восстановление программ с незараженных копий;
- заклеивание (закрывание) отверстия защиты записи дискеты;
- физическая блокировка ключом клавиатуры ЭВМ;
- запрет и регистрация попыток записи в файлы операционной системы в области памяти, занятые системной информацией.

Известны и другие подобные перечисленным меры: разделение областей памяти между программами, разделение программ по приоритетам и т. п.

В целях повышения эффективности защиты ЭВМ от вредоносных программ в последнее время ведутся разработки защищенных противовирусных компьютеров и специальных плат, встраиваемых в существующие компьютеры.

В частности, в процессорах AMD (а затем и Intel) в последние годы были реализованы технологии «невыполнимых битов» — XD-bit — (eXecute Disable Bit), или NX-битов (Non-eXecute) — маскирующих разделы ОП — сегменты, страницы и пр., как недоступные для запуска в качестве программ. Этим может быть запрещено выполнение программного кода, находящегося в некоторых страницах памяти, таким образом, ограничивая возможность вирусных или хакерских атак [31].

Основными мероприятиями по защите программ и данных в организациях, использующих программы, представляются следующие:

- приобретение только законным путем необходимых технических средств и программ, сертифицированных на отсутствие вредоносных закладок;
- создание и хранение эталонных копий основных программ и резервирование баз данных;
- организация автоматизированной обработки данных с соблюдением всех необходимых приемов и правил;
- тщательная периодическая проверка состояния программного обеспечения и баз данных.

Защита от опасных компьютерных червей. Черви распространяются, используя бреши в операционных системах. Пользователям следует опасаться открытия неожидаемых или подозрительных почтовых сообщений, не запускать присоединенные файлы или программы, или посещать Web-сайты, которые связаны с такими письмами. Однако всегда существует вероятность того, что поддавшись на какие-либо трюки (как в случае с червем IloveYou), пользователь все же может запустить вредоносный код.

Как правило, следует с подозрением относиться к чрезмерному количеству спама и всплывающих рекламных окон: их причиной может быть программа-шпион. Кроме того, если ваш браузер открывает Web-сайты, к которым вы определенно не обращались, добавляет новые ссылки и параметры настройки, то весьма возможно, что виновата в этом программа-шпион. Лучший способ ее обнаружить и удалить состоит в использовании специальных инструментов.

Рассмотрим вкратце характеристики одного из популярных средств программной защиты ПК — Ad-Aware (разработчик Lavasoft AB, Швеция; последний релиз 7.0.2.6 / 11 января 2008 г.; платформа — ОС Microsoft Windows).

Ad-Aware SE и ряд других средств обеспечения безопасности ПК

fAd-Aware 2007 является представителем современного поколения программ поиска и удаления ЗПС. Использует новую технологию идентификации кодовых последовательностей (Code Sequence Identification — CSI), которая позволяет не только обнаруживать ранее известные образцы ЗПС, но также предсказывать свойства и зафиксировать их неизвестные варианты. Ad-Aware обнаруживает и удаляет также запущенные вредоносные процессы, определяет наличие вредоносных закладок в компьютере пользователя, оценивает уровень угрозы, а затем предоставляет пользователю возможность удалить нежелательное содержание.

Ad-Aware 2007 позволяет полностью проверить память ПК, НЖМД, НГМД, CD/DVD-накопители и обнаружить известные экземпляры таких вредоносных закладок, как анализаторы данных (Data miners), программы навязчивого рекламирования (Aggressive advertising), программы-паразиты (Parasites), шпионские программы (Spyware, Scumware, Malware), перехватчики клавиатуры (Keyloggers), номеронабиратели (Dialers), захватчики браузеров (Browser hijackers), а также традиционные троянцы (Trojans) и ряд других кодов.

Сканируется также реестр операционной системы и, если там обнаруживается запись, установленная вредоносной программой, она удаляется. Для предотвращения случайного удаления нужного файла или записи в реестре предусмотрена функция восстановления (для этого автоматически создаются копии удаляемых данных).

Системные требования:

- Процессор: Pentium 600 МГц (или выше).
- Оперативная память: рекомендовано минимум 50 Мбайт, 100 Мбайт.
- НЖМД: 50 Мбайт свободного пространства.

Совместимые операционные системы:
- Windows 2000 Professional;
- Windows 2000 Server;
- Windows Server 2003;
- Windows XP (Home/Professional);
- Windows Vista (32-битовая версия).

Другие требования (браузеры):
- Internet Explorer версии 5.5 и выше;
- Firefox 1.5 или выше;
- Opera 9 или выше.

Элементы интерфейса Ad-Aware. Интерфейс приложения включает следующие элементы:

Меню быстрого запуска (рис. 4.4, *1*, табл. 4.3);
- Главное меню (рис. 4.4, *2*, табл. 4.4);
- Окно главного экрана (рис. 4.4, *3—9*).

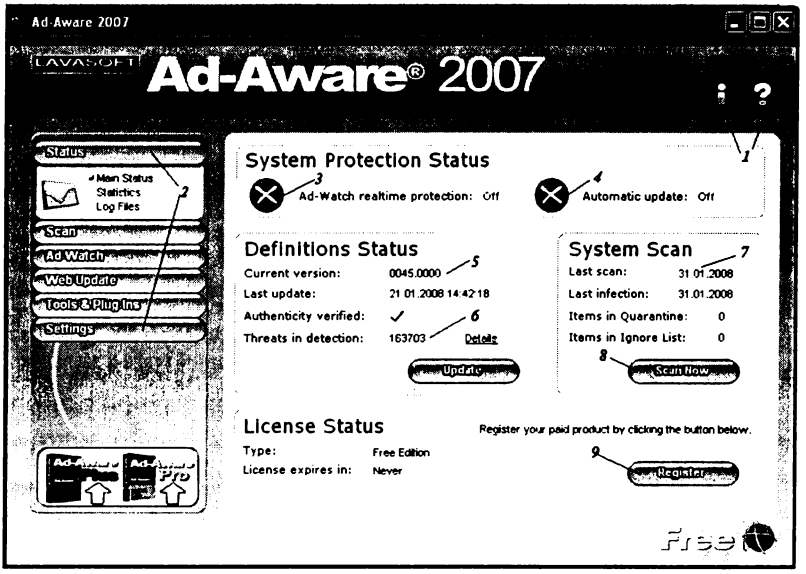


Рис. 4.4. Экран состояния защиты:
1 — Меню быстрого запуска; *2* — Главное меню; *3* — указатель состояния монитора реального времени AD-Watch (отключен); *4* — указатель состояния автоматического Web-обновления (отключен); *5* — используемая версия базы данных описаний угроз; *6* — количество единиц в БД описаний угроз; *7* — информация о последней выполненной проверке; *8* — кнопка перехода к экрану задания режима сканирования (Scan Mode); *9* — информация о действующей лицензии на продукт

Таблица 4.3. **Кнопки Меню быстрого запуска (Quick launch menu)**

Символ	Действия
	Получение информации об Ad-Aware SE
	Открытие файла справки о программе

Таблица. 4.4. **Кнопки Главного меню интерфейса**

Кнопка меню	Действия
Status Main Status Statistics Log Files	Открывает главный экран статуса (состояния защиты) Ad-Aware (см. рис. 4.4)
Scan Scan Mode Quarantine & Ignore Scheduler	Открывает экран подготовки проверки (рис. 4.5)
Ad-Watch Ad-Watch	Запускает монитор реального времени Ad-Watch
Web Update Web Update Settings	Подключает к Web-узлу Ad-Aware 2007 с целью обновления файла определений угроз и закладок (рис. 4.6)
Tools & Plug-Ins Tools Plug-Ins TrackSweep	Открывает экран расширений функций системы (Add-ons)
Settings Settings	Настраивает систему на потребности пользователя

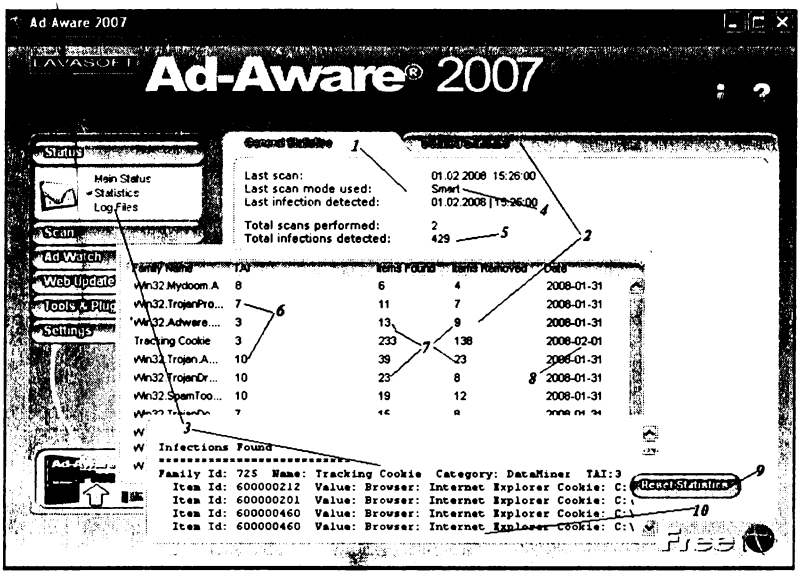


Рис. 4.5. Экраны статистики и протоколов (журналов) проверок:
1 — окно общей статистики; *2* — окно подробной статистики; *3* — окно протокола; *4* — данные о последней выполненной проверке; *5* — совокупные данные, полученные при проверках после установки системы либо после последнего обнуления статистики; *6* — типы (группы) выявленных объектов и соответствующие индексы опасности (TAI — Threat Analysis Index); *7* — количества обнаруженных и удаленных объектов соответствующих категорий; *8* — дата выполнения последней проверки; *9* — кнопка обнуления (сброса) статистики; *10* — протокол, описывающий обнаруженные объекты, выполняющиеся в системе процессы и предпринятые по ним действия

Экраны статистики и просмотра журнала. Кроме экрана состояния защиты, кнопкой меню `Status` могут быть вызваны:

- окна общей и детальной статистики (по соответствующим закладкам, рис. 4.5, *1* и *2*), отражающие результаты ранее выполненных и последней выполненной проверки;
- журнал (протокол) одной из проведенных проверки (рис. 4.5, *3*).

Экран подготовки проверки. Прежде чем приступить к выполнению сканирования, можно обновить файлы определений путем использования WebUpdate (рис. 4.6). Переход к подготовке проверки (установке режима сканирования) осуществляется нажатием кнопки `Scan` Главного меню. Описания элементов данного экрана приводится в табл. 4.5.

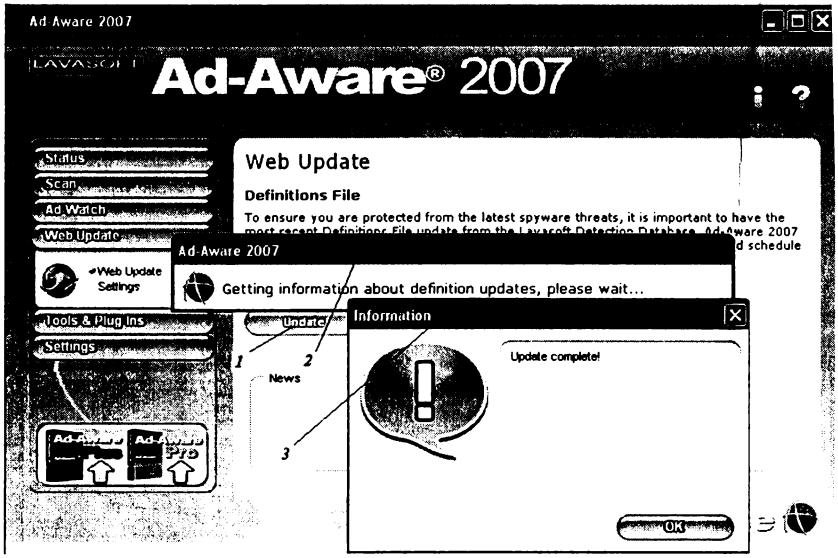


Рис. 4.6. Экран обновления БД описаний угроз:
1 — кнопка запуска загрузки обновлений; *2* — сообщение о поиске обновлений;
3 — информация о завершении обновления БД

Таблица 4.5. **Элементы экрана задания режима проверки**

Элемент	Интерпретация	Действия
`Smart scan`	Быстрая проверка (рис. 4.7, *1*)	Осуществляется проверка памяти, реестра, cookies, избранных файлов. Сканируются каталоги `Windows`, `Temp` и `Program Files`. Режим рекомендуется для ежедневной поверхностной проверки, если ранее была выполнена `Полная проверка`. Кроме того, этот режим не предусматривает поиск в архивных файлах
`Full scan`	Полная проверка (рис. 4.7, *2*)	Режим глубокого исследования ПК на предмет наличия «инфекции» Spyware (рекомендуется для первичного запуска и последующего еженедельного повтора). Режим предусматривает поиск на всех НЖМД и в архивных файлах
`Custom scan`	Использование настройки пользователя (рис. 4.7, *3*)	Ad-Aware SE может быть настроена на анализ определенных дисков или каталогов

Окончание табл. 4.5

Элемент	Интерпретация	Действия
Configure	Настройка	Переход к экрану настроек (Scan Settings — рис. 4.7, *3*). Если на этом экране нажать на ссылку Select folders, то можно перейти к экрану выбора дисков /каталогов (рис. 4.7, *4*)
Active processes	Активные процессы	Проверка всех активных процессов, запущенных на ПК
Registry	Реестр	Проверка известных областей реестра, могущих содержать угрозы
Registry executables	Приложения в реестре	Проверка реестра на наличие ссылок на вредоносные приложения
Hosts file	Списки серверов	Проверка списков серверов, используемых браузером. Их изменения могут быть связаны с атакой на домашнюю страницу браузера
Tracking cookies	Файлы списков навигации	Проверка файлов навигации (Tracking Cookies) для браузеров Internet Explorer, Mozilla Firefox и Opera
Alternate Data Stream (ADS)	Альтернативные потоки данных	Проверка альтернативных потоков данных на присутствие вредоносных объектов
Executable files only	Только исполняемые файлы	Проверка только исполняемых файлов
Archives	Архивы	Проверка содержимого архивов (.zip, .cab и пр.)
Spanned files	Заполненные архивы	Заполненные cab-архивы появляются, когда несколько cab-файлов формируют единичный cab-архив
Possible browser hijacks	Возможные атаки на браузер	Проверка настроек браузера (стартовая и поисковые страницы, списки часто посещаемых узлов и рабочий стол) на наличие подозрительных Web-ссылок
Schedule	Диспетчеризация (рис. 4.7, *5*)	Открывается окно настройки проверок по расписанию
Scan	Проверка (рис. 4.7, *6*)	Начало сканирования системы

Выполнение проверки (Performing Scan). Режим выполнения сканирования (рис. 4.8) активизируется нажатием кнопки Scan экрана задания режима (рис. 4.7).

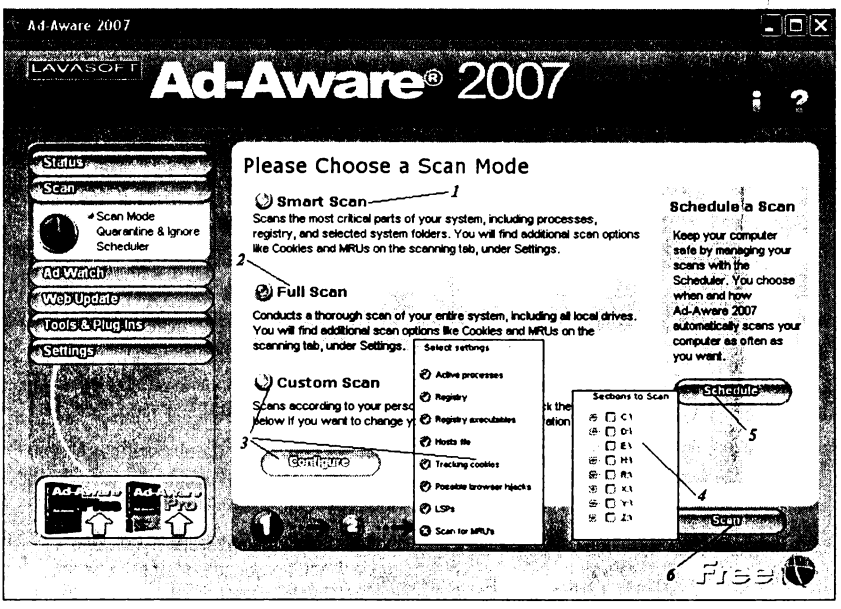


Рис. 4.7. Экран задания режима проверки:
1 — быстрая проверка; *2* — полная проверка; *3* — проверка по усмотрению пользователя; *4* — переход к экранам настройки пользовательского режима проверки (указание дисков, каталогов и пр.); *5* — задание проверок по расписанию; *6* — переход к немедленной проверке компьютера

В процессе выполнения проверки Ad-Aware 2007 антивирусные мониторы, загруженные и выполняющиеся в данной момент, могут выдавать предупреждения о том, что обнаружен вирус во временном каталоге (`%temp%`) активного пользователя. Это не обязательно означает, что компьютер действительно заражен вирусами, поскольку в процессе проверки Ad-Aware 2007 осуществляет временную разархивацию файлов (возможно, зараженных), без активации их содержимого, и этот факт может быть обнаружен антивирусным сканером. Кроме того, многие антивирусные приложения помещают зараженные файлы в карантин, и когда Ad-Aware 2007 проверяет такие файлы, антивирусный сканер может сигнализировать о том, что вирус обнаружен вне карантинного пространства.

Результаты проверки. Экран результатов проверки (`Scan Results`, рис. 4.9) позволяет просмотреть списки обнаруженных объектов, которые разделяются на безусловно опасные (`Critical`

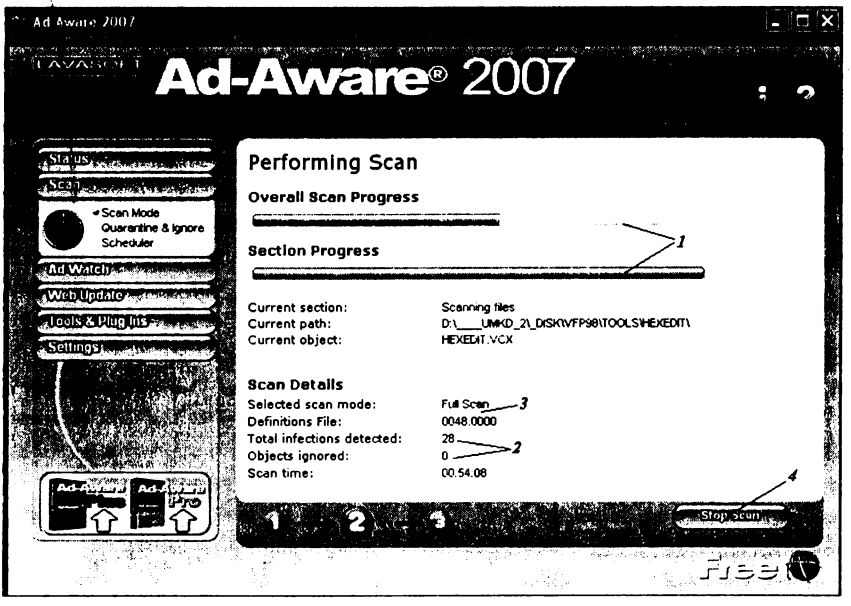


Рис. 4.8. Экран выполнения проверки:
1 — индикатор состояния проверки; *2* — статистика обнаружения угроз и пропуска объектов; *3* — тип проверки и версия используемой БД описания угроз; *4* — кнопка прекращения проверки

`Objects`) и подозрительные (`Privacy Objects`), а также ознакомиться с журналом проверки (`Scan Log`).

`Critical Objects` — список содержит объекты, представляющие собой потенциальную угрозу и предлагаемые на удаление. Они группируются по категориям, каждой из которых приписывается уровень опасности или индекс угрозы (Threat Analysis Index — TAI), который измеряется по 10-балльной шкале, причем «1» соответствует минимальной опасности, а «10» — максимальной.

Для каждого опасного объекта могут быть выполнены следующие действия:

- добавить к списку пропускаемых объектов (`Add to Ignore`) — в этом случае данные объекты не будут проверяться при последующих сканированиях системы;
- поместить в карантин (`Quarantine`) — будучи изолированным, объект не сможет в дальнейшем представлять угрозу для системы;

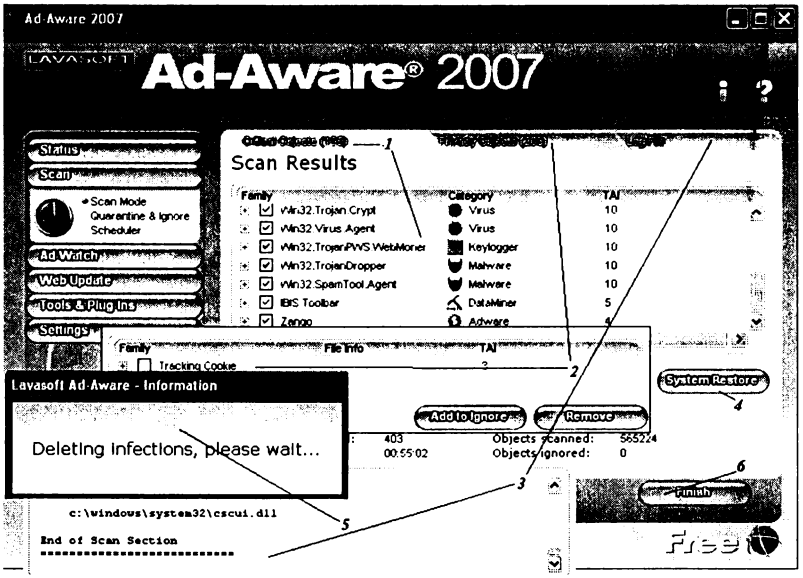


Рис. 4.9. Экран результатов проверки:
1 — список опасных объектов (помечены на удаление); *2* — список подозрительных объектов; *3* — журнал проверки; *4* — кнопка восстановления; *5* — сообщение об удалении помеченных объектов; *6* — кнопка завершения работы

- удалить (`Remove`) — удаление из системы. Перед удалением опасных объектов у пользователя есть возможность создать контрольную точку рестарта системы для ее восстановления в дальнейшем при появлении проблем.

`Privacy objects` — список включает объекты, не представляющие непосредственной угрозы, куда обычно входят индексы навигации браузеров (Tracking Cookies) и часто используемые объекты (Most Recently Used — MRU), которые могут быть удалены по желанию пользователя.

`Scan Log` (Журнал проверки) — показывает файл протокола выполненной проверки (рис. 4.10).

Кроме того, пользователю доступны списки объектов, помещенных в карантин, и тех, которые были пропущены при выполненном сканировании.

Настройки характеристик по умолчанию. Кроме настроек, которые могут быть выполнены пользователем по отношению к конкретной проверке системы (см. табл. 4.5), предусмотрена настройка умолчаний (рис. 4.10), экран которой включает пять за-

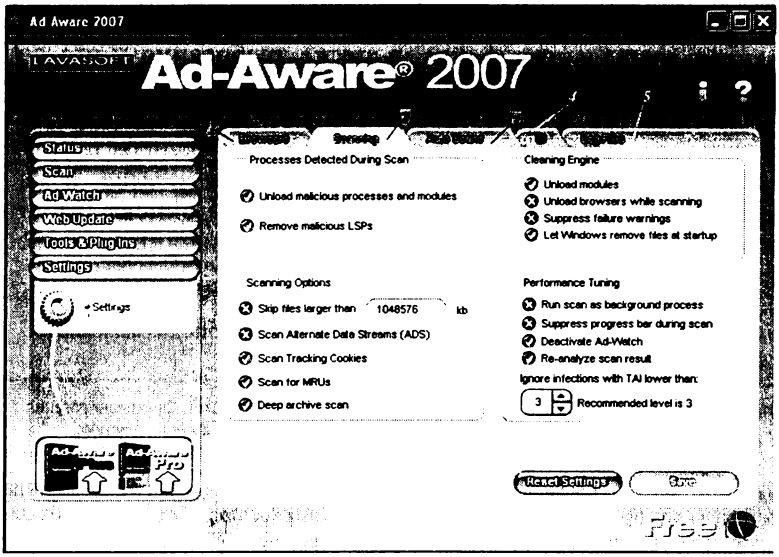


Рис. 4.10. Экран настроек приложения:
1 — настройки браузера по умолчанию; *2* — характеристики сканера; *3* — автоматический запуск сканера; *4* — интерфейс пользователя; *5* — файлы журналов проверки

кладок, управляющих различными аспектами настроек. Перечислим некоторые из них:

- настройки браузеров — задаются домашняя и поисковая страницы браузера, которые в случае их изменения при атаке ЗПС на браузер будут восстановлены;
- режим сканирования — определяются такие параметры, как выгрузка из памяти подозрительных модулей или процессов, отложенное удаление некоторых модулей (при последующем запуске ОС), пропуск при проверке слишком больших файлов, показ или нет элементов экрана сканирования (см. рис. 4.8), сканирование альтернативных потоков данных, индексов навигации, архивов, часто используемых модулей и пр.;
- автосканирование — устанавливаются такие возможности, как автоматический запуск проверки при загрузке ОС, выбор при этом полной или частичной проверки, автоматическое удаление объектов, уровень опасности которых выше определенного предела и пр.;
- интерфейс — позволяет задать вид оболочки, звуковые сигналы при обнаружении угроз или других событиях, язык сообщений или подсказок и т. д.;

- журналы проверок — определяются адрес размещения и имя журнального файла, а также требования к его содержимому, например, записывать ли в него идентификатор компьютера и пользователя, списки игнорируемых объектов, базовые и расширенные настройки сканера и пр.

Некоторые другие программно-технические изделия. В заключение приведем характеристики выборочного списка (табл. 4.6) программно-технических изделий, ориентированных на обеспечение защиты информации в ПК.

Таблица 4.6. **Некоторые программно-технические изделия, предназначенные для защиты информации в ПК**

Программно-техническое изделие	Функции/общий вид изделия	Принципы функционирования и характеристики
`Zbackup` — защита информации при резервном копировании	Зашифровка данных при записи на ленту, CD или DVD и расшифровка при чтении. Ключи шифрования хранятся на смарт-карте, защищенной PIN-кодом. Три попытки неправильного ввода PIN-кода блокируют карту. Предоставляется возможность удаленного ввода ключей шифрования и администрирования системы с любой рабочей станции локальной сети или через Internet	Использование для шифрования данных криптостойких алгоритмов шифрования с длиной ключа от 128 бит. Возможность подключения сертифицированного ФАПСИ криптографического модуля или платы «Криптон», реализующих алгоритм шифрования ГОСТ 28147—89 с длиной ключа 256 бит. Формирование уникальных ключей шифрования на основе последовательности случайных чисел. Возможность подачи сигнала «тревога»
`Zdisk` — защита данных в ноутбуках и на НЖМД	Защита в ситуации похищения ноутбука или изъятия НЖМД и подключения его к другому компьютеру	Создание на НЖМД защищенной области — виртуального логического диска, где информация хранится в зашифрованном виде и доступна только по ключу шифрования. Для работы с защищенными данными следует воспользоваться электронным ключом и ввести пароль. После с виртуальным диском можно работать так же, как с обычным НЖМД или съемным USB-диском. Пароль для «входа под принуждением» позволяет в экстренной ситуации сымитировать системный сбой и потерю защищенных данных

Продолжение табл. 4.6

Программно-техническое изделие	Функции/общий вид изделия	Принципы функционирования и характеристики
`Zserver` — шифрование данных на диске	Защита в случае физического доступа злоумышленника к носителю с конфиденциальной информацией в случаях: размещения серверов в стороннем дата-центре; отправки серверов или НЖМД в ремонт; перевозки компьютеров из одного офиса в другой; утилизации компьютеров, серверов, НЖМД и лент; хранения МЛ в специальном депозитарии; перевозки МЛ, например, в депозитарий; кражи или потери НЖМЛ/МЛ	Защита информации, размещенной на НЖМД, на дисковых массивах (RAID-массивы любых конфигураций) и в хранилищах SAN методом прозрачного шифрования
`Zlock` — разграничение прав доступа пользователей к внешним устройствам и портам рабочих станций в масштабе предприятия	Для каждого физического или логического устройства и для каждого пользователя или группы пользователей из `Active Directory` можно разрешить либо полный доступ, либо только чтение, либо запретить доступ	Подключаемые USB-устройства могут идентифицироваться по любым признакам, таким как класс устройства, код производителя, код устройства, серийный номер и т. д., что позволяет назначать разные права доступа к устройствам. Возможность настройки доступа к устройствам по расписанию. Функция мониторинга клиентских модулей, которая обеспечивает своевременное уведомление о подключениях внешних устройств, как запрещенных, так и разрешенных, а также о попытках несанкционированной деактивации клиентского модуля и изменения настроек системы
`Zlogin` — аутентификация пользователей	Двухфакторная аутентификации пользователей сети с использованием электронных ключей. Пользователь должен предъявить электронный USB-ключ и ввести PIN-код	После загрузки ОС пользователю предлагается вставить ключ и ввести PIN-код. После ввода правильного PIN-кода система считывает с электронного ключа профиль пользователя и осуществляет аутентификацию сначала в Windows-домен или локально на рабочую станцию, и, если эта операция завершена успешно, в NDS (если в профиле имеются соответствующие

Окончание табл. 4.6

Программно-техническое изделие	Функции/общий вид изделия	Принципы функционирования и характеристики
		данные). Если ни один из серверов NDS не доступен, то пользователь может продолжить работу в Windows без доступа к соответствующим ресурсам NetWare
`Printer Activity Monitor` — контроль принтеров	Централизованный контроль всех принтеров организации, выявление и пресечение попыток использования офисных принтеров в личных целях сотрудников	При запуске компьютера модуль `PrinterMon.exe` загружается в память, где находится на протяжении всего сеанса работы с компьютером. Информация о распечатываемых документах (название документа, имя принтера, компьютера, пользователя, количество распечатываемых страниц/байтов, и т. д.) сохраняется в базе данных. Для выдачи отчета о распечатанных документах служит модуль `PrinterActivityMonitor.exe`
«Шкатулка» — устройство стирания информации	Мгновенное уничтожение информации на магнитных носителях	Не требует электропитания; может эксплуатироваться в любых условиях и не требует протяжки магнитной ленты вдоль рабочей области прибора при уничтожении информации; не имеет механических и гидравлических приводов; маскировка под интерьер рабочего стола. Напряженность магнитного поля — 340 кА/м; вес — не более 4 кг; размеры — 145 × 90 × 100 мм; беспрерывная работа — не менее 10 лет
«ПК 2С-994-В1» — устройство уничтожения информации на НЖМД	Уничтожение информации с магнитного носителя непосредственно в системном блоке компьютера вне зависимости от работы пользователя с информацией	Стирание производится нажатием потайной кнопки или дистанционно (радиобрелок). Устанавливается на штатное место 5,25"-устройств. Не имеет с компьютером электрических соединений. Время стирания информации менее 0,1 с. Только внешнее электропитание. Защита жестких дисков, дискет и кассет стримера непосредственно в устройствах чтения-записи. Имеет сертификаты: Управления ГенШтаба МО; МО в системе сертификации «Военный регистр» ГОССТАНДАРТА

Контрольные вопросы

1. Каковы отличительные особенности ПЭВМ как объекта защиты?
2. Каковы потенциальные угрозы информации, обрабатываемой ПЭВМ?
3. Укажите возможные каналы преднамеренного несанкционированного доступа к информации в ПЭВМ.
4. Укажите основные меры защиты информации в ПЭВМ от неквалифицированного нарушителя.
5. Каковы основные функции управления и контроля в ПЭВМ?
6. Укажите возможные каналы НСД к информации ПЭВМ и потенциальные угрозы.
7. Какова схема распределения средств защиты по возможным каналам НСД ПЭВМ?
8. Какие существуют программно-аппаратные средства разграничения доступа к информации в ПЭВМ?
9. Каким образом осуществляется оценка уровня безопасности от преднамеренного НСД в ПЭВМ?
10. Каковы методы защиты информации от преднамеренного несанкционированного доступа при использовании простых средств хранения и обработки информации?
11. Что значит разграничение и контроль доступа к информации?
12. Объясните сущность метода разделения привилегий доступа.
13. Из чего состоит комплекс средств автоматизации и как организуется его обслуживание?
14. Каковы современные основные методы защиты информации в вычислительных системах?
15. Что понимается под идентификацией и установлением подлинности субъекта (объекта)?
16. В чем заключается суть идентификации и установления подлинности технических средств?
17. В чем заключается суть идентификации и установления подлинности документов?
18. В чем заключается суть идентификации и установления подлинности информации на средствах отображения и печати?
19. Объясните суть комплексного подхода к организации систем защиты данных с применением только программных средств.
20. Какие имеются методы и средства защиты информации от случайных воздействий?
21. Какие методы функционального контроля вычислительных систем вы знаете?

Глава 5
КОМПЬЮТЕРНЫЕ ВИРУСЫ И АНТИВИРУСНЫЕ ПРОГРАММЫ

5.1. Компьютерный вирус

Компьютерный вирус — это специально написанная, небольшая по размерам программа (т. е. некоторая совокупность выполняемого кода), которая может «приписывать» себя к другим программам («заражать» их), создавать свои копии и внедрять их в файлы, системные области компьютера и т. д., а также выполнять различные нежелательные действия на компьютере.

История вопроса

По-видимому, самым ранним примером могут служить первые прототипы будущих вирусов — *программы-кролики*. Не причиняя разрушений, они тем не менее были сконструированы так, что многократно копируя себя, захватывали большую часть ресурсов системы, отнимая процессорное время у других задач. История их создания доподлинно не известна. Возможно, они явились следствием программной ошибки, которая приводила к зацикливанию и наделяла программу репродуктивными свойствами. Первоначально кролики (*rabbits*) встречались только на локальных машинах, но с появлением сетей быстро «научились» распространяться по последним.

Затем, в конце 60-х годов была обнаружена саморазмножающаяся по сети APRAnet программа, известная сегодня как *Creeper (Вьюнок)*, которая будто бы была написана Бобом Томасом (Bob Thomas).

Вьюнок проявлял себя текстовым сообщением

```
" i'm the creeper ... catch me.if you can"
(" я вьюнок... поймай меня, если сможешь")
```

и экономно относился к ресурсам пораженной машины, не причиняя ей никакого вреда и разве что слегка беспокоя владельца. Каким бы безвредным Вьюнок ни казался, но он впервые показал, что проникновение на чужой компьютер возможно без ведома и против желания его владельцев.

С появлением Вьюнка родились и первые системы защиты. Теперь компьютеры стали ценностью, которую следовало охранять не только от воров с отмычками и трейлерами (а на чем еще можно было увезти компьютеры того времени?), но и от разрушительных или злоумышленных команд, проникающих по сети или через магнитные носители.

Первым шагом в борьбе против Вьюнка стал Жнец (Reaper), репродуцирующийся наподобие Вьюнка, но уничтожающий все встретившиеся ему копии последнего. Неизвестно, чем закончилась борьба двух программ. Так или иначе от подобного подхода к защите впоследствии отказались. Однако копии обеих программ еще долго бродили по сети.

Так как вирус самостоятельно обеспечивает свое размножение и распространение, пользователь в случае обнаружения вируса должен проверить всю систему, уничтожая копии вируса. Если удалось уничтожить все копии вируса, то можно сказать, что вылечена вся система; в противном случае уцелевшие копии снова размножатся и все неприятности повторятся. Своим названием компьютерные вирусы обязаны определенному сходству с биологическими вирусами:

- по способности к саморазмножению;
- высокой скорости распространения;
- избирательности поражаемых систем (каждый вирус поражает только определенные системы или однородные группы систем);
- способности «заражать» еще незараженные системы;
- трудности борьбы с вирусами и т. д.

В последнее время к этим особенностям, характерным для вирусов компьютерных и биологических, можно добавить еще и постоянно увеличивающуюся быстроту появления модификаций и новых поколений вирусов.

Только если в случае вирусов биологических эту скорость можно объяснить могуществом и изобретательностью природы, то вирусы компьютерные скоростью возникновения новых штаммов обязаны исключительно идеям людей определенного склада ума.

Программа, внутри которой находится вирус, называется «зараженной». Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и «заражает» другие программы, а также выполняет какие-нибудь вредные действия (например, портит файлы или таблицу размещения файлов на диске, «засоряет» оперативную память и т. д.). Для маскировки вируса действия по заражению других программ и нанесению вреда могут выполняться не всегда, а, скажем, при выполнении определенных условий.

Например, вирус Anti-MIT ежегодно 1 декабря разрушает всю информацию на жестком диске, вирус Tea Time мешает вводить информацию с клавиатуры с 15:10 до 15:13, а знаменитый One Half незаметно шифрует данные на жестком диске. В 1989 г. американский студент сумел создать вирус, который вывел из строя около 6000 компьютеров Министерства обороны США. Эпидемия известного вируса Dir-II разразилась в 1991 г. Вирус использовал действительно оригинальную, принципиально новую технологию и на первых порах сумел широко распространиться за счет несовершенства традиционных антивирусных средств. Кристоферу Пайну удалось создать вирусы Pathogen и Queeq, а также вирус Smeg. Именно последний был самым опасным, его можно было накладывать на первые два вируса и из-за этого после каждого прогона программы они меняли конфигурацию. Поэтому их было невозможно уничтожить. Чтобы распространить вирусы, Пайн скопировал компьютерные игры и программы, заразил их, а затем отправил обратно в сеть. Пользователи загружали в свои компьютеры зараженные программы и инфицировали диски. Ситуация усугубилась тем, что Пайн умудрился занести вирусы и в программу, которая с ними боролась. Запустив ее, пользователи вместо уничтожения вирусов получали еще один. В результате действий этого вируса были уничтожены файлы множества фирм, убытки составили миллионы фунтов стерлингов.

Широкую известность получил американский программист Моррис. Он известен как создатель вируса, который в ноябре 1988 г. заразил порядка 7 тысяч персональных компьютеров, подключенных к Internet.

Первые исследования саморазмножающихся искусственных конструкций проводились в середине прошлого столетия. Термин *«компьютерный вирус»* появился позднее — официально его автором считается сотрудник Лехайского университета (США) Ф.Коэн, который ввел его в 1984 г. на 7-й конференции по безопасности информации.

Эксперты считают, что на сегодняшний день число существующих вирусов перевалило за 50 тысяч, причем ежедневно появляется от 6 до 9 новых. «Диких», т. е. реально циркулирующих, вирусов в настоящее время насчитывается около 260.

Классификация вирусов

Один из авторитетнейших «вирусологов» страны Евгений Касперский предлагает условно классифицировать вирусы по следующим признакам:

- по среде обитания вируса;
- по способу заражения среды обитания;
- по деструктивным возможностям;
- по особенностям алгоритма вируса.

Более подробная классификация внутри этих групп представлена в табл. 5.1.

Рассмотрим более подробно некоторые из этих типов вирусов.

Загрузочные вирусы. Известные на сегодня загрузочные вирусы заражают загрузочный (boot) сектор гибкого диска и boot-сектор или главную загрузочную запись (Master Boot Record — MBR) НЖМД. 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 установок BIOS) и передает на него управление.

При заражении дисков загрузочные вирусы «подставляют» свой код вместо какой-либо программы, получающей управление при загрузке системы. Принцип заражения, таким образом, таков: вирус «заставляет» систему при перезапуске отдать управление не оригинальному коду загрузчика, а коду вируса.

Заражение дискет производится единственным известным способом: вирус записывает свой код вместо оригинального кода

Таблица 5.1. **Основные классы вирусов**

Признак	Тип вируса	Пояснения
Среда обитания	Сетевые	Распространяются по компьютерной сети
	Файловые	Внедряются в выполняемые файлы
	Загрузочные	Внедряются в загрузочный сектор диска (`Boot-сектор`) или в сектор, содержащий системный загрузчик винчестера (`Master Boot Record`)
	Комбинированные	Например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные секторы дисков. Такие вирусы, как правило, имеют довольно сложный алгоритм работы и часто применяют оригинальные методы проникновения в систему
Способы заражения	Резидентные	При инфицировании компьютера оставляют в оперативной памяти свою резидентную часть, которая затем перехватывает обращение операционной системы к объектам заражения, и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера
	Нерезидентные	Не заражают память компьютера и являются активными ограниченное время. Некоторые вирусы оставляют в оперативной памяти небольшие резидентные программы, которые не распространяют вирус. Такие вирусы считаются нерезидентными
Деструктивные возможности	Безвредные	Не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения)
	Неопасные	Влияние ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и пр. эффектами
	Опасные	Могут привести к серьезным сбоям в работе
	Очень опасные	Могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти
Особенности алгоритма	Компаньон-вирусы (companion)	Вирусы, не изменяющие файлы. Алгоритм работы этих вирусов состоит в том, что они создают для `exe`-файлов файлы-спутники, имеющие то же самое имя, но с расширением `.com`, например, для файла `xcopy.exe` создается файл `xcopy.com`. Вирус записывается в com-файл и никак не изменяет exe-файл. При запуске такого файла ОС первой обнаружит и выполнит com-файл, т. е. вирус, который затем запустит одноименный exe-файл
	«Черви» (worm)	Распространяются в компьютерной сети и так же, как и компаньон-вирусы, не изменяют файлы или секторы на дисках. Они проникают в память компьютера из компьютерной сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Такие вирусы иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти)
	«Паразитические»	Вирусы, которые при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов. К этой группе относятся все вирусы, которые не являются «червями» или «компаньонами»
	«Студенческие»	Примитивные вирусы, часто нерезидентные и содержащие большое число ошибок
	«Стелс»-вирусы (вирусы-невидимки, stealth)	Представляют собой весьма совершенные программы, которые перехватывают обращения ОС к пораженным файлам или секторам дисков и «подставляют» вместо себя незараженные участки информации. Кроме этого, такие вирусы при обращении к файлам используют достаточно оригинальные алгоритмы, позволяющие «обманывать» резидентные антивирусные мониторы
	«Полиморфик»-вирусы	Самошифрующиеся, или вирусы-призраки (polymorphic), труднообнаруживаемые 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
	Макровирусы	Используют возможности макроязыков, встроенных в системы обработки данных (текстовые редакторы, электронные таблицы и т. д.). Наиболее распространены макровирусы, заражающие текстовые документы редактора Microsoft Word

boot-сектора дискеты. НЖМД может заражаться тремя способами — вирус записывается либо вместо кода MBR, либо вместо кода boot-сектора загрузочного диска (обычно диска c:), либо модифицирует адрес активного boot-сектора в таблице разделов диска (Disk Partition Table), расположенной в MBR НЖМД.

При инфицировании диска вирус в большинстве случаев переносит оригинальный boot-сектор (или MBR) в другую область диска (например, в первый свободный сектор). Если длина вируса больше длины сектора, то в заражаемый сектор помещается начало кода вируса, остальные части размещаются в других секторах (например, в первых незанятых).

Файловые вирусы. По способу заражения файлов эти вирусы образуют следующие классы:

- перезаписывающие (overwriting);
- паразитические (parasitic);
- вирусы-компаньоны (companion);
- вирусы-ссылки (link);
- вирусы, заражающие документы.

Перезаписывающие. Данный метод заражения является наиболее простым, поскольку вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое. Естественно, что после этого файл не восстанавливается. Такие вирусы очень быстро обнаруживают себя, поскольку могут возникнуть серьезные нарушения в работе операционной системы и приложений.

Паразитические. К этой группе относятся все файловые вирусы, которые при распространении своих копий обязательно изменяют содержимое заражаемых файлов, оставляя сами файлы при этом полностью или частично работоспособными. Основными типами таких вирусов являются вирусы, размещающиеся в начало (prepending), в конец (appending) и в середину файла (inserting). В свою очередь, внедрение вирусов в середину файлов происходит различными методами — путем переноса части файла в его конец или копирования вирусного кода в область заведомо неиспользуемых данных файла (cavity-вирусы).

Внедрение вируса в начало файла. Известны два способа внедрения паразитического файлового вируса в начало файла. Первый заключается в том, что вирус переписывает начало заражаемого файла в его конец, а сам помещается на освободившееся место. При заражении файла вторым способом вирус дописывает заражаемый файл к своему телу. Таким образом, при запуске зараженного файла управление получает код вируса. При этом

вирусы, чтобы сохранить работоспособность программы, либо лечат зараженный файл, повторно запускают его, ждут окончания его работы и снова размещаются в его начало (иногда для этого используется временный файл, в котором сохраняется обезвреженный файл), либо восстанавливают код программы в памяти компьютера и настраивают необходимые адреса в ее теле (т. е. выполняют функции ОС).

Внедрение вируса в конец файла. Наиболее распространенным способом внедрения вируса в файл является дописывание вируса в его конец. При этом вирус изменяет начало файла таким образом, что первыми выполняемыми командами программы, содержащейся в файле, являются команды вируса. Для того чтобы получить управление при старте файла, вирус корректирует стартовый адрес программы (адрес точки входа). Для этого вирус производит необходимые изменения в заголовке файла.

Внедрение вируса в середину файла. Существует несколько путей внедрения вируса в середину файла. В наиболее простом случае вирус перемещает участок файла в его конец или «раздвигает» файл и записывает свой код в освободившееся пространство. Некоторые вирусы при этом сжимают переносимый блок файла так, что длина файла при заражении не изменяется. Вторым является метод «cavity», при котором вирус записывается в заведомо неиспользуемые области файла. Вирус может быть скопирован в незадействованные области заголовка `exe`-файла, в промежутки между секциями `exe`-файлов или в область текстовых сообщений популярных компиляторов. Существуют вирусы, заражающие только те файлы, которые содержат блоки, заполненные каким-либо постоянным байтом, при этом вирус записывает свой код вместо такого блока. Кроме того, копирование вируса в середину файла может произойти в результате ошибки вируса, и в этом случае файл может быть необратимо испорчен.

Вирусы без точки входа. Отдельно следует отметить довольно незначительную группу вирусов, не имеющих «точки входа» (EPO-вирусы — Entry Point Obscuring viruses). К ним относятся вирусы, не изменяющие адрес точки старта в заголовке `exe`-файлов. Такие вирусы записывают команду перехода на свой код в какое-либо место файла и получают управление не при запуске зараженного файла, а при вызове процедуры, содержащей код передачи управления на тело вируса. Причем выполняться эта процедура может крайне редко (например, при выводе сообщения о какой-либо специфической ошибке). В результате вирус

может долгое время находиться внутри файла и проявить себя только при некоторых ограниченных условиях. Перед тем как записать в середину файла команду перехода на свой код, вирусу необходимо выбрать «правильный» адрес в файле — иначе зараженный файл может оказаться испорченным. Известно несколько способов, с помощью которых вирусы определяют такие адреса внутри файлов, например, поиск в файле последовательности стандартного кода заголовков процедур языков программирования (C/Pascal), дизассемблирование кода файла или замена адресов импортируемых функций.

