В.И. ЗАВГОРОДНИЙ

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Рекомендовано Учебно-методическим объединением по образованию в области статистики, прикладной информатики и математических методов в экономике в качестве учебного пособия для студентов высших учебных заведений

Москва • «Логос» • 2001

УДК 681.322.067
ББК 32.973-018.2
3-13

Рецензенты:
кафедра вычислительной техники Финансовой академии при Правительстве Российской Федерации (зав.каф. - канд. техн. наук проф. *В.П. Косарев);* доктор техн. наук. проф. *А.П. Пятибратов* (Московский экономико-статистический институт)

Завгородний В.И.

3-13 Комплексная защита информации в компьютерных системах: Учебное пособие. - М.: Логос; ПБОЮЛ Н.А. Егоров, 2001. - 264 с : ил.

ISBN 5-94010-088-0

Освещаются вопросы защиты информации в компьютерных системах. Анализируются и классифицируются возможные угрозы безопасности информации, рассматриваются методы и средства защиты от незаконного проникновения в вычислительные сети, раскрываются подходы к построению и эксплуатации комплексных систем защиты.

Для студентов высших учебных заведений, специалистов в области информационных технологий и защиты информации, широкого круга пользователей компьютерных систем.

ББК 32.973-018.2

ISBN 5-94010-088-0

Оглавление

ВВЕДЕНИЕ

Вступление человечества в XXI век знаменуется бурным развитием информационных технологий во всех сферах общественной жизни. Информация все в большей мере становится стратегическим ресурсом государства, производительной силой и дорогим товаром. Это не может не вызывать стремления государств, организаций и отдельных граждан получить преимущества за счет овладения информацией, недоступной оппонентам, а также за счет нанесения ущерба информационным ресурсам противника (конкурента) и защиты своих информационных ресурсов.

Значимость обеспечения безопасности государства в информационной сфере подчеркнута в принятой в сентябре 2000 года «Доктрине информационной безопасности Российской Федерации»[1]: "Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать".

Остроту межгосударственного информационного противоборства можно наблюдать в оборонной сфере, высшей формой которой являются информационные войны. Элементы такой войны уже имели место в локальных военных конфликтах на Ближнем Востоке и на Балканах. Так, войскам НАТО удалось вывести из строя систему противовоздушной обороны Ирака с помощью информационного оружия. Эксперты предполагают, что войска альянса использовали программную закладку, внедренную заблаговременно в принтеры, которые были закуплены Ираком у французской фирмы и использовались в АСУ ПВО.

Не менее остро стоит вопрос информационного противоборства и на уровне организаций, отдельных граждан. Об этом свидетельствуют многочисленные попытки криминальных элементов получить контроль над компьютерными технологиями для извлечения материальной выгоды. Достаточно привести в качестве примера случаи шантажа английских фирм преступной междуна-

[1] Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 09.09.2000 г. // Российская газета, 28 сентября 2000 г.

родной группой. За 1993-1996 годы преступники получили 40 миллионов фунтов стерлингов. Жертвам приходилось выплачивать до 13 миллионов фунтов стерлингов единовременно после демонстрации шантажистами своих возможностей остановить все сделки или получить доступ к новейшим разработкам фирм. Деньги переводились в банки, расположенные в оффшорных зонах, откуда преступники снимали их в считанные минуты.

Важно также обеспечить конституционные права граждан на получение достоверной информации, на ее использование в интересах осуществления законной деятельности, а также на защиту информации, обеспечивающую личную безопасность.

Противоборство государств в области информационных технологий, стремление криминальных структур противоправно использовать информационные ресурсы, необходимость обеспечения прав граждан в информационной сфере, наличие множества случайных угроз вызывают острую -необходимость обеспечения защиты информации в компьютерных системах (КС), являющихся материальной основой информатизации общества.

Проблема обеспечения информационной безопасности на всех уровнях может быть решена успешно только в том случае, если создана и функционирует комплексная система защиты информации, охватывающая весь жизненный цикл компьютерных систем от разработки до утилизации и всю технологическую цепочку сбора, хранения, обработки и выдачи информации. Вопросы построения и организации функционирования такой системы защиты рассматриваются в настоящем учебном пособии. Оно позволит выработать у читателей целостный, системный взгляд на проблему защиты информации в компьютерных системах.

В первом разделе даются общие понятия, раскрываются термины теории защиты информации, приводятся правовые основы защиты информации, анализируются возможные угрозы безопасности информации в КС. В наибольшем по объему втором разделе рассматриваются средства и методы защиты информации. В заключительном третьем разделе рассматривается проблема построения и организации функционирования систем защиты информации в КС.

I. ОСНОВНЫЕ ПОНЯТИЯ И ПОЛОЖЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

ГЛАВА 1
Предмет и объект защиты

1.1. Предмет защиты

В Федеральном законе РФ «Об информации, информатизации и защите информации», принятом 25 января 1995года Государственной Думой [50], определено, что «информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления». Информация имеет ряд особенностей [48]:

- она нематериальна;
- информация хранится и передается с помощью материальных носителей;
- любой материальный объект содержит информацию о самом себе или о другом объекте.

Нематериальность информации понимается в том смысле, что нельзя измерить ее параметры известными физическими методами и приборами. Информация не имеет массы, энергии и т. п.

Информация хранится и передается на материальных носителях. Такими носителями являются мозг человека, звуковые и электромагнитные волны, бумага, машинные носители (магнитные и оптические диски, магнитные ленты и барабаны) и др.

Информации присущи следующие свойства [48].

1. ***Информация доступна человеку, если она содержится на материальном носителе.*** Поэтому необходимо защищать материальные носители информации, так как с помощью материальных средств можно защищать только материальные объекты.

2. *Информация имеет ценность.* Ценность информации определяется степенью ее полезности для владельца. Обладание истинной (достоверной) информацией дает ее владельцу определенные преимущества. Истинной или достоверной информацией является информация, которая с достаточной для владельца (пользователя) точностью отражает объекты и процессы окружающего мира в определенных временных и пространственных рамках.

Информация, искаженно представляющая действительность (недостоверная информация), может нанести владельцу значительный материальный и моральный ущерб. Если информация искажена умышленно, то ее называют *дезинформацией.*

Законом «Об информации, информатизации и защите информации» гарантируется право собственника информации на ее использование и защиту от доступа к ней других лиц (организаций). Если доступ к информации ограничивается, то такая информация является *конфиденциальной.* Конфиденциальная информация может содержать государственную или коммерческую тайну. *Коммерческую тайну* могут содержать сведения, принадлежащие частному лицу, фирме, корпорации и т. п. *Государственную* тайну могут содержать сведения, принадлежащие государству (государственному учреждению). В соответствии с законом «О государственной тайне» [17] сведениям, представляющим ценность для государства, может быть присвоена одна из трех возможных степеней секретности. В порядке возрастания ценности (важности) информации ей может быть присвоена степень (гриф) *«секретно», «совершенно секретно»* или *«особой важности»*. В государственных учреждениях менее важной информации может присваиваться гриф *«для служебного пользования»*.

Для обозначения ценности конфиденциальной коммерческой информации используются три категории:

- «коммерческая тайна - строго конфиденциально»;
- «коммерческая тайна - конфиденциально»;
- «коммерческая тайна».

Используется и другой подход к градации ценности коммерческой информации:

- «строго конфиденциально - строгий учет»;
- «строго конфиденциально»;
- «конфиденциально».

3.*Ценностьинформациииизменяетсявовремени.*

Как правило, со временем ценность информации уменьшается. Зависимость ценности информации от времени приближенно определяется в соответствии с выражением:

$$C(t) = C_0 e^{-2.3t/\tau},$$

где Со - ценность информации в момент ее возникновения (получения); t - время от момента возникновения информации до момента определения ее стоимости; т - время от момента возникновения информации до момента ее устаревания.

Время, через которое информация становится устаревшей, меняется в очень широком диапазоне. Так, например, для пилотов реактивных самолетов, автогонщиков информация о положении машин в пространстве устаревает за доли секунд. В то же время информация о законах природы остается актуальной в течение многих веков.

4.*Информацияпокупаетсяипродается.*

Ее правомочно рассматривать как товар, имеющий определенную цену. Цена, как и ценность информации, связаны с полезностью информации для конкретных людей, организаций, государств. Информация может быть ценной для ее владельца, но бесполезной для других. В этом случае информация не может быть товаром, а, следовательно, она не имеет и цены. Например, сведения о состоянии здоровья обычного гражданина являются ценной информацией для него. Но эта информация, скорее всего, не заинтересует кого-то другого, а, следовательно, не станет товаром, и не будет иметь цены.

Информация может быть получена тремя путями:

- проведением научных исследований;
- покупкой информации;
- противоправным добыванием информации.

Как любой товар, информация имеет себестоимость, которая определяется затратами на ее получение. Себестоимость зависит от выбора путей получения информации и минимизации затрат при добывании необходимых сведений выбранным путем. Информация добывается с целью получения прибыли или преимуществ перед конкурентами, противоборствующими сторонами. Для этого информация:

- продается на рынке;

- внедряется в производство для получения новых технологий и товаров, приносящих прибыль;
- используется в научных исследованиях;
- позволяет принимать оптимальные решения в управлении.

5. *Сложность объективной оценки количества информации.*

Существует несколько подходов к измерению количества информации.

А. Энтропийный подход.

В теории информации количество информации оценивается мерой уменьшения у получателя неопределенности (энтропии) выбора или ожидания событий после получения информации. Количество информации тем больше, чем ниже вероятность события. Энтропийный подход широко используется при определении количества информации, передаваемой по каналам связи. Выбор при приеме информации осуществляется между символами алфавита в принятом сообщении. Пусть сообщение, принятое по каналу связи, состоит из N символов (без учета связи между символами в сообщении). Тогда количество информации в сообщении может быть подсчитано по формуле Шеннона [59]:

$$I = N \sum_{i=1}^{k} P_i \log_2 P_i ,$$

где Pi - вероятность появления в сообщении символа i; к - количество символов в алфавите языка.

Анализ формулы Шеннона показывает, что количество информации в двоичном представлении (в битах или байтах) зависит от двух величин: количества символов в сообщении и частоты появления того или иного символа в сообщениях для используемого алфавита. Этот подход абсолютно не отражает насколько полезна полученная информация, а позволяет определить лишь затраты на передачу сообщения.

Б. Тезаурусный подход.

Этот подход предложен Ю.А. Шрейдером [60]. Он основан на рассмотрении информации как знаний. Согласно этому подходу количество информации, извлекаемое человеком из сообщения, можно оценить степенью изменения его знаний. Структурированные знания, представленные в виде понятий и отношений между

ними, называются тезаурусом. Структура тезауруса иерархическая. Понятия и отношения, группируясь, образуют другие, более сложные понятия и отношения.

Знания отдельного человека, организации, государства образуют соответствующие тезаурусы. Тезаурусы организационных структур образуют тезаурусы составляющих их элементов. Так тезаурус организации образуют, прежде всего, тезаурусы сотрудников, а также других носителей информации, таких как документы, оборудование, продукция и т. д.

Для передачи знаний требуется, чтобы тезаурусы передающего и принимающего элемента пересекались. В противном случае владельцы тезаурусов не поймут друг друга.

Тезаурусы человека и любых организационных структур являются их капиталом. Поэтому владельцы тезаурусов стремятся сохранить и увеличить свой тезаурус. Увеличение тезауруса осуществляется за счет обучения, покупки лицензии, приглашения квалифицированных сотрудников или хищения информации.

В обществе наблюдаются две тенденции: развитие тезаурусов отдельных элементов (людей, организованных структур) и выравнивание тезаурусов элементов общества.

Выравнивание тезаурусов происходит как в результате целенаправленной деятельности (например, обучения), так и стихийно. Стихийное выравнивание тезаурусов происходит за счет случайной передачи знаний, в том числе и незаконной передачи.

В. Практический подход.

На практике количество информации измеряют, используя понятие «объем информации». При этом количество информации может измеряться в количестве бит (байт), в количестве страниц текста, длине магнитной ленты с видео- или аудиозаписью и т.п. Однако очевидно, что на одной странице информации может содержаться больше или меньше, по крайней мере, по двум причинам. Во-первых, разные люди могут разместить на странице различное количество сведений об одном и том же объекте, процессе или явлении материального мира. Во-вторых, разные люди могут извлечь из одного и того же текста различное количество полезной, понятной для них информации. Даже один и тот же человек в разные годы жизни получает разное количество информации при чтении книги.

В результате копирования без изменения информационных параметров носителя количество информации не изменяется, а цена снижается. Примером копирования без изменения информационных параметров может служить копирование текста с использованием качественных копировальных устройств. Текст копии, при отсутствии сбоев копировального устройства, будет содержать точно такую же информацию, как и текст оригинала. Но при копировании изображений уже не удастся избежать искажений. Они могут быть только большими или меньшими.

В соответствии с законами рынка, чем больше товара появляется, тем он дешевле. Этот закон полностью справедлив и в отношении копий информации. Действие этого закона можно проследить на примере пиратского распространения программных продуктов, видеопродукции и т. п.

В качестве **предмета защиты** рассматривается информация, хранящаяся, обрабатываемая и передаваемая в компьютерных системах. Особенностями этой информации являются:

- двоичное представление информации внутри системы, независимо от физической сущности носителей исходной информации;
- высокая степень автоматизации обработки и передачи информации;
- концентрация большого количества информации в КС.

1.2. Объект защиты информации

Объектом защиты информации является компьютерная система или автоматизированная система обработки данных (АСОД). В работах, посвященных защите информации в автоматизированных системах, до последнего времени использовался термин АСОД, который все чаще заменяется термином КС. Что же понимается под этим термином?

Компьютерная система - это комплекс аппаратных и программных средств, предназначенных для автоматизированного сбора, хранения, обработки, передачи и получения информации. Наряду с термином «информация» применительно к КС часто используют термин «данные». Используется и другое понятие - «информационные ресурсы». В соответствии с законом РФ «Об

информации, информатизации и защите информации» под информационными ресурсами понимаются отдельные документы и отдельные массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных и других информационных системах).

Понятие КС очень широкое и оно охватывает следующие системы:

- ЭВМ всех классов и назначений;
- вычислительные комплексы и системы;
- вычислительные сети (локальные, региональные и глобальные).

Такой широкий диапазон систем объединяется одним понятием по двум причинам: во-первых, для всех этих систем основные проблемы защиты информации являются общими; во-вторых, более мелкие системы являются элементами более крупных систем. Если защита информации в каких-либо системах имеет свои особенности, то они рассматриваются отдельно.

Предметом защиты в КС является информация. Материальной основой существования информации в КС являются электронные и электромеханические устройства (подсистемы), а также машинные носители. С помощью устройств ввода или систем передачи данных (СПД) информация попадает в КС. В системе информация хранится в запоминающих устройствах (ЗУ) различных уровней, преобразуется (обрабатывается) процессорами (ПЦ) и выводится из системы с помощью устройств вывода или СПД. В качестве машинных носителей используются бумага, магнитные ленты, диски различных типов. Ранее в качестве машинных носителей информации использовались бумажные перфокарты и перфоленты, магнитные барабаны и карты. Большинство типов машинных носителей информации являются съемными, т.е. могут сниматься с устройств и использоваться (бумага) или храниться (ленты, диски, бумага) отдельно от устройств.

Таким образом, для защиты информации (обеспечения безопасности информации) в КС необходимо защищать устройства (подсистемы) и машинные носители от несанкционированных (неразрешенных) воздействий на них.

Однако такое рассмотрение КС с точки зрения защиты информации является неполным. Компьютерные системы относятся

к классу человеко-машинных систем. Такие системы эксплуатируются специалистами (обслуживающим персоналом) в интересах пользователей. Причем, в последние годы пользователи имеют самый непосредственный доступ к системе. В некоторых КС (например, ПЭВМ) пользователи выполняют функции обслуживающего персонала. Обслуживающий персонал и пользователи являются также носителями информации. Поэтому от несанкционированных воздействий необходимо защищать не только устройства и носители, но также обслуживающий персонал и пользователей.

При решении проблемы защиты информации в КС необходимо учитывать также противоречивость человеческого фактора системы. Обслуживающий персонал и пользователи могут быть как объектом, так и источником несанкционированного воздействия на информацию.

Понятие **«объект защиты»** или **«объект»** чаще трактуется в более широком смысле. Для сосредоточенных КС или элементов распределенных систем понятие «объект» включает в себя не только информационные ресурсы, аппаратные, программные средства, обслуживающий персонал, пользователей, но и помещения, здания, и даже прилегающую к зданиям территорию.

Одними из основных понятий теории защиты информации являются понятия «безопасность информации» и «защищенные КС». **Безопасность (защищенность) информации в КС** - это такое состояние всех компонент компьютерной системы, при котором обеспечивается защита информации от возможных угроз на требуемом уровне. Компьютерные системы, в которых обеспечивается безопасность информации, называются **защищенными.**

Безопасность информации в КС (информационная безопасность) является одним из основных направлений обеспечения безопасности государства, отрасли, ведомства, государственной организации или частной фирмы.

Информационная безопасность достигается проведением руководством соответствующего уровня **политики информационной безопасности.** Основным документом, на основе которого проводится политика информационной безопасности, является **программа информационной безопасности.** Этот документ разрабатывается и принимается как официальный руководящий документ высшими органами управления государством, ведомст-

вом, организацией. В документе приводятся цели политики информационной безопасности и основные направления решения задач защиты информации в КС. В программах информационной безопасности содержатся также общие требования и принципы построения систем защиты информации в КС.

Под **системой защиты информации в КС** понимается единый комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в КС в соответствии с принятой политикой безопасности.

Контрольные вопросы

1. Охарактеризуйте информацию и ее свойства.
2. Что является объектом защиты информации?
3. Дайте характеристику основных понятий теории защиты информации.

ГЛАВА 2
Угрозы безопасности информации в компьютерных системах

С позиции обеспечения безопасности информации в КС такие системы целесообразно рассматривать в виде единства трех компонент, оказывающих взаимное влияние друг на друга:

- информация;
- технические и программные средства;
- обслуживающий персонал и пользователи.

В отношении приведенных компонент иногда используют и термин «информационные ресурсы», который в этом случае трактуется значительно шире, чем в Федеральном законе РФ «Об информации, информатизации и защите информации».

Целью создания любой КС является удовлетворение потребностей пользователей в своевременном получении достоверной информации и сохранении ее конфиденциальности (при необходимости). Информация является конечным «продуктом потребле-

ния» в КС и выступает в виде центральной компоненты системы. Безопасность информации на уровне КС обеспечивают две другие компоненты системы. Причем эта задача должна решаться путем защиты от внешних и внутренних неразрешенных (несанкционированных) воздействий. Особенности взаимодействия компонент заключаются в следующем. Внешние воздействия чаще всего оказывают несанкционированное влияние на информацию путем воздействия на другие компоненты системы. Следующей особенностью является возможность несанкционированных действий, вызываемых внутренними причинами, в отношении информации со стороны технических, программных средств, обслуживающего персонала и пользователей. В этом заключается основное противоречие взаимодействия этих компонент с информацией. Причем, обслуживающий персонал и пользователи могут сознательно осуществлять попытки несанкционированного воздействия на информацию. Таким образом, обеспечение безопасности информации в КС должно предусматривать защиту всех компонент от внешних и внутренних воздействий (угроз).

Под **угрозой безопасности информации** понимается потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности, конфиденциальности или доступности информации.

Все множество потенциальных угроз безопасности информации в КС может быть разделено на два класса (рис 1).

2.1. Случайные угрозы

Угрозы, которые не связаны с преднамеренными действиями злоумышленников и реализуются в случайные моменты времени, называют **случайными** или **непреднамеренными.**

Реализация угроз этого класса приводит к наибольшим потерям информации (по статистическим данным - до 80% от ущерба, наносимого информационным ресурсам КС любыми угрозами). При этом могут происходить уничтожение, нарушение целостности и доступности информации. Реже нарушается конфиденциальность информации, однако при этом создаются предпосылки для злоумышленного воздействия на информацию.

Стихийные бедствия и аварии чреваты наиболее разрушительными последствиями для КС, т.к. последние подвергаются физическому разрушению, информация утрачивается или доступ к ней становится невозможен.

Рис. 1. Угрозы безопасности информации в компьютерных системах

Сбои и отказы сложных систем неизбежны. В результате сбоев и отказов нарушается работоспособность технических средств, уничтожаются и искажаются данные и программы, нарушается алгоритм работы устройств. Нарушения алгоритмов работы от-

дельных узлов и устройств могут также привести к нарушению конфиденциальности информации. Например, сбои и отказы средств выдачи информации могут привести к несанкционированному доступу к информации путем несанкционированной ее выдачи в канал связи, на печатающее устройство и т. п.

Ошибки при разработке КС, алгоритмические и программные ошибки приводят к последствиям, аналогичным последствиям сбоев и отказов технических средств. Кроме того, такие ошибки могут быть использованы злоумышленниками для воздействия на ресурсы КС. Особую опасность представляют ошибки в операционных системах (ОС) и в программных средствах зашиты информации.

Согласно данным Национального Института Стандартов и Технологий США (NIST) 65% случаев нарушения безопасности информации происходит в результате *ошибок пользователей и обслуживающего персонала.* Некомпетентное, небрежное или невнимательное выполнение функциональных обязанностей сотрудниками приводят к уничтожению, нарушению целостности и конфиденциальности информации, а также компрометации механизмов защиты.

Характеризуя угрозы информации в КС, не связанные с преднамеренными действиями, в целом, следует отметить, что механизм их реализации изучен достаточно хорошо, накоплен значительный опыт противодействия этим угрозам. Современная технология разработки технических и программных средств, эффективная система эксплуатации КС, включающая обязательное резервирование информации, позволяют значительно снизить потери от реализации угроз этого класса.

2.2. Преднамеренные угрозы

Второй класс угроз безопасности информации в КС составляют преднамеренно создаваемые угрозы.

Данный класс угроз изучен недостаточно, очень динамичен и постоянно пополняется новыми угрозами. Угрозы этого класса в соответствии с их физической сущностью и механизмами реализации могут быть распределены по пяти группам:

- традиционный или универсальный шпионаж и диверсии;

- несанкционированный доступ к информации;
- электромагнитные излучения и наводки;
- модификация структур КС;
- вредительские программы.

2.2.1. Традиционный шпионаж и диверсии

В качестве источников нежелательного воздействия на информационные ресурсы по-прежнему актуальны *методы и средства шпионажа и диверсий,* которые использовались и используются для добывания или уничтожения информации на объектах, не имеющих КС. Эти методы также действенны и эффективны в условиях применения компьютерных систем. Чаще всего они используются для получения сведений о системе защиты с целью проникновения в КС, а также для хищения и уничтожения информационных ресурсов.

К методам шпионажа и диверсий относятся:

- подслушивание;
- визуальное наблюдение;
- хищение документов и машинных носителей информации;
- хищение программ и атрибутов системы защиты;
- подкуп и шантаж сотрудников;
- сбор и анализ отходов машинных носителей информации;
- поджоги;
- взрывы.

Для *подслушивания* злоумышленнику не обязательно проникать на объект. Современные средства позволяют подслушивать разговоры с расстояния нескольких сотен метров. Так прошла испытания система подслушивания, позволяющая с расстояния 1 км фиксировать разговор в помещении с закрытыми окнами [23]. В городских условиях дальность действия устройства сокращается до сотен и десятков метров в зависимости от уровня фонового шума. Принцип действия таких устройств основан на анализе отраженного луча лазера от стекла окна помещения, которое колеблется от звуковых волн. Колебания оконных стекол от акустических волн в помещении могут сниматься и передаваться на расстояния с помощью специальных устройств, укрепленных на

оконном стекле. Такие устройства преобразуют механические колебания стекол в электрический сигнал с последующей передачей его по радиоканалу. Вне помещений подслушивание ведется с помощью сверхчувствительных направленных микрофонов. Реальное расстояние подслушивания с помощью направленных микрофонов составляет 50-100 метров[48].

Разговоры в соседних помещениях, за стенами зданий могут контролироваться с помощью стетоскопных микрофонов. Стетоскопы преобразуют акустические колебания в электрические. Такие микрофоны позволяют прослушивать разговоры при толщине стен до 50-100 см [65]. Съем информации может осуществляться также и со стекол, металлоконструкций зданий, труб водоснабжения и отопления.

Аудиоинформация может быть получена также путем высокочастотного навязывания. Суть этого метода заключается в воздействии высокочастотным электромагнитным полем или электрическими сигналами на элементы, способные модулировать эти поля, или сигналы электрическими или акустическими сигналами с речевой информацией. В качестве таких элементов могут использоваться различные полости с электропроводной поверхностью, представляющей собой высокочастотный контур с распределенными параметрами, которые меняются под действием акустических волн. При совпадении частоты такого контура с частотой высокочастотного навязывания и при наличии воздействия акустических волн на поверхность полости контур переизлучает и модулирует внешнее поле (высокочастотный электрический сигнал). Чаще всего этот метод прослушивания реализуется с помощью телефонной линии. При этом в качестве модулирующего элемента используется телефонный аппарат, на который по телефонным проводам подается высокочастотный электрический сигнал. Нелинейные элементы телефонного аппарата под воздействием речевого сигнала модулируют высокочастотный сигнал. Модулированный высокочастотный сигнал может быть демодулирован в приемнике злоумышленника.

Одним из возможных каналов утечки звуковой информации может быть прослушивание переговоров, ведущихся с помощью средств связи. Контролироваться могут как проводные каналы связи, так и радиоканалы. Прослушивание переговоров по про-

водным и радиоканалам не требует дорогостоящего оборудования и высокой квалификации злоумышленника.

Дистанционная видеоразведка для получения информации в КС малопригодна и носит, как правило, вспомогательный характер.

Видеоразведка организуется в основном для выявления режимов работы и расположения механизмов защиты информации. Из КС информация реально может быть получена при использовании на объекте экранов, табло, плакатов, если имеются прозрачные окна и перечисленные выше средства размещены без учета необходимости противодействовать такой угрозе.

.Видеоразведка может вестись с использованием технических средств, таких как оптические приборы, фото-, кино- и телеаппаратура. Многие из этих средств допускают консервацию (запоминание) видеоинформации, а также передачу ее на определенные расстояния.

В прессе появились сообщения о создании в США мобильного микроробота для ведения дистанционной разведки. Пьезокерамический робот размером около 7 см и массой 60 г способен самостоятельно передвигаться со скоростью 30 см/с в течение 45 мин. За это время «микроразведчик» способен преодолеть расстояние в 810 метров, осуществляя транспортировку 28 г полезного груза (для сравнения - коммерческая микровидеокамера весит 15 г)[68].

Для вербовки сотрудников и физического уничтожения объектов КС также не обязательно иметь непосредственный доступ на объект. Злоумышленник, имеющий доступ на объект КС, может использовать любой из методов традиционного шпионажа.

Злоумышленниками, имеющими доступ на объект, могут использоваться миниатюрные средства фотографирования, видео - и аудиозаписи. Для аудио- и видеоконтроля помещений и при отсутствии в них злоумышленника могут использоваться закладные устройства или «жучки». Для объектов КС наиболее вероятными являются закладные устройства, обеспечивающие прослушивание помещений. Закладные устройства делятся на проводные и излучающие. Проводные закладные устройства требуют значительного времени на установку и имеют существенный демаскирующий признак - провода. Излучающие «закладки» («радиозакладки») быстро устанавливаются, но также имеют демаскирующий при-

знак - излучение в радио или оптическом диапазоне. «Радиозакладки» могут использовать в качестве источника электрические сигналы или акустические сигналы. Примером использования электрических сигналов в качестве источника является применение сигналов внутренней телефонной, громкоговорящей связи. Наибольшее распространение получили акустические «радиозакладки». Они воспринимают акустический сигнал, преобразуют его в электрический и передают в виде радиосигнала на дальность до 8 км [67]. Из применяемых на практике «радиозакладок» подавляющее большинство (около 90%) рассчитаны на работу **в** диапазоне расстояний 50 - 800 метров.

Для некоторых объектов КС существует **угроза вооруженного нападения террористических или диверсионных групп.** При этом могут быть применены средства огневого поражения.

2.2.2. Несанкционированный доступ к информации

Термин «несанкционированный доступ к информации» (НСДИ) определен как доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств вычислительной техники или автоматизированных систем [14].

Под правилами разграничения доступа понимается совокупность положений, регламентирующих права доступа лиц или процессов (субъектов доступа) к единицам информации (объектам доступа).

Право доступа к ресурсам КС определяется руководством для каждого сотрудника в соответствии с его функциональными обязанностями. Процессы инициируются в КС в интересах определенных лиц, поэтому и на них накладываются ограничения по доступу к ресурсам.

Выполнение установленных правил разграничения доступа в КС реализуется за счет создания системы разграничения доступа (СРД), которая подробно рассматривается в главе 8.

Несанкционированный доступ к информации возможен только с использованием штатных аппаратных и программных средств в следующих случаях:

- отсутствует система разграничения доступа;
- сбой или отказ в КС;

- ошибочные действия пользователей или обслуживающего персонала компьютерных систем;
- ошибки в СРД;
- фальсификация полномочий.

Если СРД отсутствует, то злоумышленник, имеющий навыки работы в КС, может получить без ограничений доступ к любой информации. В результате сбоев или отказов средств КС, а также ошибочных действий обслуживающего персонала и пользователей возможны состояния системы, при которых упрощается НСДИ. Злоумышленник может выявить ошибки в СРД и использовать их для НСДИ. Фальсификация полномочий является одним из наиболее вероятных путей (каналов) НСДИ.

2.2.3. Электромагнитные излучения и наводки

Процесс обработки и передачи информации техническими средствами КС сопровождается электромагнитными излучениями в окружающее пространство и наведением электрических сигналов в линиях связи, сигнализации, заземлении и других проводниках. Они получили названия *побочных электромагнитных излучений и наводок (ПЭМИН)*. С помощью специального оборудования сигналы принимаются, выделяются, усиливаются и могут либо просматриваться, либо записываться в запоминающих устройствах. Наибольший уровень электромагнитного излучения в КС присущ работающим устройствам отображения информации на электронно-лучевых трубках. Содержание экрана такого устройства может просматриваться с помощью обычного телевизионного приемника, дополненного несложной схемой, основной функцией которой является синхронизация сигналов. Дальность удовлетворительного приема таких сигналов при использовании дипольной антенны составляет 50 метров. Использование направленной антенны приемника позволяет увеличить зону уверенного приема сигналов до 1 км [25]. Восстановление данных возможно также путем анализа сигналов излучения неэкранированного электрического кабеля на расстоянии до 300 метров.

Наведенные в проводниках электрические сигналы могут выделяться и фиксироваться с помощью оборудования, подключаемого к этим проводникам на расстоянии в сотни метров от источ-

ника сигналов. Для добывания информации злоумышленник может использовать также «просачивание» информационных сигналов в цепи электропитания технических средств КС.

«Просачивание» информационных сигналов в цепи электропитания возможно при наличии магнитной связи между выходным трансформатором усилителя и трансформатором выпрямительного устройства. «Просачивание» также возможно за счет падения напряжения на внутреннем сопротивлении источника питания при прохождении токов усиливаемых информационных сигналов. Если затухание в фильтре выпрямительного устройства недостаточно, то информационные сигналы могут быть обнаружены в цепи питания. Информационный сигнал может быть выделен в цепи питания за счет зависимости значений потребляемого тока в оконечных каскадах усилителей (информационные сигналы) и значений токов в выпрямителях, а значит и **в** выходных цепях.

Электромагнитные излучения используются злоумышленниками не только для получения информации, но и для ее уничтожения. Электромагнитные импульсы способны уничтожить информацию на магнитных носителях. Мощные электромагнитные и сверхвысокочастотные излучения могут вывести из строя электронные блоки КС. Причем для уничтожения информации на магнитных носителях с расстояния нескольких десятков метров может быть использовано устройство, помещающееся в портфель.

2.2.4. Несанкционированная модификация структур

Большую угрозу безопасности информации в КС представляет ***несанкционированная модификация алгоритмической, программной и технической структур системы.*** Несанкционированная модификация структур может осуществляться на любом жизненном цикле КС. Несанкционированное изменение структуры КС на этапах разработки и модернизации получило название «закладка». В процессе разработки КС «закладки» внедряются, как правило, в специализированные системы, предназначенные для эксплуатации в какой-либо фирме или государственных учреждениях. В универсальные КС «закладки» внедряются реже, в основном для дискредитации таких систем конкурентом или на

государственном уровне, если предполагаются поставки КС во враждебное государство. «Закладки», внедренные на этапе разработки, сложно выявить ввиду высокой квалификации их авторов и сложности современных КС.

Алгоритмические, программные и аппаратные «закладки» используются либо для непосредственного вредительского воздействия на КС, либо для обеспечения неконтролируемого входа в систему. Вредительские воздействия «закладок» на КС осуществляются при получении соответствующей команды извне (в основном характерно для аппаратных «закладок») и при наступлении определенных событий в системе. Такими событиями могут быть: переход на определенный режим работы (например, боевой режим системы управления оружием или режим устранения аварийной ситуации на атомной электростанции т. п.), наступление установленной даты, достижение определенной наработки и т. д.

Программные и аппаратные «закладки» для осуществления неконтролируемого входа в программы, использование привилегированных режимов работы (например, режимов операционной системы), обхода средств защиты информации получили название «люки».

2.2.5. Вредительские программы

Одним из основных источников угроз безопасности информации в КС является использование специальных программ, получивших общее название «вредительские программы».

В зависимости от механизма действия вредительские программы делятся на четыре класса:

- «логические бомбы»;
- «черви»;
- «троянские кони»;
- «компьютерные вирусы».

«Логические бомбы» - это программы или их части, постоянно находящиеся в ЭВМ или вычислительных системах (ВС) и выполняемые только при соблюдении определенных условий. Примерами таких условий могут быть: наступление заданной даты, переход КС в определенный режим работы, наступление некоторых событий установленное число раз и т.п.

«Червями» называются программы, которые выполняются каждый раз при загрузке системы, обладают способностью перемещаться в ВС или сети и самовоспроизводить копии. Лавинообразное размножение программ приводит к перегрузке каналов связи, памяти и, в конечном итоге, к блокировке системы.

«Троянские кони» — это программы, полученные путем явного изменения или добавления команд в пользовательские программы. При последующем выполнении пользовательских программ наряду с заданными функциями выполняются несанкционированные, измененные или какие-то новые функции.

«Компьютерные вирусы» - это небольшие программы, которые после внедрения в ЭВМ самостоятельно распространяются путем создания своих копий, а при выполнении определенных условий оказывают негативное воздействие на КС.

Поскольку вирусам присущи свойства всех классов вредительских программ, то в последнее время любые вредительские программы часто называют вирусами.

2.2.6. Классификация злоумышленников

Возможности осуществления вредительских воздействий в большой степени зависят от статуса злоумышленника по отношению к КС. Злоумышленником может быть:

- разработчик КС;
- сотрудник из числа обслуживающего персонала;
- пользователь;
- постороннее лицо.

Разработчик владеет наиболее полной информацией о программных и аппаратных средствах КС и имеет возможность внедрения "закладок" на этапах создания и модернизации систем. Но он, как правило, не получает непосредственного доступа на эксплуатируемые объекты КС. Пользователь имеет общее представление о структурах КС, о работе механизмов защиты информации. Он может осуществлять сбор данных о системе защиты информации методами традиционного шпионажа, а также предпринимать попытки несанкционированного доступа к информации. Возможности внедрения «закладок* пользователями очень ограничены. Постороннее лицо, не имеющее отношения к КС, нахо-

дится в наименее выгодном положении по отношению к другим злоумышленникам. Если предположить, что он не имеет доступ на объект КС, то в его распоряжении имеются дистанционные методы традиционного шпионажа и возможность диверсионной деятельности. Он может осуществлять вредительские воздействия с использованием электромагнитных излучений и наводок, а также каналов связи, если КС является распределенной.

Большие возможности оказания вредительских воздействий на информацию КС имеют *специалисты, обслуживающие* эти *системы*. Причем, специалисты разных подразделений обладают различными потенциальными возможностями злоумышленных действий. Наибольший вред могут нанести работники службы безопасности информации. Далее идут системные программисты, прикладные программисты и инженерно-технический персонал.

На практике опасность злоумышленника зависит также от финансовых, материально-технических возможностей и квалификации злоумышленника.

Контрольные вопросы

1. Раскройте понятие компонент КС и их взаимное влияние.
2. Что понимается под угрозой безопасности информации?
3. Перечислите и охарактеризуйте случайные угрозы.
4. Дайте общую характеристику преднамеренных угроз.
5. Приведите методы традиционного шпионажа и диверсий.
6. В чем состоит особенность определения несанкционированного доступа к информации?
7. Какие физические процессы лежат в основе появления побочных электромагнитных излучений и наводок?
8. Охарактеризуйте особенности угроз безопасности информации, связанных с несанкционированной модификацией структур КС.
9. Назовите особенности такого вида угроз как вредительские программы.
10. Поясните классификацию злоумышленников.

II. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

ГЛАВА 3

Правовые и организационные методы защиты информации в КС

3.1. Правовое регулирование в области безопасности информации

Комплексная система защиты информации создается на объектах для блокирования (парирования) всех возможных или, по крайней мере, наиболее вероятных угроз безопасности информации. Для парирования той или иной угрозы используется определенная совокупность методов и средств защиты. Некоторые из них защищают информацию от нескольких угроз одновременно. Среди методов защиты имеются и универсальные методы, которые являются базовыми при построении любой системы защиты. Это, прежде всего, правовые методы защиты информации, которые служат основой легитимного построения и использования системы защиты любого назначения. Организационные методы защиты информации, как правило, используются для парирования нескольких угроз. Кроме того, организационные методы используются в любой системе защиты без исключений.

Государство должно обеспечить в стране защиту информации как в масштабах всего государства, так и на уровне организаций и отдельных граждан. Для решения этой проблемы государство обязано:

1) выработать государственную политику безопасности в области информационных технологий;

2) законодательно определить правовой статус компьютер-

ных систем, информации, систем защиты информации, владельцев и пользователей информации и т. д.;

3) создать иерархическую структуру государственных органов, вырабатывающих и проводящих в жизнь политику безопасности информационных технологий;

4) создать систему стандартизации, лицензирования и сертификации в области защиты информации;

5) обеспечить приоритетное развитие отечественных защищенных информационных технологий;

6) повышать уровень образования граждан в области информационных технологий, воспитывать у них патриотизм и бдительность;

7) установить ответственность граждан за нарушения законодательства в области информационных технологий.

3.1.1. Политика государства РФ в области безопасности информационных технологий

В государстве должна проводиться единая политика в области безопасности информационных технологий. В Российской Федерации вопросы информационной безопасности нашли отражение в «Концепции национальной безопасности Российской Федерации», утвержденной Указом Президента РФ № 1300 от 17 декабря 1997 года. В этом документе отмечается, что «в современных условиях всеобщей информатизации и развития информационных технологий резко возрастает значение обеспечения национальной безопасности РФ в информационной сфере». В «Концепции национальной безопасности Российской Федерации» определены важнейшие задачи государства в области информационной безопасности:

- установление необходимого баланса между потребностью в свободном обмене информацией и допустимыми ограничениями ее распространения;
- совершенствование информационной структуры, ускорение развития новых информационных технологий и их широкое внедрение, унификация средств поиска, сбора, хранения и анализа информации с учетом вхождения России в глобальную информационную инфраструктуру;

• разработка соответствующей нормативной правовой базы и координация деятельности органов государственной власти и других органов, решающих задачи обеспечения информационной безопасности;

• развитие отечественной индустрии телекоммуникационных и информационных средств, их приоритетное по сравнению с зарубежными аналогами распространение на внутреннем рынке;

• защита государственного информационного ресурса и, прежде всего, в федеральных органах государственной власти и на предприятиях оборонного комплекса.

Усилия государства должны быть направлены на воспитание ответственности граждан за неукоснительное выполнение правовых норм в области информационной безопасности. Необходимо использовать все доступные средства для формирования у граждан патриотизма, чувства гордости за принадлежность к стране, коллективу. Важной задачей государства является также повышение уровня образования граждан в области информационных технологий. Большая роль в этой работе принадлежит образовательной системе государства, государственным органам управления, средствам массовой информации. Это важное направление реализации политики информационной безопасности.

3.1.2. Законодательная база информатизации общества

Высокие темпы информатизации, а также социально-экономические изменения в обществе, происшедшие в последние годы, требовали законодательного регулирования отношений, складывающихся в области информационных технологий. Эта проблема во многом была решена принятием Государственной Думой РФ 25 января 1995 года Федерального закона «Об информации, информатизации и защите информации». В законе даны определения основных терминов: информация; информатизация; информационные системы; информационные ресурсы; конфиденциальная информация; собственник и владелец информационных ресурсов; пользователь информации. Государство гарантирует права владельца информации, независимо от форм собственности, распоряжаться ею в пределах, установленных законом. Владелец информации имеет право защищать свои информационные ресур-

сы, устанавливать режим доступа к ним. В законе определены права и обязанности граждан и государства по доступу к информации. В нем установлен общий порядок разработки и сертификации информационных систем, технологий, средств их обеспечения, а также порядок лицензирования деятельности в сфере информационных технологий. В этом законе определены цели и режимы защиты информации, а также порядок защиты прав субъектов в сфере информационных процессов и информатизации.

Другим важным правовым документом, регламентирующим вопросы защиты информации в КС, является закон РФ «О государственной тайне». Он принят Постановлением Верховного Совета РФ от 21.07.1993 г. Закон определяет уровни секретности государственной информации (грифы секретности) и соответствующую степень важности информации. Руководствуясь данным законом и «Перечнем сведений, отнесенных к государственной тайне», введенным в действие Указом Президента РФ от 30 ноября 1995 года, соответствующие государственные служащие устанавливают гриф секретности информации.

Отношения, связанные с созданием программ и баз данных, регулируются Законом Российской Федерации от 23.09.1992 г. «О правовой охране программ для электронных вычислительных машин и баз данных» и Законом Российской Федерации от 09.07.1993 г. «Об авторском праве и смежных правах».

На основании приведенных правовых документов ведомства (министерства, объединения, корпорации и т. п.) разрабатывают нормативные документы (приказы, директивы, руководства, инструкции и др.), регламентирующие порядок использования и защиты информации в подведомственных организациях.

Очень важным правовым вопросом является установление юридического статуса КС и особенно статуса информации, получаемой с применением КС. Статус информации или ее правомочность служит основанием для выполнения (невыполнения) определенных действий. Например, в одних АСУ соответствующее должностное лицо имеет юридическое право принимать решения только на основании информации, полученной из АСУ. В других АСУ для принятия решения необходимо получить подтверждающую информацию по другим каналам. В одной и той же АСУ решение может приниматься как с получением подтверждающей

информации, так и без нее. Примером может служить организация перевода денег с помощью АСУ. До определенной суммы перевод осуществляется автоматически при поступлении соответствующей заявки. Для перевода крупной суммы выполняются дополнительные процедуры проверки правомочности такой операции. Для этого может быть затребована дополнительная информация, в том числе и по дублирующей системе, а окончательное решение о переводе денег может принимать должностное лицо.

Правовой статус информации устанавливается с учетом ее стоимости (важности) и степени достоверности, которую способна обеспечить компьютерная система.

Важной составляющей правового регулирования в области информационных технологий является установление ответственности граждан за противоправные действия при работе с КС. Преступления, совершенные с использованием КС или причинившие ущерб владельцам компьютерных систем, получили название компьютерных преступлений. В нашей стране 1 января 1997 года введен в действие новый Уголовный кодекс РФ. В него впервые включена глава № 28, в которой определена уголовная ответственность за преступления в области компьютерных технологий.

В статье 272 предусмотрены наказания за неправомерный доступ к компьютерной информации. За данное деяние предусмотрены наказания, лежащие в диапазоне от денежного штрафа в размере 200 минимальных зарплат до лишения свободы на срок до 5 лет. Отягощающими вину обстоятельствами являются совершение преступления группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети.

Статья 273 устанавливает ответственность за создание, использование и распространение вредоносных (вредительских) программ для ЭВМ. По этой статье предусмотрено наказание от штрафа в размере заработной платы или иного дохода осужденного за два месяца до лишения свободы на срок до семи лет (в зависимости от последствий).

В статье 274 определена ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Нарушение правил эксплуатации лицом, имеющим доступ к ЭВМ, системе ЭВМ

или их сети, если это деяние причинило существенный вред, наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет, либо обязательными работами на срок от ста восьмидесяти до двухсот часов. Если те же деяния повлекли тяжкие последствия, то предусмотрено лишение свободы на срок до 4 лет.

3.1.3. Структура государственных органов, ***обеспечивающих*** *безопасность* ***информационных технологий***

Выработку политики информационной безопасности, подготовку законодательных актов и нормативных документов, контроль над выполнением установленных норм обеспечения безопасности информации осуществляют государственные органы, структура которых приведена на рис.2.

Возглавляет государственные органы обеспечения информационной безопасности Президент РФ. Он руководит Советом Безопасности и утверждает указы, касающиеся обеспечения безопасности информации в государстве.

Общее руководство системой информационной безопасности, наряду с другими вопросами государственной безопасности страны, осуществляют Президент и Правительство Российской Федерации.

Органом исполнительной власти, непосредственно занимающимся вопросами государственной безопасности, является Совет Безопасности при Президенте РФ. В состав Совета Безопасности входит Межведомственная комиссия по информационной безопасности. Комиссия готовит указы Президента, выступает с законодательной инициативой, координирует деятельность руководителей министерств и ведомств в области информационной безопасности государства.

Рабочим органом Межведомственной комиссии по информационной безопасности является Государственная техническая комиссия при Президенте РФ. Эта комиссия осуществляет подготовку проектов законов, разрабатывает нормативные документы (Решения Государственной технической комиссии), организует сертификацию средств защиты информации (за исключением криптографических средств), лицензирование деятельности в об-

ласти производства средств защиты и обучения специалистов по защите информации [33,34]. Гостехкомиссия руководит аттестацией КС, предназначенных для обработки информации, представляющей государственную тайну, или управляющих экологически опасными объектами [35]. Она координирует и направляет деятельность государственных научно-исследовательских учреждений, работающих в области защиты информации, обеспечивает аккредитацию органов лицензирования и испытательных центров (лабораторий) по сертификации. Эта комиссия обеспечивает также работу Межведомственной комиссии по защите государственной тайны.

Рис. 2. Структура государственных органов, обеспечивающих проведение политики информационной безопасности в РФ

На Межведомственную комиссию по защите государственной тайны возложена задача руководства лицензированием предприятий, учреждений и организаций, связанных с использованием сведений, составляющих государственную тайну, с созданием средств защиты информации, а также оказанием услуг по защите гостайны. Кроме того, эта комиссия осуществляет координацию работы по организации сертификации средств защиты информации.

Федеральное агентство правительственной связи и информации при Президенте Российской Федерации (ФАПСИ) обеспечивает правительственную связь и информационные технологии государственного управления. Агентство осуществляет сертификацию всех средств, используемых для организации правительственной связи и информатизации государственного управления, а также лицензирует все предприятия, учреждения и организации, занимающиеся производством таких средств. Кроме того, в исключительном ведении ФАПСИ находятся вопросы сертификации и лицензирования в области криптографической защиты информации.

В министерствах и ведомствах создаются иерархические структуры обеспечения безопасности информации, которые, как правило, совпадают с организационной структурой министерства (ведомства). Называться они могут по-разному, но функции выполняют сходные.

3.2. Общая характеристика организационных методов защиты информации в КС

Законы и нормативные акты исполняются только в том случае, если они подкрепляются организаторской деятельностью соответствующих структур, создаваемых в государстве, в ведомствах, учреждениях и организациях. При рассмотрении вопросов безопасности информации такая деятельность относится к организационным методам защиты информации.

Организационные методы защиты информации включают меры, мероприятия и действия, которые должны осуществлять должностные лица в процессе создания и эксплуатации КС для обеспечения заданного уровня безопасности информации.

Организационные методы защиты информации тесно связаны с правовым регулированием в области безопасности информации. В соответствии с законами и нормативными актами в министерствах, ведомствах, на предприятиях (независимо от форм собственности) для защиты информации создаются специальные службы безопасности (на практике они могут называться и иначе). Эти службы подчиняются, как правило, руководству учреждения. Руководители служб организуют создание и функционирование систем защиты информации. На организационном уровне решаются следующие задачи обеспечения безопасности информации в КС:

- организация работ по разработке системы защиты информации;
- ограничение доступа на объект и к ресурсам КС;
- разграничение доступа к ресурсам КС;
- планирование мероприятий;
- разработка документации;
- воспитание и обучение обслуживающего персонала и пользователей;
- сертификация средств защиты информации;
- лицензирование деятельности по защите информации;
- аттестация объектов защиты;
- совершенствование системы защиты информации;
- оценка эффективности функционирования системы защиты информации;
- контроль выполнения установленных правил работы в КС.

Организационные методы являются стержнем комплексной системы защиты информации в КС. Только с помощью этих методов возможно объединение на правовой основе технических, программных и криптографических средств защиты информации в единую комплексную систему. Конкретные организационные методы защиты информации будут приводиться при рассмотрении парирования угроз безопасности информации. Наибольшее внимание организационным мероприятиям уделяется при изложении вопросов построения и организации функционирования комплексной системы защиты информации.

Контрольные вопросы

1. Перечислите задачи государства в области безопасности информации.
2. Охарактеризуйте основные законы РФ, регулирующие отношения в области информационных технологий.
3. Назовите государственные органы, обеспечивающие безопасность информационных технологий, и решаемые ими задачи.
4. Дайте общую характеристику организационным методам защиты информации в КС.

ГЛАВА 4
Защита информации в КС от случайных угроз

4.1. Дублирование информации

Для блокирования (парирования) случайных угроз безопасности информации в компьютерных системах должен быть решен комплекс задач (рис. 3).

Дублирование информации является одним из самых эффективных способов обеспечения целостности информации. Оно обеспечивает защиту информации как от случайных угроз, так и от преднамеренных воздействий.

В зависимости от ценности информации, особенностей построения и режимов функционирования КС могут использоваться различные методы дублирования, которые классифицируются по различным признакам [43].

По времени восстановления информации методы дублирования могут быть разделены на:

- оперативные;
- неоперативные.

К *оперативным* методам относятся методы дублирования информации, которые позволяют использовать дублирующую информацию в реальном масштабе времени. Это означает, что переход к использованию дублирующей информации осуществляется за время, которое позволяет выполнить запрос на использование

информации в режиме реального времени для данной КС. Все методы, не обеспечивающие выполнения этого условия, относят к *неоперативным* методам дублирования.

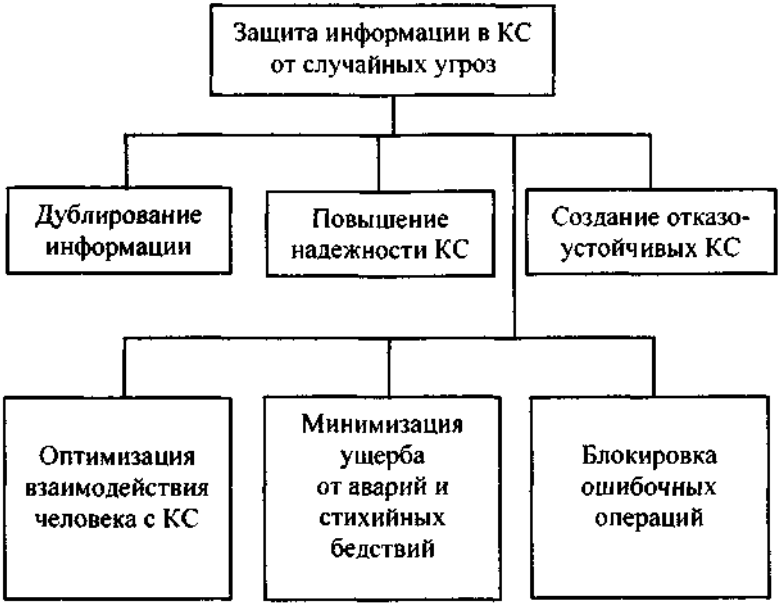


Рис. 3. Задачи защиты информации в КС от случайных угроз

По используемым для целей дублирования **средствам** методы дублирования можно разделить на методы, использующие:

- дополнительные внешние запоминающие устройства (блоки);
- специально выделенные области памяти на несъемных машинных носителях;
- съемные носители информации.

По числу копий методы дублирования делятся на:

- одноуровневые;
- многоуровневые.

Как правило, число уровней не превышает трех.

По степени пространственной удаленности носителей основной и дублирующей информации методы дублирования могут быть разделены на следующие методы:

- сосредоточенного дублирования;
- рассредоточенного дублирования

Для определенности целесообразно считать методами *сосредоточенного* дублирования такие методы, для которых носители с основной и дублирующей информацией находятся в одном помещении. Все другие методы относятся *к рассредоточенным*.

В соответствии с процедурой дублирования различают методы:

- полного копирования;
- зеркального копирования;
- частичного копирования;
- комбинированного копирования.

При полном копировании дублируются все файлы.

При зеркальном копировании любые изменения основной информации сопровождаются такими же изменениями дублирующей информации. При таком дублировании основная информация и дубль всегда идентичны.

Частичное копирование предполагает создание дублей определенных файлов, например, файлов пользователя. Одним из видов частичного копирования, получившим название инкрементного копирования, является метод создания дублей файлов, измененных со времени последнего копирования.

Комбинированное копирование допускает комбинации, например, полного и частичного копирования с различной периодичностью их проведения.

Наконец, **по виду дублирующей информации** методы дублирования разделяются на:

- методы со сжатием информации;
- методы без сжатия информации.

В качестве внешних запоминающих устройств для хранения дублирующей информации используются накопители на жестких магнитных дисках и магнитных лентах. Накопители на жестких магнитных дисках применяются обычно для оперативного дублирования информации.

Наиболее простым методом дублирования данных в КС является использование выделенных областей памяти на рабочем диске. В этих областях дублируется наиболее важная системная информация. Например, таблицы каталогов и таблицы файлов дуб-

лируются таким образом, чтобы они были размещены на цилиндрах и поверхностях жесткого диска (пакета дисков), отличных от тех, на которых находятся рабочие таблицы. Такое дублирование защищает от полной потери информации при повреждении отдельных участков поверхности дисков.

Очень надежным методом оперативного дублирования является использование зеркальных дисков. *Зеркальным* называют жесткий магнитный диск отдельного накопителя, на котором хранится информация, полностью идентичная информации на рабочем диске. Достигается это за счет параллельного выполнения всех операций записи на оба диска. При отказе рабочего накопителя осуществляется автоматический переход на работу с зеркальным диском в режиме реального времени. Информация при этом сохраняется в полном объеме.

В компьютерных системах, к которым предъявляются высокие требования по сохранности информации (военные системы, АСУ технологическими процессами, серверы сетей, коммуникационные модули сетей и другие), как правило, используются два и более резервных диска, подключенных к отдельным контроллерам и блокам питания. Зеркальное дублирование обеспечивает надежное оперативное дублирование, но требует, как минимум, вдвое больших аппаратных затрат.

Идеология надежного и эффективного хранения информации на жестких дисках нашла свое отражение в так называемой технологии RAID (Redundant Array of Independent Disks) [42]. Эта технология реализует концепцию создания блочного устройства хранения данных с возможностями параллельного выполнения запросов и восстановления информации при отказах отдельных блоков накопителей на жестких магнитных дисках. Устройства, реализующие эту технологию, называют подсистемами RAID или дисковыми массивами RAID.

В технологии RAID выделяется 6 основных уровней: с 0-го по 5-й. С учетом различных модификаций их может быть больше. Уровни RAID определяют порядок записи на независимые диски и порядок восстановления информации. Различные уровни RAID обеспечивают различное быстродействие подсистемы и различную эффективность восстановления информации.

