П. Б. ХОРЕВ

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Рекомендовано
Учебно-методическим объединением вузов
по университетскому политехническому образованию
в качестве учебного пособия для студентов высших учебных заведений,
обучающихся по направлению 230100 (654600)
«Информатика и вычислительная техника»

Москва
ACADEMIA
2005

УДК 681.3.067(075.8)
ББК 32.973-018.2я73
Х792

Рецензенты:
профессор кафедры вычислительных машин, систем и сетей МЭИ (ТУ),
д-р техн. наук *Ю. Н. Мельников*;
доцент кафедры вычислительных машин, комплексов,
систем и сетей МГТУ ГА, канд. техн. наук *А. И. Терентьев*

Хорев П. Б.

Х792 Методы и средства защиты информации в компьютерных системах: Учеб. пособие для студ. высш. учеб. заведений / Павел Борисович Хорев. — М.: Издательский центр «Академия», 2005. — 256 с.

ISBN 5-7695-1839-1

Основное внимание в учебном пособии уделено программным и программно-аппаратным методам и средствам защиты информации. Рассмотрены, в частности, модели безопасности, используемые в защищенных версиях операционной системы Windows (в том числе использование функций криптографического интерфейса приложений CryptoAPI) и операционных системах «клона» Unix.

Для студентов высших учебных заведений. Может быть полезно специалистам в области информационной безопасности.

УДК 681.3.067(075.8)
ББК 32.973-018.2я73

ISBN 5-7695-1839-1

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ

Проблема защиты информации: надежное обеспечение ее сохранности и установленного статуса использования — является одной из важнейших проблем современности.

Еще 25...30 лет назад задача защиты информация могла быть эффективно решена с помощью организационных мер (выполнения режимных мероприятий, использования средств охраны и сигнализации) и отдельных программно-аппаратных средств разграничения доступа и шифрования. Этому способствовала концентрация информационных ресурсов и средств для их обработки на автономно функционирующих вычислительных центрах. Появление персональных ЭВМ, локальных и глобальных компьютерных сетей, спутниковых каналов связи, эффективных средств технической разведки и получения конфиденциальной информации существенно обострило проблему защиты информации.

Особенностями современных информационных технологий, прямо или косвенно влияющими на безопасность информации, являются:

- увеличение числа автоматизированных процедур в системах обработки данных и важности принимаемых на их основе решений;
- территориальная распределенность компонентов компьютерных систем и передача информации между этими компонентами;
- усложнение используемых программных и аппаратных средств компьютерных систем;
- накопление и долговременное хранение больших массивов данных на электронных носителях, зачастую не имеющих твердых копий;
- интеграция в единых базах данных информации различного назначения и различных режимов доступа;
- непосредственный доступ к ресурсам компьютерных систем большого количества пользователей различных категорий и с различными полномочиями в системе;
- рост стоимости ресурсов компьютерных систем.

Рост количества и качества угроз безопасности информации в компьютерных системах не всегда приводит к адекватному ответу в виде создания надежных систем защиты информации и безопасных информационных технологий. В большинстве коммерческих и госу-

дарственных организаций, не говоря уже об отдельных пользователях, в качестве средств защиты применяются только антивирусные программы, не всегда своевременно обновляемые, и разграничение прав пользователей компьютерной системы на основе паролей.

В связи с этим следует не только увеличивать количество специалистов в области информационной безопасности и защиты информации, но и обучать современным методам и средствам защиты информации специалистов других сфер — в первую очередь специалистов в области информатики и вычислительной техники. Решению этой задачи и посвящено данное учебное пособие.

В первой главе кратко изложена сущность комплексного подхода к обеспечению информационной безопасности компьютерных систем. Поскольку последующие главы книги посвящены в основном программно-аппаратным и криптографическим методам и средствам защиты информации, в первой главе излагаются основы организационной, правовой и инженерно-технической защиты информации.

Во второй главе рассмотрены методы и средства защиты информации от локального и удаленного несанкционированного доступа к информации в компьютерных системах на основе аутентификации пользователей и процессов, а также применения специализированных протоколов типа S/Key, CHAP и Kerberos.

В третьей главе рассмотрены методы и средства защиты информации от несанкционированного доступа к ней в операционных системах Windows и Unix. Рассмотрены также особенности дискреционного и мандатного управления доступом к объектам компьютерных систем. К особенностям представленного в этой главе материала относится включение в него анализа методов и средств защиты в открытых версиях операционной системы Windows (Windows 9x/ME/XP Home Edition), сведений об основных функциях привилегированного режима (режима администратора) из набора Windows API, сведений о подсистемах аудита событий безопасности.

В четвертой главе рассмотрены методы симметричной и асимметричной криптографии и их применение при решении задачи защиты информации в компьютерных системах. В отдельный раздел этой главы вынесен вопрос об основах современной компьютерной стеганографии.

В пятой главе изложены основы криптографического интерфейса приложений Windows (CryptoAPI) и применения его функций для задач обеспечения конфиденциальности, аутентичности и целостности хранимых и передаваемых данных. Отдельно рассмотрены вопросы защиты документов Microsoft Office и шифрующая файловая система Windows, базирующиеся на CryptoAPI.

В шестой главе описаны методы и средства защиты информации от вредоносных программ — компьютерных вирусов и про-

граммных закладок. Приведена классификация вредоносных программ, методов и средств защиты от них.

В седьмой главе изложены методы защиты программного обеспечения и других информационных ресурсов от их несанкционированного использования и копирования (защиты авторских прав).

Поскольку данное учебное пособие предназначено, в первую очередь, для студентов, обучающихся по специальностям группы «Информатика и вычислительная техника», автор включил в него достаточное количество примеров программ, иллюстрирующих использование различных методов и средств защиты информации.

Автор выражает искреннюю признательность коллегам по кафедре информационной безопасности Московского государственного социального университета, а также жене и дочери за помощь и поддержку в период подготовки учебного пособия.

ГЛАВА 1

КОМПЛЕКСНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Основные понятия защиты информации

Под *информацией*, применительно к задаче ее защиты, понимают сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. В зависимости от формы представления информация может быть разделена на речевую, телекоммуникационную и документированную.

Речевая информация возникает в ходе ведения в помещениях разговоров, работы систем связи, звукоусиления и звуковоспроизведения. *Телекоммуникационная* информация циркулирует в технических средствах обработки и хранения информации, а также в каналах связи при ее передаче. К *документированной* информации, или *документам*, относят информацию, представленную на материальных носителях вместе с идентифицирующими ее реквизитами.

К *информационным процессам* относят процессы сбора, обработки, накопления, хранения, поиска и распространения информации.

Под *информационной системой* понимают упорядоченную совокупность документов и массивов документов и информационных технологий, реализующих информационные процессы.

Информационными ресурсами называют документы и массивы документов, существующие отдельно или в составе информационных систем.

Процесс создания оптимальных условий для удовлетворения информационных потребностей граждан, организаций, общества и государства в целом называют *информатизацией*.

Информацию разделяют на открытую и ограниченного доступа. К информации ограниченного доступа относятся государственная тайна и конфиденциальная информация. В соответствии с российским законодательством к конфиденциальной относится следующая информация:

- служебная тайна (врачебная, адвокатская, тайна суда и следствия и т. п.);
- коммерческая тайна;
- персональные данные (сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность).

Информация является одним из объектов гражданских прав, в том числе и прав собственности, владения и пользования. *Собственник* информационных ресурсов, систем и технологий — это субъект с полномочиями владения, пользования и распоряжения указанными объектами. *Владельцем* информационных ресурсов, систем и технологий является субъект с полномочиями владения и пользования указанными объектами. Под *пользователем* информации будем понимать субъекта, обращающегося к информационной системе за получением необходимой ему информации и пользующегося ею.

К *защищаемой* относится информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Зашитой информации называют деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Под *утечкой* понимают неконтролируемое распространение защищаемой информации путем ее разглашения, несанкционированного доступа к ней и получения разведками. *Разглашение* — это доведение защищаемой информации до неконтролируемого количества получателей информации (например, публикация информации на открытом сайте в сети Интернет или в открытой печати). *Несанкционированный доступ* — получение защищаемой информации заинтересованным субъектом с нарушением правил доступа к ней.

Несанкционированное воздействие на защищаемую информацию — воздействие с нарушением правил ее изменения (например, намеренное внедрение в защищаемые информационные ресурсы вредоносного программного кода или умышленная подмена электронного документа).

Под *непреднамеренным воздействием* на защищаемую информацию понимают воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств, природных явлений, иных нецеленаправленных воздействий (например, уничтожение документов в результате отказа накопителя на жестком магнитном диске компьютера).

Целью защиты информации (ее желаемым результатом) является предотвращение ущерба собственнику, владельцу или пользователю информации. Под *эффективностью* защиты информации понимают степень соответствия результатов защиты информации поставленной цели. *Объектом защиты* может быть информация, ее носитель или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью.

Под *качеством информации* понимают совокупность свойств, обусловливающих пригодность информации удовлетворять опре-

деленные потребности ее пользователей в соответствии с назначением информации. Одним из показателей качества информации является ее *защищенность* — поддержание на заданном уровне тех параметров информации, которые характеризуют установленный статус ее хранения, обработки и использования.

Основными характеристиками защищаемой информации являются конфиденциальность, целостность и доступность. *Конфиденциальность* информации — это известность ее содержания только имеющим соответствующие полномочия субъектам. Конфиденциальность является субъективной характеристикой информации, связанной с объективной необходимостью защиты законных интересов одних субъектов от других.

Шифрованием информации называют процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов. Результат шифрования информации называют *шифротекстом*, или *криптограммой*. Обратный процесс восстановления информации из шифротекста называют *расшифрованием* информации. Алгоритмы, используемые при шифровании и расшифровании информации, обычно не являются конфиденциальными, а конфиденциальность шифротекста обеспечивается использованием при шифровании дополнительного параметра, называемого *ключом шифрования*. Знание ключа шифрования позволяет выполнить правильное расшифрование шифротекста.

Целостностью информации называют неизменность информации в условиях ее случайного и (или) преднамеренного искажения или разрушения. Целостность является частью более широкой характеристики информации — ее достоверности, включающей помимо целостности еще полноту и точность отображения предметной области.

Хешированием информации называют процесс ее преобразования в хеш-значение фиксированной длины (дайджест). Одним из применений хеширования является обеспечение целостности информации.

Под *доступностью* информации понимают способность обеспечения беспрепятственного доступа субъектов к интересующей их информации. *Отказом в обслуживании* называют состояние информационной системы, при котором блокируется доступ к некоторому ее ресурсу. Совокупность информационных ресурсов и системы формирования, распространения и использования информации называют *информационной средой* общества.

Под *информационной безопасностью* понимают состояние защищенности информационной среды, обеспечивающее ее формирование и развитие.

Политика безопасности — это набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа.

Целью данного учебного пособия является представление методов и средств защиты информации в компьютерных системах. *Компьютерной*, или *автоматизированной*, системой обработки информации называют организационно-техническую систему, включающую в себя:

- технические средства вычислительной техники и связи;
- методы и алгоритмы обработки информации, реализованные в виде программных средств;
- информацию (файлы, базы данных) на различных носителях;
- обслуживающий персонал и пользователей, объединенных по организационно-структурному, тематическому, технологическому или другим признакам.

1.2. Угрозы информационной безопасности и каналы утечки информации

Под *угрозой* безопасности информации в компьютерной системе (КС) понимают событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.

Уязвимость информации — это возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

Атакой на КС называют действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости. Иначе говоря, атака на КС является реализацией угрозы безопасности информации в ней.

Угрозы информационной безопасности могут быть разделены на угрозы, не зависящие от деятельности человека (*естественные* угрозы физических воздействий на информацию стихийных природных явлений), и угрозы, вызванные человеческой деятельностью (*искусственные* угрозы), которые являются гораздо более опасными.