Компаньоны. К этой группе относятся вирусы, не изменяющие заражаемых файлов, и алгоритм их работы состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т. е. вирус. При заражении вирус переименовывает файл, запоминает его (для последующего запуска файла-хозяина) и записывает свой код на диск под именем заражаемого файла. Например, файл `notepad.exe` переименовывается в `notepad.exd`, а вирус записывается под именем `notepad.exe`. При запуске управление получает код вируса, который затем запускает оригинальный `notepad`.

Возможно существование и других типов вирусов-компаньонов, использующих иные оригинальные идеи или особенности других операционных систем. Например, `path`-компаньоны, которые размещают свои копии в корневом каталоге Windows, используя тот факт, что этот каталог является первым в списке `path`, и файлы для запуска Windows в первую очередь будут искать именно здесь. Данным способом самозапуска пользуются также многие компьютерные черви и троянские программы.

Прочие способы заражения. Существуют вирусы, которые не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они копируют свой код в какие-либо каталоги дисков в расчете на то, что эти новые копии будут когда-либо запущены пользователем. Иногда эти вирусы дают своим копиям «специальные» имена, чтобы подтолкнуть пользователя на их запуск — например, `install.exe` или `winstart.bat`.

Некоторые вирусы записывают свои копии в архивные файлы (`arj`, `zip`, `rar`), а другие — команду запуска зараженного файла в `bat`-файлы.

Link-вирусы также не изменяют физического содержимого файлов, однако при запуске зараженного файла принуждают ОС выполнить вирусный код. Этой цели они достигают модификацией необходимых полей файловой системы.

Автономные (вирусы-программы). Со временем вирусы, внедряющие свой код в тело других программ, сдали свои позиции во многом по той причине, что размеры вирусов выросли, а укрыть код размером в сотни килобайт довольно сложно. В итоге «исполняемые» вирусы перестали маскироваться и превратились в независимые программы, не нуждающиеся в «хозяине-переносчике». Сразу же перед авторами вирусов возникла проблема: как заставить пользователей загрузить этот вирус и запустить у себя на машине?

Программные вирусы, написанные для операционной системы Windows, обычно маскируются под разные утилиты — например, под ключи к условно-бесплатных программам, мультимедийные презентации, обновления для операционной системы или даже антивирусные программы. Большинство вирусов пользователи запускают на своем компьютере самостоятельно.

Для борьбы с подобными вирусами одной антивирусной программы недостаточно и главным условием безопасности является обязательная и регулярная загрузка обновлений к Windows (файлов-«заплаток», предназначенных для закрытия уже обнаруженных брешей в системе защиты операционной системы).

Полиморфные вирусы — вирусы, модифицирующие свой код в зараженных программах таким образом, что два экземпляра одного и того же вируса могут не совпадать ни в одном бите. Такие вирусы не только шифруют свой код, используя различные пути шифрования, но и содержат код генерации шифровщика и расшифровщика, что отличает их от обычных шифровальных вирусов, которые также могут шифровать участки своего кода, но имеют при этом постоянный код шифровальщика и расшифровщика.

Цель такого шифрования заключается в невозможности проанализировать его код с помощью обычного дизассемблирования. Этот код зашифрован и представляет собой бессмысленный набор команд. Расшифровка производится самим вирусом уже непосредственно во время выполнения. При этом возможны варианты: он может расшифровать себя всего сразу, а может выполнить такую расшифровку «по ходу дела», может вновь шифровать уже отработавшие участки. Все это делается ради затруднения анализа кода вируса.

Стелс-вирусы. В ходе проверки компьютера антивирусные программы считывают данные — файлы и системные области с жестких дисков и дискет, пользуясь средствами операционной системы и базовой системы ввода-вывода BIOS. Ряд вирусов после запуска оставляют в оперативной памяти компьютера специальные модули, перехватывающие обращение программ к файловой системе компьютера. Если такой модуль обнаруживает, что программа пытается прочитать зараженный файл или системную область диска, он на ходу подменяет читаемые данные.

Стелс-вирусы обманывают антивирусные программы и в результате остаются незамеченными. Тем не менее существует простой способ отключить механизм маскировки стелс-вирусов. Достаточно загрузить компьютер с незараженной системной дискеты и сразу, не запуская других программ с диска компьютера (которые также могут оказаться зараженными), проверить компьютер антивирусной программой.

При загрузке с системной дискеты вирус не может получить управление и установить в оперативной памяти резидентный модуль, реализующий стелс-механизм. Антивирусная программа сможет прочитать информацию, действительно записанную на диске, и легко обнаружит вирус.

Макровирусы. В отличие от классических вирусов, эти паразитировали не на исполняемых файлах, а на документах, подготовленных в популярных программах из комплекта Microsoft Office. В текстовый редактор Microsoft Word и табличный редактор Microsoft Excel был встроен свой собственный язык программирования — Visual Basic for Applications (VBA), предназначенный для созданий специальных дополнений к редакторам — макросов. Эти макросы сохранялись в теле документов Microsoft Office и легко могли быть заменены вирусами. После открытия зараженного файла вирус активировался и заражал все документы Microsoft Office на НЖМД.

Одна из самых мощных атак макровирусов была зарегистрирована в марте 1999 г., когда вирус Melissa, созданный программистом Д. Смитом, за несколько часов распространился по всему миру. И хотя этот вирус был сравнительно безопасным (Melissa ограничивалась тем, что заражала все существующие документы и рассылала свои копии людям, внесенным в адресную книгу Microsoft Outlook), его появление заставило Microsoft срочно оснастить программы Microsoft Office защитой от запуска макросов. При открытии любого документа, содержащего встро-

енные макросы, Word и Excel запрашивают подтверждение пользователя.

Скрипт-вирусы. Макровирусы являются одной из разновидностей большого семейства вредоносных программ — скрипт-вирусов. Их выделение связано с тем фактором, что именно макровирусы положили начало всему этому семейству, к тому же вирусы, ориентированные на программы Microsoft Office получили наибольшее распространение. Следует отметить также, что скрипт-вирусы являются подгруппой файловых вирусов и написаны на различных скрипт-языках (VBS, JS, BAT, PHP и т. д.).

Общая черта скрипт-вирусов — это привязка к одному из «встроенных» языков программирования. Каждый вирус привязан к конкретным изъянам в защите одной из программ Windows и представляет собой не самостоятельную программу, а набор инструкций, которые заставляют в общем-то безобидный «движок» программы совершать не свойственные ему разрушительные действия.

Большая часть скрипт-вирусов распространяется через электронную почту (такие вирусы чаще называют Internet-червями). Пожалуй, ярчайшими представителями этого семейства являются вирусы `LoveLetter` и `AnnaKournikova`, атаки которых пришлись на сезон 2001—2002 г. Оба этих вируса использовали один и тот же прием, основанный не столько на слабости защиты операционной системы, сколько на неопытности пользователей. Хитрость создателей вируса проста — файл, который показался нам картинкой, имел двойное расширение, например `AnnaKournikova.jpg.vbs`.

Второе расширение является истинным типом файла, в то время как первое является частью его имени, а поскольку расширение `vbs` Windows хорошо «знакомо», ОС прячет его от глаз пользователей, оставляя на экране лишь имя `AnnaKournikova.jpg`.

Следует отметить, что в качестве вложения в письмо относительно безопасны только файлы типов `txt`, `jpg`, `gif`, `tif`, `bmp`, `mp3`, `wma`.

К безусловно опасных типам файлов относятся: `asx`, `bas`, `bat`, `cmd`, `com`, `cpl`, `crt`, `exe`, `inf`, `ins`, `js`, `msc`, `msi`, `pif`, `reg`, `vbs`.

Кроме вирусов, к вредоносным программам принято относить также инструментальные средства, способствующие созданию вирусов и укрытию их от средств антивирусной защиты.

PolyEngine — полиморфные генераторы. Полиморфные генераторы не являются вирусами в прямом смысле этого слова, по-

скольку в их алгоритм не закладываются функции размножения, т. е. открытия, закрытия и записи в файлы, чтения и записи секторов и т. д. Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика.

Обычно полиморфные генераторы распространяются их авторами без ограничений в виде файла-архива. Основным файлом в архиве любого генератора является объектный модуль, содержащий этот генератор. Во всех встречавшихся генераторах этот модуль содержит внешнюю (external) функцию — вызов программы генератора.

Constructor — конструкторы вирусов и троянских программ или VirTools. Конструкторы вирусов и троянских программ — это утилиты, предназначенные для изготовления новых компьютерных вирусов и «троянцев» и/или их изучения в хакерских целях. Известны конструкторы вирусов для DOS, Windows и макровирусов. Они позволяют генерировать исходные тексты вирусов, объектные модули и/или непосредственно зараженные файлы.

Некоторые конструкторы снабжены стандартным оконным интерфейсом, где с помощью системы меню можно выбрать тип вируса, поражаемые объекты, наличие или отсутствие самошифровки, противодействие отладчику, внутренние текстовые строки, выбрать эффекты, сопровождающие работу вируса и т. п. Прочие конструкторы не имеют интерфейса и считывают информацию о типе вируса из конфигурационного файла.

FileCryptor, PolyCryptor — скрытие от антивирусных программ. Это хакерские утилиты, использующиеся для шифрования других вредоносных программ с целью скрытия их содержимого от антивирусной проверки

Алгоритмы вирусов

Рассмотрим схему функционирования простейшего загрузочного вируса, заражающего дискеты. При включении компьютера управление передается программе начальной загрузки, которая хранится в постоянно запоминающем устройстве (ПЗУ).

Эта программа тестирует оборудование и при успешном завершении проверок пытается найти дискету в дисководе `A:`.

Всякая дискета размечена на *секторы* и *дорожки*, секторы объединяются в кластеры.

Среди секторов есть несколько служебных, используемых операционной системой для собственных нужд (в этих секторах не могут размещаться данные пользователя). Среди служебных секторов представляет интерес один — так называемый сектор начальной загрузки (boot-sector).

В секторе начальной загрузки хранится информация о дискете — количество поверхностей, количество дорожек, количество секторов и пр. Но интересна не эта информация, а небольшая программа начальной загрузки (ПНЗ), которая должна загрузить саму операционную систему и передать ей управление.

Таким образом, нормальная схема начальной загрузки следующая:

ПНЗ (ПЗУ) — ПНЗ (диск) — СИСТЕМА

Теперь рассмотрим вирус. В загрузочных вирусах выделяют две части — так называемые голову и хвост. Хвост, вообще говоря, может быть пустым.

Пусть имеются чистая дискета и зараженный компьютер, под которым понимается компьютер с активным резидентным вирусом. Как только этот вирус обнаружит, что в дисководе появилась подходящая среда — в рассматриваемом случае не защищенная от записи и еще не зараженная дискета, он приступает к заражению. Заражая дискету, вирус производит следующие действия:

- выделяет некоторую область диска и помечает ее как недоступную операционной системе, это можно сделать по-разному, в простейшем и традиционном случае занятые вирусом секторы помечаются как сбойные (bad);
- копирует в выделенную область диска свой хвост и оригинальный (здоровый) загрузочный сектор;
- замещает программу начальной загрузки в загрузочном секторе (настоящем) своей головой;
- организует цепочку передачи управления согласно схеме.

Таким образом, голова вируса теперь первой получает управление, вирус устанавливается в память и передает управление оригинальному загрузочному сектору. В цепочке

ПНЗ (ПЗУ) — ПНЗ (диск) — СИСТЕМА

появляется новое звено:

ПНЗ (ПЗУ) — ВИРУС — ПНЗ (диск) — СИСТЕМА

Была рассмотрена схема функционирования простого загрузочного («бутового») вируса, располагающегося в загрузочных секторах дискет. Как правило, вирусы способны заражать не только загрузочные секторы дискет, но и загрузочные секторы

жестких дисков — винчестеров. При этом в отличие от дискет на винчестере имеются два типа загрузочных секторов, содержащих программы начальной загрузки, которые получают управление. При загрузке компьютера с винчестера первой берет на себя управление программа начальной загрузки в MBR. Если жесткий диск разбит на несколько разделов, то лишь один из них помечен как загрузочный (boot). Программа начальной загрузки в MBR находит загрузочный раздел винчестера и передает управление на программу начальной загрузки этого раздела. Код последней совпадает с кодом программы начальной загрузки, содержащейся на обычных дискетах, а соответствующие загрузочные секторы отличаются только таблицами параметров. Таким образом, на винчестере имеются два объекта атаки загрузочных вирусов — программа начальной загрузки в MBR и программа начальной загрузки в boot-секторе загрузочного диска.

Приведем обобщенный пример структуры программы-вируса. Она состоит из псевдокоманд DOS и подпрограмм — маленьких внутренних программ (составляющие их инструкции хранятся отдельно от главной программы), выполняющих некоторые специальные функции всякий раз, когда к ним обращаются.

```
this := findfile
LOAD (this)
loc := search (this)
insert (loc)
STORE (this)
```

Подпрограмма под названием `findfile` обращается к каталогу выполняемых файлов или программ на диске, берет произвольное имя файла и присваивает имя этого файла переменной `this` (этот). В следующей строке программы используется псевдокоманда DOS `LOAD` (загрузить), с помощью которой файл помещается в оперативную память компьютера.

Другая подпрограмма под названием `search` (поиск) просматривает только что загруженную программу в поисках инструкции, которая могла бы послужить подходящим местом, куда можно занести вирус. Когда процедура `search` находит такую инструкцию, она определяет соответствующий номер строки и присваивает его в качестве значения переменной `loc`. Теперь все готово для того, чтобы подпрограмма-вирус могла проникнуть в произвольно выбранную из каталога программу.

Подпрограмма `insert` (вставить) заменяет выбранную инструкцию другой (например такой, как вызов подпрограммы). Замененная инструкция передает управление блоку команд, составляющих главное тело подпрограммы-вируса, которая присоединяется к концу программы. Затем к концу добавленной подпрограммы присоединяется инструкция, возвращающая управление «зараженной» программе на инструкцию, следующую за вставленной. Таким образом, когда выполняется подпрограмма-вирус, выполняется также и подмененная инструкция зараженной программы. Исходная программа работает так, будто ничего особенного не произошло. Однако на самом деле подпрограмма-вирус воспользовалась каким-то мгновением, чтобы захватить власть над средствами операционной системы и прицепить свою копию к еще одной программе, хранящейся на диске. Приведенный пример демонстрирует лишь один из приемов, используемых авторами вирусов. В настоящее время специалисты выделили и другие приемы, отличающиеся друг от друга идеями и изощренностью выполнения.

Признаки проявления вируса

При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов. К ним можно отнести следующие:

- прекращение работы или неправильная работа ранее успешно функционировавших программ;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов;
- изменение размеров файлов;
- неожиданное значительное увеличение количества файлов на диске;
- существенное уменьшение размера свободной оперативной памяти;
- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- частые зависания и сбои в работе компьютера.

Следует отметить, что вышеперечисленные явления необязательно вызываются присутствием вируса, а могут быть следствием других причин. Поэтому всегда затруднена правильная диагностика состояния компьютера.

5.2. Методы защиты. Антивирусы

Каким бы ни был вирус, пользователю необходимо знать основные методы защиты от компьютерных вирусов.

Для защиты от вирусов можно использовать:

- общие средства защиты информации, которые полезны так же, как и страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя;
- профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
- специализированные программы для защиты от вирусов.

Имеются две основные разновидности общих средств защиты информации, обеспечивающие:

- копирование информации — создание копий файлов и системных областей дисков;
- разграничение доступа, которое предотвращает несанкционированное использование информации, в частности защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются антивирусными.

Классы антивирусных программ

Существует несколько классификаций антивирусных программ. В соответствии с одной из них известные к настоящему времени антивирусные программы по функциональным признакам делятся на четыре класса:

- класс А — предупреждение заражения;
- класс Б — выявление последствий заражения;

- класс В — минимизация причиненного ущерба;
- класс Г — общего характера.

Программы класса А делятся на пять групп следующего назначения:

- А1 — фильтры, следящие за операциями других исполняемых программ и реагирующие на подозрительные действия;
- А2 — резидентные детекторы и фаги, следящие за появлением в оперативной памяти конкретных вирусов и подающие при их появлении специальные сигналы оператору;
- А3 — иммунизаторы, изменяющие файлы и области оперативной памяти таким образом, что вирус их после этого не заражает;
- А4 — разграничители доступа, ограничивающие распространение вирусов путем разграничения доступа к ресурсам ЭВМ, программам и массивам данных со стороны других программ и пользователей;
- А5 — преобразователи параметров операционной среды, реализующие изменение соглашений, принятых в операционной системе (форматы записей, команды, расположение системной информации и др.), недоступные разработчикам вирусов и тем самым препятствующие заражению ЭВМ.

Программы класса Б делятся на шесть групп следующего функционального назначения:

- Б1 — нерезидентные детекторы и фаги, осуществляющие просмотр запоминающих устройств, определяющие зараженность файлов и дисков и организующие их лечение;
- Б2 — программы проверки подозрительных характеристик, осуществляющие просмотр запоминающих устройств и выявление таких характеристик, которые могут говорить о наличии вируса в системе. К таким характеристикам относятся недопустимые значения отдельных полей в заголовке файла, подозрительные переходы, странные изменения в программах и т. п.;
- Б3 — программы, осуществляющие просмотр файлов и носителей, определение различных их характеристик (контрольные суммы, криптографические суммы, длины, даты и времена создания и др.) и сравнение этих величин с эталонами в целях определения возможного заражения;

- Б4 — программы, осуществляющие слежение и регистрацию в системном журнале операций, осуществляемых на ЭВМ. При заражении анализ журнала помогает выявить источник заражения, характер поведения вируса;
- Б5 — программы-ловушки (дрозофилы, уловители), специально выделяемые для заражения, которые, заражаясь, сигнализируют о наличии вируса;
- Б6 — программы автономной защиты файла, защищающие файлы от вирусов путем дописывания своей копии к защищаемым модулям.

Программы класса В (минимизирующие ущерб, причиненный заражением РПС) делятся на следующие три группы:

- В1 — программы полного копирования, предназначенные для создания резервных копий программного обеспечения;
- В2 — программы частичного копирования, предназначенные для копирования и восстановления наиболее уязвимых частей диска (Boot-сектор, FAT, корневое оглавление);
- В3 — программы, прерывающие вычислительный процесс, т. е. осуществляющие принудительное прерывание вычислительного процесса в целях локализации распространения вируса.

Программы класса Г (общего назначения) предназначены не для прямой борьбы с вирусами, а для оказания помощи в этой борьбе. Эти программы делятся на пять групп следующего назначения:

- Г1 — программы просмотра диска, позволяющие отображать значения каждого сектора, копировать одну физическую область в другую. Применяются для определения целостности отдельных частей диска, наличия вируса в файлах и внесения небольших изменений;
- Г2 — программы, позволяющие искать на диске контекст определенного содержания. С их помощью можно найти участки кодов вирусов и пораженные ими секторы;
- Г3 — программы, позволяющие восстанавливать отдельные части диска;
- Г4 — программы, реализующие просмотр состояния оперативной памяти, состав и характеристики находящихся там модулей;
- Г5 — программы, позволяющие упорядочить информацию на диске на физическом уровне по заранее заданному закону.

Существуют и другие подходы к этой классификации. Различают, например, следующие виды антивирусных программ:

- программы-детекторы;
- программы-доктора или фаги;
- программы-ревизоры;
- программы-фильтры;
- программы-вакцины или иммунизаторы.

Программы-детекторы осуществляют поиск характерного для конкретного вируса кода (сигнатуры) в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

Программы-доктора или фаги, а также программы-вакцины не только находят зараженные вирусами файлы, но и «лечат» их, т. е. удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к «лечению» файлов. Среди фагов выделяют полифаги, т. е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов. Наиболее известные из них: Aidstest, Scan, Norton AntiVirus, Doctor Web.

Учитывая, что постоянно появляются новые вирусы, программы-детекторы и программы-доктора быстро устаревают и требуется регулярное обновление версий.

Антивирусы-полифаги. Антивирусы-полифаги — наиболее распространенные средства по борьбе с вредоносными программами. Исторически они появились первыми и до сих пор удерживают несомненное лидерство в этой области.

В основе работы полифагов стоит простой принцип — поиск в программах и документах знакомых участков вирусного кода (так называемых *сигнатур* вирусов). В общем случае сигнатура — это такая запись о вирусе, которая позволяет однозначно идентифицировать присутствие вирусного кода в программе или документе. Чаще всего сигнатура — это непосредственно участок вирусного кода или его контрольная сумма (дайджест).

Первоначально антивирусы-полифаги работали по очень простому принципу — осуществляли последовательный просмотр файлов на предмет нахождения в них вирусных программ. Если сигнатура вируса была обнаружена, то производилась процедура удаления вирусного кода из тела программы или доку-

мента. Прежде чем начать проверку файлов, программа-фаг всегда проверяет оперативную память. Если в оперативной памяти оказывается вирус, то происходит его деактивация. Это вызвано тем, что зачастую вирусные программы производят заражение тех программ, которые запускаются или открываются в тот момент, когда вирус находится в активной стадии (это связано со стремлением экономить на усилиях по поиску объектов заражения). Таким образом, если вирус останется активным в памяти, то тотальная проверка всех исполняемых файлов приведет к тотальному заражению системы.

В дальнейшем вирусные программы значительно усложнились. Например, появились так называемые «stealth-вирусы». В основе их работы лежит тот факт, что операционная система при обращении к периферийным устройствам (в том числе и к жестким дискам) использует механизм прерываний. Здесь необходимо сделать небольшое отступление на тему «Как работает механизм прерываний». При возникновении прерывания управление передается специальной программе — «Обработчику прерываний». Эта программа отвечает за ввод и вывод информации в/из периферийного устройства. Кроме того, прерывания делятся на уровни взаимодействия с периферией (в нашем случае — с жесткими и гибкими дисками). Есть уровень операционной системы (в среде MS DOS — прерывание `25h`) есть уровень базовой системы ввода-вывода (уровень BIOS — прерывание `13h`). Опытные системные программисты могут работать и напрямую, обращаясь к портам ввода-вывода устройств. Но это довольно серьезная и трудная задача. Столь многоуровневая система сделана, прежде всего, с целью сохранения переносимости приложений. Именно благодаря такой системе, скажем, оказалось возможным осуществлять запуск DOS-приложений в многозадачных средах типа MS Windows или IBM OS/2.

Но в такой системе изначально скрыта и уязвимость: управляя обработчиком прерываний, можно управлять потоком информации от периферийного устройства к пользователю. Stealth-вирусы, в частности, используют механизм перехвата управления при возникновении прерывания. Заменяя оригинальный обработчик прерывания своим кодом, stealth-вирусы контролируют чтение данных с диска.

В случае, если с диска читается зараженная программа, вирус «выкусывает» собственный код (обычно код не буквально «выкусывается», а происходит подмена номера читаемого секто-

ра диска). В итоге пользователь получает для чтения «чистый» код. Таким образом, до тех пор, пока вектор обработчика прерываний изменен вирусным кодом, сам вирус активен в памяти компьютера, обнаружить его простым чтением диска средствами операционной системы невозможно. Схожий механизм маскировки используется и загрузочными вирусами, о которых будет сказано дальше. В целях борьбы со stealth-вирусами ранее рекомендовалось (и, в принципе, рекомендуется и сейчас) осуществлять альтернативную загрузку системы с гибкого диска и только после этого проводить поиск и удаление вирусных программ. В настоящее время загрузка с гибкого диска может оказаться проблематичной (для случая с win32 — антивирусными приложениями запустить их не удастся). Ввиду всего вышесказанного, антивирусы-полифаги оказываются максимально эффективными только при борьбе с уже известными вирусами, т. е. с такими, чьи сигнатуры и методы поведения знакомы разработчикам.

Только в этом случае вирус со 100%-ной точностью будет обнаружен и удален из памяти компьютера, а потом — и из всех проверяемых файлов. Если же вирус неизвестен, то он может достаточно успешно противостоять попыткам его обнаружения и лечения. Поэтому главное при пользовании любым полифагом — как можно чаще обновлять версии программы и вирусные базы.

Эвристические анализаторы. Существует большое количество вирусов, алгоритм которых практически скопирован с алгоритма других вирусов. Как правило, такие вариации создают непрофессиональные программисты, которые по каким-то причинам решили написать вирус. Для борьбы с такими «копиями» и были придуманы эвристические анализаторы. С их помощью антивирус способен находить подобные аналоги известных вирусов, сообщая пользователю, что у него, похоже, завелся вирус. Естественно, надежность эвристического анализатора не 100 %, но все же его коэффициент полезного действия больше 50 %. Вирусы, которые не распознаются антивирусными детекторами, способны написать только наиболее опытные и квалифицированные программисты.

Эвристическим анализатором кода называется набор подпрограмм, анализирующих код исполняемых файлов, памяти или загрузочных секторов для обнаружения в нем разных типов компьютерных вирусов. Основной частью эвристического анализатора является эмулятор кода. Эмулятор кода работает в режиме про-

смотра, т. е. его основная задача — не выполнять код, а выявлять в нем всевозможные события, т. е. совокупность кода или вызов определенной функции операционной системы, направленные на преобразование системных данных, работу с файлами, или обнаруживать часто используемые вирусные конструкции. Грубо говоря, эмулятор просматривает код программы и выявляет те действия, которые эта программа совершает. Если действия этой программы укладываются в какую-то определенную схему, то делается вывод о наличии в программе вирусного кода.

Конечно, вероятность как пропуска, так и ложного срабатывания весьма высока. Однако правильно используя механизм эвристики, пользователь может самостоятельно прийти к верным выводам. Например, если антивирус выдает сообщение о подозрении на вирус для единичного файла, то вероятность ложного срабатывания весьма высока. Если же такое повторяется на многих файлах (а до этого антивирус ничего подозрительного в этих файлах не обнаруживал), то можно говорить о заражении системы вирусом с вероятностью, близкой к 100 %. Одним из наиболее мощных эвристических анализаторов обладает антивирус Dr.Web.

Использование эвристического анализатора, помимо всего вышеперечисленного, позволяет также бороться с *вирус-генераторами* и *полиморфными вирусами*.

Классический метод определения вирусов по сигнатуре в этом случае вообще оказывается неэффективен. Вирус-генератор — это специализированный набор библиотек, который позволяет пользователю легко сконструировать свой собственный вирус, даже имея слабые познания в программировании. К написанной программе подключаются библиотеки генератора, вставляются в нужных местах вызовы внешних процедур — и вот элементарный вирус превратился в достаточно сложный продукт. Самое печальное, что в этом случае сигнатура вируса будет каждый раз другая, поэтому отследить вирус оказывается возможным только по характерным вызовам внешних процедур — а это уже работа эвристического анализатора. Полиморфный вирус имеет еще более сложную структуру. Само тело вируса видоизменяется от заражения к заражению, при этом сохраняя свое функциональное наполнение.

В простейшем случае — если разбросать в теле вируса случайным образом ничего не исполняющие, пустые операторы (типа «`mov ax, ax`» или «`nop`»), то тело вирусного кода претер-

пит значительные изменения, а алгоритм останется прежним. В этом случае на помощь также приходит эвристический анализатор.

Программы-ревизоры. Программы-ревизоры относятся к самым надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран монитора. Как правило, сравнение состояний производят сразу после загрузки операционной системы. При сравнении проверяются длина файла, код циклического контроля (контрольная сумма файла), дата и время модификации, другие параметры. Программы-ревизоры имеют достаточно развитые алгоритмы, обнаруживают стелс-вирусы и могут даже очистить изменения версии проверяемой программы от изменений, внесенных вирусом. К числу программ-ревизоров относится широко распространенная в России программа Adinf.

Антивирусные программы-ревизоры позволяют обнаружить вирус. Чаще всего обнаружением вируса дело и заканчивается. Существует блок лечения для популярного антивируса-ревизора Adinf, так называемый Cure Module, но такой блок позволяет лечить лишь те файлы, которые не были заражены на момент создания базы данных программы. Однако обнаружить вирус на компьютере (или даже подозрение на него) антивирусы-ревизоры могут с большой степенью надежности. Обычно наиболее оптимальным является связка полифаг и ревизор. Ревизор служит для обнаружения факта заражения системы. Если система заражена, то в дело пускается полифаг. Если же ему не удалось уничтожить вирус, то можно обратиться к разработчику антивирусных средств — скорее всего, на компьютер попал новый, неизвестный разработчикам вирус.

Основу работы ревизоров составляет контроль за изменениями, характерными для работы вирусных программ. В них содержится информация: о контрольных суммах неизменяемых файлов, содержимом системных областей, адресах обработчиков прерываний, размере доступной оперативной памяти и т. п. Вся остальная работа ревизора состоит в сравнении текущего состояния диска с ранее сохраненными данными, поэтому крайне важно, чтобы все контрольные таблицы создавались не на зараженной машине. Только в этом случае работа ревизора будет

достаточно эффективной. Итак, перейдем к стадиям работы программы-ревизора.

Контроль оперативной памяти. Эта стадия проверки включает в себя процедуры обнаружения следов активных загрузочных и stealth-вирусов в памяти компьютера. Если такие алгоритмы будут найдены, выдается соответствующее предупреждение. Обычно сначала программа ищет уже знакомые вирусы. Далее программа проверяет, изменился ли обработчик `Int13h`. Если он изменился, то с вероятностью 90 % можно сказать, что компьютер инфицирован загрузочным вирусом (загрузочные вирусы вынуждены перехватывать это прерывание с тем, чтобы после своей активизации передать управление «нормальному» загрузочному сектору и система загрузилась без сбоев). Ревизор выдает предупреждение об этом и сообщает адрес в памяти, по которому находится новый обработчик `Int13h`. В принципе информация о местонахождении обработчика необходима программистам и системным администраторам, а рядовому пользователю следует обратить внимание на предупреждение. Даже если ревизор устанавливается на уже зараженный вирусом компьютер и реальный адрес обработчика `Int13h` маскируется вирусом, в 85 % случаев ревизору удается обнаружить истинный адрес обработчика `Int13h` в BIOS и работать, используя его. Если по каким-либо причинам ревизору не удалось получить реальный адрес обработчика, то выдается предупреждение. Истинный адрес обработчика прерывания достигается путем пошагового просмотра тела вируса (по алгоритму своей работы загрузочный вирус вынужден, в конце концов, передавать управление оригинальному обработчику).

Некоторые вирусы блокируют трассировку прерываний: при попытке трассировать их коды они приводят систему к «зависанию», перезагружают компьютер и т. д. Поэтому, если при трассировке прерываний компьютер начинает вести себя «странно», то следует быть очень осторожным — не исключено, что оперативная память поражена вирусом.

Важным параметром является и размер свободной оперативной памяти. Обычно ревизор запускается самым первым, до загрузки каких-либо программ. Если же размер оперативной памяти уменьшился — это верный признак присутствия в ОЗУ еще какой-то программы. Скорее всего, программа эта — вирус.

Контроль системных областей. Контроль системных областей предназначен для обнаружения вирусов, которые использу-

ют для своей активации механизм загрузки. Первой с диска загружается загрузочная запись (boot record), которая содержит в себе мини-программу, управляющую дальнейшей загрузкой. Для жесткого диска первой производится загрузка главной загрузочной записи (MasterBootRecord или MBR).

Необходимо дать некоторые пояснения, связанные с обнаружением загрузочных вирусов. В случае если система поражена загрузочным вирусом, то именно ему передается управление при попытке загрузиться с пораженного диска. В этом опасность вируса — если поражен жесткий диск, то управление вирусу будет передаваться при каждом включении компьютера. Загрузочные вирусы в чистом виде передаются исключительно через дискеты, причем заражение осуществляется при попытке загрузиться с пораженной дискеты. Со временем использование дискет вообще и загрузочных дискет, в частности, сократилось до минимума. Однако способ захвата управления оказался столь удобен, что в настоящее время очень распространены вирусы, которые могут поражать как файлы, так и загрузочные секторы. Попав на «чистый» компьютер, такие вирусы первым делом поражают главную загрузочную запись. Однако методы обнаружения именно загрузочных вирусов в настоящее время крайне эффективны и приближаются к 100 % надежности.

Чтобы понять, как происходит обнаружение вируса, рассмотрим обнаружение такого вируса «вручную». Произведем загрузку с чистой дискеты (при этом прерывание `13h` гарантированно не будет перехвачено загрузочным вирусом) и рассмотрим сектор 0/0/1 винчестера (это физический адрес сектора главной загрузочной записи). Если винчестер разделен (с помощью `fdisk`) на логические диски, то код занимает приблизительно половину сектора и начинается с байтов `FAh33hC0h` (вместо `33h` иногда может быть `2Bh`). Заканчиваться код должен текстовыми строками типа «Missing operating system». В конце сектора размещаются внешне разрозненные байты таблицы разделов. Нужно обратить внимание на размещение активного раздела в таблице разделов. Если операционная система расположена на диске `C:`, а активны 2-й, 3-й или 4-й разделы, то вирус мог изменить точку старта, сам разместившись в начале другого логического диска (заодно нужно посмотреть и там). Но также это может говорить о наличии на машине нескольких операционных систем и какого-либо boot-менеджера, обеспечивающего выборочную загрузку. Проверяем всю нулевую дорожку. Если она чистая, т. е. секторы содер-

жат только байт-заполнитель, все в порядке. Наличие мусора, копий сектора 0/0/1 и прочего может говорить о присутствии загрузочного вируса. Впрочем, антивирусы при лечении загрузочных вирусов лишь «обезглавливают» противника (восстанавливают исходное значение сектора 0/0/1). Проверяем boot-сектор MS-DOS, он обычно расположен в секторе 0/1/1. Его внешний вид для сравнения можно найти на любой «чистой» машине. Примерно таким же способом действуют и программы-ревизоры. Их особенность в том, что они не могут судить об изначальной «чистоте» оперативной памяти, поэтому чтение Master Boot Record происходит тремя различными способами:

- (bios) — прямым обращением в BIOS;
- (`i13h`) — чтением через BIOS-прерывание `Int13h`;
- (`i25h`) — чтением средствами операционной системы (прерывание `Int25h`).

Если считанная информация не совпадает, налицо действие stealth-алгоритмов. Для большей надежности производится чтение MBR через IDE-порты жесткого диска. До сих пор еще не встречались вирусы, которые могут маскироваться от ревизора, обладающего такой функцией.

Аналогичным образом проводится проверка и простого (не главного) загрузочного сектора.

Обычно за счет того, что ревизор сохраняет резервную копию системных областей, восстановление повреждений от загрузочного вируса происходит довольно просто: если пользователь дает на то свое согласие, ревизор просто записывает системные области заново.

Контроль неизменяемых файлов. Последняя стадия проверки, направленная на обнаружение деятельности файловых вирусов, — контроль изменения файлов. Для всех файлов, которые активно используются и в то же время не должны изменяться (обычно это программы типа `win.com` и т. п.), создаются контрольные таблицы. В них содержатся значения контрольных сумм и размеров файлов. Затем, в ходе дальнейшего использования ревизора, информация с дисков сравнивается с эталонной, хранящейся в таблицах. Если информация не совпадает, то весьма вероятно нахождение в системе файлового вируса. Самый явный признак — изменение размера или содержимого файла без изменения даты создания файла.

Очень важно определить, какие именно файлы являются неизменяемыми. При настройке программы ревизора данные о не-

изменяемых файлах заносятся в таблицы, содержащие список имен файлов и каталогов, подлежащих контролю ревизором. Каждая строка таблицы содержит одно имя или маску. В принципе, рекомендуется внести в разряд «неизменяемых» те исполняемые файлы, путь к которым указан в переменной PATH. Они чаще всего становятся жертвой файловых вирусов.

После того как все файлы проверены, ревизоры часто сохраняют копии дополнительных областей памяти, которые могут быть испорчены вирусами. Это FLASH- и CMOS-память. Эти области памяти также изменяются достаточно редко и поэтому их изменения могут быть подозрительны.

Еще раз отметим, что наиболее эффективной антивирусной защитой будет использование «связки» ревизор — полифаг. Ревизор позволяет отследить активность вируса на диске, а полифаг служит для проверки новых файлов, а также удаления уже известных вирусов.

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

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

При попытке какой-либо программы произвести указанные действия «сторож» посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Программы-фильтры весьма полезны, так как способны обнаружить вирус на самой ранней стадии его существования до размножения. Однако они не «лечат» файлы и диски. Для уничтожения вирусов требуется применить другие программы, например фаги. К недостаткам программ-сторожей можно отнести их «назойливость» (например, они постоянно выдают предупреждение о любой попытке копирования исполняемого файла), а также возможные конфликты с другим программным обеспечением. Примером программы-фильтра является программа `Vsafe`, входящая в состав пакета утилит MS DOS.

Вакцины, или иммунизаторы, — это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, «лечащие» от вируса.

Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. В настоящее время программы-вакцины имеют ограниченное применение.

5.3. Некоторые примеры антивирусных программ

Программа-полифаг Aidstest

Aidstest — это программа-полифаг предыдущего поколения. Первая версия, способная обнаруживать один вирус, была выпущена в 1988 г. Вскоре программа стала признанным лидером на российском рынке антивирусных программ. Последняя версия Aidstest вышла осенью 1997 г. и больше эта программа не поддерживается. Все вирусы, входившие в вирусную базу Aidstest, сегодня включены в сканер нового поколения Doctor Web.

Антивирус Касперского 6.0

Антивирус Касперского 6.0 **Антивирус Касперского 6.0** — это принципиально новый подход к защите информации. Главное в приложении — это объединение и заметное улучшение текущих функциональных возможностей всех продуктов компании в одно комплексное решение защиты. Приложение обеспечивает не только антивирусную защиту, но и защиту от неизвестных угроз.

Главное окно Антивируса Касперского (АК) условно можно разделить на две части:

- левая часть окна (*навигационная*) позволяет перейти к любому компоненту, к выполнению задач поиска вирусов, к сервисным функциям приложения;
- правая часть окна (*информационная*) содержит информацию по выбранному в левой части компоненту защиты, позволяет перейти к настройке каждого из них, предоставляет инструменты для выполнения задач поиска вирусов, для работы с файлами на карантине и резервными копиями, для управления лицензионными ключами и т. д.

Если выбрать в левой части окна какой-либо раздел или компонент, в правой части можно получить полную информацию, соответствующую сделанному выбору (рис. 5.1).

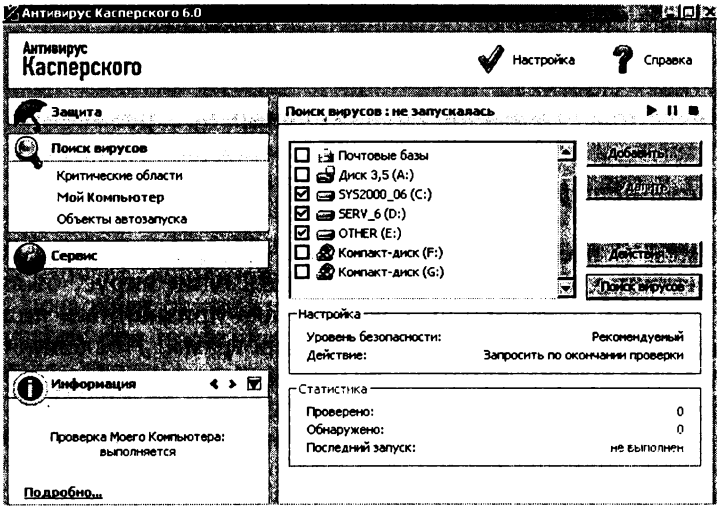
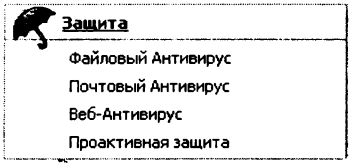


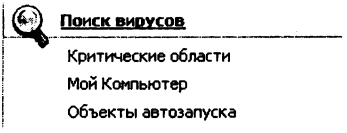
Рис. 5.1. Главное окно

Рассмотрим подробнее элементы навигационной панели главного окна (рис. 5.2):

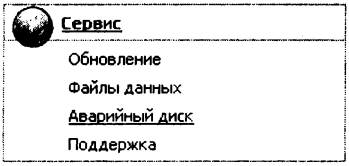
- раздел `Защита` — дает возможность просмотреть общую информацию о работе АК, ознакомиться с общей статистикой работы приложения, убедиться, все ли компоненты корректно работают. Чтобы просмотреть параметры работы конкретного компонента защиты, следует в разделе `Защита` выбрать название этого компонента;
- `Поиск вирусов` — содержит список объектов, каждый из которых может быть проверен на присутствие вирусов. Это задачи поиска вирусов в критических областях, среди объектов автозапуска, а также полная проверка компьютера;
- `Сервис` (включает дополнительные функции АК). Здесь можно перейти к обновлению приложения, просмотреть отчеты о работе любого из компонентов или задач Антивируса Касперского, перейти к работе с объектами на карантине, с резервными копиями, к информации о технической поддержке, к созданию диска аварийного восстановления системы и к окну управления лицензионными ключами;



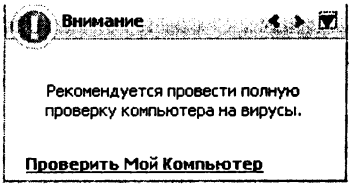
а



б



в



г

Рис. 5.2. Разделы навигационной части Главного окна:
а — Защита (информация о статусе защиты компьютера); *б* — Поиск вирусов (для проверки компьютера на присутствие вредоносных объектов); *в* — Сервис; *г* — Комментарии и советы

- Раздел комментариев и советов сопровождает работу с приложением. В этом разделе можно прочесть совет о том, как повысить степень защиты компьютера. Здесь же приводятся комментарии к текущей работе приложения и его параметрам. С помощью ссылок данного раздела можно перейти к выполнению рекомендуемых в конкретном случае действий или более подробно ознакомиться с информацией.

Компоненты защиты. Защита компьютера в реальном времени обеспечивается следующими компонентами (рис. 5.3, *а*).

Файловый Антивирус. Файловая система может содержать вирусы и другие опасные программы, причем вредоносные программы могут годами храниться в файловой системе, проникнув однажды со съемного диска или из Internet, и никак не проявлять себя. Однако стоит только открыть зараженный файл, как вирус активизируется.

Файловый Антивирус — компонент, контролирующий файловую систему компьютера. Он проверяет все открываемые, запускаемые и сохраняемые файлы на компьютере и всех присоединенных дисках. Каждое обращение к файлу перехватывается приложением, и файл проверяется на присутствие известных вирусов. Дальнейшая работа с файлом возможна толь-

ко в том случае, если файл не заражен или был успешно вылечен Антивирусом. Если же файл по каким-либо причинам невозможно вылечить, он будет удален, при этом копия файла будет сохранена в резервном хранилище, или помещен на карантин.

Почтовый Антивирус. Электронная почтовая корреспонденция широко используется злоумышленниками для распространения вредоносных программ. Она является одним из основных средств распространения червей. Поэтому крайне важно контролировать все почтовые сообщения.

Почтовый Антивирус — компонент проверки всех входящих и исходящих почтовых сообщений ПК. Он анализирует электронные письма на присутствие вредоносных программ. Письмо будет доступно адресату только в том случае, если оно не содержит опасных объектов.

Веб-Антивирус. Открывая в Internet различные веб-сайты, вы рискуете заразить компьютер вирусами, которые будут установлены на компьютер с помощью скриптов, содержащихся на веб-страницах, а также загрузить опасный объект на свой компьютер.

Веб-Антивирус специально разработан для предотвращения подобных ситуаций. Данный компонент перехватывает и блокирует выполнение скрипта, расположенного на веб-сайте, если он представляет угрозу. Строгому контролю также подвергается весь http-трафик.

Проактивная защита. С каждым днем вредоносных программ становится все больше, они усложняются, комбинируя в себе несколько видов, методы распространения становятся все более сложными для обнаружения.

Для того чтобы обнаружить новую вредоносную программу еще до того, как она успеет нанести вред, «Лабораторией Касперского» разработан специальный компонент — Проактивная защита. Он основан на контроле и анализе поведения всех программ, установленных на данном компьютере. На основании выполняемых действий АК принимает решение, является программа потенциально опасной или нет. Таким образом, компьютер защищен не только от уже известных вирусов, но и от новых, еще не исследованных.

Задачи поиска вирусов. Помимо защиты всех источников проникновения вредоносных программ крайне важно периодически проводить проверку вашего компьютера на присутствие вирусов. Это необходимо делать для того, чтобы исключить возможность

распространения вредоносных программ, которые не были обнаружены компонентами защиты из-за, например, установленного низкого уровня защиты или по другим причинам.

Для поиска вирусов в состав АК включены три задачи (рис. 5.2, *б*).

Критические области. Проверка на присутствие вирусов всех критических областей компьютера. К ним относятся: системная память, объекты, исполняемые при старте системы, загрузочные секторы дисков, системные каталоги *Windows*. Цель задачи — быстрое обнаружение в системе активных вирусов, без запуска полной проверки компьютера.

Мой Компьютер. Поиск вирусов на компьютере с тщательной проверкой всех подключенных дисков, памяти, файлов (рис. 5.3).

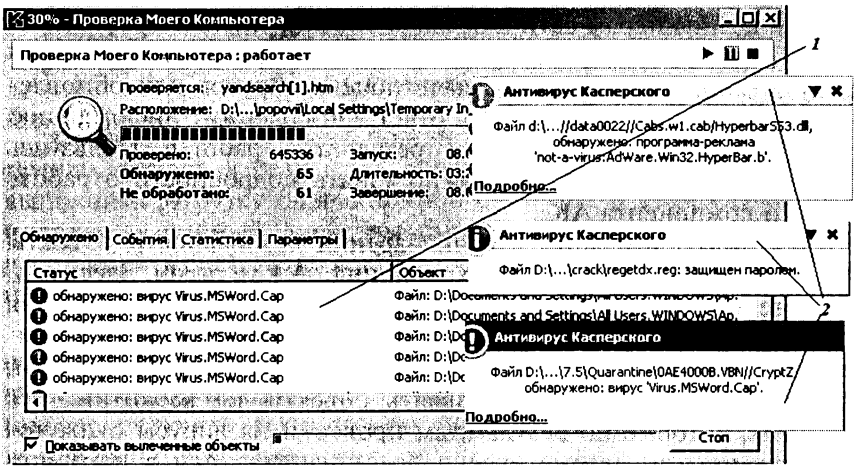


Рис. 5.3. Информационное окно протокола проверки (закладка `Обнаружено`): *1* — журнал событий; *2* — всплывающие информационные окна событий

Объекты автозапуска. Проверка на присутствие вирусов объектов, загрузка которых осуществляется при старте операционной системы, а также оперативной памяти и загрузочных секторов дисков.

Также предусмотрена возможность создавать другие задачи поиска вирусов и формировать расписание их запуска. Например, можно создать задачу проверки почтовых баз раз в неделю или задачу поиска вирусов в каталоге `Мои документы`.

Сервисные функции приложения. АК включает ряд сервисных функций. Они предусмотрены для поддержки приложения в актуальном состоянии, расширения возможностей использования приложения, для оказания помощи в работе (рис. 5.3, ***в***).