Нулевой уровень RAID предполагает поочередное использо-

- сосредоточенного дублирования;
- рассредоточенного дублирования

Для определенности целесообразно считать методами *сосредоточенного* дублирования такие методы, для которых носители с основной и дублирующей информацией находятся в одном помещении. Все другие методы относятся *к рассредоточенным*.

В соответствии с процедурой дублирования различают методы:

- полного копирования;
- зеркального копирования;
- частичного копирования;
- комбинированного копирования.

При полном копировании дублируются все файлы.

При зеркальном копировании любые изменения основной информации сопровождаются такими же изменениями дублирующей информации. При таком дублировании основная информация и дубль всегда идентичны.

Частичное копирование предполагает создание дублей определенных файлов, например, файлов пользователя. Одним из видов частичного копирования, получившим название инкрементного копирования, является метод создания дублей файлов, измененных со времени последнего копирования.

Комбинированное копирование допускает комбинации, например, полного и частичного копирования с различной периодичностью их проведения.

Наконец, **по виду дублирующей информации** методы дублирования разделяются на:

- методы со сжатием информации;
- методы без сжатия информации.

В качестве внешних запоминающих устройств для хранения дублирующей информации используются накопители на жестких магнитных дисках и магнитных лентах. Накопители на жестких магнитных дисках применяются обычно для оперативного дублирования информации.

Наиболее простым методом дублирования данных в КС является использование выделенных областей памяти на рабочем диске. В этих областях дублируется наиболее важная системная информация. Например, таблицы каталогов и таблицы файлов дуб-

лируются таким образом, чтобы они были размещены на цилиндрах и поверхностях жесткого диска (пакета дисков), отличных от тех, на которых находятся рабочие таблицы. Такое дублирование защищает от полной потери информации при повреждении отдельных участков поверхности дисков.

Очень надежным методом оперативного дублирования является использование зеркальных дисков. *Зеркальным* называют жесткий магнитный диск отдельного накопителя, на котором хранится информация, полностью идентичная информации на рабочем диске. Достигается это за счет параллельного выполнения всех операций записи на оба диска. При отказе рабочего накопителя осуществляется автоматический переход на работу с зеркальным диском в режиме реального времени. Информация при этом сохраняется в полном объеме.

В компьютерных системах, к которым предъявляются высокие требования по сохранности информации (военные системы, АСУ технологическими процессами, серверы сетей, коммуникационные модули сетей и другие), как правило, используются два и более резервных диска, подключенных к отдельным контроллерам и блокам питания. Зеркальное дублирование обеспечивает надежное оперативное дублирование, но требует, как минимум, вдвое больших аппаратных затрат.

Идеология надежного и эффективного хранения информации на жестких дисках нашла свое отражение в так называемой технологии RAID (Redundant Array of Independent Disks) [42]. Эта технология реализует концепцию создания блочного устройства хранения данных с возможностями параллельного выполнения запросов и восстановления информации при отказах отдельных блоков накопителей на жестких магнитных дисках. Устройства, реализующие эту технологию, называют подсистемами RAID или дисковыми массивами RAID.

В технологии RAID выделяется 6 основных уровней: с 0-го по 5-й. С учетом различных модификаций их может быть больше. Уровни RAID определяют порядок записи на независимые диски и порядок восстановления информации. Различные уровни RAID обеспечивают различное быстродействие подсистемы и различную эффективность восстановления информации.

Нулевой уровень RAID предполагает поочередное использо-

целостности и доступности информации при стихийных бедствиях и крупных авариях.

4.2. Повышение надежности КС

Под **надежностью** понимается свойство системы выполнять возложенные на нее задачи в определенных условиях эксплуатации. При наступлении отказа компьютерная система не может выполнять все предусмотренные документацией задачи, т.е. переходит из исправного состояния в неисправное. Если при наступлении отказа компьютерная система способна выполнять заданные функции, сохраняя значения основных характеристик в пределах, установленных технической документацией, то она находится в работоспособном состоянии.

С точки зрения обеспечения безопасности информации необходимо сохранять хотя бы работоспособное состояние КС. Для решения этой задачи необходимо обеспечить высокую надежность функционирования алгоритмов, программ и технических (аппаратных) средств.

Поскольку алгоритмы в КС реализуются за счет выполнения программ или аппаратным способом, то надежность алгоритмов отдельно не рассматривается. В этом случае считается, что надежность КС обеспечивается надежностью программных и аппаратных средств.

Надежность КС достигается на этапах:

- разработки;
- производства;
- эксплуатации.

Для программных средств рассматриваются этапы разработки и эксплуатации. Этап разработки программных средств является определяющим при создании надежных компьютерных систем.

На этом этапе основными направлениями повышения надежности программных средств являются:

- корректная постановка задачи на разработку;
- использование прогрессивных технологий программирования;
- контроль правильности функционирования

Корректность постановки задачи достигается в результате со-

вместной работы специалистов предметной области и высокопрофессиональных программистов-алгоритмистов.

В настоящее время для повышения качества программных продуктов используются современные технологии программирования (например, CASE технология). Эти технологии позволяют значительно сократить возможности внесения субъективных ошибок разработчиков. Они характеризуются высокой автоматизацией процесса программирования, использованием стандартных программных модулей, тестированием их совместной работы.

Контроль правильности функционирования алгоритмов и программ осуществляется на каждом этапе разработки и завершается комплексным контролем, охватывающим все решаемые задачи и режимы.

На этапе эксплуатации программные средства дорабатываются, в них устраняются замеченные ошибки, поддерживается целостность программных средств и актуальность данных, используемых этими средствами.

Надежность технических средств (ТС) КС обеспечивается на всех этапах. На этапе разработки выбираются элементная база, технология производства и структурные решения, обеспечивающие максимально достижимую надежность КС в целом.

Велика роль в процессе обеспечения надежности ТС и этапа производства. Главными условиями выпуска надежной продукции являются высокий технологический уровень производства и организация эффективного контроля качества выпускаемых ТС.

Удельный вес этапа эксплуатации ТС в решении проблемы обеспечения надежности КС в последние годы значительно снизился. Для определенных видов вычислительной техники, таких как персональные ЭВМ, уровень требований к процессу технической эксплуатации снизился практически до уровня эксплуатации бытовых приборов. Особенностью нынешнего этапа эксплуатации средств вычислительной техники является сближение эксплуатации технических и программных средств (особенно средств общего программного обеспечения). Тем не менее, роль этапа эксплуатации ТС остается достаточно значимой в решении задачи обеспечения надежности КС и, прежде всего, надежности сложных компьютерных систем.

4.3. Создание отказоустойчивых КС

Отказоустойчивость - это свойство КС сохранять работоспособность при отказах отдельных устройств, блоков, схем.

Известны три основных подхода к созданию отказоустойчивых систем:

- простое резервирование;
- помехоустойчивое кодирование информации;
- создание адаптивных систем.

Любая отказоустойчивая система обладает избыточностью. Одним из наиболее простых и действенных путей создания отказоустойчивых систем является **простое резервирование.** Простое резервирование основано на использовании устройств, блоков, узлов, схем только в качестве резервных. При отказе основного элемента осуществляется переход на использование резервного. Резервирование осуществляется на различных уровнях: на уровне устройств, на уровне блоков, узлов и т. д. Резервирование отличается также и глубиной. Для целей резервирования могут использоваться один резервный элемент и более. Уровни и глубина резервирования определяют возможности системы парировать отказы, а также аппаратные затраты. Такие системы должны иметь несложные аппаратно-программные средства контроля работоспособности элементов и средства перехода на использование, при необходимости, резервных элементов. Примером резервирования может служить использование «зеркальных» накопителей на жестких магнитных дисках. Недостатком простого резервирования является непроизводительное использование средств, которые применяются только для повышения отказоустойчивости.

Помехоустойчивое кодирование основано на использовании информационной избыточности. Рабочая информация в КС дополняется определенным объемом специальной контрольной информации. Наличие этой контрольной информации (контрольных двоичных разрядов) позволяет путем выполнения определенных действий над рабочей и контрольной информацией определять ошибки и даже исправлять их. Так как ошибки являются следствием отказов средств КС, то, используя исправляющие коды, можно парировать часть отказов. Исправляющие возможности кодов для конкретного метода помехоустойчивого кодирования

зависят\от степени избыточности. Чем больше используется контрольной информации, тем шире возможности кода по обнаружению и исправлению ошибок. Ошибки характеризуются кратностью, т.е. количеством двоичных разрядов, в которых одновременно искажено содержимое. Помехоустойчивые коды обладают различными возможностями по обнаружению и исправлению ошибок различной кратности. Так классический код Хемминга обнаруживает и исправляет однократные ошибки, а двукратные ошибки - только обнаруживает.

Помехоустойчивое кодирование наиболее эффективно при парировании самоустраняющихся отказов, называемых **сбоями.** Помехоустойчивое кодирование при создании отказоустойчивых систем, как правило, используется в комплексе с другими подходами повышения отказоустойчивости.

Наиболее совершенными системами, устойчивыми к отказам, являются **адаптивные системы.** В них достигается разумный компромисс между уровнем избыточности, вводимым для обеспечения устойчивости (толерантности) системы к отказам, и эффективностью использования таких систем по назначению.

В адаптивных системах реализуется так называемый принцип элегантной деградации. Этот принцип предполагает сохранение работоспособного состояния системы при некотором снижении эффективности функционирования в случаях отказов ее элементов.

Адаптивные системы содержат аппаратно-программные средства для автоматического контроля работоспособности элементов системы и осуществления ее реконфигурации при возникновении отказов элементов. При реконфигурации восстанавливается необходимая информация (при ее утрате), отключается отказавший элемент, осуществляется изменение связей и режимов работы элементов системы. Простым примером адаптивной КС может служить ЭВМ, имеющая в своем составе математический и графический сопроцессоры, а также оперативную память блочной структуры. Все сопроцессоры и блоки памяти используются для достижения максимальной производительности ЭВМ. При отказе какого-либо сопроцессора он логически отключается от ЭВМ, а его функции выполняет центральный процессор. При этом система деградирует, так как снижается производительность ЭВМ. Но

в то же время система сохраняет работоспособность и может завершить вычислительный процесс. При отказе блока оперативной памяти он отключается, и емкость памяти уменьшается. Чтобы избежать потерь информации при отказах процессоров и блоков оперативной памяти, вычислительный процесс возобновляется либо сначала, либо с последней контрольной точки. Механизм контрольных точек используется обычно при выполнении сложных трудоемких программ. Он заключается в запоминании всей необходимой информации для возобновления выполнения программы с определенной точки. Запоминание осуществляется через определенные интервалы времени.

В адаптивных системах даже внешние устройства не используются только как резервные. Информация, необходимая для восстановления данных с отказавшего ВЗУ, хранится на накопителях, которые используются для хранения и рабочей информации. Примером таких систем являются RAID системы.

4.4. Блокировка ошибочных операций

Ошибочные операции или действия могут вызываться отказами аппаратных и программных средств, а также ошибками пользователей и обслуживающего персонала. Некоторые ошибочные действия могут привести к нарушениям целостности, доступности и конфиденциальности информации. Ошибочная запись в ОП и на ВЗУ, нарушение разграничения памяти при мультипрограммных режимах работы ЭВМ, ошибочная выдача информации в канал связи, короткие замыкания и обрыв проводников - вот далеко не полный перечень ошибочных действий, которые представляют реальную угрозу безопасности информации в КС.

Для блокировки ошибочных действий используются технические и аппаратно-программные средства.

Технические средства используются в основном для предотвращения ошибочных действий людей. К таким средствам относятся блокировочные тумблеры, защитные экраны и ограждения, предохранители, средства блокировки записи на магнитные ленты и магнитные дискеты.

Аппаратно-программные средства позволяют, например, блокировать вычислительный процесс при нарушениях программами

адреснцх пространств оперативной памяти с помощью граничных регистров или ключей защиты. При мультипрограммных режимах работы ЭВМ оперативная память распределяется между программами. Приведенный механизм позволяет сравнивать адреса команд активной программы с границами разрешенной области ОП для этой программы и блокировать обращение при нарушении границ. Аппаратно-программные средства используются также для блокирования выдачи информации в неразрешенные каналы связи, запрета выполнения операций, которые доступны только в определенных режимах, например, в режиме работы операционной системы. С помощью аппаратно-программных средств может быть заблокирована запись в определенные области внешних запоминающих устройств и некоторые другие операции.

На программном уровне могут устанавливаться атрибуты файлов, в том числе и атрибут, запрещающий запись в файлы. С помощью программных средств устанавливается режим обязательного подтверждения выполнения опасных операций, таких как уничтожение файлов, разметка или форматирование ВЗУ и другие.

4.5. Оптимизация взаимодействия пользователей и обслуживающего персонала с КС

Одним из основных направлений защиты информации в КС от непреднамеренных угроз являются сокращение числа ошибок пользователей и обслуживающего персонала, а также минимизация последствий этих ошибок. Для достижения этих целей необходимы:

- научная организация труда;
- воспитание и обучение пользователей и персонала;
- анализ и совершенствование процессов взаимодействия человека с КС.

Научная организация труда предполагает:

- оборудование рабочих мест;
- оптимальный режим труда и отдыха;
- дружественный интерфейс (связь, диалог) человека с КС.

Рабочее место пользователя или специалиста из числа обслу-

живающего персонала должно быть оборудовано в соответствии с рекомендациями эргономики. Освещение рабочего места; температурно-влажностный режим; расположение табло, индикаторов, клавиш и тумблеров управления; размеры и цвет элементов оборудования, помещения; положение пользователя (специалиста) относительно оборудования; использование защитных средств - все это должно обеспечивать максимальную производительность человека в течение рабочего дня. Одновременно сводится к минимуму утомляемость работника и отрицательное воздействие на его здоровье неблагоприятных факторов производственного процесса. Для людей, работающих с КС, основными неблагоприятными факторами являются: излучения мониторов, шумы электромеханических устройств, гиподинамия, и, как правило, высокие нагрузки на нервную систему. Вредные воздействия устройств постоянно уменьшаются за счет совершенствования самих устройств и в результате использования защитных экранов.

Последствия гиподинамии (малоподвижного, статического положения человека на рабочем месте) и высокие нагрузки на нервную систему компенсируются оптимальным режимом труда и отдыха, а также совершенствованием процесса общения человека с КС. Так при работе с ЭВМ медики рекомендуют 10-15 минутные перерывы через каждый час работы. Во время перерывов следует выполнять физические упражнения и упражнения на снятие психических нагрузок. Продолжительность работы с использованием монитора не должна превышать 6 часов за рабочий день. При сменной организации труда после 6 часов работы должен предоставляться отдых, продолжительность которого определяется длительностью смены.

Прогресс в области электронной вычислительной техники (ЭВТ) позволил значительно облегчить взаимодействие человека с ЭВМ. Если на заре ЭВТ с компьютером мог работать только человек с высшим специальным образованием, то теперь на ПЭВМ работают дети дошкольного возраста. Дальнейшее развитие интерфейса человека с КС идет в направлении совершенствования процессов ввода-вывода информации и управления вычислительным процессом. Речевой ввод информации, автоматический ввод-вывод видео- и аудиоинформации, работа с графикой, вывод информации на экраны и табло создают новые возможности для об-

щения человека с КС. Важным для обеспечения безопасности информации является совершенствование диалога пользователя с КС. Наличие развитых систем меню, блокировок неправильных действий, механизма напоминаний, справочных систем, систем шаблонов существенно снимает нагрузку на нервную систему, сокращает число ошибок, повышает работоспособность человека и производительность системы в целом.

Одним из центральных вопросов обеспечения безопасности информации в КС от всех классов угроз (в том числе и от преднамеренных) является вопрос воспитания и обучения обслуживающего персонала, а также пользователей корпоративных компьютерных систем. В КС общего назначения работа с пользователями затруднена и сводится, главным образом, к контролю над их деятельностью.

У обслуживающего персонала и пользователей КС необходимо воспитывать такие качества как патриотизм (на уровне государства и на уровне корпорации), ответственность, аккуратность и др. Чувство патриотизма воспитывается у граждан страны за счет целенаправленной политики государства и реального положения дел в стране. Успешная политика государства внутри страны и на международной арене способствует воспитанию у граждан патриотизма, гордости за свое отечество. Не меньшее значение, особенно для негосударственных учреждений, имеет воспитание корпоративного патриотизма. В коллективе, где ценится трудолюбие, уважительное отношение друг к другу, поощряется аккуратность, инициатива и творчество, у работника практически не бывает внутренних мотивов нанесения вреда своему учреждению. Важной задачей руководства является также подбор и расстановка кадров с учетом их деловых и человеческих качеств. Большой положительный опыт воспитания корпоративного патриотизма накоплен в Японии, где очень удачно соединяются мировой опыт управления коллективами и национальные особенности японцев.

Наряду с воспитанием специалистов большое значение в деле обеспечения безопасности информации в КС имеет и обучение работников. Дальновидный руководитель не должен жалеть средств на обучение персонала. Обучение может быть организовано на различных уровнях. Прежде всего, руководство должно всемерно поощрять стремление работников к самостоятельному

обучению. Важно обучать наиболее способных, трудолюбивых работников в учебных заведениях, возможно и за счет учреждения.

Важной задачей оптимизации взаимодействия человека с КС является также анализ этого процесса и его совершенствование. Анализ должен проводиться на всех жизненных этапах КС и направляться на выявление слабых звеньев. Слабые звенья заменяются или совершенствуются как в процессе разработки новых КС, так и в процессе модернизации существующих.

4.6. Минимизация ущерба от аварий и стихийных бедствий

Стихийные бедствия и аварии могут причинить огромный ущерб объектам КС. Предотвратить стихийные бедствия человек пока не в силах, но уменьшить последствия таких явлений во многих случаях удается. Минимизация последствий аварий и стихийных бедствий для объектов КС может быть достигнута путем:

- правильного выбора места расположения объекта;
- учета возможных аварий и стихийных бедствий при разработке и эксплуатации КС;
- организации своевременного оповещения о возможных стихийных бедствиях;
- обучение персонала борьбе со стихийными бедствиями и авариями, методам ликвидации их последствий.

Объекты КС по возможности должны располагаться в тех районах, где не наблюдается таких стихийных бедствий как наводнения, землетрясения. Объекты необходимо размещать вдалеке от таких опасных объектов как нефтебазы и нефтеперерабатывающие заводы, склады горючих и взрывчатых веществ, плотин и т. д.

На практике далеко не всегда удается расположить объект вдалеке от опасных предприятий или районов с возможными стихийными бедствиями. Поэтому при разработке, создании и эксплуатации объектов КС необходимо предусмотреть специальные меры. В районах с возможными землетрясениями здания должны быть сейсмостойкими. В районах возможных затоплений основное оборудование целесообразно размещать на верхних этажах зданий. Все объекты должны снабжаться автоматическими систе-

мами тушения пожара. На объектах, для которых вероятность стихийных бедствий высока, необходимо осуществлять распределенное дублирование информации и предусмотреть возможность перераспределения функций объектов. На всех объектах должны предусматриваться меры на случай аварии в системах электропитания. Для объектов, работающих с ценной информацией, требуется иметь аварийные источники бесперебойного питания и подвод электроэнергии производить не менее чем от двух независимых линий электропередачи. Использование источников бесперебойного питания обеспечивает, по крайней мере, завершение вычислительного процесса и сохранение данных на внешних запоминающих устройствах. Для малых КС такие источники способны обеспечить работу в течение нескольких часов.

Потери информационных ресурсов могут быть существенно уменьшены, если обслуживающий персонал будет своевременно предупрежден о надвигающихся природных катаклизмах. В реальных условиях такая информация часто не успевает дойти до исполнителей. Поэтому персонал должен быть обучен действиям в условиях стихийных бедствий и аварий, а также уметь восстанавливать утраченную информацию.

Контрольные вопросы

1. Приведите классификацию задач защиты информации в КС от случайных угроз.
2. Дайте общую характеристику дублирования информации в компьютерных системах.
3. В чем заключается преимущество использования технологии RAID?
4. Назовите пути повышения надежности и отказоустойчивости КС.
5. Какие преимущества имеют адаптивные системы по сравнению с другими отказоустойчивыми системами?
6. По каким направлениям происходит оптимизация взаимодействия человека с КС?
7. Каким образом достигается блокировка ошибочных операций в компьютерных системах?
8. Чем достигается минимизация ущерба от аварий и стихийных бедствий?

ГЛАВА 5

Методы и средства защиты информации в КС от традиционного шпионажа и диверсий

5.1. Система охраны объекта КС

При защите информации в КС от традиционного шпионажа и диверсий используются те же средства и методы защиты, что и для защиты других объектов, на которых не используются КС. Для защиты объектов КС от угроз данного класса должны быть решены следующие задачи:

- создание системы охраны объекта;
- организация работ с конфиденциальными информационными ресурсами на объекте КС;
- противодействие наблюдению;
- противодействие подслушиванию;
- защита от злоумышленных действий персонала.

Объект, на котором производятся работы с ценной конфиденциальной информацией, имеет, как правило, несколько рубежей защиты:

1) контролируемая территория;
2) здание;
3) помещение;
4) устройство, носитель информации;
5) программа;
6) информационные ресурсы.

От шпионажа и диверсий необходимо защищать первые четыре рубежа и обслуживающий персонал.

Система охраны объекта (СОО) КС создается с целью предотвращения несанкционированного проникновения на территорию и в помещения объекта посторонних лиц, обслуживающего персонала и пользователей.

Состав системы охраны зависит от охраняемого объекта. В общем случае СОО КС должна включать следующие компоненты:

- инженерные конструкции;
- охранная сигнализация;

- средства наблюдения;
- подсистема доступа на объект;
- дежурная смена охраны.

5.1.1. Инженерные конструкции

Инженерные конструкции служат для создания механических препятствий на пути злоумышленников. Они создаются по периметру контролируемой зоны. Инженерными конструкциями оборудуются также здания и помещения объектов. По периметру контролируемой территории используются бетонные или кирпичные заборы, решетки или сеточные конструкции. Бетонные и кирпичные заборы имеют обычно высоту в пределах 1,8-2,5 м, сеточные - до 2,2 м [1]. Для повышения защитных свойств заграждений поверх заборов укрепляется колючая проволока, острые стержни, армированная колючая лента. Последняя изготавливается путем армирования колючей ленты стальной оцинкованной проволокой диаметром 2,5 мм. Армированная колючая лента часто используется в виде спирали диаметром 500-955 мм. Для затруднения проникновения злоумышленника на контролируемую территорию могут использоваться малозаметные препятствия. Примером малозаметных препятствий может служить металлическая сеть из тонкой проволоки. Такая сеть располагается вдоль забора на ширину до 10 метров. Она исключает быстрое перемещение злоумышленника.

В здания и помещения злоумышленники пытаются проникнуть, как правило, через двери или окна. Поэтому с помощью инженерных конструкций укрепляют, прежде всего, это слабое звено в защите объектов. Надежность двери зависит от механической прочности самой двери и от надежности замков. Чем выше требования к надежности двери, тем более прочной она выполняется, тем выше требования к механической прочности и способности противостоять несанкционированному открыванию предъявляются к замку.

Вместо механических замков все чаще используются кодовые замки. Самыми распространенными среди них (называемых обычно сейфовыми замками) являются дисковые кодовые замки с числом комбинаций кода ключа в пределах 10^6 - 10^7.

Наивысшую стойкость имеют электронные замки, построенные с применением микросхем. Например, при построении электронных замков широко используются микросхемы Touch Memory. Микросхема помещена в стальной корпус, который по внешнему виду напоминает элемент питания наручных часов, калькуляторов и т. п. Диаметр цилиндрической части равен 16 мм, а высота - 3-5 мм. Электропитание микросхемы обеспечивается находящимся внутри корпуса элементом питания, ресурс которого рассчитан на 10 лет эксплуатации. Корпус может размещаться на пластиковой карте или в пластмассовой оправе в виде брелка. В микросхеме хранится ее индивидуальный 64-битовый номер. Такая разрядность обеспечивает около 10^{20} комбинаций ключа, практически исключающая его подбор. Микросхема имеет также перезаписываемую память, что позволяет использовать ее для записи и считывания дополнительной информации. Обмен информацией между микросхемой и замком осуществляется при прикосновении контакта замка и определенной части корпуса микросхемы.

На базе электронных замков строятся автоматизированные системы контроля доступа в помещения. В каждый замок вводятся номера микросхем, владельцы которых допущены в соответствующее помещение. Может также задаваться индивидуальный временной интервал, в течение которого возможен доступ в помещение. Все замки могут объединяться в единую автоматизированную систему, центральной частью которой является ПЭВМ. Вся управляющая информация в замки передается из ПЭВМ администратором. Если замок открывается изнутри также при помощи электронного ключа, то система позволяет фиксировать время входа и выхода, а также время пребывания владельцев ключей в помещениях. Эта система позволяет в любой момент установить местонахождение сотрудника. Система следит за тем, чтобы дверь всегда была закрыта. При попытках открывания двери в обход электронного замка включается сигнал тревоги с оповещением на центральный пункт управления. К таким автоматизированным системам относятся отечественные системы "Менуэт" и «Полонез» [52,53].

По статистике 85% случаев проникновения на объекты происходит через оконные проемы. Эти данные говорят о необходимо-

сти инженерного укрепления окон, **которое осуществляется** двумя путями:

- установка оконных решеток;
- применение стекол, устойчивых к механическому воздействию.

Традиционной защитой окон от проникновения злоумышленников является установка решеток. Решетки должны иметь диаметр прутьев не менее 10 мм, расстояние между ними должно быть не более 120 мм, а глубина заделки прутьев в стену - не менее 200 мм [48].

Не менее серьезным препятствием на пути злоумышленника могут быть и специальные стекла. Повышение механической прочности идет по трем направлениям:

- закаливание стекол;
- изготовление многослойных стекол;
- применение защитных пленок.

Механическая прочность полузакаленного стекла в 2 раза, а закаленного в 4 раза выше обычного строительного стекла.

В многослойных стеклах используются специальные пленки с высоким сопротивлением на разрыв. С помощью этих «ламинированных» пленок и синтетического клея обеспечивается склеивание на молекулярном уровне пленки и стекол. Такие многослойные стекла толщиной 48-83 мм обеспечивают защиту от стальной 7,62 мм пули, выпущенной из автомата Калашникова.

Все большее распространение получают многофункциональные защитные полиэфирные пленки. Наклеенные на обычное оконное стекло, они повышают его прочность в 20 раз [47]. Пленка состоит из шести очень тонких (единицы микрон) слоев: лавсана (3 слоя), металлизированного и невысыхающего клея адгезива и лакового покрытия. Кроме механической прочности они придают окнам целый ряд защитных свойств и улучшают эксплуатационные характеристики. Пленки ослабляют электромагнитные излучения в 50 раз, существенно затрудняют ведение разведки визуально-оптическими методами и перехват речевой информации лазерными средствами. Кроме того, пленки улучшают внешний вид стекол, отражают до 99 % ультрафиолетовых лучей и 76 % тепловой энергии солнца, сдерживают распространение огня при пожарах в течение 40 минут.

5.1.2. Охранная сигнализация

Охранная сигнализация служит для обнаружения попыток несанкционированного проникновения на охраняемый объект. Системы охранной сигнализации должны отвечать следующим требованием:

- охват контролируемой зоны по всему периметру;
- высокая чувствительность к действиям злоумышленника;
- надежная работа в любых погодных и временных условиях;
- устойчивость к естественным помехам;
- быстрота и точность определения места нарушения;
- возможность централизованного контроля событий.

Структура типовой системы охранной сигнализации представлена на рис. 4.

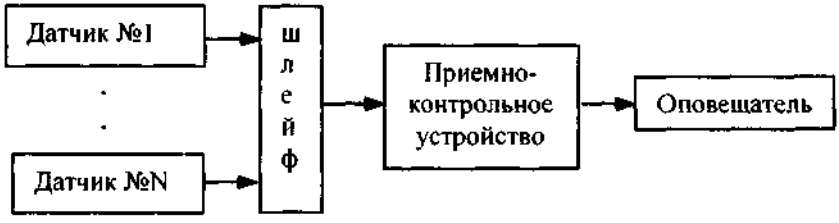


Рис. 4. Структура типовой системы охранной сигнализации

Датчик (извещатель) представляет собой устройство, формирующее электрический сигнал тревоги при воздействии на датчик или на создаваемое им поле внешних сил или объектов.

Шлейф сигнализации образует электрическую цепь для передачи сигнала тревоги от датчика к приемно-контрольному устройству.

Приемно-контрольное устройство служит для приема сигналов от датчиков, их обработки и регистрации, а также для выдачи сигналов в оповещатель.

Оповещатель выдает световые и звуковые сигналы дежурному охраннику.

По принципу обнаружения злоумышленников датчики делятся на [48]:

- контактные;
- акустические;
- оптико-электронные;
- микроволновые;
- вибрационные;
- емкостные;
- телевизионные.

Контактные датчики реагируют на замыкание или размыкание контактов, на обрыв тонкой проволоки или полоски фольги. Они бывают электроконтактными, магнитоконтактными, ударноконтактными и обрывными.

Электроконтактные датчики представляют собой кнопочные выключатели, которые размыкают (замыкают) электрические цепи, по которым сигнал тревоги поступает на приемно-контрольное устройство при несанкционированном открывании дверей, окон, люков, шкафов и т.д. К электроконтактным относятся датчики ДЭК-3, ВК-1М, СК-1М и другие.

Магнитоконтактные датчики служат также для блокирования дверей, окон и т. п. Кроме того, эти датчики используются для охраны переносимых предметов (небольших сейфов, носителей информации, переносных устройств и т. п.). Основу датчиков составляют герконы. В герконах контакты электрической цепи замыкаются (размыкаются) под действием постоянного магнитного поля. Геркон крепится на неподвижной части, а магнит на подвижной части. При закрытых дверях, окнах и т. п., а также при нахождении переносимых предметов на месте, геркон находится в поле магнита. При удалении магнита от геркона цепь размыкается (замыкается), и сигнал тревоги поступает на приемно-контрольное устройство. Магнитоконтактными являются датчики ДМК-П, ИО 102-4 (5, 6), СМК-3 и др.

Ударноконтактные датчики («Окно-5», ДИМК, ВМ-12М, УКД-1М и др.) используются для блокирования разрушающихся поверхностей. С помощью датчиков этого типа блокируются оконные стекла. В датчиках этого типа нормально замкнутые контакты размыкаются под действием силы инерции при перемещении корпуса датчика, приклеенного к стеклу.

При охране территорий, зданий используются *обрывные датчики*. Провода диаметром 0,1-0,25 мм располагают по периметру,

по возможности маскируя их. Вероятность обнаружения злоумышленника повышается при параллельной прокладке проводов на расстоянии не более 200 мм. В качестве примеров обрывных датчиков можно привести датчики «Трос-1», «Кувшинка», «Трепанг».

Акустические датчики используются для охраны зданий и помещений. Принцип действия акустических датчиков основан на использовании акустических волн, возникающих при взламывании элементов конструкции помещений или отраженных от злоумышленника. Используются датчики двух типов: пассивные и активные.

Пассивные датчики улавливают акустические волны, возникающие при разрушении элементов конструкции помещения, чаще всего оконных стекол. Пассивные датчики разделяются на пьезоэлектрические и электромагнитные. В пьезоэлектрических датчиках используется свойство пьезоэлементов создавать электрический сигнал при механическом воздействии на их поверхность. В электромагнитных датчиках используется свойство возникновения ЭДС в катушке электромагнита при изменении расстояния между сердечником электромагнита и мембраной. Пассивные акустические датчики «Грань-2» и «Окно-1» применяются для блокирования окон, стен, потолков, сейфов и т. п.

Активные датчики состоят из двух блоков. Один из них излучает акустические волны ультразвукового диапазона в помещении, а другой анализирует отраженные волны. При появлении каких-либо предметов в контролируемом помещении или возгораний изменяется акустический фон, что и фиксируется датчиком. Активные акустические (ультразвуковые) датчики (ДУЗ-4, ДУЗ-5, ДУЗ-12, «Фикус-МП-2 », «Эхо-2», «Эхо-3» и др.) служат для обнаружения злоумышленников и очагов пожаров в закрытых помещениях.

Оптико-электронные датчики построены на использовании инфракрасных лучей. Такие датчики делятся на активные и пассивные. Для работы активных датчиков используется излучатель остронаправленных ИК-лучей, которые принимаются приемником. При экранировании ИК-лучей каким-либо объектом приемник фиксирует отсутствие ИК-облучения и выдает сигнал тревоги. Пассивные датчики реагируют на тепловое излучение челове-

ка или огня. Для охраны коридоров, окон, дверей и территории по периметру используются активные датчики. Излучатель датчика создает от 2 до 16 параллельных ИК-лучей. Расстояние между излучателем и приемником датчика находится в диапазоне 20-300 метров. Для охраны территорий по периметру используются активные линейные оптико-электронные излучатели («Квант-1», «Квант-2У», «Вектор-2», «Вектор-3», «Вектор-4», «Рубеж-1М», «Рубеж-3М», «Мак», «Диалог» и др.).

Пассивные оптико-электронные датчики используются при охране помещений. Они способны зафиксировать объект, температура которого не менее чем на 3°С выше температуры фона. Датчики этого типа («Фотон-М», «Фотон-3», «Фотон-4», «Фотон-5», «Фотон-6», «Фотон-СК-2», «Квант-3» и др.) чувствительны к источникам тепла (батареи, электроприборы) и солнечным лучам. Эти особенности датчиков должны учитываться при их установке.

В микроволновых (радиоволновых) датчиках для обнаружения злоумышленников используются электромагнитные волны в СВЧ диапазоне (9 -11ГГц). Эти датчики состоят из излучателя и приемника. Различают радиолучевые и радиотехнические датчики. В *радиолучевых датчиках* используются излучатели, антенны которых формируют узкую диаграмму направленности в виде вытянутого эллипсоида с высотой и шириной в середине зоны обнаружения 2-10 м. Протяженность участка обнаружения достигает 300 м. Приемник реагирует на ослабление напряженности поля при пересечении объектом электромагнитного луча. При охране территорий по периметру используются радиолучевые датчики: «Радий-1», «Радий-2»,«Пион-Т», «Риф-РЛ», «Гарус», «Лена-2», «Протва», «Витим» и др.

В *радиотехнических датчиках* злоумышленник обнаруживается по изменению характеристик СВЧ поля. В этих датчиках в качестве антенны излучателя в СВЧ диапазоне используется специальный радиочастотный кабель, который прокладывается по периметру охраняемой территории. Антенна приемника находится в центре территории или представляет собой кабель, проложенный параллельно излучающему кабелю. При попадании злоумышленника в зону излучения характеристики сигнала на входе приемника изменяются, и приемник выдает сигнал тревоги в приемно-контрольное устройство. Система «Виадук», например, с

расположенным в центре зоны приемником, позволяет контролировать территорию радиусом до 300 метров.

В радиотехнических датчиках «Бином» и «S-Trax» электромагнитное поле создается между двумя параллельно расположенными коаксиальными кабелями с отверстиями. Кабели укладываются под землю вдоль периметра контролируемой территории на глубине 10-15 см на удалении 2-3 метра друг от друга. Один кабель через отверстия в оплетке создает электромагнитное поле, а параллельно проходящий кабель также через отверстия принимает это электромагнитное поле. Создаваемое поле имеет размеры: ширина - до 10 метров, высота и глубина - до 70 см. Такая кабельная система охраны позволяет обнаруживать не только злоумышленника, передвигающегося по поверхности земли, но и фиксировать попытки подкопа.

Вибрационные датчики обнаруживают злоумышленника по вибрации земли, заграждений, создаваемой им при проникновении на контролируемую территорию. Если датчики размещаются под землей, то их называют сейсмическими. Вибрационные датчики выполняются в виде отдельных пьезо- и электромагнитных чувствительных элементов, в виде световодов, кабелей с электрическим и магнитным полями, а также в виде шлангов с жидкостью. При механическом воздействии на датчики изменяются физические характеристики веществ, полей, светового луча, которые преобразуются в электрические сигналы тревоги. Примерами разработок вибрационных датчиков являются волоконно-оптический датчик «Ворон», кабель с магнитным полем «Guardwire» (Великобритания).

Принцип действия **емкостных датчиков** заключается в изменении эквивалентной емкости в контуре генератора сигналов датчика, которое вызывается увеличением распределенной емкости между злоумышленником и антенной датчика. Расстояние срабатывания составляет 10-30 см. В качестве антенны может быть использован охраняемый металлический объект (сейф, шкаф) или провод. Провод-антенна может быть проложен по верхней части забора, вдоль окон, дверных проемов и т. п. Емкостные датчики «Ромб-К4», «Пик», «Барьер-М», «Риф», «Градиент» и др. широко используются при охране контролируемых территорий, конструкций зданий и помещений.

Для контроля охраняемой зоны небольших размеров или отдельных важных помещений могут использоваться **телевизионные датчики.** Такой датчик представляет собой телевизионную камеру (VM 216 фирмы Retan), которая непрерывно передает изображение участка местности. Приемно-контрольное устройство с определенной дискретностью (до 20 раз в секунду) опрашивает датчики и сравнивает изображение с полученным ранее. Если в изображениях замечается различие (появление новых объектов, движение объектов), то включается монитор дежурного охранника с подачей звукового сигнала и включением видеомагнитофона.

При попытках уничтожения, обесточивания датчиков и шлейфов всех рассмотренных типов дежурный оператор охраны получает сигнал тревоги. Каждый тип датчиков фиксирует попытки проникновения на охраняемую территорию с определенной вероятностью. Для датчиков также возможно ложное срабатывание при появлении естественных помех, таких как сильный ветер, птицы и животные, гром и др. Повышение надежности работы систем контроля доступа на территорию объекта достигается путем:

- комбинированного использования датчиков разного типа;
- совершенствования датчиков и приемно-контрольных устройств.

Так в системах «Протва-3» и «Протва-4» используются одновременно вибрационные, радиолучевые и радиотехнические датчики. В системе «Гоби» применяются комплексно радиолучевые, вибрационные, контактные и емкостные датчики. Комбинированное использование датчиков различных типов значительно снижает вероятность бесконтрольного проникновения злоумышленника на территорию объекта КС. Основными направлениями[1] совершенствования датчиков являются повышение чувствительности и помехоустойчивости. Наиболее сложной задачей является повышение помехоустойчивости датчиков. Для решения этой задачи в датчиках должны быть заложены следующие возможности:

- регулировка чувствительности;
- анализ нескольких признаков возможного злоумышленника (например, размера и динамики перемещения);
- обучаемость;
- устойчивость к изменениям погодных условий.

Чтобы обеспечить реализацию таких возможностей, современные датчики создаются с использованием микропроцессорной техники.

Совершенствование приемно-контрольных устройств идет в направлении увеличения числа подключаемых шлейфов и типов датчиков, повышения достоверности сигналов тревоги за счет дополнительной обработки поступающих сигналов от датчиков, интеграции управления всеми охранными системами, включая систему пожарной безопасности, в одном устройстве управления комплексной системой охраны объекта. Такое устройство выполняется на базе ПЭВМ [46].

5.1.3. Средства наблюдения

Организация непрерывного наблюдения или видеоконтроля за объектом является одной из основных составляющих системы охраны объекта. В современных условиях функция наблюдения за объектом реализуется с помощью систем замкнутого телевидения.[1] Их называют также телевизионными системами видеоконтроля (ТСВ).

Телевизионная система видеоконтроля обеспечивает:

- автоматизированное видеонаблюдение за рубежами защиты;
- контроль за действиями персонала организации;
- видеозапись действий злоумышленников;
- режим видеоохраны.

В режиме видеоохраны ТСВ выполняет функции охранной сигнализации. Оператор ТСВ оповещается о движении в зоне наблюдения. В общем случае телевизионная система видеоконтроля включает следующие устройства (рис.5):

- передающие телевизионные камеры;
- мониторы;
- устройство обработки и коммутации видеоинформации (УОКВ);
- устройства регистрации информации (УРИ).

Диапазон применяемых телевизионных камер в ТСВ очень широк. Используются черно-белые и цветные камеры. Телекамеры могут устанавливаться скрытно. Для этих целей используются

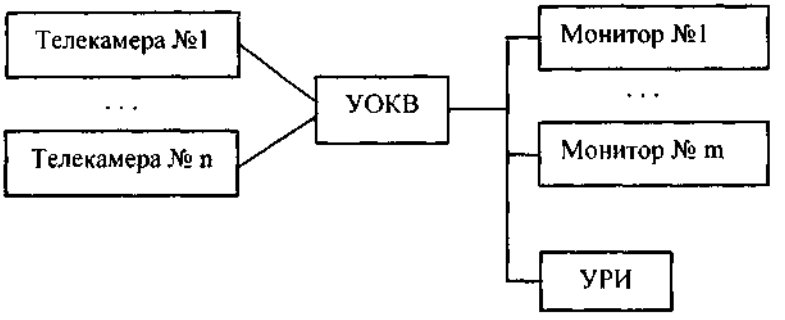


Рис. 5. Структурная схема телевизионной системы видеоконтроля

миниатюрные специальные камеры с уменьшенным наружным диаметром глазка. Камеры различаются также разрешающей способностью, длиной фокусного расстояния и рядом других характеристик. Для нормального функционирования телекамер в зоне их применения должна поддерживаться требуемая освещенность.

Используются черно-белые и цветные мониторы. Они отличаются также разрешающей способностью и размерами экрана.

В простейших ТСВ изображение от телекамер непосредственно подается на входы мониторов.

При наличии мониторов от 4-х и более оператору сложно вести наблюдение. Для сокращения числа мониторов используются устройства управления. В качестве устройств обработки и коммутации видеоинформации могут применяться следующие устройства:

- коммутаторы;
- квадраторы;
- мультиплексоры;
- детекторы движения.

Коммутаторы позволяют подключить к одному монитору от 4 до 16 телекамер с возможностью ручного или автоматического переключения с камеры на камеру.

Квадраторы обеспечивают одновременную выдачу изображения на одном мониторе от нескольких телекамер. Для этого экран монитора делится на части по количеству телекамер.

Мультиплексор является более совершенным УОКВ. Он мо-

жет выполнять функции коммутатора и квадратора. Кроме того, он позволяет осуществлять запись изображения на видеомагнитофон с любой камеры. Мультиплексор может включать в себя встроенный детектор движения.

Детектор движения оповещает оператора о движении в зоне контроля телекамеры, подключает эту камеру для записи видеоинформации на видеомагнитофон.

Видеомагнитофон относится к устройствам регистрации видеоинформации. В системах ТСВ используются специальные видеомагнитофоны, которые обеспечивают гораздо большее время записи (от 24 часов до 40 суток), чем бытовые видеомагнитофоны. Это достигается за счет пропуска кадров, уплотнения записи, записи при срабатывании детектора движения или по команде оператора.

Для фиксации отдельных кадров на бумаге используется другое УРИ - видеопринтер.

В Российской Федерации в основном применяется импортная телевизионная техника. Десятки российских компаний занимаются поставкой оборудования, и лишь некоторые из них осуществляют проектирование, монтаж, обслуживание ТСВ и обучение персонала.

*5.1.4. **Подсистема** доступа на объект*

Доступ на объекты производится на контрольно-пропускных пунктах (КПП), проходных, через контролируемый вход в здания и помещения. На КПП и проходных дежурят контролеры из состава дежурной смены охраны. Вход в здания и помещения может контролироваться только техническими средствами. Проходные, КПП, входы в здания и помещения оборудуются средствами автоматизации и контроля доступа.

Одной из основных задач, решаемых при организации допуска на объект, является **идентификация и аутентификация** лиц, допускаемых на объект. Их называют субъектами доступа.

Под **идентификацией** понимается присвоение субъектам доступа идентификаторов и (или) сравнение предъявляемых идентификаторов с перечнем присвоенных идентификаторов, владельцы (носители) которых допущены на объект.

Аутентификация означает проверку принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

Различают два способа идентификации людей: атрибутивный и биометрический. ***Атрибутивный*** *способ* предполагает выдачу субъекту доступа либо уникального предмета, либо пароля (кода), либо предмета, содержащего код.

Предметами, идентифицирующими субъект доступа, могут быть пропуска, жетоны или ключи от входных дверей (крышек устройств). Пропуска, жетоны и тому подобные идентификаторы не позволяют автоматизировать процесс допуска. Идентификация и аутентификация личности осуществляется контролером и поэтому носит субъективный характер. Пароль представляет собой набор символов и цифр, который известен только владельцу пароля и введен в систему, обеспечивающую доступ. Пароли используются, как правило, в системах разграничения доступа к устройствам КС. При допуске на объекты КС чаще используются коды. Они используются для открытия кодовых замков и содержат, в основном, цифры. Наиболее перспективными являются идентификаторы, которые представляют собой материальный носитель информации, содержащий идентификационный код субъекта доступа. Чаще всего носитель кода выполняется в виде пластиковой карты небольшого размера (площадь карты примерно в 2 раза больше площади поверхности спичечного коробка). Код идентификатора может быть считан только с помощью специального устройства. Кроме кода карта может содержать фотографию, краткие данные о владельце, т. е. ту информацию, которая обычно имеется в пропусках.

Пластиковые карты должны отвечать ряду требований:

- сложность несанкционированного считывания кода и изготовления дубля карты;
- высокие эксплуатационные качества;
- достаточная длина кода;
- низкая стоимость.

Под эксплуатационными качествами понимается надежность функционирования, возможность периодической смены кода, устойчивость к воздействиям внешней среды, удобство хранения и использования, длительный срок службы.

В зависимости от физических принципов записи, хранения и считывания идентификационной информации карты делятся на [48]:

- магнитные;
- инфракрасные;
- карты оптической памяти;
- штриховые;
- карты «Виганд»;
- полупроводниковые.

Магнитные карты имеют магнитную полосу, на которой может храниться около 100 байт информации. Эта информация считывается специальным устройством при протаскивании карты в прорези устройства.

На внутреннем слое *инфракрасных карт* с помощью специального вещества, поглощающего инфракрасные лучи, наносится идентификационная информация. Верхний слой карт прозрачен для инфракрасных лучей. Идентификационный код считывается при облучении карты внешним источником инфракрасных лучей.

При изготовлении *карт оптической памяти* используется WORM-технология, которая применяется при производстве компакт-дисков. Зеркальная поверхность обрабатывается лучом лазера, который прожигает в нужных позициях отверстия на этой поверхности. Информация считывается в специальных устройствах путем анализа отраженных от поверхности лучей. Емкость такой карты от 2 до 16 Мбайт информации.

В *штриховых картах* на внутреннем слое наносятся штрихи, которые доступны для восприятия только при специальном облучении лучами света. Варьируя толщину штрихов и их последовательность, получают идентификационный код. Процесс считывания осуществляется протаскиванием карты в прорези считывающего устройства.

Карточки «Виганд» содержат в пластиковой основе впрессованные отрезки тонкой проволоки со случайной ориентацией. Благодаря уникальности расположения отрезков проволоки каждая карта особым образом реагирует на внешнее электромагнитное поле. Эта реакция и служит идентифицирующим признаком.

Полупроводниковые карты содержат полупроводниковые микросхемы и могут быть контактными и бесконтактными. Кон-

тактные карты имеют по стандарту ISO 7816-1:1988 восемь металлических контактов с золотым покрытием. Наиболее простыми полупроводниковыми контактными картами являются карты, содержащие только микросхемы памяти. Наибольшее распространение из карт такого типа получили карты Touch Memory. Карта содержит постоянную память объемом 64 бита, в которой хранится серийный номер **Touch** Memory. Карта может иметь и перезаписываемую энергонезависимую память объемом от 1Кбит до 4Кбит. Карта этого типа не имеет разъема. Его заменяет двухпроводный интерфейс последовательного типа.

Полупроводниковые карты, имеющие в своем составе микропроцессор и память, называют интеллектуальными или *смарт-картами*. Смарт-карты фактически содержат микро-ЭВМ. Кроме задач идентификации такие карты решают целый ряд других задач, связанных с разграничением доступа к информации в КС. Еще более широкий круг задач способны решать *суперсмарт-карты*. Примером может служить многоцелевая карта фирмы Toshiba, которая используется в системе VISA. Возможности смарт-карты в таких картах дополнены миниатюрным монитором и клавиатурой.

Бесконтактные («проксимити») карты имеют в своем составе энергонезависимую память, радиочастотный идентификатор и рамочную антенну. Идентификатор передает код считывающему устройству на расстоянии до 80 см.

Наименее защищенными от фальсификации являются магнитные карты. Максимальную защищенность имеют смарт-карты. Карты «проксимити» очень удобны в эксплуатации.

Все атрибутивные идентификаторы обладают одним существенным недостатком. Идентификационный признак слабо или совсем не связан с личностью предъявителя.

Этого недостатка лишены методы биометрической идентификации. Они основаны на использовании индивидуальных биологических особенностей человека.

Для ***биометрической идентификации*** человека используются [51,68]:

- папиллярные узоры пальцев;
- узоры сетчатки глаз;
- форма кисти руки;

- особенности речи;
- форма и размеры лица.
- динамика подписи;
- ритм работы на клавиатуре;
- запах тела;
- термические характеристики тела.

Дактилоскопический метод идентификации человека используется давно. Он показал высокую достоверность идентификации. Папиллярные узоры считываются с пальца специальным сканером. Полученные результаты сравниваются с данными, хранящимися в системе идентификации.

Для удешевления оборудования идентификация проводится с использованием не всех признаков. На вероятность ошибки влияют некоторые факторы, например, температура пальцев. Из отечественных разработок таких систем известны системы «Кордон», «Папилон», DALLAS Bio-95 [70] .

По надежности и затратам времени метод идентификации *по узорам сетчатки глаз* сопоставим с дактилоскопическим методом [69]. С помощью высококачественной телекамеры осуществляется сканирование сетчатки глаза. Фиксируется угловое распределение кровеносных сосудов на поверхности сетчатки относительно слепого пятна глаза и других признаков. Всего насчитывается около 250 признаков. Оба метода доставляют субъектам доступа некоторый дискомфорт. Дактилоскопический метод у многих ассоциируется со снятием отпечатков пальцев у преступников. Метод сканирования сетчатки глаза доставляет неудобства, которые человек испытывает в процессе сканирования. Кроме того, метод идентификации по узору сетчатки глаза требует использования дорогостоящего оборудования.

Идентификация человека *по форме кисти руки* основана на анализе трехмерного изображения кисти. Метод менее надежен, устройство идентификации довольно громоздко. Вместе с тем метод технологичен и не требует хранения больших объемов информации.

Широкое распространение нашли способы идентификации человека *по голосу и по параметрам лица.* По надежности методы уступают методам идентификации по отпечаткам пальцев и узорам сетчатки глаза. Объясняется это значительно меньшей ста-

бильностью параметров голоса и лица человека. Однако лучшие системы обеспечивают вероятность достоверной идентификации порядка 0,98, что позволяет использовать их на практике (Voice Bolt).

Системы идентификации *по почерку* анализируют графическое начертание, интенсивность нажатия и быстроту написания букв. Контрольное слово пишется на специальном планшете, который преобразует характеристики письма в электрические сигналы. Системы такого типа обеспечивают высокую надежность идентификации.

Идентификация *по ритму работы на клавиатуре* [38] основывается на измерении времени между последовательным нажатием двух клавиш. В системе хранятся результаты измерений на тестовом тексте, обработанные методами математической статистики. Идентификация производится путем набора, статистической обработки произвольного или фиксированного текста и сравнения с хранящимися данными. Метод обеспечивает высокую надежность идентификации. Это единственный биометрический метод идентификации, не требующий дополнительных аппаратных затрат, если он используется для допуска к работе на технических средствах, имеющих наборные устройства.

Методы идентификации *по запаху и термическим характеристикам тела* пока не нашли широкого применения.

Основным достоинством биометрических методов идентификации является очень высокая вероятность обнаружения попыток несанкционированного доступа. Но этим методам присущи два недостатка. Даже в лучших системах вероятность ошибочного отказа в доступе субъекту, имеющему право на доступ, составляет 0,01. Затраты на обеспечение биометрических методов доступа, как правило, превосходят затраты на организацию атрибутивных методов доступа.

Для повышения надежности аутентификации используются несколько идентификаторов.

Подсистема доступа на объект выполняет также функции регистрации субъектов доступа и управления доступом. Если на объекте реализована идентификация с использованием автоматизированной системы на базе ПЭВМ, то с ее помощью может вестись протокол пребывания сотрудников на объекте, в помещени-

ях. Такая система позволяет осуществлять дистанционный контроль открывания дверей, ворот и т. п., а также оперативно изменять режим доступа сотрудников в помещения.

К средствам управления доступом можно отнести средства дистанционного управления замками, приводами дверей, ворот, турникетов и т. п.

5.1.5. Дежурная смена охраны

Состав дежурной смены, его экипировка, место размещения определяется статусом охраняемого объекта. Используя охранную сигнализацию, системы наблюдения и автоматизации доступа, дежурная смена охраны обеспечивает только санкционированный доступ на объект и в охраняемые помещения. Дежурная смена может находиться на объекте постоянно или прибывать на объект при получении сигналов тревоги от систем сигнализации и наблюдения.

5.2. Организация работ с конфиденциальными информационными ресурсами на объектах КС

Для противодействия таким угрозам как хищение документов, носителей информации, атрибутов систем защиты, а также изучение отходов носителей информации и создание неучтенных копий документов необходимо определить порядок учета, хранения, выдачи, работы и уничтожения носителей информации. Для обеспечения такой работы в учреждении могут создаваться специальные подразделения конфиденциального делопроизводства, либо вводиться штатные или нештатные должности сотрудников. Работа с конфиденциальными информационными ресурсами осуществляется в соответствии с законами РФ и ведомственными инструкциями. В каждой организации должны быть:

- разграничены полномочия должностных лиц по допуску их к информационным ресурсам:
- определены и оборудованы места хранения конфиденциальных информационных ресурсов и места работы с ними;
- установлен порядок учета, выдачи, работы и сдачи на хранение конфиденциальных информационных ресурсов;

- назначены ответственные лица с определением их полномочий и обязанностей;
- организован сбор и уничтожение ненужных документов и списанных машинных носителей;
- организован контроль над выполнением установленного порядка работы с конфиденциальными ресурсами.

5.3. Противодействие наблюдению в оптическом диапазоне

Наблюдение в оптическом диапазоне злоумышленником, находящимся за пределами объекта с КС, малоэффективно. С расстояния 50 метров даже совершенным длиннофокусным фотоаппаратом невозможно прочитать текст с документа или монитора. Так телеобъектив с фокусным расстоянием 300 мм обеспечивает разрешающую способность лишь 15х15 мм. Кроме того, угрозы такого типа легко парируются с помощью:

- использования оконных стекол с односторонней проводимостью света;
- применения штор и защитного окрашивания стекол;
- размещения рабочих столов, мониторов, табло и плакатов таким образом, чтобы они не просматривались через окна или открытые двери.

Для противодействия наблюдению в оптическом диапазоне злоумышленником, находящимся на объекте, необходимо, чтобы:

- двери помещений были закрытыми;
- расположение столов и мониторов ЭВМ исключало возможность наблюдения документов или выдаваемой информации на соседнем столе или мониторе;
- стенды с конфиденциальной информацией имели шторы.

5.4. Противодействие подслушиванию

Методы борьбы с подслушиванием можно разделить на два класса:

1) методы защиты речевой информации при передаче ее по каналам связи;

2) методы защиты от прослушивания акустических сигналов в помещениях.

Речевая информация, передаваемая по каналам связи, защищается от прослушивания (закрывается) с использованием методов аналогового скремблирования и дискретизации речи с последующим шифрованием [70].

Под *скремблированием* понимается изменение характеристик речевого сигнала таким образом, что полученный модулированный сигнал, обладая свойствами неразборчивости и неузнаваемости, занимает такую же полосу частот спектра, как и исходный открытый.