Искусственные угрозы исходя из их мотивов разделяются на *непреднамеренные* (случайные) и *преднамеренные* (умышленные).

К непреднамеренным угрозам относятся:

- ошибки в проектировании КС;
- ошибки в разработке программных средств КС;
- случайные сбои в работе аппаратных средств КС, линий связи, энергоснабжения;
- ошибки пользователей КС;
- воздействие на аппаратные средства КС физических полей других электронных устройств (при несоблюдении условий их электромагнитной совместимости) и др.

К умышленным угрозам относятся:

• несанкционированные действия обслуживающего персонала КС (например, ослабление политики безопасности администратором, отвечающим за безопасность КС);

• несанкционированный доступ к ресурсам КС со стороны пользователей КС и посторонних лиц, ущерб от которого определяется полученными нарушителем полномочиями.

В зависимости от целей преднамеренных угроз безопасности информации в КС угрозы могут быть разделены на три основные группы:

• угроза нарушения конфиденциальности, т.е. утечки информации ограниченного доступа, хранящейся в КС или передаваемой от одной КС к другой;

• угроза нарушения целостности, т.е. преднамеренного воздействия на информацию, хранящуюся в КС или передаваемую между КС (заметим, что целостность информации может быть также нарушена, если к несанкционированному изменению или уничтожению информации приводит случайная ошибка в работе программных или аппаратных средств КС; санкционированным является изменение или уничтожение информации, сделанное уполномоченным лицом с обоснованной целью);

• угроза нарушения доступности информации, т.е. отказа в обслуживании, вызванного преднамеренными действиями одного из пользователей КС (нарушителя), при котором блокируется доступ к некоторому ресурсу КС со стороны других пользователей КС (постоянно или на большой период времени).

Опосредованной угрозой безопасности информации в КС является угроза раскрытия параметров подсистемы защиты информации, входящей в состав КС. Реализация этой угрозы дает возможность реализации перечисленных ранее непосредственных угроз безопасности информации.

Результатом реализации угроз безопасности информации в КС может быть утечка (копирование) информации, ее утрата (разрушение) или искажение (подделка), блокирование информации. Поскольку сложно заранее определить возможную совокупность угроз безопасности информации и результатов их реализации, модель потенциальных угроз безопасности информации в КС должна создаваться совместно собственником (владельцем) КС и специалистами по защите информации на этапе проектирования КС. Созданная модель должна затем уточняться в ходе эксплуатации КС.

Рассмотрим возможные каналы утечки информации в КС. *Косвенными* каналами утечки называют каналы, не связанные с физическим доступом к элементам КС:

• использование подслушивающих (радиозакладных) устройств;

• дистанционное видеонаблюдение;

• перехват побочных электромагнитных излучений и наводок (ПЭМИН).

Побочные электромагнитные излучения создаются техническими средствами КС при обработке информации, существуют в диапазоне от единиц герц до 1,5 ГГц и могут распространять обрабатываемую информацию с дальностью до 1 км. Наиболее опасными с точки зрения ПЭМИН являются дисплеи, кабельные линии связи, накопители на магнитных дисках, матричные принтеры. Для перехвата ПЭМИН используется специальная портативная аппаратура, включающая в себя широкополосный автоматизированный супергетеродинный приемник с устройством регистрации информации на магнитном носителе и (или) дисплеем.

Побочные электромагнитные наводки представляют собой сигналы в цепях электропитания и заземления аппаратных средств КС и в находящихся в зоне воздействия ПЭМИН работающих аппаратных средств КС кабелях вспомогательных устройств (звукоусиления, связи, времени, сигнализации), металлических конструкциях зданий, сантехническом оборудовании. Эти наведенные сигналы могут выходить за пределы зоны безопасности КС.

Другим классом каналов утечки информации являются *непосредственные* каналы, связанные с физическим доступом к элементам КС. К непосредственным каналам утечки, не требующим изменения элементов КС, относятся:

• хищение носителей информации;

• сбор производственных отходов с информацией (бумажных и магнитных носителей);

• намеренное копирование файлов других пользователей КС;

• чтение остаточной информации после выполнения заданий других пользователей (областей оперативной памяти, удаленных файлов, ошибочно сохраненных временных файлов);

• копирование носителей информации;

• намеренное использование для несанкционированного доступа к информации незаблокированных терминалов других пользователей КС;

• маскировка под других пользователей путем похищения их идентифицирующей информации (паролей, карт и т. п.);

• обход средств разграничения доступа к информационным ресурсам вследствие недостатков в их программном обеспечении и др.

К непосредственным каналам утечки, предполагающим изменение элементов КС и ее структуры, относятся:

• незаконное подключение специальной регистрирующей аппаратуры к устройствам или линиям связи (пассивное для фиксации и сохранения передаваемых данных или активное для их уничтожения, искажения или подмены);

• злоумышленное изменение программ для выполнения ими несанкционированного копирования информации при ее обработке;

• злоумышленный вывод из строя средств защиты информации.

Пассивное подключение нарушителя к устройствам или линиям связи легко предотвратить (например, с помощью шифрования передаваемой информации), но невозможно обнаружить. Активное подключение, напротив, легко обнаружить (например, с помощью хеширования и шифрования передаваемой информации), но невозможно предотвратить.

Помимо утечки информации в КС возможны также ее несанкционированное уничтожение или искажение (например, заражение компьютерными вирусами), а также несанкционированное использование информации при санкционированном доступе к ней (например, нарушение авторских прав владельцев или собственников программного обеспечения или баз данных).

Наличие в КС значительного числа потенциальных каналов утечки информации является объективным фактором и обусловливает уязвимость информации в подобных системах с точки зрения ее несанкционированного использования.

Поскольку наиболее опасные угрозы информационной безопасности вызваны преднамеренными действиями нарушителя, которые в общем случае являются неформальными, проблема защиты информации относится к формально не определенным проблемам. Отсюда следуют два основных вывода:

• надежная защита информации в КС не может быть обеспечена только формальными методами (например, только программными и аппаратными средствами);

• защита информации в КС не может быть абсолютной.

При решении задачи защиты информации в КС необходимо применять так называемый системно-концептуальный подход. В соответствии с ним решение задачи должно подразумевать:

• системность целевую, при которой защищенность информации рассматривается как составная неотъемлемая часть ее качества;

• системность пространственную, предполагающую взаимосвязанность защиты информации во всех элементах КС;

• системность временную, предполагающую непрерывность защиты информации;

• системность организационную, предполагающую единство организации всех работ по защите информации в КС и управления ими.

Концептуальность подхода к решению задачи защиты информации в КС предусматривает ее решение на основе единой концепции (совокупности научно обоснованных решений, необхо-

димых и достаточных для оптимальной организации защиты информации в КС).

Обеспечение информационной безопасности КС является непрерывным процессом, целенаправленно проводимым на всех этапах ее жизненного цикла с комплексным применением всех имеющихся методов и средств.

Существующие методы и средства защиты информации можно подразделить на четыре основные группы:

- методы и средства организационно-правовой защиты информации;
- методы и средства инженерно-технической защиты информации;
- криптографические методы и средства защиты информации;
- программно-аппаратные методы и средства защиты информации.

1.3. Организационно-правовое обеспечение информационной безопасности

К методам и средствам *организационной* защиты информации относятся организационно-технические и организационно-правовые мероприятия, проводимые в процессе создания и эксплуатации КС для обеспечения защиты информации. Эти мероприятия должны проводиться при строительстве или ремонте помещений, в которых будет размещаться КС; проектировании системы, монтаже и наладке ее технических и программных средств; испытаниях и проверке работоспособности КС.

Основные свойства методов и средств организационной защиты:

- обеспечение полного или частичного перекрытия значительной части каналов утечки информации (например, хищения или копирования носителей информации);
- объединение всех используемых в КС средств в целостный механизм защиты информации.

Методы и средства организационной защиты информации включают в себя:

- ограничение физического доступа к объектам КС и реализация режимных мер;
- ограничение возможности перехвата ПЭМИН;
- разграничение доступа к информационным ресурсам и процессам КС (установка правил разграничения доступа, шифрование информации при ее хранении и передаче, обнаружение и уничтожение аппаратных и программных закладок);
- резервное копирование наиболее важных с точки зрения утраты массивов документов;

• профилактику заражения компьютерными вирусами.

Перечислим основные виды мероприятий, которые должны проводиться на различных этапах жизненного цикла КС:

1) на этапе создания КС: при разработке ее общего проекта и проектов отдельных структурных элементов — анализ возможных угроз и методов их нейтрализации; при строительстве и переоборудовании помещений — приобретение сертифицированного оборудования, выбор лицензированных организаций; при разработке математического, программного, информационного и лингвистического обеспечения — использование сертифицированных программных и инструментальных средств; при монтаже и наладке оборудования — контроль за работой технического персонала; при испытаниях и приемке в эксплуатацию — включение в состав аттестационных комиссий сертифицированных специалистов;

2) в процессе эксплуатации КС — организация пропускного режима, определение технологии автоматизированной обработки документов, организация работы обслуживающего персонала, распределение реквизитов разграничения доступа пользователей к элементам КС (паролей, ключей, карт и т. п.), организация ведения протоколов работы КС, контроль выполнения требований служебных инструкций и т. п.;

3) мероприятия общего характера — подбор и подготовка кадров, организация плановых и предупреждающих проверок средств защиты информации, планирование мероприятий по защите информации, обучение персонала, участие в семинарах, конференциях и выставках по проблемам безопасности информации и т. п.

Основой проведения организационных мероприятий является использование и подготовка законодательных и нормативных документов в области информационной безопасности, которые на правовом уровне должны регулировать доступ к информации со стороны потребителей. В российском законодательстве позже, чем в законодательстве других развитых стран, появились необходимые правовые акты (хотя далеко не все).

Можно выделить четыре уровня правового обеспечения информационной безопасности. *Первый уровень* образуют международные договоры, к которым присоединилась Российская Федерация, и федеральные законы России:

• международные (всемирные) конвенции об охране промышленной собственности, охране интеллектуальной собственности, авторском праве;

• Конституция РФ (ст. 23 определяет право граждан на тайну переписки, телефонных, телеграфных и иных сообщений);

• Гражданский кодекс РФ (в ст. 139 устанавливается право на возмещение убытков от утечки с помощью незаконных методов информации, относящейся к служебной и коммерческой тайне);

• Уголовный кодекс РФ (ст. 272 устанавливает ответственность за неправомерный доступ к компьютерной информации, ст. 273 — за создание, использование и распространение вредоносных программ для ЭВМ, ст. 274 — за нарушение правил эксплуатации ЭВМ, систем и сетей);

• Федеральный закон «Об информации, информатизации и защите информации» от 20.02.95 № 24-ФЗ (ст. 10 устанавливает разнесение информационных ресурсов по категориям доступа: открытая информация, государственная тайна, конфиденциальная информация, ст. 21 определяет порядок защиты информации);

• Федеральный закон «О государственной тайне» от 21.07.93 № 5485-1 (ст. 5 устанавливает перечень сведений, составляющих государственную тайну; ст. 8 — степени секретности сведений и грифы секретности их носителей: «особой важности», «совершенно секретно» и «секретно»; ст. 20 — органы по защите государственной тайны, межведомственную комиссию по защите государственной тайны для координации деятельности этих органов; ст. 28 — порядок сертификации средств защиты информации, относящейся к государственной тайне);

• Федеральные законы «О лицензировании отдельных видов деятельности» от 08.08.2001 № 128-ФЗ, «О связи» от 16.02.95 № 15-ФЗ, «Об электронной цифровой подписи» от 10.01.02 № 1-ФЗ, «Об авторском праве и смежных правах» от 09.07.93 № 5351-1, «О правовой охране программ для электронных вычислительных машин и баз данных» от 23.09.92 № 3523-1 (ст. 4 определяет условие признания авторского права — знак © с указанием правообладателя и года первого выпуска продукта в свет; ст. 18 — защиту прав на программы для ЭВМ и базы данных путем выплаты компенсации в размере от 5000 до 50 000 минимальных размеров оплаты труда при нарушении этих прав с целью извлечения прибыли или путем возмещения причиненных убытков, в сумму которых включаются полученные нарушителем доходы).