Обновление. Чтобы всегда быть готовым отразить любую хакерскую атаку, уничтожить вирус или другую опасную программу, необходимо поддерживать Антивирус Касперского в актуальном состоянии. Для этого предназначен компонент *Обновление.* Он отвечает за обновление сигнатур угроз и модулей приложения Антивируса Касперского, используемых в работе приложения.

Сервис копирования обновлений позволяет сохранять обновления баз сигнатур угроз, сетевых драйверов, а также модулей приложения, полученных с серверов «Лаборатории Касперского», в локальном каталоге, а затем предоставлять доступ к ним другим компьютерам сети в целях экономии Internet-трафика.

Файлы данных. В процессе работы приложения по каждому компоненту защиты, задаче поиска вирусов или обновлению приложения формируется отчет. Он содержит информацию о выполненных операциях и результаты работы. Пользуясь функцией `Отчеты`, всегда можно узнать подробности о работе любого компонента АК.

Все подозрительные с точки зрения безопасности объекты АК переносит в специальное хранилище — `Карантин`. Здесь они хранятся в зашифрованном виде, чтобы избежать заражения компьютера. Пользователь может проверять эти объекты на присутствие вирусов, восстанавливать в исходном местоположении, удалять, самостоятельно добавлять объекты на карантин. Все объекты, которые по результатам проверки на вирусы окажутся незараженными, автоматически восстанавливаются в исходном местоположении.

В `Резервное хранилище` помещаются копии вылеченных и удаленных приложением объектов (рис. 5.4). Данные копии создаются на случай необходимости восстановить объекты или картину их заражения. Резервные копии объектов также хранятся в зашифрованном виде, чтобы избежать заражения компьютера. Всегда можно восстановить объект из резервного хранилища в исходном местоположении или удалить копию.

Аварийный диск. В состав Антивируса Касперского включен специальный сервис, позволяющий создавать диск аварийного восстановления системы.

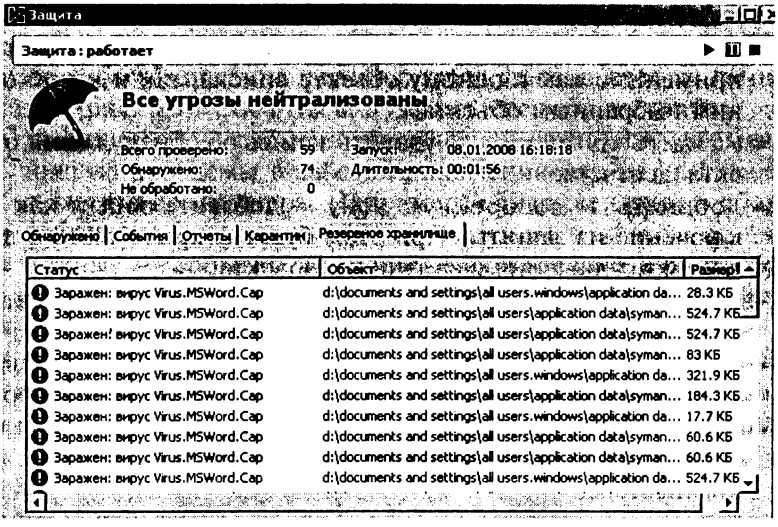


Рис. 5.4. Резервное хранилище

Создание такого диска полезно на случай повреждения системных файлов в результате вирусной атаки и невозможности выполнить загрузку операционной системы. В этом случае, используя аварийный диск, вы сможете загрузить компьютер и восстановить систему до состояния, предшествующего вредоносному воздействию.

Поддержка. Все зарегистрированные пользователи Антивируса Касперского могут воспользоваться Службой технической поддержки. Для того чтобы узнать о том, где именно вы можете получить техническую поддержку, следует воспользоваться функцией `Поддержка`.

Закладка Обнаружено — содержит список опасных объектов, обнаруженных АК (см. рис. 5.3). Для каждого объекта указываются его полное имя и статус, присвоенный приложением при его проверке/обработке. Чтобы список содержал не только опасные объекты, но и те, что были успешно обезврежены, следует установить флажок `Показывать вылеченные объекты`.

Можно произвести ряд действий над объектами списка, для этого следует нажать на кнопку `Действия` и в раскрывшемся меню выбрать одну из альтернатив:

- `Лечить` — произвести попытку лечения опасного объекта. Если обезвредить объект не получится, он может быть ос-

тавлен в этом списке для отложенной проверки с обновленными сигнатурами угроз или удален. Данное действие применимо как к одному объекту списка, так и к нескольким выбранным объектам;

- `Удалить из списка` — удалить запись об обнаружении объекта из отчета;
- `Добавить в доверенную зону` — добавить объект как исключение из защиты. При этом будет открыто окно с правилом исключения для данного объекта;
- `Показать файл` — открыть Microsoft Windows Explorer на каталоге, где расположен данный объект;
- `Лечить все` — обезвредить все объекты списка. АК попытается обработать объекты с использованием сигнатур угроз;
- `Очистить` — очистить отчет об обнаруженных объектах. При этом все обнаруженные опасные объекты останутся на компьютере;
- `Посмотреть на www.viruslist.ru` — перейти к описанию объекта в Вирусной энциклопедии на сайте «Лаборатории Касперского»;
- `Посмотреть на www.google.com` — найти информацию об объекте с помощью поисковой системы;
- `Поиск` — задать условия поиска объекта в списке по имени или статусу;
- `Выделить все` — выбрать все объекты списка. Это может понадобиться для выполнения групповых действий над объектами;
- `Копировать` — скопировать строку отчета в буфер. Далее эта информация может быть вставлена в текстовый файл или электронное сообщение.

Кроме того, предусмотрена возможность сортировки информации, представленной в окне по возрастанию и убыванию каждого из столбцов.

Обработка опасных объектов, обнаруженных в ходе работы АК, выполняется с помощью кнопок `Лечить` (для одного объекта или группы выбранных объектов) или `Лечить все` (для обработки всех объектов списка). При обработке каждого объекта на экран будет выведено уведомление о необходимости принятия решения о дальнейших действиях над ним. Если в окне уведомления установить флажок `Применить во всех подобных случаях`, то выбранное действие будет применено ко всем объектам с тем же статусом, выбранным в списке перед началом обработки.

Закладка События — полный список всех важных событий в работе компонента защиты или при выполнении задачи поиска вирусов либо обновления сигнатур угроз фиксируется на данной закладке (рис. 5.5). События могут быть следующих типов:

- критические — события критической важности, указывающие на проблемы в работе приложения или на уязвимости в защите компьютера. Например, обнаружен вирус, сбой в работе;
- важные — события, на которые обязательно нужно обратить внимание, поскольку они отображают важные ситуации в работе приложения. Например, `Прервано`;
- информационные — события справочного характера, как правило, не несущие важной информации. Например, `ok, не обработан`. Данные события отображаются в журнале событий только в том случае, если установлен флажок `Показывать все события`.

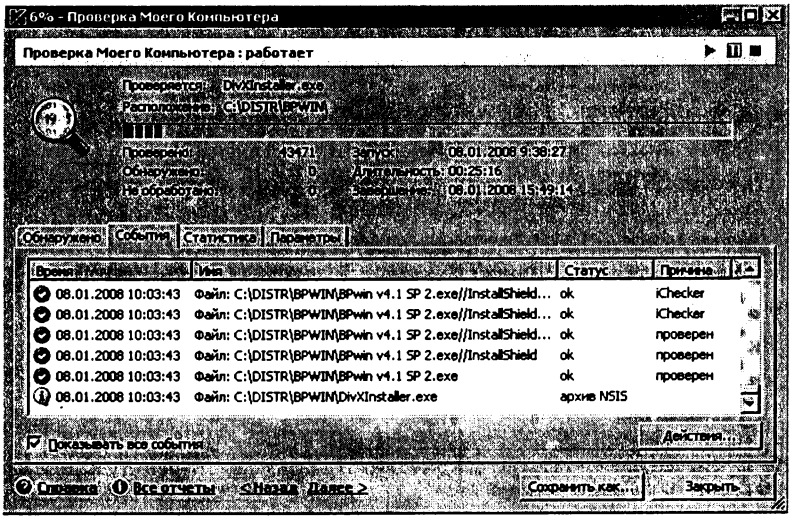


Рис. 5.5. Закладка `События`

Формат представления событий в журнале событий может различаться в зависимости от компонента или задачи. Так, для задачи обновления приводится:

- название события;
- имя объекта, для которого зафиксировано это событие;

- время, когда произошло событие;
- размер загружаемого файла.

Для задачи поиска вирусов журнал событий содержит имя проверяемого объекта и статус, присвоенный объекту в результате проверки/обработки.

Закладка Статистика. На данной закладке фиксируется подробная статистика работы компонента или выполнения задачи поиска вирусов (рис. 5.6). Здесь можно получить следующую информацию:

- сколько объектов было проверено на наличие опасных объектов в текущем сеансе работы компонента или при выполнении задачи. В том числе указано количество проверенных архивов, упакованных файлов, защищенных паролем и поврежденных объектов;
- сколько было обнаружено опасных объектов, сколько из них не вылечено, удалено и помещено на карантин.

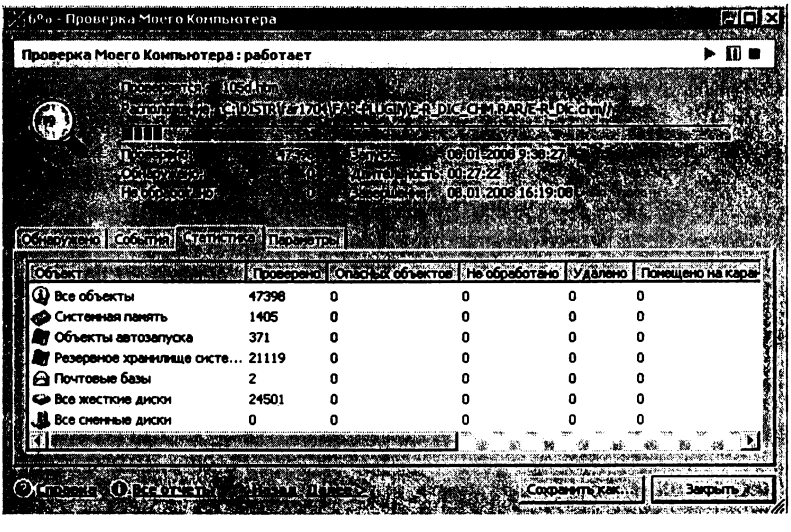


Рис. 5.6. Закладка Статистика

Антивирус-ревизор диска ADinf для Windows

К достоинствам ревизора Adinf (Advanced Diskinfoscope) можно отнести то, что он позволяет реализовать контроль целостности не только программ, но и информационных файлов и работа-

ет с диском непосредственно по секторам путем прямого обращения к функциям BIOS без использования функций DOS. Такой способ проверок полностью исключает маскировку Stealth-вирусов и обеспечивает весьма высокую скорость проверок.

Перед инсталляцией и первым запуском ревизора следует с помощью имеющихся сканеров, например DrWeb или AidsTest, осуществить тщательный поиск и обезвреживание вирусов в оперативной памяти и на всех логических дисках компьютера. Кроме того, нужно не забыть проанализировать файлы конфигурирования и настройки на предмет отсутствия вызовов несанкционированных программ. При обнаружении такие вызовы следует удалить, а также установить и устранить причину их появления.

В процессе инсталляции ревизора Adinf осуществляется добавление строки его вызова в файл `AUTOEXEC.BAT` и при первом запуске ревизора формируются следующие эталонные характеристики компьютерной системы:

- объем занимаемой оперативной памяти;
- адрес обработчика прерывания 13h, используемого операционной системой и программами для низкоуровневого доступа к дискам;
- код внесистемного загрузчика, таблица разделов и вторичные загрузочные записи жестких дисков;
- количество и адреса расположения сбойных кластеров логических дисков;
- структура системных областей логических дисков каждого винчестера;
- контрольные суммы содержимого файлов с программами, а также их системные характеристики: путь, дата и время создания, длина, значения атрибутов, адреса физического расположения.

При следующих запусках Adinf выполняет проверки на соответствие эталонным характеристикам в следующей последовательности:

- проверяется объем занятой оперативной памяти и адрес обработчика прерывания 13h;
- анализируются главная и вторичные загрузочные записи жестких дисков;
- проверяются загрузочные секторы логических дисков каждого винчестера;
- анализируется количество и адреса сбойных кластеров логических дисков;

- проверяются деревья каталогов заданных логических дисков;
- сверяются характеристики и контрольные суммы файлов.

Обнаруженные изменения анализируются и если они безобидны, например изменения даты и времени создания, то Adinf помещает информацию об изменениях в список, который можно просмотреть и принять. Если же происходят подозрительные изменения, то ревизор предупреждает об этом пользователя.

К подозрительным изменениям относятся следующие:

- изменение объема доступной оперативной памяти или адреса обработчика прерывания 13h;
- изменения в системных областях жестких дисков;
- появление новых сбойных кластеров;
- изменение контрольных сумм заданных файлов;
- изменение длины файлов без изменения даты и времени модификации;
- изменение файлов с появлением странных даты и времени модификации, например 35 марта.

Новые сбойные кластеры на винчестере могут появиться после использования таких утилит проверки и восстановления дисковой памяти, как NDD, ScanDisk, Calibrat и других, которые могли сами пометить неустойчивые или дефектные кластеры как сбойные.

При обнаружении изменений в загрузочных записях жестких дисков Adinf автоматически восстанавливает их исходное содержимое по эталонной информации с выдачей сообщения пользователю.

При обнаружении этих и других изменений следует установить их причину.

Если несвоевременно была обновлена системная информация, ее следует обновить.

Наиболее вероятной причиной изменения загрузчиков и программных файлов является заражение компьютерным вирусом. Следует также учитывать, что некоторые программы могут сами изменять файлы своего хранения, модифицируя в них какие-либо параметры настройки.

В любом случае при обнаружении изменений загрузчиков и программных файлов необходимо приступить к поиску и обезвреживанию вирусов, для этого можно использовать любые транзитные сканеры.

Главное окно. Управление программой осуществляется с помощью кнопок на главном окне или с помощью контекстных меню, вызываемых по нажатию правой кнопки «мыши».

Главное окно может находиться в четырех состояниях. Вид и назначение управляющих элементов (кнопок) в этих состояниях могут изменяться.

Для получения справки об элементах главного окна необходимо подвести к ним указатель «мышки» и нажать на левую кнопку.

Программа может находиться в следующих состояниях:

1. Исходное состояние.
2. Состояние сканирования.
3. Сканирование завершено.
4. Ожидание начала сканирования при автозапуске.

В последнем режиме программа находится, если установлена задержка начала сканирования при автоматической проверке дисков при загрузке Windows.

В режиме ожидания главная управляющая кнопка позволяет прервать ожидание и начать сканирование, кнопка Выход позволяет завершить ADinf32. Также возможно изменить установки сканирования без CRC и режима обновления таблиц. Другие управляющие элементы недоступны.

По истечении заданного времени задержки ADinf32 автоматически переходит в режим сканирования. Задержка бывает полезна, чтобы не замедлять запуск других приложений, стартующих при загрузке Windows.

ADinf32 может работать в четырех режимах:

- построения таблиц — рис. 5.7;
- проверки дисков — рис. 5.8;
- поиска стелс-вирусов;
- просмотра истории изменений.

Режим построения таблиц запускается для всех отмеченных в главном окне дисков, для которых не существуют таблицы ADinf32, если нажать кнопку `Старт` или выбрать пункт `Обработать` отмеченные диски в общем контекстном меню.

В режиме построения таблиц сначала производится сканирование диска, в процессе которого считывается загрузочный сектор, формируется список сбойных кластеров, проходится дерево каталогов, вычисляются контрольные суммы файлов. Сканирование диска производится без участия операционной системы.

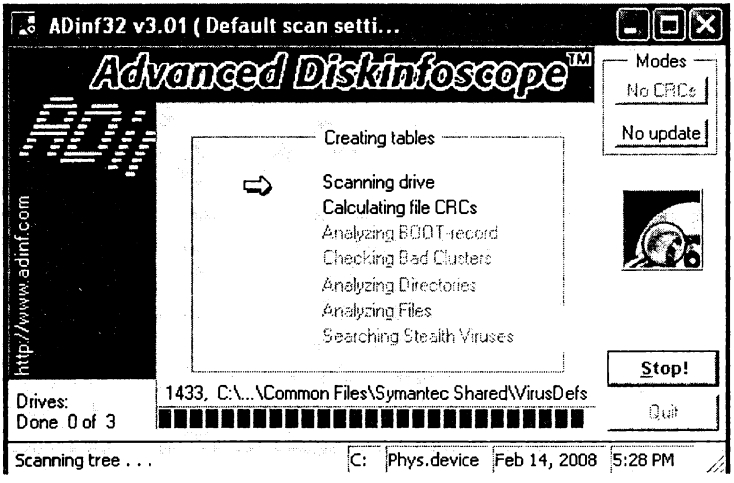


Рис. 5.7. Главное окно. Режим создания таблиц

ADinf32 самостоятельно разбирает структуру файловых систем, читая диск по секторам.

Когда сканирование завершено, собранная информация для каждого диска записывается в таблицах ADinf32.

Если для диска уже существуют таблицы ADinf32, то для запуска режима построения таблиц необходимо предварительно удалить существующие таблицы. Удалить таблицы для всех отмеченных дисков можно через общее контекстное меню главного окна. Для одного диска таблицы можно удалить через контекстное меню диска.

Режим проверки дисков. Режим проверки запускается для всех отмеченных в главном окне дисков, для которых существуют таблицы ADinf32, если нажать кнопку `Старт` или выбрать пункт `Обработать` отмеченные диски в общем контекстном меню — рис. 5.8.

Режим проверки для одного диска, для которого существуют таблицы ADinf, можно запустить двойным щелчком мыши на значке этого диска или через контекстное меню диска.

В режиме проверки дисков сначала производится сканирование диска, в процессе которого считывается загрузочный сектор, формируется список сбойных кластеров, проходится дерево каталогов, вычисляются контрольные суммы файлов. Сканирование диска производится без участия операционной системы.

Рис. 5.8. Режим проверки дисков

ADinf32 самостоятельно разбирает структуру файловых систем, читая диск по секторам.

Когда сканирование завершено, производится сравнение собранной информации с информацией, сохраненной в таблицах ADinf32. В процессе сравнения анализируются изменения загрузочного сектора, появление новых сбойных кластеров, появление новых или удаление каталогов. Также фиксируются новые, стертые, переименованные, перемещенные из каталога в каталог и измененные файлы.

Изменения файлов определяются по изменению длины или контрольной суммы (CRC). Исключением являются файлы формата OLE2 (документы MS Word `.doc` и `.dot`, таблицы Excel `.xls`). Если для таких файлов установлен тип контрольных сумм `Макро`, то измененными считаются только те файлы, в которых поменялись макрокоманды. Обычные изменения файлов, происходящие при ежедневной работе с документами, игнорируются. Таким образом, заражение макровирусами будет немедленно замечено и не потеряется за текущими изменениями документов или таблиц.

Обнаруженные изменения анализируются. Если обнаружены подозрительные изменения, похожие на проявления вируса, выдается предупреждение. Изменения отображаются в окне просмотра результатов. Если обрабатывается несколько дисков, то

результаты отображаются и могут анализироваться по мере готовности, поскольку сканирование дисков происходит в асинхронном фоновом режиме. Порядок обработки дисков выбирается так, чтобы можно было начать анализировать информацию об изменениях за минимальное время.

Просмотр истории изменений. Режим просмотра истории изменений запускается для всех отмеченных в главном окне дисков, если выбрать пункт История изменений для отмеченных дисков в общем контекстном меню. Режим просмотра истории изменений для одного диска можно запустить через контекстное меню диска.

История изменений позволяет анализировать списки новых, измененных, переименованных и перемещенных файлов за заданный интервал времени. Это может быть полезно, например, для обнаружения файла, с которым был занесен в систему вирус.

Просмотр результатов. Результаты проверки дисков отображаются в окнах просмотра результатов — рис. 5.9. Окна просмотра результатов открываются нажатием кнопки Результат в главном окне программы. Если на главном окне программы стоит отметка на переключателе Авто-откр., то первое окно просмотра результатов автоматически открывается в начале скани-

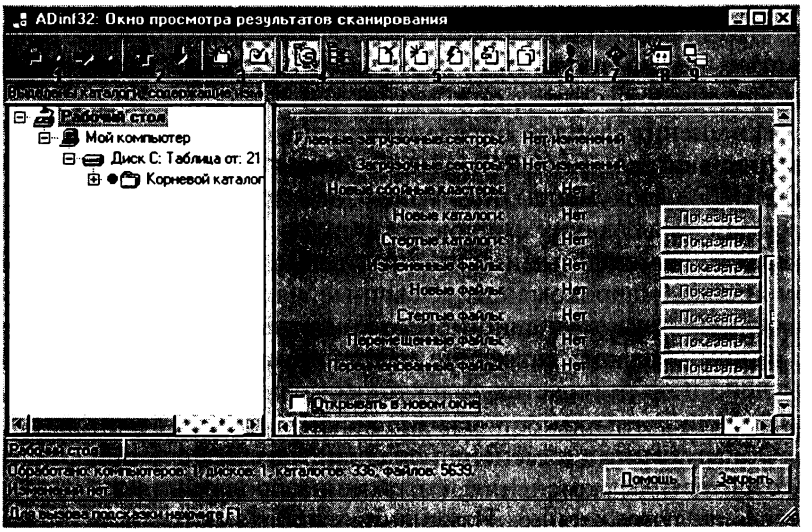


Рис. 5.9. Окно просмотра результатов и управления просмотром

рования дисков. Одновременно можно открыть произвольное количество окон просмотра результатов, в каждом из которых можно выбрать свой состав отображаемой информации. Все окна синхронизированы между собой и изменения, производимые в одном окне, автоматически отображаются в других окнах, если они затрагивают отображаемую в них информацию. После окончания анализа изменений закрывать все окна просмотра результатов не обязательно. После нажатия кнопки `Закрыть` главное окно программы все окна автоматически закроются.

Сканирование дисков осуществляется в асинхронном режиме и по мере готовности информация в окнах просмотра результатов пополняется.

Структура представления результатов. Окно просмотра результатов состоит из двух частей. В левом окне отображается дерево проверяемых объектов, в правом — информация о выбранном в дереве объекте или список файлов в поддереве, начиная с выбранного слева объекта. В верхней части окна расположены кнопки панели инструментов. В нижней части окна расположена информационная панель, в которой выдается полное название и краткая информация о выбранном объекте. Подробную информацию о каждом объекте, о его изменениях и истории можно получить через контекстное меню, раздел `Свойства`.

Левая часть окна просмотра результатов может находиться в двух режимах. В этом поле всегда показано дерево проверенных объектов. В одном режиме среди них отмечены каталоги, содержащие изменения в файлах, в другом — новые и стертые каталоги. Переключение режимов осуществляется с помощью кнопок на панели инструментов в верхней части окна.

Правая часть окна просмотра результатов также может находиться в двух состояниях. В одном режиме в правом окне отображается подробная информация о проверенном объекте, в другом — список измененных файлов во всем поддереве ниже выбранного в левом окне объекта.

Выбор типов контрольных сумм. В этой диалоговой панели (рис. 5.10) можно установить состав информации, включаемой в таблицы ревизора ADinf32, и типы контрольных сумм для контроля целостности файлов. Контрольные суммы, поддерживаемые ADinf32, можно условно разделить на две группы. Первая группа включает специализированные контрольные суммы, а вторая — стандартные. Специализированные контрольные суммы используют знание внутренней структуры файлов и не рас-

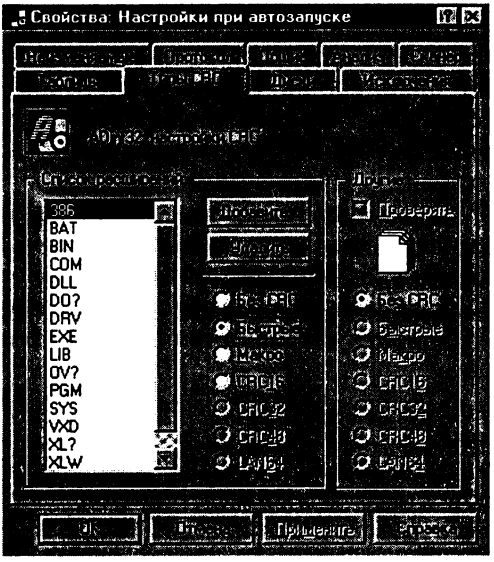


Рис. 5.10. Окно выбора типа контрольных сумм

считываются по всему файлу. Такие типы контрольных сумм можно использовать только для обнаружения вирусов и только для определенных типов файлов. Контрольные суммы `Быстрые Win32` можно использовать для обнаружения вирусов в исполняемых файлах типа `com`, `exe`, `dll`, `VxD`. Контрольные суммы `Макро` предназначены для обнаружения макровирусов в файлах-документах `doc`, `dot`, `xls`.

Стандартные контрольные суммы реализуют алгоритмы CRC16 и CRC32, рассчитываемые по всему файлу. Их необходимо использовать для обнаружения вирусов, поражающих BAT-файлы, и для контроля за целостностью файлов, которая может быть нарушена из-за случайных сбоев. Чем выше размерность контрольной суммы, тем выше надежность обнаружения случайного сбоя. Наибольшую надежность обеспечивают контрольные суммы типа CRC48, реализованные как одновременный расчет алгоритмов CRC16 и CRC32 по всему файлу.

Отдельно надо сказать про тип контрольных сумм LAN64. Эти контрольные суммы доступны только в модификации ADinf32 Pro. Использование данного типа контрольных сумм гарантирует обнаружение не только случайных сбоев, но делает невозможной незаметную преднамеренную модификацию дан-

ных злоумышленником. Этот тип контрольных сумм предназначен для контроля за сохранностью особо ценных файлов, например баз данных или документов.

Антивирусная программа Dr.Web

Dr.Web относится к классу детекторов-докторов, имеет «эвристический анализатор» — алгоритм, позволяющий обнаруживать неизвестные вирусы. «Лечебная паутина», как переводится с английского название программы, стала ответом отечественных программистов на нашествие самомодифицирующихся вирусов-мутантов, которые при размножении модифицируют свое тело так, что не остается ни одной характерной цепочки бит, присутствовавшей в исходной версии вируса. Пользователь может указать программе тестировать как весь диск, так и отдельные подкаталоги или группы файлов, либо же отказаться от проверки дисков и тестировать только оперативную память. Тестирование винчестера Dr.Web-ом занимает очень большой промежуток времени и практически всю оперативную память.

На рис. 5.11 приведен стартовый экран Dr.Web версии, рассчитанной на проверку более чем 300 тыс. вирусов.

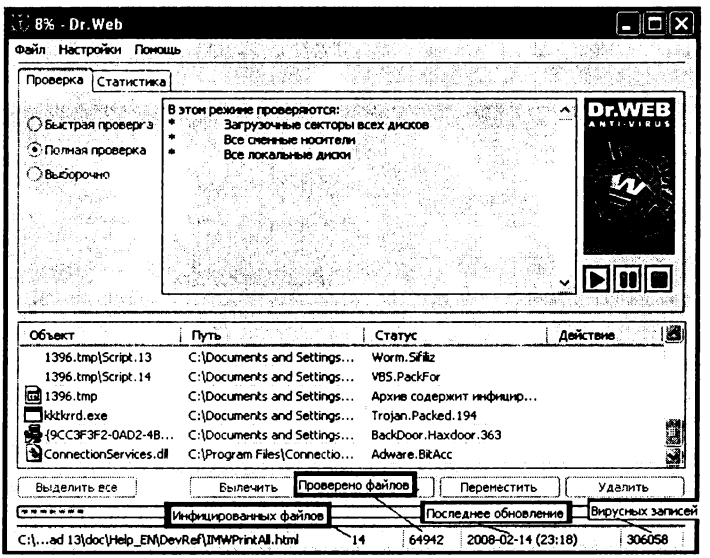


Рис. 5.11. Стартовый экран Dr.Web

На рис. 5.12 приводится пример экрана Статистика, отражающего результаты сканирования, а на рис 5.13 — меню Настройки/Действия, позволяющее пользователю установить области проверки, действия при обнаружении угроз и пр.

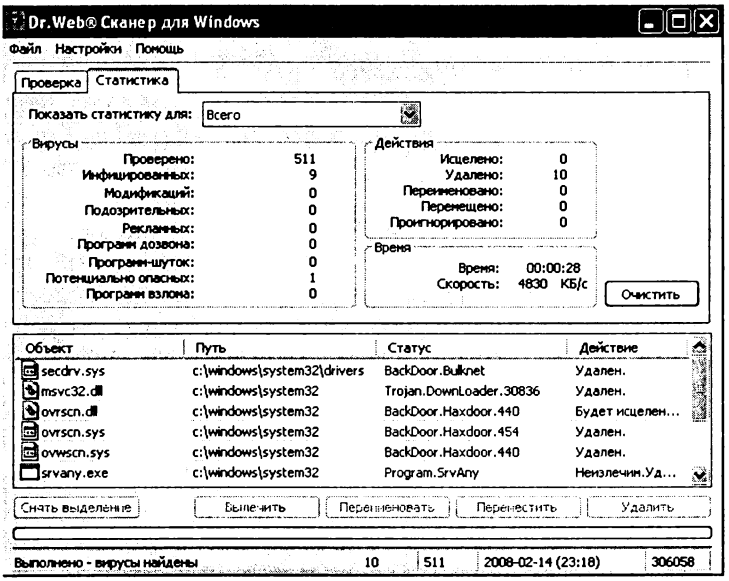


Рис. 5.12. Экран настройки на типы проверки

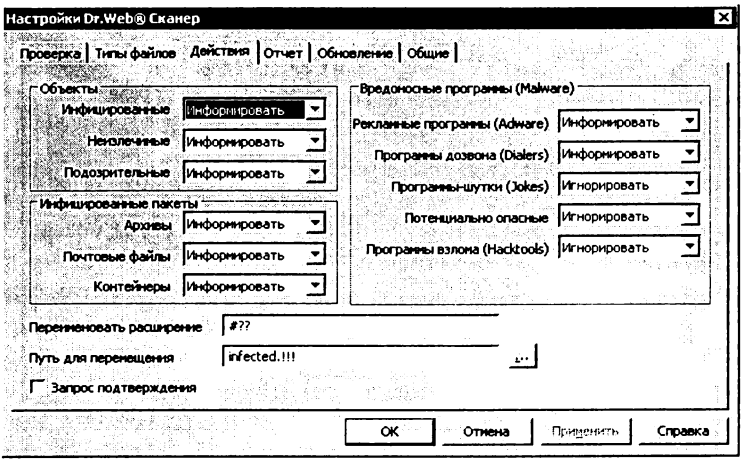


Рис. 5.13. Экран настройки на типы действий

Symantec AntiVirus

Популярный американский антивирус (рис. 5.14). Выпускается подразделением компании Symantec. Контролирует работу Windows начиная с загрузки и до выключения компьютера. Более 70 000 описаний вирусов, возможность обновления через сеть.

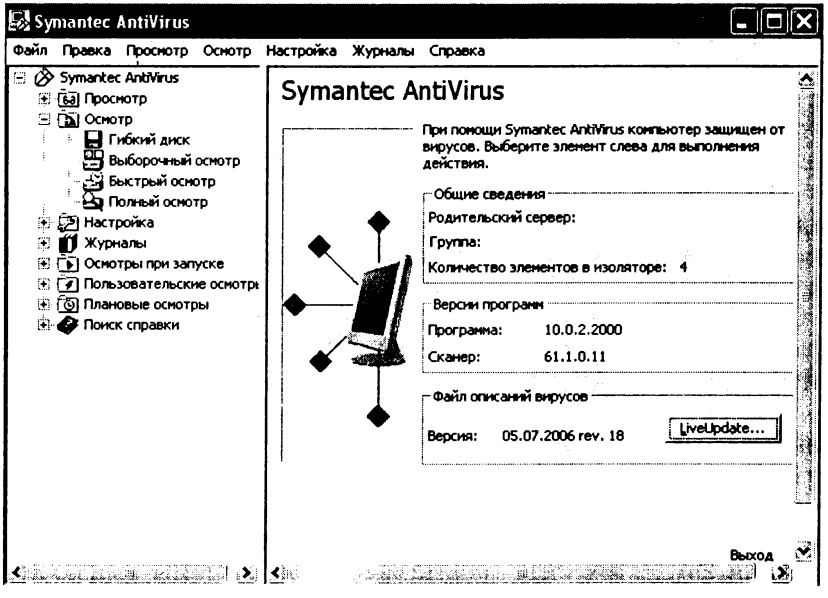


Рис. 5.14. Стартовый экран Symantec AntiVirus (SAV)

Главное окно содержит две панели. В левой панели доступные действия объединены в категории. Например, задачи осмотра дискет, выборочного осмотра, быстрого осмотра и полного осмотра относятся к категории Осмотр. Каждая категория в левой панели показана в виде отдельного значка. При выборе в левой панели категорий и других элементов в правой панели будет показана информация, необходимая для выполнения соответствующей задачи.

Автоматическая защита файловой системы. По умолчанию автоматическая защита от вирусов и других угроз безопасности загружается при запуске системы. Она проверяет программы на наличие вирусов и угроз безопасности, а также отслеживает вы-

полнение тех операций, которые могут указывать на наличие вируса или угрозы. При обнаружении вируса, вирусоподобных действий (событий, которые могут быть результатом наличия вируса) или угрозы безопасности функция автоматической защиты предупреждает об этом пользователя.

В некоторых случаях функция автоматической защиты может предупреждать о действиях, указывающих на наличие вируса, хотя известно, что эти действия не являются следствием работы вируса. Например, это может произойти при установке новых программ. При выполнении подобных действий для того чтобы избежать вывода предупреждений, рекомендуется временно отключить автоматическую защиту. Обязательно включите автоматическую защиту сразу после завершения задачи, чтобы компьютер оставался защищенным от вирусов.

Отключение автоматической защиты может быть заблокировано системным администратором; кроме того, автоматическую защиту можно отключить временно, чтобы она автоматически включилась через указанный промежуток времени.

Обычно значок Symantec AntiVirus показан на панели задач в правом нижнем углу рабочего стола Windows. В некоторых конфигурациях значок не отображается на экране.

Значок Symantec AntiVirus имеет форму щита. Для включения или выключения автоматической защиты следует щелкнуть правой кнопкой «мыши» на этом значке. Если напротив пункта `Включить автоматическую защиту` показана галочка, значит автоматическая защита файловой системы включена.

Если автоматическая защита файловой системы выключена, то на значок Symantec AntiVirus накладывается знак запрета (красная окружность, перечеркнутая по диагонали).

Для поиска и устранения побочных эффектов вирусов и других угроз безопасности Symantec AntiVirus всегда должен применять свежую информацию. Для надежной защиты файлы описаний вирусов и угроз безопасности должны регулярно обновляться после установки. Файлы описаний содержат информацию об обнаружении и устранении всех известных вирусов и угроз безопасности (рис. 5.15).

Symantec поставляет обновленные файлы описаний еженедельно через службу LiveUpdate и ежедневно через файлы Intelligent Updater, публикуемые на веб-узле Symantec Security Response. Кроме того, обновления распространяются при обнаружении новых серьезных угроз. Рекомендуется обновлять опи-

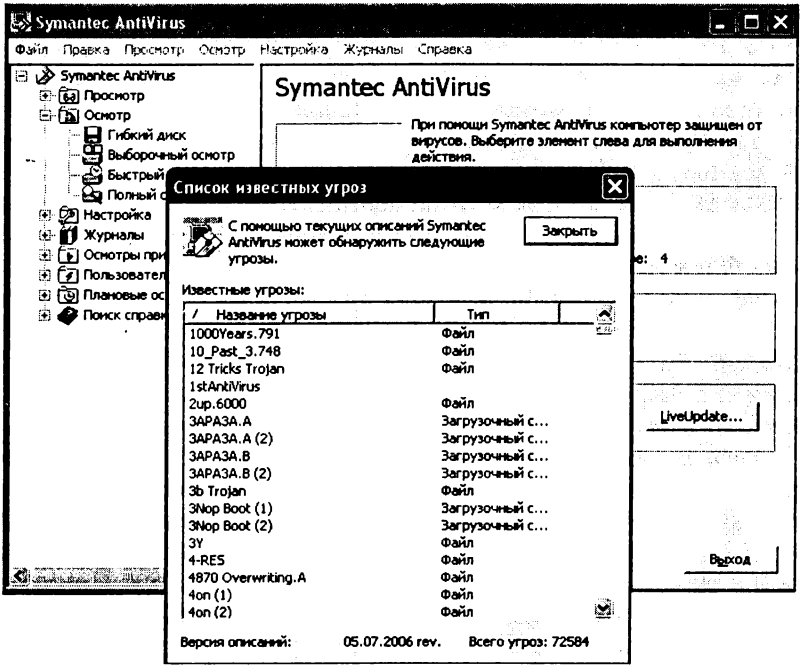


Рис. 5.15. Экран просмотра базы данных по вирусам Symantec AntiVirus

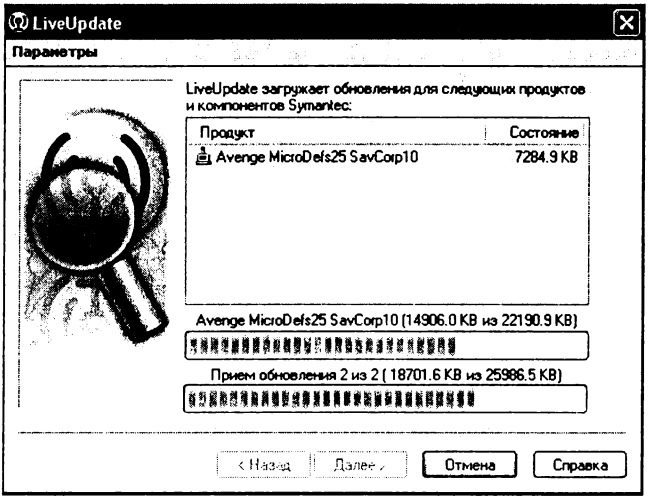


Рис. 5.16. Загрузка обновлений вирусной базы данных

сания по крайней мере раз в неделю. Простейший способ обеспечить это — запланировать автоматический запуск LiveUpdate.

С помощью функции LiveUpdate (рис. 5.16) программа Symantec AntiVirus автоматически подключается к специальному веб-узлу Symantec и определяет, нужно ли обновлять описания вирусов и угроз. Если это необходимо, то указанная функция загружает нужные файлы и устанавливает их в системе. Обычно для настройки LiveUpdate не требуется выполнять никаких действий. Единственное требование — наличие подключения к сети Internet.

Администратор может задать максимальный период работы с устаревшими описаниями вирусов и угроз безопасности. Через указанное число дней Symantec AntiVirus автоматически запустит функцию LiveUpdate, если компьютер подключен к Internet.

Действия над зараженным файлом. На рис. 5.17 приводится экран настройки (выбор обрабатываемых файлов). По умолчанию в автоматической защите и во всех типах осмотров Symantec AntiVirus настроено удаление вирусов из файла при их обнаружении и изоляция файла, если вирус удалить не удается. При обнаружении угрозы безопасности зараженный файл по умолчанию изолируется, после чего делается попытка устранить побочные

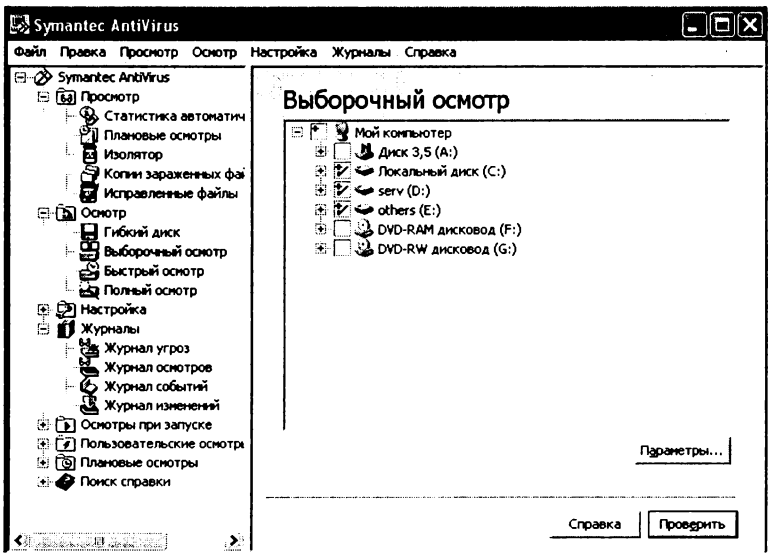


Рис. 5.17. Экран настройки режима сканирования Symantec AntiVirus

эффекты угрозы. Если это сделать не удается, то информация об обнаруженной угрозе заносится в журнал.

Если вирус был удален из зараженного файла, либо зараженный угрозой файл был изолирован и исправлен, то пользователю не требуется выполнять дополнительные действия.

Окно диалога с информацией о состоянии осмотра позволяет выполнить операции над зараженными файлами сразу после завершения осмотра. Например, исправленный файл можно удалить, если имеется его копия. Позднее с зараженными вирусами или угрозами файлами можно работать с помощью Журнала угроз, Журнала событий или Изолятора.

Журнал событий. В журнал событий (рис. 5.18) ежедневно заносятся записи о действиях, которые связаны с вирусами и угрозами и имеют отношение к защите компьютера. В их число входит изменение конфигурации, сведения об ошибках и информация о файле описаний вирусов и угроз. Эти записи, называемые событиями, отображаются вместе с соответствующей дополнительной информацией в виде списка.

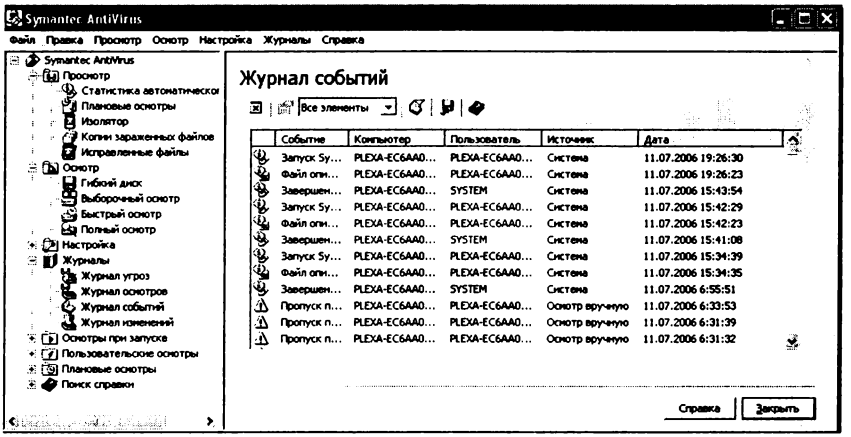


Рис. 5.18. Просмотр Журнала событий

Проанализировав записи журнала событий, можно получить представление о тенденциях, связанных с заражением компьютера вирусами и угрозами. Если компьютер используется несколькими пользователями, можно определить того из них, от кого исходит большинство вирусов и угроз, и помочь этому пользователю принять необходимые меры предосторожности.

Изолятор. Файлы помещаются в Изолятор одним из следующих способов:

- Symantec AntiVirus перемещает в Изолятор зараженные объекты, обнаруженные автоматической защитой файловой системы или процедурой осмотра;
- файл может быть вручную помещен в Изолятор пользователем.

По умолчанию в автоматической защите и во всех типах осмотров Symantec AntiVirus настроено удаление вирусов из файла при их обнаружении, и изоляция файла, если вирус удалить не удается. При обнаружении угроз безопасности зараженные файлы по умолчанию помещаются в Изолятор, после этого устраняются побочные эффекты угрозы (рис. 5.19).

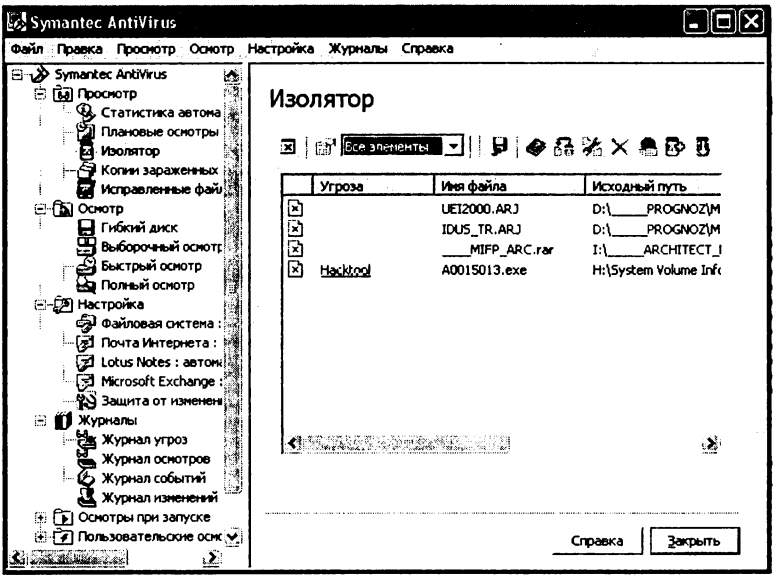


Рис. 5.19. Экран просмотра Изолятора

Задания

1. Запустите программу SAV и протестируйте диск, а затем дискету. В случае обнаружения вируса произведите лечение диска.
2. Измените настройки SAV (проверка только командных файлов) и проведите тестирование и лечение дискеты.

3. Запустите программу Dr.Web или AVP и протестируйте диск, а затем дискету. В случае обнаружения вируса произведите лечение диска.
4. Командой `attrib` установите атрибуты командных файлов в состояние «только чтение». Как это повлияет на работу антивирусных программ Dr.Web (SAV)?

Контрольные вопросы

1. Какие классы антивирусных программ вам известны?
2. Какие вредоносные программные закладки, кроме вирусов, вам известны?
3. Что такое компьютерный вирус и троянская программа?
4. Укажите пути проникновения компьютерного вируса в компьютер.
5. Какие типы компьютерных вирусов вам известны?
6. Укажите основные признаки заражения компьютера.
7. Что такое стелс-вирус?
8. Что такое boot-вирус?
9. Что такое макровирус?
10. Какие существуют методы борьбы с компьютерными вирусами?
11. Какие основные антивирусные программы вы знаете?
12. Каким образом производится лечение зараженных дисков?
13. Что такое программа-полифаг?
14. Что такое программа-детектор?
15. Каковы возможности и особенности антивирусной программы AidTest?
16. Каковы возможности и особенности антивирусной программы Symantec AntiVirus?
17. Каковы возможности и особенности антивирусной программы ADINF?
18. Каковы возможности и особенности антивирусной программы Dr.Web?