Обычно аналоговые скремблеры преобразуют исходный речевой сигнал путем изменения его частотных и временных характеристик.

Применяются несколько *способов частотного преобразования* сигнала:

- частотная инверсия спектра сигнала;
- частотная инверсия спектра сигнала со смещением несущей частоты;
- разделение полосы частот речевого сигнала на поддиапазоны с последующей перестановкой и инверсией.

Частотная инверсия спектра сигнала заключается в зеркальном отображении спектра исходного сигнала относительно выбранной частоты f_0 спектра. В результате низкие частоты преобразуются в высокие, и наоборот (рис. 6).

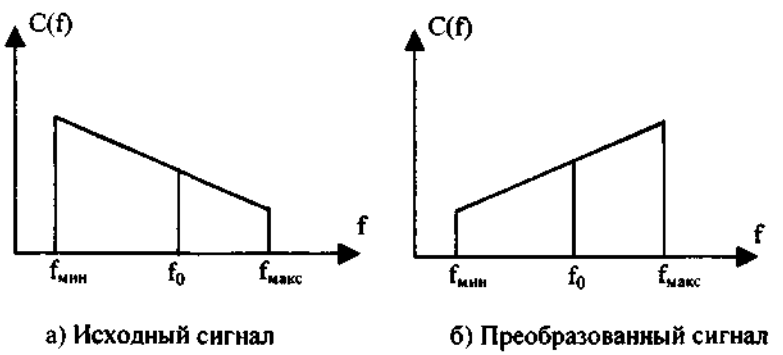


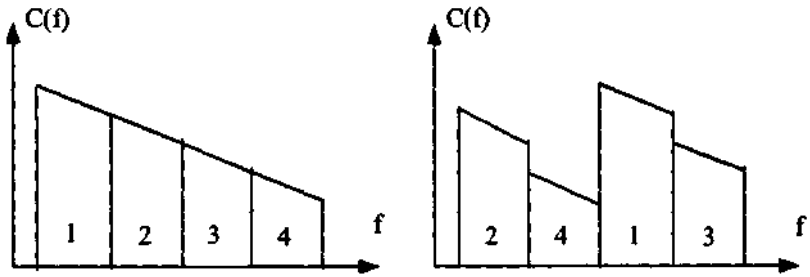
Рис. 6. Частотная инверсия сигнала

Такой способ скремблирования обеспечивает невысокий уровень защиты, так как частота fo легко определяется. Устройства, реализующие такой метод защиты, называют *маскираторами*.

Частотная инверсия спектра сигнала со смещением несущей частоты обеспечивает более высокую степень защиты.

Способ частотных перестановок заключается в разделении спектра исходного сигнала на поддиапазоны равной ширины (до 10-15 поддиапазонов) с последующим их перемешиванием в соответствии с некоторым алгоритмом.

Алгоритм зависит от ключа - некоторого числа (рис. 7).



а) Исходный сигнал б) Преобразованный сигнал

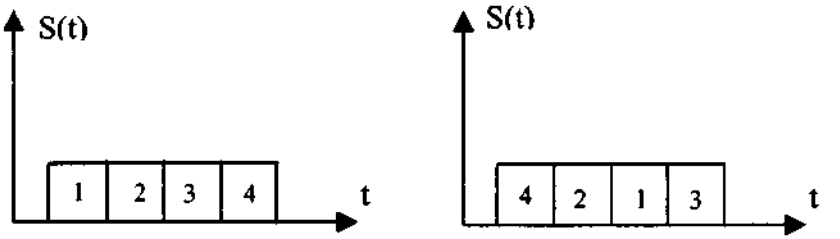
Рис. 7. Частотная перестановка сигнала

При временном скремблировании квант речевой информации (кадр) перед отправлением запоминается и разбивается на сегменты одинаковой длительности. Сегменты перемешиваются аналогично частотным перестановкам (рис. 8). При приеме кадр подвергается обратному преобразованию.

Комбинации временного и частотного скремблирования позволяют значительно повысить степень защиты речевой информации. За это приходится платить существенным повышением сложности скремблеров.

Дискретизация речевой информации с последующим шифрованием обеспечивает наивысшую степень защиты. В процессе дискретизации речевая информация представляется в цифровой форме. В таком виде она преобразуется в соответствии с выбранными алгоритмами шифрования, которые применяются для пре-

образования данных в **КС. Методы шифрования подробно** рассматриваются в гл. 9.



а) Исходный кадр **б) Преобразованный кадр**

Рис. 8. Временная перестановка

Удовлетворительное качество речевой информации, передаваемой в цифровом виде, обеспечивается при скорости передачи не ниже 64 кбит/с. Для снижения требований к каналам связи используются устройства кодирования речи (вокодеры). Спектр речевого сигнала изменяется относительно медленно. Это позволяет дискретно снимать характеристики сигнала, представлять их в цифровом виде и передавать по каналу связи. На приемной стороне вокодер по полученным характеристикам реализует один из алгоритмов синтеза речи. Наибольшее распространение получили вокодеры с линейным предсказанием речи. Такие вокодеры в процессе формирования речи реализуют кусочно-линейную аппроксимацию. Применение вокодеров позволяет снизить требования к скорости передачи данных до 2400 бит/с, а с некоторой потерей качества - до 800 бит/с.

Защита акустической информации в помещениях КС является важным направлением противодействия подслушиванию. Существует несколько **методов защиты от прослушивания акустических сигналов:**

- звукоизоляция и звукопоглощение акустического сигнала;
- зашумление помещений или твердой среды для маскировки акустических сигналов;
- защита от несанкционированной записи речевой информации на диктофон;
- обнаружение и изъятие закладных устройств.

Звукоизоляция обеспечивает локализацию источника звука в

замкнутом пространстве. Звукоизоляционные свойства конструкций и элементов помещений оцениваются величиной ослабления акустической волны и выражаются в децибелах. Наиболее слабыми звукоизолирующими свойствами в помещениях обладают двери и окна. Для усиления звукопоглощения дверей применяются следующие приемы:

- устраняются зазоры и щели за счет использования уплотнителей по периметру дверей;
- двери покрываются дополнительными звукопоглощающими материалами;
- используются двойные двери с покрытием тамбуров звукопоглощающими материалами.

Звукоизоляция окон повышается следующими способами:

- использование штор;
- увеличение числа рядов стекол (ширина воздушного промежутка между стеклами должна быть не менее 200 мм);
- применение полиэфирных пленок (затрудняют прослушивание лазерным методом);
- использование специальных оконных блоков с созданием разрежения в межстекольном пространстве.

Звукопоглощение осуществляется путем преобразования кинетической энергии звуковой волны в тепловую энергию. Звукопоглощающие материалы используются для затруднения прослушивания через стены, потолок, воздуховоды вентиляции и кондиционирования воздуха, кабельные каналы и тому подобные элементы зданий. Звукопоглощающие материалы могут быть сплошными и пористыми (плиты минераловатные "Акмигран", "Силакпор", "Винипор"; звукопоглощающие облицовки из слоя пористоволокнистого материала).

Активным методом защиты является *зашумление помещений* с помощью генераторов акустических сигналов (АД-23, WNG 023) [40]. Зашумление может быть эффективным, если генератор шума находится ближе к подслушивающему устройству, чем источник полезной акустической информации.

Более надежным способом защиты акустической информации является вибрационное зашумление (генераторы «Барон», «Заслон», «Кабинет») [44]. Шумы звукового диапазона создаются пьезокерамическими вибраторами в твердых телах, через которые

злоумышленник пытается прослушивать помещение. Вибраторы приклеиваются к поверхности зашумляемого ограждения (окна, стены, потолки и т. д.) или твердотельного звукопровода (трубы водоснабжения и отопления). Один вибратор создает зашумление в радиусе 1,5-5 метров.

Для *предотвращения несанкционированной записи речевой информации* необходимо иметь средства обнаружения работающего диктофона и средств воздействия на него, в результате которого качество записи снижается ниже допустимого уровня.

Несанкционированная запись речевой информации осуществляется специальными диктофонами, в которых снижены демаскирующие признаки: бесшумная работа лентопротяжного механизма, отсутствуют генераторы подмагничивания и стирания, используются экранированные головки и т. п.

Наибольшую информативность имеет низкочастотное пульсирующее магнитное поле работающего электродвигателя. Слабое поле электродвигателя может быть обнаружено на небольшом расстоянии. Например, отечественная система PRTD 018 обнаруживает диктофон на расстоянии 1,5 метра от датчика, которых в этой системе насчитывается 16 штук [40]. Малое магнитное поле электродвигателя выделяется за счет изменения в месте расположения работающего диктофона параметров полей, создаваемых другими работающими приборами.

При выявлении работающего диктофона руководитель может принять одно из возможных решений:

- отменить переговоры, совещание и т. п.;
- не вести конфиденциальных разговоров;
- использовать средства, создающие помехи записи на диктофон речевой информации;

Устройства защиты от записи речевой информации с помощью диктофона воздействуют создаваемыми ими полями на усилители записи диктофонов. В результате такого воздействия качество записи ухудшается настолько, что невозможно разборчивое воспроизведение речи. Современные средства подавления записи класса («Рубеж», «Шумотрон», «УПД», «Буран») [44] действуют на расстоянии до 3 метров и способны непрерывно работать до 2 часов. Устройство «Буран-2» является мобильным и размещается в портфеле («дипломате»).

5.5. Средства борьбы с закладными подслушивающими устройствами

5.5.1. Средства радиоконтроля помещений

Поиск и нейтрализация закладных подслушивающих устройств усложняется многообразием их типов. Велик список и средств борьбы с закладками этого типа.

Средства борьбы с закладными подслушивающими устройствами делятся на:

- средства радиоконтроля помещений;
- средства поиска неизлучающих закладок;
- средства подавления закладных устройств.

Для осуществления радиоконтроля помещений - обнаружения радиоизлучающих закладок - применяются следующие типы устройств:

- индикаторы электромагнитного поля;
- бытовые радиоприемники;
- специальные радиоприемники;
- автоматизированные комплексы.

Индикаторы электромагнитного поля (ИПФ-4, **D-008, «Оса»)** информируют о наличии электромагнитного поля выше фонового. Чувствительность таких устройств мала, и они способны обнаруживать поля радиозакладок в непосредственной близости от источника излучения (несколько метров).

Бытовые радиоприемники обладают большей чувствительностью, чем обнаружители поля. Основным недостатком бытовых приемников является узкий диапазон контролируемых частот.

Широко распространенным типом устройств обнаружения излучающих закладок является *специальный приемник* **(IC-R10, AR-**8000, MVT-7200) [45]. Среди устройств этого типа наиболее перспективными являются радиоприемники с автоматическим сканированием радиодиапазона и излучателем тестового акустического сигнала. Встроенный микропроцессор обеспечивает поиск «своего» сигнала, т. е. сигнала, который выдает радиозакладка при получении тестового акустического сигнала. Специальные приемники позволяют контролировать диапазон частот от долей МГц до

единиц ГГц. Сканирование всего диапазона частот занимает 3-4 минуты.

Наиболее совершенными средствами обнаружения радиозакладок являются *автоматизированные аппаратно-программные комплексы.* Основу таких комплексов составляют специальный радиоприемник и мобильная персональная ЭВМ. Такие комплексы хранят в памяти ПЭВМ уровни и частоты радиосигналов в контролируемом помещении и выявляют, при их наличии, закладки по изменению спектрограмм излучений. Автоматизированные комплексы определяют координаты радиозакладок и содержат, как правило, также блок контроля проводных линий. Все операции автоматизированы, поэтому такие комплексы являются многофункциональными и могут использоваться непрерывно. Лучшие образцы автоматизированных комплексов («Дельта», «Крона-6Н», АРК-ДЗ) обеспечивают точность пеленгации 2-8 градуса (точность измерения координат - до 10 см), измерение характеристик сигналов радиозакладок и могут контролировать до 12 помещений [45].

5.5.2. Средства поиска неизлучающих закладок

Для обнаружения неизлучающих закладок используются:

- средства контроля проводных линий;
- средства обнаружения элементов закладок.

Наиболее распространенными проводными линиями, по которым закладные устройства передают информацию, являются телефонные линии и линии электропитания, а также линии пожарной и охранной сигнализации, линии селекторной связи. Принцип работы аппаратуры контроля проводных линий основан на том, что любое подключение к ним вызывает изменение электрических параметров линий, таких как напряжение, ток, сопротивление, емкость и индуктивность. Аппаратура контроля устанавливает также наличие нештатных электрических сигналов в линии. Закладки могут подключаться к линиям параллельно и последовательно. При параллельном подключении и высоком входном сопротивлении закладок (>1,5 МОм) обнаружить их очень сложно [58]. Для повышения чувствительности средств контроля увеличивают число измеряемых параметров, вводят статистическую

обработку результатов измерений (ССТО-1000). Некоторые устройства контроля (АПЛ-1, АТ-2, «Бор», Р5-8) позволяют определять длину участка проводной линии до закладки. Эти устройства используют свойство сигнала отражаться от неоднородностей, которые создаются в местах физического подключения.

Для *выявления закладок,* в том числе и находящихся в неработающем состоянии, используются следующие средства:

- устройства нелинейной локации;
- обнаружители пустот;
- металлодетекторы;
- рентгеновские установки.

В *устройствах нелинейной локации* [5]используются нелинейные свойства полупроводников. При облучении полупроводников высокочастотным электромагнитным излучением с частотой f_0 в отраженных волнах появляются гармоники с частотами, кратными f_0 - $2f_0$, 3fo и т. д. Амплитуда отраженных волн резко уменьшается с ростом кратности частоты. На практике анализируются гармоники с частотами $2f_0$ и $3f_0$. Факт наличия отраженных волн с гармониками, кратными по частоте волне облучения, еще не доказывает наличие закладки с полупроводниковыми элементами. Подобные отраженные сигналы могут появляться при облучении, например, бетонных конструкций с находящимися внутри них ржавыми прутьями. Именно поэтому для повышения достоверности результатов локации и обеспечивается анализ двух гармоник с частотами 2fo и $3f_0$. Нелинейные локаторы («Родник», «Обь», «Октава» «Циклон-М», «Super Broom») [5] обеспечивают дальность обнаружения полупроводниковых приборов до 3 метров при ошибке обнаружения координат, не превышающей единицы сантиметров. В строительных конструкциях глубина обнаружения закладок уменьшается (в бетоне - до 0,5 метра).

Для скрытого размещения закладок в элементах конструкций зданий, в мебели и других сплошных физических средах необходимо создать закамуфлированные углубления, отверстия и т. п. Такие изменения конструкций являются демаскирующим признаком закладки. Поэтому возможен косвенный поиск закладок путем *поиска пустот* в сплошных физических средах. При обнаружении пустот они могут быть обследованы более тщательно другими средствами контроля.

Пустоты в сплошных средах обнаруживаются с использованием устройств, принцип действия которых основывается на различных физических свойствах пустот:

- изменение характера распространения звука;
- отличие в значениях диэлектрической проницаемости;
- различие в теплопроводности среды и пустоты.

Пустоты обнаруживаются простым простукиванием сплошных сред. Для этой же цели используются ультразвуковые приборы. Электрическое поле деформируется пустотами за счет разницы диэлектрических свойств среды и пустоты. Это свойство электрического поля используется для поиска пустот. Пустоты обнаруживаются также по разнице температур с помощью тепловизоров. Такие приборы способны фиксировать разницу температур 0,05° С (тепловизионная система «Иртис-200») [36].

Принцип действия *металлодетекторов* основан на использовании свойств проводников взаимодействовать с внешним электрическим и магнитным полем. Любая закладка содержит проводники: резисторы, шины, корпус элементов питания и самой закладки и др.

При воздействии электромагнитного поля в проводниках объекта возникают вихревые токи. Поля, создаваемые этими токами, усиливаются и затем анализируются микропроцессором металлодетектора. Расстояние, с которого обнаруживается объект, зависит от размеров проводника и типа металлодетектора. Так, прибор «Метокс МД311» обнаруживает диск диаметром 22 мм на расстоянии 140 см. [48].

Реже используются для поиска закладок переносные *рентгеновские установки* («Шмель-90/К», «Рона») [41]. Используются такие установки для контроля неразборных предметов.

5.5.3. Средства подавления закладных устройств

Обнаруженную закладку можно изъять, использовать для дезинформации или подавить. Под подавлением понимается такое воздействие на закладку, в результате которого она не способна выполнять возложенные на нее функции. Для подавления закладок используются:

- генераторы помех;

- средства нарушения функционирования закладок;
- средства разрушения закладок.

Генераторы используются для подавления сигналов закладок как в линиях, так и для пространственного зашумления радиозакладок. Генераторы создают сигналы помех, перекрывающие по частоте диапазоны частот, на которых работают закладки. Амплитуда сигнала-помехи должна в несколько раз превышать амплитуду сигналов закладки.

Средства нарушения работы закладки воздействуют на закладку с целью изменения режимов ее работы, изменения условий функционирования. Например, устройство защиты телефонных линий УЗТ-02 генерирует сигнал помехи амплитудой 35 В, который приводит к искажению спектра сигнала, излучаемого закладкой, и снижению соотношения сигнал/шум на входе приемника злоумышленника. Другим примером применения средств нарушения работы закладки является воздействие помех, нарушающих работу устройств автоматической регулировки уровня записи и автоматического включения диктофона голосом.

Разрушение закладок без их изъятия осуществляется в линиях (телефонной, громкой связи, электропитания и т. п.) путем подачи коротких импульсов высокого напряжения (до 4000 В). Предварительно от линий отключаются все оконечные радиоэлектронные устройства.

5.6. Защита от злоумышленных действий обслуживающего персонала и пользователей

По статистике 80% случаев злоумышленных воздействий на информационные ресурсы совершаются людьми, имеющими непосредственное отношение к эксплуатации КС. Такие действия совершаются либо под воздействием преступных групп (разведывательных служб), либо побуждаются внутренними причинами (зависть, месть, корысть и т. п.). Для блокирования угроз такого типа руководство организации с помощью службы безопасности должно осуществлять следующие организационные мероприятия:

- добывать всеми доступными законными путями информацию о своих сотрудниках, о людях или организациях, представляющих потенциальную угрозу информационным ресурсам;

- обеспечивать охрану сотрудников;
- устанавливать разграничение доступа к защищаемым ресурсам;
- контролировать выполнение установленных мер безопасности;
- создавать и поддерживать в коллективе здоровый нравственный климат.

Руководство должно владеть, по возможности, полной информацией об образе жизни своих сотрудников. Основное внимание при этом следует обращать на получение информации о ближайшем окружении, о соответствии легальных доходов и расходов, о наличии вредных привычек, об отрицательных чертах характера, о состоянии здоровья, о степени удовлетворенности профессиональной деятельностью и занимаемой должностью. Для получения такой информации используются сотрудники службы безопасности, психологи, руководящий состав учреждения. С этой же целью осуществляется взаимодействие с органами МВД и спецслужбами. Сбор информации необходимо вести, не нарушая законы и права личности.

Вне пределов объекта охраняются, как правило, только руководители и сотрудники, которым реально угрожает воздействие злоумышленников.

В организации, работающей с конфиденциальной информацией, обязательно разграничение доступа к информационным ресурсам. В случае предательства или других злоумышленных действий сотрудника ущерб должен быть ограничен рамками его компетенции. Сотрудники учреждения должны знать, что выполнение установленных правил контролируется руководством и службой безопасности.

Далеко не последнюю роль в парировании угроз данного типа играет нравственный климат в коллективе. В идеале каждый сотрудник является патриотом коллектива, дорожит своим местом, его инициатива и отличия ценятся руководством.

Контрольные вопросы

1. Приведите состав системы охраны объекта и охарактеризуйте защитные свойства инженерных конструкций.

2. Каковы состав, назначение и принцип действия элементов охранной сигнализации?
3. Охарактеризуйте подсистему доступа на объект.
4. Поясните принципы защиты речевой информации в каналах связи.
5. Перечислите и охарактеризуйте методы защиты от прослушивания акустических сигналов.
6. Охарактеризуйте средства борьбы с закладными подслушивающими устройствами.
7. Приведите мероприятия, проводимые для защиты от злоумышленных действий обслуживающего персонала.

ГЛАВА 6
Методы и средства защиты от электромагнитных излучений и наводок

6.1. Пассивные методы защиты от побочных электромагнитных излучений и наводок

Все методы защиты от электромагнитных излучений и наводок можно разделить на **пассивные** и **активные.**

Пассивные методы обеспечивают уменьшение уровня опасного сигнала или снижение информативности сигналов.

Активные методы защиты направлены на создание помех в каналах побочных электромагнитных излучений и наводок, затрудняющих прием и выделение полезной информации из перехваченных злоумышленником сигналов.

Для блокирования угрозы воздействия на электронные блоки и магнитные запоминающие устройства мощными внешними электромагнитными импульсами и высокочастотными излучениями, приводящими к неисправности электронных блоков и стирающими информацию с магнитных носителей информации, используется экранирование защищаемых средств.

Защита от побочных электромагнитных излучений и наводок осуществляется как пассивными, так и активными методами.

Пассивные методы защиты от ПЭМИН могут быть разбиты на три группы (рис. 9).

Рис. 9. Классификация пассивных методов защиты от ПЭМИН

6.1.1. Экранирование

Экранирование является одним из ^амых эффективных методов защиты от электромагнитных излучений. Под *экранированием* понимается размещение элементов КС, создающих электрические, магнитные и электромагнитные поля, в пространственно замкнутых конструкциях. Способы экранирования зависят от особенностей полей, создаваемых элементами КС при протекании в них электрического тока.

Характеристики полей зависят от параметров электрических сигналов в КС. Так при малых токах и высоких напряжениях в создаваемом поле преобладает электрическая составляющая. Такое поле называется электрическим (электростатическим). Если в проводнике протекает ток большой величины при малых значениях напряжения, то в поле преобладает магнитная составляющая, а поле называется магнитным. Поля, у которых электрическая и магнитная составляющие соизмеримы, называются электромагнитными.

В зависимости от типа создаваемого электромагнитного поля различают следующие виды экранирования:

- экранирование электрического поля;
- экранирование магнитного поля;
- экранирование электромагнитного поля.

Экранирование электрического поля заземленным металлическим экраном обеспечивает нейтрализацию электрических зарядов, которые стекают по заземляющему контуру. Контур заземления должен иметь сопротивление не более 4 Ом. Электрическое поле может экранироваться и с помощью диэлектрических экранов, имеющих высокую относительную диэлектрическую проницаемость *г.* При этом поле ослабляется в s раз [64].

При экранировании магнитных полей различают низкочастотные магнитные поля (до 10 кГц) и высокочастотные магнитные поля. .

Низкочастотные магнитные поля шунтируются экраном за счет направленности силовых линий вдоль стенок экрана. Этот эффект вызывается большей магнитной проницаемостью материала экрана по сравнению с воздухом.

Высокочастотное магнитное поле вызывает возникновение в экране переменных индукционных вихревых токов, которые создаваемым ими магнитным полем препятствуют распространению побочного магнитного поля. Заземление не влияет на экранирование магнитных полей. Поглощающая способность экрана зависит от частоты побочного излучения и от материала, из которого изготавливается экран. Чем ниже частота излучения, тем большей должна быть толщина экрана. Для излучений в диапазоне средних волн и выше достаточно эффективным является экран толщиной 0,5-1,5 мм. Для излучений на частотах свыше 10 МГц достаточно иметь экран из меди или серебра толщиной 0,1 мм.

Электромагнитные излучения блокируются методами высокочастотного электрического и магнитного экранирования.

Экранирование осуществляется на пяти уровнях:

- уровень элементов схем;
- уровень блоков;
- уровень устройств;
- уровень кабельных линий;
- уровень помещений.

Элементы схем с высоким уровнем побочных излучений могут помещаться в металлические или металлизированные напылением заземленные корпуса. Начиная с уровня блоков, экранирование осуществляется с помощью конструкций из листовой стали, металлических сеток и напыления. Экранирование кабелей осу-

ществляется с помощью металлической оплетки, стальных коробов или труб.

При экранировании помещений используются: листовая сталь толщиной до 2 мм, стальная (медная, латунная) сетка с ячейкой до 2,5 мм. В защищенных помещениях экранируются двери и окна. Окна экранируются сеткой, металлизированными шторами, металлизацией стекол и оклеиванием их токопроводящими пленками. Двери выполняются из стали или покрываются токопроводящими материалами (стальной лист, металлическая сетка). Особое внимание обращается на наличие электрического контакта токопроводящих слоев двери и стен по всему периметру дверного проема. При экранировании полей недопустимо наличие зазоров, щелей в экране. Размер ячейки сетки должен быть не более 0,1 длины волны излучения.

Выбор числа уровней и материалов экранирования осуществляется с учетом:

- характеристик излучения (тип, частота и мощность);
- требований к уровню излучения за пределами контролируемой зоны и размеров зоны;
- наличия или отсутствия других методов защиты от ПЭМИН;
- минимизации затрат на экранирование.

В защищенной ПЭВМ, например, экранируются блоки управления электронно-лучевой трубкой, корпус выполняется из стали или металлизируется изнутри, экран монитора покрывается токопроводящей заземленной пленкой и (или) защищается металлической сеткой.

Экранирование, помимо выполнения своей прямой функции - защиты от ПЭМИН, значительно снижает вредное воздействие электромагнитных излучений на организм человека. Экранирование позволяет также уменьшить влияние электромагнитных шумов на работу устройств.

6.1.2. Снижение мощности излучений и наводок

Способы защиты от ПЭМИН, объединенные в эту группу, реализуются с целью снижения уровня излучения и взаимного влияния элементов КС.

К данной группе относятся следующие методы:

- изменение электрических схем;
- использование оптических каналов связи;
- изменение конструкции;
- использование фильтров;
- гальваническая развязка в системе питания.

Изменения электрических схем осуществляются для уменьшения мощности побочных излучений. Это достигается за счет использования элементов с меньшим излучением, уменьшения крутизны фронтов сигналов, предотвращения возникновения паразитной генерации, нарушения регулярности повторений информации.

Перспективным направлением борьбы с ПЭМИН является использование *оптических каналов* связи. Для передачи информации на большие расстояния успешно используются волоконно-оптические кабели. Передачу информации в пределах одного помещения (даже больших размеров) можно осуществлять с помощью беспроводных систем, использующих излучения в инфракрасном диапазоне. Оптические каналы связи не порождают ПЭМИН. Они обеспечивают высокую скорость передачи и не подвержены воздействию электромагнитных помех.

Изменения конструкции сводятся к изменению взаимного расположения отдельных узлов, блоков, кабелей, сокращению длины шин.

Использование фильтров [64] является одним из основных способов защиты от ПЭМИН. Фильтры устанавливаются как внутри устройств, систем для устранения распространения и возможного усиления наведенных побочных электромагнитных сигналов, так и на выходе из объектов линий связи, сигнализации и электропитания. Фильтры рассчитываются таким образом, чтобы они обеспечивали снижение сигналов в диапазоне побочных наводок до безопасного уровня и не вносили существенных искажений полезного сигнала.

Полностью исключается попадание побочных наведенных сигналов во внешнюю цепь электропитания при наличии генераторов питания, которые обеспечивают *гальваническую развязку* между первичной и вторичной цепями.

Использование генераторов позволяет также подавать во вто-

ричную цепь электропитание с другими параметрами по сравнению с первичной цепью. Так, во вторичной цепи может быть изменена частота по сравнению с первичной цепью.

Генераторы питания, за счет инерционности механической части, позволяют сглаживать пульсации напряжения и кратковременные отключения в первичной цепи.

6.1.3. Снижение информативности сигналов

Снижение информативности сигналов ПЭМИН, затрудняющее их использование при перехвате, осуществляется следующими путями:

- специальные схемные решения;
- кодирование информации.

В качестве примеров специальных схемных решений можно привести такие, как замена последовательного кода параллельным, увеличение разрядности параллельных кодов, изменение очередности развертки строк на мониторе и т. п. Эти меры затрудняют процесс получения информации из перехваченного злоумышленником сигнала. Так, если в мониторе изображение формируется не за счет последовательной развертки строк, а по какому-то особому закону, то при перехвате электромагнитного поля и использовании стандартной развертки изображение на экране монитора злоумышленника не будет соответствовать исходному.

Для предотвращения утечки информации может использоваться кодирование информации, в том числе и криптографическое преобразование.

6.2. Активные методы защиты от ПЭМИН

Активные методы защиты от ПЭМИН предполагают применение генераторов шумов, различающихся принципами формирования маскирующих помех. В качестве маскирующих используются случайные помехи с нормальным законом распределения спектральной плотности мгновенных значений амплитуд (гауссовские помехи) и прицельные помехи, представляющие собой случайную последовательность сигналов помехи, идентичных побочным сигналам.

Используется пространственное и линейное зашумление. ***Пространственное зашумление*** осуществляется за счет излучения с помощью антенн электромагнитных сигналов в пространство. Применяется *локальное пространгтвенное зашумление* для защиты конкретного элемента КС и *объектовое пространственное зашумление* для защиты от побочных электромагнитных излучений КС всего объекта. При *локальном пространственном зашумлении* используются прицельные помехи. Антенна находится рядом с защищаемым элементом КС. *Объектовое пространственное зашумление* осуществляется, как правило, несколькими генераторами со своими антеннами, что позволяет создавать помехи во всех диапазонах побочных электромагнитных излучений всех излучающих устройств объекта.

Пространственное зашумление должно обеспечивать невозможность выделения побочных излучений на фоне создаваемых помех во всех диапазонах излучения и, вместе с тем, уровень создаваемых помех не должен превышать санитарных норм и норм по электромагнитной совместимости радиоэлектронной аппаратуры.

При использовании *линейного* ***зашумления*** генераторы прицельных помех подключаются к токопроводящим линиям для создания в них электрических помех, которые не позволяют злоумышленникам выделять наведенные сигналы.

Контрольные вопросы

1. Дайте общую характеристику методам защиты от электромагнитных излучений.
2. Поясните сущность экранирования.
3. Чем достигается снижение мощности электромагнитных излучений и наводок?
4. Каким образом снижается информативность сигналов в КС?
5. Охарактеризуйте активные методы защиты от побочных электромагнитных излучений и наводок.

ГЛАВА 7

Методы защиты от несанкционированного изменения структур КС

7.1. Общие требования к защищенности КС от несанкционированного изменения структур

Несанкционированному изменению могут быть подвергнуты алгоритмическая, программная и техническая структуры КС на этапах ее разработки и эксплуатации. На этапе эксплуатации необходимо выделить работы по модернизации КС, представляющие повышенную опасность для безопасности информации.

Особенностью защиты от несанкционированного изменения структур (НИС) КС является универсальность методов, позволяющих наряду с умышленными воздействиями выявлять и блокировать непреднамеренные ошибки разработчиков и обслуживающего персонала, а также сбои и отказы аппаратных и программных средств. Обычно НИС КС, выполненные на этапе разработки и при модернизации системы, называют **закладками.**

Для парирования угроз данного класса на различных этапах жизненного цикла КС решаются различные задачи. На этапе разработки и при модернизации КС основной задачей является исключение ошибок и возможности внедрения закладок. На этапе эксплуатации выявляются закладки и ошибки, а также обеспечивается целостность, неизменность структур.

Разработке программных и аппаратных средств предшествует разработка алгоритмов. Ошибки и закладки, внесенные и не устраненные на этапе разработки алгоритмов, переходят в программы и оборудование, если не будут своевременно обнаружены.

При разработке алгоритмов, программ и аппаратных средств необходимо придерживаться **основных принципов,** которые являются общими:

- привлечение к разработке высококвалифицированных специалистов;
- использование иерархических структур;
- применение стандартных блоков;

- дублирование разработки;
- контроль адекватности;
- многослойная фильтрация;
- автоматизация разработки;
- контроль процесса разработки;
- сертификация готового продукта.

Особые требования предъявляются к квалификации специалистов, занятых разработкой технического задания и алгоритмов, осуществляющих контроль над ходом разработки, и привлекаемых к сертификации готовых продуктов.

Представление любой системы в виде иерархической блочной структуры позволяет представлять любой блок в виде черного ящика (рис.10).

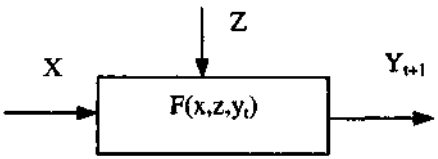


Рис. 10. Графическоепредставлениеблока

Блок осуществляет преобразование вектора X входных воздействий при наличии вектора внешних условий Z и с учетом состояния блока Y_t. Функциональное преобразование F (x, z, y_t) переводит блок в состояние, характеризуемое состоянием Y_t +ь где x e X, z € Z, y e Y.

Блочная структура системы позволяет упростить контроль функционирования системы, использовать стандартные отлаженные и проверенные блоки, допускает параллельную разработку всех блоков и дублирование разработки.

Под дублированием разработки алгоритма программы или устройства понимается независимая (возможно разными организациями) разработка одного и того же блока. Сравнение блоков позволяет, во-первых, выявить ошибки и закладки, а во-вторых, выбрать наиболее эффективный блок.

Проверка адекватности функционирования алгоритма, программы, устройства реализуется путем моделирования процессов,

использования упрощенных (усеченных) алгоритмов, решения обратной задачи (если она существует), а также с помощью тестирования.

Тестирование является универсальным средством проверки как адекватности, так и работоспособности блоков. Если число входных воздействий и внешних условий конечно и может быть задано при испытании блока за приемлемое для практики время, а также известны все требуемые реакции блока, то адекватность функционирования блока может быть однозначно подтверждена, т. е. в блоке полностью отсутствуют ошибки и закладки. Обнаружение ошибок и закладок тестированием осложняется тем, что мощность входного множества по оценкам специалистов может достигать 10^{70} - 10^{100} [19]. Поэтому для тестирования по всей области входных воздействий потребуется практически бесконечное время. В таких случаях используется вероятностный подход к выборке входных воздействий. Но такая проверка не может гарантировать отсутствия закладок и ошибок.

Принцип многослойной «фильтрации» предполагает поэтапное выявление ошибок и закладок определенного класса. Например, могут использоваться «фильтрующие» программные средства для выявления возможных «временных», «интервальных», «частотных» и других типов закладок.

Автоматизация процесса разработки существенно снижает возможности внедрения закладок. Это объясняется, прежде всего, наличием большого числа типовых решений, которые исполнитель изменить не может, формализованностью процесса разработки, возможностью автоматизированного контроля принимаемых решений.

Контроль установленного порядка разработки предполагает регулярный контроль над действиями исполнителей, поэтапный контроль алгоритмов, программ и устройств, приемо-сдаточные испытания.

Разработка защищенных КС и элементов для них завершается сертификацией готового продукта. Сертификация проводится в специальных лабораториях, оснащенных испытательными стендами, укомплектованных специалистами соответствующей квалификации и имеющих официальное разрешение (лицензию) на такой вид деятельности. В таких лабораториях по определенным

методикам осуществляется проверка программных и аппаратных средств на отсутствие закладок, а также соответствие средств защиты информации их назначению.

7.2. Защита от закладок при разработке программ

7. *2.1. Современные технологии программирования*

Для разработки программных средств, свободных от ошибок и закладок, необходимо выполнение следующих условий:

- использование современных технологий программирования;
- наличие автоматизированной системы разработки;
- наличие автоматизированных контрольно-испытательных стендов;
- представление готовых программ на языках высокого уровня;
- наличие трансляторов для обнаружения закладок.

Современные технологии программирования предполагают высокую степень автоматизации процессов создания, отладки и тестирования программ. Применение стандартных модулей позволяет упростить процесс создания программ, поиска ошибок и закладок.

Одним из перспективных направлений создания программного обеспечения повышенной безопасности является использование объектно-ориентированного программирования, идущего на смену структурному программированию [19].

Применение объектно-ориентированного программирования (ООП) позволяет разделить фазы описания и фазы реализации абстрактных типов данных. Два выделенных модуля допускают раздельную компиляцию. В модуле описания задаются имена и типы внутренних защищенных и внешних данных, а также перечень процедур (методов) с описанием типов и количества параметров для них. В модуле реализации находятся собственно процедуры, обрабатывающие данные. Такое разделение повышает надежность программирования, так как доступ к внутренним данным возможен только с помощью процедур, перечисленных в модуле описания. Это позволяет определять большую часть ошибок

в обработке абстрактного типа данных на этапе компиляции, а не на этапе выполнения. Анализ программных средств на наличие закладок облегчается, так как допустимые действия с абстрактными данными задаются в модуле описания, а не в теле процедур.

Одним из центральных понятий ООП является понятие «класс». С помощью этого понятия осуществляется связывание определенного типа данных с набором процедур и функций, которые могут манипулировать с этим типом данных.

Преимущество ООП заключается также в предоставлении возможности модификации функционирования, добавления новых свойств или уничтожении ненужных элементов, не изменяя того, что уже написано и отлажено. Пользователю достаточно определить объекты, принадлежащие уже созданным классам и посылать им сообщения. При этом контроль безопасности программного продукта сводится к анализу модулей описания классов. Если класс из библиотеки классов не удовлетворяет разработчика, то он может создать класс, производный от базового, произвести в нем необходимые изменения и работать с объектами полученного производного класса. Если данные и методы базового класса не должны быть доступны в производных классах, то их следует описать как внутренние.

Концепция ООП вынуждает разработчиков программных продуктов тщательно продумывать структуру данных класса и набор методов (процедур), которые необходимы для обработки этих данных. Получаемые программы представляют собой множество легко читаемых, самодокументируемых модулей описаний классов и множество модулей реализации тел методов. Такое представление программ упрощает их семантический анализ и контроль на наличие в них закладок.

7.2.2. Автоматизированная система разработки программных средств

Автоматизированная система создается на базе локальной вычислительной сети (ЛВС). В состав ЛВС входят рабочие станции программистов и сервер администратора [19]. Программисты имеют полный доступ только к информации своей ЭВМ и доступ к ЭВМ других программистов в режиме чтения. С рабочего места

администратора возможен доступ в режиме чтения к любой ЭВМ разработчиков.

База данных алгоритмов разрабатываемого программного средства находится на„сервере администратора и включает в себя архив утвержденных организацией-разработчиком и контролирующей организацией алгоритмов программного средства в виде блок-схем, описания на псевдокоде для их контроля администратором.

На сервере администратора располагается база данных листингов программ разрабатываемого программного средства, включающая в себя архив утвержденных организацией-разработчиком и контролирующей организацией программ для их контроля администратором с применением программ сравнения листингов и поиска измененных и добавленных участков программ.

На сервере администратора находится также база данных эталонных выполняемых модулей программ разрабатываемого программного средства для их контроля с применением программ поиска изменений в этих модулях.

Программы контроля версий листингов программ и сравнения выполняемых модулей должны быть разработаны организацией, не связанной ни с организацией-разработчиком, ни с контролирующей организацией и должны контролировать программы любого назначения.

Контроль за безопасностью разработки может осуществляться следующим образом.

Администратор в соответствии со своим графиком без уведомления разработчиков считывает в базы данных листинги программ и выполняемые модули. С помощью программ сравнения администратор выявляет и анализирует изменения, которые внесены разработчиком, по сравнению с последним контролем.

По мере разработки выполняемых модулей в базе администратора накапливаются готовые к сдаче заказчику эталонные образцы выполняемых модулей, сохранность которых контролируется администратором.

Применение такой организации работ позволяет администратору выявлять закладки и непреднамеренные ошибки на всех стадиях разработки программного средства. Администратор не мо-

жет сам внедрить закладку, так как у него нет права на модификацию программ, разрабатываемых программистами.

7.2.3. Контрольно-испытательный стенд

Одним из наиболее эффективных путей обнаружения закладок и ошибок в разрабатываемых программных средствах является создание комплексного контрольно-испытательного стенда разрабатываемой системы. Он позволяет анализировать программные средства путем подачи многократных входных воздействий на фоне изменяющихся внешних факторов, с помощью которых имитируется воздействие возможных закладок. Таким образом, контрольно-испытательный стенд может рассматриваться как детальная имитационная модель разрабатываемой системы, позволяющая обеспечить всесторонний анализ функционирования разрабатываемого программного средства в условиях воздействия закладок.

Контрольно-испытательный стенд должен отвечать следующим требованиям [19]:

1. Стенд строится как открытая система, допускающая модернизацию и наращивание возможностей.

2. Стенд должен обеспечивать адекватность структуры и информационных потоков структуре и информационным потокам реальной системы.

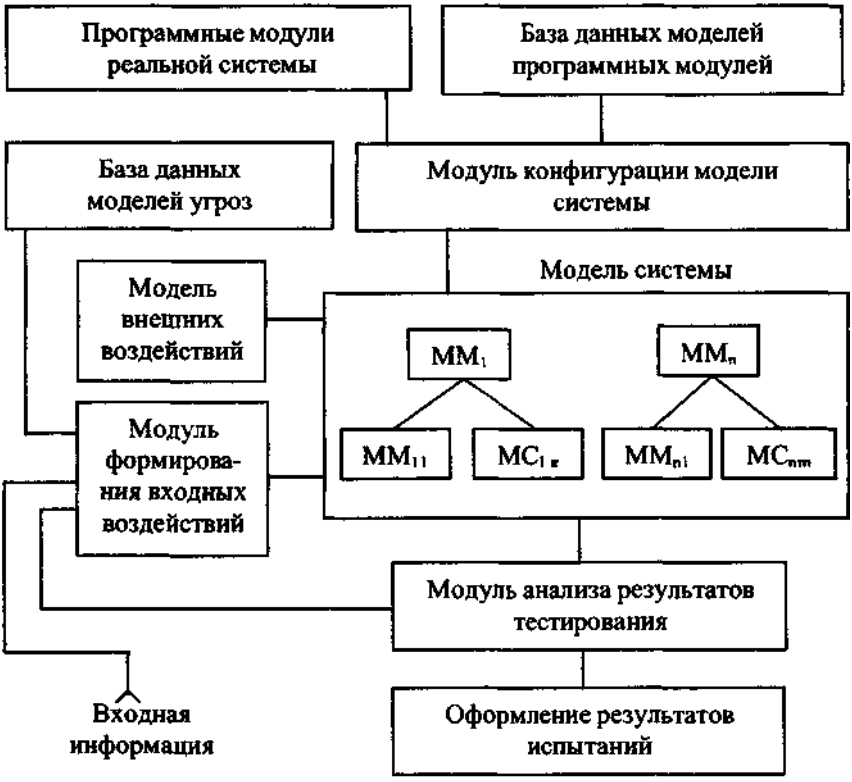
3. Необходимо поддерживать взаимозаменяемость программных модулей модели и реальной системы.

4. Стенд должен позволять проводить как автономные испытания модулей, так и всего программного средства в целом.

Контрольно-испытательный стенд может содержать следующие модули (рис. 11):

- модель системы, которая состоит из моделей программных модулей и программных модулей реальной системы;
- модуль конфигурации модели системы, осуществляющий регистрацию и динамическое включение программных модулей реальной системы и моделей программных модулей из соответствующих баз данных;
- база данных моделей угроз - для накопления и модификации моделей угроз, представленных в формализованном виде;

• модуль формирования входных воздействий, учитывающий возможные угрозы, ограничения на входную информацию и результаты тестирования на предыдущем шаге;



ММ — модель программного модуля; МС - программный модуль реальной системы.

Рис. 11. Структурная схема контрольно-испытательного стенда

• модель внешних воздействий, предназначенная для учета воздействий, внешних по отношению к моделируемой системе;

• модуль анализа результатов тестирования.

При разработке программных продуктов для обработки конфиденциальных данных готовые программы должны представляться на сертификацию в виде исходных программ на языках

высокого уровня и в виде выполняемого модуля. Наличие программы на языке высокого уровня значительно упрощает процесс контроля программы на отсутствие закладок. На этом уровне программирования применяются стандартные подходы к разработке конструкций языка, как правило, не используются особенности конкретных аппаратных средств, на которых выполняется программа. При наличии транслятора, проверенного на отсутствие ошибок и закладок, из проверенной программы на языке высокого уровня легко получается выполняемый модуль, который сравнивается с представленным разработчиком выполняемым модулем. Проверка программных средств осуществляется с помощью специальных программ, которые позволяют автоматизировать анализ на ошибки и закладки. Они контролируют отсутствие скрытых входов в блоки («люков»), отсутствие тупиковых ветвей алгоритмов, выдают информацию о наличии операторов, блоков, назначение которых программе неизвестно. Особое внимание уделяется участкам программ, написанных на языках более низкого уровня, а также попыткам выполнения действий в обход операционной системы (если это допускает система программирования). Окончательное решение принимается программистом после тщательного анализа информации, полученной специальной программой контроля.

Выполняемые модули программных средств проверяются в процессе сертификации на специальных аппаратно-программных стендах, способных имитировать функционирование испытываемого программного средства на допустимом множестве входных и внешних воздействий. При контроле выполняется операция, обратная транслированию - дизассемблирование. Для упрощения анализа выполняемых модулей применяются также отладчики, программы-трассировщики, которые позволяют проконтролировать последовательность событий, порядок выполнения команд.

7.3. Защита от внедрения аппаратных закладок на этапе разработки и производства

Аппаратные закладки могут внедряться не только в процессе разработки и модернизации, но и в процессе серийного производства, транспортирования и хранения аппаратных средств.

Для защиты от внедрения аппаратных закладок, кроме следования общим принципам защиты, необходимо обеспечить всестороннюю проверку комплектующих изделий, поступающих к разработчику (производителю) извне.

Комплектующие изделия должны подвергаться тщательному осмотру и испытанию на специальных стендах. Испытания, по возможности, проводятся путем подачи всех возможных входных сигналов во всех допустимых режимах.

Если полный перебор всех комбинаций входных сигналов практически невозможен, то используются вероятностные методы контроля. Чаще всего вероятностное тестирование осуществляется путем получения комбинаций входных сигналов с помощью датчика случайных чисел и подачей этих сигналов на тестируемое и контрольное изделие. В качестве контрольного используется такое же изделие, как и тестируемое, но проверенное на отсутствие закладок, ошибок и отказов. Выходные сигналы обоих изделий сравниваются. Если они не совпадают, то принимается решение о замене тестируемого изделия.

При испытаниях изделий путем подачи детерминированных последовательностей входных сигналов и сравнения выходных сигналов с эталонами, часто используются методы сжатия выходных сигналов (данных). Это позволяет сократить объем памяти, необходимый для размещения эталонов выходных сигналов.

Для исследования неразборных конструкций (микросхем, конденсаторов, резисторов, печатных плат и др.) используются рентгеновские установки. При необходимости осуществляется послойное рентгеновское исследование изделий.

В процессе производства основное внимание уделяется автоматизации технологических процессов и контролю за соблюдением технологической дисциплины. Особо ответственные операции могут производиться под наблюдением должностных лиц с последующим документальным оформлением.

Этапы разработки, производства и модернизации аппаратных средств КС завершаются контролем на наличие конструктивных ошибок, производственного брака и закладок.

Блоки и устройства, успешно прошедшие контроль, хранятся и транспортируются таким образом, чтобы исключалась возможность внедрения закладок.

7.4. Защита от несанкционированного изменения структур КС в процессе эксплуатации

7.4.1. Разграничение доступа к оборудованию

При эксплуатации КС неизменность аппаратной и программной структур обеспечивается за счет предотвращения несанкционированного доступа к аппаратным и программным средствам, а также организацией постоянного контроля за целостностью этих средств.

Несанкционированный доступ к аппаратным и программным средствам может быть исключен или существенно затруднен при выполнении следующего комплекса мероприятий:

- охрана помещений, в которых находятся аппаратные средства КС;
- разграничение доступа к оборудованию;
- противодействие несанкционированному подключению оборудования;
- защита внутреннего монтажа, средств управления и коммутации от несанкционированного вмешательства;
- противодействие внедрению вредительских программ.

Методы и средства охраны помещений рассмотрены в гл.5.

Под *доступом к оборудованию* понимается предоставление субъекту возможности выполнять определенные разрешенные ему действия с использованием указанного оборудования. Так, пользователю ЭВМ разрешается включать и выключать ЭВМ, работать с программами, вводить и выводить информацию. Обслуживающий персонал имеет право в установленном порядке тестировать ЭВМ, заменять и восстанавливать отказавшие блоки.

При организации доступа к оборудованию пользователей, операторов, администраторов выполняются следующие действия:

- идентификация и аутентификация субъекта доступа;
- разблокирование устройства;
- ведение журнала учета действий субъекта доступа.

Для идентификации субъекта доступа в КС чаще всего используются атрибутивные идентификаторы. Биометрическая идентификация проще всего осуществляется по ритму работы на

клавиатуре. Из **атрибутивных идентификаторов, как правило,** используются:

- пароли;
- съемные носители информации;
- электронные жетоны;
- пластиковые карты (см. гл.5);
- механические ключи.

Практически во всех КС, работающих с конфиденциальной информацией, аутентификация пользователей осуществляется с помощью паролей.

Паролем называют комбинацию символов (букв, цифр, специальных знаков), которая должна быть известна только владельцу пароля и, возможно, администратору системы безопасности.

После подачи питания на устройство пароль вводится субъектом доступа в систему с помощью штатной клавиатуры, пульта управления или специального наборного устройства, предназначенного только для ввода пароля. В КС, как правило, используется штатная клавиатура.

В современных операционных системах ПЭВМ заложена возможность использования пароля. Пароль хранится в специальной памяти, имеющей автономный источник питания. Сравнение паролей осуществляется до загрузки ОС. Защита считалась эффективной, если злоумышленник не имеет возможности отключить автономное питание памяти, в которой хранится пароль. Однако оказалось, что кроме пароля пользователя для загрузки ОС ПЭВМ можно использовать некоторые «технологические» пароли, перечень которых представлен в Internet [43].

В настоящее время разработаны средства защиты от несанкционированного доступа (НСД) к ПЭВМ, которые проверяют пароль до загрузки ОС. Для этого изменяются участки программ, осуществляющих загрузку ОС. Эти изменения позволяют прервать процесс загрузки до ввода правильного пароля.

При использовании паролей в момент загрузки ОС должно выполняться условие: в ЭВМ невозможно изменить установленный порядок загрузки ОС. Для этого жестко определяется ВЗУ, с которого осуществляется загрузка ОС. Желательно для этой цели использовать запоминающее устройство с несъемным носителем. Если загрузка ОС осуществляется со съемного носителя, то необ-

ходимо предусмотреть ряд дополнительных мер. Например, ВЗУ/ с которого осуществляется загрузка ОС, настраивается таким образом, что оно может работать только с определенными носителями. В ПЭВМ это может быть достигнуто изменением порядка форматирования магнитных дисков. Отключение на время загрузки ОС всех ВЗУ, кроме выделенного для загрузки, осуществляется настройками программ загрузки ОС.

Необходимо также обеспечить режим загрузки ОС, исключающий ее прерывание и возможное вмешательство злоумышленника в процесс загрузки. В ПЭВМ это может быть реализовано блокированием клавиатуры и «мыши» до полного завершения загрузки ОС.

Идентификация субъекта доступа осуществляется средствами защиты и при загруженной ОС. Такой режим парольной защиты используется для организации многопользовательской работы на ЭВМ.

При организации парольной защиты необходимо выполнять следующие рекомендации:

1. Пароль должен запоминаться субъектом доступа. Запись пароля значительно повышает вероятность его компрометации (нарушение конфиденциальности).

2. Длина пароля должна исключать возможность его раскрытия путем подбора. Рекомендуется устанавливать длину пароля $S > 9$ символов.

3. Пароли должны периодически меняться. Безопасное время использования пароля ($T_б$) может быть рассчитано по форму-1 ле [54]:

$$T_б = (A^s \cdot t)/2,$$

где t - время, необходимое на ввод слова длиной s; s - длина пачг роля; А - количество символов, из которых может быть составлен» пароль.

Время t определяется из соотношения: t=E/R,

где Е - число символов в сообщении, содержащем пароль; R - скорость передачи символов пароля (симв./мин.). Величина Е зависит от длины пароля и количества служебных символов.

В приведенной формуле расчета величины $T_б$ считается, что злоумышленник имеет возможность непрерывно осуществлять подбор пароля. Если предусмотрена задержка в несколько секунд

после неудачной попытки ввода пароля, то безопасное время значительно возрастает. Период смены пароля не должен превышать Тб- В любом случае использовать пароль свыше 1 года недопустимо.

4. В КС должны фиксироваться моменты времени успешного получения доступа и время неудачного ввода пароля. После трех ошибок подряд при вводе пароля устройство блокируется, и информация о предполагаемом факте подбора пароля поступает дежурному администратору системы безопасности.

5. Пароли должны храниться в КС таким образом, чтобы они были недоступны посторонним лицам. Этого можно достичь двумя способами:

- использовать для хранения паролей специальное запоминающее устройство, считанная информация из которого не попадает за пределы блока ЗУ (схема сравнения паролей находится в самом блоке). Запись в такое ЗУ осуществляется в специальном режиме;
- криптографическое преобразование пароля.

6. Пароль не выдается при вводе на экран монитора. Чтобы субъект доступа мог ориентироваться в количестве введенных символов на экран, взамен введенного выдается специальный символ (обычно звездочка).

7. Пароль должен легко запоминаться и в то же время быть сложным для отгадывания. Не рекомендуется использовать в качестве пароля имена, фамилии, даты рождения и т.п. Желательно при наборе пароля использование символов различных регистров, чередование букв, цифр, специальных символов. Очень эффективным является способ использования парадоксального сочетания слов («книга висит», «плот летит» и т.п.) и набора русских букв пароля на латинском регистре. В результате получается бессмысленный набор букв латинского алфавита.

В качестве идентификатора во многих КС используется *съемный носитель информации,* на котором записан идентификационный код субъекта доступа. В ПЭВМ для этой цели используется гибкий магнитный диск. Такой идентификатор обладает рядом достоинств:

- не требуется использовать дополнительные аппаратные средства;

• кроме идентификационного кода, на носителе может храниться другая информация, используемая для аутентификации, контроля целостности информации, атрибуты шифрования и т. д.

Для идентификации пользователей широко используются электронные *жетоны-генераторы* случайных идентификационных кодов [18]. Жетон - это прибор, вырабатывающий псевдослучайную буквенно-цифровую последовательность (слово). Это слово меняется примерно раз в минуту синхронно со сменой такого же слова в КС. В результате вырабатывается одноразовый пароль, который годится для использования только в определенный промежуток времени и только для однократного входа в систему. Первый такой жетон SecurlD американской фирмы Security Dynamics появился в 1987 году.

Жетон другого типа внешне напоминает калькулятор. В процессе аутентификации КС выдает на монитор пользователя цифровую последовательность запроса, пользователь набирает ее на клавиатуре жетона. Жетон формирует ответную последовательность, которую пользователь считывает с индикатора жетона и вводит в КС. В результате опять получается одноразовый неповторяющийся пароль. Без жетона войти в систему оказывается невозможным. Вдобавок ко всему, прежде чем воспользоваться жетоном, нужно ввести в него свой личный пароль.

Атрибутивные идентификаторы (кроме паролей) могут использоваться только на момент доступа и регистрации, или постоянно должны быть подключены к устройству считывания до окончания работы. На время даже кратковременного отсутствия идентификатор изымается, и доступ к устройству блокируется. Такие аппаратно-программные устройства способны решать задачи не только разграничения доступа к устройствам, но и обеспечивают защиту от НСДИ. Принцип действия таких устройств основан на расширении функций ОС на аппаратном уровне.

Процесс аутентификации может включать также диалог субъекта доступа с КС. Субъекту доступа задаются вопросы, ответы на которые анализируются, и делается окончательное заключение о подлинности субъекта доступа.