Второй уровень правового обеспечения информационной безопасности составляют подзаконные акты, к которым относятся указы Президента РФ и постановления Правительства РФ, а также письма Высшего Арбитражного Суда РФ и постановления пленумов Верховного Суда РФ. Примерами таких актов могут являться Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера» от 06.03.97 № 188 или Постановление Правительства РФ «О перечне сведений, которые не могут составлять коммерческую тайну» от 05.12.91 № 35.

Третий уровень правового обеспечения информационной безопасности составляют государственные стандарты (ГОСТы) в области защиты информации, руководящие документы, нормы, методики и классификаторы, разработанные соответствующими

государственными органами. В качестве примеров можно привести следующие документы:

- ГОСТ Р 50922—96 «Защита информации. Основные термины и определения», ГОСТ Р 50739—95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования», ГОСТ 28147—89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» и др.;
- руководящие документы Государственной технической комиссии при Президенте Российской Федерации (Гостехкомиссии России) «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации», «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» и др.

Четвертый уровень правового обеспечения информационной безопасности образуют локальные нормативные акты, положения, инструкции, методические рекомендации и другие документы по комплексной защите информации в КС конкретной организации. К таким нормативным документам относятся:

- приказ об утверждении перечня сведений, составляющих коммерческую тайну предприятия;
- трудовые и гражданско-правовые договоры (подряда, поручения, комиссии и т. п.), в которые включены пункты об обязанности возмещения ущерба за разглашение сведений, составляющих коммерческую тайну предприятия, и др.

1.4. Инженерно-технические методы и средства защиты информации

Под инженерно-техническими средствами защиты информации понимают физические объекты, механические, электрические и электронные устройства, элементы конструкции зданий, средства пожаротушения и другие средства, обеспечивающие:

- защиту территории и помещений КС от проникновения нарушителей;
- защиту аппаратных средств КС и носителей информации от хищения;
- предотвращение возможности удаленного (из-за пределов охраняемой территории) видеонаблюдения (подслушивания) за работой персонала и функционированием технических средств КС;
- предотвращение возможности перехвата ПЭМИН, вызванных работающими техническими средствами КС и линиями передачи данных;
- организацию доступа в помещения КС сотрудников;

• контроль над режимом работы персонала КС;

• контроль над перемещением сотрудников КС в различных производственных зонах;

• противопожарную защиту помещений КС;

• минимизацию материального ущерба от потерь информации, возникших в результате стихийных бедствий и техногенных аварий.

Важнейшей составной частью инженерно-технических средств защиты информации являются технические средства охраны, которые образуют первый рубеж защиты КС и являются необходимым, но недостаточным условием сохранения конфиденциальности и целостности информации в КС.

Рассмотрим немного подробнее методы и средства защиты информации от утечки по каналам ПЭМИН. Основной задачей является уменьшение соотношения сигнал/шум в этих каналах до предела, при котором восстановление информации становится принципиально невозможным. Возможными методами решения этой задачи могут быть:

1) снижение уровня излучений сигналов в аппаратных средствах КС;

2) увеличение мощности помех в соответствующих этим сигналам частотных диапазонах.

Для применения *первого метода* необходим выбор системно-технических и конструкторских решений при создании технических средств КС в защищенном исполнении, а также рациональный выбор места размещения этих средств относительно мест возможного перехвата ПЭМИН (для соблюдения условия максимального затухания информационного сигнала). Требования к средствам вычислительной техники в защищенном исполнении определяются в специальных ГОСТах.

Реализация *второго метода* возможна путем применения активных средств защиты в виде генераторов сигналоподобных помех или шума.

Отметим перспективные методы и средства защиты информации в КС от утечки по каналам ПЭМИН:

• выбор элементной базы технических средств КС с возможно более малым уровнем информационных сигналов;

• замена в информационных каналах КС электрических цепей волоконно-оптическими линиями;

• локальное экранирование узлов технических средств, являющихся первичными источниками информационных сигналов;

• включение в состав информационных каналов КС устройств предварительного шифрования обрабатываемой информации.

Отметим, что при использовании технических средств КС для обработки информации ограниченного доступа необходимо проведение специальных проверок, целью которых является обнару-

жение и устранение внедренных специальных электронных устройств подслушивания, перехвата информации или вывода технических средств из строя (аппаратных закладок). При проведении таких проверок может потребоваться практически полная их разборка, что иногда может привести к возникновению неисправностей в работе технических средств и дополнительным затратам на их устранение.

Рассмотрим средства обнаружения электронных подслушивающих (радиозакладных) устройств, простейшими из которых являются нелинейные локаторы. Они с помощью специального передатчика в сверхвысокочастотном диапазоне радиоволн облучают окружающее пространство и регистрируют вторичный, переизлученный сигнал, поступающий от различных полупроводниковых элементов, находящихся как во включенном, так и в выключенном состоянии. Нелинейные локаторы могут не выявить радиозакладное устройство, если оно вмонтировано в электронное устройство (системный блок компьютера, телевизор, телефонный аппарат и т. п.), так как сигнал отклика от подслушивающего устройства будет замаскирован откликом от электронной аппаратуры. В этом случае потребуется применение более сложных устройств контроля постороннего радиоизлучения — индикаторов электромагнитного излучения, сканирующих приемников, компьютерных анализаторов.

1.5. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности

К аппаратным средствам защиты информации относятся электронные и электронно-механические устройства, включаемые в состав технических средств КС и выполняющие (самостоятельно или в едином комплексе с программными средствами) некоторые функции обеспечения информационной безопасности. Критерием отнесения устройства к аппаратным, а не к инженерно-техническим средствам защиты является обязательное включение в состав технических средств КС.

К основным аппаратным средствам защиты информации относятся:

- устройства для ввода идентифицирующей пользователя информации (магнитных и пластиковых карт, отпечатков пальцев и т. п.);
- устройства для шифрования информации;
- устройства для воспрепятствования несанкционированному включению рабочих станций и серверов (электронные замки и блокираторы).

Примеры вспомогательных аппаратных средств защиты информации:

- устройства уничтожения информации на магнитных носителях;
- устройства сигнализации о попытках несанкционированных действий пользователей КС и др.

Под программными средствами защиты информации понимают специальные программы, включаемые в состав программного обеспечения КС исключительно для выполнения защитных функций.

К основным программным средствам защиты информации относятся:

- программы идентификации и аутентификации пользователей КС;
- программы разграничения доступа пользователей к ресурсам КС;
- программы шифрования информации;
- программы защиты информационных ресурсов (системного и прикладного программного обеспечения, баз данных, компьютерных средств обучения и т. п.) от несанкционированного изменения, использования и копирования.

Заметим, что под *идентификацией*, применительно к обеспечению информационной безопасности КС, понимают однозначное распознавание уникального имени субъекта КС. *Аутентификация* означает подтверждение того, что предъявленное имя соответствует данному субъекту (подтверждение подлинности субъекта).

Примеры вспомогательных программных средств защиты информации:

- программы уничтожения остаточной информации (в блоках оперативной памяти, временных файлах и т. п.);
- программы аудита (ведения регистрационных журналов) событий, связанных с безопасностью КС, для обеспечения возможности восстановления и доказательства факта происшествия этих событий;
- программы имитации работы с нарушителем (отвлечения его на получение якобы конфиденциальной информации);
- программы тестового контроля защищенности КС и др.

К преимуществам программных средств защиты информации относятся:

- простота тиражирования;
- гибкость (возможность настройки на различные условия применения, учитывающие специфику угроз информационной безопасности конкретных КС);
- простота применения — одни программные средства, например шифрования, работают в «прозрачном» (незаметном для пользователя) режиме, а другие не требуют от пользователя никаких новых (по сравнению с другими программами) навыков;

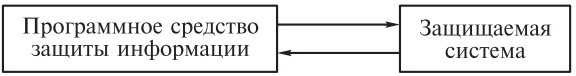

Рис. 1.1. Пример пристыкованного программного средства защиты

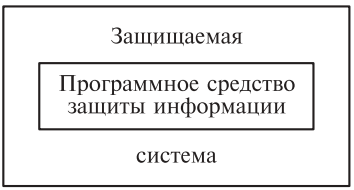

Рис. 1.2. Пример встроенного программного средства защиты

• практически неограниченные возможности их развития путем внесения изменений для учета новых угроз безопасности информации.

К недостаткам программных средств защиты информации относятся:

• снижение эффективности КС за счет потребления ее ресурсов, требуемых для функционирование программ защиты;

• более низкая производительность (по сравнению с выполняющими аналогичные функции аппаратными средствами защиты, например шифрования);

• пристыкованность многих программных средств защиты (а не их встроенность в программное обеспечение КС, рис. 1.1 и 1.2), что создает для нарушителя принципиальную возможность их обхода;

• возможность злоумышленного изменения программных средств защиты в процессе эксплуатации КС.

1.6. Требования к комплексным системам защиты информации

Поскольку потенциальные угрозы безопасности информации весьма многообразны, цели защиты информации могут быть достигнуты только путем создания комплексной системы защиты информации (КСЗИ), под которой понимается совокупность методов и средств, объединенных единым целевым назначением и обеспечивающих необходимую эффективность защиты информации в КС.

Основные требования к комплексной системе защиты информации:

• разработка на основе положений и требований существующих законов, стандартов и нормативно-методических документов по обеспечению информационной безопасности;

• использование комплекса программно-технических средств и организационных мер для защиты КС;

• надежность, производительность, конфигурируемость;

• экономическая целесообразность (поскольку стоимость КСЗИ включается в стоимость КС, стоимость средств защиты не должна быть выше возможного ущерба от потери информации);

• выполнение на всех этапах жизненного цикла обработки информации в КС (в том числе при проведении ремонтных и регламентных работ);

• возможность совершенствования;

• обеспечение разграничения доступа к конфиденциальной информации с отвлечением нарушителя на ложную информацию (обеспечение не только пассивной, но и активной защиты);

• взаимодействие с незащищенными КС по установленным для этого правилам разграничения доступа;

• обеспечение проведения учета и расследования случаев нарушения безопасности информации в КС;

• сложная для пользователя (не должна вызывать у него психологического противодействия и стремления обойтись без применения ее средств);

• возможность оценки эффективности ее применения.

Впервые основные категории требований к защищенности КС были сформулированы в документе Министерства обороны США «Trusted Computer System Evaluation Criteria» («Критерии оценки безопасности компьютерных систем», или «Оранжевая книга»), 1985 г. В этом документе предложены три основные категории требований.

1. Политика:

• наличие явной и хорошо определенной политики обеспечения безопасности;

• использование маркировки объектов КС для управления доступом к ним.

2. Подотчетность:

• индивидуальная идентификация субъектов КС;

• сохранение и защита информации аудита.

3. Гарантии:

• включение в состав КС программно-аппаратных средств для получения гарантий выполнения требований категорий 1 и 2;

• постоянная защищенность средств обеспечения безопасности информации в КС от их преодоления и (или) несанкционированного изменения.

В «Оранжевой книге» были введены семь классов защищенности КС — от минимальной защиты (класс D1) до верифициро-

ванной (формально доказанной) защиты (класс А1). Требования «Оранжевой книги» явились первой попыткой создать единый стандарт безопасности КС, рассчитанный на проектировщиков, разработчиков (программистов), пользователей подобных систем и специалистов по их сертификации.

Отличительной чертой этого стандарта является ориентация на государственные (в первую очередь военные) организации и операционные системы.

В 1992 г. Гостехкомиссия России опубликовала первый комплект руководящих документов по защите средств вычислительной техники (СВТ) и автоматизированных систем (АС) от несанкционированного доступа.