Глава 6
ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В СЕТЯХ ЭВМ

6.1. Сети ЭВМ — построение и использование

Сетью ЭВМ или вычислительной сетью (ВС) принято называть совокупность взаимодействующих станций, организованных на базе ЭВМ (в том числе и ПЭВМ), называемых узлами сети (УС), взаимосвязанных между собой посредством каналов передачи данных (КПД), образующих среду передачи данных (СПД). Каждый УС может осуществлять обработку информации в автономном режиме и обмениваться информационными сообщениями с другими УС.

Сетевые операции регулируются набором правил и соглашений (называемых сетевым протоколом), который определяет: типы разъемов и кабелей, виды сигналов, форматы данных, алгоритмы работы сетевых интерфейсов, способы контроля и исправления ошибок, взаимодействие прикладных процессов и др.

К настоящему времени разработано значительное число разновидностей организационного и архитектурного построения ВС. Системную их классификацию можно осуществить по следующим критериям:

1) по масштабу — локальные и глобальные;

2) по способу организации — централизованные и децентрализованные;

3) по топологии (конфигурации) — звездообразные, кольцевые, шинные, смешанные.

Разновидности ВС по выделенным значениям перечисленных критериев характеризуются следующим образом.

Локальные ВС (ЛВС) — сети, узлы которых располагаются на небольших расстояниях друг от друга (в различных помещениях одного и того же здания, в различных зданиях, расположенных на одной и той же территории). В глобальных ВС (ГВС) узлы сети расположены на значительных расстояниях друг от друга (в различных частях крупного города, в удаленных друг от друга населенных пунктах, в различных регионах страны и даже в различных странах).

Централизованные ВС — сети, в которых предусмотрен главный узел, через который осуществляются все обмены информацией и который осуществляет управление всеми процессами взаимодействия узлов.

Децентрализованные ВС — сети с относительно равноправными узлами, управление доступом к каналам передачи данных в этих сетях распределено между узлами.

Разновидности ВС по топологии

Разновидности ВС по топологии (конфигурации) ввиду повышенной важности данного вопроса рассмотрим несколько детальней.

Как отмечалось выше, различают четыре разновидности конфигурации ВС: звездообразную, кольцевую, шинную и комбинированную. Отличительные их признаки состоят в следующем.

Звездообразная конфигурация (рис. 6.1, *а*). В сети предусматривается центральный узел (ЦУС), через который передаются все сообщения. Такие сети появились раньше других, когда на базе большой центральной ЭВМ создавалась развитая сеть удаленных терминалов пользователей.

Достоинства звездообразных сетей:

1) простая адресация передаваемых сообщений, которая контролируется ЦУС;

2) возможности обеспечения высокого уровня защиты данных в ЦУС;

3) упрощенные процессы поиска неисправностей.

Недостатки:

1) полная зависимость надежности функционирования сети от надежности ЦУС, выход из строя которого однозначно ведет к выходу из строя всей сети;

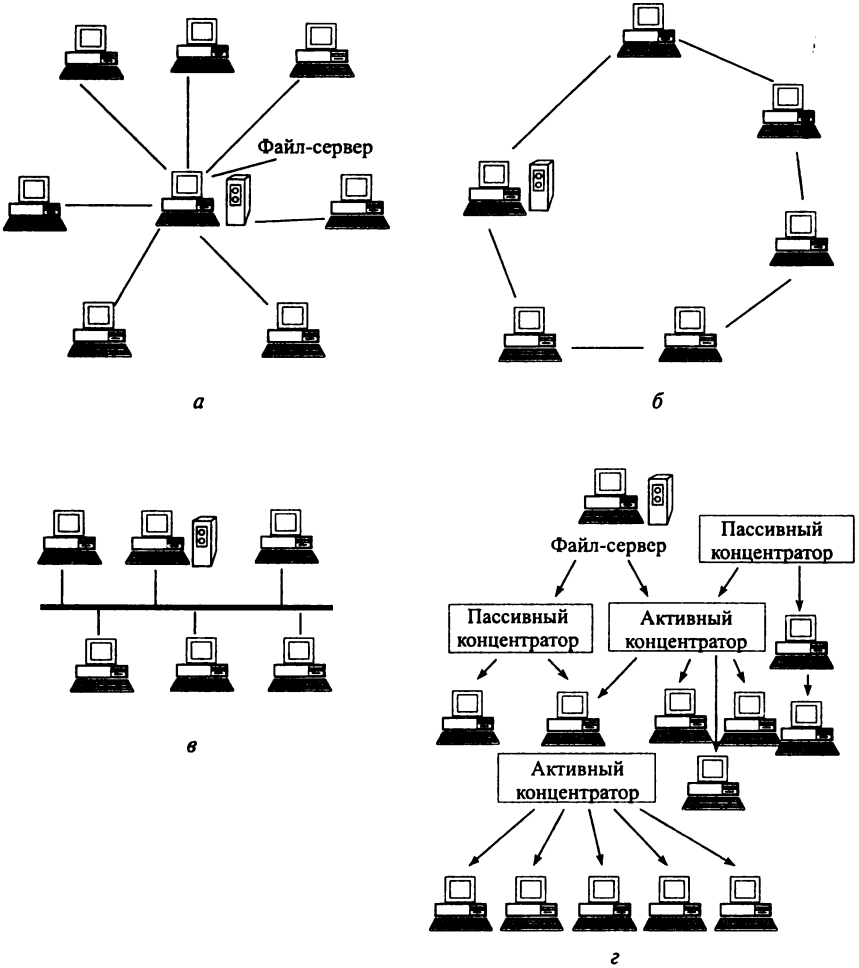


Рис. 6.1. Базовые топологии ЛВС:
а — «звезда»; *б* — «кольцо»; *в* — шинная топология; *г* — логическое кольцо

2) сложность ЦУС, на который возложены практически все сетевые функции.

Кольцевая конфигурация — рис. 6.1, *б*. В кольцевой сети не выделяется узел, управляющий передачей сообщений, их передача осуществляется в одном направлении через специальные повторители, к которым подключаются все узлы сети. Повторители бывают пассивные и активные.

Пассивный повторитель обеспечивает узлу лишь возможность соединения со средой передачи, активный — выполняет несколько сетевых функций, а именно:

1) принимает сообщения от узла-источника и усиливает несущие их сигналы;

2) формирует сообщения в вид, доступный узлу-приемнику;

3) обеспечивает соответствующему узлу возможности передачи собственных сообщений;

4) пересылает пакет следующему узлу или производит его буферизацию.

Достоинства кольцевых ВС:

1) отсутствие зависимости сети от функционирования отдельных ее узлов, причем отключение какого-либо узла не нарушает работу сети;

2) использование простой маршрутизации передаваемых сообщений;

3) легкая идентификация неисправных узлов и возможность осуществления реконфигурации сети в случае сбоя или неисправности.

Недостатки:

1) надежность сети полностью зависит от надежности кабельной системы, поскольку неисправность этой системы в каком-либо одном месте полностью выводит из строя всю сеть;

2) необходимость использования более сложного программного обеспечения для узлов, например для обработки сбойных ситуаций, реконфигурации и т. п.;

3) усложняется решение задач защиты информации, поскольку сообщения при передаче проходят через все узлы сети.

Шинная структура (рис. 6.1, *в*). Шина — это незамкнутая в кольцо среда передачи данных. Все узлы сети подключаются к шине одинаковым образом через усилители-повторители сигналов, поскольку сигналы в шине затухают. Сигналы в шине от передающего узла распространяются в обе стороны со скоростью, соизмеримой со скоростью света. Так как все принимающие узлы получают передаваемые сообщения практически одновременно, то особое внимание должно обращаться на управление доступом к среде передачи.

Достоинства шинной структуры:

1) простота организации, особенно при создании ЛВС;

2) легкость подключения новых узлов;

3) простота реализации широковещательных передач;

4) приспособленность к передаче сообщений с резкими колебаниями их потока.

Основные недостатки:

1) пассивность среды передачи, в силу этого необходимо усиление сигналов, затухающих в среде;

2) усложнение решения задач защиты информации;

3) при увеличении числа УС растет опасность насыщения среды передачи, что ведет к снижению пропускной способности.

Комбинированные сети, как это следует из самого названия, организуются путем объединения отдельных фрагментов сети с различной топологией в общую сеть.

На основе даже такого беглого рассмотрения возможных структур ВС нетрудно заключить, что для тех объектов (предприятий, учреждений, других организаций), в которых регулярно обрабатываются значительные объемы подлежащей защите информации, наиболее целесообразной будет комбинированная структура ЛВС. Например, для обработки конфиденциальной информации может быть создана самостоятельная подсеть, организованная по звездообразной схеме, а для обработки общедоступной — подсеть, организованная по шинной схеме, причем ЦУС первой подсистемы может быть подсоединен к общей шине второй подсистемы в качестве ее полноправного узла. Выдача же на общую шину защищаемой информации может блокироваться центральным узлом первой подсистемы.

Рассмотрим базовые компоненты распределенной информационной системы типичной современной организации, базирующейся на сетевых информационных технологиях (рис. 6.2). С точки зрения безопасности существенными представляются следующие особенности сети:

- корпоративная сеть имеет несколько территориально разнесенных частей (поскольку организация располагается на нескольких производственных площадках), связи между которыми находятся в ведении внешнего поставщика сетевых услуг, выходя за пределы контролируемой зоны;
- корпоративная сеть имеет одно или несколько подключений к Internet;
- на каждой из производственных площадок могут находиться критически важные серверы, в доступе к которым нуждаются работники, базирующиеся на других площадках, мобильные работники и, возможно, сотрудники сторонних организаций и другие внешние пользователи;

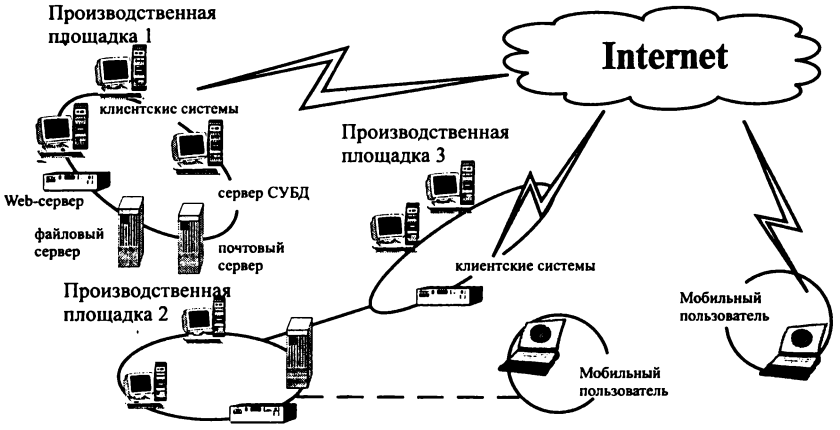


Рис. 6.2. Базовые компоненты информационной системы типичной современной организации

- для доступа пользователей могут применяться не только компьютеры, но и другие устройства, использующие, в частности, беспроводную связь;
- в течение сеанса работы пользователю приходится обращаться к нескольким информационным сервисам, опирающимся на разные аппаратно-программные платформы;
- к доступности информационных сервисов предъявляются жесткие требования, обычно выражающиеся в необходимости круглосуточного функционирования с максимальным временем простоя порядка минут или десятков минут;
- информационная система представляет собой сеть с активными агентами, т. е. в процессе работы программные компоненты передаются с одной машины на другую и выполняются в целевой среде, поддерживая связь с удаленными компонентами;
- не все пользовательские системы контролируются администраторами организации;
- программное обеспечение, особенно полученное по сети, не может считаться безопасным, в нем могут присутствовать зловредные элементы или ошибки, создающие слабости в защите;
- конфигурация информационной системы постоянно изменяется на уровнях административных данных, программ и аппаратуры (меняется состав пользователей, их привиле-

гии, версии программ, появляются новые сервисы, новая аппаратура и т. п.).

Следует учитывать также, что основная угроза информационной безопасности организаций исходит не от внешних хакеров, а от собственных сотрудников, по той или иной причине не являющихся лояльными.

Необходимо обратить внимание еще и на такое обстоятельство. В настоящее время есть возможности расширить само содержание понятия среды передачи, включив в него также организационную передачу сообщений, например, путем переноса дискет с помощью посыльного. Нетрудно представить, насколько это может расширить организацию сетевой обработки данных, хотя и будет сопряжено с решением дополнительных задач, в том числе и связанных с защитой информации.

Элементы сетей

Рассмотрим далее основные положения концепции построения сетевых протоколов, представляющих наборы правил и соглашений, определяющих, как отмечалось выше, следующие элементы сети.

1. Типы разъемов и кабелей, используемых для создания среды передачи.
2. Способы и методы передачи данных.
3. Алгоритмы работы сетевых интерфейсов.
4. Способы контроля и исправления ошибок.
5. Методы взаимодействия прикладных процессов.

Ниже в общем виде излагается содержание перечисленных элементов.

Типы разъемов и кабелей, используемых для создания среды передачи данных. В настоящее время для создания физической среды передачи преимущественно используются три типа кабелей: витая пара, коаксиальный и оптоволоконный (табл. 6.1).

Витая пара представляет собой два изолированных провода, спиралевидно сплетенных друг с другом. Такие кабели используются давно в телефонной связи. Они обеспечивают надежную передачу данных при сравнительно небольших скоростях (несколько Мбит/с) и небольших расстояниях передачи (несколько десятков метров). Поэтому их целесообразно ис-

Таблица 6.1. **Основные характеристики средств проводной связи**

Показатели	Среда передачи данных		
	Витая пара	Коаксиальный кабель	Оптоволоконный кабель
Цена	Невысокая	Относительно высокая	Высокая
Наращивание	Очень простое	Проблематично	Простое
Защита от прослушивания	Незначительная	Хорошая	Высокая
Проблемы с заземлением	Нет	Возможны	Нет
Восприимчивость к помехам	Существует	Существует	Отсутствует

пользовать в компактных ЛВС с не очень большими потоками данных.

Существуют две разновидности кабелей рассматриваемого типа: неэкранированные и экранированные, причем в экранированных кабелях гасятся побочные электромагнитные излучения, поэтому они защищены от перехвата передаваемой информации путем неконтактного подсоединения.

Коаксиальный кабель содержит два проводника: один служит для передачи сигналов, второй — для заземления. Роль заземления всегда играет внешний цилиндрический проводник. Пространство между проводниками заполнено изоляционным материалом.

Коаксиальный кабель способен передавать широкополосные сигналы, т. е. одновременно много сигналов, каждый на своей частоте, что обеспечивает высокую скорость передачи данных. Кроме того, коаксиальные кабели отличаются высокой помехоустойчивостью.

Промышленностью выпускаются стандартный (толстый) и дешевый (тонкий) коаксиальный кабели. Толстый кабель отличается повышенной помехоустойчивостью и малым затуханием передаваемых сигналов, однако для его подключения необходимы специальные разъемы — соединения. Тонкий кабель уступает толстому по помехоустойчивости и степени затухания сигнала, но он подключается к стандартным разъемам — соединениям. Кроме того, названные разновидности кабеля отличаются максимальной длиной между узлами сети: толстый — до 2500 м, тонкий — до 925 м.

Оптоволоконный кабель представляет собой световод на кремниевой или пластмассовой основе, который защищен материалом с низким коэффициентом преломления. Он позволяет решить все проблемы создания эффективной среды передачи данных с высокой скоростью передачи (до 50 Мбит/с), отсутствием потерь при передаче, практически полной невосприимчивостью к помехам, отсутствием ограничений на расстояние передачи и полосу пропускания. Недостатки его заключаются в сложности установки и диагностики, а также высокой стоимости. Кроме того, в настоящее время мало опыта в его применении. Однако, несмотря на названные недостатки, оптоволоконный кабель является весьма перспективным для организации среды передачи данных ВС.

Способы и методы передачи данных. Для передачи данных в сетях используются как традиционные способы передачи по техническим каналам связи, так и новые, разрабатываемые специально для создания среды передачи в ВС.

Из традиционных способов большое распространение в ВС получили телефонные каналы. Основной проблемой при этом стало преобразование высокоскоростных потоков цифровых (дискретных) данных в форму, удобную для передачи по телефонным каналам, рассчитанным на передачу речевых аналоговых сигналов. Решение проблемы было найдено разработкой методов предварительного, перед выдачей в телефонный канал связи, преобразования цифровых сигналов в аналоговые и обратного преобразования сигналов перед приемом их из телефонных каналов связи. Первый процесс преобразования получил название модуляции, второй — демодуляции, а устройство, осуществляющее эти преобразования, — модулятора-демодулятора (или сокращенно — модема). Сама модуляция может осуществляться несколькими методами: путем модуляции амплитуды (амплитуда некоторой несущей частоты меняется в соответствии с входной последовательностью бит: 1 — соответствует волне несущего сигнала, а отсутствие несущей — 0); путем модуляции частоты (частота меняется в обе стороны, крайние значения интерпретируются как 1 и 0); путем модуляции фазы — меняется фаза несущей.

Для формирования среды передачи в ВС специально разработаны методы цифрового кодирования данных: 1 представляется положительным напряжением высокого уровня, 0 — напряжением низкого уровня. В зависимости от способа отделения

друг от друга битов одинакового значения различают синхронное и асинхронное кодирование.

При *синхронном кодировании* узлы сети синхронизируются путем задания одинакового отсчета времени. Для этого передающий узел посылает сигналы тактовой частоты. Приемник в этом случае выбирает сигнал данных в моменты появления тактовых импульсов. Серьезный недостаток данного метода заключается в необходимости отдельной линии связи для передачи синхроимпульсов.

При *асинхронной передаче* поток бит делится на блоки фиксированной длины (например, байты). Узлы сети имеют генераторы импульсов одинаковой частоты. Генераторы периодически подстраиваются друг к другу (например, в начале каждого байта данных). Синхронизация в этом случае достигается передачей старт-бита в начале байта и стоп-бита в его конце.

Алгоритмы работы сетевых интерфейсов. Названные алгоритмы реализуют методы доступа к среде передачи данных. В настоящее время используется несколько таких методов, наиболее распространенные из них коротко рассматриваются ниже.

Множественный доступ с контролем несущей и обнаружением коллизий — это способ с состязаниями, где узлы сети соревнуются за право использования среды. Узел, выигравший в соревновании, может передать свой пакет данных, после этого освободить среду. Узлы периодически проверяют активность среды (наличие несущей). Отсутствие активности означает, что среда свободна и узлы могут начать передачу. Первый начавший передачу узел занимает среду, а остальные ожидают ее освобождения. При одновременном начале передачи несколькими узлами возникает коллизия. При ее появлении узлы прекращают передачу и в течение некоторого времени ожидают ее возобновления, после этого процедура повторяется.

Метод доступа в кольцевой среде с передачей маркера. Метод основан на однонаправленном двухточечном подключении узлов сети к среде передачи через порты приема и порты передачи. Физическая среда реализуется в виде звездно-кольцевой топологии, причем узлы сети соединяются кабелями через специальный концентратор. Если какой-либо узел неисправен, то он отключается от среды передачи. Если передача данных в кольце отсутствует, то в ней циркулирует специальный

маркер в состоянии «свободно». Узел сети, который желает передать данные, меняет содержание маркера в состояние «занято» и присоединяет к нему пакет передаваемых данных. После завершения передачи передающий узел меняет содержание маркера в состояние «свободно». Все остальные узлы лишь ретранслируют передаваемый пакет.

Метод доступа типа шины с передачей маркера. Данный метод основывается на передаче вдоль логического кольца узлов сети специального маркера, содержащего адрес следующего узла. Каждому узлу известен адрес следующего узла. Каждый узел может находиться в одном из следующих состояний: прослушивание, прием кадра, передача пакета и передача маркера.

Способы контроля и исправления ошибок. Существует ряд эффективных способов подавления помех как в оборудовании и линиях электропитания, так и в информационных каналах сети. Рассмотрим основные из них.

Способы подавления помех в сетях электропитания. Основной причиной искажений формы стандартного сигнала первичного электропитания обычно является резкое изменение нагрузки сети электропитания. При наличии такой опасности необходимо использовать специальное электрооборудование для развязки питания оборудования коммуникаций сети, например в виде специальных распределительных силовых щитов.

Помимо этого применяются широкополосные фильтры на вводе питания коммуникационного оборудования в целях подавления кратковременных помех. Используется электростатическое экранирование линий электропитания и коммуникаций.

Защита от помех по линии «земля». Существуют два основных типа «земли»: корпусная и схемная. Корпусное устройство «земли» должно быть обязательно подключено к общей линии «земля», проложенной в помещении. Схемное устройство «земли» — это нулевой потенциал, относительно которого отсчитываются уровни напряжения информационных сигналов. Общее правило заключается в том, что корпусные «земли» объединяются индивидуальными линиями в одной точке, а схемные — в другой. Причем эти точки могут быть не соединены, либо соединены, но обязательно располагаться в непосредственной близости друг от друга.

Способы помехозащищенной передачи по согласованным информационным линиям связи. Существуют специальные схемотехнические средства и правила согласования волнового сопротивления (например, витой пары или коаксиального кабеля) и нагрузочного сопротивления коммуникационного устройства. Особо тщательно должны быть выполнены распайка разъемов и ответвления от линии информационной связи. Все это существенно повышает помехозащищенность. В линиях связи большой протяженности применяют оптоволоконные развязки сетевых узлов.

Способы обеспечения помехозащищенности и коррекции ошибок в модемной связи. Основной задачей приема сигналов по телефонным каналам с использованием модема является нормализация их параметров и компенсация дестабилизирующих факторов и помех. Правильный выбор модема зависит от объективных данных о дестабилизирующих факторах конкретной телефонной линии, которые могут быть определены с помощью специального измерительного и имитационного оборудования.

Методы взаимодействия прикладных процессов. Способы объединения компьютеров в сеть условно можно разделить на два вида:

- способы, отвечающие всем признакам ЛВС, основным из которых считается возможность одновременного доступа пользователей к общим программно-информационным ресурсам нескольких компьютеров;
- способы, отвечающие не всем признакам ЛВС, но которые все же дают возможность пользователям делать многое из того, что обеспечивают настоящие ЛВС. Такие системы принято называть ЛВС-подобными.

К последним системам можно отнести:

1) коллективизаторы периферии и коммутаторы данных;

2) системы беспроводной локальной связи между компьютерами, которые позволяют совместно использовать данные и обмениваться сообщениями;

3) системы локальных электронных досок объявлений, когда имеются возможности обмена сообщениями и файлами, но нельзя совместно использовать периферию.

В настоящее время у нас в стране наибольшее распространение получили сети Ethernet, Token-Ring, ArcNet и некоторые другие (табл. 6.2).

Таблица 6.2. **Сравнительные характеристики наиболее распространенных ЛВС**

Наименование характеристик	Наименование сети		
	Ethernet	Token-Ring	ArcNet
Скорость передачи данных, Мбит/с	1—10	4—16	2,5
Средняя длина кадров передаваемых данных, байт	100	18 200	8000
Надежность	Неисправность кабеля выводит из строя всю сеть или отдельные ее сегменты	Функционирует даже при повреждении сетевого кабеля	Неисправность кабеля выводит из строя всю сеть или отдельный ее сегмент
Рекомендации по применению	Организации научного плана	Организации, пользующиеся поддержкой фирмы IBM	Небольшие офисные системы

Сетевые операционные системы (ОС)

Сетевые ОС можно разделить на три класса: «DOS-ориентированные», «OS/2-ориентированные», «UNIX-ориентированные».

DOS-ориентированные сетевые системы предполагают наличие сетевого программного обеспечения на каждой рабочей станции ЛВС или выделение под файл-сервер одной из станций. При этом возможны разделение ресурсов (например, принтеров, жестких дисков и т. д.), пересылка файлов и сообщений и др. Каждый компьютер в сети может воспользоваться ресурсами другого компьютера. Это означает довольно высокую гибкость в применении ЛВС.

Сетевые ОС данного типа имеют два существенных недостатка: они сложны в управлении (администрировании) сетью и занимают довольно много оперативной памяти в рабочих станциях. Например, для ОС типа PC LAN может потребоваться до 400 Кбайт ОЗУ ПЭВМ.

OS/2-ориентированные ОС. Определенный интерес представляют сетевые ОС, которые используют ОС типа OS/2 рабочих станций серии PS/2 фирмы IBM. Это связано с тем, что наряду с рабочими станциями на базе OS/2 допускается функционирование в сети ПЭВМ на основе DOS.

Кроме того, возможно использование системной программы LAN Manager фирмы Microsoft и программы доступа к многопользовательским базам данных SQL Server, разработанной фирмами Ashton-Tate и Microsoft.

UNIX-ориентированные сетевые ОС. Если предполагается, что ЛВС будет использоваться только для коллективного применения дорогостоящей периферии (например, лазерного принтера и др.), обмена файлами или «электронной почты», когда необходима совместная обработка данных (например, в базе данных), то нужны средства поддержки программирования распределенных систем (создание единой операционной сетевой среды). В этом случае часто используется центральный компьютер или несовмещенный файл-сервер (НФС) с соответствующей сетевой UNIX-ориентированной ОС.

Особенностью данных ОС является то, что в НФС инсталлируется главная часть ОС — ее «ядро», на которое ложится ответственность за выполнение основных сетевых функций. Программное обеспечение остальных станций поэтому является достаточно простым. Очевидно для размещения резидентных сетевых программ в памяти рабочих станций требуется меньше места, чем в DOS-ориентированных сетевых ОС.

Ядро рассматриваемой сетевой ОС должно обеспечивать следующие функции: интерфейс с ОС рабочих станций сети, коллективное использование ресурсов ЛВС, обеспечение безопасности и целостности данных путем контроля прав доступа к ресурсам, многозадачное и многопользовательское выполнение прикладных программ и др.

Различные типы сетевых ОС, построенных на одинаковых фундаментальных принципах работы компьютерных сетей, могут отличаться средствами администрирования сети и процедурами начальной установки (инсталляции и инициализации).

К новейшим разработкам сетевых ОС фирмы Novell можно отнести Novell NetWare v. 4.0 и v. 4.1, предназначенные для крупных корпоративных ЛВС с числом рабочих станций до 1000, а также Novell Personal NetWare, ориентированную на средние ЛВС с числом пользователей до 50, в которой пользователи предъявляют невысокие требования к сети.

Главной особенностью ОС Novell NetWare v. 4.x следует считать то, что с помощью новой специальной службы каталогов NDS (NetWare Directory Services) системный администратор может централизованно управлять всеми файл-серверами

(ФС) и вести единый список пользователей на всех серверах. В этом случае существенно упрощается определение прав доступа пользователей сети. Упрощается и работа пользователя, поскольку у него нет необходимости в подключении к отдельным ФС сети.

Другой полезной особенностью NetWare v. 4.x является технология виртуально загружаемых программных модулей VLM (Virtual Loadable Moduls) наряду с известными NLM-модулями. Использование VLM-модулей позволяет пользователям загружать и удалять собственное ПО по мере необходимости. При этом в качестве ФС можно использовать ПК на основе процессоров типа 386, 486 и P5 (Pentium). В ЛВС необходимо использовать также устройство для считывания оптических дисков CD-ROM. Это связано с тем, что NetWare v. 4.x поставляются только на накопителях типа CD-ROM.

В последних версиях Novell NetWare появились дополнительные возможности, которые позволяют преодолеть ограничения на число подключенных к ФС принтеров и выполнять архивирование файлов. При этом можно инициализировать процесс на ФС или специальный процесс на выделенной рабочей станции (принт-сервере), которые позволяют управлять работой до 16 принтеров. Удобной возможностью является использование одного принтера для нескольких ЛВС, объединенных мостами (см. раздел, посвященный межсетевому взаимодействию), и организация и обслуживание принт-сервером очереди на печать от восьми ФС.

Для архивирования файлов необходимо запустить специальный процесс типа Backup на ФС или «мосте». Эта операция может проходить с запретом входа в сессию текущих пользователей и инициализироваться без промедления или с определенной паузой.

Межсетевое взаимодействие

Данный вопрос рассмотрим на примере наиболее распространенной и признанной эталонной модели взаимодействия открытых систем ISO/OSI (ВОС).

В основу эталонной модели положена идея декомпозиции процесса функционирования открытых систем на уровни, при-

чем разбиение на уровни производится таким образом, чтобы сгруппировать в рамках каждого из них функционально наиболее близкие компоненты. Кроме того, требуется, чтобы взаимодействие между смежными уровнями было минимальным, число уровней сравнительно небольшим, а изменения, производимые в рамках одного уровня, не требовали бы перестройки смежных. Отдельный уровень, таким образом, представляет собой логически и функционально замкнутую подсистему, сообщающуюся с другими уровнями посредством специально определенного интерфейса. В рамках модели ISO/OSI каждый конкретный уровень может взаимодействовать только с соседними. Совокупность правил (процедур) взаимодействия объектов одноименных уровней называется протоколом.

Эталонная модель содержит семь уровней (снизу вверх):

1. Физический.
2. Канальный (или передачи данных).
3. Сетевой.
4. Транспортный.
5. Сеансовый.
6. Представительный.
7. Прикладной.

Каждый уровень передающей станции в этой иерархической структуре взаимодействует с соответствующим уровнем принимающей станции посредством нижележащих уровней. При этом каждая пара уровней с помощью служебной информации в сообщениях устанавливает между собой логическое соединение, обеспечивая тем самым логический канал связи соответствующего уровня. С помощью такого логического канала каждая пара верхних уровней может обеспечивать между собой взаимодействие, абстрагируясь от особенностей нижних. Другими словами, каждый уровень реализует строго определенный набор функций, который может использоваться верхними уровнями независимо от деталей реализации этих функций (табл. 6.3).

Рассмотрим подробнее функциональное назначение каждого уровня.

Физический уровень. Физический уровень обеспечивает электрические, функциональные и процедурные средства установления, поддержания и разъединения физического соединения. Реально он представлен аппаратурой генерации и управления электрическими сигналами и каналом передачи данных. На этом уровне данные представляются в виде последовательности битов

Таблица 6.3. **Семиуровневая модель (стек) протоколов межсетевого обмена OSI**

№ уровня	Наименование уровня	Содержание
7	Уровень приложений	Предоставление услуг на уровне конечного пользователя: почта, теледоступ и пр.
6	Уровень представления данных	Интерпретация и сжатие данных
5	Уровень сессии	Аутентификация и проверка полномочий
4	Транспортный уровень	Обеспечение корректной сквозной пересылки данных
3	Сетевой уровень	Маршрутизация и ведение учета
2	Канальный уровень	Передача и прием пакетов, определение аппаратных адресов
1	Физический уровень	Собственно кабель или физический носитель

или аналогового электрического сигнала. Задачей физического уровня является передача последовательности битов из буфера отправителя в буфер получателя.

Канальный уровень. Протоколы канального уровня (или протоколы управления звеном передачи данных) занимают особое место в иерархии уровней: они служат связующим звеном между реальным каналом, вносящим ошибки в передаваемые данные, и протоколами более высоких уровней, обеспечивая безошибочную передачу данных. Этот уровень используется для организации связи между двумя станциями с помощью имеющегося в наличии (обычно ненадежного) канала связи. При этом станции могут быть связаны несколькими каналами.

Протокол канального уровня должен обеспечить: независимость протоколов высших уровней от используемой среды передачи данных, кодонезависимость передаваемых данных, выбор качества обслуживания при передаче данных. Это означает, что более высокие уровни освобождаются от всех забот, связанных с конкретным каналом связи (тип, уровень шумов, используемый код, параметры помехоустойчивости и т. д.).

На этом уровне данные представляются кадром, который содержит информационное поле, а также заголовок и концевик

(трейлер), присваиваемые протоколом. Заголовок содержит служебную информацию, используемую протоколом канального уровня принимающей станции и служащую для идентификации сообщения, правильного приема кадров, восстановления и повторной передачи в случае ошибок и т. д. Концевик содержит проверочное поле, служащее для коррекции и исправления ошибок (при помехоустойчивом кодировании), внесенных каналом. Задача протокола канального уровня — составление кадров, правильная передача и прием последовательности кадров, контроль последовательности кадров, обнаружение и исправление ошибок в информационном поле (если это необходимо).

Сетевой уровень. Сетевой уровень предоставляет вышестоящему транспортному уровню набор услуг, главными из которых являются сквозная передача блоков данных между передающей и приемной станциями (т. е. выполнение функций маршрутизации и ретрансляции) и глобальное адресование пользователей. Другими словами, нахождение получателя по указанному адресу, выбор оптимального (в условиях данной сети) маршрута и доставка блока сообщения по указанному адресу.

Таким образом, на границе сетевого и транспортного уровней обеспечивается независимость процесса передачи данных от используемых сред за исключением качества обслуживания. Под качеством обслуживания понимается набор параметров, обеспечивающих функционирование сетевой службы, отражающий рабочие (транзитная задержка, коэффициент необнаруженных ошибок и др.) и другие характеристики (защита от НСД, стоимость, приоритет и др.). Система адресов, используемая на сетевом уровне, должна иметь иерархическую структуру и обеспечивать следующие свойства: глобальную однозначность, маршрутную независимость и независимость от уровня услуг.

На сетевом уровне данные представляются в виде пакета, который содержит информационное поле и заголовок, присваиваемый протоколом. Заголовок пакета содержит управляющую информацию, указывающую адрес отправителя, возможно, маршрут и параметры передачи пакета (приоритет, номер пакета в сообщении, параметры безопасности, максимум ретрансляции и др.). Различают следующие виды сетевого взаимодействия:

- с установлением соединения — между отправителем и получателем сначала с помощью служебных пакетов организуется логический канал (отправитель — отправляет пакет,

получатель — ждет получения пакета, плюс взаимное уведомление об ошибках), который разъединяется после окончания сообщения или в случае неисправимой ошибки. Такой способ используется протоколом X.25;

- без установления соединения (дейтаграммный режим) — обмен информацией осуществляется с помощью дейтаграмм (разновидность пакетов), независимых друг от друга, которые принимаются также независимо друг от друга и собираются в сообщение на приемной станции. Такой способ используется в архитектуре протоколов DARPA.

Транспортный уровень. Транспортный уровень предназначен для сквозной передачи данных через сеть между оконечными пользователями — абонентами сети. Протоколы транспортного уровня функционируют только между оконечными системами.

Основными функциями протоколов транспортного уровня являются разбиение сообщений или фрагментов сообщений на пакеты, передача пакетов через сеть и сборка пакетов. Они также выполняют следующие функции: отображение транспортного адреса в сетевой, мультиплексирование и расщепление транспортных соединений, межконцевое управление потоком и исправление ошибок. Набор процедур протокола транспортного уровня зависит как от требований протоколов верхнего уровня, так и от характеристик сетевого уровня.

Наиболее известным протоколом транспортного уровня является TCP (Transmission Control Protocol), используемый в архитектуре протоколов DARPA и принятый в качестве стандарта Министерством обороны США. Он используется в качестве высоконадежного протокола взаимодействия между ЭВМ в сети с коммутацией пакетов.

Протоколы верхних уровней. К протоколам верхних уровней относятся протоколы сеансового, представительного и прикладного уровней. Они совместно выполняют одну задачу — обеспечение сеанса обмена информацией между двумя прикладными процессами, причем информация должна быть представлена в том виде, который понятен обоим процессам. Поэтому обычно эти три уровня рассматривают совместно. Под прикладным процессом понимается элемент оконечной системы, который принимает участие в выполнении одного или нескольких заданий по обработке информации. Связь между ними осуществляется с помощью прикладных объектов — элементов прикладных процессов, участвующих в обмене информацией. При этом прото-

колы верхних уровней не учитывают особенности конфигурации сети, каналов и средств передачи информации.

Протоколы представительного уровня предоставляют услуги по согласованию синтаксиса передачи (правил, задающих представление данных при их передаче) и конкретным представлениям данных в прикладной системе. Другими словами, на представительном уровне осуществляется синтаксическое преобразование данных от вида, используемого на прикладном уровне, к виду, используемому на остальных уровнях (и наоборот).

Прикладной уровень, будучи самым верхним в эталонной модели, обеспечивает доступ прикладных процессов в среду взаимодействия открытых систем. Основной задачей протоколов прикладного уровня является интерпретация данных, полученных с нижних уровней, и выполнение соответствующих действий в оконечной системе в рамках прикладного процесса. В частности, эти действия могут заключаться в передаче управления определенным службам ОС вместе с соответствующими параметрами. Кроме того, протоколы прикладного уровня могут предоставлять услуги по идентификации и аутентификации партнеров, установлению полномочий для передачи данных, проверке параметров безопасности, управлению диалогом и др.

Прикладное программное обеспечение в ЛВС

Существуют следующие типы приложений, которые могут быть использованы в ЛВС.

Несетевые (однопользовательские) — это программы для одной ПЭВМ и одного пользователя, которые, однако, могут запускаться с ФС и использоваться на рабочих станциях ЛВС, но лишь одним пользователем. При одновременной же работе двух пользователей, например с базой данных (БД), может произойти нарушение целостности данных.

Сетевые — это модифицированные версии программ для одновременного использования несколькими пользователями ЛВС. Модификация программ связана с координацией доступа к данным (например, возможна блокировка записей и др.). Преимущества этих версий по сравнению с однопользовательскими программами стимулируют распространение ЛВС.

Специализированные сетевые — это программы, которые позволяют реализовать модель «клиент-сервер» для различных приложений, в которой при обработке данных эффективно используется мощность нескольких компьютеров. В упрощенном виде клиент — это та часть программы, которая ведет диалог с пользователем, а сервер ведет обработку данных. Сервер БД — лучший пример такого приложения в ЛВС. Другим примером программ, предназначенных для сетей, можно считать программы электронной почты и программы группового планирования.

Электронная почта — это сообщение, оформленное в виде файла (с текстовыми, графическими и т. п. данными или комбинация этих типов данных), переданное в линию связи ПЭВМ с ЛВС, и одновременно комплекс программно-аппаратных средств и организационных мероприятий по хранению и доставке сообщений.

Основной элемент электронной почты — «почтовый ящик» (например, в виде специальной области на диске). Эта область имеет отделения получения/приема сообщений для каждого пользователя. Сообщение считается отправленным после того, как оно перенесено из отделения отправителя в отделение адресата. После этого получатель информируется, что для него имеется почта. Получатель может прочесть сообщения лишь после подключения к сети и пересылки его в свою ПЭВМ. Если получатель и отправитель сообщения работают в сети одновременно, то сообщение («экспресс-почта») может быть передано непосредственно на ПЭВМ адресата. Сообщение можно отправить одному или группе пользователей ЛВС путем создания списка рассылки. При этом никто, кроме получателя, не может «открыть» почтовый ящик, удалить его содержимое без знания имени и пароля владельца этого ящика.

Программы-планировщики или программы группового обеспечения в офисных компьютерных системах являются новой категорией сетевого ПО. Пакеты данного типа выполняют те же функции, что и пакеты электронной почты. Кроме того, с их помощью можно не только отправлять и получать сообщения, но и устанавливать приоритетность сообщений, обеспечивать сопровождение проектов и сложную обработку документов (например, индексирование и поиск документов, генерацию отчетов и др.), поддержку оперативного проведения совещаний. Программы-планировщики могут иметь интерфейс для программирования.

6.2. Цели, функции и задачи защиты информации в сетях ЭВМ

Цели защиты информации в сетях ЭВМ

Цели защиты информации в сетях ЭВМ общие для всех АСОД, а именно: обеспечение целостности (физической и логической) информации, а также предупреждение несанкционированной ее модификации, несанкционированного получения и размножения. Функции защиты также носят общий для всех АСОД характер. Задачи защиты информации в сетях ЭВМ определяются теми угрозами, которые потенциально возможны в процессе их функционирования.

Угрозы. Для сетей передачи данных реальную опасность представляют следующие угрозы.

1. Прослушивание каналов, т. е. запись и последующий анализ всего проходящего потока сообщений. Прослушивание в большинстве случаев не замечается легальными участниками информационного обмена.

2. Умышленное уничтожение или искажение (фальсификация) проходящих по сети сообщений, а также включение в поток ложных сообщений. Ложные сообщения могут быть восприняты получателем как подлинные.

3. Присвоение злоумышленником своему узлу или ретранслятору чужого идентификатора, это дает возможность получать или отправлять сообщения от чужого имени.

4. Преднамеренный разрыв линии связи, что приводит к полному прекращению доставки всех (или только выбранных злоумышленником) сообщений.

5. Внедрение сетевых вирусов, т. е. передача по сети тела вируса с его последующей активизацией пользователем удаленного или локального узла.

Задачи. В соответствии с этим специфические задачи защиты в сетях передачи данных состоят в следующем.

1. Аутентификация одноуровневых объектов, заключающаяся в подтверждении подлинности одного или нескольких взаимодействующих объектов при обмене информацией между ними.

2. Контроль доступа, т. е. защита от несанкционированного использования ресурсов сети.

3. Маскировка данных, циркулирующих в сети.

4. Контроль и восстановление целостности всех находящихся в сети данных.

5. Арбитражное обеспечение, т. е. защита от возможных отказов от фактов отправки, приема или содержания отправленных или принятых данных.

Применительно к различным уровням семиуровневого протокола передачи данных в сети задачи могут быть конкретизированы следующим образом.

1. Физический уровень — контроль электромагнитных излучений линий связи и устройств, поддержка коммутационного оборудования в рабочем состоянии. Защита на данном уровне обеспечивается с помощью экранирующих устройств, генераторов помех, средств физической защиты передающей среды.

2. Канальный уровень — увеличение надежности защиты (при необходимости) с помощью шифрования передаваемых по каналу данных. В этом случае шифруются все передаваемые данные, включая служебную информацию.

3. Сетевой уровень — наиболее уязвимый уровень с точки зрения защиты. На нем формируется вся маршрутизирующая информация, отправитель и получатель фигурируют явно, осуществляется управление потоком. Кроме того, протоколами сетевого уровня пакеты обрабатываются на всех маршрутизаторах, шлюзах и других промежуточных узлах. Почти все специфические сетевые нарушения осуществляются с использованием протоколов данного уровня (чтение, модификация, уничтожение, дублирование, переориентация отдельных сообщений или потока в целом, маскировка под другой узел и др.).

Защита от подобных угроз осуществляется протоколами сетевого и транспортного уровней (см. ниже) и с помощью средств криптозащиты. На данном уровне может быть реализована, например, выборочная маршрутизация.

4. Транспортный уровень — осуществляет контроль за функциями сетевого уровня на приемном и передающем узлах (на промежуточных узлах протокол транспортного уровня не функционирует). Механизмы транспортного уровня проверяют целостность отдельных пакетов данных, последовательности пакетов, пройденный маршрут, время отправления и доставки, идентификацию и аутентификацию отправителя и получателя и другие функции. Все активные угрозы становятся видимыми на данном уровне.

Гарантом целостности передаваемых данных является криптозащита как самих данных, так и служебной информации. Никто, кроме имеющих секретный ключ получателя и/или отправителя, не может прочитать или изменить информацию таким образом, чтобы изменение осталось незамеченным.

Анализ трафика предотвращается передачей сообщений, не содержащих информацию, которые, однако, выглядят как реальные сообщения. Регулируя интенсивность этих сообщений в зависимости от объема передаваемой информации, можно постоянно добиваться равномерного трафика. Однако все эти меры не могут предотвратить угрозу уничтожения, переориентации или задержки сообщения. Единственной защитой от таких нарушений может быть параллельная доставка дубликатов сообщения по другим путям.

5. Протоколы верхних уровней обеспечивают контроль взаимодействия принятой или переданной информации с локальной системой. Протоколы сеансового и представительного уровня функций защиты не выполняют. В функции защиты протокола прикладного уровня входит управление доступом к определенным наборам данных, идентификация и аутентификация определенных пользователей, а также другие функции, определяемые конкретным протоколом. Более сложными эти функции являются в случае реализации полномочной политики безопасности в сети.

Особенности защиты информации в вычислительных сетях обусловлены тем, что сети, обладающие несомненными (по сравнению с локальными ЭВМ) преимуществами обработки информации, усложняют организацию защиты, причем основные проблемы при этом состоят в следующем.

1. Разделение совместно используемых ресурсов. В силу совместного использования большого количества ресурсов различными пользователями сети, возможно находящимися на большом расстоянии друг от друга, значительно повышается риск НСД — в сети его можно осуществить проще и незаметнее.

2. Расширение зоны контроля. Администратор или оператор отдельной системы или подсети должен контролировать деятельность пользователей, находящихся вне пределов его досягаемости, возможно в другой стране. При этом он должен поддерживать рабочий контакт со своими коллегами в других организациях.

3. Комбинация различных программно-аппаратных средств. Соединение нескольких подсистем, пусть даже однородных по характеристикам, в сеть увеличивает уязвимость всей системы в целом. Подсистема обычно настроена на выполнение своих специфических требований безопасности, которые могут оказаться несовместимы с требованиями на других подсистемах. В случае соединения разнородных систем риск повышается.

4. Неизвестный периметр. Легкая расширяемость сетей ведет к тому, что определить границы сети подчас бывает сложно; один и тот же узел может быть доступен для пользователей различных сетей.

Более того, для многих из них не всегда можно точно определить, сколько пользователей имеют доступ к определенному узлу и кто они.

5. Множество точек атаки. В сетях один и тот же набор данных или сообщение могут передаваться через несколько промежуточных узлов, каждый из которых является потенциальным источником угрозы. Естественно, это не может способствовать повышению защищенности сети. Кроме того, ко многим современным сетям можно получить доступ с помощью коммутируемых линий связи и модема, что во много раз увеличивает количество возможных точек атаки. Такой способ прост, легко осуществим и трудно контролируем; поэтому он считается одним из наиболее опасных. В списке уязвимых мест сети также фигурируют линии связи и различные виды коммуникационного оборудования: усилители сигнала, ретрансляторы, модемы и т. д.

6. Сложность управления и контроля доступа к системе. Многие атаки на сеть могут осуществляться без получения физического доступа к определенному узлу — с помощью сети из удаленных точек. В этом случае идентификация нарушителя может оказаться очень сложной, если не невозможной. Кроме того, время атаки может оказаться слишком мало для принятия адекватных мер.

Понятие сервисов безопасности

Для решения перечисленных задач в ВС создаются специальные механизмы защиты (или сервисы безопасности). Их перечень и содержание для общего случая могут быть представлены следующим образом.

Идентификация/аутентификация. Современные средства идентификации/аутентификации должны удовлетворять двум условиям:

- быть устойчивыми к сетевым угрозам (пассивному и активному прослушиванию сети);
- поддерживать концепцию единого входа в сеть.

Первое требование можно выполнить, используя криптографические методы. (Еще раз подчеркнем тот очевидный факт, что современная криптография есть нечто гораздо большее, чем шифрование; соответственно, разные ветви этой дисциплины нуждаются в дифференцированном подходе с нормативной точки зрения.) В настоящее время общепринятыми являются подходы, основанные на системе Kerberos или службе каталогов с сертификатами в стандарте X.509.