В качестве простого идентификатора часто используют *механические ключи.* Механический замок может быть совмещен с блоком подачи питания на устройство. На замок может закры-

ваться крышка, под которой находятся основные органы управления устройством. Без вскрытия крышки невозможна работа с устройством. Наличие такого замка является дополнительным препятствием на пути злоумышленника при попытке осуществить НСД к устройству.

Доступ к устройствам КС объекта может блокироваться дистанционно. Так в ЛВС подключение к сети рабочей станции может блокироваться с рабочего места администратора. Управлять доступом к устройствам можно и с помощью такого простого, но эффективного способа, как отключение питания. В нерабочее время питание может отключаться с помощью коммутационных устройств, контролируемых охраной.

Комплекс мер и средств управления доступом к устройствам должен выполнять и функцию автоматической регистрации действий субъекта доступа. Журнал регистрации событий может вестись как на автономной ЭВМ, так и в сети. Периодически или при фиксации нарушений протоколов доступа, администратор просматривает журнал регистрации с целью контроля действий субъектов доступа.

Организация доступа обслуживающего персонала к устройствам отличается от организации доступа пользователей. Прежде всего, по возможности, устройство освобождается от конфиденциальной информации и осуществляется отключение информационных связей. Техническое обслуживание и восстановление работоспособности устройств выполняются под контролем должностных лиц. Особое внимание обращается на работы, связанные с доступом к внутреннему монтажу и заменой блоков.

7.4.2. Противодействие несанкционированному подключению устройств

Одним из возможных путей несанкционированного изменения технической структуры КС является подключение незарегистрированных устройств или замена ими штатных средств КС.

Для парирования такой угрозы используются следующие методы:

- проверка особенностей устройства;
- использование идентификаторов устройств.

В запоминающих устройствах КС, как правило, содержится информация о конфигурации системы. К такой информации относятся: типы устройств (блоков) и их характеристики, количество и особенности подключения внешних устройств, режимы работы и другая информация. Конкретный состав особенностей конфигурации определяется типом КС и ОС. В любом случае, с помощью программных средств может быть организован сбор и сравнение информации о конфигурации КС. Если ЭВМ работает в сети, то, по крайней мере, при подключении к сети осуществляется контроль конфигурации ЭВМ.

Еще более надежным и оперативным методом контроля является использование специального кода-идентификатора устройства. Этот код может генерироваться аппаратными средствами, а может храниться в ЗУ. Генератор может инициировать выдачу в контролирующее устройство (в вычислительной сети это может быть рабочее место администратора) уникального номера устройства. Код из ЗУ может периодически считываться и анализироваться средствами администратора КС. Комплексное использование методов анализа особенностей конфигурации и использование идентификаторов устройств значительно повышают вероятность обнаружения попыток несанкционированного подключения или подмены.

*7.4.3. **Защита** внутреннего **монтажа,** средств **управления и коммутации от несанкционированного вмешательства***

Для защиты от несанкционированных действий по изменению монтажа, замене элементов, переключению коммутирующих устройств необходимо выполнить условия:

- доступ к внутреннему монтажу, к органам управления и коммутации устройств блокируется имеющими замок дверями, крышками, защитными экранами и т. п.;
- наличие автоматизированного контроля вскрытия аппаратуры.

Создание физических препятствий на пути злоумышленника должно предусматриваться на этапе проектирования. Эти конструкции не должны создавать существенных неудобств при эксплуатации устройств.

Например, крышки и защитные экраны, защищающие наборные устройства, тумблеры, переключатели и т. п. желательно изготавливать из прозрачного и прочного материала, позволяющего контролировать состояние органов управления без снятия (открывания) защитных конструкций.

Контроль вскрытия аппаратуры обеспечивается за счет использования несложных электрических схем, аналогичных системам охранной сигнализации. Контроль вскрытия обеспечивается путем использования датчиков контактного типа. Они устанавливаются на всех съемных и открывающихся конструкциях, через которые возможен доступ к внутреннему монтажу устройств, элементам управления и коммутации. Датчики объединяются в единую систему контроля вскрытия устройств (СКВУ) с помощью проводных линий. Известно множество вариантов объединения датчиков в систему [28]. При построении таких систем решаются две взаимосвязанные задачи: обеспечение максимальной информативности системы и минимизация числа проводных линий. Максимум информативности автоматизированной СКВУ достигается в системах, позволяющих определить факт вскрытия конкретной защитной конструкции на определенном устройстве. Однако во многих случаях достаточно получить дежурному администратору системы безопасности сигнал о вскрытии устройства, чтобы принять адекватные меры. Конкретное нарушение внешней целостности устройства определяется на месте. Этому может способствовать контроль целостности специальных защитных знаков на защитных конструкциях [12]. Специальные защитные знаки реализуются в виде материалов, веществ, самоклеющихся лент, наклеек, самоклеющихся пломб. Целостность специальных защитных знаков определяется по внешнему виду и определенным признакам, которые могут контролироваться с применением технических средств. Специальные защитные средства на защитных конструкциях служат дополнительным индикатором вскрытия. Периодический контроль целостности специальных защитных средств позволяет (хотя бы с некоторым опозданием) выявить нарушение внешней целостности устройства при отсутствии или обходе злоумышленником аппаратных средств СКВУ.

Если разрешающая способность СКВУ ограничивается устройством, то существенно сокращается число проводных линий.

В этом случае датчики с нормально замкнутыми контактами всех защитных конструкций устройства соединяются последовательно.

По возможности проводные линии СКВУ желательно маскировать под линии информационных трактов устройств.

Факт снятия разъема может быть легко зафиксирован. Для этого достаточно выделить один контакт разъема на цели контроля. При снятии разъема линия СКВУ разрывается.

7.4.4. Контроль целостности программной структуры в процессе эксплуатации

Контроль целостности программ и данных выполняется одними и теми же методами. Исполняемые программы изменяются крайне редко на этапе их эксплуатации. Существует достаточно широкий класс программ, для которых все исходные данные или их часть также изменяются редко. Поэтому контроль целостности таких файлов выполняется так же, как и контроль программ.

Контроль целостности программных средств и данных осуществляется путем получения (вычисления) характеристик и сравнения их с контрольными характеристиками. Контрольные характеристики вычисляются при каждом изменении соответствующего файла. Характеристики вычисляются по определенным алгоритмам. Наиболее простым алгоритмом является ***контрольное суммирование.*** Контролируемый файл в двоичном виде разбивается на слова, обычно состоящие из четного числа байт. Все двоичные слова поразрядно суммируются с накоплением по mod2, образуя в результате контрольную сумму. Разрядность контрольной суммы равняется разрядности двоичного слова. Алгоритм получения контрольной суммы может отличаться от приведенного, но, как правило, не является сложным и может быть получен по имеющейся контрольной сумме и соответствующему файлу.

Другой подход к получению характеристик целостности связан с использованием ***циклических*** *кодов* [63]. Суть метода состоит в следующем. Исходная двоичная последовательность представляется в виде полинома F(x) степени п-1, где п - число бит последовательности. Для выбранного порождающего полинома P(x) можно записать равенство:

$$F(x) \cdot x^m = G(x) \cdot P(x) \oplus R(x),$$

где m - степень порождающего полинома, G(x) - частное, а R(x) - остаток от деления $F(x) \cdot x^m$ на P(x).

Из приведенного соотношения можно получить новое выражение:

$$F(x) \cdot x^m \oplus R(x) = G(x) \cdot P(x)$$

Из последнего выражения можно сделать вывод: если исходный полином увеличить на x^m (сдвинуть в сторону старших разрядов на m разрядов) и сложить с остатком R(x) по модулю 2, то полученный многочлен разделится без остатка на порождающий полином P(x).

При контроле целостности информации контролируемая последовательность (сектор на диске, файл и т. д.), сдвинутая на m разрядов, делится на выбранный порождающий полином, и запоминается полученный остаток, который называют синдромом. Синдром хранится как эталон. При контроле целостности к полиному контролируемой последовательности добавляется синдром и осуществляется деление на порождающий полином. Если остаток от деления равен нулю, то считается, что целостность контролируемой последовательности не нарушена. Обнаруживающая способность метода зависит от степени порождающего полинома и не зависит от длины контролируемой последовательности. Чем выше степень полинома, тем выше вероятность определения изменений d, которая определяется из соотношения: $d = 1/2^m$.

Использование контрольных сумм и циклических кодов, как и других подобных методов, имеет существенный недостаток. Алгоритм получения контрольных характеристик хорошо известен, и поэтому злоумышленник может произвести изменения таким образом, чтобы контрольная характеристика не изменилась (например, добавив коды).

Задача злоумышленника усложнится, если использовать переменную длину двоичной последовательности при подсчете контрольной характеристики, а характеристику хранить в зашифрованном виде или вне КС (например, в ЗУ Touch Memory).

Рассмотрим пример использования циклических кодов для контроля целостности двоичной последовательности.

Пусть требуется проконтролировать целостность двоичной последовательности A=1010010. Используется порождаемый полином вида: $P(x)=x^3+x+1$.

А. Получение контрольной характеристики.

$G_A(x) = 1 \cdot x^6 + 0 \cdot x^5 + 1 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x^1 + 0 \cdot x^0 = x^6 + x^4 + x.$

$G_A(x) \cdot x^3 = x^9 + x^7 + x^4.$

При вычислении синдрома RA(X) действия выполняются по правилам деления полиномов, заменяя операцию вычитания операцией сложения по модулю:

$$
\begin{array}{ll}
 & x^9 + x^7 + x^4 \quad \big| \; x^3 + x + 1 \\
\oplus & \underline{x^9 + x^7 + x^6} \qquad\qquad\quad x^6 + x^3 + 1 \\
 & x^6 + x^4 \\
\oplus & \underline{x^6 + x^4 + x^3} \\
 & x^3 \\
\oplus & \underline{x^3 + x + 1} \\
 & x + 1 \qquad \text{— остаток } R_A(x)
\end{array}
$$

$F_A(x) = G_A(x) \cdot x^3 \oplus R_A(x) = x^9 + x^7 + x^4 + x + 1.$

Двоичная последовательность с синдромом имеет вид :

A' = 1010010011 (синдром подчеркнут). Последовательность A' хранится и(или) передается в КС.

Б. Контроль целостности информации.

Если изменений последовательности A' = 1010010011 не произошло, то соответствующий ей полином должен разделиться на порождающий полином без остатка:

$$
\begin{array}{ll}
 & x^9 + x^7 + x^3 + x + 1 \quad \big| \; x^3 + x + 1 \\
\oplus & \underline{x^9 + x^7 + x^6} \qquad\qquad\quad x^6 + x^3 + 1 \\
 & x^6 + x^4 + x + 1 \\
\oplus & \underline{x^6 + x^4 + x^3} \\
 & x^3 + x + 1 \\
\oplus & \underline{x^3 + x + 1} \\
 & 0 \qquad \text{– остаток } R_A(x)
\end{array}
$$

Результат произведенных вычислений свидетельствует о целостности информации.

Если синдром отличен от нуля, то это означает, что произошла ошибка при хранении (передаче) двоичной последовательности. Ошибка определяется и в контрольных разрядах (в синдроме).

Существует метод, который позволяет практически исключить возможность неконтролируемого изменения информации в КС. Для этого необходимо использовать хэш-функцию. Под *хэш-функцией* понимается процедура получения контрольной характеристики двоичной последовательности, основанная на контрольном суммировании и криптографических преобразованиях. Алгоритм хэш-функции приведен в ГОСТ Р34.11-94. Алгоритм не является секретным, так же как и алгоритм используемого при получении хэш-функции криптографического преобразования, изложенного в ГОСТ 28147-89 [9].

Исходными данными для вычисления хэш-функции являются исходная двоичная последовательность и стартовый вектор хэширования. Стартовый вектор хэширования представляет собой двоичную последовательность длиной 256 бит. Он должен быть недоступен злоумышленнику. Вектор либо подвергается зашифрованию, либо хранится вне КС.

Итерационный процесс вычисления хэш-функции H предусматривает:

- генерацию четырех ключей (слов длиной 256 бит);
- шифрующее преобразование с помощью ключей текущего значения H методом простой замены (ГОСТ 28147-89);
- перемешивание результатов;
- поразрядное суммирование по mod2 слов длиной 256 бит исходной последовательности;
- вычисление функции H.

В результате получается хэш-функция длиной 256 бит. Значение хэш-функции можно хранить вместе с контролируемой информацией, т. к., не имея стартового вектора хэширования, злоумышленник не может получить новую правильную функцию хэширования после внесения изменений в исходную последовательность. А получить стартовый вектор по функции хэширования практически невозможно.

Для каждой двоичной последовательности используются две контрольные характеристики: стартовый вектор и хэш-функция. При контроле по стартовому вектору и контролируемой последо-

вательности вычисляется **значение хэш-функции** и **сравнивается с** контрольным значением.

Контрольные вопросы

1. Назовите основные принципы разработки алгоритмов, программ и технических средств.
2. В чем заключается суть современных технологий программирования?
3. Дайте характеристику автоматизированной системы разработки программных средств.
4. Каким образом достигается защита от несанкционированного изменения структур КС на этапах разработки и эксплуатации?
5. Как осуществляется контроль целостности информации?

ГЛАВА 8
Защита информации в КС от несанкционированного доступа

Для осуществления НСДИ злоумышленник не применяет никаких аппаратных или программных средств, не входящих в состав КС. Он осуществляет НСДИ, используя:

- знания о КС и умения работать с ней;
- сведения о системе защиты информации;
- сбои, отказы технических и программных средств;
- ошибки, небрежность обслуживающего персонала и пользователей.

Для защиты информации от НСД создается система разграничения доступа к информации. Получить несанкционированный доступ к информации при наличии системы разграничения доступа (СРД) возможно только при сбоях и отказах КС, а также используя слабые места в комплексной системе защиты информации. Чтобы использовать слабости в системе защиты, злоумышленник должен знать о них.

Одним из путей добывания информации о недостатках систе-

мы защиты является изучение механизмов защиты. Злоумышленник может тестировать систему защиты путем непосредственного контакта с ней. В этом случае велика вероятность обнаружения системой защиты попыток ее тестирования. В результате этого службой безопасности могут быть предприняты дополнительные меры защиты.

Гораздо более привлекательным для злоумышленника является другой подход. Сначала получается копия программного средства системы защиты или техническое средство защиты, а затем производится их исследование в лабораторных условиях. Кроме того, создание неучтенных копий на съемных носителях информации является одним из распространенных и удобных способов хищения информации. Этим способом осуществляется несанкционированное тиражирование программ. Скрытно получить техническое средство защиты для исследования гораздо сложнее, чем программное, и такая угроза блокируется средствами и методами обеспечивающими целостность технической структуры КС.

Для блокирования несанкционированного исследования и копирования информации КС используется комплекс средств и мер защиты, которые объединяются в систему защиты от исследования и копирования информации (СЗИК).

Таким образом, СРД и СЗИК могут рассматриваться как подсистемы системы защиты от НСДИ.

8.1. Система разграничения доступа к информации в КС

8.1.1. Управление доступом

Исходной информацией для создания СРД является решение владельца (администратора) КС о допуске пользователей к определенным информационным ресурсам КС. Так как информация в КС хранится, обрабатывается и передается файлами (частями файлов), то доступ к информации регламентируется на уровне файлов (объектов доступа). Сложнее организуется доступ в базах данных, в которых он может регламентироваться к отдельным ее частям по определенным правилам. При определении полномочий доступа администратор устанавливает операции, которые разрешено выполнять пользователю (субъекту доступа).

Различают следующие **операции** с **файлами):**

- чтение (R);
- запись;
- выполнение программ (E).

Операция записи в файл имеет две модификации. Субъекту доступа может быть дано право осуществлять запись с изменением содержимого файла (W). Другая организация доступа предполагает разрешение только дописывания в файл, без изменения старого содержимого (A).

В КС нашли применение два подхода к организации разграничения доступа [6]:

- матричный:
- полномочный (мандатный).

Матричное управление доступом предполагает использование матриц доступа. Матрица доступа представляет собой таблицу, в которой объекту доступа соответствует столбец Oj, а субъекту доступа - строка Si. На пересечении столбцов и строк записываются операция или операции, которые допускается выполнять субъекту доступа i с объектом доступа] (рис. 12).

	O_1	O_2	...	O_j	...	O_m
S_1	R	R,W		E		R
S_2	R,A	–		R		E
...						
S_i	R	–		–		R
...						
S_n	R,W	–		E		E

Рис. 12. Матрицадоступа

Матричное управление доступом позволяет с максимальной детализацией установить права субъекта доступа по выполнению разрешенных операций над объектами доступа. Такой подход нагляден и легко реализуем. Однако в реальных системах из-за

большого количества субъектов и объектов доступа матрица доступа достигает таких размеров, при которых сложно поддерживать ее в адекватном состоянии.

Полномочный или *мандатный* метод базируется на многоуровневой модели защиты. Такой подход построен по аналогии с «ручным» конфиденциальным (секретным) делопроизводством. Документу присваивается уровень конфиденциальности (гриф секретности), а также могут присваиваться метки, отражающие категории конфиденциальности (секретности) документа. Таким образом, конфиденциальный документ имеет гриф конфиденциальности (конфиденциально, строго конфиденциально, секретно, совершенно секретно и т. д.) и может иметь одну или несколько меток, которые уточняют категории лиц, допущенных к этому документу («для руководящего состава», «для инженерно-технического состава» и т. д.). Субъектам доступа устанавливается уровень допуска, определяющего максимальный для данного субъекта уровень конфиденциальности документа, к которому разрешается допуск. Субъекту доступа устанавливаются также категории, которые связаны с метками документа.

Правило разграничения доступа заключается в следующем: лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа равен или выше уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, содержатся все категории, определенные для данного документа.

В КС все права субъекта доступа фиксируются в его мандате. Объекты доступа содержат метки, в которых записаны признаки конфиденциальности. Права доступа каждого субъекта и характеристики конфиденциальности каждого объекта отображаются в виде совокупности уровня конфиденциальности и набора категорий конфиденциальности.

Мандатное управление позволяет упростить процесс регулирования доступа, так как при создании нового объекта достаточно создать его метку. Однако при таком управлении приходится завышать конфиденциальность информации из-за невозможности детального разграничения доступа.

Если право установления правил доступа к объекту предоставляется владельцу объекта (или его доверенному лицу), то та-

кой метод контроля доступа к информации называется *дискреционным*.

8.1.2. Состав системы разграничения доступа

Система разграничения доступа к информации должна содержать четыре функциональных блока:

- блок идентификации и аутентификации субъектов доступа;
- диспетчер доступа;
- блок криптографического преобразования информации при ее хранении и передаче;
- блок очистки памяти.

Идентификация и аутентификация субъектов осуществляется в момент их доступа к устройствам, в том числе и дистанционного доступа.

Диспетчер доступа реализуется в виде аппаратно-программных механизмов (рис.13) и обеспечивает необходимую дисциплину разграничения доступа субъектов к объектам доступа (в том числе и к аппаратным блокам, узлам, устройствам). Диспетчер доступа разграничивает доступ к внутренним ресурсам КС субъектов, уже получивших доступ к этим системам. Необходимость использования диспетчера доступа возникает только в многопользовательских КС.

Запрос на доступ i-го субъекта и j-му объекту поступает в блок управления базой полномочий и характеристик доступа и в блок регистрации событий. Полномочия субъекта и характеристики объекта доступа анализируются в блоке принятия решения, который выдает сигнал разрешения выполнения запроса, либо сигнал отказа в допуске. Если число попыток субъекта допуска получить доступ к запрещенным для него объектам превысит определенную границу (обычно 3 раза), то блок принятия решения на основании данных блока регистрации выдает сигнал «НСДИ» администратору системы безопасности. Администратор может блокировать работу субъекта, нарушающего правила доступа в системе, и выяснить причину нарушений. Кроме преднамеренных попыток НСДИ диспетчер фиксирует нарушения правил разграничения, явившихся следствием отказов, сбоев аппаратных и программных

средств, а также вызванных ошибками персонала **и пользователей.**

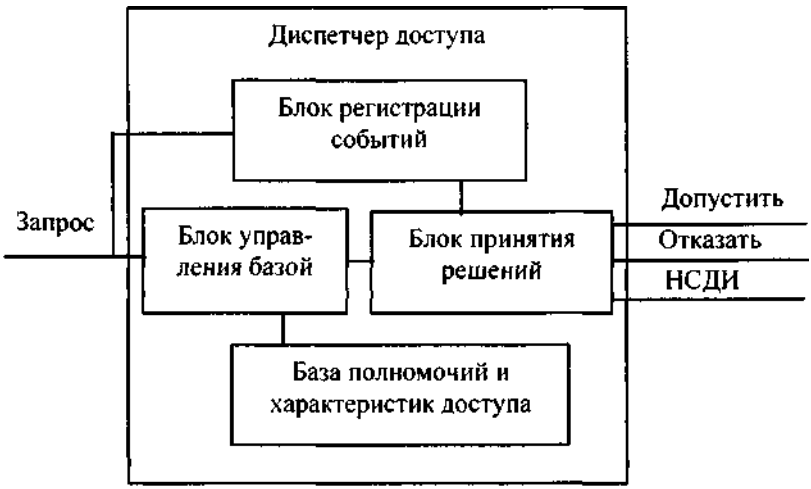


Рис. 13 Диспетчер доступа

Следует отметить, что в распределенных КС криптографическое закрытие информации является единственным надежным способом защиты от НСДИ. Сущность криптографического закрытия информации изложена в главе 9.

В СРД должна быть реализована функция очистки оперативной памяти и рабочих областей на внешних запоминающих устройствах после завершения выполнения программы, обрабатывающей конфиденциальные данные. Причем очистка должна производиться путем записи в освободившиеся участки памяти определенной последовательности двоичных кодов, а не удалением только учетной информации о файлах из таблиц ОС, как это делается **при** стандартном удалении средствами ОС.

8.1.3. Концепция построения систем разграничения доступа

В основе построения СРД лежит концепция разработки защищенной универсальной ОС на базе ядра безопасности [6]. Под **ядром безопасности** понимают локализованную, минимизированную, четко ограниченную и надежно изолированную совокуп-

ность программно-аппаратных механизмов, доказательно правильно реализующих функции диспетчера доступа [29]. Правильность функционирования ядра безопасности доказывается путем полной формальной верификации его программ и пошаговым доказательством их соответствия выбранной математической модели защиты.

Применение ядра безопасности требует провести изменения ОС и архитектуры ЭВМ. Ограничение размеров и сложности ядра необходимо для обеспечения его верифицируемости.

Для аппаратной поддержки защиты и изоляции ядра в архитектуре ЭВМ должны быть предусмотрены:

- многоуровневый режим выполнения команд;
- использование ключей защиты и сегментирование памяти;
- реализация механизма виртуальной памяти с разделением адресных пространств;
- аппаратная реализация части функций ОС;
- хранение программ ядра в постоянном запоминающем устройстве (ПЗУ);
- использование новых архитектур ЭВМ, отличных от фоннеймановской архитектуры (архитектуры с реализацией абстрактных типов данных, теговые архитектуры с привилегиями и др.).

Обеспечение многоуровневого режима выполнения команд является главным условием создания ядра безопасности. Таких уровней должно быть не менее двух. Часть машинных команд ЭВМ должна выполняться только в режиме работы ОС. Основной проблемой создания высокоэффективной защиты от НСД является предотвращение несанкционированного перехода пользовательских процессов в привилегированное состояние. Для современных сложных ОС практически нет доказательств отсутствия возможности несанкционированного получения пользовательскими программами статуса программ ОС.

Использование ключей защиты, сегментирование памяти и применение механизма виртуальной памяти предусматривает аппаратную поддержку концепции изоляции областей памяти при работе ЭВМ в мультипрограммных режимах. Эти механизмы служат основой для организации работы ЭВМ в режиме виртуальных машин. Режим виртуальных машин позволяет создать наибольшую изолированность пользователей, допуская использо-

вание даже различных ОС пользователями в режиме разделения времени.

Аппаратная реализация наиболее ответственных функций ОС и хранение программ ядра в ПЗУ существенно повышают изолированность ядра, его устойчивость к попыткам модификации. Аппаратно должны быть реализованы прежде всего функции идентификации и аутентификации субъектов доступа, хранения атрибутов системы защиты, поддержки криптографического закрытия информации, обработки сбоев и отказов и некоторые другие.

Универсальные ЭВМ и их ОС, используемые ранее, практически не имели встроенных механизмов защиты от НСД. Такие распространенные ОС как IBM System/370, MS-DOS и целый ряд других ОС не имели встроенных средств идентификации и аутентификации и разграничения доступа. Более современные универсальные ОС UNIX, VAX/VMS, Solaris и др. имеют встроенные механизмы разграничения доступа и аутентификации. Однако возможности этих встроенных функций ограничены и не могут удовлетворять требованиям, предъявляемым к защищенным ЭВМ.

Имеется два пути получения защищенных от НСД КС:

- создание специализированных КС;
- оснащение универсальных КС дополнительными средствами защиты.

Первый путь построения защищенных КС пока еще не получил широкого распространения в связи с нерешенностью целого ряда проблем. Основной из них является отсутствие эффективных методов разработки доказательно корректных аппаратных и программных средств сложных систем. Среди немногих примеров специализированных ЭВМ можно назвать систему SCOMP фирмы «Honeywell», предназначенную для использования в центрах коммутации вычислительных сетей, обрабатывающих секретную информацию. Система разработана на базе концепции ядра безопасности. Узкая специализация позволила создать защищенную систему, обеспечивающую требуемую эффективность функционирования по прямому назначению.

Чаще всего защита КС от НСД осуществляется путем использования дополнительных программных или аппаратно-программных средств. Программные средства RACF, SECURC,

TOPSECRET и другие использовались для защиты ЭВМ типа IBM-370.

В настоящее время появились десятки отдельных программ, программных и аппаратных комплексов, рассчитанных на защиту персональных ЭВМ от несанкционированного доступа к ЭВМ, которые разграничивают доступ к информации и устройствам ПЭВМ.

8.1.4. Современные системы защиты ПЭВМ от несанкционированного доступа к информации

В качестве примеров отдельных программ, повышающих защищенность КС от НСД, можно привести утилиты из пакета Norton Utilities, такие как программа шифрования информации при записи на диск Diskreet или Secret disk, программа стирания информации с диска WipeInfo, программа контроля обращения к дискам Disk Monitor и др. [32].

Отечественными разработчиками предлагаются программные системы защиты ПЭВМ «Снег-1.0», «Кобра», «Страж-1.1» и др. В качестве примеров отечественных аппаратно-программных средств защиты, имеющих сертификат Гостехкомиссии, можно привести системы «Аккорд-4», «DALLAS LOCK 3.1», «Редут», «ДИЗ-1». Аппаратно-программные комплексы защиты реализуют максимальное число защитных механизмов:

- идентификация и аутентификация пользователей;
- разграничение доступа к файлам, каталогам, дискам;
- контроль целостности программных средств и информации;
- возможность создания функционально замкнутой среды пользователя;
- защита процесса загрузки ОС;
- блокировка ПЭВМ на время отсутствия пользователя;
- криптографическое преобразование информации;
- регистрация событий;
- очистка памяти.

Программные системы защиты в качестве идентификатора используют, как правило, только пароль. Пароль может быть пере-

хвачен резидентными программами двух видов. Программы первого вида перехватывают прерывания от клавиатуры, записывают символы в специальный файл, а затем передают управление ОС. После перехвата установленного числа символов программа удаляется из ОП. Программы другого вида выполняются вместо штатных программ считывания пароля. Такие программы первыми получают управление и имитируют для пользователя работу со штатной программой проверки пароля. Они запоминают пароль, имитируют ошибку ввода пароля и передают управление штатной программе парольной идентификации. Отказ при первом наборе пароля пользователь воспринимает как сбой системы или свою ошибку и осуществляет повторный набор пароля, который должен завершиться допуском его к работе. При перехвате пароля в обоих случаях пользователь не почувствует, что его пароль скомпрометирован. Для получения возможности перехвата паролей злоумышленник должен изменить программную структуру системы. В некоторых программных системах защиты («Страж-1.1») для повышения достоверности аутентификации используются съемные магнитные диски, на которых записывается идентификатор пользователя.

Значительно сложнее обойти блок идентификации и аутентификации в аппаратно-программных системах защиты от НСД. В таких системах используются электронные идентификаторы, чаще всего - Touch Memory.

Для каждого пользователя устанавливаются его полномочия в отношении файлов, каталогов, логических дисков. Элементы, в отношении которых пользователю запрещены любые действия, становятся «невидимыми» для него, т. е. они не отображаются на экране монитора при просмотре содержимого внешних запоминающих устройств.

Для пользователей может устанавливаться запрет на использование таких устройств, как накопители на съемных носителях, печатающие устройства. Эти ограничения позволяют предотвращать-реализацию угроз, связанных с попытками несанкционированного копирования и ввода информации, изучения системы защиты.

В наиболее совершенных системах реализован механизм контроля целостности файлов с использованием хэш-функции При-

чем существуют системы, в которых контрольная характеристика хранится не только в ПЭВМ, но и в автономном ПЗУ пользователя. Постоянное запоминающее устройство, как правило, входит в состав карты или жетона, используемого для идентификации пользователя. Так в системе «Аккорд-4» хэш-функции вычисляются для контролируемых файлов и хранятся в специальном файле в ПЭВМ, а хэш-функция, вычисляемая для специального файла, хранится в Touch Memory.

После завершения работы на ПЭВМ осуществляется запись контрольных характеристик файлов на карту или жетон пользователя. При входе в систему осуществляется считывание контрольных характеристик из ПЗУ карты или жетона и сравнение их с характеристиками, вычисленными по контролируемым файлам. Для того, чтобы изменение файлов осталось незамеченным, злоумышленнику необходимо изменить контрольные характеристики как в ПЭВМ, так и на карте или жетоне, что практически невозможно при условии выполнения пользователем простых правил.

Очень эффективным механизмом борьбы с НСДИ является создание функционально-замкнутых сред пользователей. Суть его состоит в следующем. Для каждого пользователя создается меню, в которое попадает пользователь после загрузки ОС. В нем указываются программы, к выполнению которых допущен пользователь. Пользователь может выполнить любую из программ из меню. После выполнения программы пользователь снова попадает в меню. Если эти программы не имеют возможностей инициировать выполнение других программ, а также предусмотрена корректная обработка ошибок, сбоев и отказов, то пользователь не сможет выйти за рамки установленной замкнутой функциональной среды. Такой режим работы вполне осуществим во многих АСУ.

Защита процесса загрузки ОС предполагает осуществление загрузки именно штатной ОС и исключение вмешательства в ее структуру на этапе загрузки. Для обеспечения такой защиты на аппаратном или программном уровне блокируется работа всех ВЗУ, за исключением того, на котором установлен носитель со штатной ОС. Если загрузка осуществляется со съемных носителей информации, то до начала загрузки необходимо удостовериться в том, что установлен носитель со штатной ОС. Такой контроль может быть осуществлен программой, записанной в ПЗУ ЭВМ.

Способы контроля могут быть разными: от контроля идентификатора до сравнения хэш-функций. Загрузка с несъемного носителя информации все же является предпочтительнее.

Процесс загрузки ОС должен исключать возможность вмешательства до полного завершения загрузки, пока не будут работать все механизмы системы защиты. В КС достаточно блокировать на время загрузки ОС все устройства ввода информации и каналы связи.

При организации многопользовательского режима часто возникает необходимость на непродолжительное время отлучиться от рабочего места, либо передать ЭВМ другому пользователю. На это время необходимо блокировать работу ЭВМ. В этих случаях очень удобно использовать электронные идентификаторы, которые при работе должны постоянно находиться в приемном устройстве блока идентификации ЭВМ. При изъятии идентификатора гасится экран монитора и блокируются устройства управления. При предъявлении идентификатора, который использовался при доступе к ЭВМ, осуществляется разблокировка, и работа может быть продолжена. При смене пользователей целесообразно производить ее без выключения ЭВМ. Для этого необходим аппаратно-программный или программный механизм корректной смены полномочий. Если предыдущий пользователь корректно завершил работу, то новый пользователь получает доступ со своими полномочиями после успешного завершения процедуры аутентификации.

Одним из наиболее эффективных методов разграничения доступа является криптографическое преобразование информации. Этот метод является универсальным. Он защищает информацию от изучения, внедрения программных закладок, делает операцию копирования бессмысленной. Поэтому криптографические методы защиты информации рассматриваются довольно подробно в гл. 9. Здесь необходимо лишь отметить, что пользователи могут использовать одни и те же аппаратно-программные или программные средства криптографического преобразования или применять индивидуальные средства.

Для своевременного пресечения несанкционированных действий в отношении информации, а также для контроля за соблюдением установленных правил субъектами доступа, необходимо

обеспечить регистрацию событий, связанных с защитой информации. Степень подробности фиксируемой информации может изменяться и обычно определяется администратором системы защиты. Информация накапливается на ВЗУ. Доступ к ней имеет только администратор системы защиты.

Важно обеспечивать стирание информации в ОП и в рабочих областях ВЗУ. В ОП размещается вся обрабатываемая информация, причем, в открытом виде. Если после завершения работы пользователя не осуществить очистку рабочих областей памяти всех уровней, то к ней может быть осуществлен несанкционированный доступ.

8.2. Система защиты программных средств от копирования и исследования

8.2.1. Методы, затрудняющие считывание скопированной информации

Создание копий программных средств для изучения или несанкционированного использования осуществляется с помощью устройств вывода или каналов связи.

Одним из самых распространенных каналов несанкционированного копирования является использование накопителей на съемных магнитных носителях. Угроза несанкционированного копирования информации блокируется методами, которые могут быть распределены по двум группам:

методы, затрудняющие считывание скопированной информации;

методы, препятствующие использованию информации.

Методы из первой группы основываются на придании особенностей процессу записи информации, которые не позволяют считывать полученную копию на других накопителях, не входящих в защищаемую КС. Таким образом, эти методы направлены на создание совместимости накопителей только внутри объекта. В КС должна быть ЭВМ, имеющая в своем составе стандартные и нестандартные накопители. На этой ЭВМ осуществляется ввод (вывод) информации для обмена с другими КС, а также переписывается информация со стандартных носителей на нестандартные, и

наоборот. Эти операции осуществляются под контролем администратора системы безопасности. Такая организация ввода-вывода информации существенно затрудняет действия злоумышленника не только при несанкционированном копировании, но и при попытках несанкционированного ввода информации.

Особенности работы накопителей на съемных магнитных носителях должны задаваться за счет изменения программных средств, поддерживающих их работу, а также за счет простых аппаратных регулировок и настроек. Такой подход позволит использовать серийные образцы накопителей.

Самым простым решением является нестандартная разметка (форматирование) носителя информации [18]. Изменение длины секторов, межсекторных расстояний, порядка нумерации секторов и некоторые другие способы нестандартного форматирования дискет затрудняют их использование стандартными средствами операционных систем. Нестандартное форматирование защищает только от стандартных средств работы с накопителями. Использование специальных программных средств (например, DISK EXPLORER для IBM-совместимых ПЭВМ) позволяет получить характеристики нестандартного форматирования.

Перепрограммирование контроллеров ВЗУ, аппаратные регулировки и настройки вызывают сбой оборудования при использовании носителей на стандартных ВЗУ, если форматирование и запись информации производились на нестандартном ВЗУ. В качестве примеров можно привести изменения стандартного алгоритма подсчета контрольной суммы и работы системы позиционирования накопителей на гибких магнитных дисках.

В контроллерах накопителей подсчитывается и записывается контрольная сумма данных сектора. Если изменить алгоритм подсчета контрольной суммы, то прочитать информацию на стандартном накопителе будет невозможно из-за сбоев.

Позиционирование в накопителях на магнитных дисках осуществляется следующим образом. Определяется номер дорожки, на которой установлены магнитные головки. Вычисляется количество дорожек, на которое необходимо переместить головки и направление движения. Если нумерацию дорожек магнитного диска начинать не с дорожек с максимальным радиусом, как это делается в стандартных накопителях, а нумеровать их в обратном

направлении, то система позиционирования стандартного накопителя не сможет выполнять свои функции при установке на него такого диска. Направление движения будет задаваться в направлении, обратном фактически записанным на дискете номерам дорожек, и успешное завершение позиционирования невозможно.

Выбор конкретного метода изменения алгоритма работы ВЗУ (или их композиции) осуществляется с учетом удобства практической реализации и сложности повторения алгоритма злоумышленником. При разработке ВЗУ необходимо учитывать потребность использования устройств в двух режимах: в стандартном режиме и в режиме совместимости на уровне КС. Выбор одного из режимов, а также выбор конкретного алгоритма нестандартного использования должен осуществляться, например, записью в ПЗУ двоичного кода. Число нестандартных режимов должно быть таким, чтобы исключался подбор режима методом перебора. Процесс смены режима должен исключать возможность автоматизированного подбора кода. Установку кода на ВЗУ всего объекта должен производить администратор системы безопасности.

8.2.2. Методы, препятствующие использованию скопированной информации

Эта группа методов имеет целью затруднить использование полученных копированием данных. Скопированная информация может быть программой или данными. Данные и программы могут быть защищены, если они хранятся на ВЗУ в преобразованном криптографическими методами виде. Программы, кроме того, могут защищаться от несанкционированного исполнения и тиражирования, а также от исследования.

Наиболее действенным (после криптографического преобразования) методом противодействия несанкционированному выполнению скопированных программ является использование блока контроля среды размещения программы [18]. Блок контроля среды размещения является дополнительной частью программ. Он создается при инсталляции (установке) программ. В него включаются характеристики среды, в которой размещается программа, а также средства получения и сравнения характеристик.

В качестве характеристик используются характеристики ЭВМ

или носителя информации, или совместно, характеристики ЭВМ и носителя. С помощью характеристик программа связывается с конкретной ЭВМ и (или) носителем информации. Программа может выполняться только на тех ЭВМ или запускаться только с тех носителей информации, характеристики которых совпадут с характеристиками, записанными в блоке контроля среды выполнения.

В качестве характеристик ЭВМ используются особенности архитектуры: тип и частота центрального процессора, номер процессора (если он есть), состав и характеристики внешних устройств, особенности их подключения, режимы работы блоков и устройств и т. п.

Сложнее осуществляется привязка программ к носителям информации, так как они стандартны и не имеют индивидуальных признаков [38]. Поэтому такие индивидуальные признаки создаются искусственно путем нанесения физических повреждений или изменением системной информации и структуры физических записей на носителе. Например, на гибких магнитных дисках могут прожигаться лазером отверстия, используется нестандартное форматирование, пометка некоторых секторов как дефектных. Приведенные средства защиты от несанкционированного использования дискет эффективны против стандартных способов создания копий (COPY, XCOPY, Diskcopy, Pctools, Norton Utilities в MS DOS и др.).

Однако существуют программные средства (COPYWRITE, DISK EXPLORER), позволяющие создавать полностью идентичные копии дискет с воспроизведением всех уникальных характеристик. Все же приведенный метод защиты нельзя считать абсолютно неэффективным, так как трудоемкость преодоления защиты велика и требования, предъявляемые к квалификации взломщика, высоки.

Общий алгоритм механизма защиты от несанкционированного использования программ в «чужой» среде размещения сводится к выполнению следующих шагов.

Шаг 1. Запоминание множества индивидуальных контрольных характеристик ЭВМ и (или) съемного носителя информации на этапе инсталляции защищаемой программы.

Шаг 2. При запуске защищенной программы управление пере-

дается на блок контроля среды размещения. Блок осуществляет сбор и сравнение характеристик среды размещения с контрольными характеристиками.

Шаг 3. Если сравнение прошло успешно, то программа выполняется, иначе - отказ в выполнении. Отказ в выполнении может быть дополнен выполнением деструктивных действий в отношении этой программы, приводящих к невозможности выполнения этой программы, если такую самоликвидацию позволяет выполнить ОС.

Привязка программ к среде размещения требует повторной их инсталляции после проведения модернизации, изменения структуры или ремонта КС с заменой устройств.

Для защиты от несанкционированного использования программ могут применяться и электронные ключи [51] . Электронный ключ «HASP» имеет размеры со спичечный коробок и подключается к параллельному порту принтера. Принтер подключается к компьютеру через электронный ключ. На работу принтера ключ не оказывает никакого влияния. Ключ распространяется с защищаемой программой. Программа в начале и в ходе выполнения считывает контрольную информацию из ключа. При отсутствии ключа выполнение программы блокируется.

8.2.3. Защита программных средств от исследования

Изучение логики работы программы может выполняться в одном из двух режимов: статическом и динамическом [60,61]. Сущность статического режима заключается в изучении исходного текста программы. Для получения листингов исходного текста выполняемый программный модуль дизассемблируют, то есть получают из программы на машинном языке программу на языке Ассемблер.

Динамический режим изучения алгоритма программы предполагает выполнение трассировки программы. Под трассировкой программы понимается выполнение программы на ЭВМ с использованием специальных средств, позволяющих выполнять программу в пошаговом режиме, получать доступ к регистрам, областям памяти, производить остановку программы по определенным адресам и т. д. В динамическом режиме изучение алгоритма рабо-

ты программы осуществляется либо в процессе трассировки, либо по данным трассировки, которые записаны в запоминающем устройстве.

Средства противодействия дизассемблированию не могут защитить программу от трассировки и наоборот: программы, защищенные только от трассировки, могут быть дизассемблированы. Поэтому для защиты программ от изучения необходимо иметь средства противодействия как дизассемблированию, так и трассировке.

Существует несколько методов противодействия дизассемблированию:

- шифрование;
- архивация:
- использование самогенерирующих кодов;
- «обман» дизассемблера.

Архивацию можно рассматривать как простейшее *шифрование*. Причем архивация может быть объединена с шифрованием. Комбинация таких методов позволяет получать надежно закрытые компактные программы. Зашифрованную программу невозможно дизассемблировать без расшифрования. Зашифрование (расшифрование) программ может осуществляться аппаратными средствами или отдельными программами. Такое шифрование используется перед передачей программы по каналам связи или при хранении ее на ВЗУ. Дизассемблирование программ в этом случае возможно только при получении доступа к расшифрованной программе, находящейся в ОП перед ее выполнением (если считается, что преодолеть криптографическую защиту невозможно).

Другой подход к защите от дизассемблирования связан с совмещением процесса расшифрования с процессом выполнения программ. Если расшифрование всей программы осуществляется блоком, получающим управление первым, то такую программу расшифровать довольно просто. Гораздо сложнее расшифровать и дизассемблировать программу, которая поэтапно расшифровывает информацию, и этапы разнесены по ходу выполнения программы. Задача становится еще более сложной, если процесс расшифрования разнесен по тексту программы.

Сущность метода, основанного на использовании *самогенерируемых* кодов, заключается в том, что исполняемые коды про-

граммы получаются самой программой в процессе ее выполнения. Самогенерируемые коды получаются в результате определенных действий над специально выбранным массивом данных. В качестве исходных данных могут использоваться исполняемые коды самой программы или специально подготовленный массив данных. Данный метод показал свою высокую эффективность, но он сложен в реализации.

Под *«обманом»* дизассемблера понимают такой стиль программирования, который вызывает нарушение правильной работы стандартного дизассемблера за счет нестандартных приемов использования отдельных команд, нарушения общепринятых соглашений. «Обман» дизассемблера осуществляется несколькими способами:

- нестандартная структура программы;
- скрытые переходы, вызовы процедур, возвраты из них и из прерываний;
- переходы и вызовы подпрограмм по динамически изменяемым адресам;
- модификация исполняемых кодов.

Для дезориентации дизассемблера часто используются скрытые переходы, вызовы и возвраты за счет применения нестандартных возможностей команд.

Маскировка скрытых действий часто осуществляется с применением стеков.

Трассировка программ обычно осуществляется с помощью программных продуктов, называемых отладчиками. Основное назначение их - выявление ошибок в программах. При анализе алгоритмов программ используются такие возможности отладчиков как пошаговое (покомандное) выполнение программ, возможность останова в контрольной точке.

Покомандное выполнение осуществляется процессором при установке пошагового режима работы. Контрольной точкой называют любое место в программе, на котором обычное выполнение программы приостанавливается, и осуществляется переход в особый режим, например, в режим покомандного выполнения. Для реализации механизма контрольной точки обычно используется прерывание по соответствующей команде ЭВМ (для IBM-совместных ПЭВМ такой командой является команда INT). В со-

временных процессорах можно использовать специальные регистры для установки нескольких контрольных точек при выполнении определенных операций: обращение к участку памяти, изменение участка памяти, выборка по определенному адресу, обращение к определенному порту ввода-вывода и т. д.

При наличии современных средств отладки программ полностью исключить возможность изучения алгоритма программы невозможно, но существенно затруднить трассировку возможно. Основной задачей противодействия трассировке является увеличение числа и сложности ручных операций, которые необходимо выполнить программисту-аналитику.

Для противодействия трассировке программы в ее состав вводятся следующие механизмы:

- изменение среды функционирования;
- модификация кодов программы;
- «случайные» переходы.

Под изменением среды функционирования понимается запрет или переопределение прерываний (если это возможно), изменение режимов работы, состояния управляющих регистров, триггеров и т. п. Такие изменения вынуждают аналитика отслеживать изменения и вручную восстанавливать среду функционирования.

Изменяющиеся коды программ, например, в процедурах приводят к тому, что каждое выполнение процедуры выполняется по различным ветвям алгоритма.

«Случайные» переходы выполняются за счет вычисления адресов переходов. Исходными данными для этого служат характеристики среды функционирования, контрольные суммы процедур (модифицируемых) и т. п. Включение таких механизмов в текст программ существенно усложняет изучение алгоритмов программ путем их трассировки.

Контрольные вопросы

1. Дайте определение несанкционированного доступа к информации.
2. Сравните два подхода к организации разграничения доступа.
3. Поясните принцип действия и концепцию создания системы разграничения доступа.

4. Приведите примеры современных систем защиты ПЭВМ и их возможности.
5. Поясните сущность защиты информации от копирования.
6. Какие методы применяются для защиты программных средств от исследования?

ГЛАВА 9
Криптографические методы защиты информации

9.1. Классификация методов криптографического преобразования информации

Под **криптографической защитой информации** понимается такое преобразование исходной информации, в результате которого она становится недоступной для ознакомления и использования лицами, не имеющими на это полномочий.

Известны различные подходы к классификации методов криптографического преобразования информации. По виду воздействия на исходную информацию методы криптографического преобразования информации могут быть разделены на четыре группы (рис. 14).

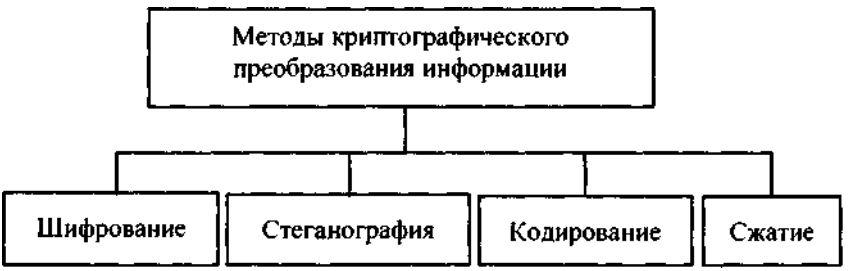


Рис. 14. Классификация методов криптографического преобразования информации

Процесс **шифрования** заключается в проведении обратимых математических, логических, комбинаторных и других преобразований исходной информации, в результате которых зашифрован-

ная информация представляет собой хаотический набор букв, цифр, других символов и двоичных кодов.

Для шифрования информации используются алгоритм преобразования и ключ. Как правило, алгоритм для определенного метода шифрования является неизменным. Исходными данными для алгоритма шифрования служат информация, подлежащая зашифрованию, и ключ шифрования. Ключ содержит управляющую информацию, которая определяет выбор преобразования на определенных шагах алгоритма и величины операндов, используемые при реализации алгоритма шифрования.

В отличие от других методов криптографического преобразования информации, методы **стеганографии** [2] позволяют скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации. В компьютерных системах практическое использование стеганографии только начинается, но проведенные исследования показывают ее перспективность. В основе всех методов стеганографии лежит маскирование закрытой информации среди открытых файлов. Обработка мультимедийных файлов в КС открыла практически неограниченные возможности перед стеганографией.

Существует несколько методов скрытой передачи информации. Одним из них является простой метод скрытия файлов при работе в операционной системе MS DOS. За текстовым открытым файлом записывается скрытый двоичный файл, объем которого много меньше текстового файла. В конце текстового файла помещается метка EOF (комбинация клавиш Control и Z). При обращении к этому текстовому файлу стандартными средствами ОС считывание прекращается по достижению метки EOF и скрытый файл остается недоступен. Для двоичных файлов никаких меток в конце файла не предусмотрено. Конец такого файла определяется при обработке атрибутов, в которых хранится длина файла в байтах. Доступ к скрытому файлу может быть получен, если файл открыть как двоичный. Скрытый файл может быть зашифрован. Если кто-то случайно обнаружит скрытый файл, то зашифрованная информация будет воспринята как сбой в работе системы.

Графическая и звуковая информация представляются в числовом виде. Так в графических объектах наименьший элемент изображения может кодироваться одним байтом. В младшие разряды

определенных байтов изображения в соответствии с алгоритмом криптографического преобразования помещаются биты скрытого файла. Если правильно подобрать алгоритм преобразования и изображение, на фоне которого помещается скрытый файл, то человеческому глазу практически невозможно отличить полученное изображение от исходного. Очень сложно выявить скрытую информацию и с помощью специальных программ. Наилучшим образом для внедрения скрытой информации подходят изображения местности: фотоснимки со спутников, самолетов и т. п. С помощью средств стеганографии могут маскироваться текст, изображение, речь, цифровая подпись, зашифрованное сообщение. Комплексное использование стеганографии и шифрования многократно повышает сложность решения задачи обнаружения и раскрытия конфиденциальной информации.

Содержанием процесса **кодирования** информации является замена смысловых конструкций исходной информации (слов, предложений) кодами. В качестве кодов могут использоваться сочетания букв, цифр, букв и цифр. При кодировании и обратном преобразовании используются специальные таблицы или словари. Кодирование информации целесообразно применять в системах с ограниченным набором смысловых конструкций. Такой вид криптографического преобразования применим, например, в командных линиях АСУ. Недостатками кодирования конфиденциальной информации является необходимость хранения и распространения кодировочных таблиц, которые необходимо часто менять, чтобы избежать раскрытия кодов статистическими методами обработки перехваченных сообщений.

Сжатие информации может быть отнесено к методам криптографического преобразования информации с определенными оговорками. Целью сжатия является сокращение объема информации. В то же время сжатая информация не может быть прочитана или использована без обратного преобразования. Учитывая доступность средств сжатия и обратного преобразования, эти методы нельзя рассматривать как надежные средства криптографического преобразования информации. Даже если держать в секрете алгоритмы, то они могут быть сравнительно легко раскрыты статистическими методами обработки. Поэтому сжатые файлы конфиденциальной информации подвергаются последующему шифрова-

нию. Для сокращения времени целесообразно совмещать процесс сжатия и шифрования информации.

9.2. Шифрование. Основные понятия

Основным видом криптографического преобразования информации в КС является шифрование. Под шифрованием понимается процесс преобразования открытой информации в зашифрованную информацию (шифртекст) или процесс обратного преобразования зашифрованной информации в открытую. Процесс преобразования открытой информации в закрытую получил название зашифрование, а процесс преобразования закрытой информации в открытую - расшифрование.

За многовековую историю использования шифрования информации человечеством изобретено множество методов шифрования или шифров. Методом шифрования (шифром) называется совокупность обратимых преобразований открытой информации в закрытую информацию в соответствии с алгоритмом шифрования. Большинство методов шифрования не выдержали проверку временем, а некоторые используются и до сих пор. Появление ЭВМ и КС инициировало процесс разработки новых шифров, учитывающих возможности использования ЭВМ как для зашифрования/расшифрования информации, так и для атак на шифр. Атака на шифр (криптоанализ) - это процесс расшифрования закрытой информации без знания ключа и, возможно, при отсутствии сведений об алгоритме шифрования.

Современные методы шифрования должны отвечать следующим требованиям:

- стойкость шифра противостоять криптоанализу (криптостойкость) должна быть такой, чтобы вскрытие его могло быть осуществлено только путем решения задачи полного перебора ключей;
- криптостойкость обеспечивается не секретностью алгоритма шифрования, а секретностью ключа;
- шифртекст не должен существенно превосходить по объему исходную информацию;
- ошибки, возникающие при шифровании, не должны приводить к искажениям и потерям информации;

- время шифрования не должно быть большим;
- стоимость шифрования должна быть согласована со стоимостью закрываемой информации.

Криптостойкость шифра является его основным показателем эффективности. Она измеряется временем или стоимостью средств, необходимых криптоаналитику для получения исходной информации по шифртексту, при условии, что ему неизвестен ключ.

Сохранить в секрете широко используемый алгоритм шифрования практически невозможно. Поэтому алгоритм не должен иметь скрытых слабых мест, которыми могли бы воспользоваться криптоаналитики. Если это условие выполняется, то криптостойкость шифра определяется длиной ключа, так как единственный путь вскрытия зашифрованной информации - перебор комбинаций ключа и выполнение алгоритма расшифрования. Таким образом, время и средства, затрачиваемые на криптоанализ, зависят от длины ключа и сложности алгоритма шифрования.

В качестве примера удачного метода шифрования можно привести шифр DES (Data Encryption Standard), применяемый в США с 1978 года в качестве государственного стандарта. Алгоритм шифрования не является секретным и был опубликован в открытой печати. За все время использования этого шифра не было обнароловано ни одного случая обнаружения слабых мест в алгоритме шифрования.

В конце 70-х годов использование ключа длиной в 56 бит гарантировало, что для раскрытия шифра потребуется несколько лет непрерывной работы самых мощных по тем временам компьютеров. Прогресс в области вычислительной техники позволил значительно сократить время определения ключа путем полного перебора. Согласно заявлению специалистов Агентства национальной безопасности США 56-битный ключ для DES может быть найден менее чем за 453 дня с использованием суперЭВМ Cray T3D, которая имеет 1024 узла и стоит 30 млн. долл. Используя чип FPGA (Field Progammably Gate Array - программируемая вентильная матрица) стоимостью 400 долл., можно восстановить 40-битный ключ DES за 5 часов. Потратив 10000 долл. за 25 чипов FPGA, 40-битный ключ можно найти в среднем за 12 мин. Для вскрытия 56-битного ключа DES при опоре на серийную техноло-

\

гию и затратах в 300000 долл. требуется в среднем 19 дней, а если разработать специальный чип, то - 3 часа. При затратах в 300 млн. долл. 56-битные ключи могут быть найдены за 12 сек. Расчеты показывают, что в настоящее время для надежного закрытия информации длина ключа должна быть не менее 90 бит.

Все методы шифрования могут быть классифицированы по различным признакам. Один из вариантов классификации приведен на рис. 15 [8].

9.3. Методы шифрования с симметричным ключом

9.3.1. Методы замены

Сущность методов замены (подстановки) заключается в замене символов исходной информации, записанных в одном алфавите, символами из другого алфавита по определенному правилу [56]. Самым простым является *метод прямой замены*. Символам So; исходного алфавита Ao, с помощью которых записывается исходная информация, однозначно ставятся в соответствие символы Su шифрующего алфавита Аь В простейшем случае оба алфавита могут состоять из одного и того же набора символов. Например, оба алфавита могут содержать буквы русского алфавита.

Задание соответствия между символами обоих алфавитов осуществляется с помощью преобразования числовых эквивалентов символов исходного текста To, длиной - K символов, по определенному алгоритму.

Алгоритм моноалфавитной замены может быть представлен в виде последовательности шагов.

Шаг 1. Формирование числового кортежа Lot, путем замены каждого символа s^ e T_o (i=l,K), представленного в исходном алфавите Ao размера [1xR], на число hoi(soi), соответствующее порядковому номеру символа soi в алфавите Ao.