СВТ не решают непосредственно прикладных задач, а используются в качестве элементов АС. Примерами СВТ являются плата расширения BIOS с соответствующим аппаратным и программным интерфейсом для аутентификации пользователей АС или программа «прозрачного» шифрования информации на жестком диске.

В руководящих документах Гостехкомиссии России определены семь классов защищенности СВТ от несанкционированного доступа к обрабатываемой (сохраняемой, передаваемой) с помощью этих средств информации (наиболее защищенным является первый класс),

АС рассматривается как комплекс СВТ и имеет дополнительные характеристики: полномочия пользователей, модель нарушителя, технология обработки информации. Типичным примером АС является многопользовательская и многозадачная операционная система.

В руководящих документах Гостехкомиссии России определены девять классов защищенности АС от несанкционированного доступа, объединенных в три группы:

- однопользовательские АС с информацией, размещенной на носителях одного уровня конфиденциальности (класс 3Б и 3А);
- многопользовательские АС с одинаковыми полномочиями пользователей и информацией на носителях разного уровня конфиденциальности (классы 2Б и 2А);
- многопользовательские АС с разными полномочиями пользователей и информацией разного уровня конфиденциальности (в порядке возрастания защищенности от класса 1Д до класса 1А).

Под несанкционированным доступом к информации в руководящих документах Гостехкомиссии России понимается доступ к информации, нарушающий установленные правила разграничения доступа и использующий штатные возможности СВТ и АС. Руководящие документы Гостехкомиссии России, подобно «Оранжевой книге», ориентированы прежде всего на применение в КС силовых структур Российской Федерации.

Дальнейшее развитие стандартов в области информационной безопасности КС привело к появлению европейских «Критериев оценки безопасности информационных технологий» (Information Technology Security Evaluation Criteria), американских «Федеральных критериев безопасности информационных технологий» (Federal Criteria for Information Technology Security), канадских «Критериев оценки безопасности компьютерных продуктов» (Canadian Trusted Computer Product Evaluation Criteria) и завершилось на сегодняшний день принятием «Общих критериев оценки безопасности информационных технологий» (Common Criteria for Information Technology Security Evaluation).

«Общие критерии...» адресованы трем группам специалистов (пользователям, разработчикам и экспертам по классификации КС) и представляют собой новый межгосударственный уровень в стандартизации безопасности информационных технологий.

В Российской Федерации «Общие критерии...» изданы в качестве ГОСТа (ГОСТ РИСО/МЭК 15408—2001 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»).

В «Общих критериях...» предложена система функциональных требований к защищенным КС и критерии их независимого ранжирования.

Иначе говоря, в этих стандартах не устанавливается линейная шкала уровней безопасности КС, характерная для «Оранжевой книги». Это объясняется тем, что для одних КС наиболее важным требованием является идентификация и аутентификация пользователей, а для других — реализация конкретной политики разграничения доступа к ресурсам или обеспечение доступности информации.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. В каких формах может быть представлена информация?
2. Какая информация называется документированной?
3. Что относится к информации ограниченного доступа?
4. Что понимается под защитой информации?
5. Что относится к основным характеристикам защищаемой информации?
6. Что такое угроза безопасности информации? Каковы основные виды угроз?
7. Какие существуют каналы утечки конфиденциальной информации?
8. Что такое ПЭМИН?
9. В чем сущность системно-концептуального подхода к защите информации в компьютерных системах?
10. Почему проблема защиты информации не может быть решена с помощью только формальных методов и средств?
11. В чем сущность организационной защиты информации?

12. Каковы уровни правового обеспечения информационной безопасности?

13. Какие законодательные акты составляют основу российского информационного права?

14. Что относится к средствам инженерно-технической защиты информации и для чего они предназначены?

15. В чем заключаются достоинства и недостатки программных средств защиты информации?

16. Какие требования предъявляются к комплексным системам защиты информации?

17. Какие существуют международные и российские стандарты в области безопасности компьютерных систем и информационных технологий?

ГЛАВА 2

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

2.1. Способы несанкционированного доступа к информации в компьютерных системах и защиты от него

В руководящих документах Гостехкомиссии России приведены следующие основные способы несанкционированного доступа к информации в КС:

- непосредственное обращение к объекту с конфиденциальной информацией (например, с помощью управляемой пользователем программы, читающей данные из файла или записывающей их в него);
- создание программных и технических средств, выполняющих обращение к объекту в обход средств защиты (например, с использованием случайно или намеренно оставленных разработчиком этих средств, так называемых люков);
- модификация средств защиты для осуществления несанкционированного доступа (например, внедрение программных закладок);
- внедрение в технические средства СВТ или АС программных или технических механизмов, нарушающих структуру и функции этих средств для осуществления несанкционированного доступа (например, путем загрузки на компьютере иной, незащищенной операционной системы).

Модель нарушителя в руководящих документах Гостехкомиссии России определяется исходя из следующих предположений:

- нарушитель имеет доступ к работе со штатными средствами КС;
- нарушитель является специалистом высшей квалификации (знает все о КС и, в частности, о системе и средствах ее защиты).

Можно выделить следующие уровни возможностей нарушителя, предоставляемые ему штатными средствами КС (каждый следующий уровень включает в себя предыдущий):

1) запуск программ из фиксированного набора (например, подготовка документов или получение почтовых сообщений);

2) создание и запуск собственных программ (возможности опытного пользователя или пользователя с полномочиями отладки программ);

3) управление функционированием КС — воздействие на ее базовое программное обеспечение, состав и конфигурацию КС (например, внедрение программной закладки);

4) весь объем возможностей лиц, осуществляющих проектирование, реализацию и ремонт средств КС, вплоть до включения в состав КС собственных СВТ с новыми функциями.

С учетом различных уровней возможностей нарушителя выделяют следующие вспомогательные способы несанкционированного доступа к информации в КС, позволяющие нарушителю использовать перечисленные ранее основные способы:

- ручной или программный подбор паролей путем их полного перебора или при помощи специального словаря (взлом КС);
- подключение к КС в момент кратковременного прекращения работы легального пользователя, работающего в интерактивном режиме и не заблокировавшего свой терминал;
- подключение к линии связи и перехват доступа к КС после отправки пакета завершения сеанса легального пользователя, работающего в удаленном режиме;
- выдача себя за легального пользователя с применением похищенной у него или полученной обманным путем (с помощью так называемой социальной инженерии) идентифицирующей информации — «маскарад»;
- создание условий для связи по компьютерной сети легального пользователя с терминалом нарушителя, выдающего себя за легального объекта КС (например, одного из ее серверов), — «мистификация»;
- создание условий для возникновения в работе КС сбоев, которые могут повлечь за собой отключение средств защиты информации или нарушение правил политики безопасности;
- тщательное изучение подсистемы защиты КС и используемой в ней политики безопасности, выявление ошибочных участков в программных средствах защиты информации в КС, введение программных закладок, разрешающих доступ нарушителю.

Приведем пример использования способа несанкционированного доступа к информации в КС, основанный на создании аварийной ситуации. Если у нарушителя есть физический доступ хотя бы к одной рабочей станции локальной вычислительной сети (ЛВС) организации или к линии связи, то он сможет внедрить на рабочей станции программную закладку (или подключить к линии связи специальное устройство), перехватывать все пакеты подключения легального пользователя этой рабочей станции к серверу ЛВС и искажать имя пользователя в этих пакетах (иначе говоря, создать условия, при которых легальный пользователь КС никогда не сможет подключиться к серверу).

В этой ситуации на атакуемую рабочую станцию рано или поздно придет администратор ЛВС для того, чтобы разобраться в причинах сбоев при подключении к серверу. Если при этом администратор пошлет пакет подключения к серверу под своей привилегированной учетной записью, в которой оставлено имя адми-

нистратора по умолчанию (например, «Supervisor» в операционной системе Novell Netware или «Администратор» в операционных системах Windows NT/2000/XP Professional), то тем самым цель нарушителя (перехват пароля администратора) будет достигнута.

Причиной успеха описанной в данном примере атаки является нарушение администратором системы правил политики безопасности, в соответствии с которыми он должен использовать привилегированную учетную запись только для выполнения административных функций и только с защищенной рабочей станции, а для выполнения других действия требуется создать другую учетную запись администратора с отличным от принятого по умолчанию именем.

В соответствии с руководящими документами Гостехкомиссии России основными направлениями обеспечения защиты СВТ и АС от несанкционированного доступа являются создание системы разграничения доступа (СРД) субъектов к объектам доступа и создание обеспечивающих средств для СРД.

К основным функциям СРД относятся:

- реализация правил разграничения доступа субъектов и их процессов к информации и устройствам создания ее твердых копий;
- изоляция процессов, выполняемых в интересах субъекта доступа, от других субъектов;
- управление потоками информации в целях предотвращения ее записи на носители несоответствующего уровня конфиденциальности;
- реализация правил обмена информацией между субъектами в компьютерных сетях.

К функциям обеспечивающих средств для СРД относятся:

- идентификация и аутентификация субъектов и поддержание привязки субъекта к процессу, выполняемому для него;
- регистрация действий субъекта и активизированного им процесса;
- исключение и включение новых субъектов и объектов доступа, изменение полномочий субъектов;
- реакция на попытки несанкционированного доступа (сигнализация, блокировка, восстановление объекта после несанкционированного доступа);
- учет выходных печатных форм в КС;
- контроль целостности программной и информационной части СРД и обеспечивающих ее средств.

Итак, основными способами защиты от несанкционированного доступа к информации в компьютерных системах являются аутентификация, *авторизация* (определение прав доступа субъекта к объекту с конфиденциальной информацией) и шифрование информации.

Под *протоколом* в общем случае понимают конечную последовательность однозначно и точно определенных действий, выполняемых двумя или более сторонами для достижения желаемого результата за конечное время. Рассмотрим протокол идентификации пользователя при его входе в КС (под «С» понимается система, под «П» — пользователь):

1. С: запрос имени, под которым пользователь зарегистрирован в базе данных учетных записей КС (логического имени пользователя или так называемого логина).
2. П: ввод логического имени (ID).
3. С: проверка наличия ID в регистрационной базе данных. Если пользователь с таким именем зарегистрирован, то запрос его идентифицирующей информации, в противном случае — возврат к п. 1.
4. П: ввод идентифицирующей информации (P).
5. С: проверка совпадения P с идентифицирующей информацией для пользователя ID в регистрационной базе данных. Если совпадение есть, то допуск пользователя к работе в КС, в противном случае — возврат к п. 3.

Присвоение каждому пользователю КС уникального логического имени, под которым он регистрируется в базе данных учетных записей, не только позволяет предоставить разным пользователям КС различный уровень прав в ней, но и дает возможность полного учета всех входов пользователя в систему в журнале аудита.

Приведем типичную структуру учетной записи i в регистрационной базе данных КС:

- относительный номер учетной записи RID_i;
- логическое имя пользователя ID_i;
- полное имя пользователя и его должность в организации D_i;
- случайное значение S_i, генерируемое при регистрации пользователя в КС (используется для предотвращения возможности получения одним пользователем полномочий другого пользователя при случайном совпадении идентифицирующей информации);
- идентифицирующая пользователя информация P_i;
- информация о правах пользователя в КС R_i.

Доступ к базе данных учетных записей КС как по чтению, так и по записи должен быть разрешен только привилегированному пользователю (администратору). Рассмотрим возможные угрозы безопасности информации в КС, если доступ к регистрационной базе данных будет разрешен всем зарегистрированным в КС пользователям.

Если разрешен доступ по записи (без права добавления данных в регистрационную базу), то тогда возможна следующая ситуация. Пользователь i после входа в КС изменяет идентифицирующую информацию в учетной записи пользователя j на идентифицирующую информацию из своей учетной записи, сохраняя при этом старую информацию из учетной записи j, после чего завершает

сеанс работы с КС и возобновляет его уже как пользователь *j*. Применив полномочия другого пользователя, нарушитель восстанавливает идентифицирующую информацию в учетной записи *j*, после чего завершает сеанс работы с КС.