Единый вход в сеть — это, в первую очередь, требование удобства для пользователей. Если в корпоративной сети много информационных сервисов, допускающих независимое обращение, то многократная идентификация/аутентификация становится слишком обременительной. К сожалению, пока нельзя сказать, что единый вход в сеть стал нормой, доминирующие решения пока не сформировались.

Дополнительные удобства создает применение биометрических методов аутентификации, основанных на анализе отпечатков (точнее, результатов сканирования) пальцев. В отличие от специальных карт, которые нужно хранить, пальцы «всегда под рукой» (правда, под рукой должен быть и сканер). Подчеркнем, что и здесь защита от нарушения целостности и перехвата с последующим воспроизведением осуществляется методами криптографии.

Разграничение доступа. Разграничение доступа является самой исследованной областью информационной безопасности.

В настоящее время следует признать устаревшим (или, по крайней мере, не полностью соответствующим действительности) положение о том, что разграничение доступа направлено исключительно на защиту от злоумышленных пользователей. Современные информационные системы характеризуются чрезвычайной сложностью и их внутренние ошибки представляют не меньшую опасность.

Динамичность современной программной среды в сочетании со сложностью отдельных компонентов существенно сужает область применимости самой употребительной — *дискреционной*

модели управления доступом (называемой также моделью с произвольным управлением). При определении допустимости доступа важно не только (и не столько) то, кто обратился к объекту, но и то, какова семантика действия. Без привлечения семантики нельзя выявить троянские программы, противостоять которым произвольное управление доступом не в состоянии.

В последнее время появляются новые модели управления доступом, например модель *«песочницы»* (Sandbox) в Java-технологии.

Активно развиваемое *ролевое управление* доступом решает не столько проблемы безопасности, сколько улучшает управляемость систем (что, конечно, очень важно). Суть его в том, что между пользователями и их привилегиями помещаются промежуточные сущности — роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права.

Сложность информационной системы характеризуется, прежде всего, числом имеющихся в ней связей. Поскольку ролей много меньше, чем пользователей и привилегий, их (ролей) использование способствует понижению сложности и, следовательно, улучшению управляемости. Кроме того, на основании ролевой модели можно реализовать такие важные принципы, как разделение обязанностей (невозможность в одиночку скомпрометировать критически важный процесс). Между ролями могут быть определены статические или динамические отношения несовместимости (невозможности одному субъекту по очереди или одновременно активизировать обе роли), что и обеспечивает требуемую защиту.

Для некоторых употребительных сервисов, таких, как Web, ролевое управление доступом может быть реализовано относительно просто (в Web-случае — на основе cgi-процедур).

Протоколирование/аудит. Протоколирование и аудит традиционно являлись рубежом обороны, обеспечивающим анализ последствий нарушения информационной безопасности и выявление злоумышленников. Такой аудит можно назвать пассивным.

Довольно очевидным обобщением пассивного аудита для сетевой среды является совместный анализ регистрационных журналов отдельных компонентов на предмет выявления противоречий, что важно в случаях, когда злоумышленнику удалось отключить протоколирование или модифицировать журналы.

В современный арсенал защитных средств несколько лет назад вошел активный аудит, направленный на выявление подозрительных действий в реальном масштабе времени. Активный аудит включает два вида действий:

- выявление нетипичного поведения (пользователей, программ или аппаратуры);
- выявление начала злоумышленной активности.

Нетипичное поведение выявляется статистическими методами, путем сопоставления с предварительно полученными образцами. Начало злоумышленной активности обнаруживается по совпадению с сигнатурами известных атак. За обнаружением следует заранее запрограммированная реакция (как минимум — информирование системного администратора, как максимум — контратака на систему предполагаемого злоумышленника).

Важным элементом современной трактовки протоколирования/аудита является протокол автоматизированного обмена информацией о нарушениях безопасности между корпоративными системами, подключенными к одной внешней сети. В наше время системы не могут считаться изолированными, они не должны жить по закону «каждый за себя»; угрозам следует противостоять сообща.

Экранирование. Экранирование как сервис безопасности выполняет следующие функции:

- разграничение межсетевого доступа путем фильтрации передаваемых данных;
- преобразование передаваемых данных.

Современные межсетевые экраны фильтруют данные на основе заранее заданной базы правил, что позволяет, по сравнению с традиционными операционными системами, реализовывать гораздо более гибкую политику безопасности. При комплексной фильтрации, охватывающей сетевой, транспортный и прикладной уровни, в правилах могут фигурировать сетевые адреса, количество переданных данных, операции прикладного уровня, параметры окружения (например, время) и т. п.

Преобразование передаваемых данных может затрагивать как служебные поля пакетов, так и прикладные данные. В первом случае обычно имеется в виду трансляция адресов, помогающая скрыть топологию защищаемой системы. Это уникальное свойство сервиса экранирования, позволяющее скрывать существование некоторых объектов доступа. Преобразование данных может состоять, например, в их шифровании.

В процессе фильтрации (точнее, параллельно с ней) может выполняться дополнительный контроль (например, антивирусный). Возможны и дополнительные преобразования, наиболее актуальным из которых является исправление заголовков или иной служебной информации, ставшей некорректной после наступления 2000 года.

Применение межсетевого экранирования поставщиками Internet-услуг в соответствии с рекомендациями разработчиков позволило бы существенно снизить шансы злоумышленников и облегчить их прослеживание. Данная мера еще раз показывает, как важно рассматривать каждую информационную систему как часть глобальной инфраструктуры и принимать на себя долю ответственности за общую информационную безопасность.

Туннелирование. Его суть состоит в том, чтобы «упаковать» передаваемую порцию данных вместе со служебными полями в новый «конверт». Данный сервис может применяться для нескольких целей:

- осуществления перехода между сетями с разными протоколами (например, IPv4 и IPv6);
- обеспечения конфиденциальности и целостности всей передаваемой порции, включая служебные поля.

Туннелирование может применяться как на сетевом, так и прикладном уровнях. Например, стандартизовано туннелирование для IP и двойное конвертование для почты X.400.

Комбинация туннелирования и шифрования (с необходимой криптографической инфраструктурой) на выделенных шлюзах позволяет реализовать такое важное в современных условиях защитное средство, как виртуальные частные сети. Такие сети, «наложенные» обычно поверх Internet, существенно дешевле и гораздо безопаснее, чем действительно собственные сети организации, построенные на выделенных каналах. Коммуникации на всем их протяжении физически защитить невозможно, поэтому лучше изначально исходить из предположения об уязвимости и соответственно обеспечивать защиту. Современные протоколы, направленные на поддержку классов обслуживания, помогут гарантировать для виртуальных частных сетей заданную пропускную способность, величину задержек и т. п., ликвидируя тем самым единственное на сегодняшний день реальное преимущество собственных сетей.

Шифрование. Шифрование — важнейшее средство обеспечения конфиденциальности и одновременно самое конфликтное

место информационной безопасности. У компьютерной криптографии две стороны — собственно криптографическая и интерфейсная, позволяющая сопрягаться с другими частями информационной системы. Важно, чтобы были обеспечены достаточное функциональное богатство интерфейсов и их стандартизация. Криптографией, в особенности шифрованием, должны, разумеется, заниматься профессионалы. От них требуется разработка защищенных инвариантных компонентов, которые можно было бы свободно (по крайней мере, с технической точки зрения) встраивать в существующие и перспективные конфигурации.

У современного шифрования есть и внутренние проблемы как технические, так и нормативные. Из технических наиболее острой является проблема производительности. Программная реализация на универсальных процессорах не является адекватным средством (здесь можно провести аналогию с компрессией видеоизображений). Еще одна техническая задача — разработка широкого спектра продуктов, предназначенных для использования во всех видах компьютерного и сетевого оборудования, — от персональных коммуникаторов до мощных шлюзов.

Контроль целостности. В современных системах контроль целостности должен распространяться не только на отдельные порции данных, аппаратные или программные компоненты. Он обязан охватывать распределенные конфигурации, защищать от несанкционированной модификации потоки данных.

В настоящее время существует достаточно решений для контроля целостности и с системной, и с сетевой направленностью (обычно контроль выполняется прозрачным для приложений образом как часть общей протокольной активности). Стандартизован программный интерфейс к этому сервису.

Контроль защищенности. Контроль защищенности по сути представляет собой попытку «взлома» информационной системы, осуществляемого силами самой организации или уполномоченными лицами. Идея данного сервиса в том, чтобы обнаружить слабости в защите раньше злоумышленников. В первую очередь, имеются в виду не архитектурные (их ликвидировать сложно), а «оперативные» бреши, появившиеся в результате ошибок администрирования или из-за невнимания к обновлению версий программного обеспечения.

Средства контроля защищенности позволяют накапливать и многократно использовать знания об известных атаках. Очевидна их схожесть с антивирусными средствами; формально послед-

ние можно считать их подмножеством. Очевиден и реактивный, запаздывающий характер подобного контроля (он не защищает от новых атак). Следует помнить, что оборона должна быть эшелонированной, так что в качестве одного из рубежей контроль защищенности вполне адекватен. Подавляющее большинство атак носит рутинный характер; они возможны только потому, что известные уязвимости годами остаются неустраненными.

Существуют как коммерческие, так и свободно распространяемые продукты для контроля защищенности. Впрочем, в данном случае важно не просто один раз получить и установить их, но и постоянно обновлять базу данных уязвимостей. Это может оказаться не проще, чем следить за информацией о новых атаках и рекомендуемых способах противодействия.

Обнаружение отказов и оперативное восстановление. Обнаружение отказов и оперативное восстановление относятся к числу сервисов, обеспечивающих высокую доступность (готовность). Его работа опирается на элементы архитектурной безопасности, а именно на существование избыточности в аппаратно-программной конфигурации.

В настоящее время спектр программных и аппаратных средств данного класса можно считать сформировавшимся. На программном уровне соответствующие функции берет на себя программное обеспечение промежуточного слоя. Среди аппаратно-программных продуктов стандартом стали кластерные конфигурации. Восстановление производится действительно оперативно (десятки секунд, в крайнем случае, минуты), прозрачным для приложений образом.

Обнаружение отказов и оперативное восстановление может играть по отношению к другим средствам безопасности роль инфраструктурного сервиса, обеспечивая высокую готовность последних. Это особенно важно для межсетевых экранов, средств поддержки виртуальных частных сетей, серверов аутентификации, нормальное функционирование которых критически важно для корпоративной информационной системы в целом. Такие комбинированные продукты получают все более широкое распространение.

Управление. Управление относится к числу инфраструктурных сервисов, обеспечивающих нормальную работу функционально полезных компонентов и средств безопасности. Сложность современных систем такова, что без правильно организованного управления они постепенно (а иногда и довольно

быстро) деградируют как в плане эффективности, так и в плане защищенности.

Особенно важной функцией управления является контроль согласованности конфигураций различных компонентов (имеется в виду семантическая согласованность, относящаяся, например, к наборам правил нескольких межсетевых экранов). Процесс администрирования идет постоянно; требуется, однако, чтобы при этом не нарушалась политика безопасности.

Место сервисов безопасности в архитектуре информационных систем. Выше был приведен перечень сервисов безопасности. Как объединить их для создания эшелонированной обороны, каково их место в общей архитектуре информационных систем?

На внешнем рубеже располагаются средства выявления злоумышленной активности и контроля защищенности. Далее идут межсетевые экраны, защищающие внешние подключения. Они вместе со средствами поддержки виртуальных частных сетей (обычно объединяемых с межсетевыми экранами) образуют периметр безопасности, отделяющий корпоративную систему от внешнего мира.

Сервис активного аудита должен присутствовать во всех критически важных компонентах и, в частности, в защитных. Это позволит быстро обнаружить атаку, даже если по каким-либо причинам она окажется успешной.

Управление доступом также должно присутствовать на всех сервисах, функционально полезных и инфраструктурных. Доступу должна предшествовать идентификация и аутентификация субъектов.

Криптографические средства целесообразно выносить на специальные шлюзы, где им может быть обеспечено квалифицированное администрирование. Масштабы пользовательской криптографии следует минимизировать.

Наконец, последний рубеж образуют средства пассивного аудита, помогающие оценить последствия нарушения безопасности, найти виновного, выяснить, почему успех атаки стал возможным.

Расположение средств обеспечения высокой доступности определяется критичностью соответствующих сервисов или их компонентов. Для обеспечения доступности (непрерывности функционирования) могут применяться следующие защитные меры:

- внесение в конфигурацию той или иной формы избыточности (резервное оборудование, запасные каналы связи и

т. п.). Это элемент архитектурной безопасности, рассматриваемой в следующем разделе;

- наличие средств обнаружения отказов. Если требуется постоянная высокая готовность, необходим специализированный сервис. В остальных случаях достаточно протоколирования/аудита в квазиреальном времени;
- наличие средств реконфигурирования для восстановления, изоляции и/или замены компонентов, отказавших или подвергшихся атаке на доступность. Это или специализированная функция, или одна из функций управления;
- рассредоточенность сетевого управления, отсутствие единой точки отказа. Это, как и следующий пункт, — элементы архитектурной безопасности;
- выделение подсетей и изоляция групп пользователей друг от друга. Данная мера ограничивает зону поражения при возможных нарушениях информационной безопасности.

Каждый компонент, вообще говоря, не обязан поддерживать все перечисленные выше сервисы безопасности. Важно, чтобы он обладал программными и/или протокольными интерфейсами для получения недостающих сервисов от других компонентов и чтобы не существовало возможности обхода основных и дополнительных защитных средств.

Международные стандарты

Стандарт X.800 описывает основы безопасности в привязке к эталонной семиуровневой модели. Это довольно обширный документ. Совсем коротко остановимся на предлагаемых в нем сервисах (функциях) безопасности и на администрировании средств безопасности.

Стандарт предусматривает следующие сервисы безопасности:

- аутентификация (имеется в виду аутентификация партнеров по общению и аутентификация источника данных);
- управление доступом — обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети;
- конфиденциальность данных. В X.800 под этим названием объединены существенно разные вещи — от защиты отдельной порции данных до конфиденциальности трафика;
- целостность данных. Данный сервис подразделяется на подвиды в зависимости от того, что контролируется — це-

лостность сообщений или потока данных, обеспечивается ли восстановление в случае нарушения целостности;

- неотказуемость. Данный сервис относится к прикладному уровню, т. е. имеется в виду невозможность отказаться от содержательных действий, таких, например, как отправка или прочтение письма.

Администрирование средств безопасности включает в себя распространение информации, необходимой для работы сервисов безопасности, а также сбор и анализ информации об их функционировании. Примерами могут служить распространение криптографических ключей, установка прав доступа, анализ регистрационного журнала и т. п.

Концептуальной основой администрирования является информационная база управления безопасностью. Эта база может не существовать как единое (распределенное) хранилище, но каждый компонент системы должен располагать информацией, достаточной для проведения в жизнь избранной политики безопасности.

В условиях глобальной связности администрирование перестает быть внутренним делом организации. Во-первых, плохо защищенная система может стать плацдармом для подготовки и проведения злоумышленных действий. Во-вторых, прослеживание нарушителя эффективно лишь при согласованных действиях многих администраторов.

Стандарт X.509 описывает процедуру аутентификации с использованием службы каталогов. Впрочем, наиболее ценной в стандарте оказалась не сама процедура, а ее служебный элемент — структура сертификатов, хранящих имя пользователя, криптографические ключи и сопутствующую информацию. Подобные сертификаты — важнейший элемент современных схем аутентификации и контроля целостности.

Рекомендации IETF. Сообществом Internet под эгидой Тематической группы по технологии Internet (Internet Engineering Task Force — IETF) разработано много рекомендаций по отдельным аспектам сетевой безопасности. Тем не менее какой-либо целостной концепции или архитектуры безопасности пока предложено не было.

Рекомендации периодически организуемых конференций по архитектуре безопасности Internet носят весьма общий, а порой и формальный характер. Основная идея состоит в том, чтобы средствами оконечных систем обеспечивать сквозную безопас-

ность. От сетевой инфраструктуры в лучшем случае ожидается устойчивость по отношению к атакам на доступность.

Базовые протоколы, наиболее полезные с точки зрения безопасности, включают в себя — IPsec, DNSsec, S/MIME, X.509v3, TLS и ассоциированные с ними. Наиболее проработанными на сегодняшний день являются вопросы защиты на IP-уровне. Спецификации семейства IPsec регламентируют следующие аспекты:

- управление доступом;
- контроль целостности на уровне пакетов;
- аутентификация источника данных;
- защита от воспроизведения;
- конфиденциальность (включая частичную защиту от анализа трафика);
- администрирование (управление криптографическими ключами).

Протоколы обеспечения аутентичности и конфиденциальности могут использоваться в двух режимах: транспортном и туннельном. В первом случае защищается только содержимое пакетов и, быть может, некоторые поля заголовков. Как правило, транспортный режим используется хостами (серверами). В туннельном режиме защищается весь пакет — он инкапсулируется в другой IP-пакет. Туннельный режим обычно реализуют на специально выделенных защитных шлюзах (в роли которых могут выступать маршрутизаторы или межсетевые экраны).

Следует отметить, что IP-уровень можно считать оптимальным для размещения защитных средств, поскольку при этом достигается удачный компромисс между защищенностью, эффективностью функционирования и прозрачностью для приложений. Стандартизованными механизмами IP-безопасности могут (и должны) пользоваться протоколы более высоких уровней и, в частности, управляющие протоколы, протоколы конфигурирования и маршрутизации.

На транспортном уровне аутентичность, конфиденциальность и целостность потоков данных обеспечивается протоколом TLS (Transport Layer Security, RFC 2246). Подчеркнем, что здесь объектом защиты являются не отдельные сетевые пакеты, а именно потоки данных (последовательности пакетов). Злоумышленник не сможет переупорядочить пакеты, удалить некоторые из них или вставить свои.

На основе TLS могут строиться защищенные протоколы прикладного уровня. В частности, предложены спецификации для HTTP над TLS.

6.3. Архитектура механизмов защиты информации в сетях ЭВМ

Архитектуру механизмов защиты информации рассмотрим на примере наиболее распространенной эталонной модели взаимодействия открытых систем (ВОС).

Основные концепции применения методов и средств защиты информации на уровне базовой эталонной модели изложены в международном стандарте ISO/IEC 7498-2 «Базовая эталонная модель взаимодействия открытых систем», часть 2 «Архитектура безопасности». В самом наименовании ВОС термин «открытые» подразумевает, что если вычислительная система соответствует стандартам ВОС, то она будет открыта для взаимосвязи с любой другой системой, которая соответствует тем же стандартам. Это, естественно, относится и к вопросам защиты информации.

Все функции открытых систем, обеспечивающие взаимосвязь, распределены в эталонной модели по семи уровням. Разработанная в этом документе архитектура защиты информации ВОС создает единую основу для создания серии стандартов по защите информации, цель которых — уменьшить до приемлемого уровня риск несанкционированного доступа, осуществляемого с целью хищения, порчи (в том числе введения вируса), подмены, уничтожения информации. Воздействие на информацию может произойти по причинам случайного и умышленного характера. Последние могут носить пассивный (прослушивание без нарушения работы системы, копирование информации) и активный (модификация и подмена информации, изменение состояния системы, введение вирусов и т. п.) характер. В ВОС различают следующие основные активные способы несанкционированного доступа к информации:

1) маскировка одного логического объекта под другой, который обладает бо́льшими полномочиями (ложная аутентификация абонента);

2) переадресация сообщений (преднамеренное искажение адресных реквизитов);

3) модификация сообщений (преднамеренное искажение информационной части сообщения);

4) блокировка логического объекта с целью подавления некоторых типов сообщений (выборочный или сплошной перехват сообщений определенного абонента, нарушение управляющих последовательностей и т. п.).

Поскольку эталонная модель относится только к взаимосвязи открытых систем, то и защита информации рассматривается в том же аспекте. Прежде всего приведем перечень видов услуг, предоставляемых по защите информации, которые обеспечиваются с помощью специальных механизмов защиты.

Услуги механизмов защиты

В настоящее время определено четырнадцать таких услуг:

1) аутентификация равнозначного логического объекта (удостоверение подлинности удаленного абонента-получателя) — обеспечивается во время установления их соединения или во время нормального обмена данными для гарантии того, что равноправный логический объект, с которым осуществляется взаимодействие, является тем, за кого себя выдает. Для аутентификации равнозначного логического объекта требуется, чтобы лежащий ниже уровень обеспечивал услуги с установлением соединения;

2) аутентификация источника данных — подтверждение подлинности источника (абонента-отправителя) сообщения. Эта услуга не ориентирована на соединение и не обеспечивает защиту от дублирования («проигрывания» ранее перехваченного и записанного нарушителем) блока данных;

3) управление доступом (разграничение доступа) — обеспечивает защиту от несанкционированного доступа к ресурсам, потенциально доступным посредством ВОС. Доступ может быть ограничен полностью или частично. Например, для информационного ресурса может быть ограничен доступ по чтению, записи, уничтожению информации;

4) засекречивание соединения — обеспечивает конфиденциальность всех сообщений, передаваемых пользователями в рамках данного соединения. Данная услуга направлена на предотвращение возможности ознакомления с содержанием сообщений со стороны любых лиц, не являющихся легальными пользовате-

лями соединения. При этом в некоторых случаях нет необходимости в защите срочных данных, а также данных в запросе на установление соединения;

5) засекречивание в режиме без установления соединения — обеспечивает конфиденциальность всех данных пользователя в сообщении (единственном сервисном блоке данных), передаваемом в режиме без установления соединения;

6) засекречивание поля данных — обеспечивает конфиденциальность отдельных полей данных пользователя на всем соединении или в отдельном сервисном блоке данных;

7) засекречивание трафика — препятствует возможности извлечения информации из наблюдаемого трафика;

8) целостность соединения с восстановлением — позволяет обнаружить попытки вставки, удаления, модификации или переадресации в последовательности сервисных блоков данных. При нарушении целостности предпринимается попытка ее восстановления;

9) целостность соединения без восстановления — обеспечивает те же возможности, что и предыдущая услуга, но без попытки восстановления целостности;

10) целостность поля данных в режиме с установлением соединения — обеспечивает целостность отдельного поля данных пользователя во всем потоке сервисных блоков данных, передаваемых через это соединение, и обнаруживает вставку, удаление, модификацию или переадресацию этого поля;

11) целостность блока данных в режиме без установления соединения — обеспечивает целостность единственного сервисного блока данных при работе без установления соединения и позволяет обнаружить модификацию и некоторые формы вставки и переадресации;

12) целостность поля данных в режиме без установления соединения — позволяет обнаружить модификацию выбранного поля в единственном сервисном блоке данных;

13) информирование об отправке данных — позволяет обнаружить логические объекты, которые посылают информацию о нарушении правил защиты информации. Информирование об отправке предоставляет получателю информацию о факте передачи данных в его адрес, обеспечивает подтверждение подлинности абонента-отправителя. Услуга направлена на предотвращение отрицания отправления, т. е. возможности отказа от факта передачи данного сообщения со стороны отправителя;

14) информирование о доставке — позволяет обнаружить логические объекты, которые не выполняют требуемых действий после приема информации, предоставляет отправителю информацию о факте получения данных адресатом. Услуга направлена на предотвращение отрицания доставки, т. е. обеспечивает защиту от попыток получателя отрицать факт получения данных.

Теоретически доказано, а практика защиты сетей подтвердила, что все перечисленные услуги могут быть обеспечены криптографическими средствами защиты, в силу этого эти средства и составляют основу всех механизмов защиты информации в ВС. Центральными при этом являются следующие задачи:

1) взаимное опознавание (аутентификация) вступающих в связь абонентов сети;

2) обеспечение конфиденциальности циркулирующих в сети данных;

3) обеспечение юридической ответственности абонентов за передаваемые и принимаемые данные.

К настоящему времени разработан ряд протоколов аутентификации, основанных на использовании шифрования, которые обеспечивают надежную взаимную аутентификацию абонентов вычислительной сети без экспозиции любого из абонентов. Эти протоколы являются стойкими по отношению ко всем рассмотренным выше угрозам безопасности сети.

Общий принцип взаимной аутентификации, положенный в основу этих протоколов, состоит в шифровании быстро изменяющейся уникальной величины, например времени сеанса связи, при этом используются предварительно распределенные между абонентами ключи. Для применения этих протоколов необходимо установить взаимное согласие между абонентами по начальному значению последовательного числа или цепочки блоков. Начальное значение числа должно иметь величину, которая либо ранее не использовалась, либо выбиралась случайным образом для защиты от возможной угрозы предъявления ответов предыдущих сеансов.

Для того чтобы несколько участников сетевых переговоров (взаимодействия) могли осуществлять между собой секретную связь, необходимо, чтобы они получили согласованные пары ключей для шифрования и дешифрования передаваемых данных.

Необходимо отметить, что согласованная пара ключей образует логический канал, который не зависит от всех других логических каналов, но является столь же реальным, как и любой

другой канал связи, образуемый протоколами обмена в вычислительной сети. Владение ключом допускает абонента к каналу связи (без ключа канал для него недоступен). Исключительно важным является вопрос, как распределяются ключи, которые создают соответствующие каналы взаимодействия. Ниже перечислены различные методы и алгоритмы распределения ключей как для систем с использованием традиционного шифрования, так и для систем шифрования с открытыми ключами.

Так как предполагается, что не существует других каналов, кроме определенных физических каналов связи, то необходимо сконструировать алгоритмы распределения ключей между абонентами по тем же самым физическим каналам связи, по которым передаются данные. Безопасность логических каналов связи, по которым передаются ключи, приобретает решающее значение. Единственным методом, с помощью которого любые данные, включая ключи, могут быть переданы секретным способом, является шифрование.

Отметим ряд особенностей, имеющих место при распределении ключей в системах управления базами данных (СУБД). Прежде всего надо обратить внимание на некоторые фундаментальные различия между безопасностью операционных систем и защитой в базах данных:

1) количество подлежащих защите объектов в базе данных может быть больше на несколько порядков;

2) как правило, защита в базах данных связана с различными уровнями организации объектов: файл, тип записи, тип полей, экземпляр поля и т. д.;

3) в СУБД объекты могут представлять собой сложные логические структуры, лишь некоторые из которых могут соответствовать физическим объектам;

4) безопасность в базах данных более связана с семантикой данных, а не с их физическими характеристиками.

Любая СУБД есть полная или частичная реализация некоторой политики безопасности, которая может содержать или не содержать криптографические механизмы безопасности. Основной проблемой использования криптографических методов для защиты информации в СУБД является проблема распределения ключей шифрования, управления ключами.

Ключи шифрования для баз данных требуют использования специфических мер защиты. Если база данных разделяется между многими пользователями (что, как правило, и имеет место на

практике), то предпочтительно хранить ключи в самой системе под защитой главного ключа, чем распределять ключи прямо между пользователями. Сама задача управления при этом может возлагаться на пользователя. Вторичные ключи могут храниться либо в самой базе данных, либо в отдельном файле.

Отметим, что любой протокол шифрования должен отвечать на следующие основные вопросы:

1) каким образом устанавливается первоначальный канал связи между отправителем и получателем с операциями «открытый текст — шифротекст — открытый текст»?

2) какие предоставляются средства для восстановления процесса обмена и восстановления синхронизации протокола?

3) каким образом закрываются каналы?

4) каким образом взаимодействуют протоколы шифрования с остальными протоколами сети?

5) каков объем необходимого математического обеспечения для реализации протоколов шифрования и зависит ли безопасность сети от этих программ?

6) каким образом адресация открытого текста, проставляемая отправителем, проходит через средства информации в сети, чтобы предотвратить пути, по которым данные открытого текста могли бы быть намеренно или случайно скомпрометированы?

Желательно иметь протокол, который позволяет производить динамическое открытие и закрытие канала, обеспечивать защиту от сбоев и все это с минимальными объемами механизма, от которого зависит безопасность сети. Характеристики сети, получающиеся при использовании соответствующего протокола шифрования, должны сравниваться с характеристиками сети без использования протоколов шифрования. Несомненно, что предпочтительней использование общего сетевого протокола, который мог бы встраиваться в сеть с минимальным нарушением существующих механизмов передачи.

Распределение базовых ключей (например, главных) может выполняться вне рамок ВОС администратором системы, центром распределения ключей и т. д.

Механизм управления доступом, предназначенный для реализации соответствующего вида перечисленных выше услуг, основан на идентификации логического объекта (или информации о нем) для проверки его полномочий и разграничения доступа. Если логический объект пытается получить доступ к ресурсу, использование которого ему не разрешено, механизм управления

доступом (в основе которого также наиболее эффективными средствами являются криптографические) отклонит эту попытку и сформирует запись в специальном системном журнале для последующего анализа. Механизмы управления доступом могут быть основаны:

1) на информационных базах управления доступом, где содержатся сведения о полномочиях всех логических объектов;

2) системах управления криптографическими ключами, обеспечивающими доступ к соответствующей информации;

3) идентифицирующей информации (такой, как пароли), предъявление которой дает право доступа;

4) специальных режимах и особенностях работы логического объекта, которые дают право доступа к определенным ресурсам;

5) специальных метках, которые, будучи ассоциированы с конкретным логическим объектом, дают ему определенные права доступа;

6) времени, маршруте и продолжительности доступа.

Механизмы удостоверения целостности данных подразделяются на два типа: обеспечивающие целостность единственного блока данных и обеспечивающие целостность потока блоков данных или отдельных полей этих блоков. Целостность единственного блока данных достигается добавлением к нему при передаче проверочной величины (контрольной суммы, имитовставки), которая является секретной функцией самих данных. При приеме генерируется (формируется) такая же величина и сравнивается с принятой. Защита целостности последовательности блоков данных требует явного упорядочения блоков с помощью их последовательной нумерации, криптографического упорядочения или отметки времени.

Механизмы аутентификации (взаимного удостоверения подлинности) абонентов, вступающих в связь, используют пароли, криптографические методы, а также характеристики и взаимоотношения подчиненности логических объектов. Криптографические методы могут использоваться в сочетании с протоколами взаимных ответов («рукопожатия») для защиты от переадресации. Если обмен идентификаторами не даст положительного результата, то соединение отклоняется или заканчивается с соответствующей записью в системном журнале и выдачей сообщения об этом событии.

Механизм заполнения трафика используется для защиты от попыток анализа трафика. Он эффективен только в случае шиф-

рования всего трафика, когда нельзя отличить информацию от заполнения.

Механизм управления маршрутизацией позволяет использовать только безопасные с точки зрения защиты информации фрагменты сети, участки переприема, коммуникации, звенья. Может быть запрещена передача некоторых данных по определенным маршрутам или оконечная система, обнаружив воздействие на ее информацию, может потребовать предоставить ей маршрут доставки данных, обеспечивающий их конфиденциальность и целостность.

Механизм нотариального заверения обеспечивается участием третьей стороны — «нотариуса», позволяет подтвердить целостность данных, удостоверить источник и приемник данных, время сеанса связи и т. п.

Методы цифровой подписи данных, передаваемых в сети

Механизм цифровой подписи, реализуемый также криптографическими методами, состоит из двух процессов:

1) формирования подписи блока данных при передаче;

2) проверки подписи в принятом блоке данных.

Первый процесс заключается в формировании подписи по определенному алгоритму с использованием секретного ключа, второй — в обратном преобразовании.

Цифровая подпись оказывается необходимой во многих практических приложениях. Считается, что для реализации цифровой подписи методы шифрования с открытыми ключами предпочтительнее традиционных методов шифрования. При наличии подходящего алгоритма шифрования с секретным ключом метод реализации цифровой подписи для отправителя состоит в шифровании сообщения секретным ключом и отправке этого сообщения получателю. Получатель, дешифруя сообщение общим с отправителем секретным ключом, убеждается в том, что его автором действительно был отправитель. Обычно эта процедура не требует центрального уполномоченного (нотариуса). Необходимо, однако, отметить два момента. Во-первых, ключ необходим принимающему абоненту для помощи в дешифровании первого сообщения, в процедуре аутентификации. Во-вторых, центральный уполномоченный должен надежным образом под-

держивать все старые значения общих ключей, чтобы правильно разрешать возможные конфликты между старыми подписями. Кроме того, приведенный протокол подписи с общим секретным ключом имеет и такой важный недостаток. Автор подписанных сообщений может не признать свою подпись, просто утверждая, что его ключ был скомпрометирован. Если такое происходит преднамеренно или случайно, то все ранее подписанные сообщения данным личным ключом становятся недействительными, так как единственное доказательство их подлинности было разрушено. Следовательно, в таком случае действительность подписи на сообщении будет полностью определяться защитой личного ключа. Важная задача при реализации цифровой подписи заключается в обеспечении такой ответственности за содержание сообщения и за собственно подпись, чтобы от нее нельзя было отказаться. Очевидно, что для решения такой задачи должны быть созданы соответствующие механизмы и математически строго показаны их действенность и корректность.

Может быть предложен метод организации цифровой подписи, основанный на любом достаточно сильном методе традиционного шифрования. Такой метод требует также участия центрального уполномоченного либо явного согласия абонентов на разрешение возникающих вопросов. Для взаимной же аутентификации требуется центральный уполномоченный. Таким образом, этот метод реализации цифровой подписи использует большое число ключей, поэтому, если несколько ключей скомпрометировано, то подписи, основанные на других ключах, продолжают быть действительными. Все это не является, однако, явным преимуществом по сравнению с методами цифровой подписи в режиме с общим ключом, так как не трудно внести аналогичный дополнительный уровень и в протокол цифровой подписи на базе общего ключа, чтобы изменять ключи для каждого сообщения.

Все описанные методы цифровой подписи имеют общий недостаток, связанный с проблемой отказа от подписи при компрометации ключа. В методе, основанном на традиционном шифровании, просто ограничивался возможный ущерб (как отмечалось выше). Эта проблема присуща любому подходу, когда действительность авторской подписи зависит от секретной информации, которая может быть потенциально скомпрометирована либо самим автором, либо злоумышленником.

Известен ряд предложений по модификации описанных выше методов, которые основаны на аналогах удостоверения

подлинности, принятых при удостоверении векселей или в процедурах удостоверения скопированных из архива документов, когда используется зависящий от времени механизм удостоверения подлинности, при котором авторы не могут отказаться от ранее подписанной корреспонденции на основании утверждения о возможной компрометации ключа.

Реализация подписи на основе регистрации базируется на расположении некоторого доверенного интерпретирующего уровня: аппаратного или программного средства между автором и его ключами для реализации цифровой подписи. В таком случае можно достаточно просто организовать компоновку этих средств в сеть. Все взаимодействующие в данном случае компоненты размещаются в регистрирующем журнале (NR). При этом необходим некоторый безопасный коммуникационный протокол между компонентами реестра, причем достаточно использовать только канальное шифрование.

Если указанные возможности предоставлены, то реализация цифровой подписи, не требующая специализированных протоколов или алгоритмов шифрования, будет выглядеть следующим образом. Во-первых, автор аутентифицируется с локальной компонентой сетевого журнала регистрации, создает сообщение и передает сообщение в сетевой реестр NR вместе с идентификатором получателя и указанием необходимости получения зарегистрированной подписи. Во-вторых, сетевой реестр NR (не обязательно локальная компонента) вычисляет характеристическую функцию для сообщения автора, идентификатора получателя, текущего времени; шифрует результат ключом, известным только NR, и направляет результирующий блок цифровой подписи получателю. Реестр NR при этом сохраняет использованный ключ шифрования. Наконец, получатель при приеме сообщения может запросить сетевой реестр NR о подлинности подписи автора сообщения, предоставляя реестру блок цифровой подписи и сообщение. Здесь необходимы определенные меры предосторожности для гарантирования безопасности ключей, используемых для шифрования блоков цифровой подписи.

Реализацию безопасной цифровой подписи, основанную на концепции общего нотариуса и архива, можно осуществить с использованием алгоритма шифрования с общим ключом. Один из подходов основан на правилах нотариального удостоверения подлинности документов. Пусть существует ряд подключенных к сети нотариальных общедоступных машин. Нотариальная маши-

на осуществляет удостоверение сообщения с временной отметкой, подписывается сама с помощью повторного шифрования и возвращает автору. Затем автор может присоединить информацию в виде открытого текста к дважды подписанной корреспонденции и послать ее предполагаемому абоненту.

Принимающий абонент проверяет нотариальную подпись посредством расшифровывания ее общедоступным нотариальным ключом, затем расшифровывает сообщение, используя общедоступный авторский ключ. Основополагающим допущением в этом методе является предположение о доверии к нотариусу. Кроме того, в данном случае оказывается еще возможным для кого-нибудь заявить, что его ключ был раскрыт когда-то в прошлом и некоторые сообщения были впоследствии подделаны. От такой ситуации можно защититься путем выдачи под каждый нотариальный вывод копии каждого заверенного сообщения к автору текущего адреса. В силу независимости нотариусов нет необходимости в координации их действий.

Весьма близкий способ получения надежного времени регистрации подписанных сообщений заключается в организации ряда независимых приемных пунктов, куда любой автор или получатель подписанной почты может скопировать корреспонденцию для постоянного хранения с удостоверением времени поступления. При этом нет необходимости хранить все сообщения, достаточно хранения только некоторой характеристической функции. Вызовы обрабатываются с помощью запрашивания архивов.

Алгоритмы реализации цифровой подписи, основанные как на традиционных алгоритмах шифрования, так и на системах шифрования с общим ключом, имеют много общих характеристик. В каждый из этих алгоритмов встроены некоторые доверенные механизмы, которые разделяются между всеми участниками связи. Безопасность подписей, как и прежде, будет зависеть от защиты ключей, включаемых в этом случае в сетевую регистрацию доверия общедоступному нотариусу или средствам архива. Однако существует и несколько решающих отличий от предыдущих протоколов цифровой подписи. Во-первых, авторы не имеют возможности по своему желанию отречься от своей подписи. Во-вторых, новые средства цифровой подписи могут быть структурированы таким образом, что только авария или компрометация нескольких компонентов приводит к утере действительности цифровой подписи.

Пример системы защиты локальной вычислительной сети

Для иллюстрации приведем краткое описание системы защиты локальной вычислительной сети на основе ОС Novell NetWare, известной под названием «Secret NET» [1, 9].

Назначение системы защиты. Система защиты «Secret NET» (далее по тексту Система защиты) предназначена для обеспечения защиты хранимой и обрабатываемой в локальной вычислительной сети (ЛВС) информации от несанкционированного доступа (ознакомления, искажения, разрушения) и противодействия попыткам нарушения нормального функционирования ЛВС и прикладных систем на ее основе.

В качестве защищаемого объекта выступает ЛВС персональных ЭВМ типа IBM PC/AT и старше, работающих под управлением операционной системы MS-DOS версий 3.30-6.2 (рабочие станции) и сетевой операционной системы Novell NetWare 3.1x (файловые серверы), объединенных с помощью сетевого оборудования Ethernet, Arcnet или Token-Ring. Максимальное количество защищенных станций — 256, защищенных файловых серверов — 8, уникально идентифицируемых пользователей — 255.

Системой защиты обеспечивается:

1) защита от лиц, не допущенных к работе с системой обработки информации;

2) регламентация (разграничение) доступа законных пользователей и программ к информационным, программным и аппаратным ресурсам системы в строгом соответствии с принятой в организации политикой безопасности;

3) защита ЭВМ сети от внедрения вредоносных программ (закладок), а также инструментальных и технологических средств проникновения;

4) целостность критических ресурсов Системы защиты и среды исполнения прикладных программ;

5) регистрация, сбор, хранение и выдача сведений обо всех событиях, происходящих в сети и имеющих отношение к ее безопасности;

6) централизованное управление средствами Системы защиты.

Для решения перечисленных задач Система защиты включает следующие подсистемы (ПС):

1) идентификации и аутентификации пользователей;

2) разграничения доступа к ресурсам;
3) контроля целостности;
4) регистрации;
5) управления средствами защиты (администрирования).

Функциональное назначение названных подсистем видно из их названия.

Общее содержание функций подсистем заключается в следующем.

ПС идентификации и аутентификации. Подсистема выполняет функцию идентификации/аутентификации (проверки подлинности) пользователя при каждом его входе в Систему защиты, а также после каждой приостановки его работы. Для идентификации в системе каждому пользователю присваивается уникальное имя. Обеспечивается работа с именами длиной до 12 символов (символов латинского алфавита и специальных символов). Вводимое имя отображается на экране рабочей станции.

Проверка подлинности пользователя осуществляется после его идентификации для подтверждения того, что пользователь действительно является тем, кем представился. Она осуществляется путем проверки правильности введенного пароля. Поддерживается работа с паролями длиной до 16 символов. Вводимый пароль не отображается на экране рабочей станции.

При неправильно введенном пароле на экран выдается сообщение об ошибке и подается звуковой сигнал. При трехкратном неверном вводе пароля блокируется клавиатура, выдается сообщение о попытке НСД на сервер управления доступом и осуществляется оперативное оповещение администратора безопасности, регистрируется попытка НСД в системном журнале и выдается звуковой сигнал.

Пароли администратора и всех пользователей системы хранятся в зашифрованном виде и могут быть изменены как администратором безопасности, так и конкретным пользователем (изменение только своего пароля) с помощью специальных программных средств.

Для повышения защищенности идентификация/аутентификация пользователя может проводиться до загрузки операционной системы. Это обеспечивается специальным техническим устройством (микросхемой ПЗУ или платой Secret NET Card).

ПС разграничения доступа. ПС реализует концепцию диспетчера доступа, при которой ПС является посредником при всех

обращениях субъектов к объектам доступа (попытки обращения к объекту в обход ПС приводят к отказу в доступе); может работать в одном из двух режимов функционирования: основном и технологическом.

Технологический режим предназначен для точного определения объектов, к которым должен иметь доступ пользователь, и прав доступа к ним. При работе в этом режиме Система защиты только регистрирует все попытки доступа к защищаемым ресурсам в системном журнале и выдает предупреждающие сообщения на экран.

В основном режиме Система защиты не только регистрирует попытки доступа к защищаемым ресурсам, но и блокирует их.

ПС обеспечивает контроль доступа субъектов к следующим объектам:

1) физическим и логическим устройствам (дискам, принтерам);
2) каталогам дисков;
3) файлам;
4) физическим и логическим секторам дисков.

В подсистеме реализована сквозная иерархическая схема действия прав доступа к локальным объектам рабочей станции, при которой объект нижнего уровня наследует права доступа объектов доступа верхних уровней (диск-каталог-файл).

Любой объект на рабочей станции может обладать меткой безопасности. Метка безопасности указывает, какие операции может произвести субъект над данным объектом, кто является его владельцем, а также признак, разрешающий программе (если данный объект — программа) работу с физическими секторами дисков. Метка безопасности заполняется при создании объекта и может корректироваться как пользователем-владельцем объекта, так и администратором.

Права доступа пользователя к объектам системы могут принимать следующие значения:

- запрет доступа — пользователь не имеет возможности выполнять с объектом какие-либо действия;
- наличие доступа — в этом случае уровень доступа может быть одним из следующих: доступ на чтение, доступ на запись, доступ на исполнение (субъект может только запустить объект на исполнение).

Управление доступом. Управление доступом к локальным логическим или физическим дискам осуществляется с помощью

информации о доступе, помещаемой в паспорт пользователя при его создании администратором. Управление доступом к удаленным дискам, каталогам и файлам осуществляется администратором системы с помощью утилит системы разграничения доступа сетевой ОС Novell NetWare 3. lx.

Пользователю предоставлена только возможность назначения прав доступа других пользователей к принадлежащим ему (созданным им) объектам.

Для реализации избирательного управления доступом подсистема поддерживает замкнутую среду доверенного программного обеспечения (с помощью индивидуальных для каждого пользователя списков программ, разрешенных для запуска). Создание и ведение списков программ возложено на администратора. Для этого в его распоряжении имеются специальные программные средства.

Для совместного использования программ и данных Система защиты предусматривает возможность объединения пользователей в группы. Права доступа группы наследуются всеми пользователями этой группы.

ПС контроля целостности. В системе контролируется целостность следующих объектов: операционных систем локальных рабочих станций, программ Системы защиты, файлов паспортов пользователей и системных областей локальных дисков рабочих станций, а также файлов пользователей (по их требованию). Контроль осуществляется методом контрольного суммирования с использованием специального алгоритма и производится периодически администратором. Для этого ему предоставлены соответствующие программные средства.

В случае обнаружения нарушения целостности контролируемых объектов производится регистрация этого события в системном журнале и оперативное оповещение администратора. В случае нарушения целостности системных областей диска, кроме того, производится их восстановление с использованием резервных копий.

ПС регистрации событий безопасности. ПС регистрации обеспечивает:

1) ведение и анализ журналов регистрации событий безопасности (системных журналов), причем журнал регистрации ведется для каждой рабочей станции сети;

2) оперативное ознакомление администратора с системным журналом любой станции и с журналом событий об НСД;

3) получение твердой копии системного журнала;

4) преобразование содержимого системных журналов в формат DBF для их дальнейшего анализа;

5) объединение системных журналов и их архивирование;

6) оперативное оповещение администратора о нарушениях безопасности.

ПС управления средствами защиты. Подсистема позволяет администрации безопасности осуществлять:

1) централизованное (с АРМ администратора) создание и удаление пользователей, изменение их полномочий и паролей;

2) установку атрибутов доступа пользователей к ресурсам;

3) централизованное создание, удаление и изменение состава групп пользователей, а также их прав доступа;

4) централизованное управление группами компьютеров;

5) централизованное управление оперативным оповещением о НСД;

6) централизованное управление регистрацией событий и просмотр системных журналов.

Требования к условиям эксплуатации. Предполагается, что для эффективного применения Системы защиты и поддержания необходимого уровня защищенности ЛВС специальной службой (администрацией безопасности системы) осуществляется непрерывное управление и организационно-административная поддержка ее функционирования по реализации принятой в организации политики безопасности.

Система функционирует на ПЭВМ, совместимых с IBM PC/AT/386/486. В состав ПЭВМ каждой рабочей станции должен входить накопитель на жестком диске и сетевая плата ЛВС.

Затраты ресурсов. Объем занимаемой оперативной памяти под резидентные части Системы защиты:

1) на рабочей станции — до 19—25 Кбайт (в зависимости от используемого драйвера);

2) на файловом сервере — до 500 Кбайт.

Относительные затраты производительности процессора:

1) на рабочей станции — до 2 %;

2) на файловом сервере — до 3 %.

Объем дисковой памяти для программ и данных:

1) на рабочей станции — до 500 Кбайт;

2) на файловом сервере — до 10 Мбайт.

Межсетевые экраны — брандмауэры (FireWall) [1]

Гостехкомиссией при Президенте РФ разработан Руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» в дополнение к руководящим документам «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» и «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». В указанном документе межсетевой экран (МЭ) определяется как локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему (АС) и /или выходящей из АС. МЭ обеспечивает защиту АС посредством фильтрации информации (как минимум на сетевом уровне), т. е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС на основе заданных правил, проводя таким образом разграничение доступа субъектов из одной АС к объектам другой АС. Каждое правило запрещает или разрешает передачу информации определенного вида между субъектами и объектами. Как следствие субъекты из одной АС получают доступ только к разрешенным информационным объектам из другой АС. Интерпретация набора правил выполняется последовательностью фильтров, которые разрешают или запрещают передачу данных (пакетов) на следующий фильтр или уровень протокола.