Шаг 2. Формирование числового кортежа Li_h путем замены каждого числа кортежа Lo_h на соответствующее число hn кортежа Li_h, вычисляемое по формуле:

$$h_u = (k,xhoi(soi)+k_2)(mod\ R),$$

где ki - десятичный коэффициент; k_2 - коэффициент сдвига. Выбранные коэффициенты ki, k_2 должны обеспечивать однозначное

соответствие чисел ho, и hi,, а при получении hi, = 0 выполнить замену hi, = R.

Шаг 3. Получение шифртекста Ti путем замены каждого числа h],(si,) кортежа $L]_h$ соответствующим символом Si, e Ti (i=l,K) алфавита шифрования A] размера $[1^X R]$.

Шаг 4. Полученный шифртекст разбивается на блоки фиксированной длины Ь. Если последний блок оказывается неполным, то в конец блока помещаются специальные символы-заполнители (например, символ *).

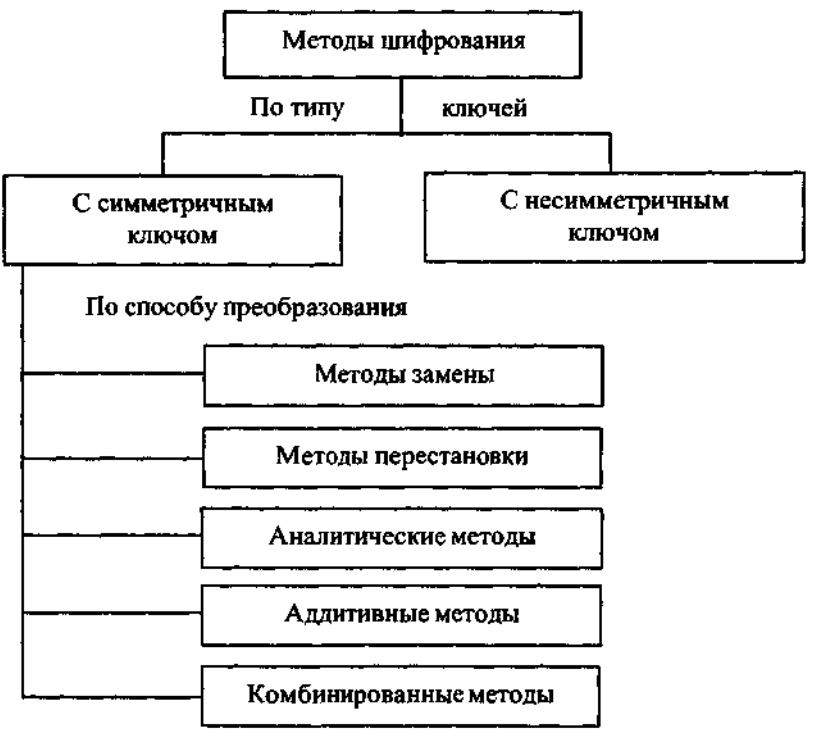


Рис 15. Классификация методов шифрования

Пример. Исходными данными для шифрования **являются:**
T_0 = < М Е Т О Д _ Ш И Ф Р О В А Н И Я > ;
Ao = < А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ **Ъ Ы Ь Э Ю Я** >;

A_1 = <О Р Щ Ь Я Т Э _ Ж М Ч Х А В Д Ы Ф К С Е З П И Ц Г Н Л Ъ Ш Б У Ю>;

R=32; k_1=3; k_2=15, b=4.

Пошаговое выполнение алгоритма приводит к получению следующих результатов.

Шаг 1. L_{0h} = <12,6,18,14,5,32,24,9,20,16,14,3,1,13,9,31>.

Шаг 2. L_{1h} = <19,1,5,25,30,15,23,10,11,31,25,24,18,22,10,12>.

Шаг 3. T_1 = <С О Я Г Б Д И М Ч У Г Ц К П М Х>.

Шаг 4. T_2 = <С О Я Г Б Д И М Ч У Г Ц К П М Х>.

При расшифровании сначала устраняется разбиение на блоки. Получается непрерывный шифртекст T_1 длиной К символов. Расшифрование осуществляется путем решения целочисленного уравнения:

При известных целых величинах $k_b k_2$, h_h и R величина ho, вычисляется методом перебора п.

Последовательное применение этой процедуры ко всем символам шифртекста приводит к его расшифрованию.

По условиям приведенного примера может быть построена таблица замены, в которой взаимозаменяемые символы располагаются в одном столбце (табл. 1).

Таблица 1

Таблица замены

s_{0i}	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
h_{0i}	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
s_{1i}	К	З	Ц	Л	Б	О	Ь	Э	М	А	Ы	С	П	Г	Ъ	У	Р	Я	_	Ч	В	Ф	Е	И
h_{1i}	18	21	24	27	30	1	4	7	10	13	16	19	22	25	28	31	2	5	8	11	14	17	20	23

s_{0i}	Щ	Ъ	Ы	Ь	Э	Ю	Я	_
h_{0i}	25	26	27	28	29	30	31	32
s_{1i}	Н	Ш	Ю	Щ	Т	Ж	Х	Д
h_{1i}	26	29	32	3	6	9	12	15

Использование таблицы замены значительно упрощает процесс шифрования. При шифровании символ исходного текста сравнивается с символами строки S_0, таблицы. Если произошло совпадение в i-м столбце, то символ исходного текста заменяется символом из строки $s_{i,}$, находящегося в том же столбце i таблицы.

Расшифрование осуществляется аналогичным образом, но вход в таблицу производится по строке Sn.

Основным недостатком метода прямой замены является наличие одних и тех же статистических характеристик исходного и закрытого текста. Зная, на каком языке написан исходный текст и частотную характеристику употребления символов алфавита этого языка, криптоаналитик путем статистической обработки перехваченных сообщений может установить соответствие между символами обоих алфавитов.

Существенно более стойкими являются методы полиалфавитной замены. Такие методы основаны на использовании нескольких алфавитов для замены символов исходного текста. Формально полиалфавитную замену можно представить следующим образом. При N- алфавитной замене символ soi из исходного алфавита A_o заменяется символом вц из алфавита Аь S02 заменяется символом S22 из алфавита Аг и так далее. После замены SON СИМВОЛОМ S MM ИЗ AN СИМВОЛ SO(N+D замещается символом Si(N+i) ИЗ алфавита Ai и так далее.

Наибольшее распространение получил алгоритм полиалфавитной замены с использованием таблицы (матрицы) Вижинера $T_в$, которая представляет собой квадратную матрицу [RxR], где R - количество символов в используемом алфавите. В первой строке располагаются символы в алфавитном порядке. Начиная со второй строки, символы записываются со сдвигом влево на одну позицию. Выталкиваемые символы заполняют освобождающиеся позиции справа (циклический сдвиг). Если используется русский алфавит, то матрица Вижинера имеет размерность [32x32] (рис. 16).

```
        АБВГД. . . . . ЪЭЮЯ_
        ВВГДЕ. . . . . ЭЮЯ_А
Тв=     ВГДЕЖ. . . . . ЮЯ_АБ

        _АБВГ. . . . . ЫЪЭЮЯ
```

Рис. 16. Матрица Вижинера

Шифрование осуществляется с помощью ключа, состоящего из М неповторяющихся символов. Из полной матрицы Вижинера

выделяется матрица шифрования $T_ш$, размерностью [(M+1),R]. Она включает первую строку и строки, первые элементы которых совпадают с символами ключа. Если в качестве ключа выбрано слово <ЗОНД>, то матрица шифрования содержит пять строк (рис. 17).

```
АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ_
ЗИКЛМН0ПРСТУФХЦЧШЩЪЫЬЭЮЯ_АБВГДЕЖ
ОПРСТУФХЦЧШЩЪЫЬЭЮЯ_АБВГДЕЖЗИКЛМН
Я0ПРСТУФХЦЧШЩЪЫЬЭЮЯ_АБВГДЕЖЗИКЛМ
ДЕЖЗИКЛМН0ПРСТУФХЦЧШЩЪЫЬЭЮЯ_АБВГ
```

Рис. 17. Матрица шифрования для ключа <ЗОНД>

Алгоритм зашифрования с помощью таблицы Вижинера представляет собой следующую последовательность шагов.

Шаг 1. Выбор ключа K длиной M символов.

Шаг 2. Построение матрицы шифрования $T_ш$=(Ьу) размерностью [(M+1),R] для выбранного ключа K.

Шаг 3. Под каждым символом s^ исходного текста длиной I символов размещается символ ключа k_m (рис. 20). Ключ повторяется необходимое число раз.

Шаг 4. Символы исходного текста последовательно замещаются символами, выбираемыми из $T_ш$ по следующему правилу:

1) определяется символ k_m ключа K, соответствующий замещаемому символу $s_{ог}$;
2) находится строка i в $T_ш$, для которой выполняется условие кт=$Ь_п$;
3) определяется столбец j, для которого выполняется условие:

4) символ $s_{ог}$ замещается символом Ь^.

Шаг 5. Полученная зашифрованная последовательность разбивается на блоки определенной длины, например, по четыре символа. Последний блок дополняется, при необходимости, служебными символами до полного объема.

Расшифрование осуществляется в следующей последовательности:

Шаг 1. Под шифртекстом записывается последовательность символов ключа по аналогии с шагом 3 алгоритма зашифрования.

Шаг 2. Последовательно выбираются символы Sj_r из шифртек»-ста и соответствующие символы ключа k_m. В матрице $T_ш$ определяется строка i, для которой выполняется условие $k_m = Ь_{;1}$. В строке i определяется элемент by= Si_r. В расшифрованный текст на позицию г помещается символ bij.

Шаг 3. Расшифрованный текст записывается без разделения на блоки. Убираются служебные символы.

Пример.

Требуется с помощью ключа K = <ЗОНД> зашифровать исходный текст T = <БЕЗОБЛАЧНОЕ_НЕБО>. Механизмы зашифрования и расшифрования представлены на рис. 18.

Исходный текст	Б Е З 0 Б Л А Ч Н 0 Е _ Н Е Б 0
Ключ	З О Н Д З О Н Д З О Н Д З О Н Д
Текст после замены	ИУФТИШНЫФЫТГФУОТ
Шифртекст	ИУФТ ИШНЫ ФЫТГ ФУОТ
Ключ	ЗОНД ЗОНД ЗОНД ЗОНД
Расшифрованный текст	БЕЗО БЛАЧ НОЕ_ НЕБО
Исходный текст	БЕЗ0БЛАЧН0Е_НЕБ0

Рис. 18. Пример шифрования с помощью матрицы Вижинера

Криптостойкость методов полиалфавитной замены значительно выше методов простой замены, так как одни и те же символы исходной последовательности могут заменяться разными символами. Однако стойкость шифра к статистическим методам криптоанализа зависит от длины ключа.

Для повышения криптостойкости может использоваться модифицированная матрица шифрования. Она представляет собой матрицу размерности [11,R], где R - число символов алфавита. В первой строке располагаются символы в алфавитном порядке. Остальные 10 строк нумеруются от 0 до 9. В этих строках символы располагаются случайным образом.

В качестве ключей используются, например, непериодические бесконечные числа *n,* е и другие. Очередной n-й символ исходного текста заменяется соответствующим символом из строки матрицы шифрования, номер которой совпадает с n-й цифрой бесконечного числа.

9.3.2. Методы перестановки

Суть методов перестановки заключается в разделении исходного текста на блоки фиксированной длины и последующей перестановке символов внутри каждого блока по определенному алгоритму[56].

Перестановки получаются за счет разницы путей записи исходной информации и путей считывания зашифрованной информации в пределах геометрической фигуры. Примером простейшей перестановки является запись блока исходной информации в матрицу по строкам, а считывание - по столбцам. Последовательность заполнения строк матрицы и считывания зашифрованной информации по столбцам может задаваться ключом. Криптостойкость метода зависит от длины блока (размерности матрицы). Так для блока длиной 64 символа (размерность матрицы 8x8) возможны $1{,}6 \times Ю^{9}$ комбинаций ключа. Для блока длиной 256 символов (матрица размерностью 16x16) число возможных ключей достигает $1{,}4 \times 10^{26}$. Решение задачи перебора ключей в последнем случае даже для современных ЭВМ представляет существенную сложность.

Перестановки используются также в методе, основанном на применении *маршрутов Гамильтона*. Этот метод реализуется путем выполнения следующих шагов.

Шаг 1. Исходная информация разбивается на блоки. Если длина шифруемой информации не кратна длине блока, то на свободные места последнего блока помещаются специальные служебные символы-заполнители (например, *).

Шаг 2. Символами блока заполняется таблица, в которой для каждого порядкового номера символа в блоке отводится вполне определенное место (рис. 19).

Шаг 3. Считывание символов из таблицы осуществляется по одному из маршрутов. Увеличение числа маршрутов повышает криптостойкость шифра. Маршруты выбираются либо последовательно, либо их очередность задается ключом K.

Шаг 4. Зашифрованная последовательность символов разбивается на блоки фиксированной длины L. Величина L может отличаться от длины блоков, на которые разбивается исходная информация на шаге 1.

Расшифрование производится в обратном порядке. В соответствии с ключом выбирается маршрут и заполняется таблица согласно этому маршруту.

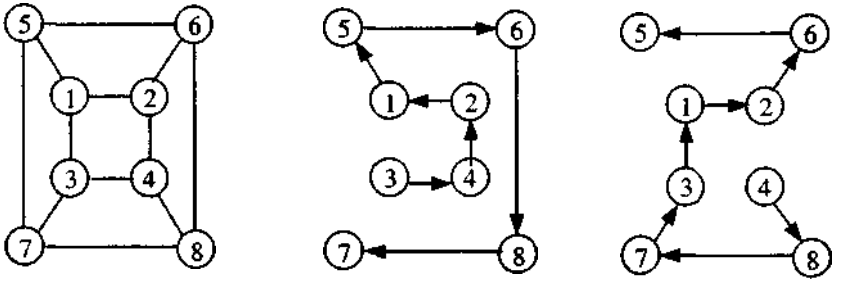


Рис. 19. Вариант 8-элементной таблицы и маршрутов Гамильтона

Из таблицы символы считываются в порядке следования номеров элементов. Ниже приводится пример шифрования информации с использованием маршрутов Гамильтона.

Пусть требуется зашифровать исходный текст T_o = <МЕТОДЫ_ПЕРЕСТАНОВКИ>. Ключ и длина зашифрованных блоков соответственно равны: K=<2,1.1>, L=4. Для шифрования используются таблица и два маршрута, представленные на рис. 19. Для заданных условий маршруты с заполненными матрицами имеют вид, показанный на рис. 20.

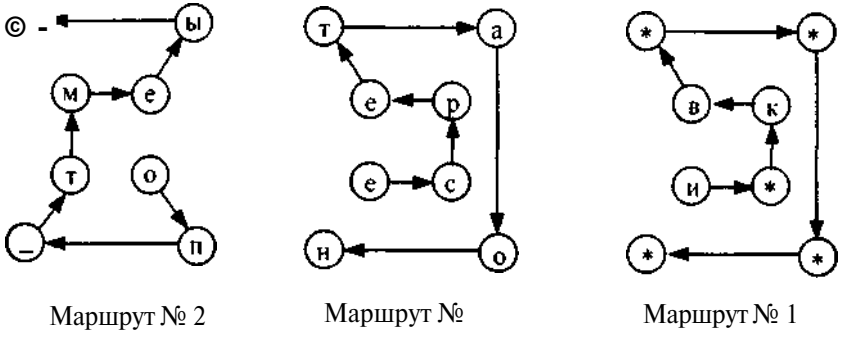


*Рис. **20. Пример** шифрования с помощью маршрутов Гамильтона*

Шаг 1. Исходный текст разбивается на три блока:

Б1 =<МЕТОДЫ_П>;

Б2 =<ЕРЕСТАНО>;

БЗ = <ВКИ*****>.

Шаг 2. Заполняются три матрицы с маршрутами 2,1,1 (рис.20).

Шаг 3. Получение шифртекста путем расстановки символов в соответствии с маршрутами.

Tj=<ОП_ТМЕЫДЕСРЕТАОНИ*КВ****>.

Шаг 4. Разбиение на блоки шифртекста

Т, =<ОП_Т МЕЫД ЕСРЕ ТАОН И*КВ ****>.

В практике большое значение имеет использование специальных аппаратных схем, реализующих метод перестановок (рис. 21).

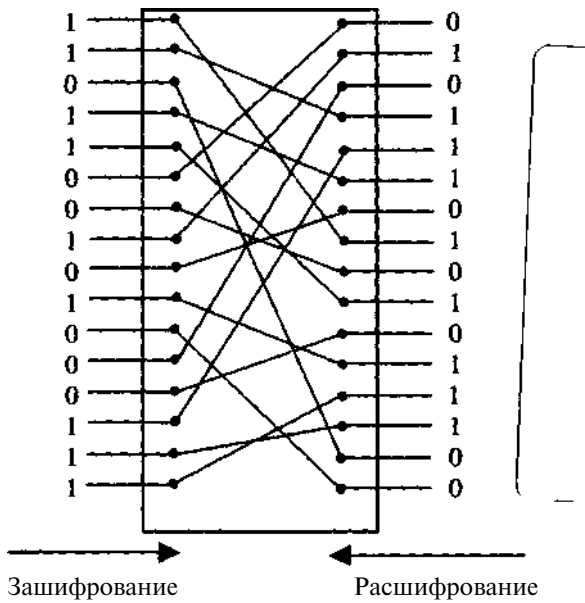


Рис. 21. Схема перестановок

Параллельный двоичный код блока исходной информации (например, два байта) подаются на схему. За счет внутренней коммутации в схеме осуществляется перестановка бит в пределах блока. Для расшифрования блока информации входы и выходы схемы меняются местами [49].

Методы перестановок просто реализуются, но имеют два существенных недостатка. Во-первых, они допускают раскрытие шифртекста при помощи статистической обработки. Во-вторых, если исходный текст разбивается на блоки длиной K символов, то криптоайалитику для раскрытия шифра достаточно направить в систему шифрования K-1 блок тестовой информации, в которых все символы за исключением одного одинаковы.

9.3.3.Аналитические методы шифрования

Для шифрования информации могут использоваться аналитические преобразования [8]. Наибольшее распространение получили методы шифрования, основанные на использовании матричной алгебры. Зашифрование k-го блока исходной информации, представленного в виде вектора B^ = ‖ bj‖ , осуществляется путем перемножения матрицы-ключа A= ‖ *щ*\ и вектора $B_к$. В результате перемножения получается блок шифртекста в виде вектора Ck= Iks ||, где элементы вектора Ск определяются по формуле:

$$c_i = \sum_j a_{ij} b_j.$$

Расшифрование информации осуществляется путем последовательного перемножения векторов C^ и матрицы $A^{"l}$, обратной матрице A.

Пример шифрования информации с использованием алгебры матриц.

Пусть необходимо зашифровать и расшифровать слово

To = < ЗАБАВА> с помощью матрицы-ключа A:

$$A = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix}$$

Для зашифрования исходного слова необходимо выполнить следующие шаги.

Шаг 1. Определяется числовой эквивалент исходного слова как последовательность соответствующих порядковых номеров букв слова $T_э$:

$$T, = <8, 1, 2, 1, 3, 1>.$$

Шаг 2. Умножение матрицы А на векторы Bi={8, 1, 2} **и** B*={1.3,1}:

$$C_1 = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix} \cdot \begin{vmatrix} 8 \\ 1 \\ 2 \end{vmatrix} = \begin{vmatrix} 28 \\ 35 \\ 67 \end{vmatrix};$$

$$C_2 = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix} \cdot \begin{vmatrix} 1 \\ 3 \\ 1 \end{vmatrix} = \begin{vmatrix} 21 \\ 26 \\ 38 \end{vmatrix}.$$

Шаг 3. Зашифрованное слово записывается в виде последовательности чисел Ti = <28, 35, 67, 21,26, 38>.

Расшифрование слова осуществляется следующим образом.

Шаг 1. Вычисляется определитель |A|= -115.

Шаг 2. Определяется присоединенная матрица А*, каждый элемент которой является алгебраическим дополнением элемента *щ* матрицы А

$$A^* = \begin{vmatrix} 17 & -3 & -15 \\ 52 & -43 & 15 \\ -48 & 22 & -5 \end{vmatrix}.$$

Шаг 3. Получается транспонированная **матрица А**

$$A^T = \begin{vmatrix} 17 & 52 & -48 \\ -3 & -43 & 22 \\ -15 & 15 & -5 \end{vmatrix}.$$

Шаг 4. Вычисляется обратная матрица A^{-1} по формуле:

$$A^{-1} = A^T / |A|.$$

В результате вычислений обратная матрица имеет **вид:**

$$A^{-1} = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix}.$$

Шаг 4. Определяются векторы Bi и Bг:
$\mathbf{B_1 = A^{-1} \cdot C_1}$; $\mathbf{B_2 = A^{-1} \cdot C_2}$.

$$\mathbf{B_1} = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix} \cdot \begin{vmatrix} 28 \\ 35 \\ 67 \end{vmatrix} = \begin{vmatrix} 8 \\ 1 \\ 2 \end{vmatrix},$$

$$\mathbf{B_2} = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix} \cdot \begin{vmatrix} 21 \\ 26 \\ 38 \end{vmatrix} = \begin{vmatrix} 1 \\ 3 \\ 1 \end{vmatrix}.$$

Шаг 5. Числовой эквивалент расшифрованного слова
$T_э$=<8, 1,2, 1, 3, 1 > заменяется символами, в результате чего получается исходное слово $T_о$ = <ЗАБАВА>.

9.3.4. Аддитивные методы шифрования

Сущность аддитивных методов шифрования заключается в последовательном суммировании цифровых кодов, соответствующих символам исходной информации, с последовательностью кодов, которая соответствует некоторому кортежу символов [56]. Этот кортеж называется *гаммой*. Поэтому аддитивные методы шифрования называют также *гаммированием*.

Для данных методов шифрования ключом является гамма. Криптостойкость аддитивных методов зависит от длины ключа и равномерности его статистических характеристик. Если ключ короче, чем шифруемая последовательность символов, то шифртекст может быть расшифрован криптоаналитиком статистическими методами исследования. Чем больше разница длин ключа и исходной информации, тем выше вероятность успешной атаки на шифртекст. Если ключ представляет собой непериодическую последовательность случайных чисел, длина которой превышает длину шифруемой информации, то без знания ключа расшифровать шифртекст практически невозможно. Как и для методов замены в качестве ключа могут использоваться неповторяющиеся последовательности цифр, например, в числах *к, е и* других.

На практике самыми эффективными и распространенными являются аддитивные методы, в основу которых положено исполь-

зование *генераторов (датчиков) псевдослучайных чисел.* Генератор использует исходную информацию относительно малой длины для получения практически бесконечной последовательности псевдослучайных чисел.

Для получения последовательности псевдослучайных чисел (ПСЧ) могут использоваться конгруэнтные генераторы. Генераторы этого класса вырабатывают псевдослучайные последовательности чисел, для которых могут быть строго математически определены такие основные характеристики генераторов как периодичность и случайность выходных последовательностей.

Среди конгруэнтных генераторов ПСЧ выделяется своей простотой и эффективностью линейный генератор, вырабатывающий псевдослучайную последовательность чисел T(i) в соответствии с соотношением

$$T(i+1) = (a \cdot T(i) + c) \bmod m,$$

где a и c - константы, T(0) - исходная величина, выбранная в качестве порождающего числа.

Период повторения такого датчика ПСЧ зависит от величин a и c. Значение m обычно принимается равным 2^s, где s - длина слова ЭВМ в битах. Период повторения последовательности генерируемых чисел будет максимальным тогда и только тогда, когда c - нечетное число и $a \pmod 4 = 1$ [39]: Такой генератор может быть сравнительно легко создан как аппаратными средствами, так и программно.

9.4. Системы шифрования с открытым ключом

Наряду с традиционным шифрованием на основе секретного ключа в последние годы все большее признание получают системы шифрования с открытым ключом. В таких системах используются два ключа. Информация шифруется с помощью открытого ключа, а расшифровывается с использованием секретного ключа.

В основе применения систем с открытым ключом лежит использование необратимых или односторонних функций [8]. Эти функции обладают следующим свойством. По известному x легко определяется функция $y = f(x)$. Но по известному значению y практически невозможно получить x. В криптографии используются односторонние функции, имеющие так называемый потай-

ной ход. Эти функции с параметром z обладают следующими свойствами. Для определенного z могут быть найдены алгоритмы Ez и D_z. С помощью Ez легко получить функцию $f_z(x)$ для всех x из области определения. Так же просто с помощью алгоритма D_z получается и обратная функция $x = f^{t}(y)$ для всех y из области допустимых значений. В то же время практически для всех z и почти для всех y из области допустимых значений нахождение $f^{t}(y)$ при помощи вычислений невозможно даже при известном E^. В качестве открытого ключа используется y, а в качестве закрытого - x.

При шифровании с использованием открытого ключа нет необходимости в передаче секретного ключа между взаимодействующими субъектами, что существенно упрощает криптозащиту передаваемой информации.

Криптосистемы с открытыми ключами различаются видом односторонних функций. Среди них самыми известными являются системы RSA, Эль-Гамаля и Мак-Элиса. В настоящее время наиболее эффективным и распространенным алгоритмом шифрования с открытым ключом является алгоритм RSA, получивший свое название от первых букв фамилий его создателей: Rivest, Shamir и Adleman.

Алгоритм основан на использовании операции возведения в степень модульной арифметики. Его можно представить в виде следующей последовательности шагов [39].

Шаг 1. Выбираются два больших простых числа p и q. Простыми называются числа, которые делятся только на самих себя и на 1. Величина этих чисел должна быть больше 200.

Шаг 2. Получается открытая компонента ключа n:

$$n=pq.$$

Шаг 3. Вычисляется функция Эйлера по формуле:

$$f(p,q) = (p-1)(q-1).$$

Функция Эйлера показывает количество целых положительных чисел от 1 до n, которые взаимно просты с n. Взаимно простыми являются такие числа, которые не имеют ни одного общего делителя, кроме 1.

Шаг 4. Выбирается большое простое число d, которое является взаимно простым со значением $f(p,q)$.

Шаг 5. Определяется число e, удовлетворяющее условию:

$$e*d = l(modf(p,q)).$$

Данное условие означает, что остаток от деления (вычет) произведения *e-d* на функцию *f(p,q)* равен 1. Число *e* принимается в качестве второй компоненты открытого ключа. В качестве секретного ключа используются числа *d* и *n*.

Шаг 6. Исходная информация, независимо от ее физической природы, представляется в числовом двоичном виде. Последовательность бит разделяется на блоки длиной L бит, где L - наименьшее целое число, удовлетворяющее условию: L>log2(w+7). Каждый блок рассматривается как целое положительное число *X(i),* принадлежащее интервалу [0,п-1]. Таким образом, исходная информация представляется последовательностью чисел X(0, /=1,1. Значение I определяется длиной шифруемой последовательности.

Шаг 7. Зашифрованная информация получается в виде последовательности чисел Y(i), вычисляемых по формуле:

$$Y(i) = (X(i))^{e} \pmod{n}.$$

Шаг 8. Для расшифрования информации используется следующая зависимость:

$$X(i) = (Y(i))^{\cdot} \pmod{n}.$$

Пример применения метода RSA для криптографического закрытия информации. Примечание: для простоты вычислений использованы минимально возможные числа.

Пусть требуется зашифровать сообщение на русском языке «ГАЗ».

Для зашифрования и расшифрования сообщения необходимо выполнить следующие шаги.

Шаг 1. Выбирается *p — 3* и *q*= 11.

Шаг 2. Вычисляется *n* = 3*11=33.

Шаг 3. Определяется функция Эйлера

$$f(p,q) = (3-1)-(11-1) = 20.$$

Шаг 4. В качестве взаимно простого числа выбирается число *d=3.*

Шаг 5. Выбирается такое число *e,* которое удовлетворяло бы соотношению: *(e*3)* (mod 20) = 1. Пусть e = 7.

Шаг 6. Исходное сообщение представляется как последовательность целых чисел. Пусть букве А соответствует число 1, букве Г — число 4, букве З - число 9. Для представления чисел в двоичном коде требуется 6 двоичных разрядов, так как в русском

алфавите используются 33 буквы (случайное совпадение с числом п). Исходная информация в двоичном коде имеет вид:

000100 000001001001.

Длина блока L определяется как минимальное число из целых чисел, удовлетворяющих условию: L>log2(33+1), так как п=33. Отсюда L=6. Тогда исходный текст представляется в виде кортежа X(i) = <4, 1,9>.

Шаг 7. Кортеж X(i) зашифровывается с помощью открытого ключа {7, 33}:

$$Y(1) = (4^7) \pmod{33} = 16384 \pmod{33} = 16;$$
$$Y(2) = (1^7) \pmod{33} = 1 \pmod{33} = 1;$$
$$Y(3) = (9^7) \pmod{33} = 4782969 \pmod{33} = 15.$$

Получено зашифрованное сообщение Y(i) = <16, 1, 15>.

Шаг 8. Расшифровка сообщения Y(i) = <16, 1, 15> осуществляется с помощью секретного ключа {3, 33}:

$X(1) = (16^3) \pmod{33} = 4096 \pmod{33} = 4;$

$X(2) = (1^3) \pmod{33} = 1 \pmod{33} = 1;$

$X(3) = (15^3) \pmod{33} = 3375 \pmod{33} = 9.$

Исходная числовая последовательность в расшифрованном виде X (i) = <4, 1, 9> заменяется исходным текстом «ГАЗ».

Система Эль-Гамаля основана на сложности вычисления дискретных логарифмов в конечных полях [22]. Основным недостатком систем RSA и Эль-Гамаля является необходимость выполнения трудоемких операций в модульной арифметике, что требует привлечения значительных вычислительных ресурсов.

Криптосистема Мак-Элиса использует коды, исправляющие ошибки. Она реализуется в несколько раз быстрее, чем криптосистема RSA, но имеет и существенный недостаток. В криптосистеме *Мак-Элиса* используется ключ большой длины и получаемый шифртекст в два раза превышает длину исходного текста.

Для всех методов шифрования с открытым ключом математически строго не доказано отсутствие других методов криптоанализа кроме решения NP-полной задачи (задачи полного перебора). Если появятся методы эффективного решения таких задач, то криптосистемы такого типа будут дискредитированы. Например, ранее считалось, что задача укладки рюкзака является NP-полной. В настоящее время известен метод решения такой задачи, позволяющий избежать полного перебора.

9.5. Стандарты шифрования

9.5.1. Российский стандарт на шифрование информации ГОСТ 28147-89

В Российской Федерации установлен государственный стандарт (ГОСТ 28147—89 [9]) на алгоритмы криптографического преобразования информации в ЭВМ, вычислительных комплексах и вычислительных сетях. Эти алгоритмы допускается использовать без ограничений для шифрования информации любого уровня секретности. Алгоритмы могут быть реализованы аппаратными и программными способами.

Стандартом определены следующие алгоритмы криптографического преобразования информации:

- простая замена;
- гаммирование;
- гаммирование с обратной связью;
- выработка имитовставки.

Общим для всех алгоритмов шифрования является использование ключа размерностью 256 бит, разделенного на восемь 32-разрядных двоичных слов, и разделение исходной шифруемой двоичной последовательности на блоки по 64 бита.

Сущность алгоритма *простой замены* состоит в следующем. Блок из 64 - х бит исходной последовательности разбивается на два двоичных слова A и B по 32 разряда. Слово A образуют младшие биты, а слово B - старшие биты блока. Эти слова подвергаются итерационной обработке с числом итераций равным i=32. Слово, находящееся на месте младших бит блока, (A на первой итерации) суммируется по mod 2^{32} с 32-разрядным словом ключа; разбивается на части по 4 бита в каждой (4-х разрядные входные векторы); с помощью специальных узлов замены каждый вектор заменятся на другой вектор (4 бита); полученные векторы объединяются в 32-разрядное слово, которое циклически сдвигается влево на 32 разряда и суммируется по mod 2 с другим 32-разрядным словом из 64-разрядного блока (слово B на первой итерации).

После выполнения первой итерации в блоке на месте младших бит будет расположено слово B, а слева преобразованное слово A.

На следующих итерациях операции над словами повторяются.

На каждой итерации i 32-разрядное слово ключа j (всего их 8) выбирается по следующему правилу:

$$j = \begin{cases} (i-1) \bmod 8, & \text{при } 1 < i < 24; \\ 32-i, & \text{при } i > 25; \\ 0, & \text{при } i=32. \end{cases}$$

Блок замены состоит из 8 узлов замены, которые выбираются поочередно. Узел замены представляет собой таблицу из шестнадцати строк, в каждой из которых находятся векторы замены (4 бита). Входной вектор определяет адрес строки в таблице, число из которой является выходным вектором замены. Информация в таблицы замены заносится заранее и изменяется редко.

Алгоритм *гаммирования* предусматривает сложение по mod 2 исходной последовательности бит с последовательностью бит гаммы. Гамма получается в соответствии с алгоритмом простой замены. При выработке гаммы используются две специальные константы, заданные в ГОСТ 28147-89, а также 64-разрядная двоичная последовательность - синхропосылка. Расшифрование информации возможно только при наличии синхропосылки, которая не является секретной и может в открытом виде храниться в памяти ЭВМ или передаваться по каналам связи.

Алгоритм *гаммирования с обратной связью* очень схож с алгоритмом гаммирования. Они различаются лишь действиями на первом шаге итерационного процесса шифрования.

В ГОСТ 28147-89 определен алгоритм выработки *имитовставки*. Она используется для защиты от навязывания ложной информации. Имитовставка является функцией преобразования исходной информации и секретного ключа. Она представляет собой двоичную последовательность длиной *к* бит. Значение параметра *к* выбирается с учетом вероятности навязывания ложной информации $P_н$, которая связана с параметром *к* соотношением:

$$P_н = 1/2\backslash$$

Алгоритм выработки имитовставки может быть представлен следующей последовательностью действий. Открытая информация разбивается на блоки T(i) (i = 1, 2,...,m), где *m* определяется объемом шифруемой информации. Объем каждого блока - 64 би-

та. Первый блок Т(1) подвергается преобразованию в соответствии с первыми 16-ю итерациями алгоритма простой замены. В качестве ключа используется ключ, по которому будет шифроваться исходная информация. Полученное 64-битовое двоичное слово суммируется по mod 2 со вторым блоком Т(2). Результат суммирования подвергается тем же итерационным преобразованиям, что и блок Т(1), а на завершающем этапе суммируется по mod 2 с третьим блоком Т(3). Эти действия повторяются для ***m-1*** блоков исходной информации. Если последний блок Т(т) не полный, то он дополняется соответствующим числом нулей до 64 разрядов. Этот блок суммируется по mod 2 с результатом, полученным при обработке Т(m-i) блока, и подвергается преобразованию в соответствии с первыми 16-ю итерациями алгоритма простой замены. Из полученного 64-разрядного блока выделяется слово длиной *к* бит, которое и является имитовставкой.

Имитовставка помещается в конце зашифрованной информации. При получении (считывании) этой информации осуществляется ее расшифрование. По расшифрованной информации определяется имитовставка и сравнивается с полученной (считанной) имитовставкой. Если имитовставки не совпадают, то считается, что вся расшифрованная информация является ложной.

9.5.2. Стандарт США на шифрование информации

Государственным стандартом на шифрование информации является стандарт **DES (Data Encryption Standard).** Алгоритм шифрования, положенный в основу стандарта, был разработан фирмой ШМ. После проверки специалистами Агентства Национальной Безопасности США алгоритм получил статус государственного стандарта. Стандарт DES используется федеральными департаментами для закрытия информации в автоматизированных системах, за исключением некоторых видов информации, определенных специальными актами. Кроме того, этот стандарт шифрования широко используется негосударственными организациями не только в США, но и во всем мире.

В стандарте DES исходная информация разбивается на блоки по 64 бита в каждом и подвергается криптографическому преобразованию с использованием ключа, длиной 56 или 64 бита [39].

Блоки исходной информации подвергаются итерационной обработке с использованием операций перестановки и функции шифрования. Для вычисления функции шифрования предусматривается получение 48-битового ключа из 64-битового, расширение 32-битового кода до 48-битового, преобразование 6-битового кода в 4-битовый и перестановка бит в 32-битовой последовательности [3].

Процесс расшифрования является инверсным по отношению к процессу шифрования и выполняется с использованием того же ключа, что и при шифровании.

9.6. Перспективы использования криптозащиты информации в КС

Криптостойкость рассмотренных методов шифрования определяется длиной ключа, которая для современных систем должна быть, по крайней мере, больше 90 бит.

Для особо ответственных применений секретным является не только ключ, но и алгоритм шифрования. Для повышения криптостойкости шифров могут использоваться несколько ключей (обычно три ключа). Зашифрованная с помощью первого ключа информация подвергается шифрованию с помощью второго ключа и т. д.

Предлагается использовать переменные алгоритмы шифрования. В этом случае ключ шифрования используется еще и для выбора конкретного алгоритма шифрования. Развитие этого направления шифрования сдерживает сложность строгого доказательства криптостойкости такого шифрования.

Привлекательность методов шифрования с использованием открытых ключей заключается, прежде всего, в отсутствии необходимости рассылки секретных ключей. Для распределенных на больших расстояниях объектов КС рассылка секретных ключей становится довольно сложной и трудоемкой задачей. Распространение систем с открытыми ключами сдерживается отсутствием доказательств невозможности получения секретных ключей, кроме как путем их полного перебора.

Перспективным направлением развития криптозащиты информации является стеганография. Комплексное использование

стеганографии и шифрования намного повышает крйптостойкость закрытой информации.

Контрольные вопросы

1. Дайте определение криптографической защиты информации.
2. Приведите классификацию методов криптографического преобразования информации и поясните сущность методов.
3. Назовите и охарактеризуйте методы шифрования.
4. Сравните наиболее распространенные стандарты шифрования.
5. Каковы перспективы криптозащиты информации в КС?

ГЛАВА 10
Компьютерные вирусы и механизмы борьбы с ними

Вредительские программы и, прежде всего, вирусы представляют очень серьезную опасность для информации в КС. Недооценка этой опасности может иметь серьезные последствия для информации пользователей. Вредит использованию всех возможностей КС и чрезмерное преувеличение опасности вирусов. Знание механизмов действия вирусов, методов и средств борьбы с ними позволяет эффективно организовать противодействие вирусам, свести к минимуму вероятность заражения и потерь от их воздействия.

Термин «компьютерный вирус» был введен сравнительно недавно - в середине 80-х годов. Малые размеры, способность быстро распространяться, размножаясь и внедряясь в объекты (заражая их), негативное воздействие на систему - все эти признаки биологических вирусов присущи и вредительским программам, получившим по этой причине название «компьютерные вирусы». Вместе с термином «вирус» при работе с компьютерными вирусами используются и другие медицинские термины: «заражение», «среда обитания», «профилактика» и др.

«Компьютерные вирусы» - это небольшие исполняемые или интерпретируемые программы, обладающие свойством распространения и самовоспроизведения (репликации) в КС. Вирусы могут выполнять изменение или уничтожение программного

обеспечения или данных, хранящихся в КС. В процессе распространения вирусы могут себя модифицировать.

10.1. Классификация компьютерных вирусов

.В настоящее время в мире насчитывается более 40 тысяч только зарегистрированных компьютерных вирусов. Так как подавляющее большинство современных вредительских программ обладают способностью к саморазмножению, то часто их относят к компьютерным вирусам. Все компьютерные вирусы могут быть классифицированы по следующим признакам [4,20]:

- по среде обитания;
- по способу заражения;
- по степени опасности деструктивных (вредительских) воздействий;
- по алгоритму функционирования.

По среде обитания компьютерные вирусы делятся на:

- сетевые;
- файловые;
- загрузочные;
- комбинированные.

Средой обитания *сетевых* вирусов являются элементы компьютерных сетей. *Файловые* вирусы размещаются в исполняемых файлах. *Загрузочные* вирусы находятся в загрузочных секторах (областях) внешних запоминающих устройств (boot-секторах). Иногда загрузочные вирусы называют бутовыми. *Комбинированные* вирусы размещаются в нескольких средах обитания. Примером таких вирусов служат загрузочно-файловые вирусы. Эти вирусы могут размещаться как в загрузочных секторах накопителей на магнитных дисках, так и в теле загрузочных файлов.

По способу заражения среды обитания компьютерные вирусы делятся на:

- резидентные;
- нерезидентные.

Резидентные вирусы после их активизации полностью или частично перемещаются из среды обитания (сеть, загрузочный сектор, файл) в оперативную память ЭВМ. Эти вирусы, исполь-

зуя, как правило, привилегированные режимы работы, разрешенные только операционной системе, заражают среду обитания и при выполнении определенных условий реализуют деструктивную функцию. В отличие от резидентных ***нерезидентные*** вирусы попадают в оперативную память ЭВМ только на время их активности, в течение которого выполняют деструктивную функцию и функцию заражения. Затем вирусы полностью покидают оперативную память, оставаясь в среде обитания. Если вирус помещает в оперативную память программу, которая не заражает среду обитания, то такой вирус считается нерезидентным.

Арсенал деструктивных или вредительских возможностей компьютерных вирусов весьма обширен. Деструктивные возможности вирусов зависят от целей и квалификации их создателя, а также от особенностей компьютерных систем.

По **степени опасности для информационных ресурсов** пользователя компьютерные вирусы можно разделить на:

- *безвредные вирусы;*
- *опасные вирусы;*
- *очень опасные вирусы.*

Безвредные компьютерные вирусы создаются авторами, которые не ставят себе цели нанести какой-либо ущерб ресурсам КС. Ими, как правило, движет желание показать свои возможности программиста. Другими словами, создание компьютерных вирусов для таких людей - своеобразная попытка самоутверждения. Деструктивное воздействие таких вирусов сводится к выводу на экран монитора невинных текстов и картинок, исполнению музыкальных фрагментов и т. п.

Однако при всей кажущейся безобидности таких вирусов они наносят определенный ущерб КС. Во-первых, такие вирусы расходуют ресурсы КС, в той или иной мере снижая ее эффективность функционирования. Во-вторых, компьютерные вирусы могут содержать ошибки, вызывающие опасные последствия для информационных ресурсов КС. Кроме того, при модернизации операционной системы или аппаратных средств КС вирусы, созданные ранее, могут приводить к нарушениям штатного алгоритма работы системы.

К ***опасным*** относятся вирусы, которые вызывают существенное снижение эффективности КС, но не приводящие к наруше-

нию целостности и конфиденциальности информации, хранящей*[1] ся в запоминающих устройствах. Последствия таких вирусов МОЙ гут быть ликвидированы без особых затрат материальных и временных ресурсов. Примерами таких вирусов являются вирусы, занимающие память ЭВМ и каналы связи, но не блокирующие работу сети; вирусы, вызывающие необходимость повторного вын полнения программ, перезагрузки операционной системы или по-« вторной передачи данных по каналам связи и т. п.

Очень опасными следует считать вирусы, вызывающие нарун* шение конфиденциальности, уничтожение, необратимую модификацию (в том числе и шифрование) информации, а также вирусы, блокирующие доступ к информации, приводящие к отказу аппаратных средств и наносящие ущерб здоровью пользователям. Такие вирусы стирают отдельные файлы, системные области памяти, форматируют диски, получают несанкционированный доступ к информации, шифруют данные и т. п.

Известны публикации, в которых упоминаются вирусы, вызывающие неисправности аппаратных средств. Предполагается, что на резонансной частоте движущиеся части электромеханических устройств, например в системе позиционирования накопителя на магнитных дисках, могут быть разрушены. Именно такой режим и может быть создан с помощью программы-вируса. Другие авторы утверждают, что возможно задание режимов интенсивного использования отдельных электронных схем (например, больших интегральных схем), при которых наступает их перегрев и выход из строя.

Использование в современных ПЭВМ постоянной памяти с возможностью перезаписи привело к появлению вирусов, изменяющих программы BIOS, что приводит к необходимости замены постоянных запоминающих устройств.

Возможны также воздействия на психику человека - оператора ЭВМ с помощью подбора видеоизображения, выдаваемого на экран монитора с определенной частотой (каждый двадцать пятый кадр). Встроенные кадры этой видеоинформации воспринимаются человеком на подсознательном уровне. В результате такого воздействия возможно нанесение серьезного ущерба психике человека. В 1997 году 700 японцев попали в больницу с признаками эпилепсии после просмотра компьютерного мультфильма по телеви-

дению. Предполагают, что именно таким образом была опробована возможность воздействия на человека с помощью встраивания 25-го кадра [57].

В соответствии с особенностями алгоритма функционирования вирусы можно разделить на два класса:

- вирусы, не изменяющие среду обитания (файлы и секторы) при распространении;
- вирусы, изменяющие среду обитания при распространении.

В свою очередь, вирусы, *не изменяющие среду обитания,* могут быть разделены на две группы:

- *вирусы-«спутники» (compañion);*
- *вирусы-«черви» (worm).*

Вирусы-«спутники» не изменяют файлы. Механизм их действия состоит в создании копий исполняемых файлов. Например, в MS DOS такие вирусы создают копии для файлов, имеющих расширение .EXE. Копии присваивается то же имя, что и исполняемому файлу, но расширение изменяется на .COM. При запуске файла с общим именем операционная система первым загружает на выполнение файл с расширением .COM, который является программой-вирусом. Файл-вирус запускает затем и файл с расширением .EXE.

Вирусы-«черви» попадают в рабочую станцию из сети, вычисляют адреса рассылки вируса по другим абонентам сети и осуществляют передачу вируса. Вирус не изменяет файлов и не записывается в загрузочные секторы дисков. Некоторые вирусы-«черви» создают рабочие копии вируса на диске, другие - размещаются только в оперативной памяти ЭВМ.

По сложности, степени совершенства и особенностям маскировки алгоритмов вирусы, *изменяющие среду обитания,* делятся на:

- *студенческие;*
- *«стеле» - вирусы (вирусы-невидимки);*
- *полиморфные.*

К *студенческим* относят вирусы, создатели которых имеют низкую квалификацию. Такие вирусы, как правило, являются нерезидентными, часто содержат ошибки, довольно просто обнаруживаются и удаляются.

«Стеле»- вирусы и полиморфные вирусы создаются квалифицированными специалистами, хорошо знающими принцип работы аппаратных средств и операционной системы, а также владеющими навыками работы с машиноориентированными системами программирования.

«Стелс»-вирусы маскируют свое присутствие в среде обитания путем перехвата обращений операционной системы к пораженным файлам, секторам и переадресуют ОС к незараженным участкам информации. Вирус является резидентным, маскируется под программы ОС, может перемещаться в памяти. Такие вирусы активизируются при возникновении прерываний, выполняют определенные действия, в том числе и по маскировке, и только затем управление передается на программы ОС, обрабатывающие эти прерывания. «Стеле»- вирусы обладают способностью противодействовать резидентным антивирусным средствам.

Полиморфные вирусы не имеют постоянных опознавательных групп - сигнатур. Обычные вирусы для распознавания факта заражения среды обитания размещают в зараженном объекте специальную опознавательную двоичную последовательность или последовательность символов (сигнатуру), которая однозначно идентифицирует зараженность файла или сектора. Сигнатуры используются на этапе распространения вирусов для того, чтобы избежать многократного заражения одних и тех же объектов, так как при многократном заражении объекта значительно возрастает вероятность обнаружения вируса. Для устранения демаскирующих признаков полиморфные вирусы используют шифрование тела вируса и модификацию программы шифрования. За счет такого преобразования полиморфные вирусы не имеют совпадений кодов.

Любой вирус, независимо от принадлежности к определенным классам, должен иметь три функциональных блока: блок заражения (распространения), блок маскирования и блок выполнения деструктивных действий. Разделение на функциональные блоки означает, что к определенному блоку относятся команды программы вируса, выполняющие одну из трех функций, независимо от места нахождения команд в теле вируса.

После передачи управления вирусу, как правило, выполняются определенные функции блока маскировки. Например, осущест-

вляется расшифрование тела вируса. Затем вирус осуществляет функцию внедрения в незараженную среду обитания. Если вирусом должны выполняться деструктивные воздействия, то они выполняются либо безусловно, либо при выполнении определенных условий.

Завершает работу вируса всегда блок маскирования. При этом выполняются, например, следующие действия: шифрование вируса (если функция шифрования реализована), восстановление старой даты изменения файла, восстановление атрибутов файла, корректировка таблиц ОС и др.

Последней командой вируса выполняется команда перехода на выполнение зараженных файлов или на выполнение программ ОС.

Для удобства работы с известными вирусами используются каталоги вирусов. В каталог помещаются следующие сведения о стандартных свойствах вируса: имя, длина, заражаемые файлы, место внедрения в файл, метод заражения, способ внедрения в ОП для резидентных вирусов, вызываемые эффекты, наличие (отсутствие) деструктивной функции и ошибки. Наличие каталогов позволяет при описании вирусов указывать только особые свойства, опуская стандартные свойства и действия.

10.2. Файловые вирусы

10.2.1. Структура файлового вируса

Файловые вирусы могут внедряться только в исполняемые файлы: командные файлы (файлы, состоящие из команд операционной системы), саморазархивирующиеся файлы, пользовательские и системные программы в машинных кодах, а также в документы (таблицы), имеющие макрокоманды. Макрокоманды или макросы представляют собой исполняемые программы для автоматизации работы с документами (таблицами). Поэтому такие документы (таблицы) можно рассматривать как исполняемый файл.

Для IBM - совместимых ПЭВМ вирус может внедряться в файлы следующих типов: командные файлы (BAT), загружаемые драйверы (SYS), программы в машинных (двоичных) кодах (EXE, COM), документы Word (DOC) с версии 6.0 и выше, таблицы

EXCEL (XLS). Макровирусы могут внедрятся и в другие файлы, содержащие макрокоманды.

Файловые вирусы могут размещаться в начале, середине и конце заражаемого файла (рис. 22).

Независимо от места расположения вируса в теле зараженного! файла после передачи управления файлу первыми выполняются команды вируса.

В начало файла вирус внедряется одним из трех способов. Первый из них заключается в переписывании начала файла в его конец, а на освободившееся место записывается вирус. Второй способ предполагает считывание вируса и зараженного файла в оперативную память, объединение их в один файл и запись его на место файла. При третьем способе заражения вирус записывается в начало файла без сохранения содержимого. В этом случае зараженный файл становится неработоспособным.

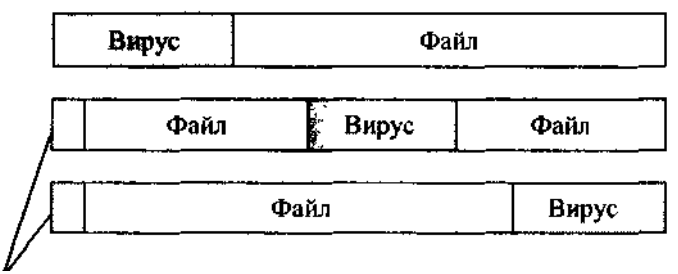


Рис. 22. Варианты размещения вирусов в файлах

В середину файла вирус может быть записан также различными способами. Файл может «раздвигаться», а в освободившееся место может быть записан вирус. Вирус может внедряться в середину файла без сохранения участка файла, на место которого помещается вирус. Есть и более экзотические способы внедрения вируса в середину файла. Например, вирус «Mutant» применяет метод сжатия отдельных участков файла, при этом длина файла после внедрения вируса может не измениться.

Чаще всего вирус внедряется в конец файла. При этом, как и в случае с внедрением вируса в середину файла, первые команды файла заменяются командами перехода на тело вируса.

10.2.2. Алгоритм работы файлового вируса

Несмотря на многообразие файловых вирусов, можно выделить действия и порядок их выполнения, которые присутствуют при реализации большинства вирусов этого класса. Такой обобщенный алгоритм может быть представлен в виде следующей последовательности шагов:

Шаг 1. Резидентный вирус проверяет, заражена ли оперативная память, и при необходимости заражает ее. Нерезидентный вирус ищет незараженные файлы и заражает их.

Шаг 2. Выполняются действия по сохранению работоспособности программы, в файл которой внедряется вирус (восстановление первых байт программы, настройка адресов программ и т. д.)

Шаг 3. Осуществляется деструктивная функция вируса, если выполняются соответствующие условия.

Шаг 4. Передается управление программе, в файле которой находится вирус.

При реализации конкретных вирусов состав действий и их последовательность могут отличаться от приведенных в алгоритме.

10.2.3. Особенности макровирусов

Особое место среди файловых вирусов занимают макровирусы. Макровирусы представляют собой вредительские программы, написанные на макроязыках, встроенных в текстовые редакторы, электронные таблицы и др.

Для существования вирусов в конкретной системе (редакторе) необходимо, чтобы встроенный в нее макроязык,имел следующие возможности:

- привязку программы на макроязыке к конкретному файлу;
- копирование макропрограмм из одного файла в другой;
- получение управления макропрограммой без вмешательства пользователя.

Таким условиям отвечают редакторы MS Word, MS Office, Ami Pro, табличный процессор MS Excel. В этих системах используются макроязыки **Word** Basic и Visual Basic.

При выполнении определенных действий над файлами, содержащими макропрограммы (открытие, сохранение, закрытие и

т. д.), автоматически выполняются макропрограммы файлов. При этом управление получают макровирусы, которые сохраняют активность до тех пор, пока активен соответствующий редактор (процессор). Поэтому при работе с другим файлом в «зараженном редакторе (процессоре)», он также заражается. Здесь прослеживается аналогия с резидентными вирусами по механизму заражения. Для получения управления макровирусы, заражающие файлы MS Office, как правило, используют один из приемов:

1) в вирусе имеется автомакрос (выполняется автоматически, при открытии документа, таблицы);

2) в вирусе переопределен один из стандартных макросов, который выполняется при выборе определенного пункта меню;

3) макрос вируса автоматически вызывается на выполнение при нажатии определенной клавиши или комбинаций клавиш.

Первый макровирус WinWord. Concept, поражающий документы Word, появился летом 1995 года. Вредительская функция этого вируса заключается в изменении формата документов текстового редактора Word в формат файлов стилей. Другой макровирус WinWord Nuclear уже не столь безобиден. Он дописывает фразу с требованием запрещения ядерных испытаний, проводимых Францией в Тихом океане. Кроме того, этот вирус ежегодно 5 апреля пытается уничтожить важные системные файлы.

10.3. Загрузочные вирусы

Загрузочные вирусы заражают загрузочные (Boot) сектора гибких дисков и Boot-сектора или Master Boot Record (MBR) жестких дисков (рис. 23).

Загрузочные вирусы являются резидентными. Заражение происходит при загрузке операционной системы с дисков.

После включения ЭВМ осуществляется контроль ее работоспособности с помощью программы, записанной в постоянном запоминающем устройстве. Если проверка завершилась успешно, то осуществляется считывание первого сектора с гибкого или жесткого диска. Порядок использования дисководов для загрузки задается пользователем при помощи программы Setup. Если диск, с которого производится загрузка ОС заражен загрузочным вирусом, то обычно выполняются следующие шаги:

Шаг 1. Считанный из 1-го сектора диска загрузочный вирус (часть вируса) получает управление, уменьшает объем свободной памяти ОП и считывает с диска тело вируса.

Шаг 2. Вирус переписывает сам себя в другую область Oil, чаще всего - в старшие адреса памяти.

Шаг 3. Устанавливаются необходимые вектора прерываний (вирус резидентный).

Шаг 4. При выполнении определенных условий производятся деструктивные действия.

Шаг 5. Копируется Boot-сектор в ОП и передается ему управление.

Рис. 23. Размещение загрузочного вируса на диске

Если вирус был активизирован с гибкого диска, то он записывается в загрузочный сектор жесткого диска. Активный вирус, постоянно находясь в ОП, заражает загрузочные сектора всех гибких дисков, а не только системные диски.