Если к регистрационной базе данных КС разрешен доступ по чтению, то пользователь-нарушитель сможет скопировать ее на собственный носитель или просто в другой файл и осуществить попытку подбора идентифицирующей информации (например, пароля) привилегированного пользователя для осуществления несанкционированного доступа с помощью «маскарада».

Для удобства назначения полномочий пользователям КС они могут объединяться в группы в соответствии с должностным положением пользователей в организации и (или) их принадлежностью одному из ее структурных подразделений. Информация о группах пользователей также может размещаться в регистрационной базе данных КС.

Рассмотрим способы аутентификации пользователей в КС, которые можно подразделить на три группы. К *первой группе* относятся способы аутентификации, основанные на том, что пользователь знает некоторую подтверждающую его подлинность информацию (парольная аутентификация и аутентификация на основе модели «рукопожатия»).

Ко *второй группе* относятся способы аутентификации, основанные на том, что пользователь имеет некоторый материальный объект, который может подтвердить его подлинность (например, пластиковую карту с идентифицирующей пользователя информацией).

К *третьей группе* относятся способы аутентификации, основанные на таких данных, которые позволяют однозначно считать, что пользователь и есть тот самый субъект, за которого себя выдает (биометрические данные, особенности клавиатурного почерка и росписи мышью и т. п.).

В соответствии с «Оранжевой книгой» (см. подразд. 1.6) в защищенных КС, начиная с класса С1, должен использоваться хотя бы один из способов аутентификации (например, пароль), а данные аутентификации должны быть защищены от доступа неавторизованного пользователя.

В руководящих документах Гостехкомиссии России (см. подразд. 1.6) в АС, отнесенных к классу защищенности 1Д, должна осуществляться идентификация и проверка подлинности субъектов при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов. Для классов защищенности 1Г и 1В дополнительно требуется использовать идентификатор (код, логическое имя) пользователя. Для отнесения АС к классу защищенности 1Б дополнительно необходимо использовать пароль временного действия длиной не менее восьми буквенно-цифровых символов. В требованиях к классу защи-

щенности 1А определена необходимость применения пользователями при входе в АС биометрических характеристик или специальных устройств (жетонов, карт, электронных ключей) и пароля временного действия длиной не менее восьми буквенно-цифровых символов.

2.2. Аутентификация пользователей на основе паролей и модели «рукопожатия»

При выборе паролей пользователи КС должны руководствоваться двумя, по сути взаимоисключающими, правилами — пароли должны трудно подбираться и легко запоминаться (поскольку пароль ни при каких условиях не должен нигде записываться, так как в этом случае необходимо будет дополнительно решать задачу защиты носителя пароля).

Сложность подбора пароля определяется, в первую очередь, мощностью множества символов, используемого при выборе пароля (N), и минимально возможной длиной пароля (k). В этом случае число различных паролей может быть оценено снизу как $C_p = N^k$. Например, если множество символов пароля образуют строчные латинские буквы, а минимальная длина пароля равна 3, то $C_p = 26^3 = 17\,576$ (что совсем немного для программного подбора). Если же множество символов пароля состоит из строчных и прописных латинских букв, а также из цифр и минимальная длина пароля равна 6, то $C_p = 62^6 = 56\,800\,235\,584$.

Сложность выбираемых пользователями КС паролей должна устанавливаться администратором при реализации установленной для данной системы политики безопасности. Другими параметрами политики учетных записей при использовании парольной аутентификации должны быть:

- максимальный срок действия пароля (любой секрет не может сохраняться в тайне вечно);
- несовпадение пароля с логическим именем пользователя, под которым он зарегистрирован в КС;
- неповторяемость паролей одного пользователя.

Требование неповторяемости паролей может быть реализовано двумя способами. Во-первых, можно установить минимальный срок действия пароля (в противном случае пользователь, вынужденный после истечения срока действия своего пароля поменять его, сможет тут же сменить пароль на старый). Во-вторых, можно вести список уже использовавшихся данным пользователем паролей (максимальная длина списка при этом может устанавливаться администратором).

К сожалению, обеспечить реальную уникальность каждого вновь выбираемого пользователем пароля с помощью приведенных выше

мер практически невозможно. Пользователь может, не нарушая установленных ограничений, выбирать пароли «A1», «A2», ... где A — первый пароль пользователя, удовлетворяющий требованиям сложности.

Обеспечить приемлемую степень сложности паролей и их реальную уникальность можно путем назначения паролей всем пользователям администратором КС с одновременным запретом на изменение пароля самим пользователем. Для генерации паролей администратор при этом может использовать программный генератор, позволяющий создавать пароли различной сложности (пример окна настройки одного из подобных генераторов приведен на рис. 2.1).

Однако при таком способе назначения паролей возникают проблемы, связанные с необходимостью создания защищенного канала для передачи пароля от администратора к пользователю, трудностью проверки сохранения пользователем не им выбранного пароля только в своей памяти и потенциальной возможностью администратора, знающего пароли всех пользователей, злоупотребления своими полномочиями. Поэтому наиболее целесообразным является выбор пароля пользователем на основе установленных администратором правил с возможностью задания администратором нового пароля пользователю в случае, если тот забыл свой пароль.

Еще одним аспектом политики учетных записей пользователей КС должно стать определение противодействия системы попыткам подбора паролей.

Могут применяться следующие правила:

- ограничение числа попыток входа в систему;

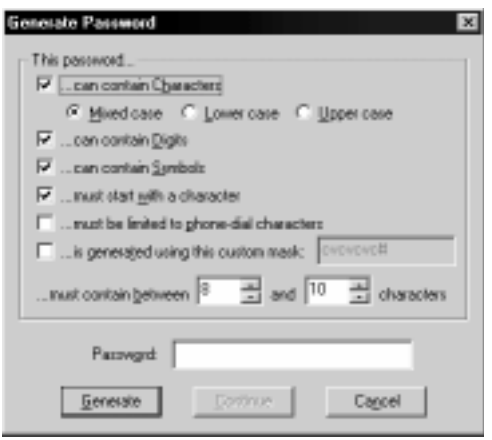

Рис. 2.1. Пример окна настройки программного генератора паролей

• скрытие логического имени последнего работавшего пользователя (знание логического имени может помочь нарушителю подобрать или угадать его пароль);

• учет всех попыток (успешных и неудачных) входа в систему в журнале аудита.

Реакцией системы на неудачную попытку входа пользователя могут быть:

• блокировка учетной записи, под которой осуществляется попытка входа, при превышении максимально возможного числа попыток (на заданное время или до ручного снятия блокировки администратором);

• нарастающее увеличение временной задержки перед предоставлением пользователю следующей попытки входа.

Постоянная блокировка учетной записи при обнаружении попытки подбора пароля (до снятия блокировки администратором) менее целесообразна, поскольку она позволит нарушителю намеренно заблокировать работу в КС легального пользователя (реализовать угрозу нарушения доступности информации).

При любой реакции системы на попытку подбора пароля необходимо в настройках параметров политики учетных записей обеспечить сброс значения счетчика попыток входа в систему под конкретной учетной записью через заданный промежуток времени, иначе значения счетчика будут суммироваться для разных сеансов работы пользователя.

При первоначальном вводе или смене пароля пользователя обычно применяются два классических правила:

• символы вводимого пароля не отображаются на экране (это же правило применяется и для ввода пользователем пароля при его входе в систему);

• для подтверждения правильности ввода пароля (с учетом первого правила) этот ввод повторяется дважды.

Одним из следствий первого правила является нецелесообразность назначения пользователю пароля системой, поскольку в этом случае пароль должен быть выведен пользователю в открытом виде или записан на специальном носителе (второй способ противоречит принципу сохранения пароля только в памяти пользователя).

Однако отказ от отображения символов вводимого пароля может создать проблему, так как увеличивается вероятность того, что случайная ошибка, допущенная при вводе пароля, останется не замеченной, а это может привести к блокировке учетной записи легального пользователя. Поэтому, если вход пользователя в КС происходит в защищенном помещении, в которое не могут попасть посторонние лица, от правила скрытия символов вводимого пароля можно и отказаться.

Очевидно, что в базе данных учетных записей пользователей КС пароли не могут храниться в открытом виде (иначе к ним мо-

жет получить доступ как минимум администратор системы). Для хранения паролей возможно их предварительное шифрование или хеширование.

Шифрование паролей имеет два недостатка:

- поскольку при шифровании необходимо использовать ключ, требуется обеспечить его защищенное хранение в КС (знание ключа шифрования пароля позволит выполнить его расшифрование и осуществить несанкционированный доступ к информации);
- существует опасность расшифрования любого пароля и получения его в открытом виде.

Хеширование является необратимым преобразованием и знание хеш-значения пароля не даст нарушителю возможности его получения в открытом виде (он сможет только пытаться подобрать пароль при известной функции хеширования). Поэтому гораздо более безопасным является хранение паролей в хешированном виде. Недостатком является то, что не существует даже теоретической возможности восстановить забытый пользователем пароль.

Несмотря на то, что с помощью применения перечисленных выше правил парольную аутентификацию можно сделать более безопасной, она все-таки остается весьма уязвимой. Для ее усиления могут использоваться так называемые одноразовые пароли. Пусть пользователь КС получает список паролей P_1, P_2, ..., P_i, ..., P_n. Каждый из паролей действует только на один сеанс входа (P_1 — на первый, P_2 — на второй и т. д.). В этом случае знание уже использовавшегося пользователем пароля ничего не даст нарушителю, а при каждом входе легального пользователя возможна проверка на использование данного пароля кем-либо еще.

Недостатки схемы одноразовых паролей:

- организация защищенного хранения длинного списка паролей (либо его запоминание, что маловероятно);
- неясность с номером следующего пароля, если после ввода предыдущего пароля из списка вход пользователя в систему не был осуществлен из-за сбоя в работе КС.

Эти недостатки могут быть устранены, если список паролей генерировать на основе некоторой необратимой функции, например функции хеширования. Пусть P — начальный пароль пользователя, а F — необратимая функция. Обозначим: $F^i(P) = F(F(...F(P)...))$ (функция F применяется последовательно i раз). Тогда список одноразовых паролей создается следующим образом: $P_1 = F^n(P)$, $P_2 = F^{n-1}(P)$, ..., $P_{n-1} = F(F(P))$, $P_n = F(P)$.

При сбое в процессе входа пользователя в КС всегда осуществляется выбор следующего пароля из списка, а система последовательно применяет функцию F к введенному пользователем паролю, вплоть до совпадения с последним принятым от него паролем (и тогда пользователь допускается к работе в системе) или до

превышения длины списка паролей (в этом случае попытка входа пользователя в КС отвергается).

Но в любом варианте парольной аутентификации подтверждение подлинности пользователя осуществляется на основе ввода им некоторой конфиденциальной информации, которую можно подсмотреть, выманить, подобрать, угадать и т. п. Рассмотрим аутентификацию пользователей на основе модели «рукопожатия», во многом свободную от указанных недостатков.

В соответствии с этой моделью пользователь П и система С согласовывают при регистрации пользователя в КС функцию f, известную только им. Протокол аутентификации пользователя в этом случае выглядит следующим образом:

1. С: генерация случайного значения x; вычисление $y = f(x)$; вывод x.
2. П: вычисление $y' = f'(x)$; ввод y'.
3. С: если y и y' совпадают, то пользователь допускается к работе в системе, иначе попытка входа в систему отклоняется.

К функции f предъявляется требование, чтобы по известным x и $f(x)$ нельзя было угадать f.

Преимущества аутентификации на основе модели «рукопожатия» перед парольной аутентификацией:

- между пользователем и системой не передается никакой конфиденциальной информации, которую нужно сохранять в тайне;
- каждый следующий сеанс входа пользователя в систему отличен от предыдущего, поэтому даже длительное наблюдение за этими сеансами ничего не даст нарушителю.