Выделяются пять классов МЭ, где пятый — низший, а первый — высший. Классифицируемый экран должен фильтровать потоки данных, по крайней мере, на сетевом уровне. При умеренных требованиях по защите информации можно ограничиться МЭ пятого или четвертого классов, реализованных в виде маршрутизаторов с включенными средствами фильтрации (экранирующих маршрутизаторов).

Для обеспечения контроля доступа к определенным массивам информации во многих точках Intranet-сети наиболее целесообразно применять так называемые аппаратные брандмауэры. Они являются специализированными компьютерами, как прави-

ло, встраиваемыми в стойку с сетевой ОС, адаптированной под выполняемые функции (загрузка ОС производится с гибкого диска или же из постоянной памяти). Чтобы представить, какие возможности имеют аппаратные брандмауэры, достаточно рассмотреть функциональные возможности следующих изделий.

Брандмауэр FireBox (производства WatchGuard) имеет смешанную архитектуру — динамической фильтрации пакетов и «прозрачного» прокси (proxy) (при этом с глобальной сетью организуется двухсторонняя связь, о proxy-технологии более подробно будет сказано далее). В архитектуре брандмауэра:

- обеспечивается оптимальный баланс между безопасностью и производительностью;
- динамическая фильтрация пакетов отслеживает состояние соединения, что позволяет «отфильтровывать» не только пакеты, но и соединения;
- наборы правил являются динамическими и могут быть изменены во время работы (в набор входит 28 стандартных правил типа DNS, Telnet и др. и могут определяться правила пользователями в зависимости от потребностей и угроз безопасности);
- прокси анализирует график на сетевом уровне, что дает возможность получить более надежную защиту;
- могут распознаваться подмены сервисов и пакетов;
- имеется функция регистрации пользователей (это позволяет не только повысить безопасность, но и вести мониторинг сети на основе имен пользователей, а не IP-адресов и имен хостов);
- обеспечивается поддержка VPN (Virtual Private Network — виртуальная частная сеть), т. е. безопасный доступ в корпоративную сеть через Internet (для авторизованных удаленных пользователей. При этом используется протокол PPTP (Point-to-Point Tunelling Protocol — туннельный протокол точка-точка), который создает в общей сети безопасный «туннель», через который «прозрачно» проходит весь трафик.

Брандмауэр от компании Bay Network отличается тем, что он входит в состав маршрутизатора BCN. Так как маршрутизатор является устройством, которое выполняет функции передачи пакетов, вычислительные возможности указанного маршрутизатора таковы, что ему можно поручить и решение задачи сортировки пакетов. Маршрутизаторы работают на сетевом уровне модели

OSI и поэтому должны иметь высокопроизводительную ОС, а она вполне может одновременно выполнять указанную дополнительную задачу. Следовательно, брандмауэр от Bay Networks, с одной стороны, представляется чисто программным средством, но, с другой стороны, он не использует никакого компьютера общего назначения (рабочую станцию), устанавливается в стойке и всем остальным похож на другие брандмауэры (кроме заботы о безопасности он выполняет еще и другие функции). Этот маршрутизатор-брандмауэр является специализированным компьютером, но его специализация оказалась гораздо шире, чем было изначально задумано.

Как правило, брандмауэры обеспечивают многоуровневую защиту и используют механизмы предупреждения, сообщают сетевым менеджерам о случаях попытки несанкционированного доступа к сети. Необходимо также подчеркнуть, что некоторые брандмауэры поддерживают частные виртуальные сети (например, между головным и дочерним офисами через общедоступную сеть).

Для защиты сетей разработано большое количество разнообразных довольно сложных и дорогих продуктов, реализующих множество механизмов защиты. Естественно, мы не сможем (и такая цель и не ставилась) их рассмотреть. Но коротко рассмотрим еще одно, широко применяемое сейчас средство.

Прокси- (Proxy) серверы

Очевидно, что самой защищенной является сеть, которая вообще не подключена к Internet. Тогда пользователи такой сети не смогут работать в Internet, что само по себя является существенным недостатком. Выходом из этого положения, видимо, может быть претворение в жизнь следующей идеи: к Internet подключить не всю сеть, а всего один ее компьютер, снабдить этот компьютер защитными средствами и только его использовать для работы с глобальной сетью. Но при этом возникают другие проблемы (большие очереди, замедление работы и пр.). Другим выходом из создавшейся ситуации является наличие на данном компьютере специальной программы, которая позволяла бы остальным компьютерам эмулировать выход в Internet, оставаясь при этом «невидимыми» со стороны глобальной сети. Такой компьютер и называется прокси-сервером (proxy — доверенный).

В качестве примера вкратце рассмотрим Microsoft Proxy Server 2.0. Этот продукт, являясь кэширующим сервером (повышает эффективность работы сети — сокращается сетевой трафик), выполняет функции брандмауэра и обеспечивает безопасный доступ в Internet. Серверный компьютер имеет два сетевых адаптера — один соединяет компьютер с сетью, а другой — с Internet.

Основной функцией IP-протокола (IP — Internet Protocol) является передача пакетов между сетями. IP-адрес характеризует одно соединение и является основным типом адресов, на основании которых сетевой уровень передает пакеты между сетями (адрес состоит из четырех байт и разбивается на две части: номер сети и номер узла). Символьные имена в IP-сетях называются доменными и строятся по иерархическому принципу (доменные имена также называют DNS-именами). На сетевом уровне не устанавливаются соединения и поэтому нет никаких гарантий, что все пакеты будут доставлены в место назначения целыми, невредимыми и в исходном порядке. Эти задачи (надежная информационная связь между двумя конечными узлами) решает транспортный уровень стека TCP/IP, где функционирует протокол управления передачей TCP (Transmission Control Protocol) и протокол дейтаграмм пользователя UDP (User Datagramm Protocol). TCP обеспечивает надежную передачу сообщений между удаленными прикладными процессами за счет образования логических соединений.

Так как локальная сеть «не видна» из Internet, то легальный IP-адрес должен иметь только внешний сетевой интерфейс. IP-адреса внутри сети можно выдавать из пула, зарезервированного для изолированных сетей. Шлюз по умолчанию должен быть указан только для внешнего сетевого интерфейса. Надо установить Microsoft IIP 2.0 и сервис WWW, если нет других намерений по использованию данного компьютера (так как WWW использует Web Proxy для аутентификации пользователей). Для Web Proxy при количестве клиентов до 300 рекомендуется не менее 32 Мбайт оперативной памяти. Кроме того, для кэширования запросов необходимо выделить оперативной памяти 100 Мбайт постоянно и 0,5 Мбайт для каждого клиента. Дополнительно для Web Proxy требуется 10 Мбайт свободного дискового пространства. Если клиентов более 2000, рекомендуется использовать массив прокси-серверов. Естественно, имеются средства для регулирования доступа пользователей к Internet и возможность записи

протокола использования сервисов (для учета действий пользователей в Internet). Необходимо сформировать таблицу локальных адресов в соответствии с конфигурацией сети.

Примеры систем активного аудита

Рассмотрим системы активного аудита, наиболее интересные с точки зрения архитектуры или реализованных в них идей.

Система EMERALD является старейшей разработкой в области активного аудита, так как она вобрала в себя опыт более ранних систем — IDES и NIDES, созданных в Лаборатории информатики Стэнфордского исследовательского института (Stanford Research Institute, известен как SRI International) по контракту с DARPA.

EMERALD расшифровывается как Event Monitoring Enabling Responses to Anomalous Live Disturbances — мониторинг событий, допускающий реакцию на аномалии и нарушения. EMERALD включает в себя все компоненты и архитектурные решения, необходимые для систем активного аудита, оказываясь тем самым не только старейшей, но и самой полной разработкой как среди исследовательских, так и среди коммерческих систем.

Строго говоря, EMERALD является не готовым продуктом, а программной средой, которая строится по модульному принципу. Основным «кирпичиком» служит монитор (рис. 6.3). Каждый монитор включает в себя компонент распознавания сигнатур злоумышленных действий, компонент выявления аномальной активности, решатель, выбирающий способ реагирования на нарушения, а также описание контролируемого объекта. Каждый монитор настраивается по описанию и следит за своим объектом. Мониторы распределяются по информационной системе, образуя иерархию. Отметим, что контролируемые объекты могут иметь как системную, так и сетевую природу. Таким образом, совокупность мониторов может покрыть всю информационную систему. Отметим также, что в иерархию могут включаться не только свои, но и чужие компоненты, разработанные другими производителями.

В общем случае мониторы системы EMERALD развертываются динамически, после этого в реальном времени контролируют поведение инфраструктурных и/или прикладных сервисов. Данные для анализа могут собираться как «пассивным» чтением

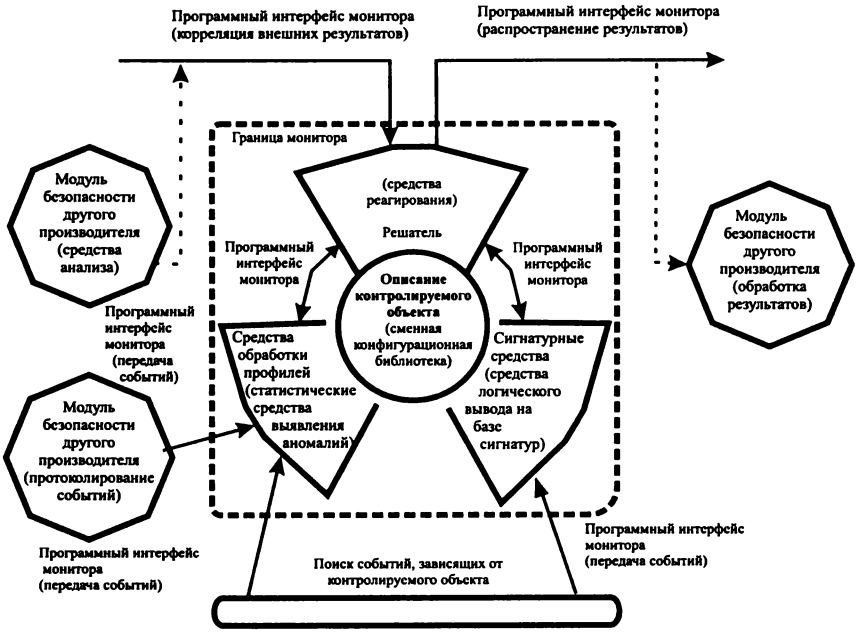


Рис. 6.3. Модуль системы EMERALD и его возможные связи

регистрационных журналов или сетевых пакетов, так и с помощью активных проб. Результаты анализа могут направляться в асинхронном режиме другим мониторам.

Для распознавания сигнатур злоумышленных действий используется экспертная система P-BEST, а выявление аномальной активности основано на применении четырех классов величин (категориальных, непрерывных, показателей интенсивности, распределениях). Статистическому анализу подвергается поведение не пользователей, а сервисов. Профили сервисов существенно меньше и они гораздо стабильнее, чем у пользователей.

В основе своей монитор не зависит от отслеживаемого объекта. Все специфическое вынесено в описание объекта, служащее для настройки подключаемых библиотек. Настраиваются такие методы, как сбор регистрационной информации, реагирование, а также аналитические параметры анализа, список соседей, с которыми нужно обмениваться сигналами тревоги, и т. п.

EMERALD не навязывает определенной архитектуры. Можно выстроить совокупность слабосвязанных мониторов с «легко-

весным» локальным анализом или же жесткую иерархию с мощным централизованным анализом. Можно делать акцент на сетевых или системных сенсорах.

В среде EMERALD изначально существуют описания для элементов инфраструктуры (маршрутизаторы, межсетевые экраны) и прикладных сервисов (FTP, SMTP, HTTP и т. д.). Это означает, что, наряду с гибкостью и расширяемостью, EMERALD в достаточной степени удобен для быстрого развертывания в типичной информационной системе.

Одной из важнейших новаций системы EMERALD является статистический анализ сигналов тревоги, поступающих от разных мониторов. Такой анализ проводится по четырем категориям:

- выявление общих характеристик;
- исследование одного события с разных точек зрения;
- выявление связей между сигналами тревоги;
- выявление тренда (детерминированной составляющей).

EMERALD годится не только для активного аудита, но и для решения других задач информационной безопасности и управления (например, поддержания высокой доступности или анализа поведения сети). Иерархическая организация мониторов и корреляционный анализ помогают выявлять скоординированные, распределенные атаки.

Система NFR (Network Flight Recorder) относится к числу сетевых систем, существующих в виде свободно распространяемого инструментария и коммерчески «упакованного» продукта NFR Intrusion Detection Appliance. С внешней точки зрения NFR представляет собой либо одну станцию, осуществляющую мониторинг сегмента сети, к которому она подключена, либо совокупность таких станций с центральной управляющей консолью.

Строго говоря, NFR — это нечто большее, чем система выявления подозрительной сетевой активности. Правильнее рассматривать ее как компонент сетевого управления, одним из аспектов которого является борьба с нарушениями политики безопасности (равно как и со сбоями и отказами оборудования и программного обеспечения).

Основные компоненты внутренней архитектуры NFR показаны на рис. 6.4. Один или несколько сетевых сенсоров (packet suckers в терминологии NFR) поставляют данные решателю, который эти данные фильтрует, реассемблирует потоки, при обнаружении нарушений реагирует на них, а также передает инфор-

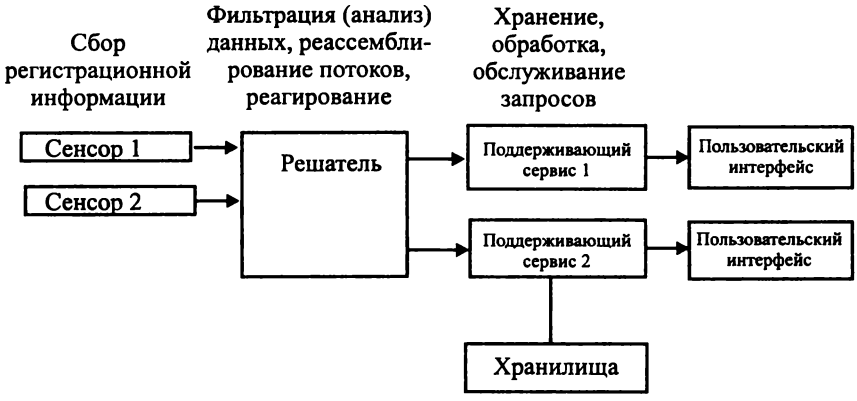


Рис. 6.4. Основные элементы архитектуры NFR

мацию поддерживающему сервису для сохранения с последующей статистической обработкой и обслуживанием запросов. Поддерживающий сервис может также просматривать переданную ему информацию на предмет выявления сигнатур злоумышленных действий.

Для всех стыков определены программные интерфейсы, так что возможна, например, смена или добавление сенсора или поддерживающего сервиса. Разделение поддерживающего сервиса от сбора и первичного анализа регистрационной информации позволяет распределять нагрузку, чтобы сложная обработка не тормозила процессы, от которых требуется работа в реальном масштабе времени.

Ядром NFR является решатель, а основой решателя — язык описания фильтров, который называется N. Это универсальный язык программирования, содержащий переменные с областями видимости, списочные типы данных, управляющие структуры, процедуры. Кроме того, в N есть специфические типы данных, такие, как IP-адрес. Под значения разного рода счетчиков отводится по 64 разряда, что освобождает от проблем переполнения даже в больших сетях.

N — интерпретируемый язык. Программы, написанные на N, переводятся в коды для простой стековой машины. Такие программы (и, следовательно, фильтры) оказываются весьма компактными. Что касается скорости интерпретации, то при достаточно высоком уровне базовых операций она оказывается не намного ниже, чем при выполнении скомпилированной программы.

Кроме того, применяемый при интерпретации N-программ механизм ленивых вычислений позволяет избежать лишних операций, обычно сопутствующих проверке сложных условий.

В N заложены знания о структуре сетевых пакетов и протоколах более высоких уровней. Например, допустимы обращения вида ip.src, tcp.hdr или syslog.message. Возможно и обращение к произвольным частям пакетов. В принципе, на N можно написать интерпретатор любого прикладного протокола.

Приведем пример простого фильтра, выбирающего запрашиваемые клиентом по протоколу HTTP локаторы ресурсов

```
filter server tcp (client, port: 80, start: "GET",
stop: " ") {
record ip.src, ip.dst, tcp.sport, tcp.dport,
tcp.bytes to urlRecorder;
}
```

Этот фильтр анализирует TCP-соединения с серверным портом 80, ищет в потоке данных цепочку символов «GET», записывает все от места совпадения до пробела в поле tcp.bytes (предполагается, что это и будет URL), после этого отправляет поддерживающему сервису исходные и целевые IP-адреса и номера TCP-портов, а также выявленный URL.

В данном случае разыскиваемый шаблон весьма прост. Подчеркнем, что язык N позволяет сделать его сколь угодно сложным.

Программы на N, поддерживающий сервис, интерпретатор могут генерировать сигналы тревоги, для обработки которых существует специальная программа, работающая в фоновом режиме. Эта программа на основе ассоциированной информации определяет дальнейший маршрут и приоритет сигналов тревоги.

NFR не является универсальной системой активного аудита, но представляет несомненный интерес, прежде всего, как хорошо выполненный строительный блок, который можно установить в управляющую среду, объединить со средствами выявления подозрительной активности на хостах и т. п. Язык N обладает достаточной мощностью и для записи сигнатур атак с учетом возможных вариаций, и для выражения сетевых аспектов политики безопасности организации. В качестве рекомендуемой конфигурации для NFR Intrusion Detection Appliance выбран компьютер с процессором Intel Pentium II 400 МГц и ОЗУ 256 Мб.

Контрольные вопросы

1. Дайте определение вычислительных сетей и приведите их классификацию.
2. Дайте краткую характеристику основным топологическим разновидностям сетей.
3. Приведите и охарактеризуйте основные положения концепции построения сетевых протоколов.
4. Приведите сравнительные характеристики наиболее распространенных локальных вычислительных сетей.
5. Назовите и охарактеризуйте основные сетевые ОС.
6. Дайте краткую характеристику принципам и методам организации межсетевого взаимодействия.
7. Дайте краткую характеристику прикладному программному обеспечению локальных сетей.
8. Сформулируйте цели защиты информации в сетях ЭВМ и назовите основные угрозы информации в сетях.
9. Приведите перечень основных механизмов защиты информации в сетях и дайте им краткую характеристику.
10. Приведите и охарактеризуйте основные положения концепции защиты информации в эталонной модели взаимодействия открытых сетей.
11. Приведите структуру и содержание процедуры взаимной аутентификации пользователей сети.
12. Раскройте сущность метода распределения ключей при использовании:
    — традиционных систем шифрования;
    — систем шифрования с открытым ключом;
    — методов цифровой подписи данных, передаваемых в сетях.
13. Приведите краткое описание системы защиты локальной вычислительной сети «Secret NET».
14. Дайте характеристики системам активного аудита.

Глава 7
ТЕХНИЧЕСКИЕ СРЕДСТВА И КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

7.1. Технические средства защиты

Техническими являются такие средства защиты (ТСЗ), в которых основная защитная функция реализуется некоторым техническим устройством (комплексом, системой). К достоинствам технических средств относятся: широкий круг решаемых задач; высокая надежность; возможность создания развитых комплексных систем защиты; гибкое реагирование на попытки несанкционированных действий; традиционность используемых методов осуществления защитных функций [4].

Основные недостатки: высокая стоимость многих средств; необходимость регулярного проведения регламентных работ и контроля; возможность подачи ложных тревог.

Классы ТСЗ

Классификация технических средств производится по следующим критериям:

- сопряженность с основными средствами АСОД;
- выполняемая функция защиты;
- степень сложности устройства.

Сопряженность с основными средствами АСОД:

- *автономные* — средства, выполняющие свои защитные функции независимо от функционирования средств АСОД, т. е. полностью автономно;

- *сопряженные* — средства, выполненные в виде самостоятельных устройств, но осуществляющие защитные функции в сопряжении (совместно) с основными средствами;
- *встроенные* — средства, которые конструктивно включены в состав аппаратуры технических средств АСОД.

Выполняемая функция защиты:

- *внешняя защита* — защита от воздействия дестабилизирующих факторов, проявляющихся за пределами основных средств АСОД;
- *опознавание* — специфическая группа средств, предназначенных для опознавания людей по различным индивидуальным характеристикам;
- *внутренняя защита* — защита от воздействия дестабилизирующих факторов, проявляющихся непосредственно в средствах обработки информации.

Степень сложности устройства:

- *простые устройства* — несложные приборы и приспособления, выполняющие отдельные процедуры защиты;
- *сложные устройства* — комбинированные агрегаты, состоящие из некоторого количества простых устройств, способные к осуществлению сложных процедур защиты;
- *системы* — законченные технические комплексы, способные осуществлять некоторую комбинированную процедуру защиты, имеющую самостоятельное значение.

В приведенной классификационной системе определяющей является классификация по критерию выполняемой функции; классификация по критериям сопряженности и степени сложности отражает, главным образом, особенности конструктивной и организационной реализации средств. Поскольку для наших целей наиболее важной является функциональная классификация, то под данным углом зрения и рассмотрим технические средства защиты. К настоящему времени разработано большое количество различных технических средств защиты, причем налажено промышленное производство многих из них.

Типы систем защиты

Современный комплекс защиты территории охраняемых объектов может включать в себя следующие основные компоненты:

- механическую систему защиты;
- систему оповещения о попытках вторжения;

- оптическую (обычно телевизионную) систему опознавания нарушителей;
- оборонительную систему (звуковую и световую сигнализацию, применение в случае необходимости оружия);
- связную инфраструктуру;
- центральный пост охраны, осуществляющий сбор, анализ, регистрацию и отображение поступающих данных, а также управление периферийными устройствами;
- персонал охраны (патрули, дежурные на центральном посту).

Механические системы защиты. Основой любой механической системы защиты являются механические или строительные элементы, создающие для лица, пытающегося проникнуть на охраняемую территорию, реальное физическое препятствие. Важнейшей характеристикой механической системы защиты является *время сопротивления*, т. е. время, которое требуется злоумышленнику для ее преодоления. Исходя из требуемой величины названной характеристики, должен производиться и выбор типа механической системы защиты.

Как правило, механическими или строительными элементами служат стены и ограды. Если позволяют условия, могут применяться рвы и ограждения из колючей проволоки.

Вышеназванные элементы могут сочетаться в различных комбинациях в одной системе механической защиты. В настоящее время на важных охраняемых объектах используются системы механической защиты с тройной изгородью, со специальными элементами, затрудняющими попытки перебраться через ограждения, и с применением S-образных мотков колючей проволоки.

При использовании многорядных механических систем защиты датчики оповещения о попытке вторжения целесообразно располагать между внутренним и внешним ограждением. При этом внутреннее ограждение должно обладать повышенным временем сопротивления.

Системы оповещения. В современных системах оповещения (системах тревожной сигнализации) о попытках вторжения на охраняемую территорию находят применение датчики нескольких типов.

Поскольку основные характеристики подобных систем определяются, главным образом, характеристиками используемых датчиков, рассмотрим принципы действия и особенности применения последних более подробно.

В системах защиты периметра территории без ограды используются микроволновые, инфракрасные, емкостные, электрические и магнитные датчики.

С помощью датчиков первых двух типов формируется протяженная контрольная зона барьерного типа. Действие систем с *микроволновыми* датчиками основывается на контроле интенсивности высокочастотного направленного излучения передатчика, которое воспринимается приемником. Срабатывание сигнализации происходит при прерывании этого направленного излучения. Ложные срабатывания могут быть обусловлены перемещением в контролируемой зоне животных, воздействием растительности, атмосферных осадков, передвижением транспортных средств, а также воздействием посторонних передатчиков.

При использовании *инфракрасных* систем оповещения между передатчиком и приемником появляется монохроматическое световое излучение в невидимой области спектра. Срабатывание сигнализации происходит при прерывании одного или нескольких световых лучей. Ложные срабатывания могут быть обусловлены перемещением в контролируемой зоне животных, сильным туманом или снегопадом.

Принцип действия *емкостной* системы оповещения основывается на формировании электростатического поля между параллельно расположенными, так называемыми передающими и воспринимающими проволочными элементами специального ограждения. Срабатывание сигнализации происходит при регистрации определенного изменения электростатического поля, имеющего место при приближении человека к элементам ограждения. Ложные срабатывания могут быть обусловлены перемещением животных, воздействием растительности, обледенением элементов ограждения, атмосферными воздействиями или загрязнением изоляторов.

Электрические системы оповещения базируются на использовании специального ограждения с токопроводящими проволочными элементами. Критерием срабатывания сигнализации является регистрация изменений электрического сопротивления токопроводящих элементов при прикосновении к ним. Ложные срабатывания могут быть вызваны животными, растительностью или загрязнением изоляторов.

Принцип действия систем с *магнитными* датчиками предполагает контроль параметров магнитного поля. Срабатывание сигнализации происходит при регистрации искажений, которые обусловлены появлением в зоне действия датчиков предметов из

ферромагнитного материала. Ложное срабатывание может иметь место из-за изменений характеристик почвы, обусловленных, например, продолжительным дождем.

При наличии механической системы защиты территории (например, ограды, расположенной по периметру) находят применение системы оповещения с вибрационными датчиками, датчиками звука, распространяющегося по твердым телам, акустическими датчиками, электрическими переключателями, а также системы с электрическими проволочными петлями.

Вибрационные датчики закрепляются непосредственно на элементах ограды. Срабатывание сигнализации происходит при появлении на выходе датчиков сигналов, которые обусловлены вибрациями элементов ограды. Ложные срабатывания могут быть обусловлены сильным ветром, дождем или градом.

Датчики звука также устанавливаются непосредственно на элементы ограды и контролируют распространение по ним звуковых колебаний. Срабатывание сигнализации происходит при регистрации так называемых шумов прикосновения к элементам ограды. Ложные срабатывания могут быть обусловлены сильным ветром, дождем, градом или срывающимися с элементов ограды сосульками.

В системах оповещения с *акустическими* датчиками контролируются звуковые колебания, передаваемые через воздушную среду. Срабатывание сигнализации происходит при регистрации акустических сигналов, имеющих место при попытках перерезать проволочные элементы ограды. Ложные срабатывания могут быть обусловлены сильным ветром, дождем, градом, а также различными посторонними шумами.

Действие систем с *электрическими* переключателями основано на регистрации изменения состояния переключателей, вмонтированных в ограду, которое происходит при соответствующем изменении натяжения проволочных элементов или нагрузки на направляющие трубки ограды. Ложные срабатывания сигнализации могут быть вызваны очень сильным ветром при недостаточном натяжении элементов ограды.

Если в системах оповещения в качестве чувствительных элементов применяются изолированные *токопроводящие* проволочные элементы, срабатывание сигнализации происходит при перерезании или деформации этих элементов. Ложные срабатывания могут произойти при возникновении неисправности в сети электропитания.

Для контроля участков почвы по периметру охраняемой территории находят применение системы оповещения с датчиками звука, распространяющегося по твердым телам, а также с датчиками давления.

В системах *первого* типа регистрируются звуковые, сейсмические колебания. Срабатывание сигнализации происходит при регистрации сотрясений почвы, например ударного шума. Ложные срабатывания могут быть обусловлены перемещением достаточно крупных животных, движением транспорта вблизи охраняемой территории.

В системах *второго* типа используются пневматические или емкостные датчики давления, позволяющие регистрировать изменения нагрузки на почву. Срабатывание сигнализации происходит при регистрации соответствующего роста давления, например ударного. Ложные срабатывания возможны из-за перемещений достаточно крупных животных, разгерметизации пневматических датчиков или коррозии.

Для контроля участков охраняемой территории фирмой Multisafe AG разработана система оповещения Multiplain, датчики которой работают на принципе регистрации разности давления. Датчик состоит из двух полых тел с избыточным давлением, которые соединены между собой через специальный преобразователь разности давлений. При возникновении даже незначительной разницы давлений в этих телах в преобразователе срабатывает контакт, через который может коммутироваться цепь включения тревожной сигнализации. При использовании указанного датчика достаточно просто локализовать участок, на котором сработал чувствительный элемент. Кроме того, преобразователь оснащен устройством автоматического восстановления нулевой точки, что исключает срабатывание контакта при медленных изменениях давления, которые могут быть обусловлены различными возмущающими воздействиями, например колебаниями температуры. Датчик также нечувствителен к колебаниям и вибрациям, обусловленным движением автомобильного или железнодорожного транспорта. Чувствительная часть рассматриваемого устройства конструктивно выполнена в виде набора специальных ковриков, которые могут устанавливаться под слоем гравия, дерна, земли или под плитами пешеходных дорожек. Срабатывание контактов в преобразователях происходит при изменении нагрузки не менее чем на 30 кг. Таким образом, система оповещения не реагирует на перемещение мелких животных

по контролируемому участку территории. Предварительная нагрузка за счет маскировочного покрытия ковриков может достигать 250 кг/м^2 без влияния на их чувствительность.

Приведенное описание характеристик различных датчиков позволяет сделать вывод об отсутствии идеальной системы оповещения. Основное техническое требование к подобной системе может быть сформулировано следующим образом: максимально возможная вероятность обнаружения нарушителей и надежность в сочетании с минимальной частотой ложных срабатываний.

Повышение вероятности обнаружения нарушителя системой оповещения обязательно сопровождается увеличением числа ложных срабатываний. Таким образом, разработка систем оповещения связана, прежде всего, с поиском рационального компромисса относительно соотношения величин названных показателей. Из этого следует, что дальнейшее совершенствование систем оповещения должно быть направлено на повышение вероятности обнаружения и снижение интенсивности ложных срабатываний путем использования нескольких систем оповещения различного принципа действия в едином комплексе и применения в этих системах микропроцессорных анализаторов.

Системы опознавания

Обязательным условием надежного функционирования всего комплекса защиты охраняемой территории является последующий анализ поступающих сообщений о проникновении для точного определения их вида и причин появления. Названное условие может быть выполнено посредством использования систем опознавания. Наиболее широкое распространение в подобных системах получили телевизионные установки дистанционного наблюдения. Несомненно, что объект со стационарными постами охраны обладает более высокой защищенностью, однако при этом значительно возрастают затраты на его охрану. Так, при необходимости круглосуточного наблюдения требуется трехсменная работа персонала охраны. В этих условиях телевизионная техника становится средством повышения эффективности работы персонала охраны, прежде всего, при организации наблюдения в удаленных, опасных или труднодоступных зонах.

Вся контролируемая системой оповещения зона разграничивается на отдельные участки протяженностью не более 100 м, на

которых устанавливается по крайней мере одна передающая телекамера. При срабатывании датчиков системы оповещения, установленных на определенном участке контролируемой зоны, изображение, передаваемое соответствующей телекамерой, автоматически выводится на экран монитора на центральном посту охраны. Кроме того, при необходимости должно быть обеспечено дополнительное освещение данного участка. Немаловажно, чтобы внимание дежурного охранника было быстрее привлечено к выведенному на экран монитора изображению.

Фактические причины срабатывания сигнализации во многих случаях могут быть идентифицированы только при условии достаточно высокой оперативности дежурного охранника. Важно, что данное положение прежде всего имеет место при действительных попытках вторжения на охраняемую территорию и при преднамеренных обманных действиях злоумышленников. Одним из перспективных путей выполнения сформулированного выше условия является применение устройства видеопамяти, которое обеспечивает автоматическую запись изображения сразу же после срабатывания сигнализации. При этом дежурному охраннику предоставляется возможность вывести из устройства памяти на экран монитора первые кадры изображения и идентифицировать причину срабатывания датчиков системы оповещения.

В ряде телесистем наблюдения применены передающие камеры, ориентация которых может дистанционно меняться дежурным охранником. При включении сигнализации тревоги служащий охраны должен ориентировать телекамеру на участок, где сработали датчики системы оповещения. Однако практический опыт показывает, что такие телеустановки менее эффективны по сравнению с жестко ориентированными передающими телекамерами.

Отличительной особенностью некоторых объектов является их большая протяженность.

Большое количество площадок таких объектов может быть расположено на значительном удалении друг от друга, что серьезно удорожает монтаж и эксплуатацию оборудования. В этих случаях можно применить систему малокадрового телевидения типа Slowscan. Она функционирует на больших дальностях, имеет невысокую стоимость и совместима с любой существующей замкнутой телевизионной системой, которая уже установлена на объекте. Для передачи видеокадров и команд в этой системе используется телефонная сеть общего пользования. Особые пре-

имущества в системах охраны имеют камеры на приборах с зарядовой связью (ПЗС). По сравнению с обычными камерами на ЭЛТ они обладают меньшими габаритами, более высокой надежностью, практически не нуждаются в техническом обслуживании, отлично работают в условиях низкой освещенности, обладают чувствительностью в инфракрасной области спектра. Однако наиболее важным является то, что видеоинформация на чувствительном элементе указанной камеры сразу представлена в цифровой форме и без дополнительных преобразований пригодна для дальнейшей обработки. Это дает возможность легко идентифицировать различия или изменения элементов изображения, реализовать в камере встроенный датчик перемещений. Подобная камера со встроенным детектором и маломощным ИК-осветителем может вести наблюдение охраняемой территории и при появлении нарушителя в поле зрения распознавать изменения элементов изображения, а также подавать сигнал тревоги.

Несомненно, что в будущем появятся более миниатюрные и эффективные телекамеры, а по мере снижения стоимости расширится использование камер на ПЗС и формирователях видеосигналов. Прогресс в области видеосредств обнаружения перемещений, разрабатываемых в основном для военных целей, неизбежно приведет к появлению и на коммерческом рынке интеллектуальных камер, способных решать простые задачи распознавания.

По мере роста преступности все большее число предпринимателей начинают осознавать преимущества использования видеотехники в целях защиты собственности. Телевизионные системы могут применяться не только для внешней защиты объектов, но и для контроля действия персонала внутри объектов. Хорошим примером тому служит внедрение замкнутых телевизионных систем на автозаправочных станциях Великобритании. Такие системы позволяют идентифицировать нарушителей, получать вещественные доказательства вины мошенников, являются средством сдерживания потенциальных расхитителей.

Оборонительные системы

Для предотвращения вторжения на охраняемую территорию используется оборонительная система, в которой находят применение осветительные или звуковые установки. В обоих случаях субъект, пытающийся проникнуть на охраняемую территорию,

информируется о том, что он обнаружен охраной. Таким образом, на него оказывается целенаправленное психологическое воздействие. Кроме того, использование осветительных установок обеспечивает благоприятные условия для действий охраны.

Для задержания преступника охрана предпринимает соответствующие оперативные меры или вызывает милицию (полицию). Если злоумышленнику удалось скрыться, то для успеха последующего расследования важное значение приобретает информация, которая может быть получена с помощью рассмотренной выше системы опознавания.

В особых случаях функции оборонительной системы выполняет специальное ограждение, через которое пропущен ток высокого напряжения.

Охранное освещение

Обязательной составной частью комплексной системы защиты любого вида объектов является охранное освещение. Различают два вида охранного освещения — дежурное (или постоянное) и тревожное.

Дежурное освещение предназначается для постоянного, непрерывного использования во внерабочие часы, в вечернее и ночное время как на территории объекта, так и внутри зданий. Дежурное освещение оборудуется с расчетом его равномерности по всему пространству охраняемых зон объекта.

Для дежурного охранного освещения используются обычные уличные (вне здания) и потолочные (внутри здания) светильники. На посту охраны объекта должен находиться силовой рубильник включения внешнего дежурного освещения или устройство автоматического включения внешнего освещения с наступлением темного времени суток.

Тревожное освещение включается сотрудниками охраны вручную или автоматически при поступлении сигнала тревоги от системы сигнализации. Если тревожное освещение располагается по периметру территории, то по сигналу тревоги могут включаться светильники либо только в том месте, откуда поступил сигнал тревоги, либо по всему периметру территории.

Для тревожного освещения обычно используют прожектор большой мощности или несколько прожекторов средней мощности до 1000 Вт.

Так же, как и сигнализация, дежурное освещение должно иметь резервное электропитание на случай аварии или выключения электросети. Наиболее распространенный способ резервирования дежурного освещения — установка светильников, имеющих собственные аккумуляторы. Такие светильники постоянно подключены к электросети (для подзарядки аккумуляторов), а в случае ее аварии автоматически включаются от собственного аккумулятора.

Средства контроля доступа

При выборе системы контроля доступа рекомендуется проделать следующие действия:

- определить количество необходимых контрольно-пропускных пунктов, исходя из числа пропускаемых через них служащих, которых требуется проконтролировать с максимальной скоростью во время пиковой нагрузки;
- оценить требуемую степень безопасности организации. Ее можно повысить, к примеру, путем дополнения устройства считывания карточек средствами ввода персонального кода;
- предусмотреть средства аварийного выхода;
- оценить ассигнования, необходимые на приобретение, установку и эксплуатацию системы контроля доступа.

При выборе варианта системы, наряду с оценкой требуемого уровня безопасности и стоимости в сопоставлении с решаемыми задачами по контролю доступа, важно убедиться в том, что система достаточно проста в эксплуатации, обладает нужной гибкостью при изменении предъявляемых к ней требований, что ее можно наращивать, не теряя сделанных инвестиций. При выборе системы желательно заглянуть минимум на два года вперед.

Руководству организации рекомендуется останавливать свой выбор на той системе, принцип действия которой ему понятен. Следует учитывать также уровень технического обслуживания, репутацию изготовителя и поставщика оборудования.

Замки. Различаются механические и электрические замки. Механический замок — оптимальное средство контроля доступа в здание (помещение), занимаемое небольшой организацией или посещаемое малым количеством людей. Он удобен, экономичен и обеспечивает необходимый уровень защиты.

При выборе требуемой модели замка, как, впрочем, и любого другого способа контроля доступа, следует прежде всего учитывать условия эксплуатации и необходимый уровень защиты. Существует множество замков повышенной секретности, висячих замков, которые могут устанавливаться в местах, требующих дополнительной защиты — на воротах, складах, аппаратных и т. д. Промышленные предприятия рассматривают механические замки повышенной секретности в качестве гибкого, эффективного и недорогого средства обеспечения потребностей в защите собственности.

Залогом правильной эксплуатации замковых устройств является управление ключами к ним, которое представляет собой наиболее важный аспект безопасности. Без эффективного управления ключами даже самый надежный замок теряет способность обеспечивать защиту. Вместе с тем отслеживать круг лиц, имеющих доступ в определенные помещения, и сохранять информацию о том, какие и у каких сотрудников находятся ключи, можно столь же легко, как и вести обычную картотеку. Существуют программы для персональных компьютеров, которые позволяют поддерживать информацию о наличии ключей у служащих. Правда, соответствие этой информации реальности следует периодически контролировать.

Управление задвижкой электрического замка осуществляется вручную путем нажатия кнопок либо автоматически. Для отпирания двери с кнопочными замками (клавиатурой) требуется набрать правильный буквенно-цифровой код. Клавиатуру совместно с электрозамком обычно называют бесключевым средством контроля доступа. Недостатком кнопочных систем является возможность выявления кода путем подсматривания процесса его набора, анализа потертостей и загрязнений на кнопках и т. д.

В системах повышенной защищенности клавиатура может быть дополнена системой считывания карточек. Недостатком систем контроля доступа по карточкам является возможность утери последних, их хищения, передачи другому лицу. Альтернативой системам контроля доступа по карточкам являются системы с так называемыми электронными ключами. Системы этого типа установлены в сотнях конторских зданий и гостиниц по всему миру. Они работают по принципу восприятия кода посредством оптического инфракрасного устройства. Записанный в ключе код представляет собой последовательность отверстий, выбитых на металле. Главные достоинства электронных клю-

чей — невысокая стоимость, долговечность, удобство и простота эксплуатации.

Автоматизированные системы контроля доступа. Работа современных автоматизированных систем контроля доступа (АСКД) основана на анализе идентификационных документов [9].

В последнее время в особо чувствительных АСОД (например, банковских) стали применяться системы электронных платежей на основе *пластиковых идентификационных карточек* (ПИК), которые известны также под названиями *кредитные карточки, смарт-карты или «пластиковые деньги»* и т. п. ПИК предназначены для осуществления взаимодействия человека с АСОД, поэтому могут быть определены как аппаратное средство АСОД, выполненные в виде прямоугольной пластиковой карточки, предназначенное для идентификации субъекта системы и являющееся носителем идентифицирующей и другой информации.

Типичный идентификационный документ имеет многослойную структуру и размеры, аналогичные стандартному формату кредитных карточек. Носитель идентификационной информации расположен между двумя защитными пленками из пластика.

В современных АСКД достаточно широко применяются магнитные карточки, носителем идентификационной информации в которых является полоска намагниченного материала. Следует отметить, однако, что такие документы не обладают высокой степенью защищенности в отношении попыток их подделки.

Применение голографического способа кодирования позволяет достичь повышенного уровня защищенности идентификационных документов от подделки или фальсификации. Пропуска этого вида содержат голограммы, которые представляют собой запись эффекта интерференции между двумя или более когерентными полями.

Трехмерные голограммы позволяют записывать с высокой плотностью информацию, содержащуюся в изображении. На 1 мм^2 голограммы может быть записано до миллиона бит информации.

Практическая идентификация пользователей заключается в установлении и закреплении за каждым пользователем АСОД уникального идентификатора (признака) в виде номера, шифра, кода и т. д. Это связано с тем, что традиционный идентификатор вида *фамилия-имя-отчество* не всегда приемлем, уже хотя бы в силу возможных повторений и общеизвестности. Поэтому в раз-

личных автоматизированных системах широко применяется персональный идентификационный номер (ПИН/PIN).

ПИН обычно состоит из 4—12 цифр и вводится идентифицируемым пользователем с клавиатуры. На практике встречаются назначаемые или выбираемые ПИН. Последний устанавливается пользователем самостоятельно. Назначаемый ПИН устанавливается уполномоченным органом АСОД.

На практике существуют два основных способа проверки ПИН: алгоритмический и неалгоритмический. Алгоритмический способ проверки заключается в том, что у пользователя запрашивается ПИН, который преобразуется по определенному алгоритму с использованием секретного ключа и затем сравнивается со значением ПИН, хранящимся на карточке с соблюдением необходимых мер защиты. Главным достоинством этого метода проверки является отсутствие необходимости интерактивного обмена информацией в системе. При неалгоритмическом способе проверка ПИН осуществляется путем прямого сравнения ПИН на карте со значением, хранимым в базе данных. Это обязывает использовать средства связи, работающие в реальном масштабе времени, и предусматривать средства защиты информации в базе данных и линиях телекоммуникаций. Идентификатор используется при построении различных подсистем разграничения доступа.

Любая пластиковая идентификационная карточка (ПИК) используется в качестве носителя информации, необходимой для идентификации, и информации, используемой в других целях. Эта информация представляется в различных формах: графической, символьной, алфавитно-цифровой, кодированной, двоичной. Множество форм представления информации на ПИК объясняется тем, что карточка служит своеобразным связующим звеном между человеком (пользователем) и машинной системой, для которых характерны различные формы представления информации.

Например, на карточку графически наносят специальный логотип, рисунок, фотографию, фамилию владельца, серийный номер, срок годности, штрих-код и т. п.

Логотип — графический символ организации, выпускающей карточку. Он служит своеобразным знаком обслуживания, т. е. обозначением, дающим возможность отличать услуги одной организации от однородных услуг другой организации. Очевидно, что логотип должен обладать различительной способностью и не повторять общеупотребительные обозначения (гербы, флаги и

т. п.). Для обеспечения безопасности изображение, в том числе голографическое или видимое только в инфракрасных лучах, наносят на специальном оборудовании, что существенно затрудняет подделку карточки.

Другим средством повышения безопасности визуальной информации служит тиснение или выдавливание (*эмбоссирование*) некоторых идентификационных характеристик пользователя на поверхности идентификационной карточки (ИК).

Эти характеристики с помощью специального устройства (*импринтера*) могут отпечатываться и дублироваться на бумажном носителе (*слипе*) для дальнейшего учета.

В настоящее время нашли широкое применение магнитные, полупроводниковые и оптические карточки, перечисленные в порядке снижения распространенности.

ИК нашли широкое применение в различных АСОД. Самое большое распространение карточек наблюдается в финансовой сфере.

Можно условно выделить три связанные области применения ПИК:

1) электронные документы;

2) контрольно-регистрационные системы;

3) системы электронных платежей.

Карточки как средство контроля, разграничения и регистрации доступа к объектам, устройствам, информационным ресурсам АСОД используются при создании контрольно-регистрационных охранных систем. Например, известны разнообразные электронные замки к помещениям и аппаратуре. Разграничение доступа к данным ПЭВМ реализовано на уровне предъявления *ключ-карты*, содержащей идентификационные данные пользователя и его электронный ключ.

Наиболее прост процесс изготовления так называемых печатных и тисненных голограмм, которые могут наноситься на уже имеющиеся идентификационные документы. Более сложна технология получения рефлексных голограмм, что и определяет обеспечиваемую ими повышенную степень защищенности документов от попыток подделки.

В последние годы заметно выросли масштабы применения в различных системах контроля доступа пропусков со встроенными интегральными схемами (ИС).

Информация, хранящаяся в памяти карточки и/или вводимая пользователем, может обрабатываться встроенным микро-

процессором карточки, устройством считывания или передаваться в центральную ЭВМ.

Использование пропусков с ИС позволяет проводить контроль доступа с высоким уровнем надежности, однако стоимость таких документов существенно выше, чем карточек с магнитной полосой (1—2 доллара и 50—60 центов, соответственно).

Существенным недостатком многих систем контроля доступа рассматриваемого вида является то, что при проходе на объект или выходе с его территории владелец пропуска должен каждый раз вынимать документ из кармана и приближать его к устройству считывания. В последние годы были разработаны более совершенные бесконтактные системы, в которых расстояние между пропуском и устройством считывания составляет 40—100 см. При применении этих систем не приходится останавливаться, доставать пропуск и приближать его к устройству считывания, что обусловливает большие удобства для пользователей и более высокую пропускную способность.

В настоящее время выпускается несколько типов рассматриваемых бесконтактных систем. В некоторых из них, кроме периферийных устройств считывания, используется также и центральный блок, который выполняет основные процедуры по проверке правомочий доступа на охраняемый объект предъявителя пропуска и формирует сигналы управления механизмами блокировки прохода.

Идентификационные документы, используемые в бесконтактных системах контроля доступа, представляют собой пропуска со встроенной ИС. При этом находят применение как пассивные, так и активные носители информации. В первом случае в электронной схеме отсутствует собственный источник питания и ее активизация производится за счет преобразования энергии электромагнитного излучения передатчика устройства считывания. В электронной схеме активного носителя предусмотрен собственный источник электропитания — миниатюрная батарейка, которая может периодически подзаряжаться или заменяться.