Заражение рабочих гибких дисков загрузочными вирусами выполняется в расчете на ошибочные действия пользователя ЭВМ в момент загрузки ОС. Если установлен порядок загрузки ОС сначала с гибкого диска, а затем - с жесткого, то при наличии гибкого диска в накопители будет считан 1-й сектор с гибкого диска. Если диск был заражен, то этого достаточно для заражения ЭВМ. Такая ситуация наиболее часто имеет место при перезагрузке ОС после «зависаний» или отказов ЭВМ.

10.4. Вирусы и операционные системы

Программы-вирусы создаются для ЭВМ определенного типа, работающих с конкретными ОС. Для одних ОС созданы тысячи вирусов. В качестве примера можно привести ОС MS DOS, устанавливаемую на ЮМ совместимые персональные компьютеры.

Для ОС Unix, OS/2, Windows и некоторых других ОС известно незначительное количество вирусов. Привлекательность ОС для создателей вирусов определяется следующими факторами:

- распространенность ОС;
- отсутствие встроенных антивирусных механизмов;
- относительная простота;
- продолжительность эксплуатации.

Все приведенные факторы характерны для MS DOS. Наличие антивирусных механизмов, сложность систем и относительно малые сроки эксплуатации делают задачу создания вирусов трудно решаемой. Поэтому авторы вирусов для Windows, OS/2 часто прибегают к использованию из этих операционных систем хорошо знакомой MS DOS для внедрения вирусов.

Главным недостатком MS DOS является возможность полного и бесконтрольного доступа любой активной программы ко всем системным ресурсам ЭВМ, включая и модули самой ОС.

Операционная система Microsoft Windows 3.1 и ее модификация Microsoft Windows for Workgroups 3.11 не являются самостоятельными ОС, а больше похожи на очень большие программы MS DOS. В этих ОС введены ограничения на доступ к ОП. Каждая программа получает доступ только к своему виртуальному пространству ОП. Доступ же к дискам, файлам и портам внешних устройств не ограничены. Сохраняют работоспособность и загрузочные вирусы, разработанные для MS DOS, так как они получают управление еще до загрузки Microsoft Windows 3.1 ив этот период времени действия их ничем не ограничены.

Слабость защитных функций ОС Microsoft Windows 95/98 также объясняется совместимостью с MS DOS. Эта ОС имеет такую же устойчивость к воздействию вирусов, как и Microsoft Windows 3.1. К тому же в этой ОС получили распространение и макровирусы.

Значительно лучше защищена от вирусов операционная система ЮМ OS/2. Эта система полностью независима от MS DOS. Все программы, выполняемые в OS/2, работают в отдельных адресных пространствах, что полностью исключает возможность взаимного влияния программ. Существует возможность запретить рабочим программам (несистемным) иметь доступ к портам периферийных устройств. Если ЭВМ с Microsoft OS/2 используется

в качестве файл-сервера IBM LAN Server, то с помощью драйвера 386 HPFS можно указывать права доступа к каталогам и файлам. Можно также защитить каталоги от записи в файлы, содержащиеся в них. В этой системе существует возможность выполнения программ MS DOS. Но в OS/2 для вирусов, созданных для MS DOS, гораздо меньше возможностей.

Хорошую защиту от вирусов имеют сетевые операционные системы Microsoft Windows NT и Novell Net Ware, а также операционная система Windows 2000.

10.5. Методы и средства борьбы с вирусами

Массовое распространение вирусов, серьезность последствий их воздействия на ресурсы КС вызвали необходимость разработки и использования специальных антивирусных средств и методов их применения. Антивирусные средства применяются для решения следующих задач [55]:

- обнаружение вирусов в КС;
- блокирование работы программ-вирусов;
- устранение последствий воздействия вирусов.

Обнаружение вирусов желательно осуществлять на стадии их внедрения или, по крайней мере, до начала осуществления деструктивных функций вирусов. Необходимо отметить, что не существует антивирусных средств, гарантирующих обнаружение всех возможных вирусов.

При обнаружении вируса необходимо сразу же прекратить работу программы-вируса, чтобы минимизировать ущерб от его воздействия на систему.

Устранение последствий воздействия вирусов ведется в двух направлениях:

- удаление вирусов;
- восстановление (при необходимости) файлов, областей памяти.

Восстановление системы зависит от типа вируса, а также от момента времени обнаружения вируса по отношению к началу деструктивных действий. Восстановление информации без использования дублирующей информации может быть невыполнимым, если вирусы при внедрении не сохраняют информацию, на

место которой они помещаются в память, а также, если деструктивные действия уже начались, и они предусматривают изменения информации.

Для борьбы с вирусами используются программные и аппаратно-программные средства, которые применяются в определенной последовательности и комбинации, образуя методы борьбы с вирусами. Можно выделить методы обнаружения вирусов и методы удаления вирусов.

10.5.1. Методы обнаружения вирусов

Известны следующие методы обнаружения вирусов [55]:

- сканирование;
- обнаружение изменений;
- эвристический анализ;
- использование резидентных сторожей;
- вакцинирование программ;
- аппаратно-программная защита от вирусов.

Сканирование - один из самых простых методов обнаружения вирусов. Сканирование осуществляется программой-сканером, которая просматривает файлы в поисках опознавательной части вируса - сигнатуры. Программа фиксирует наличие уже известных вирусов, за исключением полиморфных вирусов, которые применяют шифрование тела вируса, изменяя при этом каждый раз и сигнатуру. Программы-сканеры могут хранить не сигнатуры известных вирусов, а их контрольные суммы. Программы-сканеры часто могут удалять обнаруженные вирусы. Такие программы называются полифагами.

Метод сканирования применим для обнаружения вирусов, сигнатуры которых уже выделены и являются постоянными. Для эффективного использования метода необходимо регулярное обновление сведений о новых вирусах.

Самой известной программой-сканером в России является Aidstest Дмитрия Лозинского.

Метод обнаружения изменении базируется на использовании программ-ревизоров. Эти программы определяют и запоминают характеристики всех областей на дисках, в которых обычно размещаются вирусы. При периодическом выполнении программ-

ревизоров сравниваются хранящиеся характеристики и характеристики, получаемые при контроле областей дисков. По результатам ревизии программа выдает сведения о предположительном наличии вирусов.

Обычно программы-ревизоры запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, характеристики всех контролируемых файлов, каталогов и номера дефектных кластеров. Могут контролироваться также объем установленной оперативной памяти, количество подключенных к компьютеру дисков и их параметры.

Главным достоинством метода является возможность обнаружения вирусов всех типов, а также новых неизвестных вирусов. Совершенные программы-ревизоры обнаруживают даже «стеле»-вирусы. Например, программа-ревизор Adinf, разработанная Д. Ю Мостовым, работает с диском непосредственно по секторам через BIOS. Это не позволяет использовать «стелс»-вирусам возможность перехвата прерываний и «подставки» для контроля нужной вирусу области памяти.

Имеются у этого метода и недостатки. С помощью программ-ревизоров невозможно определить вирус в файлах, которые поступают в систему уже зараженными. Вирусы будут обнаружены только после размножения в системе.

Программы-ревизоры непригодны для обнаружения заражения макровирусами, так как документы и таблицы очень часто изменяются.

Эвристический анализ сравнительно недавно начал использоваться для обнаружения вирусов. Как и метод обнаружения изменений, данный метод позволяет определять неизвестные вирусы, но не требует предварительного сбора, обработки и хранения информации о файловой системе.

Сущность эвристического анализа заключается в проверке возможных сред обитания вирусов и выявление в них команд (групп команд), характерных для вирусов. Такими командами могут быть команды создания резидентных модулей в оперативной памяти, команды прямого обращения к дискам, минуя ОС. Эвристические анализаторы при обнаружении «подозрительных» команд в файлах или загрузочных секторах выдают сообщение о возможном заражении. После получения таких сообщений необ-

ходимо тщательно проверить предположительно зараженные файлы и загрузочные сектора всеми имеющимися антивирусными средствами. Эвристический анализатор имеется, например, в антивирусной программе Doctor Web.

Метод использования *резидентных сторожей* основан на применении программ, которые постоянно находятся в ОП ЭВМ и отслеживают все действия остальных программ.

В случае выполнения какой-либо программой подозрительных действий (обращение для записи в загрузочные сектора, помещение в ОП резидентных модулей, попытки перехвата прерываний и т. п.) резидентный сторож выдает сообщение пользователю. Программа-сторож может загружать на выполнение другие антивирусные программы для проверки «подозрительных» программ, а также для контроля всех поступающих извне файлов (со сменных дисков, по сети).

Существенным недостатком данного метода является значительный процент ложных тревог, что мешает работе пользователя, вызывает раздражение и желание отказаться от использования резидентных сторожей. Примером резидентного сторожа может служить программа Vsafe, входящая в состав MS DOS.

Под *вакцинацией программ* понимается создание специального модуля для контроля ее целостности. В качестве характеристики целостности файла обычно используется контрольная сумма. При заражении вакцинированного файла, модуль контроля обнаруживает изменение контрольной суммы и сообщает об этом пользователю. Метод позволяет обнаруживать все вирусы, в том числе и незнакомые, за исключением «стеле»- вирусов.

Самым надежным методом защиты от вирусов является использование *аппаратно-программных антивирусных средств.* В настоящее время для защиты ПЭВМ используются специальные контроллеры и их программное обеспечение. Контроллер устанавливается в разъем расширения и имеет доступ к общей шине. Это позволяет ему контролировать все обращения к дисковой системе. В программном обеспечении контроллера запоминаются области на дисках, изменение которых в обычных режимах работы не допускается. Таким образом, можно установить защиту на изменение главной загрузочной записи, загрузочных секторов, файлов конфигурации, исполняемых файлов и др.

При выполнении запретных действий любой программой контроллер выдает соответствующее сообщение пользователю **и** блокирует работу ПЭВМ.

Аппаратно-программные антивирусные средства обладают рядом достоинств перед программными:

- работают постоянно;
- обнаруживают все вирусы, независимо от механизма их действия;
- блокируют неразрешенные действия, являющиеся результатом работы вируса или неквалифицированного пользователя.

Недостаток у этих средств один - зависимость от аппаратных средств ПЭВМ. Изменение последних ведет к необходимости замены контроллера.

Примером аппаратно-программной защиты от вирусов может служить комплекс Sheriff.

10.5.2. Методы удаления последствий заражения вирусами

В процессе удаления последствий заражения вирусами осуществляется удаление вирусов, а также восстановление файлов и областей памяти, в которых находился вирус. Существует два метода удаления последствий воздействия вирусов антивирусными программами.

Первый метод предполагает восстановление системы после воздействия известных вирусов. Разработчик программы-фага, удаляющей вирус, должен знать структуру вируса и его характеристики размещения в среде обитания.

Второй метод позволяет восстанавливать файлы и загрузочные сектора, зараженные неизвестными вирусами. Для восстановления файлов программа восстановления должна заблаговременно создать и хранить информацию о файлах, полученную в условиях отсутствия вирусов. Имея информацию о незараженном файле и используя сведения об общих принципах работы вирусов, осуществляется восстановление файлов. Если вирус подверг файл необратимым изменениям, то восстановление возможно только с использованием резервной копии или с дистрибутива. При их отсутствии существует только один выход - уничтожить файл и восстановить его вручную.

Если антивирусная программа не может восстановить главную загрузочную запись или загрузочные сектора, то можно попытаться это сделать вручную. В случае неудачи следует отформатировать диск и установить ОС.

Существуют вирусы, которые, попадая в ЭВМ, становятся частью его ОС. Если просто удалить такой вирус, то система становится неработоспособной.

Одним из таких вирусов является вирус One Half. При загрузке ЭВМ вирус постепенно зашифровывает жесткий диск. При обращении к уже зашифрованным секторам резидентный вирус One Half перехватывает обращения и расшифровывает информацию. Удаление вируса приведет к невозможности использовать зашифрованную часть диска. При удалении такого вируса необходимо сначала расшифровать информацию на диске. Для этого необходимо знать механизм действия вируса.

10.6. Профилактика заражения вирусами компьютерных систем

Чтобы обезопасить ЭВМ от воздействия вирусов, пользователь, прежде всего, должен иметь представление о механизме действия вирусов, чтобы адекватно оценивать возможность и последствия заражения КС. Главным же условием безопасной работы в КС является соблюдение ряда правил, которые апробированы на практике и показали свою высокую эффективность.

Правило первое. Использование программных продуктов, полученных законным официальным путем.

Вероятность наличия вируса в пиратской копии во много раз выше, чем в официально полученном программном обеспечении.

Правило второе. Дублирование информации.

Прежде всего, необходимо сохранять дистрибутивные носители программного обеспечения. При этом запись на носители, допускающие выполнение этой операции, должна быть, по возможности, заблокирована. Следует особо позаботиться о сохранении рабочей информации. Предпочтительнее регулярно создавать копии рабочих файлов на съемных машинных носителях информации с защитой от записи. Если создается копия на несъемном носителе, то желательно ее создавать на других ВЗУ или ЭВМ. Ко-

пируется либо весь файл, либо **только вносимые изменения.** Последний вариант применим, например, **при** работе **с** базами данных.

Правило третье. Регулярно использовать антивирусные средства. Перед началом работы целесообразно выполнять программы-сканеры и программы-ревизоры (Aidstest и Adinf). Антивирусные средства должны регулярно обновляться.

Правило четвертое. Особую осторожность следует проявлять при использовании новых съемных носителей информации и новых файлов. Новые дискеты обязательно должны быть проверены на отсутствие загрузочных и файловых вирусов, а полученные файлы - на наличие файловых вирусов. Проверка осуществляется программами-сканерами и программами, осуществляющими эвристический анализ (Aidstest, Doctor Web, AntiVirus). При первом выполнении исполняемого файла используются резидентные сторожа. При работе с полученными документами и таблицами целесообразно запретить выполнение макрокоманд средствами, встроенными в текстовые и табличные редакторы (MS Word, MS Excel), до завершения полной проверки этих файлов.

Правило пятое. При работе в распределенных системах или в системах коллективного пользования целесообразно новые сменные носители информации и вводимые в систему файлы проверять на специально выделенных для этой цели ЭВМ. Целесообразно для этого использовать автоматизированное рабочее место администратора системы или лица, отвечающего за безопасность информации. Только после всесторонней антивирусной проверки дисков и файлов они могут передаваться пользователям системы.

Правило шестое. Если не предполагается осуществлять запись информации на носитель, то необходимо заблокировать выполнение этой операции. На магнитных дискетах 3,5 дюйма для этого достаточно открыть квадратное отверстие.

Постоянное следование всем приведенным рекомендациям позволяет значительно уменьшить вероятность заражения программными вирусами и защищает пользователя от безвозвратных потерь информации.

В особо ответственных системах для борьбы с вирусами необходимо использовать аппаратно-программные средства (например, Sheriff).

10.7. Порядок действий пользователя при обнаружении заражения ЭВМ вирусами

Даже при скрупулезном выполнении всех правил профилактики возможность заражения ЭВМ компьютерными вирусами полностью исключить нельзя. И если вирус все же попал в КС, то последствия его пребывания можно свести к минимуму, придерживаясь определенной последовательности действий.

О наличии вируса в КС пользователь может судить по следующим событиям:

- появление сообщений антивирусных средств о заражении или о предполагаемом заражении;
- явные проявления присутствия вируса, такие как сообщения, выдаваемые на монитор или принтер, звуковые эффекты, уничтожение файлов и другие аналогичные действия, однозначно указывающие на наличие вируса в КС;
- неявные проявления заражения, которые могут быть вызваны и другими причинами, например, сбоями или отказами аппаратных и программных средств КС.

К неявным проявлениям наличия вирусов в КС можно отнести «зависания» системы, замедление выполнения определенных действий, нарушение адресации, сбои устройств и тому подобное.

Получив информацию о предполагаемом заражении, пользователь должен убедиться в этом. Решить такую задачу можно с помощью всего комплекса антивирусных средств. Убедившись в том, что заражение произошло, пользователю следует выполнить следующую последовательность шагов:

Шаг 1. Выключить ЭВМ для уничтожения резидентных вирусов.

Шаг 2. Осуществить загрузку эталонной операционной системы со сменного носителя информации, в которой отсутствуют вирусы.

Шаг 3. Сохранить на сменных носителях информации важные для вас файлы, которые не имеют резервных копий.

Шаг 4. Использовать антивирусные средства для удаления вирусов и восстановления файлов, областей памяти. Если работоспособность ЭВМ восстановлена, то осуществляется переход к шагу 8, иначе - к шагу 5.

Шаг 5. Осуществить полное стирание и разметку (форматирование) несъемных внешних запоминающих устройств. В ПЭВМ для этого могут быть использованы программы MS-DOS FDISK и FORMAT. Программа форматирования FORMAT не удаляет главную загрузочную запись на жестком диске, в которой может находиться загрузочный вирус [55]. Поэтому необходимо выполнить программу FDISK с недокументированным параметром **MBR,** создать с помощью этой же программы разделы и логические диски на жестком диске. Затем выполняется программа FORMAT для всех логических дисков.

Шаг 6. Восстановить ОС, другие программные системы и файлы с дистрибутивов и резервных копий, созданных до заражения.

Шаг 7. Тщательно проверить файлы, сохраненные после обнаружения заражения, и, при необходимости, удалить вирусы и восстановить файлы;

Шаг 8. Завершить восстановление информации всесторонней проверкой ЭВМ с помощью всех имеющихся в распоряжении пользователя антивирусных средств.

При выполнении рекомендаций по профилактике заражения компьютерными вирусами, а также при умелых и своевременных действиях в случае заражения,вирусами, ущерб информационным ресурсам КС может быть сведен к минимуму.

Контрольные вопросы

1. Назовите признаки классификации компьютерных вирусов.
2. Поясните принцип действия «стелс»-вирусов и полиморфных вирусов.
3. Приведите структуру файлового вируса и поясните алгоритм его работы.
4. В чем заключаются особенности алгоритмов функционирования макровирусов и загрузочных вирусов?
5. Дайте характеристику методов обнаружения вирусов.
6. Назовите методы удаления последствий заражения вирусами.
7. Перечислите профилактические меры предотвращения заражения вирусами КС.
8. Приведите порядок действий пользователя при заражении ЭВМ вирусами.

ГЛАВА 11
Защита информации в распределенных КС

11.1. Архитектура распределенных КС

Под распределенными понимаются КС, которые не располагаются на одной контролируемой территории, на одном объекте.

В общем случае **распределенная** компьютерная система (РКС) представляет собой множество сосредоточенных КС, связанных в единую систему с помощью коммуникационной подсистемы. **Сосредоточенными** КС могут быть отдельные ЭВМ, в том числе и ПЭВМ, вычислительные системы и комплексы, а также локальные вычислительные сети (ЛВС). В настоящее время практически не используются неинтеллектуальные абонентские пункты, не имеющие в своем составе ЭВМ. Поэтому правомочно считать, что наименьшей структурной единицей РКС является ЭВМ (рис. 24). Распределенные КС строятся по сетевым технологиям и представляют собой вычислительные сети (ВСт). Коммуникационная подсистема включает в себя:

- коммуникационные модули (КМ);
- каналы связи;
- концентраторы;
- межсетевые шлюзы (мосты).

Основной функцией ***коммуникационных*** *модулей* является передача полученного пакета к другому КМ или абонентскому пункту в соответствии с маршрутом передачи. Коммуникационный модуль называют также центром коммутации пакетов.

Каналы связи объединяют элементы сети в единую сеть. Каналы могут иметь различную скорость передачи данных. ***Концентраторы*** используются для уплотнения информации перед передачей ее по высокоскоростным каналам. ***Межсетевые шлюзы и мосты*** используются для связи сети с ЛВС или для связи сегментов глобальных сетей. С помощью мостов связываются сегменты сети с одинаковыми сетевыми протоколами.

В любой РКС в соответствии с функциональным назначением может быть выделено три подсистемы:

- пользовательская подсистема;
- подсистема управления;
- коммуникационная подсистема.

Пользовательская или ***абонентская*** подсистема включает в себя компьютерные системы пользователей (абонентов) и предназначается для удовлетворения потребностей пользователей в хранении, обработке и получении информации.

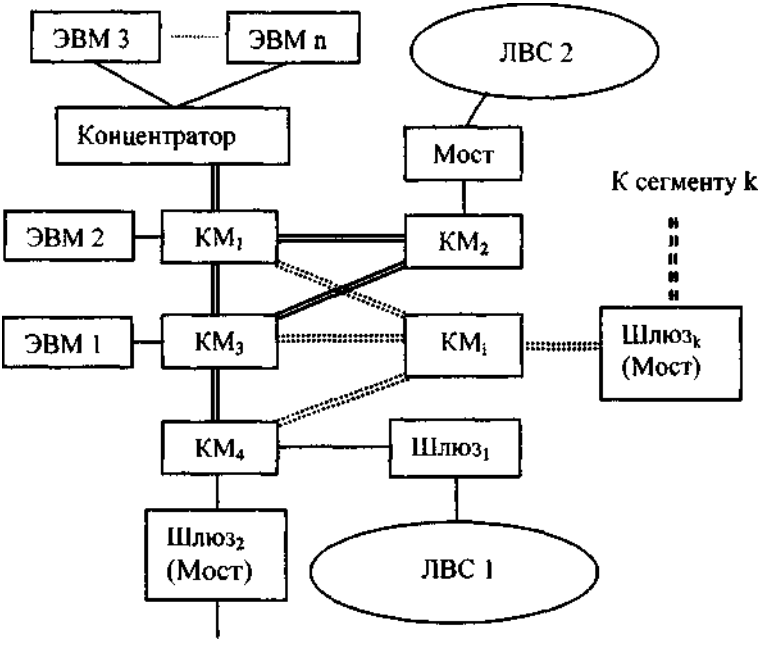


Рис. 24. Фрагмент распределенной компьютерной системы

Наличие ***подсистемы управления*** позволяет объединить **все** элементы РКС в единую систему, **в** которой взаимодействие элементов осуществляется по единым правилам. Подсистема обеспечивает взаимодействие элементов системы путем сбора и анализа служебной информации и воздействия на элементы с целью создания оптимальных условий для функционирования всей сети.

Коммуникационная подсистема обеспечивает передачу информации в сети в интересах пользователей и управления РКС.

Функционирование РКС можно рассматривать как взаимодействие удаленных процессов через коммуникационную подсистему. Процессы вычислительной сети порождаются пользователями (абонентами) и другими процессами. Взаимодействие удаленных процессов заключается в обмене файлами, пересылке сообщений по электронной почте, посылке заявок на выполнение программ и получение результатов, обращении к базам данных и т. д.

11.2. Особенности защиты информации в РКС

С точки зрения защиты информации в РКС важно разделить вычислительные сети на корпоративные и общедоступные. В **корпоративных** сетях все элементы принадлежат одному ведомству за исключением, может быть, каналов связи. В таких сетях имеется возможность проводить единую политику обеспечения безопасности информации во всей сети. Примерами таких корпоративных сетей могут служить сети государственного и военного управления, сети авиационных и железнодорожных компаний и др. Противоположностью таким сетям являются **общедоступные** коммерческие сети, в которых во главу угла ставится распространение информации, а вопросы защиты собственных информационных ресурсов решаются, в основном, на уровне пользователей. В качестве примера такой сети можно привести сеть Internet. Корпоративные сети могут быть связаны с общедоступными сетями. В этом случае администрации (владельцам) корпоративных сетей необходимо предпринимать дополнительные меры предосторожности для блокирования возможных угроз со стороны общедоступных сетей.

При построении системы защиты информации в любой распределенной КС необходимо учитывать:

- сложность системы, которая определяется как количеством подсистем, так и разнообразием их типов и выполняемых функций;
- невозможность обеспечения эффективного контроля за доступом к ресурсам, распределенным на больших расстояниях, возможно за пределами границ страны;
- возможность принадлежности ресурсов сети различным владельцам.

Особенностью защиты информации от непреднамеренных угроз в РКС по сравнению с сосредоточенными сетями является необходимость обеспечения гарантированной передачи информации по коммуникационной подсети. Для этого в РКС должны быть предусмотрены дублирующие маршруты доставки сообщений, предприняты меры против искажения и потери информации в каналах связи. Такие сложные системы должны строиться как адаптивные, в которых обеспечивается постоянный контроль работоспособности элементов системы и возможность продолжения функционирования даже в условиях отказов отдельных подсистем. Искажения информации в каналах связи фиксируются и частично исправляются с помощью помехоустойчивого кодирования. Потери информации исключаются за счет использования контроля и учета принятых сообщений, а также за счет применения протоколов обмена с подтверждением о приеме информации.

В РКС все потенциальные преднамеренные угрозы безопасности информации делят на две группы: пассивные и активные.

К **пассивным** относятся угрозы, целью реализации которых является получение информации о системе путем прослушивания каналов связи. Подключившись к каналам связи или являясь пользователем системы, злоумышленник может:

- получить информацию путем перехвата незашифрованных сообщений;
- анализировать трафик (поток сообщений), накапливая информацию об интенсивности обмена отдельных абонентов, о структуре сообщений, о маршрутах доставки сообщений и т. п.

Активные угрозы предусматривают воздействие на передаваемые сообщения в сети и несанкционированную передачу фальсифицированных сообщений с целью воздействия на информационные ресурсы объектов РКС и дестабилизацию функционирования системы. Возможно также непосредственное воздействие на коммуникационную подсистему с целью повреждения аппаратных средств передачи информации.

Передаваемые в РКС сообщения могут несанкционированно модифицироваться или уничтожаться. Злоумышленник может размножать перехваченные сообщения, нарушать их очередность следования, изменять маршрут доставки, подменять сообщения. Злоумышленник может предпринять попытки несанкционирован-

ного доступа к информационным ресурсам удаленного объекта КС осуществления несанкционированного изменения программной структуры КС путем внедрения вредительских программ.

Анализируя приведенные особенности потенциальных угроз безопасности информации в РКС, можно сделать вывод, что все они связаны с передачей информации по каналам связи, с территориальной разобщенностью объектов системы. Таким образом, в *РК.С* наряду с мерами, предпринимаемыми для обеспечения безопасности информации в сосредоточенных КС, реализуется ряд механизмов для защиты информации при передаче ее по каналам связи, а также для защиты от несанкционированного воздействия на информацию КС с использованием каналов связи.

Все методы и средства, обеспечивающие безопасность информации в защищенной вычислительной сети, могут быть распределены по группам:

- обеспечение безопасности информации в пользовательской подсистеме и специализированных коммуникационных КС;
- защита информации на уровне подсистемы управления сетью;
- защита информации в каналах связи;
- обеспечение контроля подлинности взаимодействующих процессов.

11.3. Обеспечение безопасности информации в пользовательской подсистеме и специализированных коммуникационных КС

Обеспечение безопасности информации на объектах РКС практически не отличается от решения такой задачи для сосредоточенных систем. Особенностью защиты объектов РКС является необходимость поддержки механизмов аутентификации и разграничения доступа удаленных процессов к ресурсам объекта, а также наличие в сети специальных коммуникационных компьютерных систем. Учитывая важность проблемы подтверждения подлинности удаленных процессов (пользователей), механизмы ее решения выделены в отдельную группу.

Все элементы коммуникационной подсистемы, за исключением каналов связи, рассматриваются как специализированные ком-

муникационные компьютерные системы. В защищенных корпоративных сетях концентраторы, коммуникационные модули (серверы), шлюзы и мосты целесообразно размещать на объектах совместно с КС пользователей. Особенностью всех коммуникационных КС является информация, которая обрабатывается этими системами. В таких КС осуществляется смысловая обработка только служебной информации. К служебной относится адресная информация, избыточная информация для защиты сообщений от искажений, идентификаторы пользователей, метки времени, номера сообщений (пакетов), атрибуты шифрования и другая информация. Информация пользователей, заключенная в сообщениях (рабочая информация), на уровне коммуникационных КС рассматривается как последовательность бит, которая должна быть доставлена по коммуникационной подсистеме без изменений. Поэтому в таких системах имеется принципиальная возможность не раскрывать содержание рабочей информации. Она не должна быть доступной операторам и другому обслуживающему персоналу коммуникационных компьютерных систем для просмотра на экране монитора, изменения, уничтожения, размножения, запоминания в доступной памяти, получения твердой копии. Такая информация не должна сохраняться на внешних запоминающих устройствах после успешной передачи сообщения другому элементу коммуникационной подсистемы. В закрытых системах рабочая информация, кроме того, в пределах коммуникационной подсети циркулирует в зашифрованном виде.

Различают два вида шифрования в КС: шифрование в коммуникационной подсистеме - **линейное** - и межконцевое шифрование - **абонентское** [37]. Абонент перед отправкой осуществляет зашифрование сообщения с помощью симметричного или открытого ключа. На входе в коммуникационную подсистему сообщение подвергается линейному зашифрованию, даже если абонентское шифрование и не выполнялось. При линейном шифровании сообщение зашифровывается полностью, включая все служебные данные. Причем линейное шифрование может осуществляться в сети с разными ключами. В этом случае злоумышленник, имея один ключ, может получить доступ к информации, передаваемой в ограниченном количестве каналов. Если используются различные ключи, то в коммуникационных модулях осуществляется

расшифрование не только служебной информации, а всего сообщения полностью (рабочая информация остается зашифрованной на абонентском уровне). По открытой служебной информации осуществляется проверка целостности сообщения, выбор дальнейшего маршрута и передача «квитанции» отправителю. Сообщение подвергается зашифрованию с новым ключом и передается по соответствующему каналу связи.

Особые меры защиты должны предприниматься в отношении центра управления сетью. Учитывая концентрацию информации, критичной для работы всей сети, необходимо использовать самые совершенные средства защиты информации специализированной КС администратора сети как от непреднамеренных, так и преднамеренных угроз. Особое внимание должно обращаться на защиту процедур и средств, связанных с хранением и работой с ключами.

Администратор сети как и все операторы коммуникационной подсети, работает только со служебной информацией. Если в сети ключи для абонентского шифрования распределяются из центра управления сетью, то администратор может получить доступ ко всем ключам сети, а, следовательно, и ко всей передаваемой и хранимой в сети информации. Поэтому в специализированной КС администратора сети должны быть предусмотрены механизмы, блокирующие возможность работы с информационной частью сообщений, которые не предназначаются администратору.

Более надежным является способ управления ключами, когда они неизвестны ни администратору, ни абонентам. Ключ генерируется датчиком случайных чисел и записывается в специальное ассоциативное запоминающее устройство, и все действия с ним производятся в замкнутом пространстве, в которое оператор КС не может попасть с целью ознакомления с содержимым памяти. Нужные ключи выбираются из специальной памяти для отсылки или проверки в соответствии с идентификатором абонента или администратора.

При рассылке ключей вне РКС их можно записывать, например, на смарт-карты. Считывание ключа с таких карт возможно только при положительном результате аутентификации КС и владельца ключа.

11.4. Защита информации на уровне подсистемы управления РКС

Управление передачей сообщений осуществляется по определенным правилам, которые называются протоколами [37]. В настоящее время в распределенных вычислительных сетях реализуются два международных стандарта взаимодействия удаленных элементов сети: протокол **TCP/ГР** и протокол **X.25.**

Протокол **TCP/IP** был разработан в 70-е годы и с тех пор завоевал признание во всем мире. На основе протокола TCP/IP построена сеть Internet. Протокол X.25 явился дальнейшим развитием технологии передачи данных, построенной на основе коммутации пакетов. Протокол X.25 создан в соответствии с моделью взаимодействия открытых сетей **(OSI),** разработанной Международной организацией стандартизации (ISO). В соответствии с моделью все функции сети разбиваются на 7 уровней, а в модели ТСР/ГР насчитывается 5 уровней (рис. 25).

Протокол X.25 позволяет обеспечить более надежное взаимодействие удаленных процессов. Достоинствами протокола ТСР/ГР «вляются сравнительно низкая стоимость и простота подключе- к сети.

Задачи обеспечения безопасности информации в сети решаются на всех уровнях. Выполнение протоколов организуется с по- ющью подсистемы управления. Наряду с другими на уровне подсистемы управления решаются следующие проблемы защиты информации в РКС.

1. Создание единого центра управления сетью, в котором релались бы и вопросы обеспечения безопасности информации. Администратор и его аппарат проводят единую политику безопасности во всей защищенной сети.

2. Регистрация всех объектов сети и обеспечение их защиты. [Выдача идентификаторов и учет всех пользователей сети.

3.Управление доступом к ресурсам сети.

4. Генерация и рассылка ключей шифрования абонентам компьютерной сети.

5. Мониторинг трафика (потока сообщений в сети), контроль [соблюдения правил работы абонентами, оперативное реагирование на нарушения.

6. Организация восстановления работоспособности элементов сети при нарушении процесса их функционирования.

Рис. 25. Уровневые модели протоколов

11.5. Защита информации в каналах связи

Для защиты информации, передаваемой по каналам связи, применяется комплекс методов и средств защиты, позволяющих блокировать возможные угрозы безопасности информации. Наиболее надежным и универсальным методом защиты информации в каналах связи является шифрование. Шифрование на абонентском уровне позволяет защитить рабочую информацию от утраты конфиденциальности и навязывания ложной информации. Линейное шифрование позволяет, кроме того, защитить служебную информацию. Не имея доступа к служебной информации, злоумышленник не может фиксировать факт передачи между конкретными абонентами сети, изменить адресную часть сообщения с целью его переадресации.

Противодействие ложным соединениям абонентов (процессов) обеспечивается применением целого ряда процедур взаимного подтверждения подлинности абонентов или процессов. Против

удаления, явного искажения, переупорядочивания, передачи дублей сообщений используется механизм квитирования, нумерации сообщений или использования информации о времени отправки сообщения. Эти служебные данные должны быть зашифрованы. Для некоторых РКС важной информацией о работе системы, подлежащей защите, является интенсивность обмена по коммуникационной подсети. Интенсивность обмена может быть скрыта путем добавления к рабочему трафику обмена специальными сообщениями. Такие сообщения могут содержать произвольную случайную информацию. Дополнительный эффект такой организации обмена заключается в тестировании коммуникационной подсети. Общий трафик с учетом рабочих и специальных сообщений поддерживается примерно на одном уровне.

Попыткам блокировки коммуникационной подсистемы путем интенсивной передачи злоумышленником сообщений или распространения вредительских программ типа «червь», в подсистеме управления РКС должны быть созданы распределенные механизмы контроля интенсивности обмена и блокирования доступа в сеть абонентов при исчерпании ими лимита активности или-в случае угрожающего возрастания трафика. Для блокирования угроз физического воздействия на каналы связи (нарушение линий связи или постановка помех в радиоканалах) необходимо иметь дублирующие каналы с возможностью автоматического перехода на их использование.

11.5.1. Межсетевое экранирование

На практике часто закрытые корпоративные распределенные и сосредоточенные КС связаны с общедоступными сетями типа Internet. Режимы взаимодействия пользователей закрытой РКС с общедоступной системой могут быть различны:

- с помощью общедоступной РКС связываются в единую систему закрытые сегменты корпоративной системы или удаленные абоненты;
- пользователи закрытой РКС взаимодействуют с абонентами общедоступной сети.

В первом режиме задача подтверждения подлинности взаимодействующих абонентов (процессов) решается гораздо эффектив-

нее, чем во втором режиме. Это объясняется возможностью использования абонентского шифрования при взаимодействии КС одной корпоративной сети.

Если абоненты общедоступной сети не используют абонентское шифрование, то практически невозможно обеспечить надежную аутентификацию процессов, конфиденциальность информации, защиту от подмены и несанкционированной модификации сообщений.

Для блокирования угроз, исходящих из общедоступной системы, используется специальное программное или аппаратно-программное средство, которое получило название межсетевой экран (Firewall) (рис. 26). Как правило, межсетевой экран реализуется на выделенной ЭВМ, через которую защищенная РКС (ее фрагмент) подключается к общедоступной сети.

Общедоступная сеть | Межсетевой экран | Защищенная сеть

Рис. 26. Соединение сетей с помощью межсетевого экрана

Межсетевой экран реализует контроль за информацией, поступающей в защищенную РКС и (или) выходящей из защищенной системы [27].

Межсетевой экран выполняет четыре функции:

- фильтрация данных;
- использование экранирующих агентов;
- трансляция адресов;
- регистрация событий.

Основной функцией межсетевого экрана является *фильтрация* входного (выходного) трафика. В зависимости от степени защищенности корпоративной сети могут задаваться различные правила фильтрации. Правила фильтрации устанавливаются путем вы-

бора последовательности фильтров, которые разрешают или запрещают передачу данных (пакетов) на следующий фильтр или уровень протокола.

Межсетевой экран осуществляет фильтрацию на канальном, сетевом, транспортном и на прикладном уровнях. Чем большее количество уровней охватывает экран, тем он совершеннее. Межсетевые экраны, предназначенные для защиты информации высокой степени важности, должны обеспечивать [13]:

- фильтрацию по адресам отправителя и получателя (или по другим эквивалентным атрибутам);
- фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- фильтрацию с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;
- фильтрацию с учетом любых значимых полей сетевых пакетов;
- фильтрацию на транспортном уровне запросов на установление виртуальных соединений;
- фильтрацию на прикладном уровне запросов к прикладным сервисам;
- фильтрацию с учетом даты и времени;
- возможность сокрытия субъектов доступа защищаемой компьютерной сети;
- возможность трансляции адресов.

В межсетевом экране могут использоваться *экранирующие генты* (proxy-серверы), которые являются программами-посредниками и обеспечивают установление соединения между Ьубъектом и объектом доступа, а затем пересылают информацию, существляя контроль и регистрацию. Дополнительной функцией экранирующего агента является сокрытие от субъекта доступа истинного объекта. Действия экранирующего агента являются 1розрачными для участников взаимодействия.

Функция *трансляции адресов* межсетевого экрана предназначена для скрытия от внешних абонентов истинных внутренних 1ресов. Это позволяет скрыть топологию сети и использовать большее число адресов, если их выделено недостаточно для задищенной сети.

Межсетевой экран выполняет *регистрацию событии* в специальных журналах. Предусматривается возможность настройки экрана на ведение журнала с требуемой для конкретного применения полнотой. Анализ записей позволяет зафиксировать попытки нарушения установленных правил обмена информацией в сети и выявить злоумышленника.

Экран не является симметричным. Он различает понятия: «снаружи» и «внутри». Экран обеспечивает защиту внутренней области от неконтролируемой и потенциально враждебной внешней среды. В то же время экран позволяет разграничить доступ к объектам общедоступной сети со стороны субъектов защищенной сети. При нарушении полномочий работа субъекта доступа блокируется, и вся необходимая информация записывается в журнал.

Межсетевые экраны могут использоваться и внутри защищенных корпоративных сетей. Если в РКС имеются фрагменты сети с различной степенью конфиденциальности информации, то такие фрагменты целесообразно отделять межсетевыми экранами. В этом случае экраны называют внутренними.

В зависимости от степени конфиденциальности и важности информации установлены 5 классов защищенности межсетевых экранов [13]. Каждый класс характеризуется определенной минимальной совокупностью требований по защите информации. Самый низкий класс защищенности - пятый, а самый высокий - первый. Межсетевой экран первого класса устанавливается при обработке информации с грифом «особой важности».

Межсетевые экраны целесообразно выполнять в виде специализированных систем. Это должно повысить производительность таких систем (весь обмен осуществляется через экран), а также повысить безопасность информации за счет упрощения структуры. Учитывая важность межсетевых экранов в обеспечении безопасности информации во всей защищенной сети, к ним предъявляются высокие требования по разграничению доступа, обеспечению целостности информации, восстанавливаемости, тестированию и т. п. Обеспечивает работу межсетевого экрана администратор. Желательно рабочее место администратора располагать непосредственно у межсетевого экрана, что упрощает идентификацию и аутентификацию администратора, а также упрощает выполнение функций администрирования.

В сетях с большой интенсивностью обмена межсетевой экран может быть реализован на двух и более ЭВМ, которые целесообразно размещать на одном объекте. Функции межсетевого экрана и шлюза (моста) могут быть реализованы на одной КС. На практике часто фрагменты защищенной сети связываются между собой через общедоступную сеть. Все фрагменты подключаются к общедоступной сети через межсетевые экраны.

11.5.2. Подтверждение подлинности взаимодействующих процессов

Одной из центральных проблем обеспечения безопасности информации в вычислительной сети является проблема взаимоподтверждения подлинности взаимодействующих процессов. Логическую связь взаимодействующих процессов определяют термином соединение. Процедура аутентификации выполняется обычно в начале взаимодействия в процессе установления соединения.

Удаленные процессы до начала взаимодействия должны убедиться в их подлинности. Взаимная проверка подлинности взаимодействующих процессов может осуществляться следующими способами [26]:

- обмен идентификаторами;
- процедура «рукопожатия»;
- аутентификация при распределении ключей.

Обмен идентификаторами применим, если в сети используется симметричное шифрование. Зашифрованное сообщение, содержащее идентификатор, однозначно указывает, что сообщение создано пользователем, который знает секретный ключ шифрования и личный идентификатор. Существует единственная возможность для злоумышленника попытаться войти во взаимодействие с нужным процессом - запоминание перехваченного сообщения с последующей выдачей в канал связи. Блокирование такой угрозы осуществляется с помощью указания в сообщении времени отправки сообщения. При проверке сообщения достаточно просмотреть журнал регистрации сеансов в КС получателя сообщения. Вместо времени может использоваться случайное число, которое генерируется перед каждой отправкой.

Различают два варианта выполнения ***процедуры «рукопожатия»:*** обмен вопросами и ответами, а также использование функции f, известной только процессам, устанавливающим взаимодействие. Процессы обмениваются вопросами, ответы на которые не должны знать посторонние. Вопросы могут касаться, например, биографических данных субъектов, в интересах которых инициированы процессы.

Алгоритм использования функции f для аутентификации процессов A и B представляет собой последовательность следующих шагов[26]:

Шаг 1. Процесс A генерирует величину x и отсылает ее процессу B.

Шаг 2. Процесс B по секретному алгоритму вычисляет функцию **y** = f(x) и отсылает ее процессу A.

Шаг 3. Процесс A вычисляет функцию **y** = f(x) и сравнивает ее с полученной от процесса B.

Если результаты сравнения положительны, то делается вывод о подлинности взаимодействующих процессов.

Процедура установления подлинности осуществляется также ***при распределении сеансовых ключей.*** Распределение ключей является одной из процедур управления ключами. Можно выделить следующие процедуры управления ключами: генерация, распределение, хранение и смена ключей.

Обычно выделяют две категории ключей: ключи шифрования данных и ключи шифрования ключей при передаче их по каналам связи и хранении. Многократное использование одного и того же ключа повышает его уязвимость, поэтому ключи шифрования данных должны регулярно сменяться. Как правило, ключи шифрования данных меняются в каждом сеансе работы и поэтому их называют сеансовыми ключами.

В процессе генерации ключи должны получаться случайным образом. Этому требованию в наибольшей степени отвечает генератор псевдослучайной последовательности, использующий в качестве исходных данных показания таймера.

Секретные ключи хранятся в запоминающем устройстве только в зашифрованном виде. Ключ от зашифрованных ключей может быть зашифрован с помощью другого ключа. Последний ключ хранится в открытом виде, но в специальной памяти. Он не

может быть считан, просмотрен, изменен или уничтожен в обычном режиме работы. Этот ключ называется главным или мастер-ключом.

Проблема распределения симметричных ключей в больших сетях не является тривиальной. Каждой паре взаимодействующих абонентов сети необходимо доставить по одному одинаковому ключу. Если необходимо предусмотреть возможность независимого обмена абонентов по принципу: "каждый с каждым", то в сети из 200 абонентов необходимо каждому из них доставить 199 мастер-ключей. Тогда в ЦРК необходимо сгенерировать N ключей. Количество ключей определяется по формуле:

$$N = 1/2 * n(n - 1) ,$$

где n - количество абонентов сети. При n = 200 получается N=9900.

Мастер-ключи при симметричном шифровании и секретные ключи при несимметричном шифровании распространяются вне РКС. При большом числе абонентов и их удалении на значительные расстояния друг от друга задача распространения мастер-ключей является довольно сложной. При несимметричном шифровании количество секретных ключей равно количеству абонентов сети. Кроме того, использование несимметричного шифрования не требует распределения сеансовых ключей, что сокращает обмен служебной информацией в сети. Списки открытых ключей всех абонентов могут храниться у каждого абонента сети. Однако у симметричного шифрования есть и два существенных преимущества. Симметричное шифрование, например, по алгоритму DES занимает значительно меньше времени по сравнению с алгоритмами несимметричного шифрования.

В системах с симметричным шифрованием проще обеспечивать взаимное подтверждение подлинности абонентов (процессов). Знание секретного ключа, общего для двух взаимодействующих процессов, дополненное защитными механизмами от повторной передачи, является основанием считать взаимодействующие процессы подлинными.

Совместить достоинства обоих методов шифрования удалось благодаря разработке У. Диффи и М. Хеллманом метода получения секретного сеансового ключа на основе обмена открытыми

6. Организация восстановления работоспособности элементов сети при нарушении процесса их функционирования.

Рис. 25. Уровневые модели протоколов

11.5. Защита информации в каналах связи

Для защиты информации, передаваемой по каналам связи, применяется комплекс методов и средств защиты, позволяющих блокировать возможные угрозы безопасности информации. Наиболее надежным и универсальным методом защиты информации в каналах связи является шифрование. Шифрование на абонентском уровне позволяет защитить рабочую информацию от утраты конфиденциальности и навязывания ложной информации. Линейное шифрование позволяет, кроме того, защитить служебную информацию. Не имея доступа к служебной информации, злоумышленник не может фиксировать факт передачи между конкретными абонентами сети, изменить адресную часть сообщения с целью его переадресации.

Противодействие ложным соединениям абонентов (процессов) обеспечивается применением целого ряда процедур взаимного подтверждения подлинности абонентов или процессов. Против

удаления, явного искажения, переупорядочивания, передачи дублей сообщений используется механизм квитирования, нумерации сообщений или использования информации о времени отправки сообщения. Эти служебные данные должны быть зашифрованы. Для некоторых РКС важной информацией о работе системы, подлежащей защите, является интенсивность обмена по коммуникационной подсети. Интенсивность обмена может быть скрыта путем добавления к рабочему трафику обмена специальными сообщениями. Такие сообщения могут содержать произвольную случайную информацию. Дополнительный эффект такой организации обмена заключается в тестировании коммуникационной подсети. Общий трафик с учетом рабочих и специальных сообщений поддерживается примерно на одном уровне.

Попыткам блокировки коммуникационной подсистемы путем интенсивной передачи злоумышленником сообщений или распространения вредительских программ типа «червь», в подсистеме управления РКС должны быть созданы распределенные механизмы контроля интенсивности обмена и блокирования доступа в сеть абонентов при исчерпании ими лимита активности или-в случае угрожающего возрастания трафика. Для блокирования угроз физического воздействия на каналы связи (нарушение линий связи или постановка помех в радиоканалах) необходимо иметь дублирующие каналы с возможностью автоматического перехода на их использование.

11.5.1. Межсетевое экранирование

На практике часто закрытые корпоративные распределенные и сосредоточенные КС связаны с общедоступными сетями типа Internet. Режимы взаимодействия пользователей закрытой РКС с общедоступной системой могут быть различны:

- с помощью общедоступной РКС связываются в единую систему закрытые сегменты корпоративной системы или удаленные абоненты;
- пользователи закрытой РКС взаимодействуют с абонентами общедоступной сети.

В первом режиме задача подтверждения подлинности взаимодействующих абонентов (процессов) решается гораздо эффектив-

нее, чем во втором режиме. Это объясняется возможностью использования абонентского шифрования при взаимодействии КС одной корпоративной сети.

Если абоненты общедоступной сети не используют абонентское шифрование, то практически невозможно обеспечить надежную аутентификацию процессов, конфиденциальность информации, защиту от подмены и несанкционированной модификации сообщений.

Для блокирования угроз, исходящих из общедоступной системы, используется специальное программное или аппаратно-программное средство, которое получило название межсетевой экран (Firewall) (рис. 26). Как правило, межсетевой экран реализуется на выделенной ЭВМ, через которую защищенная РКС (ее фрагмент) подключается к общедоступной сети.

Общедоступная сеть | Межсетевой экран | Защищенная сеть

Рис. 26. Соединение сетей с помощью межсетевого экрана

Межсетевой экран реализует контроль за информацией, поступающей в защищенную РКС и (или) выходящей из защищенной системы [27].

Межсетевой экран выполняет четыре функции:

- фильтрация данных;
- использование экранирующих агентов;
- трансляция адресов;
- регистрация событий.

Основной функцией межсетевого экрана является *фильтрация* входного (выходного) трафика. В зависимости от степени защищенности корпоративной сети могут задаваться различные правила фильтрации. Правила фильтрации устанавливаются путем вы-

бора последовательности фильтров, которые разрешают или запрещают передачу данных (пакетов) на следующий фильтр или уровень протокола.

Межсетевой экран осуществляет фильтрацию на канальном, сетевом, транспортном и на прикладном уровнях. Чем большее количество уровней охватывает экран, тем он совершеннее. Межсетевые экраны, предназначенные для защиты информации высокой степени важности, должны обеспечивать [13]:

- фильтрацию по адресам отправителя и получателя (или по другим эквивалентным атрибутам);
- фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- фильтрацию с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;
- фильтрацию с учетом любых значимых полей сетевых пакетов;
- фильтрацию на транспортном уровне запросов на установление виртуальных соединений;
- фильтрацию на прикладном уровне запросов к прикладным сервисам;
- фильтрацию с учетом даты и времени;
- возможность сокрытия субъектов доступа защищаемой компьютерной сети;
- возможность трансляции адресов.

В межсетевом экране могут использоваться *экранирующие генты* (proxy-серверы), которые являются программами-посредниками и обеспечивают установление соединения между Ьубъектом и объектом доступа, а затем пересылают информацию, существляя контроль и регистрацию. Дополнительной функцией экранирующего агента является сокрытие от субъекта доступа истинного объекта. Действия экранирующего агента являются 1розрачными для участников взаимодействия.

Функция *трансляции адресов* межсетевого экрана предназначена для скрытия от внешних абонентов истинных внутренних 1ресов. Это позволяет скрыть топологию сети и использовать большее число адресов, если их выделено недостаточно для задищенной сети.

Межсетевой экран выполняет *регистрацию событии* в специальных журналах. Предусматривается возможность настройки экрана на ведение журнала с требуемой для конкретного применения полнотой. Анализ записей позволяет зафиксировать попытки нарушения установленных правил обмена информацией в сети и выявить злоумышленника.

Экран не является симметричным. Он различает понятия: «снаружи» и «внутри». Экран обеспечивает защиту внутренней области от неконтролируемой и потенциально враждебной внешней среды. В то же время экран позволяет разграничить доступ к объектам общедоступной сети со стороны субъектов защищенной сети. При нарушении полномочий работа субъекта доступа блокируется, и вся необходимая информация записывается в журнал.

Межсетевые экраны могут использоваться и внутри защищенных корпоративных сетей. Если в РКС имеются фрагменты сети с различной степенью конфиденциальности информации, то такие фрагменты целесообразно отделять межсетевыми экранами. В этом случае экраны называют внутренними.

В зависимости от степени конфиденциальности и важности информации установлены 5 классов защищенности межсетевых экранов [13]. Каждый класс характеризуется определенной минимальной совокупностью требований по защите информации. Самый низкий класс защищенности - пятый, а самый высокий - первый. Межсетевой экран первого класса устанавливается при обработке информации с грифом «особой важности».

Межсетевые экраны целесообразно выполнять в виде специализированных систем. Это должно повысить производительность таких систем (весь обмен осуществляется через экран), а также повысить безопасность информации за счет упрощения структуры. Учитывая важность межсетевых экранов в обеспечении безопасности информации во всей защищенной сети, к ним предъявляются высокие требования по разграничению доступа, обеспечению целостности информации, восстанавливаемости, тестированию и т. п. Обеспечивает работу межсетевого экрана администратор. Желательно рабочее место администратора располагать непосредственно у межсетевого экрана, что упрощает идентификацию и аутентификацию администратора, а также упрощает выполнение функций администрирования.

В сетях с большой интенсивностью обмена межсетевой экран может быть реализован на двух и более ЭВМ, которые целесообразно размещать на одном объекте. Функции межсетевого экрана и шлюза (моста) могут быть реализованы на одной КС. На практике часто фрагменты защищенной сети связываются между собой через общедоступную сеть. Все фрагменты подключаются к общедоступной сети через межсетевые экраны.

11.5.2. Подтверждение подлинности взаимодействующих процессов

Одной из центральных проблем обеспечения безопасности информации в вычислительной сети является проблема взаимоподтверждения подлинности взаимодействующих процессов. Логическую связь взаимодействующих процессов определяют термином соединение. Процедура аутентификации выполняется обычно в начале взаимодействия в процессе установления соединения.

Удаленные процессы до начала взаимодействия должны убедиться в их подлинности. Взаимная проверка подлинности взаимодействующих процессов может осуществляться следующими способами [26]:

- обмен идентификаторами;
- процедура «рукопожатия»;
- аутентификация при распределении ключей.

Обмен идентификаторами применим, если в сети используется симметричное шифрование. Зашифрованное сообщение, содержащее идентификатор, однозначно указывает, что сообщение создано пользователем, который знает секретный ключ шифрования и личный идентификатор. Существует единственная возможность для злоумышленника попытаться войти во взаимодействие с нужным процессом - запоминание перехваченного сообщения с последующей выдачей в канал связи. Блокирование такой угрозы осуществляется с помощью указания в сообщении времени отправки сообщения. При проверке сообщения достаточно просмотреть журнал регистрации сеансов в КС получателя сообщения. Вместо времени может использоваться случайное число, которое генерируется перед каждой отправкой.

Различают два варианта выполнения ***процедуры «рукопожатия»:*** обмен вопросами и ответами, а также использование функции f, известной только процессам, устанавливающим взаимодействие. Процессы обмениваются вопросами, ответы на которые не должны знать посторонние. Вопросы могут касаться, например, биографических данных субъектов, в интересах которых инициированы процессы.

Алгоритм использования функции f для аутентификации процессов A и B представляет собой последовательность следующих шагов[26]:

Шаг 1. Процесс A генерирует величину x и отсылает ее процессу B.

Шаг 2. Процесс B по секретному алгоритму вычисляет функцию **y** = f(x) и отсылает ее процессу A.

Шаг 3. Процесс A вычисляет функцию **y** = f(x) и сравнивает ее с полученной от процесса B.

Если результаты сравнения положительны, то делается вывод о подлинности взаимодействующих процессов.

Процедура установления подлинности осуществляется также ***при распределении сеансовых ключей.*** Распределение ключей является одной из процедур управления ключами. Можно выделить следующие процедуры управления ключами: генерация, распределение, хранение и смена ключей.

Обычно выделяют две категории ключей: ключи шифрования данных и ключи шифрования ключей при передаче их по каналам связи и хранении. Многократное использование одного и того же ключа повышает его уязвимость, поэтому ключи шифрования данных должны регулярно сменяться. Как правило, ключи шифрования данных меняются в каждом сеансе работы и поэтому их называют сеансовыми ключами.

В процессе генерации ключи должны получаться случайным образом. Этому требованию в наибольшей степени отвечает генератор псевдослучайной последовательности, использующий в качестве исходных данных показания таймера.

Секретные ключи хранятся в запоминающем устройстве только в зашифрованном виде. Ключ от зашифрованных ключей может быть зашифрован с помощью другого ключа. Последний ключ хранится в открытом виде, но в специальной памяти. Он не

может быть считан, просмотрен, изменен или уничтожен в обычном режиме работы. Этот ключ называется главным или мастер-ключом.