К недостаткам аутентификации на основе модели «рукопожатия» относится большая длительность этой процедуры по сравнению с парольной аутентификацией.

Парольная аутентификация совершенно неприменима в случае взаимного подтверждения подлинности пользователей компьютерной сети. Действительно, пусть А и Б обозначают двух пользователей сети, имеющих соответственно пароли $P_А$ и $P_Б$. Тогда протокол взаимной аутентификации А и Б мог бы выглядеть следующим образом:

1. А→Б: А, запрос $P_Б$.
2. Б→А: Б, запрос $P_А$.
3. А→Б: А, $P_А$.
4. Б→А: Б, $P_Б$.

Но в момент отправки своего пароля (неважно, в открытой или защищенной форме) А не может быть уверен в подлинности Б, который может воспользоваться паролем А, чтобы выдать себя за А при взаимодействии еще с одним пользователем компьютерной сети В.

Модель «рукопожатия» вполне приемлема для взаимной аутентификации:

1. А: выбор значения x; вычисление $y = f(x)$.
2. А→Б: А, x.
3. Б: вычисление $y' = f(x)$.
4. Б→А: Б, y'.
5. А: если y и y' совпадают, то А может доверять Б.

Затем процедура аутентификации повторяется с переменой ролей (теперь Б начинает процесс и выбирает значение x), чтобы Б мог быть также уверен в подлинности А.

Для повышения безопасности протокола взаимной аутентификации перед отправкой по сети значения x и y' (пп. 2 и 4 протокола) могут быть зашифрованы на секретном ключе, которым должны предварительно обменяться по защищенному каналу А и Б. В этом случае потенциальному нарушителю, который имеет возможность перехвата всех передаваемых по сети данных и желает выдать себя за одного из легальных пользователей сети, придется не только определить функцию f, но и предварительно взломать шифротекст.

При интерактивном доступе пользователя к системе функция f может быть задана таблицей своих значений. Рассмотрим два примера. В первом примере система предлагает пользователю ответить при регистрации его в КС на несколько вопросов, имеющих частично объективное и частично вымышленное содержание (например: «девичья фамилия Вашей матери», «в каком городе Вы проживали в июне 2002 г.», «где находится клуб», «когда откроется пул» и т. п.). При входе в систему пользователю предлагается ответить на другой список вопросов, среди которых есть некоторые из заданных ему при регистрации. Для правильной аутентификации пользователь должен дать те же ответы, которые он давал на аналогичные вопросы при регистрации.

Второй пример — аутентификация на основе модели «рукопожатия». При регистрации в КС пользователю предлагается набор небольших изображений (например, пиктограмм), среди которых он должен выбрать заданное число картинок. При последующем входе в систему ему выводится другой набор изображений, часть из которых он видел при регистрации. Для правильной аутентификации пользователь должен отметить те картинки, которые он выбрал при регистрации.

2.3. Аутентификация пользователей по их биометрическим характеристикам, клавиатурному почерку и росписи мышью

К основным биометрическим характеристикам пользователей КС, которые могут применяться при их аутентификации, относятся:

- отпечатки пальцев;
- геометрическая форма руки;
- узор радужной оболочки глаза;
- рисунок сетчатки глаза;
- геометрическая форма и размеры лица;
- тембр голоса;
- геометрическая форма и размеры уха и др.

Наиболее распространенными являются программно-аппаратные средства аутентификации пользователей по их отпечаткам пальцев. Для считывания этих отпечатков обычно применяются оснащенные специальными сканерами клавиатуры и мыши. Наличие достаточно больших банков данных с отпечатками пальцев граждан является основной причиной достаточно широкого применения подобных средств аутентификации в государственных структурах, а также в крупных коммерческих организациях. Недостатком таких средств является потенциальная возможность применения отпечатков пальцев пользователей для контроля над их частной жизнью.

Если по объективным причинам (например, из-за загрязненности помещений, в которых проводится аутентификация) получение четкого отпечатка пальца невозможно, то может применяться аутентификация по геометрической форме руки пользователя. В этом случае сканеры могут быть установлены на стене помещения.

Наиболее достоверными (но и наиболее дорогостоящими) являются средства аутентификации пользователей, основанные на характеристиках глаза (узоре радужной оболочки или рисунке сетчатки). Вероятность повторения этих признаков оценивается в 10^{-78}.

Наиболее дешевыми (но и наименее достоверными) являются средства аутентификации, основанные на геометрической форме и размере лица пользователя или на тембре его голоса. Это позволяет использовать эти средства и для аутентификации при удаленном доступе пользователей к КС.

Основные достоинства аутентификации пользователей по их биометрическим характеристикам:

- трудность фальсификации этих признаков;
- высокая достоверность аутентификации из-за уникальности таких признаков;
- неотделимость биометрических признаков от личности пользователя.

Для сравнения аутентификации пользователей на основе тех или иных биометрических характеристик применяются оценки вероятностей ошибок первого и второго рода. Вероятность ошибки первого рода (отказа в доступе к КС легальному пользователю) составляет $10^{-6} \ldots 10^{-3}$. Вероятность ошибки второго рода (допуска к работе в

КС незарегистрированного пользователя) в современных системах биометрической аутентификации составляет $10^{-5} \ldots 10^{-2}$.

Общим недостатком средств аутентификации пользователей КС по их биометрическим характеристикам является их более высокая стоимость по сравнению с другими средствами аутентификации, что обусловлено, в первую очередь, необходимостью приобретения дополнительных аппаратных средств. Способы аутентификации, основанные на особенностях клавиатурного почерка и росписи мышью пользователей, не требуют применения специальной аппаратуры.

Одним из первых идею аутентификации пользователей по особенностям их работы с клавиатурой и мышью предложил С.П.Расторгуев. При разработке математической модели аутентификации на основе клавиатурного почерка пользователей было сделано предположение, что временные интервалы между нажатиями соседних символов ключевой фразы и между нажатиями конкретных сочетаний клавиш в ней подчиняются нормальному закону распределения. Сутью данного способа аутентификации является проверка гипотезы о равенстве центров распределения двух нормальных генеральных совокупностей (полученных при настройке системы на характеристики пользователя и при его аутентификации).

Рассмотрим вариант аутентификации пользователя по набору ключевой фразы (одной и той же в режимах настройки и подтверждения подлинности).

Процедура настройки на характеристики регистрируемого в КС пользователя:

1) выбор пользователем ключевой фразы (ее символы должны быть равномерно разнесены по клавиатуре);

2) набор ключевой фразы несколько раз;

3) исключение грубых ошибок (по специальному алгоритму);

4) расчет и сохранение оценок математических ожиданий, дисперсий и числа наблюдений для временных интервалов между наборами каждой пары соседних символов ключевой фразы.

Процедура аутентификации пользователя может проводиться в двух вариантах. Первый вариант процедуры аутентификации:

1) набор ключевой фразы пользователем несколько раз;

2) исключение грубых ошибок (по специальному алгоритму);

3) расчет оценок математических ожиданий и дисперсий для временных интервалов между нажатиями каждой пары соседних символов ключевой фразы;

4) решение задачи проверки гипотезы о равенстве дисперсий двух нормальных генеральных совокупностей для каждой пары соседних символов ключевой фразы (по специальному алгоритму);

5) если дисперсии равны, то решение задачи проверки гипотезы о равенстве центров распределения двух нормальных гене-

ральных совокупностей при неизвестной дисперсии для каждой пары соседних символов ключевой фразы (по специальному алгоритму);

6) вычисление вероятности подлинности пользователя как отношения числа сочетаний соседних клавиш, для которых подтверждены гипотезы (пп. 4 и 5), к общему числу сочетаний соседних символов ключевой фразы;

7) сравнение полученной оценки вероятности с выбранным пороговым значением для принятия решения о допуске пользователя.

Второй вариант процедуры аутентификации:

1) набор ключевой фразы один раз;

2) решение задачи проверки гипотезы о равенстве дисперсий двух нормальных генеральных совокупностей для временных интервалов между нажатиями соседних символов ключевой фразы;

3) если дисперсии равны, то исключение временных интервалов между нажатиями соседних символов ключевой фразы, которые существенно отличаются от эталонных (полученных при настройке);

4) вычисление вероятности подлинности пользователя как отношения числа оставшихся интервалов к общему числу интервалов в ключевой фразе;

5) сравнение полученной оценки вероятности с выбранным пороговым значением для принятия решения о допуске пользователя.

Вместо использования постоянной для пользователя КС ключевой фразы можно проводить аутентификацию с помощью набора псевдослучайного текста. В этом случае клавиатура разделяется на поля и вводится понятие расстояния d_{ij} между клавишами i и j, под которым понимается число клавиш, расположенных на соединяющей i и j прямой линии. Клавиша i принадлежит полю m, если $\forall j \in m \; d_{ij} \le k$.

Величину k назовем степенью поля m (если $k = 0$, то m — отдельная клавиша). Обозначим через x_{ij} временной интервал между нажатиями клавиш, принадлежащих полям i и j.

Введем следующие допущения:

- характеристики нажатия клавиш одного поля тем ближе друг к другу, чем меньше k;
- для пользователя, работающего двумя руками, получение характеристик клавиатурного почерка возможно с помощью исследования работы только с одной половиной клавиатуры;
- ключевой фразой может быть любой набор символов;
- число полей должно быть одним и тем же в режимах настройки и аутентификации.

Процедура настройки при наборе псевдослучайного текста:

1) генерация и вывод пользователю текста из фиксированного множества слов, символы которых максимально разбросаны по клавиатуре;

2) набор текста пользователем;

3) фиксация и сохранение значений x_{ij}, которые затем используются для расчета статистических характеристик клавиатурного почерка.

Процедура аутентификации совпадает с процедурой аутентификации, используемой при наборе ключевой фразы.

Достоверность аутентификации на основе клавиатурного почерка пользователя ниже, чем при использовании его биометрических характеристик.

Однако этот способ аутентификации имеет и свои преимущества:

- возможность скрытия факта применения дополнительной аутентификации пользователя, если в качестве ключевой фразы используется вводимая пользователем парольная фраза;
- возможность реализации данного способа только с помощью программных средств (снижение стоимости средств аутентификации).

Теперь рассмотрим способ аутентификации, основанный на росписи мышью (с помощью этого манипулятора, естественно, нельзя выполнить реальную роспись пользователя, поэтому данная роспись будет достаточно простым росчерком). Назовем линией росписи ломаную линию, полученную соединением точек от начала росписи до ее завершения (соседние точки при этом не должны иметь одинаковых координат). Длину линии росписи рассчитаем как сумму длин отрезков, соединяющих точки росписи.

Введем понятие разрыва в линии росписи, признаком которого будет выполнение условия

$$d_{i,\,i-1} > \frac{d}{k},$$

где $d_{i,\,i-1}$ — расстояние между двумя соседними точками линии росписи; d — длина всей линии; k — число точек в линии.

Для устранения разрывов в линии росписи С. П. Расторгуевым предложен алгоритм ее сглаживания, состоящий в добавлении в линию в точках ее разрывов дополнительных точек. Каждая дополнительная точка a с координатами x_a и y_a, добавляемая между точками $i - 1$ и i линии росписи, должна удовлетворять условию

$$\min\,(d_{i-1,\,a} + d_{a,\,i}) \;\forall\; a \;\; d_{i-1,\,a} \le \sqrt{2}.$$

По сглаженной линии росписи можно выделить все замкнутые контуры в ней (по специальному алгоритму).

Процедура настройки на характеристики пользователя может состоять из следующих этапов:

1) ввод нескольких эталонных росписей;

2) для каждой росписи получение числа точек в ней и длины ее линии, определение числа и местоположения разрывов в линии росписи;

3) для каждой линии росписи выполнение сглаживания, получение числа и местоположения замкнутых контуров;

4) расчет среднего значения полученных характеристик росписи и их допустимых отклонений.