Биометрические системы идентификации. В настоящее время в банках и других организациях с повышенными требованиями к безопасности находят все более широкое распространение биометрические системы контроля доступа, что можно объяснить снижением их стоимости. Все биометрические системы характеризуются высоким уровнем безопасности, прежде всего, потому, что используемые в них данные не могут быть утеряны пользова-

телем, похищены или скопированы. В силу своего принципа действия биометрические системы отличаются малым быстродействием и низкой пропускной способностью. Тем не менее они представляют собой единственное решение проблемы контроля доступа на особо важные объекты с малочисленным персоналом.

Биометрические системы идентификации, функционирующие в настоящее время или находящиеся в стадии разработки, включают в себя системы идентификации по отпечатку пальца, запаху, ДНК, форме уха, геометрии лица, температуре кожи лица, клавиатурному почерку, отпечатку ладони, сетчатке глаза, рисунку радужной оболочки глаза, подписи и голосу.

Отпечаток пальца. В последние годы идентификация личности по отпечатку пальца рассматривается как биометрическая технология, которая, вероятно, будет наиболее широко использоваться в будущем. В дополнение к системе общей безопасности и контроля устройства доступа по отпечатку пальцев установлены в военных учреждениях США, включая Пентагон и правительственные лаборатории. Хотя отказ в доступе уполномоченных пользователей составляет около 3 %, процент ошибочного доступа — меньше одной миллионной. Широкое применение данная технология получила в системе автоматической идентификации по отпечатку пальца (AFIS), используемой полицией по всем Соединенным Штатам Америки и в более 30 странах мира. Преимущества доступа по отпечатку пальца — простота использования, удобство и надежность. Весь процесс идентификации занимает мало времени и не требует усилий от персонала, использующего данную систему. Исследования показали, что использование отпечатка пальца для идентификации личности является самым удобным из всех биометрических методов. Вероятность ошибки при идентификации пользователя для него намного меньше в сравнении с другими биометрическими методами. Кроме того, устройство идентификации по отпечатку пальца не требует много места на клавиатуре или в механизме. В настоящее время производятся подобные системы размером меньше колоды карт.

Геометрия руки. Метод идентификации пользователей по геометрии руки используется в более чем в 10 000 организациях, включая Колумбийское законодательное собрание, Международный аэропорт Сан-Франциско, больницы и иммиграционные службы. Преимущества идентификации по геометрии ладони сравнимы с плюсами идентификации по отпечатку пальца

в вопросе надежности, хотя устройство для считывания отпечатков ладоней занимает больше места. Наиболее удачное устройство, HandKey, сканирует как внутреннюю, так и боковую сторону руки, используя для этого встроенную видеокамеру и алгоритмы сжатия. Устройства, которые могут сканировать и другие параметры руки, находятся в процессе разработки несколькими компаниями, такими, как BioMet Partnres, Palmetric и BTG.

Радужная оболочка глаза. Преимущество сканеров для радужной оболочки состоит в том, что образец пятен на радужной оболочке находится на поверхности глаза и видеоизображение может быть получено на расстоянии до одного метра, что делает возможным использование таких сканеров в банкоматах. У людей с ослабленным зрением, но неповрежденной радужной оболочкой также могут сканироваться и кодироваться идентифицирующие параметры. Если есть катаракта — повреждение хрусталика глаза, которое находится позади радужной оболочки, она никаким образом не влияет на процесс сканирования радужной оболочки.

Сетчатка глаза. Сканирование сетчатки происходит с использованием инфракрасного излучения низкой интенсивности, направленного через зрачок к кровеносным сосудам на задней стенке глаза. Сканеры для сетчатки глаза получили большое распространение в сверхсекретных системах контроля доступа, так как у них один из самых низких процентов отказа доступа зарегистрированных пользователей и почти 0 % ошибочного доступа.

Голосовая идентификация. Привлекательность данного метода — удобство в применении. Основным беспокойством, связанным с этим биометрическим подходом, является точность идентификации. Однако это не является серьезной проблемой с того момента, как устройства идентификации личности по голосу различают характеристики человеческой речи. Голос формируется из комбинации физиологических и поведенческих факторов. В настоящее время идентификация по голосу используется для управления доступом в помещения средней степени безопасности, например лаборатории и компьютерные классы. Идентификация по голосу удобный, но в то же время не такой надежный, как другие биометрические методы. Например, человек с простудой или ларингитом может испытывать трудности при использовании данных систем.

Геометрия лица. Идентификация по чертам лица — одно из наиболее быстро растущих направлений в биометрической

технологии. Развитие этого направления связано с быстрым ростом мультимедийных приложений. Можно ожидать появления в ближайшем будущем специальных устройств идентификации личности по чертам лица в залах аэропортов для защиты от террористов и т. п.

Клавиатурный почерк. Клавиатурный почерк, также называемый ритмом печатания, анализирует способ печатания пользователем той или иной фразы. Это аналогично ранним этапам развития радиотелеграфа, когда радисты идентифицировали друг друга «по почерку».

Подпись. Статическое закрепление подписи становится весьма популярным средством взамен росписи ручкой на банковской кредитной карточке, бланке службы доставки (например, FedEx). Устройства идентификации подписи используют специальные ручки или чувствительные к давлению столы, или комбинацию обоих средств. Устройства, использующие специальные ручки, менее дороги и занимают меньше места, но в то же время имеют меньший срок службы. Поскольку подписи слишком легко подделать, это служит препятствием внедрению идентификации личности по подписи в системы безопасности.

На крупных предприятиях возникает потребность в объединенных автоматизированных системах контроля доступа (АСКД). Такие АСКД могут связывать воедино устройства считывания карточек и кнопочные устройства доступа со средствами пожарной и тревожной сигнализации и замкнутыми телевизионными системами. Многие АСКД позволяют распечатывать записи по каждому сигналу тревоги, а также осуществлять сбор данных по времени посещения помещений сотрудниками, по разрешенным входам в помещения, по попыткам несанкционированного входа, по полученным сигналам тревоги и их подтверждению.

Подобные системы используются при высокой плотности потока проходящих лиц и большом числе устройств считывания с карточек. Будучи включенной в общую систему управления зданием, система контроля доступа может повысить уровень его защищенности. Основным достоинством объединенных систем является их гибкость, позволяющая руководству оперативно реализовывать решения по открытию или закрытию доступа в здания, помещения, лифты и целые этажи в установленное время зарегистрированным владельцам карточек.

На рис. 7.1 приведены сравнительные характеристики обеспечения безопасности современными электронными средствами

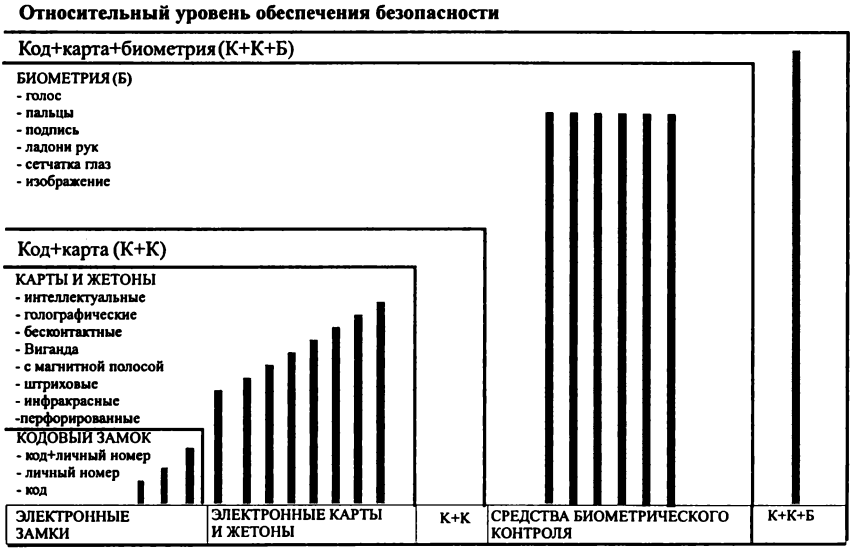


Рис. 7.1. Современные электронные средства контроля доступа

контроля доступа, которые позволяют оптимизировать решение задач по физической защите объектов. В зависимости от конкретных условий могут применяться комбинации различных систем контроля доступа, например бесконтактные устройства считывания карточек при входе и выходе из здания в сочетании с системой контроля доступа по голосу в зоны обработки секретной информации. Наилучший выбор системы или сочетания систем может быть сделан только на основе четкого определения текущих и перспективных потребностей организации.

Центральный пост и персонал охраны

Сложные комплексы защиты охраняемых территорий, состоящие, как правило, из нескольких систем, могут эффективно функционировать только при условии, что работа всех технических установок постоянно контролируется и управляется с центрального поста охраны. Учитывая повышенную психологическую нагрузку на дежурных охранников центрального поста, необходимость оперативной выработки и реализации оптимальных решений в случае тревоги, к центральным устройствам комплек-

сов защиты предъявляются особые требования. Так, они должны обеспечивать автоматическую регистрацию и отображение всех поступающих в центральный пост сообщений и сигналов тревоги, выполнение всех необходимых процедур. Важную роль играет и уровень эргономики аппаратуры, которой оснащаются рабочие места дежурных охранников.

Каналами связи в системе охранной сигнализации могут быть специально проложенные проводные линии, телефонные линии объекта, телеграфные линии и радиосвязь. Наиболее распространенные каналы связи — многожильные экранированные кабели, которые для повышения надежности и безопасности работы сигнализации помещают в металлические или пластмассовые трубы или металлорукава. Энергоснабжение системы охранной сигнализации должно обязательно резервироваться. Тогда в случае выхода его из строя функционирование сигнализации не прекращается за счет автоматического подключения резервного (аварийного) энергоисточника.

7.2. Комплексный подход к обеспечению безопасности

Комплексный подход к обеспечению безопасности основан на интеграции различных подсистем связи, подсистем обеспечения безопасности в единую систему с общими техническими средствами, каналами связи, программным обеспечением и базами данных [4].

Комплексная безопасность предполагает обязательную непрерывность процесса обеспечения безопасности как во времени, так и в пространстве (по всему технологическому циклу деятельности) с обязательным учетом всех возможных видов угроз (несанкционированный доступ, съем информации, терроризм, пожар, стихийные бедствия и т. п.).

В какой бы форме ни применялся комплексный подход, он связан с решением ряда сложных разноплановых частных задач в их тесной взаимосвязи. Наиболее очевидными из них являются задачи ограничения доступа к информации, технического и криптографического закрытия информации, ограничения уровней паразитных излучений технических средств, технической укрепленности объектов, охраны и оснащения их тревожной сигнализацией.

Однако необходимо решение и других, не менее важных задач. Так, например, выведение из строя руководителей предприятия или ключевых работников может поставить под сомнение само существование данного предприятия. Этому же могут способствовать стихийные бедствия, аварии, терроризм и т. п.

Первым шагом в создании системы физической безопасности (как и информационной безопасности вообще) должен стать анализ угроз (рисков) как реальных (действующих в данный момент), так и потенциальных (способных к проявлению в будущем).

По результатам анализа рисков с использованием критериев оптимизации формируются требования к системе безопасности конкретного предприятия и объекта в конкретной обстановке. Завышение требований приводит к неоправданным расходам, занижение — к возрастанию вероятности реализации угроз.

В общем случае система физической безопасности должна включать в себя следующие подсистемы:

- управления доступом (с функцией досмотра);
- обнаружения проникновения, аварийной и пожарной сигнализации (тревожной сигнализации);
- инженерно-технической защиты (пассивной защиты);
- отображения и оценки обстановки;
- управления в аварийных и тревожных ситуациях;
- оповещения и связи в экстремальных ситуациях;
- личной безопасности персонала.

При построении системы физической безопасности, удовлетворяющей сформулированным требованиям, разработчик выбирает и объединяет средства противодействия из числа указанных ниже:

- здания и строительные препятствия, мешающие действиям злоумышленника и задерживающие его;
- аппаратура тревожной сигнализации, обеспечивающая обнаружение попыток проникновения и несанкционированных действий, а также оценку их опасности;
- системы связи, обеспечивающие сбор, объединение и передачу тревожной информации и других данных;
- системы управления, необходимые для отображения и анализа тревожной информации, а также для реализации ответных действий оператора и управления оборонительными силами;
- персонал охраны, выполняющий ежедневные программы безопасности, управление системой и ее использование в нештатных ситуациях;

- процедуры обеспечения безопасности, предписывающие определенные защитные мероприятия, их направленность и управление ими.

На рис. 7.2 представлены технические средства противодействия и соответствующие подсистемы, имеющиеся в распоряжении разработчика. Как показывает опыт, успешная разработка

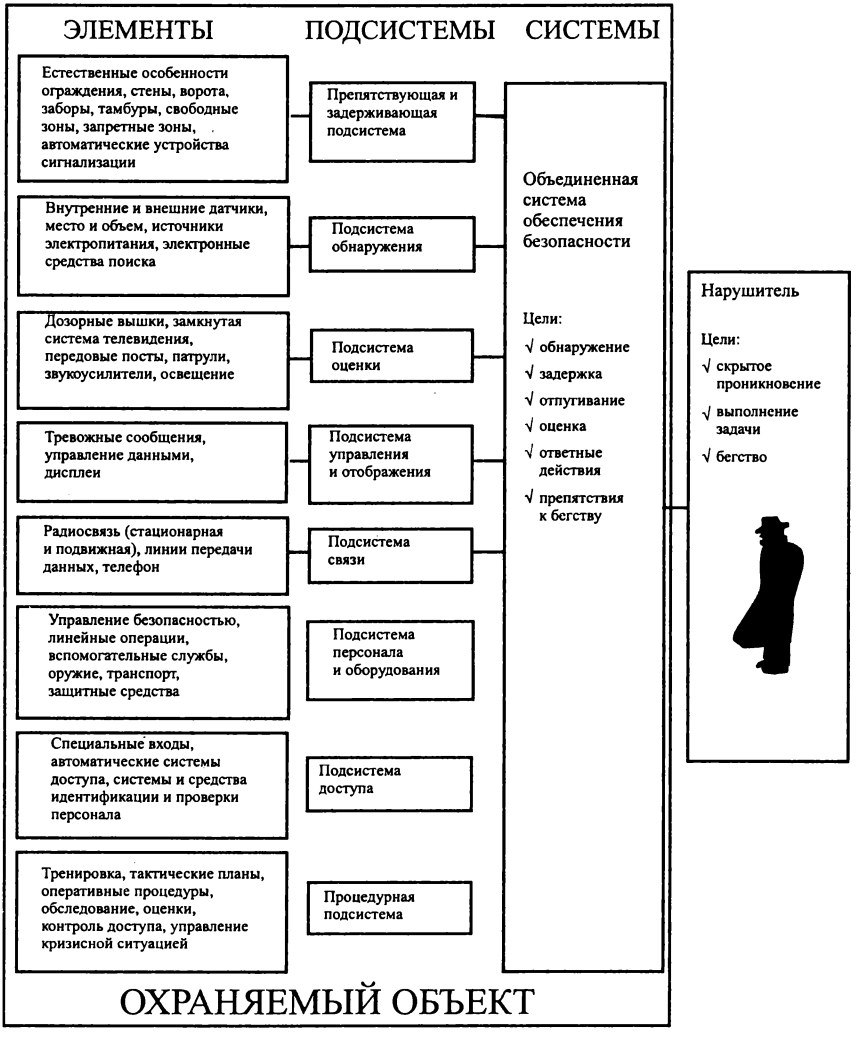


Рис. 7.2. Структура объединенной системы обеспечения безопасности

системы безопасности возможна только в том случае, когда процесс выбора средств противодействия и объединения их в единую систему разделен на этапы и определены соответствующие каждому этапу задачи.

Первоначально определяются объекты, которые надо защитить, и выполняемые ими функции. Затем оценивается степень интереса потенциального противника к этим объектам, вероятные виды нападения и вызываемый ими ущерб. Наконец, определяются уязвимые для воздействия области, в которых имеющиеся средства противодействия не обеспечивают достаточной защиты.

Для эффективного применения процесс выбора средств противодействия должен содержать оценку каждого объекта с точки зрения возможных угроз и видов нападения, потенциальной вероятности применения специальных инструментов, оружия и взрывчатых веществ. Особо важным допущением в этом процессе является предположение о том, что наиболее ценный для потенциального злоумышленника объект привлечет наибольшее внимание и будет служить вероятной целью, против которой злоумышленник использует основные силы.

Разработка средств противодействия должна соответствовать концепции полной и эшелонированной защиты. Это означает, что средства противодействия следует размещать на концентрических кругах, пересекающих все возможные пути противника к любому объекту. Рисунок 7.3 иллюстрирует данную концепцию. Каждый рубеж обороны организуется таким образом, чтобы задержать нападающих на время, достаточное для принятия персоналом охраны ответных мер.

На заключительном этапе разработчик объединяет выбранные средства противодействия в соответствии с принятой концепцией защиты. Производится также предварительная оценка начальной и ожидаемой общей стоимости жизненного цикла всей системы.

Разработчик должен принимать во внимание такое понятие, как жизненный цикл защищаемых объектов. В частности, он должен учитывать возможные перемещения объектов, а также изменение требований в местах входа.

В том случае, когда внутри одного здания располагаются объекты с существенно разными требованиями к безопасности, применяется разделение здания на отсеки, что позволяет выделить внутренние периметры внутри общего контролируемого про-

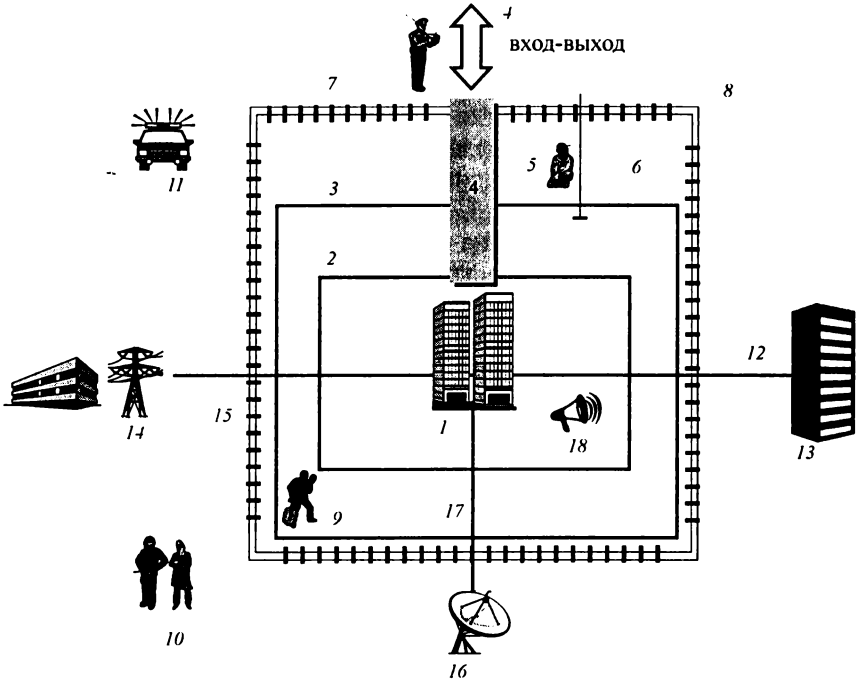


Рис. 7.3. Элементы классической системы обеспечения безопасности (охраны) объекта:

1 — охраняемый объект; *2* — задерживающее ограждение; *3* — обнаруживающее ограждение; *4* — контролируемый вход; *5* — зона оценки; *6* — нейтральная зона; *7* — забор; *8* — дальняя защита; *9* — силы внутренней обороны; *10* — силы внешней обороны; *11* — подвижный патруль; *12* — канал связи; *13* — внешний объект; *14* — электроподстанция; *15* — линия электропередачи; *16* — объекты технического обеспечения; *17* — инженерные коммуникации; *18* — радиосигнализация

странства и создать внутренние защитные средства от несанкционированного доступа. Периметр обычно выделяется физическими препятствиями, проход через которые контролируется электронным способом или с помощью специальных процедур. При защите группы зданий, имеющих общую границу или периметр, необходимо учитывать не только отдельный объект или здание, но и место, на котором они расположены. Обычно участки местности с большим количеством зданий имеют общие или частично совпадающие требования по обеспечению безопасности, а некоторые участки имеют ограждение по периметру и единую проходную. Организация общего периметра позволяет уменьшить коли-

чество защитных средств в каждом здании и устанавливать их только для наиболее важных объектов или зданий, нападение на которые наиболее вероятно. Аналогичным образом, каждое строение или объект на участке следует оценить с точки зрения их возможностей задержать нападающих. С учетом вышеизложенного рассмотрим в качестве примера проблему защиты вычислительного центра (ВЦ).

Надежная система должна обеспечивать защиту помещений и поддерживающей инфраструктуры, аппаратуры, программ, данных и персонала. Требования к таким системам сформулированы, в частности, в федеральном законе ФРГ по охране данных. Закон содержит перечень из девяти требований к защите, которые следует выполнять путем осуществления соответствующих технических и организационных мероприятий. Должны быть исключены:

- неправомочный доступ к аппаратуре обработки информации путем контроля доступа в производственные помещения;
- неправомочный вынос носителей информации персоналом, занимающимся обработкой данных, посредством выходного контроля в соответствующих производственных помещениях;
- несанкционированное введение данных в память, изменение или стирание информации, хранящейся в памяти;
- неправомочное пользование системами обработки информации и незаконное получение в результате этого данных;
- доступ в системы обработки информации посредством самодельных устройств и незаконное получение данных;
- возможность неправомочной передачи данных через ВЦ;
- бесконтрольный ввод данных в систему;
- обработка данных заказчика без соответствующего указания последнего;
- неправомочное считывание, изменение или стирание данных в процессе их передачи или транспортировки носителей информации.

Хотя перечень сформулирован в законе ФРГ, он справедлив и для любой другой страны при защите объектов (в частности, ВЦ).

Анализ перечисленных требований показывает, что они сводятся к исключению возможности неправомочного доступа к устройствам обработки и передачи информации, похищения носителей информации и проведения актов саботажа. Данные требования могут быть выполнены путем осуществления комплекса

мероприятий службой безопасности, администрацией ВЦ и специальными уполномоченными по охране информации.

Разработку концепции защиты рекомендуется проводить в три этапа. На первом этапе должна быть четко определена целевая установка защиты, т. е. установлено, какие реальные ценности, производственные процессы, программы, массивы данных необходимо защищать. На этом этапе целесообразно проводить дифференциацию по значимости отдельных объектов, требующих защиты. На втором этапе должен быть проведен анализ видов преступных действий, которые потенциально могут быть совершены в отношении ВЦ. Важно определить степень реальной опасности таких наиболее широко распространенных категорий преступлений, как экономический шпионаж, терроризм, саботаж, кражи со взломом.

Затем необходимо проанализировать наиболее вероятные действия злоумышленников в отношении основных объектов ВЦ, нуждающихся в защите.

Главной задачей третьего этапа является анализ обстановки в ВЦ, в том числе местных специфических условий, производственных процессов, уже установленных в ВЦ технических средств защиты. Собственно концепция защиты должна содержать перечень организационных, технических и других защитных мер, которые обеспечивают максимальную безопасность при заданном остаточном риске и при минимальных затратах на практическое осуществление этих мероприятий.

По уровню физической защиты все зоны и производственные помещения современных ВЦ могут быть подразделены на три группы:

- тщательно контролируемые зоны с защитой высокого уровня;
- защищенные зоны;
- слабо защищенные зоны.

К первой группе относятся, как правило, машинный зал (серверные комнаты), помещения с сетевым и связным оборудованием, архив программ и данных.

Ко второй группе относятся помещения, в которых расположены рабочие места администраторов, контролирующих работу ВЦ, а также периферийное оборудование ограниченного пользования.

В третью группу входят помещения, в которых оборудованы рабочие места пользователей и установлено периферийное оборудование общего пользования.

Комплекс физической защиты

На рис. 7.4 представлена блок-схема интегрального комплекса физической защиты объекта, обеспечивающего функциони-

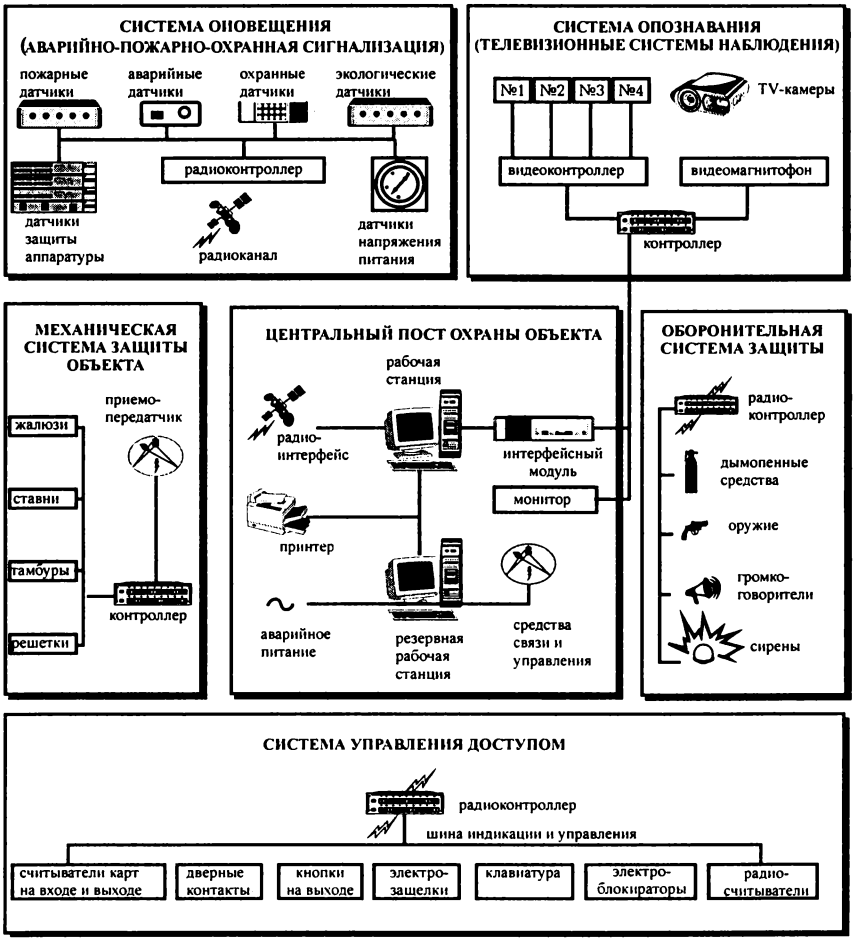


Рис. 7.4. Блок-схема интегрального комплекса физической защиты объекта

рование всех рассмотренных выше систем. Отличительной особенностью подобных комплексов является интеграция различных подсистем связи, подсистем обеспечения безопасности в единую систему с общими техническими средствами, каналами связи, программным обеспечением и базами данных.

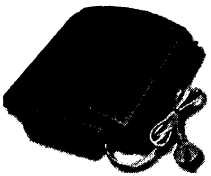
Необходимо отметить, что в рассматриваемой блок-схеме технические средства скомпонованы по системам достаточно условно, для того чтобы схема приобрела более логичную форму и была более понятна. На самом деле одни и те же средства выполняют различные функции для разных систем обеспечения безопасности.

Некоторые образцы технических средств обеспечения информационной и общей безопасности

В заключение приведем функции, характеристики и принципы функционирования небольшой выборки из обширного перечня изделий, представленных на российском рынке технических средств обеспечения безопасности [30], образующих следующие основные классы продуктов (список также далеко не полный):

- средства маскировки информации;
- закрытия каналов передачи;
- обнаружения/подавления закладок несанкционированного доступа к информации и других малоприятных сюрпризов.

Средства маскировки



VNG-012GL — комплекс виброакустической защиты

Функции: защита от утечки информации по акустическим и виброакустическим каналам, в том числе от прямого прослушивания; от прослушивания с помощью электронных стетоскопов, от съема информации с помощью лазерных и микроволновых систем.

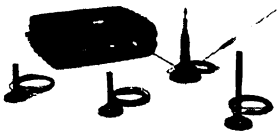
Позволяет зашумлять стены, пол, потолок, оконные проемы, трубы тепло-, водоснабжения, а также вентиляционные каналы и дверные тамбуры. В состав входят генератор шума VNG-012GL; виброизлучатели VN-GL с комплектом крепления; кабель соединительный генератора VNG-012GL с компьютером; дискета с

дистрибутивом программы управления генератором «ЭКВАЛАЙЗЕР». Пять независимых шумовых каналов и возможность регулировки их спектра в октавных или 1/3-октавных частотных полосах. Настройка параметров комплекса программным способом через ПК. Сертификат Гостехкомиссии России.

SEL SP-55 — система защиты помещений по виброакустическому каналу

Функции: защита от микроволновых систем, в том числе лазерных микрофонов, используемых для дистанционного съема акустической информации с остекления оконных проемов; стетоскопных/контактных микрофонов, используемых для съема акустической информации через строительные конструкции (стены, потолки, полы, оконные проемы и их остекление) и трубы водо- и газоснабжения; радио- и проводных микрофонов и средств магнитной записи, установленных в полостях стен, в пространстве подвесных потолков, каналах вентиляционных систем и др.

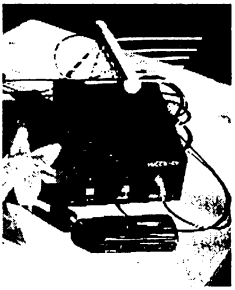
Система включает многоканальный генератор шума и подключаемые к нему виброизлучатели SEL SP-51/AV или акустические колонки. Отсутствие аналоговых узлов исключает утечку информации за счет самовозбуждения, паразитной генерации и модуляции опасным речевым сигналом, а также за счет электрических сигналов, вызванных электроакустическими преобразованиями в элементах схемы, и их утечки по цепям питания и пр. Независимые формирователи шума для каждого выходного канала с длительностью автокорреляции 40 мин позволяют полностью исключить возможность шумоочистки существующими программно-аппаратными средствами, включая системы с опорным каналом.



Пелена-6У — постановщик радиопомех

Функции: предотвращение несанкционированного получения информации с использованием малогабаритных радиопередатчиков, а также для защиты от радиоуправляемых взрывных устройств. Может использоваться для подавления устройств сотовой, транкинговой, пэйджинговой связи.

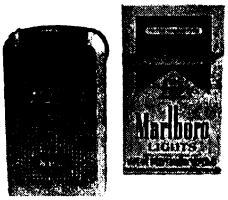
Принцип работы основан на постановке шумовой помехи в широком диапазоне частот.



ЛГШ-101 «Рубеж» — подавитель диктофонов

Функции: защита конфиденциальных переговоров от несанкционированной работы аппаратуры звукозаписи (магнитофонов, диктофонов, включая цифровые).

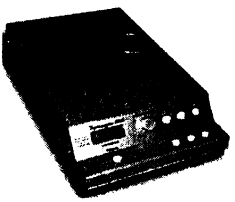
Предназначено для использования в стационарных условиях (в офисных помещениях с питанием от сети переменного тока 220 В). Зона подавления устройства определена углом в 65—70°, поэтому очень важно правильно расположить излучающую антенну. Антенна может быть установлена, например, под панелью стола переговоров и направлена на место предполагаемого расположения собеседника. Дальность подавления: для диктофонов с неметаллическими корпусами не менее 1,5 м; для диктофонов с металлическими корпусами до 1,5 м.



«Мозаика-мини» — портативный блокиратор сотовых телефонов

Функции: блокирование работы подслушивающих устройств, использующих каналы систем мобильной связи стандартов GSM-900/1800, E-GSM, AMPS, DAMPS, CDMA, а также блокирования работы телефонов названных систем мобильной связи.

Камуфлирован под малогабаритный приемник. Диапазон рабочих частот 860—960 МГц, 1805—1880 МГц; радиус действия примерно 2 м.



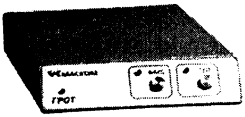
«Прокруст-2000» — устройство защиты телефонных переговоров от прослушивания и записи

Функции: максимальная защита линии (от телефонного аппарата до АТС) методом постановки активной помехи, подавляющей действие практически любых, существующих на сегодняшний день, телефонных закладок во время разговора.

Подавление нормальной работы телефонных закладок любых типов подключения осуществляется путем перегрузки входных цепей двумя активными помехами с разными физическими характеристиками. Режимы работы — детектор, помеха, уровень,

стробирование, блокировка. Организуется участок дополнительной защищенности для гарантированного предотвращения снятия и передачи информации по телефонной линии при положенной трубке. Световая индикация пиратского использования линии в промежутках между переговорами, возможность подключения звукозаписывающих устройств для документирования переговоров. Сертификат Гостехкомиссии России.

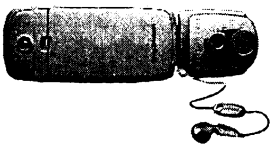
Средства закрытия



Телефонные/факсимильные скремблеры серии ГРОТ

Функции: шифрование речевого сигнала и защита факсимильных сообщений, передаваемых по телефонной сети общего применения.

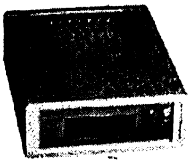
Идентификация за счет использования электронного блокнота индивидуальных ключей; метод шифрования — мозаичный: частотные и временные перестановки; метод открытого распределения ключей, позволяющий работать без ручного набора ключей; общее количество ключевых комбинаций 2×10^{18}, возможность введения дополнительного 7-значного ключа для идентификации абонента; высокая степень криптографической защиты за счет наличия дополнительных мастер-ключей, которые устанавливаются по желанию заказчика



«Референт GSM» (версия basic) — устройство для защиты от прослушивания разговоров по мобильному телефону

Функции: предотвращение возможности прослушивания разговоров по мобильному телефону как на уровне операторов сотовой связи, так и с помощью комплексов перехвата GSM. Работает в составе мобильного телефона в качестве внешнего устройства.

Исходная речь подвергается аналого-цифровому преобразованию, представляющему собой высокоскоростной 64 Кбит цифровой поток, который сжимается до скорости 2,4 Кбит/с, а затем шифруется специальным алгоритмом шифрования и в таком виде передается модемом мобильного телефона по каналу передачи данных GSM. Устройство предназначено для работы с мобильными телефонами производства Ericsson и Sony-Ericsson.



«Цикада-М» — устройство защиты телефонных переговоров

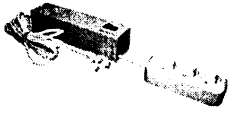
Функции: защита телефонных переговоров на участке линии от абонента до ГАТС. Борьба с параллельно подключенными телефонными аппаратами, диктофонами, устройствами съема различного типа, в том числе и индуктивного.

Принцип работы устройства основан на подавлении устройств последовательного съема; подавлении устройств параллельного съема; блокировании устройств съема с питанием от ТЛ; сигнализации использования параллельных ТА.

«Гранит-8» — абонентское устройство защиты информации

Функции: защита речевой информации от утечки за счет акустоэлектрических преобразований через двухпроводные линии открытых телефонных сетей, сетей радиотрансляции, систем директорской и диспетчерской связи.

Фильтр «Гранит-8» представляет собой четырехполюсник, состоящий из двух П-образных индуктивно-емкостных звеньев и диодного моста. Диодный мост схемы является входом изделия и предназначен для уменьшения коэффициента передачи фильтра при малых уровнях сигнала. Сигналы, которые могут возникать на выходе ТСПИ при акустоэлектрических преобразованиях, подавляются.



«Соната-РК1» — устройство комбинированной защиты объектов информатизации от утечки информации

Функции: защита информации, обрабатываемой основными техническими средствами и системами до 1-й категории включительно, от утечки по ПЭМИН путем постановки маскирующих помех.

Эффективное и недорогое решение задачи комплексной защиты («ЭМИ + наводки + утечка по сети электропитания») одиночного технического средства в ситуациях, когда остро стоит проблема помех, создаваемых генераторами маскирующего шума. Является комбинацией фильтра поглощающего типа, генераторов шумового тока с корректировкой спектра и регулировкой интегрального уровня и элементов антенной системы.

Средства обнаружения/подавления

ST031P «Пиранья» — универсальный поисковый прибор

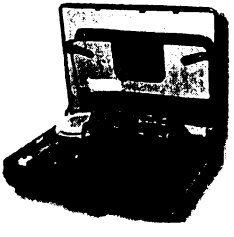
Функции: обнаружение и локализация средств негласного получения информации, выявление естественных и искусственно созданных каналов утечки информации.

Режимы работы: высокочастотный детектор-частотомер (диапазон частот 30—2500 МГц); сканирующий анализатор проводных линий (диапазон 0,05—9 МГц); детектор инфракрасных излучений (диапазон 770—1000 нм); детектор низкочастотных магнитных полей (0,5—300 кГц); виброакустический преобразователь (0,3—6 кГц); акустический преобразователь (0,3—8 кГц); дифференциальный низкочастотный усилитель (динамический диапазон более 60 дБ; диапазон частот 0,2—15 кГц). Сертификат Гостехкомиссии России.

ГИ-1500 — выжигатель устройств съема информации в проводных линиях связи и в обесточенной электросети

Функции: защита от несанкционированного прослушивания переговоров как по телефону, так и в помещении с помощью устройств, работающих в проводных линиях либо в электросети.

Принцип действия прибора основан на электрическом пробое радиоэлементов. В линию подается мощный короткий высоковольтный импульс, способный полностью разрушить или нарушить функциональную деятельность средств съема информации. Амплитуда импульса: 1600 или 2000 В.

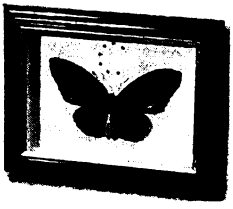


LBD-50 — анализатор проводных коммуникаций

Функции: поиск несанкционированных гальванических подключений к проводным линиям любого назначения.

Используется комплекс методов обнаружения — исследование нелинейных преобразований сигналов, подаваемых в линию, анализ переходных процессов в линии, измерения параметров линий (ток утечки, сопротивление изоляции).

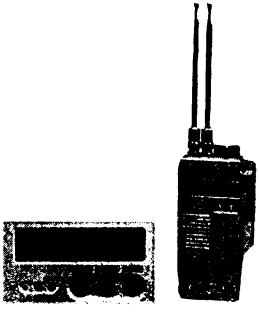
Анализатор обнаруживает подключения устройств, предназначенных для перехвата информации; передачи материалов перехвата; обеспечения электропитанием. Алгоритм обследования, заложенный в анализаторе, исключает срабатывание защитных сторожевых схем в объектах поиска. Комплект прибора содержит специальный трассоискатель, позволяющий бесконтактным способом найти обследуемую линию в распределительном шкафу, жгуте и т. п.



«Панно» — индикатор поля

Функции: выявление следующих объектов — скрытно носимых радиомикрофонов и включенных мобильных телефонов; мощных (СВЧ) электромагнитных полей, создаваемых подавителями диктофонов и радиомикрофонов; вредных излучений неисправных микроволновых печей; радиозакладок, в том числе акустических, телефонных и телевизионных.

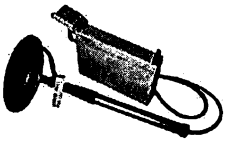
Выполнен (закамуфлирован) в виде настенного панно с бабочкой. Индикация световая. Диапазон рабочих частот: 60... ...2500 МГц.



«Скорпион» — скоростной поисковый приемник

Функции: средство радиотехнического контроля, предназначенное для автоматического обнаружения сигналов, излучаемых нелегальными радиопередатчиками, и подавления каналов их приема.

Осуществляет изучение радиоэлектронной обстановки в конкретном месте его эксплуатации с запоминанием частот сигналов; обнаружение и определение местоположения нелегально существующего передатчика в контролируемом помещении; подавление канала приема сигнала обнаруженного нелегального передатчика путем постановки на его частоте прицельной помехи. Диапазон принимаемых частот: 30—2000 МГц; чувствительность: 50 мкВ; время просмотра диапазона — 10 с; количество исключаемых каналов приема — 4850; количество запоминаемых обнаруженных сигналов — 256; мощность прицельной помехи — 50 мВт.



«КАТРАН-3М» — нелинейный локатор

Функции: выявление средств несанкционированного получения информации, установленных в строительных конструкциях, предметах мебели и интерьера, находящихся как в активном, так и в выключенном состоянии.

Работа локатора основана на свойстве полупроводниковых элементов излучать вторую и третью гармоники при облучении их зондирующим СВЧ-сигналом. «Катран» обеспечивает обнаружение устройств, содержащих полупроводниковые элементы, и предварительную оценку природы обнаруженного объекта по соотношению уровней переизлучаемых им 2-й и 3-й гармоник (транзисторы, диоды, микросхемы — преобладание 2-й гармоники, коррозийные диоды, оксидные пленки, образованные естественным путем, — 3-й гармоники).

ИРТИС-2000 — термограф

Функции: прецизионный оптико-механический сканирующий инфракрасный прибор для визуализации и измерения тепловых полей с высокой (не хуже 0,05 °С) чувствительностью в широком диапазоне температур.

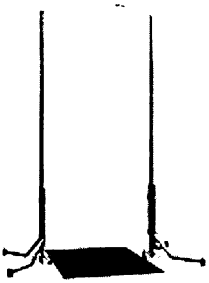
Осуществляет сканирование температурного излучения в поле зрения камеры оптико-механическим сканером с одноэлементным высокочувствительным ИК-приемником и трансформацию этого излучения в электрический сигнал аналого-цифровым преобразователем. Термограф может применяться для обнаружения неоднородностей в стене вследствие установки радиомикрофонов. Может быть подключен к ПК с помощью параллельного, сетевого, USB или беспроводного (Wi- Fi) интерфейсов.

НОРКА — переносная рентгенотелевизионная установка

Функции: обнаружение элементов взрывных устройств, оружия, скрыто установленных средств прослушивания, а также контейнеров с опасными вложениями в отдельных предметах, посылках, мебели, багаже и т. д.

При создании рентгенотелевизионных установок «РОНА» и «НОРКА» использован модульный принцип построения. В со-

став комплекта могут входить различные излучатели, преобразователи и блоки управления. По желанию заказчика можно подобрать конфигурацию системы, наилучшим образом отвечающую его требованиям.



«Фракталь-01/21» — металлодетектор быстрого развертывания

Функции: обеспечение 100 % обнаружения холодного и огнестрельного оружия, оболочек взрывчатых устройств и любых предметов, в состав которых входят ферромагнитные материалы.

Регистрирует изменения параметров внешнего магнитного поля в зоне охраны при перемещении в ней предмета поиска. При проносе изделия, содержащего ферромагнитный материал через зону охраны (контролируемый проем), изменяются параметры магнитного поля. В результате чувствительный элемент формирует аналоговый сигнал, который регистрируется блоком обработки сигнала, находящимся в пульте управления.

АКА-7202 — ручной металлодетектор

Функции: обнаружение металлических предметов, находящихся в диэлектрических средах. Прибор может быть также использован для обследования почв, зданий, мебели и т. д.

Обнаруживает 5-мм обломок иглы. Дальность обнаружения пистолета Макарова — 28 см; время непрерывной работы от новой батареи 700 ч; индикация — световая и звуковая.

НПО-3М — поисковый сигнализатор ионизирующего излучения

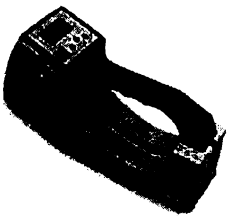
Функции: экспресс-контроль мощности экспозиционной дозы и локализации источников радиоактивного излучения.

Состоит из блока радиометра и блока подзарядки аккумулятора. Предусмотрена возможность автоматического переключения шкал и непрерывной индикации мощности дозы на жидкокристаллическом индикаторе в цифровом виде. Время экспозиции: 1 с; диапазон измерения мощности дозы, мкР/ч: 5—50 000.

E3500 — портативный детектор обнаружения взрывчатых веществ (производство Scintrex Trace)

Функция: обнаружение следовых количеств (низкий нанограммный уровень) ВВ.

Принцип определения — люминол хелюминисценс — картридж одноразового использования; компоненты обнаружения: большинство военных (включая пластиковые) и коммерчески используемых взрывчатых веществ: C4, TNT, нитроглицерина, динамита, PETM, Semtex, RDX, ANFO, ICAD, составляющие (DMNB, EGDN, j-MNT, p-MNT) нитрата аммония, нитрата мочевины (карбамида) и TATP; детекция — 5...30 с (селективная); анализ — в течение 15 с.



Pilot-M — газоанализатор-обнаружитель паров взрывчатых веществ

Функции: дрейфспектрометрический детектор паров ВВ. Обнаружение зарядов взрывчатых веществ (ВВ) в негерметичных объемах и следов ВВ на поверхности обследуемых объектов.

Обнаружение осуществляется путем отбора проб воздуха с поверхности или из внутреннего объема обследуемых объектов и анализа проб на содержание паров ВВ. Конструкция прибора и применяемые алгоритмы обработки сигнала обеспечивают высокую избирательность и помехоустойчивость. Пороговая чувствительность (по ТНТ) не хуже 10^{-13} г/см^3, время отклика на наличие паров ВВ 1—2 с, дистанционность при пробоотборе до 10 см.

Контрольные вопросы

1. Какие технические средства охранной сигнализации вам известны?
2. Что представляют собой и на каких принципах функционирования основаны объемные датчики?
3. Что представляют собой и на каких принципах функционирования основаны линейные датчики?
4. Что представляют собой и на каких принципах функционирования основаны локальные датчики?
5. Что представляют собой инфраакустические датчики?

6. Каковы принципы функционирования датчиков электрического поля?
7. Что представляют собой инфракрасные датчики?
8. Что представляют собой магнитные датчики?
9. На каких принципах действия основаны ультразвуковые датчики?
10. Что представляют собой емкостные датчики?
11. Что представляют собой микроволновые датчики?
12. Каковы принципы функционирования датчиков давления?
13. Каковы принципы организации и основные достоинства охранного телевидения?
14. Какие средства оповещения и связи вам известны?
15. Перечислите основные методы биометрической идентификации.

Заключение

Информационная безопасность относится к числу дисциплин, развивающихся чрезвычайно быстрыми темпами. Этому способствуют как общий прогресс информационных технологий, так и постоянное противоборство нападающих и защищающихся.

К сожалению, подобная динамичность объективно затрудняет обеспечение надежной защиты. Причин тому несколько:

- повышение быстродействия микросхем, развитие архитектур с высокой степенью параллелизма позволяет методом грубой силы (перебором вариантов) преодолевать барьеры (прежде всего криптографические), ранее казавшиеся неприступными;
- развитие сетей, увеличение числа связей между информационными системами, рост пропускной способности каналов расширяют число потенциальных злоумышленников, имеющих техническую возможность осуществить нападение;
- появление новых информационных сервисов ведет и к появлению новых угроз как «внутри» сервисов, так и на их стыках;
- конкуренция среди производителей программного обеспечения заставляет сокращать сроки разработки системы, что ведет к снижению качества тестирования и выпуску продуктов с дефектами защиты;
- навязываемая потребителям парадигма постоянного наращивания аппаратного и программного обеспечения вступает в конфликт с бюджетными ограничениями, из-за чего снижается доля ассигнований на безопасность.