Проблема распределения симметричных ключей в больших сетях не является тривиальной. Каждой паре взаимодействующих абонентов сети необходимо доставить по одному одинаковому ключу. Если необходимо предусмотреть возможность независимого обмена абонентов по принципу: "каждый с каждым", то в сети из 200 абонентов необходимо каждому из них доставить 199 мастер-ключей. Тогда в ЦРК необходимо сгенерировать N ключей. Количество ключей определяется по формуле:

$$N = 1/2 * n(n - 1) ,$$

где n - количество абонентов сети. При n = 200 получается N=9900.

Мастер-ключи при симметричном шифровании и секретные ключи при несимметричном шифровании распространяются вне РКС. При большом числе абонентов и их удалении на значительные расстояния друг от друга задача распространения мастер-ключей является довольно сложной. При несимметричном шифровании количество секретных ключей равно количеству абонентов сети. Кроме того, использование несимметричного шифрования не требует распределения сеансовых ключей, что сокращает обмен служебной информацией в сети. Списки открытых ключей всех абонентов могут храниться у каждого абонента сети. Однако у симметричного шифрования есть и два существенных преимущества. Симметричное шифрование, например, по алгоритму DES занимает значительно меньше времени по сравнению с алгоритмами несимметричного шифрования.

В системах с симметричным шифрованием проще обеспечивать взаимное подтверждение подлинности абонентов (процессов). Знание секретного ключа, общего для двух взаимодействующих процессов, дополненное защитными механизмами от повторной передачи, является основанием считать взаимодействующие процессы подлинными.

Совместить достоинства обоих методов шифрования удалось благодаря разработке У. Диффи и М. Хеллманом метода получения секретного сеансового ключа на основе обмена открытыми

ключами (рис.27). По известному виду и значениям функций f(x) и f(y) при больших значениях x, y, a и p (больше 200 бит) практически невозможно за приемлемое время восстановить секретные ключи x и y.

Распределение ключей в сети между пользователями реализуется двумя способами:

1. Путем создания одного или нескольких центров распреде^ления ключей (ЦРК).

2. Прямой обмен сеансовыми ключами между абонентами сети.

Недостатком первого способа является наличие возможности доступа в ЦРК ко всей передаваемой по сети информации. В слу-к чае организации прямого обмена сеансовыми ключами возникают сложности в проверке подлинности процессов или абонентов.

Распределение ключей совмещается с процедурой проверки[1] подлинности взаимодействующих процессов. *

Протоколы распределения ключей для систем с симметричными и несимметричными ключами отличаются.

А. Проверка подлинности процессов при распределении ключей с использованием ЦРК *' ''''

Пусть вызывающий процесс обозначается через А, а вызываемый - через В. Оба процесса (абонента) имеют идентификаторы 1А и 1в. Абоненты имеют также мастер-ключи KM_A KMв, известные только соответственно А и В, а также ЦРК. Мастер-ключи распределяются между абонентами вне РКС. Это может быть специальная почта, другие автоматизированные системы и т. п.

Абонент А посылает в ЦРК в открытом виде идентификатор 1д и зашифрованные на KM_A идентификатор 1в, случайное число Г] и просьбу обеспечить связь с В [26]:

1. А —> ЦРК : 1_A, KMд (1в. Гь «Прошу установить связь с В»).

По открытому идентификатору 1д соответствующая процедура обеспечивает выбор мастер-ключа KMд, расшифровывает сообщение, а затем генерируется сеансовый ключ Ks и отсылается зашифрованное сообщение А:

2. ЦРК -* А : KM_A (Г,, K_S, I_B, KM_B (KS, I_A))

Это сообщение может расшифровать только абонент А,

ключами (рис.27). По известному виду и значениям функций f(x) и f(y) при больших значениях x, y, a и p (больше 200 бит) практически невозможно за приемлемое время восстановить секретные ключи x и y.

Распределение ключей в сети между пользователями реализуется двумя способами:

1. Путем создания одного или нескольких центров распреде^ления ключей (ЦРК).

2. Прямой обмен сеансовыми ключами между абонентами сети.

Недостатком первого способа является наличие возможности доступа в ЦРК ко всей передаваемой по сети информации. В слу-к чае организации прямого обмена сеансовыми ключами возникают сложности в проверке подлинности процессов или абонентов.

Распределение ключей совмещается с процедурой проверки[1] подлинности взаимодействующих процессов. *

Протоколы распределения ключей для систем с симметричными и несимметричными ключами отличаются.

А. Проверка подлинности процессов при распределении ключей с использованием ЦРК *' ''''

Пусть вызывающий процесс обозначается через А, а вызываемый - через В. Оба процесса (абонента) имеют идентификаторы 1А и 1в. Абоненты имеют также мастер-ключи KM_A KMв, известные только соответственно А и В, а также ЦРК. Мастер-ключи распределяются между абонентами вне РКС. Это может быть специальная почта, другие автоматизированные системы и т. п.

Абонент А посылает в ЦРК в открытом виде идентификатор 1д и зашифрованные на KM_A идентификатор 1в, случайное число Г] и просьбу обеспечить связь с В [26]:

1. А —> ЦРК : 1_A, KMд (1в. Гь «Прошу установить связь с В»).

По открытому идентификатору 1д соответствующая процедура обеспечивает выбор мастер-ключа KMд, расшифровывает сообщение, а затем генерируется сеансовый ключ Ks и отсылается зашифрованное сообщение А:

2. ЦРК -* А : KM_A (Г,, K_S, I_B, KM_B (KS, I_A))

Это сообщение может расшифровать только абонент А,

имеющий ключ КМд. Случайное число Г] подтверждает, что полученное сообщение не является повторным, а выдано ЦРК в ответ на сообщение А. Абонент А оставляет у себя Ks, генерирует случайное число r_2 и отправляет сообщение абоненту В:

3. A -> B : $KM_B (K_s, I_A)$, $K_s(r_2)$.

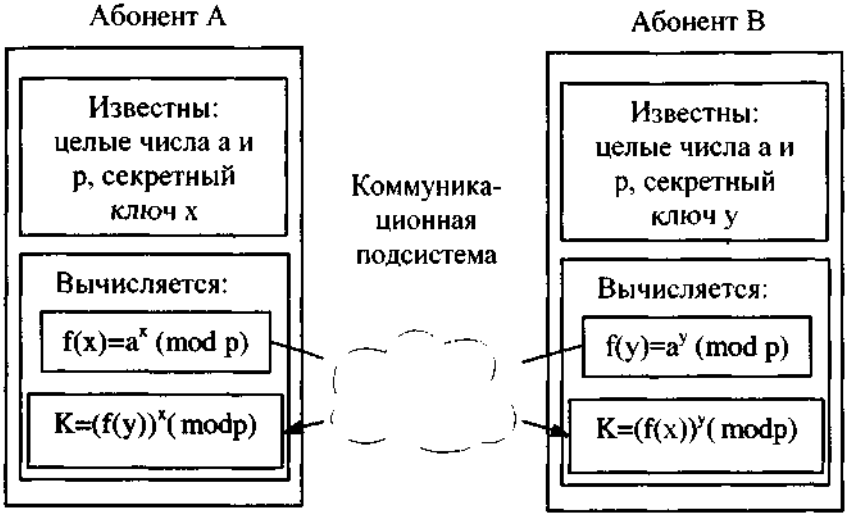


Рис. 27. Схема получения секретного сеансового ключа K

Сообщение может расшифровать только В. Полученный идентификатор 1_A указывает, что именно абонент А инициирует сеанс связи. Часть сообщения, зашифрованная мастер-ключом KM_B, подтверждает, что сеансовый ключ K_s получен в ЦРК. Абонент В расшифровывает с помощью Ks случайное число r_2. Если используется односторонняя процедура подтверждения подлинности, то абонент В передает абоненту А сообщение:

4. B->A: Ks(f(r_2)).

Такая процедура не обеспечивает полной уверенности В в том, что именно А является действительным инициатором обмена. Так существует возможность попытки повторной посылки сообщения 4 злоумышленником С позднее. Такое воздействие практически не будет иметь отрицательных последствий для В, так как у С нет сеансового ключа Ks. Он не сможет ни прочесть сообщение В, ни послать ему фальсифицированное сообщение. Чтобы исключить и

такую возможность, необходимо использовать процедуру тройного «рукопожатия». Тогда вместо сообщения 4 абонент В посылает А следующее сообщение:

4'. В -> А : K_s (гт, Гз), где Гз - случайное число.

В ответ А передает сообщение, подтверждающее его подлинность:

5. А -> В : K_s (гз)

Если все шаги выполнены успешно, то считается, что абоненты А и В - подлинные, и они могут проводить сеанс обмена сообщениями с помощью ключа Ks.

Недостатками такого алгоритма проверки подлинности и распределения ключей являются:

- большая нагрузка на ЦРК, так как при каждом сеансе осуществляется обращение к ЦРК;
- очень высокие требования предъявляются к защищенности и отказоустойчивости ЦРК.

Процедура взаимного подтверждения подлинности в системах с открытым ключом также заключается в обмене ключами и последующем подтверждении подлинности. Администратор ЦРК имеет доступ к открытому ключу $КО_{ЦРК}$ и закрытому ключу КЗцрк, а также к открытым ключам всех абонентов сети. Абонент А обращается с запросом в ЦРК для получения своего открытого ключа и открытого ключа вызываемого абонента В:

1. А —> ЦРК : $1_А$, 1в, «Вышлите ключи».

В ответ на полученный запрос ЦРК формирует сообщение, зашифрованное с помощью закрытого ключа ЦРК. Отдельно зашифровывается открытый ключ А и его идентификатор, а также открытый ключ абонента В и его идентификатор.

2. ЦРК -> А : $КЗ_{ЦРК}$ ($КО_А$, $1_А$), $КЗ_{ЦРК}$ ($КО_В$, ^{т}в).

Абонент А расшифровывает сообщение с помощью открытого ключа КОЦРК, который доставлен ему надежным путем. Полученные идентификаторы абонентов А и В подтверждают, что ЦРК правильно воспринял запрос и КОв- открытый ключ абонента В.

На следующем шаге процедуры абонент А посылает абоненту В сообщение, в котором сгенерированное число ri и идентификатор $1_А$ зашифрованы открытым ключом КОв, а открытый ключ КОд И идентификатор $1_А$ зашифрованы закрытым ключом ЦРК.

3. А -> В : КОв (г,, 1А), $КЗ_{ЦРК}$ ($КО_А$, 1А).

Абонент В расшифровывает первую часть сообщения с помощью своего закрытого ключа КЗв, а вторую часть - с помощью открытого ключа $КО_{ЦРК}$. На основании полученной информации абонент В делает вывод, что связь с ним устанавливает абонент А, что подтверждается зашифрованием открытого ключа А и его идентификатора с помощью секретного ключа ЦРК $КЗцр_к$. После шага 3 абоненты А и В имеют по два открытых ключа. Если используется одностороннее подтверждение подлинности, то на последнем шаге В посылает сообщение:

4. В -> А : КОд (f(r,)).

Если расшифрованное число ri совпадает с тем, которое посылалось абоненту В, то абонент А получает подтверждение подлинности абонента В, так как число ri при передаче по сети было зашифровано открытым ключом абонента В и могло быть расшифровано только владельцем закрытого ключа абонента В. Если используется процедура взаимного подтверждения подлинности, то осуществляется трехстороннее «рукопожатие». Тогда на четвертом шаге абонент В, наряду с числом гь передает абоненту А сгенерированное им случайное число $г_2$.

4'. В ^ А : $КО_А$ ($Г_ь$ $Г_2$).

В ответ абонент А передает сообщение:

5. А -> В : $КО_В$ ($г_2$).

Вместо случайных чисел в процедуре взаимного подтверждения могут использоваться временные метки. Если сообщение принимается после истечения контрольного интервала времени от создания сообщения до его получения, то такое сообщение считается фальсифицированным. Реализация такой процедуры затрудняется в больших сетях. Во-первых, в них сложнее поддерживать единое время. Во-вторых, разброс во времени доставки может колебаться в довольно широких пределах. Это связано с возможными изменениями маршрутов, а также повторных передач при сбоях в каналах связи.

Примером реальной системы, в которой реализован принцип подтверждения подлинности процессов при распределении ключей с использованием ЦРК, является вычислительная сеть со специальным сервером аутентификации Kerberos. Клиентские компоненты Kerberos присутствуют в большинстве современных операционных систем (наиболее полно в ОС Solaris). В защищенном

сервере Kerberos хранятся секретные ключи всех абонентов сети.

Процедура подтверждения подлинности клиента с и сервера s реализуется следующей последовательностью шагов.

1. Клиент с —* Kerberos: Ic, si, timeexp, r_b

Клиент с передает Kerberos в открытом виде свой идентификатор 1c, запрашиваемый сервис s_b срок годности билета timeexp и случайное число п.

2. Kerberos — • клиент с: $K_c(K_{cs}$, timeexp, ri); $K_s(K_{cs})$.

Kerberos возвращает сеансовый ключ Kcs, идентификатор сервера I_s, атрибуты timeexp и r_b зашифрованные ключом клиента, а также сеансовый ключ Kc_s, зашифрованный ключом сервера с.

3. Клиент с — • сервер s: Kcs(Ic, ts, ck); $K_s(K_{cs})$.

Клиент посылает серверу свой идентификатор lc, временной штамп ts и контрольную сумму ck, зашифрованные сеансовым ключом, а также пересылает без изменений зашифрованный ключ Ks(Kcs), который называется билетом.

4. Сервер s — • клиент с: $K_{cs}(I_s$, ts).

Сервер подтверждает свою подлинность, возвращая дополнительную информацию, зашифрованную сеансовым ключом.

Каждый сервер Kerberos обслуживает определенную область управления. Чтобы субъекты из различных областей управления могли общаться друг с другом, серверам Kerberos необходимо обмениваться секретными ключами.

Б. Проверка подлинности взаимодействующих процессов при прямом обмене сеансовыми ключами

Необходимо рассмотреть процедуры проверки подлинности при прямом обмене с секретным и открытым ключом [26].

1. Процедура подтверждения подлинности при взаимном обмене с секретным ключом.

Абоненты А и В используют общий для них секретный ключ Кдв, полученный ранее (вне РКС). Процедура выполняется за три шага.

1. А -> В: 1А, ГЬ

На первом шаге инициатор обмена абонент А передает в открытом виде абоненту В свой идентификатор 1_A и случайное число r_b Это сообщение могло быть послано любым абонентом сети.

2. B->A: $K_{AB}(f(r_1), IB, r_2, K_s)$.

На шаге 2 абонент В генерирует случайное число r_2 и сеансовый ключ Ks, посылает А сообщение, зашифрованное общим секретным ключом Кдв- Абонент может быть уверен, что сообщение пришло от В, т. к. только ему известен ключ K_Aв- Функция f (ri) подтверждает, что сообщение получено в ответ на сообщение 1, а не является повтором старого сообщения.

3. A-»B: Ks(f(r_2)).

На шаге 3 абонент А подтверждает, что сеансовый ключ находится именно у него. На этом процедура завершается.

Процедура подтверждения подлинности в процессе двустороннего распределения сеансового ключа в сети с применением открытых ключей также выполняется за три шага.

1. A->B: KOB(Г,ДА).

На первом шаге абонент зашифровывает сообщение для В с помощью открытого ключа KO_B. Случайное число ri и идентификатор абонента А может прочесть только абонент В с помощью секретного личного ключа.

2. B->A: $KO_A(f(r_1)_> r_2, I_B, K_s)$.

На втором шаге абонент вычисляет функцию f(ri), генерирует случайное число r_2 и сеансовый ключ Ks и зашифровывает все сообщение с помощью открытого ключа абонента А. Абонент А делает вывод, что сообщение 1 получено абонентом В.

3. A -> B : K_s (f(r_2)).

Взаимное опознание заканчивается на шаге 3 получением зашифрованной функции f(r_2). Абонент В убеждается, что сеансовый ключ передан именно абоненту А.

Если даже сеансовые ключи передаются, минуя РКС, то распределение мастер-ключей и индивидуальных ключей абонентов в защищенной корпоративной сети осуществляется ЦРК.

11.6. Подтверждение подлинности информации, получаемой по коммуникационной подсети

После установления соединения необходимо обеспечить защиту от фальсификации в процессе обмена сообщениями. Для этого требуется обеспечить выполнение следующих четырех условий[26]:

1) получатель должен быть уверен в истинности источника данных;

2) получатель должен быть уверен в истинности представляем мых данных;

3) отправитель должен быть уверен в доставке данных получателю;

4) отправитель должен быть уверен в истинности полученного подтверждения о приеме информации.

Подтверждение истинности источника данных и истинности передаваемых (доставленных) данных осуществляется с помощью цифровой подписи. Подтверждение приема сообщений обеспечивается организацией режима передачи квитанций. Квитанция представляет собой короткое сообщение, содержащее контрольную информацию о принятом сообщении и электронную подпись. В качестве контрольной информации могут использоваться зашифрованные данные о номере полученного сообщения и времени получения, а также цифровая подпись отправителя рабочего сообщения. Получив такую квитанцию, заверенную цифровой подписью, отправитель делает вывод об успешной передаче сообщения.

Цифровая подпись сообщения представляет собой контрольную двоичную последовательность. Она получается путем специальных преобразований хэш-функции от данных сообщения и секретного ключа отправителя сообщения. Таким образом цифровая подпись, с одной стороны, несет в себе контрольную характеристику (хэш-функцию) содержимого сообщения, а с другой - однозначно указывает на связь содержимого сообщения и владельца секретного ключа. Использование хэш-функции позволяет зафиксировать подмену или модификацию данных сообщения. Порядок получения хэш-функции приведен в гл.7. При удовлетворительных результатах проверки цифровой подписи получатель может быть уверен, что полученное сообщение пришло от субъекта, владеющего секретным ключом, и содержательная часть сообщения не подвергалась изменениям. Если цифровая подпись получается в соответствии с официальным государственным стандартом, то она имеет юридическую силу обычной подписи под документом.

Впервые идею цифровой подписи предложили в 1976 году

американские специалисты У. Диффи и М. Хеллман. В настоящее время для получения цифровой подписи используются методы, применяемые в шифровании с несимметричными ключами.

Первым по времени изобретения алгоритмом цифровой подписи был разработанный в 1977 году алгоритм RSA. Предложенный в 1984 году алгоритм Т. Эль-Гамаля позволял повысить стойкость подписи при ключе в 64 байта примерно в 1000 раз, но длина самой цифровой подписи увеличивалась в два раза и составляла 128 байт.

Алгоритм Эль-Гамаля послужил основой для разработки национального стандарта США DSA, введенного в 1991 году, и государственного стандарта РФ ГОСТ Р 34.10-94, введенного в действие с 1995 года. В алгоритме DSA удалось сократить длину цифровой подписи до 40 байт при сохранении ее стойкости на прежнем уровне. Дальнейшим развитием стандарта DSA стал стандарт США DSS.

Российский стандарт ГОСТ Р 34.10 схож со стандартом DSS, но предполагает более сложный алгоритм вычисления хэш-функции. Стандартом ГОСТ Р 34.10 определен следующий алгоритм вычисления цифровой подписи и аутентификации сообщения. Отправитель и получатель сообщения имеют в своем распоряжении некоторые открытые атрибуты создания и проверки цифровой подписи: начальный вектор хэширования H и параметры p, g и a. Параметры вычисляются в соответствии с процедурой ГОСТ. Отправитель выбирает свой секретный ключ x и вычисляет открытый ключ $y = a^x \pmod p$. Открытый ключ y отсылается получателю. Секретный ключ выбирается из интервала $0 < x < 2^{256}$. Число k генерируется в процессе получения подписи сообщения, является секретным и должно быть уничтожено после выработки подписи. Упрощенный алгоритм процедуры выработки подписи включат следующие шаги.

1. Вычисление хэш-функции h (M) от сообщения M.
2. Получение целого числа к, $0 < к < g$.
3. Вычисление значений $r = a^k \pmod p$ и $r' = r \pmod g$.

Если $r' = 0$, перейти к шагу 2.

4. Вычисление значения $s = (xr'+kh(M)) \pmod g$.

Если $s = 0$, то переход к шагу 2, иначе конец работы алгоритма.

Цифровой подписью сообщения M является вектор < r' >25б II

<s >256, который состоит из двух двоичных слов по 256 бит каждое, т. е. длина цифровой подписи составляет 512 бит.

Для проверки подписи (верификации сообщения) получатель сообщения выполняет следующие шаги.

1. Проверка условий: $o < s < g$ и $o < r' < g$.

Если хотя бы одно условие не выполнено, то подпись считается недействительной.

2. Определяется хэш-функция h (Mi) от полученного сообщения M].

3. Вычисляется значение $v = (h(Mi))^{s^2} \pmod g$.

4. Вычисляются значения $z\backslash = sv \pmod g$, $Z2 = (g-r')v \pmod g$.

5. Вычисление значения $u = (a^{z1} y^{z2} \pmod p) \pmod g$.

6. Проверка условия: r' = u.

Если условие выполнено, то получатель считает, что полученное сообщение подписано отправителем, от которого был получен ключ y. Кроме того, получатель считает, что в процессе передачи целостность сообщения не нарушена. В противном случае подпись считается недействительной и сообщение отвергается.

Имея открытые атрибуты цифровой подписи и тексты открытых сообщений, определить секретный ключ x можно только путем полного перебора. Причем при длине цифровой подписи 40 байт стандарт DSA гарантирует число комбинаций ключа 10^{21}. Для получения ключа перебором потребуется 30 лет непрерывной работы 1000 компьютеров производительностью 1 млрд. операций в секунду.

Использование цифровой подписи для аутентификации коротких сообщений, подтверждающих прием информационных сообщений, существенно увеличивает длину служебного подтверждающего сообщения. Для подписи служебного сообщения может быть использована подпись полученного информационного сообщения, модифицированная по определенному алгоритму. Например, выбраны разряды по маске. Если в сети реализован режим передачи пакетов, то цифровая подпись передается в конце всего сообщения, а не с каждым пакетом. Иначе трафик в сети увеличится. Степень увеличения трафика будет зависеть от длины пакета. При длине информационной части пакета в 2048 бит использование цифровой подписи каждого пакета привело бы к возрастанию трафика примерно на 25%.

При организации электронной почты необходимо учитывать особенности подтверждения полученных сообщений. Получатель в момент передачи сообщения может быть не активным. Поэтому следует организовать отложенную проверку подлинности сообщения и передачу подтверждения.

11.7. Особенности защиты информации в базах данных

Базы данных рассматриваются как надежное хранилище структурированных данных, снабженное специальным механизмом для их эффективного использования в интересах пользователей (процессов). Таким механизмом является система управления базой данных (СУБД). Под системой управления базой данных понимаются программные или аппаратно-программные средства, реализующие функции управления данными, такие как: просмотр, сортировка, выборка, модификация, выполнение операций определения статистических характеристик и т. п. Базы данных размещаются:

- на компьютерной системе пользователя;
- на специально выделенной ЭВМ (сервере).

Как правило, на компьютерной системе пользователя размещаются личные или персональные базы данных, которые обслуживают процессы одного пользователя.

В вычислительных сетях базы данных размещаются на серверах. В локальных и корпоративных сетях, как правило, используются централизованные базы данных. Общедоступные глобальные сети имеют распределенные базы данных. В таких сетях серверы размещаются на различных объектах сети. В качестве серверов часто используются специализированные ЭВМ, приспособленные к хранению больших объемов данных, обеспечивающие сохранность и доступность информации, а также оперативность обработки поступающих запросов. В централизованных базах данных проще решаются проблемы защиты информации от преднамеренных угроз, поддержания актуальности и непротиворечивости данных. Достоинством распределенных баз данных, при условии дублирования данных, является их высокая защищенность от стихийных бедствий, аварий, сбоев технических средств, а также диверсий.

Защита информации в базах данных, в отличие от защиты данных в файлах, имеет и свои особенности:

- необходимость учета функционирования системы управления базой данных при выборе механизмов защиты;
- разграничение доступа к информации реализуется не на уровне файлов, а на уровне частей баз данных;

При создании средств защиты информации в базах данных необходимо учитывать взаимодействие этих средств не только с ОС, но и с СУБД. При этом возможно встраивание механизмов защиты в СУБД или использование их в виде отдельных компонент. Для большинства СУБД придание им дополнительных функций возможно только на этапе разработки СУБД. В эксплуатируемые системы управления базами данных дополнительные компоненты могут быть внесены путем расширения или модификации языка управления. Таким путем можно осуществлять наращивание возможностей, например, в СУБД CA-Clipper 5.0.

В современных базах данных довольно успешно решаются задачи разграничения доступа, поддержания физической целостности и логической сохранности данных. Алгоритмы разграничения доступа к записям и даже к полям записей в соответствии с полномочиями пользователя хорошо отработаны, и преодолеть эту защиту злоумышленник может лишь с помощью фальсификации полномочий или внедрения вредительских программ. Разграничение доступа к файлам баз данных и к частям баз данных осуществляется СУБД путем установления полномочий пользователей и контроля этих полномочий при допуске к объектам доступа.

Полномочия пользователей устанавливаются администратором СУБД. Обычно стандартным идентификатором пользователя является пароль, передаваемый в зашифрованном виде. В распределенных КС процесс подтверждения подлинности пользователя дополняется специальной процедурой взаимной аутентификации удаленных процессов. Базы данных, содержащих конфиденциальную информацию, хранятся на внешних запоминающих устройствах в зашифрованном виде.

Физическая целостность баз данных достигается путем использования отказоустойчивых устройств, построенных, например, по технологии RAID. Логическая сохранность данных означает невозможность нарушения структуры модели данных. Со-

временные СУБД обеспечивают такую логическую целостность и непротиворечивость на этапе описания модели данных.

В базах данных, работающих с конфиденциальной информацией, необходимо дополнительно использовать криптографические средства закрытия информации. Для этой цели используется шифрование как с помощью единого ключа, так и с помощью индивидуальных ключей пользователей. Применение шифрования с индивидуальными ключами повышает надежность механизма разграничения доступа, но существенно усложняет управление.

Возможны два режима работы с зашифрованными базами данных. Наиболее простым является такой порядок работы с закрытыми данными, при котором для выполнения запроса необходимый файл или часть файла расшифровывается на внешнем носителе, с открытой информацией производятся необходимые действия, после чего информация на ВЗУ снова зашифровывается. Достоинством такого режима является независимость функционирования средств шифрования и СУБД, которые работают последовательно друг за другом. В то же время сбой или отказ в системе может привести к тому, что на ВЗУ часть базы данных останется записанной в открытом виде.

Второй режим предполагает возможность выполнения СУБД запросов пользователей без расшифрования информации на ВЗУ. Поиск необходимых файлов, записей, полей, групп полей не требует расшифрования. Расшифрование производится в ОП непосредственно перед выполнением конкретных действий с данными. Такой режим возможен, если процедуры шифрования встроены в СУБД. При этом достигается высокий уровень защиты от несанкционированного доступа, но реализация режима связана с усложнением СУБД. Придание СУБД возможности поддержки такого режима работы осуществляется, как правило, на этапе разработки СУБД.

При построении защиты баз данных необходимо учитывать ряд специфических угроз безопасности информации, связанных с концентрацией в базах данных большого количества разнообразной информации, а также с возможностью использования сложных запросов обработки данных. К таким угрозам относятся:

- инференция;
- агрегирование;

• комбинация разрешенных запросов для получения закрьН / тых данных. i

Под **инференцией** понимается получение конфиденциальной ! информации из сведений с меньшей степенью конфиденциально-* сти путем умозаключений. Если учитывать, что в базах данных* хранится информация, полученная из различных источников в разное время, отличающаяся степенью обобщенности, то аналитик может получить конфиденциальные сведения путем сравнения, дополнения и фильтрации данных, к которым он допущен. Кроме того, он обрабатывает информацию, полученную из открытых баз данных, средств массовой информации, а также использует просчеты лиц, определяющих степень важности и конфиденциальности отдельных явлений, процессов, фактов, полученных результатов. Такой способ получения конфиденциальных сведений, например, по материалам средств массовой информации, используется давно, и показал свою эффективность.

Близким к инференции является другой способ добывания конфиденциальных сведений - агрегирование. Под **агрегированием** понимается способ получения более важных сведений по сравнению с важностью тех отдельно взятых данных, на основе которых и получаются эти сведения. Так, сведения о деятельности одного отделения или филиала корпорации обладают определенным весом. Данные же за всю корпорацию имеют куда большую значимость.

Если инференция и агрегирование являются способами добывания информации, которые применяются не только в отношении баз данных, то способ специального **комбинирования запросов** используется только при работе с базами данных. Использование сложных, а также последовательности простых логически связанных запросов позволяет получать данные, к которым доступ пользователю закрыт. Такая возможность имеется, прежде всего, в базах данных, позволяющих получать статистические данные. При этом отдельные записи, поля, (индивидуальные данные) являются закрытыми. В результате запроса, в котором могут использоваться логические операции AND, OR, NOT, пользователь может получить такие величины как количество записей, сумма, максимальное или минимальное значение. Используя сложные перекрестные запросы и имеющуюся в его распоряжении дополнительную ин-

формацию об особенностях интересующей записи (поля), злоумышленник путем последовательной фильтрации записей может получить доступ к нужной записи (полю).

Противодействие подобным угрозам осуществляется следующими методами:

- блокировка ответа при неправильном числе запросов;
- искажение ответа путем округления и другой преднамеренной коррекции данных;
- разделение баз данных;
- случайный выбор записи для обработки;
- контекстно-ориентированная защита;
- контроль поступающих запросов.

Метод **блокировки ответа** при неправильном числе запросов предполагает отказ в выполнении запроса, если в нем содержится больше определенного числа совпадающих записей из предыдущих запросов. Таким образом, данный метод обеспечивает выполнение принципа минимальной взаимосвязи вопросов. Этот метод сложен в реализации, так как необходимо запоминать и сравнивать все предыдущие запросы.

Метод **коррекции** заключается в незначительном изменении точного ответа на запрос пользователя. Для того, чтобы сохранить приемлемую точность статистической информации, применяется так называемый свопинг данных. Сущность его заключается во взаимном обмене значений полей записи, в результате чего все статистики i-го порядка, включающие i атрибутов, оказываются защищенными для всех i, меньших или равных некоторому числу. Если злоумышленник сможет выявить некоторые данные, то он не сможет определить, к какой конкретно записи они относятся.

Применяется также метод **разделения баз данных** на группы. В каждую группу может быть включено не более определенного числа записей. Запросы разрешены к любому множеству групп, но запрещаются к подмножеству записей из одной группы. Применение этого метода ограничивает возможности выделения данных злоумышленником на уровне не ниже группы записей. Метод разделения баз данных не нашел широкого применения из-за сложности получения статистических данных, обновления и реструктуризации данных.

Эффективным методом противодействия исследованию баз

данных является метод **случайного выбора записей** для статистической обработки. Такая организация выбора записей не позволяет злоумышленнику проследить множество запросов.

Сущность **контекстно-ориентированной защиты** заключается в назначении атрибутов доступа (чтение, вставка, удаление, обновление, управление и т. д.) элементам базы данных (записям, полям, группам полей) в зависимости от предыдущих запросов пользователя. Например, пусть пользователю доступны в отдельных запросах поля: «идентификационные номера» и «фамилии сотрудников», а также «идентификационные номера» и «размер заработной платы». Сопоставив ответы по этим запросам, пользователь может получить закрытую информацию о заработной плате конкретных работников. Для исключения такой возможности пользователю следует запретить доступ к полю «идентификатор сотрудника» во втором запросе, если он уже выполнил первый запрос.

Одним из наиболее эффективных методов защиты информации в базах данных является **контроль поступающих запросов** на наличие «подозрительных» запросов или комбинации запросов. Анализ подобных попыток позволяет выявить возможные каналы получения несанкционированного доступа к закрытым данным.

Контрольные вопросы

1. Назовите особенности защиты информации в РКС.
2. Каким образом обеспечивается защита информации в пользовательских подсистемах и специализированных коммуникационных КС?
3. Приведите основные особенности защиты информации в подсистемах распределенных КС.
4. В чем заключается сущность межсетевого экранирования?
5. Охарактеризуйте защиту информации в базах данных.

Ш. ПОСТРОЕНИЕ И ОРГАНИЗАЦИЯ ФУНКЦИОНИРОВАНИЯ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

ГЛАВА 12
Построение комплексных систем защиты информации

12.1. Концепция создания защищенных КС

При разработке и построении комплексной системы защиты информации в компьютерных системах необходимо придерживаться определенных методологических принципов проведения исследований, проектирования, производства, эксплуатации и развития таких систем. Системы защиты информации относятся к классу сложных систем и для их построения могут использоваться основные принципы построения сложных систем с учетом специфики решаемых задач:

- параллельная разработка КС и СЗИ;
- системный подход к построению защищенных КС;
- многоуровневая структура СЗИ;
- иерархическая система управления СЗИ;
- блочная архитектура защищенных КС;
- возможность развития СЗИ;
- дружественный интерфейс защищенных КС с пользователями и обслуживающим персоналом.

Первый из приведенных принципов построения СЗИ требует проведения одновременной **параллельной разработки КС и механизмов защиты.** Только в этом случае возможно эффективно обеспечить реализацию всех остальных принципов. Причем в

процессе разработки защищенных КС должен соблюдаться разумный компромисс между созданием встроенных неразделимых механизмов защиты и блочных унифицированных средств и процедур защиты. Только на этапе разработки КС можно полностью учесть взаимное влияние блоков и устройств собственно КС и механизмов защиты, добиться системности защиты оптимальным образом.

Принцип системности является одним из основных концептуальных и методологических принципов построения защищенных КС. Он предполагает:

- анализ всех возможных угроз безопасности информации;
- обеспечение защиты на всех жизненных циклах КС;
- защиту информации во всех звеньях КС;
- комплексное использование механизмов защиты.

Потенциальные угрозы выявляются в процессе создания и исследования модели угроз. В результате исследований должны быть получены данные о возможных угрозах безопасности информации, о степени их опасности и вероятности реализации. При построении СЗИ учитываются потенциальные угрозы, реализация которых может привести к существенному ущербу и вероятность таких событий не является очень близкой к нулю.

Защита ресурсов КС должна осуществляться на этапах разработки, производства, эксплуатации и модернизации, а также по всей технологической цепочке ввода, обработки, передачи, хранения и выдачи информации. Реализация этих принципов позволяет обеспечить создание СЗИ, в которой отсутствуют слабые звенья как на различных жизненных циклах КС, так и в любых элементах и режимах работы КС.

Механизмы защиты, которые используются при построении защищенных систем, должны быть взаимоувязаны по месту, времени и характеру действия. Комплексность предполагает также использование в оптимальном сочетании различных методов и средств защиты информации: технических, программных, криптографических, организационных и правовых. Любая, даже простая СЗИ является комплексной.

Система защиты информации должна иметь несколько уровней, перекрывающих друг друга, т. е. такие системы целесообразно строить по принципу построения матрешек. Чтобы добраться

до закрытой информации, злоумышленнику необходимо «взломать» все уровни защиты (рис. 28).

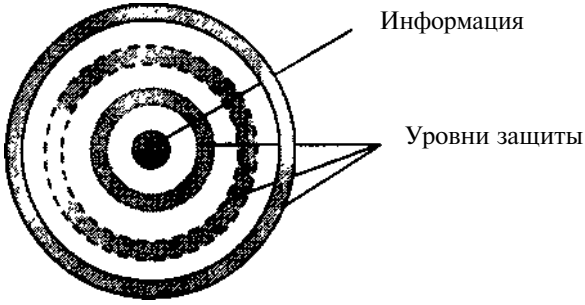


Рис. 28. Многоуровневая КСЗИ

Например, для отдельного объекта КС можно выделить 6 уровней (рубежей) защиты:

1) охрана по периметру территории объекта;
2) охрана по периметру здания;
3) охрана помещения;
4) защита аппаратных средств;
5) защита программных средств;
6) защита информации.

Комплексные системы защиты информации всегда должны иметь **централизованное управление.** В распределенных КС управление защитой может осуществляться по иерархическому принципу. Централизация управления защитой информации объясняется необходимостью проведения единой политики в области безопасности информационных ресурсов в рамках предприятия, организации, корпорации, министерства. Для осуществления централизованного управления в СЗИ должны быть предусмотрены специальные средства дистанционного контроля, распределения ключей, разграничения доступа, изготовления атрибутов идентификации и другие.

Одним из важных принципов построения защищенных КС является использование **блочной архитектуры.** Применение данного принципа позволяет получить целый ряд преимуществ:

- упрощается разработка, отладка, контроль и верификация устройств (программ, алгоритмов);
- допускается параллельность разработки блоков;
- используются унифицированные стандартные блоки;
- упрощается модернизация систем;
- удобство и простота эксплуатации.

Основываясь на принципе блочной архитектуры защищенной КС, можно представить структуру идеальной защищенной системы. В такой системе имеется минимальное ядро защиты, отвечающее нижней границе защищенности систем определенного класса (например, ПЭВМ). Если в системе необходимо обеспечить более высокий уровень защиты, то это достигается за счет согласованного подключения аппаратных блоков или инсталляции дополнительных программных средств (аналог режима «Plug and Play» в ОС Windows 98).

В случае необходимости могут быть использованы более совершенные блоки КС, чтобы не допустить снижения эффективности применения системы по прямому назначению. Это объясняется потреблением части ресурсов КС вводимыми блоками защиты.

Стандартные входные и выходные интерфейсы блоков позволяют упростить процесс модернизации СЗИ, альтернативно использовать аппаратные или программные блоки. Здесь просматривается аналогия с семиуровневой моделью OSI.

При разработке сложной КС, например, вычислительной сети, необходимо предусматривать *возможность ее развития* в двух направлениях: увеличения числа пользователей и наращивания возможностей сети по мере совершенствования информационных технологий.

С этой целью при разработке КС предусматривается определенный запас ресурсов по сравнению с потребностями на момент разработки. Наибольший запас производительности необходимо предусмотреть для наиболее консервативной части сложных систем - каналов связи. Часть резерва ресурсов КС может быть востребована при развитии СЗИ. На практике резерв ресурсов, предусмотренный на этапе разработки, исчерпывается уже на момент полного ввода в эксплуатацию сложных систем. Поэтому при разработке КС предусматривается возможность модернизации системы. В этом смысле сложные системы должны быть развиваю-

щимися или открытыми. Термин открытости в этой трактовке относится и к защищенным КС. Причем механизмы защиты, постоянно совершенствуясь, вызывают необходимость наращивания ресурсов КС. Новые возможности, режимы КС, а также появление новых угроз в свою очередь стимулируют развитие новых механизмов защиты. Важное место в процессе создания открытых систем играют международные стандарты в области взаимодействия устройств, подсистем. Они позволяют использовать подсистемы различных типов, имеющих стандартные интерфейсы взаимодействия.

Комплексная система защиты информации должна быть дружественной по отношению к пользователям и обслуживающему персоналу. Она должна быть максимально автоматизирована и не должна требовать от пользователя выполнять значительный объем действий, связанных с СЗИ. Комплексная СЗИ не должна создавать ограничений в выполнении пользователем своих функциональных обязанностей. В СЗИ необходимо предусмотреть меры снятия защиты с отказавших устройств для восстановления их работоспособности.

12.2. Этапы создания комплексной системы защиты информации

Система защиты информации должна создаваться совместно с создаваемой компьютерной системой. При построении системы защиты могут использоваться существующие средства защиты, или же они разрабатываются специально для конкретной КС. В зависимости от особенностей компьютерной системы, условий ее эксплуатации и требований к защите информации процесс создания КСЗИ может не содержать отдельных этапов, или содержание их может несколько отличаться от общепринятых норм при разработке сложных аппаратно-программных систем. Но обычно разработка таких систем включает следующие этапы:

- разработка технического задания;
- эскизное проектирование;
- техническое проектирование;
- рабочее проектирование;
- производство опытного образца.

Одним из основных этапов разработки КСЗИ является этап разработки технического задания. Именно на этом этапе решаются практически все специфические задачи, характерные именно для разработки КСЗИ.

Процесс разработки систем, заканчивающийся выработкой технического задания, называют научно-исследовательской разработкой, а остальную часть работы по созданию сложной системы называют опытно-конструкторской разработкой. Опытно-конструкторская разработка аппаратно-программных средств ведется с применением систем автоматизации проектирования, алгоритмы проектирования хорошо изучены и отработаны. Поэтому особый интерес представляет рассмотрение процесса научно-исследовательского проектирования.

12.3. Научно-исследовательская разработка КСЗИ

Целью этого этапа является разработка технического задания на проектирование КСЗИ. Техническое задание содержит основные технические требования к разрабатываемой КСЗИ, а также согласованные взаимные обязательства заказчика и исполнителя разработки. Технические требования определяют значения основных технических характеристик, выполняемые функции, режимы работы, взаимодействие с внешними системами и т. д.

Аппаратные средства оцениваются следующими характеристиками: быстродействие, производительность, емкость запоминающих устройств, разрядность, стоимость, характеристики надежности и др. Программные средства характеризуются требуемым объемом оперативной и внешней памяти, системой программирования, в которой разработаны эти средства, совместимостью с ОС и другими программными средствами, временем выполнения, стоимостью и т. д.

Получение значений этих характеристик, а также состава выполняемых функций и режимов работы средств защиты, порядка их использования и взаимодействия с внешними системами составляют основное содержание этапа научно-исследовательской разработки. Для проведения исследований на этом этапе заказчик может привлекать исполнителя или научно-исследовательское учреждение, либо организует совместную их работу.

Научно-исследовательская разработка начинается с анализа угроз безопасности информации, анализа защищаемой КС и анализа конфиденциальности и важности информации в КС (рис. 29).

Рис. 29. Последовательность и содержание научно-исследовательской разработки КСЗИ

Прежде всего производится анализ конфиденциальности и важности информации, которая должна обрабатываться, храниться и передаваться в КС. На основе анализа делается вывод о целесообразности создания КСЗИ. Если информация не является конфиденциальной и легко может быть восстановлена, то создавать КСЗИ нет необходимости. Не имеет смысла также создавать

КСЗИ в КС, если потеря целостности и конфиденциальности информации связана с незначительными потерями. . *ш*

В этих случаях достаточно использовать штатные средства КС! и, возможно, страхование от утраты информации.

При анализе информации определяются потоки конфиденциальной информации, элементы КС, в которых она обрабатывается и хранится. На этом этапе рассматриваются также вопросы разграничения доступа к информации отдельных пользователей и целых сегментов КС. На основе анализа информации определяются требования к ее защищенности. Требования задаются путем присвоения определенного грифа конфиденциальности, установления правил разграничения доступа.

Очень важная исходная информация для построения КСЗИ получается в результате анализа защищаемой КС. Так как КСЗИ является подсистемой КС, то взаимодействие системы защиты с КС можно определить как внутреннее, а взаимодействие с внешней средой - как внешнее (рис. 30).

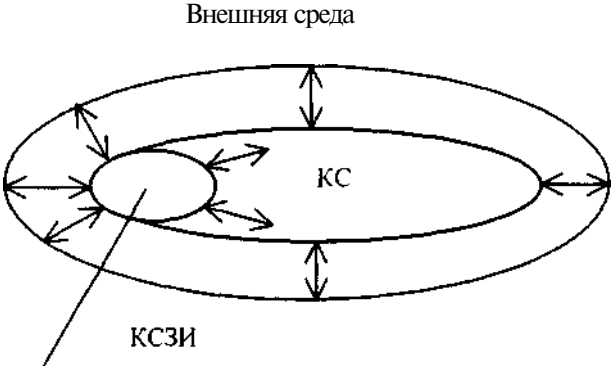


Рис. 30. Схема взаимодействия КСЗИ

Внутренние условия взаимодействия определяются архитектурой КС. При построении КСЗИ учитываются:

- географическое положение КС;
- тип КС (распределенная или сосредоточенная);
- структуры КС (техническая, программная, информационная и т. д.);
- производительность и надежность элементов КС;

- типы используемых аппаратных и программных средств и режимы их работы;
- угрозы безопасности информации, которые порождаются внутри КС (отказы аппаратных и программных средств, алгоритмические ошибки и т. п.).

Учитываются следующие внешние условия:

- взаимодействие с внешними системами;
- случайные и преднамеренные угрозы.

Анализ угроз безопасности является одним из обязательных условий построения КСЗИ. По результатам проведенного анализа строится модель угроз безопасности информации в КС. Модель угроз безопасности информации в КС содержит систематизированные данные о случайных и преднамеренных угрозах безопасности информации в конкретной КС. Систематизация данных модели предполагает наличие сведений обо всех возможных угрозах, их опасности, временных рамках действия, вероятности реализации. Часто модель угроз рассматривается как композиция модели злоумышленника и модели случайных угроз. Модели представляются в виде таблиц, графов или на вербальном уровне. При построении модели злоумышленника используются два подхода:

1) модель ориентируется только на высококвалифицированного злоумышленника-профессионала, оснащенного всем необходимым и имеющего легальный доступ на всех рубежах защиты;

2) модель учитывает квалификацию злоумышленника, его оснащенность (возможности) и официальный статус в КС.

Первый подход проще реализуется и позволяет определить верхнюю границу преднамеренных угроз безопасности информации.

Второй подход отличается гибкостью и позволяет учитывать особенности КС в полной мере. Градация злоумышленников по их квалификации может быть различной. Например, может быть выделено три класса злоумышленников:

1) высококвалифицированный злоумышленник-профессионал;

2) квалифицированный злоумышленник-непрофессионал;

3) неквалифицированный злоумышленник-непрофессионал.

Класс злоумышленника, его оснащенность и статус на объекте КС определяют возможности злоумышленника по несанкционированному доступу к ресурсам КС.

Угрозы, связанные с непреднамеренными действиями, хорошо изучены, и большая часть их может быть формализована. Сюда следует отнести угрозы безопасности, которые связаны с конечной надежностью технических систем. Угрозы, порождаемые стихией или человеком, формализовать сложнее. Но с другой стороны, по ним накоплен большой объем статистических данных. На основании этих данных можно прогнозировать проявление угроз этого класса.

Модель злоумышленника и модель случайных угроз позволяют получить полный спектр угроз и их характеристик. В совокупности с исходными данными, полученными в результате анализа информации, особенностей архитектуры проектируемой КС, модели угроз безопасности информации позволяют получить исходные данные для построения модели КСЗИ.

12.4. Моделирование КСЗИ

Оценка эффективности функционирования КСЗИ представляет собой сложную научно-техническую задачу. Комплексная СЗИ оценивается в процессе разработки КС, в период эксплуатации и при создании (модернизации) СЗИ для уже существующих КС. При разработке сложных систем распространенным методом проектирования является синтез с последующим анализом. Система синтезируется путем согласованного объединения блоков, устройств, подсистем и анализируется (оценивается) эффективность полученного решения. Из множества синтезированных систем выбирается лучшая по результатам анализа, который осуществляется с помощью моделирования.

Моделирование КСЗИ заключается в построении образа (модели) системы, с определенной точностью воспроизводящего процессы, происходящие в реальной системе [30]. Реализация модели позволяет получать и исследовать характеристики реальной системы.

Для оценки систем используются аналитические и имитационные модели. **В *аналитических моделях*** функционирование исследуемой системы записывается в виде математических или логических соотношений. Для этих целей используется мощный математический аппарат: алгебра, функциональный анализ, раз-

ностные уравнения, теория вероятностей, математическая статистика, теория множеств, теория массового обслуживания и т. д.

При *имитационном моделировании* моделируемая система представляется в виде некоторого аналога реальной системы. В процессе имитационного моделирования на ЭВМ реализуются алгоритмы изменения основных характеристик реальной системы в соответствии с эквивалентными реальным процессам математическими и логическими зависимостями.

Модели делятся также на детерминированные и стохастические. Модели, которые оперируют со случайными величинами, называются *стохастическими*. Так как на процессы защиты информации основное влияние оказывают случайные факторы, то модели систем защиты являются стохастическими.

Моделирование КСЗИ является сложной задачей, потому что такие системы относятся к классу сложных организационно-технических систем, которым присущи следующие особенности [30]:

- сложность формального представления процессов функционирования таких систем, главным образом, из-за сложности формализации действий человека;
- многообразие архитектур сложной системы, которое обуславливается многообразием структур ее подсистем и множественностью путей объединения подсистем в единую систему;
- большое число взаимосвязанных между собой элементов и подсистем;
- сложность функций, выполняемых системой;
- функционирование систем в условиях неполной определенности и случайности процессов, оказывающих воздействие на систему;
- наличие множества критериев оценки эффективности функционирования сложной системы;
- существование интегрированных признаков, присущих системе в целом, но не свойственных каждому элементу в отдельности (например, система с резервированием является надежной, при ненадежных элементах);
- наличие управления, часто имеющего сложную иерархическую структуру;

• разветвленность и высокая интенсивность **информационных** потоков.

Для преодоления этих сложностей применяются:

1) специальные методы неформального моделирования;

2) декомпозиция общей задачи на ряд частных задач;

3) макромоделирование.

12.4.1. Специальные методы неформального моделирования

Специальные методы неформального моделирования основаны на применении неформальной теории систем. Основными составными частями неформальной теории систем являются [8]:

- структурирование архитектуры и процессов функционирования сложных систем;
- неформальные методы оценивания;
- неформальные методы поиска оптимальных **решений.**

Структурирование является развитием формального описания систем, распространенного на организационно-технические системы.

Примером структурированного процесса является конвейерное производство. В основе такого производства лежат два принципа:

- строгая регламентация технологического процесса производства;
- специализация исполнителей и оборудования.

Предполагается, что конструкция производимой продукции отвечает следующим требованиям:

- изделие состоит из конструктивных иерархических элементов (блоков, узлов, схем, деталей и т.п.);
- максимальная простота, унифицированность и стандартность конструктивных решений и технологических операций.

В настоящее время процесс производства технических средств КС достаточно полно структурирован. Структурное программирование также вписывается в рамки структурированных процессов. На основе обобщения принципо'в и методов структурного программирования могут быть сформулированы условия структурированного описания изучаемых систем и процессов их функционирования [8]:

1) полнота **отображения основных элементов** и **их взаимосвязей;**

2) адекватность;

3) простота внутренней организации элементов описания и взаимосвязей элементов между собой;

4) стандартность и унифицированность внутренней структуры элементов и структуры взаимосвязей между ними;

5) модульность;

6) гибкость, под которой понимается возможность расширения и изменения структуры одних компонентов модели без существенных изменений других компонентов;

7) доступность изучения и использования модели любому специалисту средней квалификации соответствующего профиля.

В процессе проектирования систем необходимо получить их характеристики. Некоторые характеристики могут быть получены путем измерения. Другие получаются с использованием аналитических соотношений, а также в процессе обработки статистических данных. Однако существуют характеристики сложных систем, которые не могут быть получены приведенными методами. К таким характеристикам СЗИ относятся вероятности реализации некоторых угроз, отдельные характеристики эффективности систем защиты и другие.

Указанные характеристики могут быть получены единственно доступными методами - методами ***неформального оценивания.*** Сущность методов заключается в привлечении для получения некоторых характеристик специалистов-экспертов в соответствующих областях знаний.

Наибольшее распространение из неформальных методов оценивания получили методы экспертных оценок. Метод экспертных оценок представляет собой алгоритм подбора специалистов-экспертов, задания правил получения независимых оценок каждым экспертом и последующей статистической обработки полученных результатов. Методы экспертных оценок используются давно, хорошо отработаны. В некоторых случаях они являются единственно возможными методами оценивания характеристик систем.

Неформальные методы поиска оптимальных решении могут быть распределены по двум группам:

- методы неформального сведения сложной задачи к формальному описанию и решение задачи формальными методами;
- неформальный поиск оптимального решения.

Для моделирования систем защиты информации целесообразно использовать следующие теории и методы, позволяющие свести решение задачи к формальным алгоритмам:

- теория нечетких множеств;
- теория конфликтов;
- теория графов;
- формально-эвристические методы;
- эволюционное моделирование.

Методы *теории нечетких множеств* позволяют получать аналитические выражения для количественных оценок нечетких условий принадлежности элементов к тому или иному множеству. Теория нечетких множеств хорошо согласуется с условиями моделирования систем защиты, так как многие исходные данные моделирования (например, характеристики угроз и отдельных механизмов защиты) не являются строго определенными.

Теория конфликтов является относительно новым направлением исследования сложных человеко-машинных систем. Конфликт между злоумышленником и системой защиты, разворачивающийся на фоне случайных угроз, является классическим для применения теории конфликта. Две противоборствующие стороны преследуют строго противоположные цели. Конфликт развивается в условиях неоднозначности и слабой предсказуемости процессов, способности сторон оперативно изменять цели. Теория конфликтов является развитием теории игр. Теория игр позволяет:

- структурировать задачу, представить ее в обозримом виде, найти области количественных оценок, упорядочений, предпочтений, выявить доминирующие стратегии, если они существуют;
- до конца решить задачи, которые описываются стохастическими моделями.

Теория игр позволяет найти решение, оптимальное или рациональное в среднем. Она исходит из принципа минимизации среднего риска. Такой подход не вполне адекватно отражает поведение сторон в реальных конфликтах, каждый из которых является уникальным. В теории конфликтов предпринята попытка преодо-

ления этих недостатков теории игр. Теория конфликтов позволяет решать ряд практических задач исследования сложных систем. Однако она еще не получила широкого распространения и открыта для дальнейшего развития.

Из *теории графов* для исследования систем защиты информации в наибольшей степени применим аппарат сетей Петри. Управление условиями в узлах сети Петри позволяет моделировать процессы преодоления защиты злоумышленником. Аппарат сетей Петри позволяет формализовать процесс исследования эффективности СЗИ.

К *формально-эвристическим методам* отнесены методы поиска оптимальных решений не на основе строгих математических, логических соотношений, а основываясь на опыте человека, имеющихся знаниях и интуиции. Получаемые решения могут быть далеки от оптимальных, но они всегда будут лучше решений, получаемых без эвристических методов.

Наибольшее распространение из эвристических методов получили лабиринтные и концептуальные методы.

В соответствии с лабиринтной моделью задача представляется человеку в виде лабиринта возможных путей решения. Предполагается, что человек обладает способностью быстрого отсечения бесперспективных путей движения по лабиринту. В результате среди оставшихся путей с большой вероятностью находится путь, ведущий к решению поставленной задачи.

Концептуальный метод предполагает выполнение действий с концептами. Под концептами понимаются обобщенные элементы и связи между ними. Концепты получаются человеком, возможно и неосознанно, в процессе построения структурированной модели. В соответствии с концептуальным методом набор концепт универсален и ему соответствуют имеющиеся у человека механизмы вычисления, трансформации и формирования отношений. Человек проводит мысленный эксперимент со структурированной моделью и порождает ограниченный участок лабиринта, в котором уже несложно найти решение.

Эволюционное моделирование представляет собой разновидность имитационного моделирования. Особенность его заключается в том, что в процессе моделирования совершенствуется алгоритм моделирования.

Сущность неформальных методов непосредственного поиска оптимальных решений состоит в том, что человек участвует не только в построении модели, но и в процессе ее реализации.

12.4.2. Декомпозиция общей задачи оценки эффективности функционирования КСЗИ

Сложность выполняемых функций, значительная доля нечетко определенных исходных данных, большое количество механизмов защиты, сложность их взаимных связей и многие другие факторы делают практически неразрешимой проблему оценки эффективности системы в целом с помощью одного какого-либо метода моделирования.

Для решения этой проблемы применяется метод декомпозиции (разделения) общей задачи оценки эффективности на ряд частных задач. Так, задача оценки эффективности КСЗИ может разбиваться на частные задачи:

- оценку эффективности защиты от сбоев и отказов аппаратных и программных средств;
- оценку эффективности защиты от НСДИ;
- оценку эффективности защиты от ПЭМИН и т. д.

При оценке эффективности защиты от отказов, приводящих к уничтожению информации, используется, например, такая величина, как вероятность безотказной работы P(t) системы за время t.