Процедура аутентификации состоит из следующих этапов:

1) ввод росписи;

2) расчет числа точек и длины линии росписи;

3) получение числа и местоположения разрывов в линии росписи;

4) сглаживание линии росписи;

5) получение числа и местоположения замкнутых контуров;

6) сравнение полученных характеристик росписи с эталонными;

7) принятие решения о допуске пользователя к работе в КС.

Подобно аутентификации на основе клавиатурного почерка подлинность пользователя по его росписи мышью подтверждается прежде всего темпом его работы с этим устройством ввода.

К достоинствам аутентификации пользователей по их росписи мышью, подобно использованию клавиатурного почерка, относится возможность реализации этого способа только с помощью программных средств; к недостаткам — меньшая достоверность аутентификации по сравнению с применением биометрических характеристик пользователя, а также необходимость достаточно уверенного владения пользователем навыками работы с мышью.

Общей особенностью способов аутентификации, основанных на клавиатурном почерке и росписи мышью является нестабильность их характеристик у одного и того же пользователя, которая может быть вызвана:

1) естественными изменениями, связанными с улучшением навыков пользователя по работе с клавиатурой и мышью или, наоборот, с их ухудшением из-за старения организма;

2) изменениями, связанными с ненормальным физическим или эмоциональным состоянием пользователя.

Изменения характеристик пользователя, вызванные причинами первого рода, не являются скачкообразными, поэтому могут быть нейтрализованы изменением эталонных характеристик после каждой успешной аутентификацией пользователя.

Изменения характеристик пользователя, вызванные причинами второго рода, могут быть скачкообразными и привести к отклонению его попытки входа в КС. Однако эта особенность аутентификации на основе клавиатурного почерка и росписи мышью

может стать и достоинством, если речь идет о пользователях КС военного, энергетического и финансового назначения.

Перспективным направлением развития способов аутентификации пользователей КС, основанных на их личных особенностях, может стать подтверждение подлинности пользователя на основе его знаний и навыков, характеризующих уровень образования и культуры.

2.4. Программно-аппаратная защита информации от локального несанкционированного доступа

Отмеченные в подразд. 2.2 недостатки парольной аутентификации пользователей КС могут быть устранены применением так называемой двухфакторной аутентификации, при которой пользователь для входа в систему должен не только ввести пароль, но и предъявить элемент аппаратного обеспечения, содержащий подтверждающую его подлинность ключевую информацию. Такими элементами аппаратного обеспечения могут быть:

- магнитные диски, не требующие установки на компьютере пользователя КС никаких дополнительных аппаратных средств, но наиболее уязвимые с точки зрения копирования хранящейся на них ключевой информации;
- элементы Touch Memory (аналогичные изделия других производителей именуются iButton), включающие в себя энергонезависимую память в виде постоянного запоминающего устройства (ПЗУ) с уникальным для каждого изделия серийным номером и (в более дорогих вариантах) оперативного запоминающего устройства (ОЗУ) для хранения идентифицирующей пользователя информации, а также встроенный элемент питания со сроком службы до 10 лет (элемент Touch Memory напоминает миниатюрную батарейку диаметром 16 мм и толщиной 3...6 мм, он имеет один сигнальный контакт и один контакт заземления, а для контакта элемента с устройством чтения достаточно простого касания);
- пластиковые карты с магнитной полосой, на которой помимо ключевой информации могут размещаться и дополнительные реквизиты пользователя (его фамилия, имя, отчество, фотография, название организации и ее подразделения и т.п.); подобные карты наиболее дешевы, но и наименее защищены от копирования и подделки;
- карты со штрихкодом, покрытым непрозрачным составом, считывание информации с которых происходит в инфракрасных лучах; эти карты также относительно дешевы, но уязвимы для подделки;
- смарт-карты, носителем ключевой информации в которых является специальная бескорпусная микросхема, включающая в

себя только память для хранения ключевой информации (простые смарт-карты) или микропроцессор (интеллектуальные карты), позволяющий реализовывать достаточно сложные процедуры аутентификации;

• маркеры eToken (USB-брелки), представляющие собой подключаемое к USB-порту компьютера устройство, которое включает в себя аналогичную смарт-карте микросхему с процессором и защищенной от несанкционированного доступа памятью (в отличие от пластиковых карт не требуется установка устройства их чтения с кабелем для подключения этого устройства к компьютеру).

С помощью только программных средств принципиально нельзя обеспечить надежную защиту информации от несанкционированного доступа к ней в КС.

Рассмотрим порядок работы программ после включения питания компьютера и до загрузки операционной системы:

1) программа самопроверки устройств компьютера POST (Power On — Self Test);

2) программа BIOS Setup (может быть вызвана пользователем во время выполнения программы POST, обычно для этого необходимо нажать клавишу Delete);

3) программы BIOS;

4) программы расширения BIOS (BIOS Extension), если соответствующая плата установлена на компьютере;

5) программа начальной загрузки, которая размещается в первом секторе нулевой головки нулевого цилиндра жесткого диска компьютера (Master Boot Record, MBR) и в функции которой входят определение активного раздела жесткого диска и вызов программы загрузки операционной системы;

6) программа загрузки операционной системы, которая размещается в первом секторе активного раздела жесткого диска, загрузочного компакт-диска или загрузочной дискеты;

7) оболочка операционной системы.

Очевидно, что если программа начальной загрузки содержит вредоносный код (программную закладку), то и загруженная затем операционная система будет фактически функционировать под управлением программы нарушителя. Кроме того, если нарушитель получит доступ к коду процедуры хеширования идентифицирующей информации пользователя и данным с хеш-значением этой информации, то он сможет подобрать пароль любого пользователя КС и осуществить несанкционированный доступ к информации. Поэтому для гарантированной работы программно-аппаратного средства защиты от несанкционированной загрузки операционной системы достаточно, чтобы программа защиты и хеш-значения паролей пользователей были аппаратно защищены от чтения программными средствами во время сеанса работы пользователя.

Рассмотрим вариант комплекса программно-аппаратных средств для защиты от локального несанкционированного доступа к информации в КС.

Определим модель (возможности) нарушителя:

- установка системы защиты производится в его отсутствие;
- нарушитель не может вскрыть системный блок компьютера;
- нарушитель не может перезаписать информацию в ПЗУ BIOS при работающем компьютере;
- нарушитель не имеет пароля установки системы защиты;
- нарушитель не имеет пароля пользователя КС;
- нарушитель не имеет копии ключевой информации пользователя, хранящейся в элементе аппаратного обеспечения (например, в элементе Touch Memory).

Выполнение первых двух условий может быть обеспечено только с помощью методов организационной защиты информации (см. подразд. 1.3).

Программные средства системы защиты информации должны быть записаны на плате расширения BIOS, для каждой из которых определен уникальный пароль установки. Установка системы защиты информации производится на компьютере, свободном от вредоносных программ типа закладок и вирусов.

После установки платы расширения BIOS выполняется процедура установки системы защиты информации:

1) после включения питания компьютера программа, записанная на плате расширения BIOS, выдает запрос на ввод пароля;

2) после ввода пароля установки PS (как правило, администратором системы) происходят загрузка операционной системы и запуск собственно программы установки (проверочные функции системы защиты при этом отключаются);

3) по запросу программы установки вводятся пароль пользователя P, ключевая информация с элемента аппаратного обеспечения (например, серийный номер элемента Touch Memory) KI и имена подлежащих проверке системных и пользовательских файлов F_1, F_2, ..., F_n;

4) для каждого указанного файла вычисляется и сохраняется проверочная информация в виде

$$E_k(H(PS,\ P,\ KI,\ F_i)),$$

где E — функция шифрования; k — ключ шифрования; H — функция хеширования.

Рассмотрим процедуру входа пользователя в КС при использовании данной системы защиты:

1) после включения питания компьютера программа на плате расширения BIOS запрашивает пароль пользователя и просит установить элемент аппаратного обеспечения с его ключевой информацией;

2) осуществляется проверка целостности выбранных при установке системы защиты файлов путем вычисления хеш-значения для них по приведенному выше правилу и сравнения с расшифрованными эталонными хеш-значениями;

3) в зависимости от результатов проверки выполняется либо загрузка операционной системы, либо запрос на повторный ввод пароля.

После завершения работы пользователя элемент аппаратного обеспечения с его ключевой информацией изымается из компьютера.

Доступ же к хеш-значению пароля фактически заблокирован, так как программное обеспечение для его вычисления исчезает из адресного пространства компьютера и не может быть прочитано никакими программными средствами без извлечения платы расширения BIOS.

Если у нарушителя нет пароля пользователя или копии элемента аппаратного обеспечения с его ключевой информацией, то он не сможет выполнить загрузку операционной системы. Если у нарушителя есть пароль установки системы защиты, что позволит ему загрузить операционную систему без проверочных функций, или он получил доступ к терминалу с уже загруженной операционной системой, то он сможет осуществить несанкционированный доступ (НСД) к информации, но не сможет внедрить программные закладки для постоянного НСД. Наличие у нарушителя пароля установки без знания им пароля пользователя или его ключевой информации не позволит нарушителю переустановить систему защиты для постоянного НСД.

Для защиты от несанкционированного доступа к информации в ситуации, когда нарушитель получил доступ к работающему терминалу, необходимо использовать средства разграничения доступа к ресурсам КС или средства шифрования.

2.5. Аутентификация пользователей при удаленном доступе. Защита информации от несанкционированного доступа в сетях

Простейшим протоколом, который может быть использован для удаленного доступа пользователя к КС, является протокол PAP (Password Authentication Protocol). Пусть С обозначает сервер КС, П — пользователя КС с логическим именем ID и паролем P, а К — удаленный компьютер, с которого пользователь пытается получить доступ к КС при помощи соответствующей клиентской программы.

1. К→С: ID, P′ (запрос аутентификации).

2. С: выборка Р из регистрационной базы данных; сравнение Р и Р′.

3. С→К: если пароли совпадают, то подтверждение аутентификации, в противном случае — отказ в аутентификации и разрыв соединения.

Независимо от формы передачи информации о пароле (в открытом виде, зашифрованном или хешированном) нарушитель может ее перехватить и использовать для несанкционированного доступа к информации в КС с помощью «маскарада». Поэтому протокол PAP может использоваться только совместно с протоколом S/Key.

Идея протокола S/Key основывается на модели одноразовых паролей, получаемых последовательным применением необратимой функции (см. подразд. 2.2). Сервер С инициализирует список из М одноразовых паролей на основе пароля Р пользователя П, вычисляет и сохраняет в регистрационной базе данных проверочное значение $Y_{M+1} = F^{M+1}(P)$. В регистрационной базе данных КС для каждого пользователя также сохраняются значения ID, Р и М, причем только пароль пользователя Р является конфиденциальной информацией.

При очередной аутентификации пользователя удаленный компьютер (клиент) К посылает серверу логическое имя пользователя ID, а сервер в ответ направляет клиенту значение М. Клиент вычисляет значение Y'_M и отправляет его серверу, который вычисляет $Y'_{M+1} = F(Y'_M)$ и сравнивает Y'_{M+1} с извлеченным из базы данных учетных записей значением Y_{M+1}. При совпадении этих значений пользователь допускается к работе в КС, а в его учетной записи значение М уменьшается на единицу, а вместо Y_{M+1} записывается Y'_M.

Для того чтобы можно было сгенерировать новый список одноразовых паролей без личного присутствия пользователя (с удаленного компьютера), а также для повышения безопасности этого списка вычисление одноразовых паролей может быть организовано на базе не только пароля Р, но и генерируемого сервером случайного числа.

Протокол S/Key состоит из двух частей: генерации списка одноразовых паролей (парольной инициализации) и собственно аутентификации.

Рассмотрим процедуру парольной инициализации.

1. С→К: запрос ID.

2. К→С: ID.

3. С: генерация случайного числа (кода инициализации) N.

4. С→К: запрос числа М одноразовых паролей, которые будут использоваться до следующей парольной инициализации (возможно задание этого значения администратором системы, обычно М выбирается в диапазоне 300 ... 1000).