Обеспечение информационной безопасности современных информационных систем требует комплексного подхода. Оно невозможно без применения широкого спектра защитных средств, объединенных в продуманную архитектуру. Далеко не все эти

средства получили распространение в России, некоторые из них даже в мировом масштабе находятся в стадии становления.

В этих условиях позиция по отношению к информационной безопасности должна быть особенно динамичной. Теоретические воззрения, стандарты, сложившиеся порядки необходимо постоянно сверять с требованиями практики. От атак не защититься книгой (даже оранжевой) или сертификатом. Реальная безопасность нуждается в каждодневной работе всех заинтересованных сторон.

Список литературы

1. *Аскеров Т. М.* Защита информации и информационная безопасность: учебное пособие / под общей ред. К. И. Курбакова. М.: Рос. экон. акад., 2001. 387 с.

2. *Баричев С. В.* Криптография без секретов. М.: Наука, 1998. 120 с.

3. *Барсуков В. С., Водолазский В. В.* Интегральная безопасность информационно-вычислительных и телекоммуникационных сетей (часть 1). Технология электронных коммуникаций. М., 1993. 146 с.

4. *Барсуков В. В.* Физическая защита информационных систем / JetInfo online, 1997. № 1(32).

5. *Вербицкий О. В.* Вступление к криптологии. Львов: Издательство науково-техничной литературы, 1998. 300 с.

6. *Гайкович В., Першин А.* Безопасность электронных банковских систем. М.: Компания «ЕДИНАЯ ЕВРОПА», 1994. 331 с.

7. *Галатенко В. А.* Информационная безопасность. М.: Финансы и статистика, 1997. 158 с.

8. *Герасименко В. А.* Защита информации в автоматизированных системах обработки данных (кн. 1). М.: Энергоатомиздат, 1994. 400 с.

9. *Герасименко В. А., Малюк А. А.* Основы защиты информации. М.: МИФИ, 1997. 537 с.

10. *Герасименко В. А., Партыка Т. Л.* Каталог программных средств защиты информации от несанкционированного доступа в АСОД. Метод. указания. М.: ГКНТ, 1984. 214 с.

11. *Герасименко В. А., Партыка Т. Л.* Каталог каналов утечки информации в АСОД. Метод. указания. М.: ГКНТ, 1985. 273 с.

12. *Герасименко В. А., Скворцов А. А., Харитонов И. Е.* Новые направления применения криптографических методов защиты информации. М.: Радио и связь, 1989. 360 с.

13. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к

информации. Классификация автоматизированных систем и требования по защите информации. М.: Военное издательство, 1992. 39 с.

14. Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. М.: Военное издательство, 1992. 12 с.

15. Гостехкомиссия России. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. М.: Военное издательство, 1992. 12 с.

16. *Грегори С. Смит.* Программы шифрования данных // Мир ПК. 1997. № 3. С. 58—68.

17. *Диффи У.* Первые десять лет криптографии с открытым ключом // ТИИЭР, т. 76(1988)б Т5б. С. 54—74.

18. *Зима В. М., Молдовян А. А., Молдовян Н. А.* Защита компьютерных ресурсов от несанкционированных действий пользователей: учеб. пособие. СПб., 1997. 189 с.

19. *Касперский Е.* Компьютерные вирусы в MS-DOS. М.: Эдель-Ренессанс, 1992.

20. Криптология — наука о тайнописи // Компьютерное обозрение. 1999. № 3. С. 10—17.

21. *Лопатин В. Н.* Информационная безопасность России: Человек. Общество. Государство / Санкт-Петербургский университет МВД России. СПб.: Фонд «Университет», 2000. 428 с.

22. *Мельников В.* Защита информации в компьютерных системах. М.: Финансы и статистика, Электронинформ, 1997. 364 с.

23. *Миллер В.* Использования эллиптических кривых в криптографии. М., 1986. С. 417—426.

24. *Нечаев В. И.* Элементы криптографии (Основы теории защиты информации): учеб. пособие для ун-тов и пед. вузов / под ред. В. А. Садовничего. М.: Высш. шк., 1999. 109 с.

25. *Расторгуев С. П.* Программные методы защиты информации в компьютерах и сетях. М.: Издательство Агентства «Яхтсмен», 1993. 188 с.

26. *Ростовцев А. Г., Михайлова Н. В.* Методы криптоанализа классических шифров. М.: Наука, 1995. 208 с.

27. *Ухлинов Л. М.* Международные стандарты в области обеспечения безопасности данных в сетях ЭВМ. Состояние и направления развития. М.: Электросвязь, 1991.

28. Федеральный закон «Об информации, информатизации и защите информации». Собрание законодательства Российской Федерации. 20 февраля 1995 г. Официальное издание. М.: Издательство «Юридическая литература», Администрация Президента Российской Федерации. С. 1213—1225.

29. Кодекс Российской Федерации об административных правонарушениях. М.: Инфра-М, 2002. 304 с.

30. http://www.securit.ru/

31. http://www.pctechguide.com

32. http://www.wikipedia.org

Глоссарий (терминологический словарь)

Автоконтроль целостности — использование в программе специальных алгоритмов, позволяющих после запуска программы определить, были ли внесены изменения в файл, из которого загружена программа или нет.

Авторизация (authorization) — полномочия, устанавливаемые администратором системы для конкретных лиц, позволяющие последним использовать транзакции, процедуры или всю систему в целом.

Аддитивные методы. В качестве ключа шифра используется некоторая последовательность букв того же алфавита, в котором представлен исходный текст. Длина ключа равна длине сообщения. Сам процесс шифрования состоит из суммирования исходного текста и ключа по модулю, равному числу букв в алфавите (например, по модулю 2, если алфавит двоичный).

Администрирование средств безопасности включает в себя распространение информации, необходимой для работы сервисов безопасности, а также сбор и анализ информации об их функционировании. Примерами могут служить распространение криптографических ключей, установка прав доступа, анализ регистрационного журнала и т. п.

Аккредитация (accreditation) — авторизация и санкционирование обработки критичных данных в операционной среде информационной системы или сети. Решение об аккредитации выносится после получения всеми лицами из технического персонала сертификата, подтверждающего возможность этих лиц работать с защищенными системами. При этом предварительно должно быть подтверждено соответствие проекта самой системы и его конкретной реализации набору заранее определенных технических требований. Все эти условия служат единственной цели —

обеспечению степени безопасности адекватной уровню критичности данных.

Алгоритм DES состоит из многократно повторяемых шагов перестановки, гаммирования и колонной замены. В реализации этого алгоритма выделяются режимы электронного кодирования, сцепления блоков шифра, обратной связи по шифротексту и обратной связи по выходу. В базовом режиме текст разбивается на 64-битовые блоки. Они независимо шифруются при помощи одного и того же ключа длиной 56 бит (8 бит используются для контроля). При этом одинаковые блоки будут иметь одинаковые шифры (недостаток). Для повышения степени надежности алгоритма часто используют ключи двойной или тройной длины (на которые существуют стандарты).

Анализ затрат/выгоды (cost-benefit analysis) — стадия в разработке или развитии системы, на которой определяется стоимость обеспечения защиты данных в информационной системе; иногда под этой стоимостью подразумевают ущерб, который может быть нанесен в случае утери или компрометации данных, подлежащих защите.

Анализ риска (risk analysis) — процесс изучения характеристик и слабых сторон системы, проводимый с использованием вероятностных расчетов, с целью определения ожидаемого ущерба в случае возникновения неблагоприятных событий. Задача анализа риска состоит в определении степени приемлемости того или иного риска в работе системы.

Атака (attack) — нарушение безопасности информационной системы, позволяющее захватчику управлять операционной средой. Атака — действие некоторого субъекта компьютерной системы (пользователя, программы, процесса и т. д.), использующего уязвимость компьютерной системы для достижения целей, выходящих за пределы авторизации данного субъекта в компьютерной системе. Если, например, пользователь не имеет права на чтение некоторых данных, хранимых в компьютерной системе, а ему хочется незаконно его приобрести, поэтому он предпринимает ряд нестандартных манипуляций, обеспечивающих доступ к этим данным (в случае отсутствия или недостаточно надежной работы средств безопасности), либо завершившихся неудачей (в случае надежной работы средств безопасности), — тем самым этот пользователь (иногда его

называют «захватчиком») предпринимает в отношении компьютерной системы атаку.

Атака «салями» характерна для банковских систем и основывается на том, что при исчислении процентов нередко получаются дробные числа.

Аудит (audit) — контроль, образ действий, позволяющий получать независимый обзор и анализ системных записей об активности системы с целью установления ее текущего состояния безопасности.

Аутентификация (authentication) — 1) процедура идентификации или проверки полномочности узлов, инициаторов или лиц для доступа к определенной категории информации; 2) план, разрабатываемый для обеспечения защиты от незаконных передач информации за счет установления санкционированности потоков информации, сообщений, узлов или инициаторов.

Банковская тайна — защищаемые банками и иными кредитными организациями сведения о банковских операциях по счетам и сделкам в интересах клиентов, счетах и вкладах своих клиентов и корреспондентов, а также сведения о клиентах и корреспондентах, разглашение которых может нарушить право последних на неприкосновенность частной жизни.

Безопасная операционная система (secure operating system) — операционная система, эффективно управляющая аппаратными и программными средствами с целью обеспечения уровня защиты, соответствующего содержанию данных и ресурсов, контролируемых этой системой.

Безопасность (security) — состояние, в котором файлы данных и программы не могут быть использованы, просмотрены и модифицированы неавторизованными лицами (включая персонал системы), компьютерами или программами. Безопасность обеспечивается путем создания вокруг компьютера и оборудования защищенной зоны, в которой работает только авторизованный персонал, а также использования специального программного обеспечения и встроенных в операционные процедуры механизмов защиты.

Безопасность данных (data security) — защита данных от неавторизованных, случайных, умышленных или возникших по халатности модификаций, разрушений или разглашений.

Безопасность информации (information security) — защита информационных массивов от случайных либо преднамеренных, но неавторизованных разглашений, модификаций или разрушений, либо от невозможности обработки этой информации. Отсутствие несанкционированного получения ее лицами или процессами, не имеющими на это соответствующих полномочий.

Безопасность информационной системы (information system security) — совокупность элементов (действий, мер), необходимых для обеспечения адекватной защиты компьютерной системы, включая аппаратные/программные функции, характеристики и средства; операционные и учетные процедуры, средства управления доступом на центральном компьютере, удаленных компьютерах и телекоммуникационных средствах; административные мероприятия, физические конструкции и устройства; управление персоналом и коммуникациями.

Безопасность коммуникаций (communications security) — аутентификация телекоммуникаций за счет принятия мер по предотвращению предоставления неавторизованным лицам критичной информации, которая может быть выдана системой в ответ на телекоммуникационный запрос.

Безопасность персонала (personnel security) — методы обеспечения гарантий того, что весь персонал, имеющий возможность доступа к некоторой критичной информации, обладает необходимой авторизацией, равно как и всеми необходимыми разрешениями.

Безопасность программного обеспечения (software security) — свойство общецелевых (исполнительные программы, утилиты либо средства разработки программного обеспечения) и прикладных программ и средств осуществлять безопасную обработку данных в компьютерной системе и безопасно использовать ресурсы системы.

Брешь, дыра (loophole) — программное или аппаратное упущение или недоработка, позволяющая обойти процессы управления доступом. Синонимами являются термины fault, flaw.

Вакцинирование — специальная обработка файлов, дисков, каталогов, запуск резидентных программ-вакцин, имитирующих сочетание условий, которые используются данным типом вируса для определения (выявления) заражения, т. е. «обманывающих» вирус.

Ведение контроля (auditing) — процедуры управления системой, необходимые для обеспечения нормальной работы системы и выполнения имеющихся задач, а также для обеспечения эффективности работы и эффективности использования ресурсов информационной системы. Ведение контроля может осуществляться лицами, отличными от лиц, непосредственно отвечающих за работу системы и решение конкретных эадач.

Верификация (verification) — использование теста или имитированной среды для выявления идентичности двух уровней спецификаций системы, например политики безопасности в спецификации высшего уровня (исходном коде) и объектном коде.

Вирус (virus) — программа, модифицирующая другие программы. В контексте проблем безопасности этот термин обычно используется в отношении программ, злонамеренно внедряемых в систему с целью нанесения вреда или разрушений. Вирусная программа распространяется за счет самокопирования и подсоединения копий к другим программам. Когда в системе происходит определенное событие, на которое настроен вирус, вирус начинает выполнять свою целевую функцию. В настоящее время известно более 50 000 программных вирусов, число которых непрерывно растет. Известны случаи, когда создавались учебные пособия, помогающие в написании вирусов.

Вирусы неопасные — не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках; действия таких вирусов проявляются в каких-либо графических или звуковых эффектах. Имеются *опасные* вирусы, которые могут привести к различным нарушениям в работе компьютера, и *очень опасные*, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

Вирусы-мутанты — содержат алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов.

Вирусы-невидимки, или *стелс-вирусы*, которые очень трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска.

Владелец (owner) — лицо, ответственное за вынесение и доведение до заинтересованных сторон решений от имени организации в

отношении использования, идентификации, определения степени секретности и защиты конкретных информационных объектов.

Выключатели магнитные. Датчики этого типа состоят из выключателя (так называемого геркона), контакты которого размыкаются или замыкаются под воздействием магнита. Датчик состоит из двух частей: подвижной и неподвижной. На подвижной части, например двери или оконной раме, устанавливается магнит, а на неподвижной — геркон, который при открывании подвижной части размыкает электрическую цепь и вызывает появление сигнала тревоги.

Выключатели электромеханические. Действие датчиков этого типа основано на регистрации разрыва электрической цепи при воздействии нарушителя. Они применяются для контроля периметров зданий и помещений. Изготавливается два вида датчиков: как с неразрушающимися элементами (типа кнопок), так и с разрушающимися контактами при использовании, например, токопроводящего стекла или сетки из фольги.

Государственная тайна — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Датчики акустические. В состав этих датчиков входят микрофон и блок обработки сигналов. Они служат для обнаружения вторжений преступников и реагируют на шум и звуки, которые неизбежно возникают при попытке проникнуть в охраняемое помещение.

Датчики барометрические — предназначены для охраны закрытых объемов помещений. Датчик реагирует на флуктуации давления воздуха в охраняемом помещении. Устойчив к воздействию шумов, вибрации, перемещению людей и животных, не оказывает вредного влияния на людей и аппаратуру. Срабатывает в момент открывания дверей, окон, форточек или при разрушении стен, потолка, дверей и окон. Очень экономичен (ток потребления — не более 1 мА).

Датчики емкостные применяются для охраны защитных металлических решеток инженерных коммуникаций. Действие датчиков основано на регистрации изменения электрической емко-

сти между полом помещения и решетчатым внутренним ограждением.

Датчики контроля пространства инфракрасные. Принцип действия основан на изменении сигнала от излучателя к приемнику при попадании нарушителя между ними. В качестве излучателей используются инфракрасные светодиоды или небольшие лазерные установки. Расстояние между излучателем и приемником не более 100 метров. На специальные столбы обычно устанавливают несколько таких устройств для создания вертикальной полосы обнаружения необходимой высоты. Для повышения надежности иногда используется частотная модуляция сигнала излучения. Датчики могут терять свою работоспособность при густом тумане и снегопаде.

Датчики контроля пространства микроволновые состоят из двух частей: сверхвысокочастотных передатчика и приемника, которые устанавливаются на расстоянии до 150 м друг от друга. В пространстве между ними создается электромагнитное поле, изменение которого при попытке прохода регистрируется приемником. Для эффективной работы таких датчиков необходимо, чтобы высота неровностей почвы не превышала 5 — 7 см, а в зоне действия не было растительности.

Датчики магнитные изготавливаются из проволочной сетки, которая укладывается в почву. Датчики этого типа реагируют на прохождение человека с металлическим предметом достаточно большой массы. Наличие металла вызывает индукционные изменения электрического поля проволочной сетки, что и возбуждает сигнал тревоги. Магнитные датчики неэффективны вблизи автомобильных и железных дорог. Возможны ложные срабатывания от грозовых разрядов, мощных электромоторов и реле.

Датчики микроволновые работают в СВЧ-диапазоне на частотах порядка 10,5 ГГц. Излучение и прием осуществляются одной антенной.

Датчики периметра вибрационные представляют собой контактные выключатели различных видов, соединенные последовательно или параллельно. Датчики крепятся на столбах или сетках ограждений и срабатывают от качаний, сотрясений или вибраций. Такие датчики оборудуются, как правило, микропроцессорами для обработки сигналов от контактных выключателей и формирований и посылки команды тревоги на центральный

пост охраны. Контактные выключатели вибрационных датчиков по принципу действия бывают ртутными, шариковыми, пьезоэлектрическими и маятниковыми.

Датчики периметра инфраакустические устанавливаются на металлических ограждениях и улавливают низкочастотные звуковые колебания ограждений во время их преодоления. Возможны ложные срабатывания таких датчиков на уличные шумы от близко расположенных дорог.

Датчики периметра натяжного действия состоят из нескольких рядов натянутой проволоки, подсоединенной к механическим выключателям. Малейший изгиб проволоки вызывает срабатывание сигнализации. Для монтажа датчиков натяжного действия используется, как правило, колючая проволока. Выключатели устанавливаются на специальных стойках, которые отстоят друг от друга на 60 см. Проволока натягивается с усилием до 45 кг, механизм выключателя срабатывает при изгибе проволоки свыше 2 мм. Преодоление таких датчиков возможно за счет перелезания по датчиковым стойкам.

Датчики периметра электретные изготавливаются из коаксиального кабеля с радиально поляризованным диэлектриком. Такой кабель протягивается через ограждения периметра объекта. В момент преодоления ограждения происходит сотрясение кабеля и, соответственно, изменение электрического сигнала, проходящего через кабель. Как и вибрационные, электретные датчики оснащаются микропроцессорами для контроля порогового уровня срабатывания и могут быть отрегулированы на распознавание воздействий, вызываемых ветром, брошенными камнями или другими предметами, животными, птицами, вибрацией почвы от движущихся транспортных средств, градом или снегом, землетрясением, движением веток деревьев. Вибрационные и электретные датчики могут обходиться путем подкопа или преодоления сверху без их касания.

Датчики периметра электрического поля состоят из двух частей: излучателя и нескольких приемников. Обе части датчика выполнены из электрических кабелей, натянутых между столбами. Во время прохождения нарушителя между излучателем и приемниками имеет место изменение электрического поля между ними, которое и является сигналом тревоги.

Датчики сейсмические. Известны два вида датчиков этого типа. Первый, жидкостной, состоит из двух уложенных рядом в почву шлангов с жидкостью. Срабатывание таких датчиков происходит при изменении давления в одном из шлангов при прохождении нарушителя. Принцип действия датчиков второго вида основан на пьезоэлектрическом эффекте, при котором происходит изменение электрического сигнала при давлении на пьезоэлемент. Оба вида сейсмических датчиков чувствительны к посторонним вибрациям, вызываемым, например проезжающим транспортом или сильным ветром. Сейсмические датчики используются для охраны периметров территорий и зданий, устанавливаются скрытно в почву или ее покрытие, под поверхности стен и строительных конструкций.

Датчики сейсмомагнитные выполняются в виде электрического кабеля, уложенного в почву. Электрический сигнал изменяется под воздействием как сейсмических, так и магнитных возмущений, например при проходе человека и проносе им оружия. Возможны ложные срабатывания от грозовых разрядов, мощных электромоторов и реле.

Датчики ультразвуковые. Действие основано на регистрации ультразвуковых волн от нарушителя при его воздействии на элементы конструкций периметра здания или помещения. Используются как пассивные, так и активные ультразвуковые датчики. Пассивные регистрируют ультразвуковые колебания воздуха или другой среды на частотах 18—60 кГц, возникающие при попытке разрушения металлических конструкций механическим или термическим способом. Выпускается две разновидности активных ультразвуковых датчиков. В первой используются элементы конструкций периметра охраняемых помещений. При таком воздействии, как, например, разбивание оконного стекла, нарушается связь передатчика и приемника через стекло и происходит срабатывание датчика. Активные ультразвуковые датчики второго вида регистрируют изменение частоты (излучаемого датчиком сигнала) в охраняемой среде, например при открывании замка или отпиливании металлической решетки.

Датчики ультразвуковые для контроля помещений. Датчики этого типа с излучающей и приемной частями регистрируют изменение сигнала излучения, отраженного от нарушителя. Для помещений площадью до 50 м^2 могут применяться однокорпусные датчики. Большие по размерам помещения охраняются двух-

корпусными датчиками: излучатель в отдельном корпусе крепится на одной стене, а приемник (или несколько приемников) — на противоположной стене. Находящиеся в помещении крупногабаритные предметы ограничивают действие такого датчика, создавая области экранировки («мертвые зоны»), в которых датчик не реагирует на движение нарушителя.

Датчики фотоэлектрические. Работа этого вида датчиков основана на прерывании нарушителем луча света любого диапазона, сформированного соответствующим фильтром.

Доверенная вычислительная база (trusted computing base — TCB) — термин, относящийся к аппаратным, фирменным программным и просто программным механизмам защиты в компьютерной системе, обеспечивающим реализацию в этой системе избранной политики безопасности.

Доверенная компьютерная система (trusted computer system) — система, допускающая ведение безопасной обработки несортированного потока критичной информации за счет использования достаточных аппаратных и программных средств обеспечения безопасности.

Доверие к информации — отсутствие в ней подмены (несанкционированной модификации ее элементов при сохранении целостности).

Доступ (access) — 1) в обработке данных: взаимодействие между субъектом и объектом, обеспечивающее передачу информации между ними; 2) в физической безопасности: возможность входа на защищенную территорию.

Жадная программа — программа, которая монополизирует определенный ресурс сети и не дает возможность другим программам пользоваться ею.

Захватчики паролей — программы, ворующие пароли путем обманных воздействий на операционную систему.

Защита данных (data protection) — средства защиты данных от случайных или умышленных нежелательных модификаций, разрушений или разглашений.

Защита информации (ЗИ) — комплекс мероприятий, направленных на обеспечение важнейших аспектов информационной безопасности (целостности, доступности и, если нужно, конфиден-

циальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных).

Защита объектов (object protection) — средства защиты объектов типа сейфов, файлов и т. д. — того, что может быть выведено из защищенной области (protected area).

Защита персональной информации (privacy protection) — совокупность технических, административных и физических мер, реализованных с целью обеспечения безопасности и конфиденциальности записей данных, равно как и для защиты подсистем безопасности и конфиденциальности от любых случайных или преднамеренных действий, которые могут привести к затруднению, ущербу, неудобствам или несправедливости в отношении лица, о котором хранится соответствующая информация.

Защищенная область, зона (protected area) — термин, используемый для определения области, защищенной системой безопасности.

Идентификация (identification) — процесс анализа персональных, технических или организационных характеристик или кодов для получения (предоставления) доступа к компьютерным ресурсам.

Индивидуальный учет (individual accountability) — комплекс мер, за счет которых идентификация пользователя может быть использована для определения возможности доступа пользователя к машинам, материалам и т. п.; правила предоставления пользователю времени, методов и режимов доступа.

Компрометация (compromise) — утеря критичной информации, либо получение ее неавторизованными для этого субъектами (лицами, программами, процессами и т. д.).

Компьютерная безопасность (computer security) — комплекс технологических и административных мер, применяемых в отношении аппаратных средств, программ, данных и служб с целью обеспечения доступности, целостности и конфиденциальности связанных с компьютерами ресурсов; сюда же относятся и процедуры проверки выполнения системой определенных функций в строгом соответствии с их запланированным порядком работы.

Конфиденциальность (confidentiality) — некоторая классификация данных, получение либо использование которых неавторизованными для этого лицами может стать причиной серьезного ущерба для организации.

Концепция монитора ссылок (reference monitor concept) — концепция управления доступом в информационной системе, предполагающая наличие некоторой абстрактной машины (механизма), через которую осуществляется доступ обьектов к субьектам.

Критичная (sensitivies) информация — информация с различными грифами секретности; информация для служебного пользования; информация, составляющая коммерческую тайну или тайну фирмы; информация, являющаяся собственностью некоторой организации или частного лица, и т. д.

Люк (trap door) — скрытый программный или аппаратный механизм, позволяющий обойти механизмы защиты системы. Обычно это использование недокументированных точек входа (они вставляются в программы на стадиях разработки или наладки и затем при определенных условиях оказываются лишними и не удаленными) для проникновения в систему. Существует два основных типа люков: внутренние и внешние. К первым относятся некоторые внутренние элементы системы (например, дата-временное значение, счетчик и т. д.), определяющие требуемые условия; к другому типу относятся внешние элементы (например, удаленный терминал).

Маскарад — выступление одного пользователя от имени другого (присвоение прав и привилегий).

Межсетевой экран (FireWall) — устройство, программа, которые осуществляют фильтрацию данных на основе заранее заданной базы правил, что позволяет, по сравнению с традиционными операционными системами, реализовывать гораздо более гибкую политику безопасности. При комплексной фильтрации, охватывающей сетевой, транспортный и прикладной уровни, в правилах могут фигурировать сетевые адреса, количество переданных данных, операции прикладного уровня, параметры окружения (например, время) и т. п.

Методы гаммирования — способы выполнения наложения на исходный текст некоторой последовательности кодов, называемой гаммой.

Методы защиты от вирусов — общие средства защиты информации, которые полезны, также и как страховка, от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя; профилактические меры, позволяющие

уменьшить вероятность заражения вирусом; специализированные программы для защиты от вирусов.

Модификация — осуществление третьей неавторизованной стороной не только доступа к компоненту, но и манипуляции с ним. Например, модификациями являются неавторизованное изменение данных в базах данных или вообще в файлах компьютерной системы, изменение алгоритмов используемых программ с целью выполнения некоторой дополнительной незаконной обработки. Иногда модификации обнаруживаются достаточно быстро (если не сразу), но более тонкие модификации могут оставаться необнаруженными весьма длительное время;

Некритичная (несекретная) информация (unclassified) — тип данных, не требующий специальной защиты от НСД.

Объект (object) — сущность, элемент системы (т. е. запись, страница памяти, программа, принтер и т. д.), связанный с хранением или получением информации. Если субъект имеет доступ к объекту, он (субъект) исходит из того, что объект предоставит ему доступ к хранимой им информации.

Операционная безопасность данных (operational data security) — защита данных от модификации, разрушения или разглашения (случайных, неавторизованных, либо преднамеренных) во время выполнения операций ввода, обработки или вывода.

Оранжевая книга (orange book) — полное название «Department of Defence Trusted Computer System Evaluation Criteria» DOD 5200.28-STD («Критерий оценивания безопасности компьютерных систем Министерства обороны США») — государственный стандарт оценивания безопасности компьютерных систем, устанавливающий четыре иерархических класса — A, B, C и D — определенных уровней доверенности (иными словами, уверенности в безопасности) для конкретных приложений, разрабатываемых и используемых в интересах правительства.

Отслеживаемость (accountability) — возможность для ответственных лиц восстанавливать ход нарушения или попытки нарушения безопасности информационной системы.

Офицер безопасности (data security officer — DSO) — лицо, отвечающее за обеспечение безопасности обработки данных в системе и за противодействие попыткам неразрешенного использования данных.

Оценка риска (risk assessment) — методы анализа угроз и слабых сторон, известных и предполагаемых, позволяющие определить размер ожидаемого ущерба и степень его приемлемости для работы системы.

Перехват — доступ некоторой третьей неавторизованной стороны к компоненту. Примерами перехвата являются незаконное копирование программ и данных, неавторизованное чтение данных из линий связи компьютерной сети и т. д.

Период доступа (access period) — временной интервал, в течение которого действуют права доступа. В основном этот период определяется в днях или неделях.

Персональные данные — информация (зафиксированная на любом материальном носителе) о конкретном человеке, которая отождествлена или может быть отождествлена с ним. К персональным данным могут быть отнесены сведения, использование которых без согласия субъекта персональных данных может нанести вред его чести, достоинству, деловой репутации, доброму имени, иным нематериальным благам и имущественным интересам.

Персональный идентификационный номер (Personal Identification Number — PIN) — персональный код некоторого лица, обеспечивающий ему возможность входа в систему с управляемым доступом.

Подделка — добавление нарушителем некоторого фальшивого процесса в систему для выполнения нужных ему, но не учитываемых системой, действий, либо подложные записи в файлы системы или других пользователей. Например, зная формат записи в файле, на основании которого в некоторой организации начисляется зарплата, вполне можно занести в этот файл поддельную запись. При начислении зарплаты эта запись будет обрабатываться (если все сделано достаточно тонко) наравне с законными записями, при этом деньги могут переводиться на счет злоумышленника.

Полиморфные вирусы — вирусы, модифицирующие свой код в зараженных программах таким образом, что два экземпляра одного и того же вируса могут не совпадать ни в одном бите.

Полномочное управление доступом (mandatory access control) — ограничение доступа к определенным объектам, установленное на

основании выявленной степени критичности информации, содержащейся в данном объекте. При этом обеспечивается «прозрачность» данного объекта для всех неавторизованных лиц, т. е. объект как бы невидим для них. Управление является полномочным, поскольку субъект с конкретными правами доступа не может передавать эти права другому субъекту.

Проволочные сетки используются для обнаружения проникновения в помещение через стены, полы, потолки, двери, окна и другие конструкции. Охраняемая поверхность покрывается сеткой из электрического провода с размерами ячеек 10—15 см. Механическое разрушение ячеек сетки приводит к разрыву проводников и, соответственно, к разрыву электрической цепи. Для маскировки сетка датчика может покрываться обоями или облицовочными материалами.

Программы доктора-ревизоры не только обнаруживают изменения в файлах и системных областях дисков, но и могут в случае изменений автоматически вернуть их в исходное состояние. Такие программы могут быть гораздо более универсальными, чем программы-доктора, поскольку при лечении они используют заранее сохраненную информацию о состоянии файлов и областей дисков. Это позволяет им вылечивать файлы даже от тех вирусов, которые не были созданы на момент написания программы. Но они могут лечить не от всех вирусов, а только от тех, которые используют «стандартные», известные на момент написания программы, механизмы заражения файлов.

Программы-вакцины, или *иммунизаторы*, модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными.

Программы-детекторы позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов. Эти программы проверяют, имеется ли в файлах на указанном пользователем диске специфическая для данного вируса комбинация байтов. При ее обнаружении в каком-либо файле на экран выводится соответствующее сообщение. Многие детекторы имеют режимы лечения или уничтожения зараженных файлов.

Программы-ревизоры имеют две стадии работы — сначала они запоминают сведения о состоянии программ и системных областей дисков (загрузочного сектора и сектора с таблицей разбиения

жесткого диска). Предполагается, что в этот момент программы и системные области дисков не заражены. После этого с помощью программы-ревизора можно в любой момент сравнить состояние программ и системных областей дисков с исходным. О выявленных несоответствиях сообщается пользователю.

Программы-фильтры располагаются резидентно в оперативной памяти компьютера и перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователя. Пользователь может разрешить или запретить выполнение соответствующей операции. Некоторые программы-фильтры не «ловят» подозрительные действия, а проверяют вызываемые на выполнение программы на наличие вирусов. Это замедляет работу компьютера. Однако преимущества использования программ-фильтров весьма значительны — они позволяют обнаружить многие вирусы на самой ранней стадии, когда вирус еще не успел размножиться и что-либо испортить. Тем самым можно свести убытки от вируса к минимуму.

Простейшие вирусы — паразитические — изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены.

Профессиональная тайна — защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, распространение которой может нанести ущерб правам и законным интересам другого лица (доверителя), доверившего эти сведения, и не являющаяся государственной или коммерческой тайной.

Процедурная безопасность (procedural security) — ограничения со стороны управляющих органов; операционные, административные и учетные процедуры; соответствующие способы управления, используемые с целью обеспечения требуемого уровня безопасности для критичных к защите информации данных.

Радужная серия (rainbow series) — опубликованные стандарты безопасности, используемые Министерством обороны США, названные каждый по цвету обложки. Например, «красная книга» описывает вопросы безопасности в сетях, «желтая книга» —

безопасность паролей, «оранжевая книга» — доверенные компьютерные системы и т. д.

Резидентный вирус при заражении (инфицировании) компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера. *Нерезидентные вирусы* не заражают память компьютера и являются активными ограниченное время.

Риск (risk) — возможность проведения злоумышленником успешной атаки в отношении конкретной слабой стороны системы.

Сборка мусора, повторное использование объекта (object reuse) — предоставление некоторому субъекту доступа к магнитной среде памяти, содержащей один и более объектов. Будучи доступной для субъекта, магнитная среда может в то же время содержать остаточные следы данных от объекта, содержавшегося на этом месте ранее.

Сетевые вирусы распространяются по различным компьютерным сетям. *Файловые вирусы* внедряются главным образом в исполняемые модули, т. е. в файлы, имеющие расширения COM и EXE. Файловые вирусы могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах, они никогда не получают управление и, следовательно, теряют способность к размножению. *Загрузочные вирусы* внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Record). *Файлово-загрузочные* вирусы заражают как файлы, так и загрузочные сектора дисков.

Скрытый канал (covert channel) — канал коммуникации, позволяющий процессу передавать информацию путем, нарушающим политику безопасности, реализуемую в данной системе.

След контроля (audit trail) — журнал записей о транзакциях, выполняемых в системе, которые (записи) в совокупности документируют ход обработки информации в системе, что в свою очередь позволяет проследить (провести трассировку) его вперед — от исходных транзакция до создаваемых в процессе их работы записей и/или отчетов — а также назад — от конечных записей/отчетов до исходных транзакций. Последовательность

записей, составляющих след контроля, позволяет определить источники возникновения транзакций в системе и последовательность их выполнения системой.

Служебная тайна — защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости.

Субъект (subject) — активная сущность (процесс, пользователь, устройство и т. д.), вызывающая образование информационного потока между объектами или изменения состояния системы.

Терапия — дезактивация конкретного вируса в зараженных программах специальной программой-фагом или восстановление первоначального состояния программ путем «выкусывания» всех экземпляров вируса из каждого зараженного файла или диска с помощью этой программы.

Троянский конь (trojan horse) — компьютерная программа, имитирующая выполнение или реально выполняющая некоторую полезную функцию, но в то же время выполняющая и некоторую дополнительную (скрытую) функцию, позволяющую обойти систему защиты за счет скрытого использования законной авторизации вызывающего процесса. В ней содержится недокументированный (скрытый) модуль, который не вызывает подозрения и в дальнейшем выполняет недопустимые действия.

Угроза (threat) — характеристики, свойства системы и окружающей ее среды, которые в соответствующих условиях могут вызвать появление опасного события. Для компьютерной системы это условия, представляющие потенциальную возможность нанесения ущерба компьютерной системе. Атаки — частный вид угроз, так же как и стихийные бедствия, человеческие ошибки, программные сбои и т. д.

Угроза доступа к остаточным данным в оперативной и внешней памяти компьютера является одной из основных угроз хищения информации. Под остаточной информацией понимаются данные, оставшиеся в освободившихся участках оперативной и внешней памяти компьютера.

Управление в терминологии безопасности называется защитный механизм (действие, устройство, процедура, технология и т. д.), уменьшающий уязвимость компьютерной системы.

Управление доступом (access control) — в сетях или их компонентах: задачи, выполняемые аппаратурой, программным обеспечением и администрацией, с целью отслеживания выполняемых в системе операций, целостности данных, доступа и модификаций системных записей, выполнения пользователями идентификации и предоставление пользователям доступа.

Ущерб — не только явное повреждение какого-либо из компонентов компьютерной системы, но и приведение компонентов системы в неработоспособное состояние (например, обесточивание помещения, в котором находятся аппаратные средства), и различного рода утечки информации (например, незаконное копирование программ, получение конфиденциальных данных), и изменение некоторых физических и логических характеристик компьютерной системы (например, неавторизованное добавление записей в системные файлы, повышение загрузки системы за счет запуска дополнительного неучтенного процесса/программы и т. д.). Определение возможного ущерба компьютерной системы — дело весьма сложное, зависящее от многих условий. Следует понимать, что ущерб компьютерной системы — понятие также достаточно широкое.

Уязвимость (vulnerability) — любая ошибка или слабая проработка (например, неопределенность условий обработки), существующая в системе. Уязвимость создает предпосылки для нарушения безопасности системы. При этом уязвимость существует независимо от того, известны или нет какие-либо угрозы.

Физическая безопасность (physical security) — совокупность охраны, замков, пропусков и других средств управления физическим доступом к компьютеру и периферии. Термин употребляется также в отношении средств защиты помещений, в которых находится оборудование, от пожара, стихийных бедствий и катастроф.

Физическая целостность информации — отсутствие искажений или уничтожения элементов информации.

Философия защиты (protection philosophy) — общая схема системы в целом, позволяющая видеть использование механизмов защиты. При этом для демонстрации того, как данные механизмы

защищают систему, можно использовать как формальные, так и неформальные методы.

Целостность (integrity) — состояние, в котором данные или программы используются установленным образом, обеспечивающим устойчивую работу системы; автоматическое восстановление в случае обнаружения системой потенциальной ошибки; автоматическое использование альтернативных компонентов вместо вышедших из строя. Примером является дублирование важных файлов с тем, чтобы в случае обнаружения ошибки или утери оригинального файла использовать его копию. Другим примером является поддержание двух и более путей доступа к устройству хранения.

Целостность данных (data integrity) — состояние, при котором данные, представленные в компьютере, в точности соответствуют данным в исходных документах и при этом не могут быть подвержены неумышленным или умышленным искажениям или разрушениям.

Целостность системы (system integrity) — состояние системы, в котором существует полная гарантия того, что при любых условиях компьютерная система базируется на логически завершенных аппаратных и программных средствах, обеспечивающих работу защитных механизмов, логическую корректность и достоверность операционной системы и целостность данных.

Червь (worm) — программа, внедряемая в систему, часто злонамеренно, и прерывающая ход обработки информации в системе. Это вредоносные программы, которые распространяются через сеть, не оставляя своей копии на магнитном носителе, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии. В отличие от вирусов, червь обычно не искажает файлы данных или программы. Обычно червь выполняется, оставаясь необнаруженным, и затем самоуничтожается.

Экранирование — экранирование как сервис безопасности выполняет следующие функции: разграничение межсетевого доступа путем фильтрации передаваемых данных; преобразование передаваемых данных.

Экспозиция — форма возможной потери или ущерба для компьютерной системы. Например, экспозициями считаются неавторизованный доступ к данным или противодействие авторизованному использованию компьютерной системы.

Adware (иногда — Adbot) — программы назойливого рекламирования. Они рода демонстрируют рекламные объявления, обычно в виде всплывающих окон. Технология выполнения этой простой задачи может изменяться в самых широких пределах, а степень воздействия на систему пользователя — варьироваться от приемлемого уровня рекламы до отказа в обслуживании из-за множества открывающихся окон и переадресовок браузера.

Browser hijacker (налетчик, перехватчик браузера) — разновидность шпионских программ, которая изменяет домашнюю страницу и другие настройки браузера так, чтобы в дальнейшем установить на компьютере шпионские программы для несанкционированного съема и передачи информации. Некоторые разновидности таких программ перехватывают запросы и переадресуют их на посторонние страницы. Таким образом, пользователь может попасть на сайт, который он никогда бы не стал посещать по доброй воле.

Computer surveillance — технические и программные средства наблюдения за компьютерами (отслеживания деятельности пользователя, информационного трафика и пр.), а также использование компьютера для наблюдения за обстановкой и несанкционированной передачи собранной информации «на сторону». Разновидности — keylogger, tracking software.

DOD Guidelines for Computer Security — совокупность правил, установленных Министерством обороны США (DOD — Department of Defence) для определения степени безопасности узлового программного обеспечения — операционных систем, узловых средств контроля доступа и т. д.

Formal securiy policy model — формальная модель политики безопасности — политика безопасности, выраженная точным математическим образом, включающим начальное состояние системы, способы перехода системы из одного состояния в другое и определение «безопасного» состояния системы.

Hacking — неавторизованная попытка доступа к базе данных узла. Часто этот термин используется в отношении лиц, пытающихся получить доступ к узловой базе данных с удаленного узла за счет обхода (обмана) средств контроля доступа в сети.

Hosts file (указатель хостов, серверов) — текстовый файл, отражающий связь между именем сервера и его IP-адресом (например,

rhino.acme.com — 102.54.94.97), что позволяет осуществлять доступ к серверам, даже если система доменных имен (DNS) не функционирует. Файл размещается в служебных каталогах ОС (например, для Windows XP это c:\windows\system32\drivers\etc). Атака шпионских программ может привести к замещению содержания файла и установке ссылок на нежелательные Web-сайты.

HTTP cookies (индексы навигации), иногда именуемые web cookies, tracking cookies или просто cookies, представляют собой небольшие (до 4 Кбайт) текстовые файлы, посылаемые с сервера на Web-браузер пользователя, а затем передаваемые обратно при каждом обращении к серверу. Используются для аутентификации и персонализации пользователей, отслеживания навигации и сохранения специфической для пользователя информации (в частности, для формирования «электронной корзины закупок», куда пользователь «складывает» свои приобретения в Internet-магазинах).

Keylogger (клавиатурный шпион) — программная закладка (или аппаратный «жучок»), которая записывает нажатия клавиш на компьютере, фиксируя пароли, переписку по электронной почте и так далее.

Malware (сокращение от *malicious software* — вредоносное программное средство). Этот термин может относиться к конкретной программе (наподобие вируса или червя), наносящей реальный ущерб, или обозначать любое нежелательное программное обеспечение.

OMBA-123 — директива федерального правительства США, определяющая, что при выполнении любыми правительственными органами или любыми компаниями работ для правительства с использованием компьютеров подрядчики должны составить краткий план идентификации и защиты ресурсов их информационной системы.

Privacy Act of 1974 — закон о защите персональной информации 1974 года (США) — касается прав лица управлять или влиять на тип и объем информации, которая может быть о нем собрана и сохранена, а также на то, кому эта информация может быть передана.

Scumware — (программы переадресации/«переманивания»). Программное средство, которое тайком проникает на компьютер

пользователя и при открытии определенных Web-сайтов демонстрирует всплывающие окна с рекламой в попытке переадресовать пользователя на другой (конкурирующий или связанный) сайт. Фактически Scumware позволяет диверсионными методами воровать трафик с часто посещаемых сайтов.

SpyWare — шпионское программное обеспечение, которое атакует компьютеры с целью кражи личной информации, а также, чтобы получить доступ к идентификационным данным. Исследование IDC показало, что на двух третях компьютеров установлены программы-шпионы, а в 2003 г. на приобретение антишпионского программного обеспечения (AntiSpyWare) было потрачено 12 млн долл., и по предварительным прогнозам в 2008 г. эта сумма может достигнуть 305 млн долл.

Stopbadware.org — некоммерческая организация, целью которой является борьба с вредоносными программами (известными как malicious software/malware или badware). Учредителями организации являются Гарвардская юридическая школа и Оксфордский Internet-институт, поддержку осуществляют такие структуры, как Google, Sun Microsystems и пр.

Trackers — элементы программных средств, которые собирают сведения о пользователе. Опасны, поскольку среди собранной ими информации может оказаться конфиденциальная или составляющая факт вторжения в частную жизнь (privacy violation).

Оглавление

Введение 3

Глава 1. ОБЩИЕ ПРОБЛЕМЫ БЕЗОПАСНОСТИ. РОЛЬ И МЕСТО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 10

1.1. Национальные интересы и безопасность. 10

1.2. Информационная безопасность 29

1.3. Защита информации (ЗИ). 56

Глава 2. ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОБРАБОТКИ ДАННЫХ 83

2.1. Предмет и объекты защиты информации в автоматизированных системах обработки данных (АСОД) 83

2.2. Элементы и объекты защиты в АСОД. 88

2.3. Функции и задачи защиты информации 105

2.4. Методы и системы защиты информации. 111

Глава 3. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ 140

3.1. Криптология и основные этапы ее развития 140

3.2. Методы криптографического преобразования данных. . . 146

3.3. Проблемы реализации методов криптографической защиты в АСОД 175

Глава 4. ЗАЩИТА ИНФОРМАЦИИ В ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРАХ 188

4.1. Особенности защиты информации в персональных ЭВМ 188

4.2. Защита ПК от несанкционированного доступа 195

4.3. Вредоносные закладки в ПК и борьба с ними. 209

Глава 5. КОМПЬЮТЕРНЫЕ ВИРУСЫ И АНТИВИРУСНЫЕ ПРОГРАММЫ 248

5.1. Компьютерный вирус 248

5.2. Методы защиты. Антивирусы 263

5.3. Некоторые примеры антивирусных программ 275

Глава 6. ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В СЕТЯХ ЭВМ. 302

6.1. Сети ЭВМ — построение и использование 302

6.2. Цели, функции и задачи защиты информации в сетях ЭВМ 323

6.3. Архитектура механизмов защиты информации в сетях ЭВМ 337

Глава 7. ТЕХНИЧЕСКИЕ СРЕДСТВА И КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ 363

7.1. Технические средства защиты 363

7.2. Комплексный подход к обеспечению безопасности. 383

Заключение 402

Список литературы 404

Глоссарий (терминологический словарь) 407

Партыка Татьяна Леонидовна
Попов Игорь Иванович

Информационная безопасность

Учебное пособие

Редактор *В. М. Голубев*
Корректор *А. В. Волковицкая*
Компьютерная верстка *И. В. Кондратьевой*
Рисунок на обложке *А. Скотаренко*
Оформление серии *П. Родькина*

Сдано в набор 20.01.2008. Подписано в печать 13.05.2008. Формат 60×90/16.
Гарнитура «Таймс». Усл. печ. л. 27,0. Уч.-изд. л. 27,6.
Бумага офсетная. Тираж 3000 экз.
Заказ № 8295.

Издательство «ФОРУМ»
101000, Москва — Центр, Колпачный пер., д. 9а
Тел./факс: (495) 625-32-07, 625-52-43
E-mail: mail@forum-books.ru

По вопросам приобретения книг обращайтесь:

Отдел продаж издательства «ФОРУМ»
101000, Москва — Центр, Колпачный пер., д. 9а
Тел./факс: (495) 625-32-07, 625-52-43
E-mail: natali@forum-books.ru

Отдел продаж «ИНФРА-М»
127282, Москва, ул. Полярная, д. 31в
Тел.: (495) 380-05-40 (доб. 252)
Факс: (495) 363-92-12
E-mail: ati@infra-m.ru

Центр комплектования библиотек
119019, Москва, ул. Моховая, д. 16
(Российская государственная библиотека, кор. К)
Тел.: (495) 202-93-15

Магазин «Библиосфера» (розничная продажа)
109147, Москва, ул. Марксистская, д. 9
Тел.: (495) 670-52-18, (495) 670-52-19

Отпечатано с предоставленных диапозитивов
в ОАО «Тульская типография». 300600, г. Тула, пр. Ленина, 109.