5. К→С: M.

6. С: по логическому имени пользователя ID извлечение из регистрационной базы данных значения P; вычисление $Y_{M+1} = F^{M+1}(N,P)$; сохранение N, M, Y_{M+1} вместе с ID и P в регистрационной базе данных.

В этом варианте парольной инициализации не требуется передача по сети пароля пользователя P для генерации нового списка одноразовых паролей.

Рассмотрим процедуру аутентификации по протоколу S/Key.

1. К→С: ID.

2. С: извлечение из регистрационной базы данных соответствующих ID значений P, N, M, Y_{M+1}.

3. С→К: N, M.

4. П→К: P′.

5. К: вычисление $Y'_M = F^M(N, P')$.

6. К→С: Y'_M.

7. С: вычисление $Y'_{M+1} = F(Y'_M)$; сравнение Y'_{M+1} и Y_{M+1}; если эти значения совпадают, то пользователь допускается к работе, а в регистрационной базе данных соответствующее ID значение Y_{M+1} заменяется значением Y'_M, а значение M уменьшается на единицу.

Для ускорения процедуры аутентификации некоторое значение одноразовых паролей (например, 50) может быть вычислено на клиентском компьютере заранее, а для сохранения конфиденциальности — сохраняться на этом компьютере в зашифрованном виде с использованием ключа шифрования, равного паролю пользователя P.

Парольная инициализация должна выполняться:

- после назначения или изменения пароля пользователя P;
- после использования для аутентификации последнего пароля из списка (когда M станет равным нулю);
- при вероятной компрометации списка паролей, когда номер пароля, запрашиваемый сервером, меньше номера, ожидаемого клиентом.

Еще одним протоколом удаленной аутентификации пользователей КС является протокол CHAP (Challenge Handshake Authentication Protocol), основанный на модели «рукопожатия». Идеей протокола CHAP является передача клиентом пароля в хешированном виде с использованием полученного от сервера случайного числа.

1. С: генерация случайного числа N.

2. С→К: идентификатор сервера IDS, N и его длина в байтах (вызов).

3. П→К: P′.

4. К: вычисление хеш-значения D′ = H(IDS, N, P′).

5. К→С: ID, D′ (отклик).

6. С: извлечение из регистрационной базы данных соответствующего ID значения P; вычисление хеш-значения D = H(IDS, N, P); сравнение D′ и D.

7. С→К: если значения совпадают, то подтверждение аутентификации, в противном случае — отказ в аутентификации и разрыв соединения.

Используемое в протоколе CHAP значение N должно быть уникальным и непредсказуемым. Если N не уникально, то нарушитель сможет повторно использовать перехваченный им пакет с откликом клиента для несанкционированного доступа к информации на сервере в форме «маскарада». Если значение N предсказуемо, то нарушитель сможет подобрать его и, сформировав пакет с вызовом, послать его клиенту от лица сервера. Полученный от клиента пакет с откликом нарушитель сохраняет для последующей отправки от лица клиента, когда реальный сервер направит клиенту аналогичный пакет с вызовом.

Обычно в качестве N выбирается последовательность битов, представляющая собой значение текущих даты и времени в секундах, к которой присоединяется случайное число, полученное от программного или аппаратного генератора псевдослучайных чисел.

Если в распределенной компьютерной системе имеется несколько серверов, предоставляющих свои сервисы клиентам, то для надежной аутентификации пользователей КС, которые обращаются к ее серверам с различных рабочих станций, и самих серверов может использоваться протокол аутентификации Kerberos. Этот протокол предполагает использование центрального сервера аутентификации СА, в функции которого и входит идентификация серверов и пользователей КС, а также сервера выдачи мандатов (или билетов, ticket) СВМ на доступ пользователей КС к ее серверам.

Для обеспечения конфиденциальности передаваемой по сети информации в протоколе Kerberos используются функция шифрования E и сеансовые (используемые однократно) ключи шифрования для передачи данных между клиентом и сервером выдачи мандатов (Kcts), а также между клиентом и сервером КС с необходимым клиенту сервисом (Kcs). Сервер выдачи мандатов имеет постоянный ключ шифрования Kts, который известен и каждому серверу КС. Каждый из предоставляющих свои сервисы клиентам серверов также имеет постоянный ключ шифрования Ks, который в свою очередь известен серверу выдачи мандатов. Постоянные ключи шифрования серверов КС распределяются в системе по защищенному от несанкционированного доступа каналу.

Для исключения возможности повторного использования нарушителем мандата, выданного легальному пользователю, в протоколе Kerberos в передаваемые по сети мандаты добавляются штампы времени TS и информация о периоде действия мандатов TA (как правило, 8 ч).

Рассмотрим одну из версий протокола Kerberos (IDS — идентификатор сервера КС; IDT — идентификатор сервера выдачи мандатов; T_{ts} — мандат на получение мандата у СВМ; T_s — мандат на получение сервиса у сервера КС; AD — адрес рабочей станции пользователя; A — аутентификатор клиента).

1. K→CA: ID, IDT, TS_1.
2. CA: вычисление $T_{ts} = E_{Kts}(Kcts, ID, AD, IDT, TS_2, TA_2)$.
3. CA→K: $E_P(Kcts, IDT, TS_2, TA_2, T_{ts})$.
4. K: вычисление $A_1 = E_{Kcts}(ID, AD, TS_3)$.
5. K→CBM: IDS, T_{ts}, A_1.
6. CBM: вычисление $T_s = E_{Ks}(Kcs, ID, AD, IDS, TS_4, TA_4)$.
7. CBM→K: $E_{Kcts}(Kcs, ID, TS_4, T_s)$.
8. K: вычисление $A_2 = E_{Kcs}(ID, AD, TS_5)$.
9. K→C: T_s, A_2.
10. C→K: $E_{Kcs}(TS_5 + 1)$.

Пункты 1...3 протокола Kerberos (обмен службы аутентификации) предназначены для получения клиентом мандата на получение мандата, который включает в себя помимо идентификаторов адреса и отметки времени, а также сеансовый ключ для обмена между клиентом и сервером выдачи мандатов. Только клиент, работающий в интересах пользователя и знающий его пароль P, может расшифровать полученное от сервера аутентификации сообщение, содержащее запрашиваемый мандат.

Пункты 4...7 протокола Kerberos (обмен службы выдачи мандатов) предназначены для получения клиентом мандата на получение сервиса. При обращении к серверу выдачи мандатов клиент добавляет к сообщению аутентификатор, который будет использоваться только один раз, в отличие от предполагающего многократное использование мандата, и имеет весьма ограниченный срок действия. Сервер выдачи мандатов может проверить подлинность клиента с помощью аутентификатора, который он расшифровывает при помощи сеансового ключа, извлеченного из мандата на получение мандата.

Пункты 8...10 протокола Kerberos (обмен аутентификации клиента и сервера) предназначены для получения клиентом требуемого сервиса. Вместе с мандатом на получение сервиса клиент высылает серверу и свой аутентификатор. Сервер проверяет подлинность клиента с помощью этого аутентификатора, который он расшифровывает, используя извлеченный из мандата сеансовый ключ. Для подтверждения собственной подлинности перед клиентом сервер отвечает ему сообщением, содержащим увеличенную на единицу отметку времени, которая была извлечена сервером из аутентификатора клиента. Это сообщение зашифровывается на сеансовом ключе, извлеченном из полученного сервером мандата. Это убеждает клиента, что данное сообщение могло быть отправлено только сервером.

Теперь клиент и сервер имеют общий сеансовый ключ, который они могут использовать для обмена зашифрованными сообщениями и обмена новыми сеансовыми ключами.

К достоинствам протокола Kerberos относятся:

- более быстрое подсоединение клиента к серверу, так как серверу не требуется обращаться к серверу аутентификации для подтверждения подлинности клиента, что приводит к улучшению масштабируемости распределенной КС;
- возможность делегирования клиентом своих полномочий серверу для выполнения запроса;
- упрощение администрирования распределенной КС.

Основные причины, облегчающие нарушителю реализацию угроз безопасности информации в распределенных КС:

- отсутствие выделенного канала связи между объектами распределенной КС (наличие широковещательной среды передачи данных, например среды Ethernet), что позволяет нарушителю анализировать сетевой трафик в подобных системах;
- возможность взаимодействия объектов распределенной КС без установления виртуального канала между ними, что не позволяет надежно идентифицировать объект или субъект распределенной КС и организовать защиту передаваемой информации;
- использование недостаточно надежных протоколов идентификации объектов распределенной КС перед установлением виртуального канала между ними, что позволяет нарушителю при перехвате передаваемых сообщений выдать себя за одну из сторон соединения;
- отсутствие контроля создания и использования виртуальных каналов между объектами распределенной КС, что позволяет нарушителю добиться реализации угрозы отказа в обслуживании в КС (например, любой объект распределенной КС может анонимно послать любое число сообщений от имени других объектов КС);
- отсутствие возможности контроля маршрута получаемых сообщений, что не позволяет подтвердить адрес отправителя данных и определить инициатора удаленной атаки на КС;
- отсутствие полной информации об объектах КС, с которыми требуется создать соединение, что приводит к необходимости отправки широковещательного запроса или подключения к поисковому серверу (нарушитель при этом имеет возможность внедрения ложного объекта в распределенную КС и выдать один из ее объектов за другой);
- отсутствие шифрования передаваемых сообщений, что позволяет нарушителю получить несанкционированный доступ к информации в распределенной КС.

Выделим основные методы создания безопасных распределенных КС:

- использование выделенных каналов связи путем физического соединения каждой пары объектов распределенной КС или при-

менения топологии «звезда» и сетевого коммутатора, через который осуществляется связь между объектами;

• разработка дополнительных средств идентификации объектов распределенной КС перед созданием виртуального канала связи между ними и применение средств шифрования передаваемой по этому каналу информации;

• контроль маршрута поступающих сообщений;

• контроль создания и использования виртуального соединения между объектами распределенной КС (например, ограничение числа запросов от одного из объектов и разрыв соединения после истечения определенного интервала времени);

• разработка распределенной КС с полной информацией об ее объектах, если это возможно, или организация взаимодействия между объектом КС и поисковым сервером только с созданием виртуального канала.

Среди программно-аппаратных и программных средств обеспечения информационной безопасности распределенных КС можно выделить межсетевые экраны (МСЭ), средства анализа защищенности и средства обнаружения атак.

Межсетевые экраны (брандмауэры, firewall) реализуют набор правил, которые определяют условия прохождения пакетов данных из одной части распределенной КС (открытой) в другую (защищенную). Обычно межсетевые экраны устанавливаются между сетью Интернет и локальной вычислительной сетью организации (рис. 2.2), хотя они могут размещаться и внутри корпоративной сети. В зависимости от уровня взаимодействия объектов сети основными разновидностями МСЭ являются фильтрующие маршрутизаторы, шлюзы сеансового и прикладного уровней. Как правило, в состав МСЭ включаются компоненты, соответствующие двум или всем трем указанным разновидностям.

Основной функцией фильтрующих маршрутизаторов, работающих на сетевом уровне эталонной модели, является фильтрация

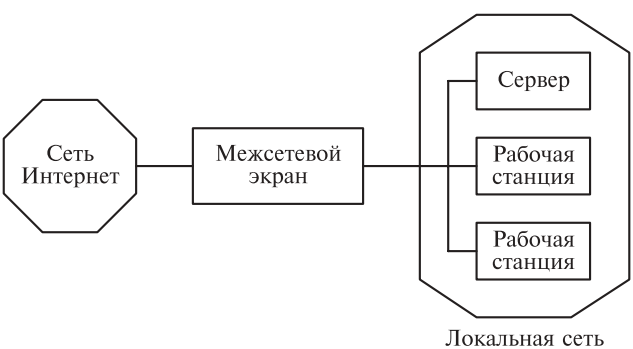

Рис. 2.2. Пример размещения межсетевого экрана