Этот показатель вычисляется по формуле:

$$P(t)=1-Pox_к(t),$$

где РотказО) - вероятность отказа системы за время t.

Величина РотказО), в свою очередь, определяется в соответствии с известным выражением:

$$P_{отк}(t) = e^{-Xt},$$

где *X* - интенсивность отказов системы.

Таким образом, частная задача оценки влияния отказов на безопасность информации может быть довольно просто решена известными формальными методами.

Довольно просто решается частная задача оценки эффективности метода шифрования при условии, что атака на шифр возможна только путем перебора ключей, и известен метод шифрования.

Среднее **время** взлома **шифра** при этих **условиях определяется по** формуле:

$$T = \frac{A^S t}{2},$$

где T - среднее время взлома шифра; A - число символов, которые могут быть использованы при выборе ключа (мощность алфавита шифрования); S - длина ключа, выраженная в количестве символов; t - время проверки одного ключа.

Время t зависит от производительности, используемой для атаки на шифр КС и сложности алгоритма шифрования. При расчете криптостойкости обычно считается, что злоумышленник имеет в своем распоряжении КС наивысшей производительности, уже существующей или перспективной.

В свою очередь частные задачи могут быть декомпозированы на подзадачи.

Главная сложность метода декомпозиции при оценке систем заключается в учете взаимосвязи и взаимного влияния частных задач оценивания и оптимизации. Это влияние учитывается как при решении задачи декомпозиции, так и в процессе получения интегральных оценок. Например, при решении задачи защиты информации от электромагнитных излучений используется экранирование металлическими экранами, а для повышения надежности функционирования системы необходимо резервирование блоков, в том числе и блоков, обеспечивающих бесперебойное питание. Решение этих двух частных задач взаимосвязано, например, при создании КСЗИ на летательных аппаратах, где существуют строгие ограничения на вес. При декомпозиции задачи оптимизации комплексной системы защиты приходится всякий раз учитывать общий лимит веса оборудования.

12.4.3. Макромоделирование

При оценке сложных систем используется также макромоделирование. Такое моделирование осуществляется для общей оценки системы. Задача при этом упрощается за счет использования при построении модели только основных характеристик. К макромоделированию прибегают в основном для получения предварительных оценок систем.

В качестве макромодели можно рассматривать модель КСЗИ, представленной на рис. 30. Если в КСЗИ используется **к** уровней защиты, то в зависимости от выбранной модели злоумышленника ему необходимо преодолеть k-m уровней защиты, где m - номер наивысшего уровня защиты, который злоумышленник беспрепятственно преодолевает в соответствии со своим официальным статусом. Если злоумышленник не имеет никакого официального статуса на объекте КС, то ему, в общем случае, необходимо преодолеть все **к** уровней защиты, чтобы получить доступ к информации. Для такого злоумышленника вероятность получения несанкционированного доступа к информации $P_{„сд}$ может быть рассчитана по формуле:

где P_i - вероятность преодоления злоумышленником i-го уровня защиты.

На макроуровне можно, например, исследовать требуемое число уровней защиты, их эффективность по отношению к предполагаемой модели нарушителя с учетом особенностей КС и финансовых возможностей проектирования и построения КСЗИ.

12.5. Выбор показателей эффективности и критериев оптимальности КСЗИ

Эффективность систем оценивается с помощью показателей эффективности. Иногда используется термин - показатель качества. Показателями качества, как правило, характеризуют степень совершенства какого-либо товара, устройства, машины. В отношении сложных человеко-машинных систем предпочтительнее использование термина **показатель эффективности функционирования,** который характеризует степень соответствия оцениваемой системы своему назначению.

Показатели эффективности системы, как правило, представляют собой некоторое множество функций y_k от характеристик системы x_i:

$$y_k = f(x_1 x_2, \ldots, x_n),\ k=1,K,\ n=1,N,$$

где K - мощность множества показателей эффективности системы, N - мощность множества характеристик системы.

Характеристиками системы $x_1, x_2, \ldots, x_n$ называются первичные данные, отражающие свойства и особенности системы. Используются количественные и качественные характеристики. Количественные характеристики систем имеют числовое выражение. Их называют также параметрами. К *количественным* характеристикам относят разрядность устройства, быстродействие процессора и памяти, длину пароля, длину ключа шифрования и т. п. *Качественные* характеристики определяют наличие (отсутствие) определенных режимов, защитных механизмов или сравнительную степень свойств систем («хорошо», «удовлетворительно», «лучше», «хуже»).

Примером показателя эффективности является криптостойкость шифра, которая выражается временем или стоимостью взлома шифра. Этот показатель для шифра DES, например, зависит от одной характеристики - разрядности ключа. Для методов замены криптостойкость зависит от количества используемых алфавитов замены, а для методов перестановок - от размерности таблицы и количества используемых маршрутов Гамильтона.

Для того чтобы оценить эффективность системы защиты информации или сравнить системы по их эффективности, необходимо задать некоторое правило предпочтения. Такое правило или соотношение, основанное на использовании показателей эффективности, называют критерием эффективности. Для получения критерия эффективности при использовании некоторого множества к показателей используют ряд подходов.

1. Выбирается один *главный показатель,* и оптимальной считается система, для которой этот показатель достигает экстремума. При условии, что остальные показатели удовлетворяют системе ограничений, заданных в виде неравенств. Например, оптимальной может считаться система, удовлетворяющая следующему критерию эффективности:

$$P_m = P\text{^}** \quad \text{при}$$

$$C<C_{доп} \quad , G<G_{Мп},$$

где $P_ю$ - вероятность непреодоления злоумышленником системы защиты за определенное время, С и G - стоимостные и весовые показатели, соответственно, которые не должны превышать допустимых значений.

2. Методы, основанные на ***ранжировании показателей*** по важности. При сравнении систем одноименные показатели эффективности сопоставляются в порядке убывания их важности по определенным алгоритмам.

Примерами таких методов могут служить лексикографический метод и метод последовательных уступок.

Лексикографический метод применим, если степень различия показателей по важности велика. Две системы сравниваются сначала по наиболее важному показателю. Оптимальной считается такая система, у которой лучше этот показатель. При равенстве самых важных показателей сравниваются показатели, занимающие по рангу вторую позицию. При равенстве и этих показателей сравнение продолжается до получения предпочтения в i-м показателе.

Метод последовательных уступок предполагает оптимизацию системы по наиболее важному показателю Yi.

Определяется допустимая величина изменения показателя Y_H которая называется уступкой. Измененная величина показателя: Y'i= Yi ± Ai (Д] - величина уступки) фиксируется. Определяется оптимальная величина показателя Y_2 при фиксированном значении Y'i, выбирается уступка A_2 и процесс повторяется до получеч нияУк-ь

3. *Мультипликативные и аддитивные методы* получения критериев эффективности основываются на объединении всех или» части показателей с помощью операций умножения или сложения^ в обобщенные показатели ($Z_п$,Zc). Показатели, используемые в обобщенных показателях, называют *частными* (у„у,).

Если в произведение (сумму) включается часть показателей» то остальные частные показатели включаются в ограничения. По-> казатели, образующие произведение (сумму), могут иметь весовые коэффициенты к, (к). В общем виде эти методы можно пред-, ставить следующим образом:

$$Z_{\Pi} = extr \prod_i k_i y_i ; \qquad Z_C = extr \sum_j k_j y_j .$$

4. Оценка эффективности СЗИ может осуществляться также ***методом Парето.*** Сущность метода заключается в следующем. При использовании **n** показателей эффективности системе соот-

ветствует точка в n-мерном пространстве. В n-мерном пространстве строится область парето-оптимальных решений. В этой области располагаются несравнимые решения, для которых улучшение какого-либо показателя невозможно без ухудшения других показателей эффективности. Выбор наилучшего решения из числа парето-оптимальных может осуществляться по различным правилам

12.6. Математическая постановка задачи разработки комплексной системы защиты информации

После выбора показателей эффективности и критерия эффективности может быть осуществлена математическая постановка задачи разработки КСЗИ. На этом этапе уже известны:

- F={fi,f2,...,f_n} - функции, которые должна выполнять КСЗИ;
- M={mi,m2,...,mk} - возможные механизмы защиты;
- U={ui,U2,...,u_p} - способы управления КСЗИ.
- \+ У={уьУ2.---.У\у} - показатели эффективности КСЗИ; .

Показатели эффективности зависят от выполняемых функций, механизмов защиты и способов управления КСЗИ: y=d>(F,M,U).

Критерий эффективности получается с использованием показателей эффективности: K=E(У).

Тогда математическая постановка задачи разработки КСЗИ в общем случае может быть представлена в следующем виде:

найти extrS(F,M*,U*), при M* е M, U* е U, которым соответствуют У* е Уд, где Уд - множество допустимых значений показателей эффективности КСЗИ.

То есть, требуется создать или выбрать такие механизмы защиты информации и способы управления системой защиты, при которых обеспечивается выполнение всего множества требуемых функций и достигается максимум или минимум выбранного критерия, а также выполняются ограничения на некоторые показатели эффективности.

Такая постановка применима не только для решения общей, но и частных задач оценки эффективности комплексной системы защиты информации.

12.7. Подходы к оценке эффективности КСЗИ

Эффективность КСЗИ оценивается как на этапе разработки, так и в процессе эксплуатации. В оценке эффективности КСЗИ, в зависимости от используемых показателей и способов их получения, можно выделить три подхода:

- классический;
- официальный;
- экспериментальный.

12.7.1. Классический подход

Под классическим подходом к оценке эффективности понимается использование критериев эффективности, полученных с помощью показателей эффективности. Значения показателей эффективности получаются путем моделирования или вычисляются по характеристикам реальной КС. Такой подход используется при разработке и модернизации КСЗИ. Однако возможности классических методов комплексного оценивания эффективности применительно к КСЗИ ограничены в силу ряда причин. Высокая степень неопределенности исходных данных, сложность формализации процессов функционирования, отсутствие общепризнанных методик расчета показателей эффективности и выбора критериев оптимальности создают значительные трудности для применения классических методов оценки эффективности.

12.7.2. Официальный подход

Большую практическую значимость имеет подход к определению эффективности КСЗИ, который условно можно назвать официальным. Политика безопасности информационных технологий проводится государством и должна опираться на нормативные акты. В этих документах необходимо определить требования к защищенности информации различных категорий конфиденциальности и важности.

Требования могут задаваться перечнем механизмов защиты информации, которые необходимо иметь в КС, чтобы она соответствовала определенному классу защиты. Используя такие до-

кументы, можно оценить эффективность КСЗИ. В этом случае критерием эффективности КСЗИ является ее класс защищенности.

Несомненным достоинством таких классификаторов (стандартов) является простота использования. Основным недостатком официального подхода к определению эффективности систем защиты является то, что не определяется эффективность конкретного механизма защиты, а констатируется лишь факт его наличия или отсутствия. Этот недостаток в какой-то мере компенсируется заданием в некоторых документах достаточно подробных требований к этим механизмам защиты.

Во всех развитых странах разработаны свои стандарты защищенности компьютерных систем критического применения. Так, в министерстве обороны США используется стандарт TCSEC (Department of Defence Trusted Computer System Evaluation Criteria) [42], который известен как Оранжевая книга.

Согласно Оранжевой книге для оценки информационных систем рассматривается четыре группы безопасности: A, B, C, D. В некоторых случаях группы безопасности делятся дополнительно на классы безопасности.

Группа А (гарантированная или проверяемая защита) обеспечивает гарантированный уровень безопасности. Методы защиты, реализованные в системе, могут быть проверены формальными методами. В этой группе имеется только один класс - A1.

Группа В (полномочная или полная защита) представляет полную защиту КС. В этой группе выделены классы безопасности B1, B2 и B3.

Класс B1 (защита через грифы или метки) обеспечивается использованием в КС грифов секретности, определяющих доступ пользователей к частям системы.

Класс B2 (структурированная защита) достигается разделением информации на защищенные и незащищенные блоки и контролем доступа к ним пользователей.

Класс B3 (области или домены безопасности) предусматривает разделение КС на подсистемы с различным уровнем безопасности и контролем доступа к ним пользователей.

Группа С (избирательная защита) представляет избирательную защиту подсистем с контролем доступа к ним пользователей. В этой группе выделены классы безопасности C1 и C2.

Класс С1 (избирательная защита информации) предусматривает разделение в КС пользователей и данных. Этот класс обеспечивает самый низкий уровень защиты КС.

Класс С2 (защита через управляемый или контролируемый доступ) обеспечивается раздельным доступом пользователей к данным.

Группу D (минимальной безопасности) составляют КС, проверенные на безопасность, но которые не могут быть отнесены к классам А, В или С.

Организация защиты информации в вычислительных сетях министерства обороны США осуществляется в соответствии с требованиями руководства «The Trusted Network Interpretation of Department of Defense Trusted Computer System Evaluation Guidelines». Этот документ получил название Красная книга (как и предыдущий - по цвету обложки).

Подобные стандарты защищенности КС приняты и в других развитых странах. Так, в 1991 году Франция, Германия, Нидерланды и Великобритания приняли согласованные «Европейские критерии», в которых рассмотрено 7 классов безопасности от ЕО до Е6.

В Российской Федерации аналогичный стандарт разработан в 1992 году Государственной технической комиссией (ГТК) при Президенте РФ. Этим стандартом является руководящий документ ГТК «Концепция защиты средств вычислительной техники и автоматизированных систем от НСД к информации» [14].

Устанавливается семь классов защищенности средств вычислительной техники (СВТ) от НСД к информации (табл. 2). Самый низкий класс - седьмой, самый высокий - первый.

Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты:

- первая группа содержит только один седьмой класс;
- вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
- третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
- четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

Таблица 2

Показатели защищенности по классам СВТ

Наименование показателя	Класс защищенности					
	6	5	4	3	2	1
1. Дискреционный принцип контроля доступа	+	+	+		+	=
2. Мандатный принцип контроля доступа	-	-	+	=	=	=
3. Очистка памяти	-	+	+	+	=	=
4. Изоляция модулей	-	-	+	=	+	=
5. Маркировка документов	-	-	+	=	=	=
6. Защита ввода и вывода на отчуждаемый физический носитель информации	-	-	+	=	=	=
7. Сопоставление пользователя с устройством	-	-	+	=	=	=
8. Идентификация и аутентификация	+	=	+	=	=	=
9. Гарантия проектирования	-	+	+	+	+	+
10. Регистрация	-	+	+	+	=	=
11. Взаимодействие пользователя с КСЗ	-	-	-	+	=	=
12. Надежное восстановление	-	-	-	+		=
13. Целостность КСЗ	-	+	+	+	=	=
14. Контроль модификации	-	-	-	-	+	=
15. Контроль дистрибуции	-	-	-	-	+	=
16. Гарантии архитектуры	-	-	-	-	-	+
17. Тестирование	+	+	+	+	+	=
18. Руководство пользователя	+		=	=	=	=
19. Руководство по КСЗ	+	+	=	+	+	=
20. Текстовая документация	+	+	+	+	+	=
21. Конструкторская (проектная) документация	+	+	+	+	+	+

Обозначения: «-» - нет требований к данному классу; «+» - новые или дополнительные требования; «=» - требования совпадают с требованиями к СВТ предыдущего класса; КСЗ - комплекс средств защиты.

Седьмой класс присваивают СВТ, к которым предъявлялись требования по защите от НСД к информации, но при оценке защищенность СВТ оказалась ниже уровня требований шестого класса.

Кроме требований к защищенности отдельных элементов СВТ, в Руководящем документе приведены требования к защищенности автоматизированных систем (АС) [14]. В отличие от СВТ автоматизированные системы являются функционально ориентированными. При создании АС учитываются особенности пользовательской информации, технология обработки, хранения и передачи информации, конкретные модели угроз.

Устанавливается девять классов защищенности АС от НСД к информации. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. Третья группа классифицирует АС, с которыми работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А. Во вторую группу сведены АС, пользователи которых имеют одинаковые права доступа ко всей информации АС. Группа содержит два класса - 2Б и 2А. Первую группу составляют многопользовательские АС, в которых пользователи имеют разные права доступа к информации. Группа включает пять классов - 1Д, 1Г, 1В. 1Б, 1А.

Требования ко всем девяти классам защищенности АС сведены в табл. 3.

Таблица 3

Требования к защищенности автоматизированных систем

Подсистемы и требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
1. Подсистема управления доступом 1.1. Идентификация, проверка подлинности и контроль доступа субъектов в систему	+	+	+	+	+	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ				+		+	+	+	+

Продолжение табл. 1.3

к программам				+		+	+	+	+
к томам, каталогам, файлам, записям, полям записей				+		+	+	+	+
1.2. Управление потоками информации				+			+	+	+
2. Подсистема регистрации и учета 2.1. Регистрация и учет: входа/выхода субъектов доступа в/из системы (узла сети)			+	+	+	+	+	+	+
выдачи печатных (графических) выходных документов				+		+	+	+	+
запуска/завершения программ и процессов (заданий, задач)				+		+	+	+	+
доступа программ субъектов к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи				+		+	+	+	+
доступа программ субъектов, доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей				+		+	+	+	+
изменения полномочий субъектов доступа							+	+	+
создаваемых защищаемых объектов доступа				+			+	+	+
2.2. Учет носителей информации			+	+	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей				+		+	+	+	+
2.4. Сигнализация попыток нарушения защиты							+	+	+
3. Криптографическая подсистема 3.1. Шифрование конфиденциальной информации				+				+	+
3.2. Шифрование информации, принадлежащей различным субъек-									+

Окончание табл.3

там доступа (группам субъектов) на разных ключах									
3.3. Использование аттестованных (сертифицированных) криптографических средств									
4. Подсистема обеспечения целостности 4.1. Обеспечение целостности программных средств и обрабатываемой информации									
4.2. Физическая охрана средств вычислительной техники и носителей информации									
4.3. Наличие администратора (службы) защиты информации в АС				+			+	+	+
4.4. Периодическое тестирование СЗИ НСД			+	+	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД			+	+	+	+	+	+	+
4.6.Использование сертифицированных средств защиты				+			+	+	+

Обозначения: «+» - есть требования к данному классу; СЗИ НСД - система защиты информации от несанкционированного доступа.

Для примера целесообразно рассмотреть подробно требования к одному из представительных классов защищенности, а именно - к классу 1 В.

В подсистеме управления доступом автоматизированной системы должны осуществляться:

- идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;
- идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам и/или адресам;
- идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;

• контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;

• управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.

Подсистема регистрации и учета должна обеспечивать:

• регистрацию входа/выхода субъектов доступа в систему/из системы, либо регистрацию загрузки и инициализации операционной системы и ее программного останова;

• регистрацию выдачи печатных (графических) документов на «твердую» копию;

• регистрацию запуска/завершения программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов;

• регистрацию попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;

• регистрацию изменений полномочий субъектов доступа и статуса объектов доступа;

• автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;

• учет всех защищаемых носителей информации с помощью их любой маркировки;

• очистку (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется путем записи последовательности 1 и 0 в любую освобождаемую область памяти, использованную для хранения защищаемой информации;

• сигнализацию попыток нарушения защиты.

Подсистема обеспечения целостности предусматривает:

• обеспечение целостности программных средств СЗИ НСД, а также неизменность программной среды. Целостность СЗИ НСД

проверяется при загрузке системы по контрольным суммам компонент СЗИ, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ при обработке и (или) хранении защищаемой информации;

- охрану СВТ (устройств и носителей информации), что предполагает охрану территории и здания, где размещается АС, с помощью технических средств и специального персонала, строгий пропускной режим, специальное оборудование помещений АС;
- наличие администратора (службы) защиты информации, ответственного за ведение, нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС;
- периодическое тестирование всех функций СЗИ НСД с помощью специальных программ не реже одного раза в год;
- наличие средств восстановления СЗИ НСД (ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности);
- использование сертифицированных средств защиты.

Представленный перечень является тем минимумом требований, которым необходимо следовать, чтобы обеспечить конфиденциальность защищаемой информации.

Стандарт требований TCSEC соответствует информационным системам с применением ЭВМ общего пользования (main frame) и мини ЭВМ. Для персональных ЭВМ (ПЭВМ) и локальных сетей ПЭВМ требования безопасности должны быть несколько иными. Такие требования изложены [42] в стандарте The Trusted Network Interpretation of Department of Defence Trusted Computer System Evaluation Guidelines, получившем название Красная книга. Неофициальные названия стандартов США Оранжевая книга и Красная книга связаны с соответствующим цветом обложек этих документов.

12.7.3. Экспериментальный подход

Под экспериментальным подходом понимается организация процесса определения эффективности существующих КСЗИ пу-

тем попыток преодоления защитных механизмов системы специалистами, выступающими в роли злоумышленников. Такие исследования проводятся следующим образом. В качестве условного злоумышленника выбирается один или несколько специалистов в области информационной борьбы наивысшей квалификации. Составляется план проведения эксперимента. В нем определяются очередность и материально-техническое обеспечение проведения экспериментов по определению слабых звеньев в системе защиты. При этом могут моделироваться действия злоумышленников, соответствующие различным моделям поведения нарушителей: от неквалифицированного злоумышленника, не имеющего официального статуса в исследуемой КС, до высококвалифицированного сотрудника службы безопасности.

Служба безопасности до момента преодоления защиты «злоумышленниками» должна ввести в КСЗИ новые механизмы защиты (изменить старые), чтобы избежать «взлома» системы защиты.

Такой подход к оценке эффективности позволяет получать объективные данные о возможностях существующих КСЗИ, но требует высокой квалификации исполнителей и больших материальных и временных затрат. Для проведения экспериментов необходимо иметь самое современное оборудование (средства инженерно-технической разведки, аппаратно-программные и испытательные комплексы (стенды) и т. п.)

12.8. Создание организационной структуры КСЗИ

Одной из основных составляющих КСЗИ является организационная структура, которая создается для выполнения организационных мер защиты, эксплуатации технических, программных и криптографических средств защиты, а также для контроля за выполнением установленных правил эксплуатации КС обслуживающим персоналом и пользователями. Такие структуры входят в состав службы безопасности ведомств, корпораций, фирм, организаций. Они могут иметь различный количественный состав и внутреннюю структуру. Это может быть отдел, группа или отдельное должностное лицо. Непосредственной эксплуатацией средств защиты и выполнением организационных мероприятий занимаются органы защиты информации, размещаемые на объек-

тах КС. Их называют объектовыми органами защиты информации или органами обеспечения безопасности информации (ОБИ). Если объекты КС располагаются на одной территории с другими объектами ведомства, корпорации, фирмы, то часть функций, таких как охрана, разведывательная и контрразведывательная и некоторые другие выполняются соответствующими отделами службы безопасности. Подразделение (должностное лицо) ОБИ может входить организационно и в состав вычислительных центров или отделов автоматизации. При этом службы безопасности сохраняют за собой функции контроля и методического обеспечения функционирования КСЗИ. Количественный состав и его структура органа ОБИ определяется после завершения разработки КСЗИ.

При создании органа ОБИ используются данные, полученные в результате разработки КСЗИ:

- официальный статус КС и информации, обрабатываемой в системе;
- перечень организационных мероприятий защиты и их характеристики;
- степень автоматизации КСЗИ;
- особенности технической структуры и режимы функционирования КС.

Органы ОБИ создаются в соответствии с законодательством РФ, регулирующим взаимоотношения граждан и юридических лиц в сфере информационных технологий. В зависимости от владельца, конфиденциальности и важности обрабатываемой в КС информации определяется юридический статус самой КС и органа ОБИ. В соответствии со статусом органа ОБИ определяются его юридические права и обязанности, определяется порядок взаимодействия с государственными органами, осуществляющими обеспечение безопасности информации в государстве.

При создании органов ОБИ руководствуются также требованиями подзаконных актов (Постановлений Правительства, решений Государственной технической комиссии и ФАПСИ, ГОСТов и других), а также руководящими документами ведомств.

В результате разработки КСЗИ определяется перечень организационных мероприятий защиты информации, которые представляют собой действия, выполняемые сотрудниками служб безопасности, органов ОБИ, обслуживающим персоналом и пользовате-

лями, в интересах обеспечения безопасности информации. Все организационные мероприятия защиты можно разделить на два класса:

1) защитные мероприятия, непосредственно направленные на обеспечение безопасности информации;

2) эксплуатационные мероприятия, связанные с организацией эксплуатации сложных систем.

Подавляющее большинство защитных, организационных мероприятий связано с обслуживанием технических, программных и криптографических средств защиты. Примерами таких мероприятий являются: использование паролей и материальных идентификаторов, контроль доступа к информационным ресурсам путем выполнения определенных действий при получении сигнала о нарушении правил разграничения доступа и анализа журнала контроля, дублирование и восстановление информации и др.

Некоторые функции системы защиты могут быть реализованы только за счет организационных мероприятий, например, доступ в помещение с информационными ресурсами может осуществлять контролер. Защита от пожара реализуется путем вызова пожарной команды, эвакуации информационных ресурсов, использования средств тушения пожара.

Часто организационные мероприятия дополняют технические, программные и криптографические средства, образуя еще один уровень защиты. Так зеркальное дублирование, которое выполняется без вмешательства человека, может быть дополнено периодическим дублированием информации на съемные магнитные носители. Автоматизированный контроль вскрытия дверей, корпусов, крышек и других элементов защиты внутреннего монтажа устройств от несанкционированной модификации может быть дополнен опечатыванием этих элементов (использованием специальных защитных знаков) и контролем целостности печатей (защитных знаков) должностными лицами.

Под эксплуатационными организационными мероприятиями понимается комплекс мероприятий, связанных с необходимостью технической эксплуатации системы защиты информации, как подсистемы сложной человеко-машинной системы. Задачи, решаемые в процессе технической эксплуатации КС, приведены в п.13.2.

Имея полный перечень организационных мероприятий защи-г ты и зная их характеристики, можно определить в общих черта* организационно-штатную структуру подразделения ОБИ. Органи-и зационно-штатная структура подразделения ОБИ уточняется в процессе анализа степени автоматизации системы защиты, а так-г же режимов функционирования КС. При этом решается вопрос а распределении обязанностей по эксплуатации средств СЗИ между обслуживающим персоналом и должностными лицами подразделения ОБИ. Так рабочая станция дежурного оператора СЗИ может" обслуживаться специалистами подразделения технического обслуживания, так как такое рабочее место по технической структуре, как правило, не отличается от рабочих мест других пользователей. В то же время устройства криптозащиты с учетом особенностей конструкции и повышенных требований по ограничению доступа к ним, как правило, обслуживаются специалистами подразделения ОБИ.

Особенности технической структуры КСЗИ и КС, а также режимы их функционирования влияют на количество рабочих мест операторов КСЗИ и режим работы операторов. При высокой степени автоматизации выполнения функций защиты число операторов может быть минимальным. При круглосуточном режиме работы число операторов КСЗИ соответственно увеличивается.

В небольших организациях, использующих защищенные КС, функции обеспечения защиты информации и технической эксплуатации могут выполняться одним должностным лицом, например, администратором ЛВС.

В процессе создания подразделений ОБИ выполняются следующий комплекс мероприятий:

1) определяются организационно-штатная структура, права и обязанности должностных лиц;

2) должностные лица обучаются практической работе с КСЗИ;

3) разрабатывается необходимая документация;

4) оборудуются рабочие места должностных лиц;

5) определяется система управления КСЗИ.

Организационно-штатная структура определяет перечень должностей, подчиненность подразделения и должностных лиц подразделения. Каждому должностному лицу определяются его права и обязанности в соответствии с занимаемой должностью.

\

Эффективность функционирования КСЗИ во многом определяется уровнем руководства всем процессом ОБИ. Орган управления КСЗИ готовит предложения руководству организации при формировании и корректировке политики безопасности, определяет права и обязанности должностных лиц, планирует и обеспечивает выполнение технического обслуживания, осуществляет методическое руководство подчиненными структурами, организует контроль и анализ эффективности КСЗИ, осуществляет подбор, расстановку и обучение специалистов.

При отборе специалистов для работы в подразделении ОБИ, кроме деловых качеств, необходимо учитывать и морально-психологические данные кандидатов. Каждый специалист должен приобрести знания и навыки в эксплуатации механизмов защиты. Специалисты подразделений обслуживания и пользователи должны быть обучены работе в защищенных КС. Перед получением допуска все обязательно проходят тестирование.

В процессе создания организационной структуры КСЗИ используются следующие документы: законы, постановления Правительства, решения Государственной технической комиссии, ГОСТы, ведомственные директивы, инструкции и методические материалы. Кроме того, используется документация, полученная с установленными средствами защиты. В процессе эксплуатации КСЗИ документы разрабатываются и ведутся силами подразделений ОБИ.

Рабочие места должностных лиц подразделения ОБИ оборудуются средствами, полученными от разработчиков. Это пульты управления, мониторы, средства дистанционного контроля и т. п. Кроме того, на рабочих местах должны быть средства связи, инструкции, эксплуатационная документация, а также средства пожаротушения.

Контрольные вопросы

1. Назовите основные принципы построения защищенных КС.
2. Дайте краткую характеристику этапов создания КСЗИ.
3. В чем заключается сущность специальных методов неформального моделирования?
4. Поясните сущность методов декомпозиции и макромоделирования.

5. Выполните **сравнительный анализ подходов к оценке** эффективности КСЗИ.

ГЛАВА 13
Организация функционирования комплексных систем защиты информации

13.1. Применение КСЗИ по назначению

13.1.1. Организация доступа к ресурсам КС

Функционирование КСЗИ зависит не только от характеристик созданной системы, но и от эффективности ее использования на этапе эксплуатации КС. Основными задачами этапа эксплуатации являются максимальное использование возможностей КСЗИ, заложенных в систему при построении, и совершенствование ее защитных функций в соответствии с изменяющимися условиями.

Процесс эксплуатации КСЗИ можно разделить на применение системы по прямому назначению, что предполагает выполнение всего комплекса мероприятий, непосредственно связанных с защитой информации в КС, и техническую эксплуатацию (рис. 31). Применение по назначению предусматривает организацию доступа к ресурсам КС и обеспечение их целостности.

Под *организацией доступа к ресурсам* понимается весь комплекс мер, который выполняется в процессе эксплуатации КС для предотвращения несанкционированного воздействия на технические и программные средства, а также на информацию.

Организация доступа к ресурсам предполагает:

- разграничение прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц;
- организацию работы с конфиденциальными информационными ресурсами на объекте;
- защиту от технических средств разведки;
- охрану объекта;
- эксплуатацию системы разграничения доступа.

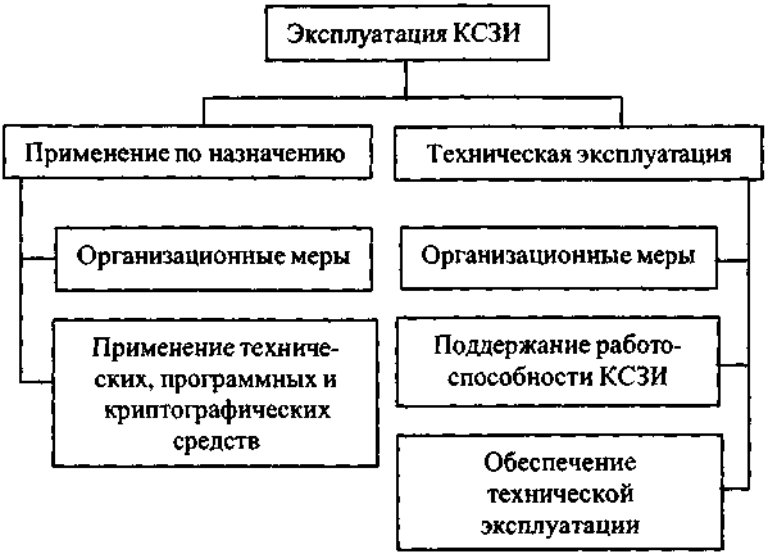


Рис. 31. Содержание процесса эксплуатации КСЗИ

Права должностных лиц по доступу к ресурсам КС устанавливаются руководством организации, в интересах которой используется КС. Каждому должностному лицу определяются для использования технические ресурсы (рабочая станция, сервер, аппаратура передачи данных и т.д.), разрешенные режимы и время работы. Руководством устанавливается уровень компетенции должностных лиц по манипулированию информацией. Лицо, ответственное за ОБИ в КС, на основании решения руководителя о разграничении доступа должностных лиц обеспечивает ввод соответствующих полномочий доступа в систему разграничения доступа.

Руководство совместно со службой безопасности определяет порядок работы с конфиденциальными информационными ресурсами, не используемыми непосредственно в КС, хотя бы и временно. К таким ресурсам относятся конфиденциальная печатная продукция, в том числе и полученная с помощью КС, а также машинные носители информации, находящиеся вне устройств КС. Учетом, хранением и выдачей таких ресурсов занимаются должностные лица из службы безопасности, либо другие должностные лица по совместительству.

Службой безопасности выполняется весь комплекс мероприятий противодействия техническим средствам разведки. Контролируется применение пассивных средств защиты от ЭМИ и наводок. Активные средства защиты от угроз этого класса используются в соответствии с графиком работы объекта. Периодически осуществляются проверки помещений на отсутствие в них закладных устройств аудио- и видеоразведки, а также обеспечивается защищенность линий связи от прослушивания.

Охрана объекта КС обеспечивает разграничение непосредственного доступа людей на контролируемую территорию, в здания и помещения. Подразделение охраны (охранник) может находиться на объекте, а может охранять несколько объектов. В последнем случае на объекте находятся только технические средства охраны и сигнализации. В соответствии с принятой политикой безопасности руководство совместно со службой безопасности определяют структуру системы охраны. Количественный состав и режим работы подразделения охраны определяется важностью и конфиденциальностью информации КС, а также используемыми техническими средствами охраны и сигнализации.

Система разграничения доступа (СРД) является одной из главных составляющих комплексной системы защиты информации. В этой системе можно выделить следующие компоненты:

- средства аутентификации субъекта доступа;
- средства разграничения доступа к техническим устройствам компьютерной системы;
- средства разграничения доступа к программам и данным;
- средства блокировки неправомочных действий;
- средства регистрации событий;
- дежурный оператор системы разграничения доступа.

Эффективность функционирования системы разграничения доступа во многом определяется надежностью механизмов аутентификации. Особое значение имеет аутентификация при взаимодействии удаленных процессов, которая всегда осуществляется с применением методов криптографии. При эксплуатации механизмов аутентификации основными задачами являются: генерация или изготовление идентификаторов, их учет и хранение, передача идентификаторов пользователю и контроль над правильностью выполнения процедур аутентификации в КС. При компрометации

атрибутов доступа (пароля, персонального кода и т. п.) необходимо срочное их исключение из списка разрешенных. Эти действия должны выполняться дежурным оператором системы разграничения доступа.

В больших распределенных КС проблема генерации и доставки атрибутов идентификации и ключей шифрования не является тривиальной задачей. Так, например, распределение секретных ключей шифрования должно осуществляться вне защищаемой компьютерной системы. Значения идентификаторов пользователя не должны храниться и передаваться в системе в открытом виде. На время ввода и сравнения идентификаторов необходимо применять особые меры защиты от подсматривания набора пароля и воздействия вредительских программ типа клавиатурных шпионов и программ-имитаторов СРД.

Средства разграничения доступа к техническим средствам препятствуют несанкционированным действиям злоумышленника, таким как включение технического средства, загрузка операционной системы, ввод-вывод информации, использование нештатных устройств и т. д. Разграничение доступа осуществляется оператором СРД путем использования технических и программных средств. Так оператор СРД может контролировать использование ключей от замков подачи питания непосредственно на техническое средство или на все устройства, находящиеся в отдельном помещении, дистанционно управлять блокировкой подачи питания на устройство или блокировкой загрузки ОС. На аппаратном или программном уровне оператор может изменять техническую структуру средств, которые может использовать конкретный пользователь.

Средства разграничения доступа к программам и данным используются наиболее интенсивно и во многом определяют характеристики СРД. Эти средства являются аппаратно-программными. Они настраиваются должностными лицами подразделения, обеспечивающего безопасность информации, и изменяются при изменении полномочий пользователя или при изменении программной и информационной структуры. Доступ к файлам регулируется диспетчером доступа. Доступ к записям и отдельным полям записей в файлах баз данных регулируется также с помощью систем управления базами данных.

Эффективность СРД можно повысить за счет шифрования файлов, хранящихся на внешних запоминающих устройствах, а также за счет полного стирания файлов при их уничтожении и стирания временных файлов. Даже если злоумышленник получит доступ к машинному носителю путем, например, несанкционированного копирования, то получить доступ к информации он не сможет без ключа шифрования.

В распределенных КС доступ между подсистемами, например удаленными ЛВС, регулируется с помощью межсетевых экранов. Межсетевой экран необходимо использовать для управления обменом между защищенной и незащищенной компьютерными системами. При этом регулируется доступ как из незащищенной КС в защищенную, так и доступ из защищенной системы в незащищенную. Компьютер, реализующий функции межсетевого экрана, целесообразно размещать на рабочем месте оператора КСЗИ.

Средства блокировки неправомочных действий субъектов доступа являются неотъемлемой компонентой СРД. Если атрибуты субъекта доступа или алгоритм его действий не являются разрешенными для данного субъекта, то дальнейшая работа в КС такого нарушителя прекращается до вмешательства оператора КСЗИ. Средства блокировки исключают или в значительной степени затрудняют автоматический подбор атрибутов доступа.

Средства регистрации событий также являются обязательной компонентой СРД. Журналы регистрации событий располагаются на ВЗУ. В таких журналах записываются данные о входе пользователей в систему и о выходе из нее, о всех попытках выполнения несанкционированных действий, о доступе к определенным ресурсам и т. п. Настройка журнала на фиксацию определенных событий и периодический анализ его содержимого осуществляется дежурным оператором и вышестоящими должностными лицами из подразделения ОБИ. Процесс настройки и анализа журнала целесообразно автоматизировать программным путем.

Непосредственное управление СРД осуществляет дежурный оператор КСЗИ, который, как правило, выполняет и функции дежурного администратора КС. Он загружает ОС, обеспечивает требуемую конфигурацию и режимы работы КС, вводит в СРД полномочия и атрибуты пользователей, осуществляет контроль и управляет доступом пользователей к ресурсам КС.

13.1.2. Обеспечение целостности и доступности информации в КС

На этапе эксплуатации КС целостность и доступность информации в системе обеспечивается путем:

- дублирования информации;
- повышения отказоустойчивости КС;
- противодействия перегрузкам и «зависаниям» системы;
- использования строго определенного множества программ;
- контроля целостности информации в КС;
- особой регламентации процессов технического обслуживания и проведения доработок;
- выполнения комплекса антивирусных мероприятий.

Одним из главных условий обеспечения целостности и доступности информации в КС является ее дублирование. Стратегия дублирования выбирается с учетом важности информации, требований к непрерывности работы КС, трудоемкости восстановления данных. Дублирование информации обеспечивается дежурным администратором КС.

Целостность и доступность информации поддерживается также путем резервирования аппаратных средств, блокировок ошибочных действий людей, использования надежных элементов КС и отказоустойчивых систем. Устраняются также преднамеренные угрозы перегрузки элементов систем. Для этого используются механизмы измерения интенсивности поступления заявок на выполнение (передачу) и механизмы ограничения или полного блокирования передачи таких заявок. Должна быть предусмотрена также возможность определения причин резкого увеличения потока заявок на выполнение программ или передачу информации.

В сложных системах практически невозможно избежать ситуаций, приводящих к «зависаниям» систем или их фрагментов. В результате сбоев аппаратных или программных средств, алгоритмических ошибок, допущенных на этапе разработки, ошибок операторов в системе происходят зацикливания программ, непредусмотренные остановы и другие ситуации, выход из которых возможен лишь путем прерывания вычислительного процесса и последующего его восстановления. На этапе эксплуатации ведется

статистика и осуществляется анализ таких ситуаций. «Зависания» своевременно обнаруживаются, и вычислительный процесс восстанавливается. При восстановлении, как правило, необходимо повторить выполнение прерванной программы с начала или с контрольной точки, если используется механизм контрольных точек. Такой механизм используется при выполнении сложных вычислительных программ, требующих значительного времени для их реализации.

В защищенной КС должно использоваться только разрешенное программное обеспечение. Перечень официально разрешенных к использованию программ, а также периодичность и способы контроля их целостности должны быть определены перед началом эксплуатации КС.

В защищенных КС, сданных в эксплуатацию, как правило, нет необходимости использовать трансляторы и компиляторы, программы-отладчики, средства трассировки программ и тому подобные программные средства. Работы по созданию и модернизации программного обеспечения должны производиться в автономных КС или, как исключение, в сегментах защищенной КС при условии использования надежных аппаратно-программных средств, исключающих возможность проведения мониторинга и несанкционированного внедрения исполняемых файлов в защищаемой КС.

Простейшим методом контроля целостности программ является метод контрольных сумм. Для исключения возможности внесения изменений в контролируемый файл с последующей коррекцией контрольной суммы необходимо хранить контрольную сумму в зашифрованном виде или использовать секретный алгоритм вычисления контрольной суммы.

Однако наиболее приемлемым методом контроля целостности информации является использование хэш-функции. Значение хэш-функции практически невозможно подделать без знания ключа. Поэтому следует хранить в зашифрованном виде или в памяти, недоступной злоумышленнику, только ключ хэширования (стартовый вектор хэширования).

Контроль состава программного обеспечения и целостности (неизменности) программ осуществляется при плановых проверках комиссиями и должностными лицами, а также дежурным опе-

ратором КСЗИ по определенному плану, неизвестному пользователям. Для осуществления контроля используются специальные программные средства. В вычислительных сетях такая «ревизия» программного обеспечения может осуществляться дистанционно с рабочего места оператора КСЗИ.

Особое внимание руководства и должностных лиц подразделения ОБИ должно быть сосредоточено на обеспечении целостности структур КС и конфиденциальности информации, защите от хищения и несанкционированного копирования информационных ресурсов во время проведения технического обслуживания, восстановления работоспособности, ликвидации аварий, а также в период модернизации КС. Так как на время проведения таких специальных работ отключаются (или находятся в неработоспособном состоянии) многие технические и программные средства защиты, то их отсутствие компенсируется системой организационных мероприятий:

- подготовка КС к выполнению работ;
- допуск специалистов к выполнению работ;
- организация работ на объекте;
- завершение работ.

Перед проведением работ, по возможности, должны предприниматься следующие шаги:

- отключить фрагмент КС, на котором необходимо выполнять работы, от функционирующей КС;
- снять носители информации с устройств;
- осуществить стирание информации в памяти КС;
- подготовить помещение для работы специалистов.

Перед проведением специальных работ необходимо всеми доступными способами изолировать ту часть КС, на которой предполагается выполнять работы, от функционирующей части КС. Для этого могут быть использованы аппаратные и программные блокировки и физические отключения цепей.

Все съемные носители с конфиденциальной информацией должны быть сняты с устройств и храниться в заземленных металлических шкафах в специальном помещении. Информация на несъемных носителях стирается путем трехкратной записи, например, двоичной последовательности чередующихся 1 и 0. На объекте необходимо определить порядок действий в случае не-

возможности стереть информацию до проведения специальных работ, например, при отказе накопителя на магнитных дисках. В этом случае восстановление работоспособности должно выполняться под непосредственным контролем должностного лица из подразделения ОБИ. При восстановлении функции записи на носитель первой же операцией осуществляется стирание конфиденциальной информации. Если восстановление работоспособности накопителя с несъемным носителем информации невозможно, то устройство подлежит утилизации, включая физическое разрушение носителя.

При оборудовании помещения для проведения специальных работ осуществляется подготовка рабочих мест и обеспечивается изоляция рабочих мест от остальной части КС. На рабочих местах должны использоваться сертифицированные и проверенные на отсутствие закладок приборы (если они не поставлялись в комплекте КС). Меры по обеспечению изолированности рабочих мест от остальной КС имеют целью исключить доступ сотрудников, выполняющих специальные работы, к элементам функционирующей КС.

Допуск специалистов осуществляется на рабочие места в определенное время и после выполнения всех подготовительных операций.

При прибытии специалистов из других организаций, например, для проведения доработок, кроме обычной проверки лиц, допускаемых на объект, должны проверяться на отсутствие закладок приборы, устройства, которые доставлены для выполнения работ.

В процессе выполнения специальных работ необходимо исключить использование не проверенных аппаратных и программных средств, отклонения от установленной документацией технологии проведения работ, доступ к носителям с конфиденциальной информацией и к функционирующим в рабочих режимах элементам КС.

Специальные работы завершаются контролем работоспособности КС и отсутствия закладок. Проверка на отсутствие аппаратных закладок осуществляется путем осмотра устройств и тестирования их во всех режимах. Отсутствие программных закладок проверяется по контрольным суммам, а также путем тестирования. Результаты доработок принимаются комиссией и оформля-

ются актом, в котором должны быть отражены результаты проверки работоспособности и отсутствия закладок. После проверок осуществляется восстановление информации и задействуются все механизмы защиты.

Для защиты КС от компьютерных вирусов необходимо руководствоваться рекомендациями, изложенными в п. 10.6.

В автономных КС непосредственную ответственность за выполнение комплекса антивирусных мероприятий целесообразно возложить на пользователя КС. В ЛВС такая работа организуется должностными лицами подразделения ОБИ. Исполняемые файлы, в том числе саморазархивирующиеся и содержащие макрокоманды, должны вводиться в ЛВС под контролем дежурного оператора КСЗИ и подвергаться проверке на отсутствие вирусов.

Успех эксплуатации КСЗИ в большой степени зависит от уровня организации управления процессом эксплуатации. Иерархическая система управления позволяет организовать реализацию политики безопасности информации на этапе эксплуатации КС. При организации системы управления следует придерживаться следующих принципов:

- уровень компетенции руководителя должен соответствовать его статусу в системе управления;
- строгая регламентация действий должностных лиц;
- документирование алгоритмов обеспечения защиты информации;
- непрерывность управления;
- адаптивность системы управления.
- контроль над реализацией политики безопасности;

Каждое должностное лицо из руководства организации, службы безопасности или подразделения ОБИ должны иметь знания и навыки работы с КСЗИ в объеме, достаточном для выполнения своих функциональных обязанностей. Причем должностные лица должны располагать минимально возможными сведениями о конкретных механизмах защиты и о защищаемой информации. Это достигается за счет очень строгой регламентации их деятельности. Документирование всех алгоритмов эксплуатации КСЗИ позволяет, при необходимости, легко заменять должностных лиц, а также осуществлять контроль над их деятельностью. Реализация этого принципа позволит избежать «незаменимости» отдельных

сотрудников и наладить эффективный контроль деятельности должностных лиц.

Непрерывность управления КСЗИ достигается за счет организации дежурства операторов КСЗИ. Система управления должна быть гибкой и оперативно адаптироваться к изменяющимся условиям функционирования.

13.2. Техническая эксплуатация КСЗИ

Техническая эксплуатация сложной системы включает в себя комплекс мероприятий, обеспечивающий эффективное использование системы по назначению. Комплексная СЗИ является подсистемой КС и ее техническая эксплуатация организуется в соответствии с общим подходом обеспечения эффективности применения КС.

Подробное изложение задач технической эксплуатации КС выходит за рамки учебного пособия. Здесь же уместно привести лишь общую характеристику задач, решаемых в процессе технической эксплуатации КСЗИ. К этим задачам относятся:

- организационные задачи;
- поддержание работоспособности КСЗИ;
- обеспечение технической эксплуатации.

К организационным задачам относятся:

- планирование технической эксплуатации;
- организация дежурства;
- работа с кадрами;
- работа с документами.

Планирование технической эксплуатации осуществляется на длительные сроки (полгода, год и более). Используется также среднесрочное (квартал, месяц) и краткосрочное планирование, (неделя, сутки). На длительные сроки планируются полугодовое техническое обслуживание и работа комиссий, поставки оборудования, запасных изделий и приборов, ремонты устройств и т. п. Среднесрочное планирование и краткосрочное применяются при, организации технического обслуживания, проведении доработок, организации дежурства и др.

Для непрерывного выполнения организационных мер защиты, и эксплуатации всех механизмов защиты организуется дежурство.

Режим дежурства зависит от режима использования КС. Дежурный оператор КСЗИ может выполнять по совместительству и функции общего администрирования в компьютерной сети. Рабочее место оператора КСЗИ, как правило, располагается в непосредственной близости от наиболее важных компонентов КС (серверов, межсетевых экранов и т. п.) и оборудуется всеми необходимыми средствами оперативного управления КСЗИ.

Работа с обслуживающим персоналом и пользователями сводится к подбору кадров, их обучению, воспитанию, к созданию условий для высокоэффективного труда.

В процессе технической эксплуатации используется четыре типа документов:

1)законы;

2) ведомственные руководящие документы;

3) документация предприятий-изготовителей;

4) документация, разрабатываемая в процессе эксплуатации.

В законах отражены общие вопросы эксплуатации КСЗИ. В ведомствах (министерствах, объединениях, корпорациях, государственных учреждениях) разрабатывают инструкции, директивы, государственные стандарты, методические рекомендации и т. п.

Предприятия-изготовители поставляют эксплуатационно-техническую документацию: технические описания, инструкции по эксплуатации, формуляры (паспорта) и др.

В организациях, эксплуатирующих КС, разрабатывают и ведут планирующую и учетно-отчетную документацию.

Одной из центральных задач технической эксплуатации является поддержание работоспособности систем. Работоспособность поддерживается в основном за счет проведения технического обслуживания, постоянного контроля работоспособности и ее восстановления в случае отказа. Работоспособность средств защиты информации контролируется постоянно с помощью аппаратно-программных средств встроенного контроля и периодически должностными лицами службы безопасности и комиссиями. Сроки проведения контроля и объем работ определяются в руководящих документах.

Успех технической эксплуатации зависит и от качества обеспечения, которое включает:

- материально-техническое обеспечение;

- транспортировка и хранение;
- метрологическое обеспечение;
- обеспечение безопасности эксплуатации.

Материально-техническое обеспечение позволяет удовлетворить потребность в расходных материалах, запасных изделиях и приборах, инструментах и других материальных средствах, необходимых для эксплуатации КСЗИ.

Транспортировка и хранение устройств защищенной КС должны предусматривать защиту от несанкционированного доступа к устройствам в пути и в хранилищах. Для обеспечения необходимых условий транспортировки и хранения выполняются мероприятия подготовки устройств согласно требованиям эксплуатационно-технической документации.

Метрологическое обеспечение позволяет поддерживать измерительные приборы в исправном состоянии.

В процессе эксплуатации важно обеспечивать безопасность обслуживающего персонала и пользователей прежде всего от угрозы поражения электрическим током, а также от возможных пожаров.

В целом от уровня технической эксплуатации во многом зависит эффективность использования КСЗИ.

Контрольные вопросы

1. Охарактеризуйте основные направления организации доступа к ресурсам КС.
2. Какими путями достигается целостность и доступность информации?
3. В чем заключается техническая эксплуатация КСЗИ?

Список принятых сокращений

АС - автоматизированная система
АСОД - автоматизированная система обработки данных
АСУ - автоматизированная система управления
ВЗУ - внешнее запоминающее устройство
ВС - вычислительная система
ВСт - вычислительная сеть
ЗУ - запоминающее устройство
КМ - коммуникационный модуль
КПП - контрольно-пропускной пункт
КС - компьютерная система
КСЗИ - комплексная система защиты информации
ЛВС - локальная вычислительная сеть
НИС - несанкционированное изменение структур
НСДИ - несанкционированный доступ к информации
ОБИ - обеспечение безопасности информации
ООП - объектно-ориентированное программирование
ОП - оперативная память
ОС - операционная система
ПЗУ - постоянное запоминающее устройство
ПЦ - процессор
ПЭМИН - побочные электромагнитные излучения и наводки
РКС - распределенная компьютерная система
СВЧ - сверхвысокая частота
СВТ - средства вычислительной техники
СЗИ - система защиты информации
СЗИК - система защиты от изучения и копирования
СКВУ - система контроля вскрытия устройств
СОО - система охраны объекта
СПД - система передачи данных
СРД - система разграничения доступа
СУБД - система управления базой данных
ТС - техническое средство
ТСВ - телевизионная система видеоконтроля
УОКВ - устройство обработки и коммутации видеоинформации
УРИ - устройство регистрации информации
ЭВТ - электронно-вычислительная техника

БИБЛИОГРАФИЯ

1. Алексеенко В.Н., Сокольский Б.В. Система защиты коммерческих объектов. Технические средства защиты. Практическое пособие для предпринимателей и руководителей служб безопасности. М., 1992. - 94 с.
2. Артехин Б.В. Стеганография // Защита информации. Конфидент. - **1996.** - №4.
3. Барсуков В.С. Обеспечение информационной безопасности. - М: ТЭК, **1996.**
4. Безруков Н.Н. Компьютерная вирусология: Справ, руководство. - М.: УРЕ, 1991.-416 с.
5. Вернигоров Н.С. Нелинейный локатор - эффективное средство обеспечения безопасности в области утечки информации // Защита информации. Конфидент. - **1996.** -№ **1.**
6. Гайкович В.. Першин А. Безопасность электронных банковских систем. - М: Компания Единая Европа. 1994.
7. Галатенко В.. Трифаленков И. Информационная безопасность в Интранет: концепции и решения // **Jet Info.** №23/24.1996.
8. Герасименко В.А. Защита информации в автоматизированных системах обработки данных: В 2 кн. М.: Энергоатомиздат, 1994.
9. ГОСТ 28147 - 89. Системы обработки информации. Защита криптографиче-; екая. Алгоритм криптофафического преобразования.
10. ГОСТ Р 34.10 - 94. Информационная технология. Криптофафическая защи-. та информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптофафического алгоритма.
11. ГОСТ Р 34.11-94. Функция хеширования.
12. Гостехкомиссия РФ. Руководящий документ. Защита информации. Специ-! альные защитные знаки. - М.: Jet Info, 1997.
13. Гостехкомиссия РФ. Руководящий документ. Средства вычислительной} техники. Межсетевые экраны. Защита от несанкционированного доступа к^ информации. Показатели защищенности от несанкционированного доступа к информации. - М.: **Jet Info, 1997.**
14. Гостехкомиссия РФ. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. - М.: **Jet** Info, 1996. - №2.
15. Груздев С.Л., Хачатурова О.Л. Электронные ключи **«YASP»** компании **«ALADDIN».** Новые технологии в маркетинге программного обеспечения //, Защита информации. Конфидент. - 1996. - №6.
16. Грушо А.А.. Тимонина Е.Е. Теоретические основы защиты информации. - М: Издательство Агентства «Яхтсмен». 1996. - 192 с.
17. Закон Российской Федерации «О государственной тайне». 21.07.1993. ?
18. Защита профаммного обеспечения: Пер. с англ./Д. Гроувер. Р. Сатер, Дж.-* Фипс и др.; Под ред. Д. Гроувера. - М: Мир. 1992. - 286 с.
19. Информационно-безопасные системы. Анализ проблемы: Учеб. пособие / Алешин И.В. и др.: Под ред. В.Н. Козлова - СПб.: Издательство С- Петербургского гос. техн. университета, 1996. - 69 с.

20. Касперский Е. Компьютерные вирусы в MS-DOS. - М: Эдэль, 1992. - 176 с.
21. Кнут Д. Искусство программирования для ЭВМ. - М.: Мир, 1976. - Т.2.
22. Лебедев А.Н. Криптография с «открытым ключом» и возможности его практического применения // Защита информации. Конфидент. - 1992. - №2.
23. Лысов А.В. Лазерные микрофоны - универсальное средство разведки или очередное поветрие моды? // Защита информации. Конфидент. - 1997. - №1.
24. Мамиконов А.Г., Кульба В.В.,Шелков А.Б. Достоверность, защита и резервирование информации в АСУ. - Энергоатомиздат, 1986. - 304 с.
25. Маркин А.В. Безопасность излучений и наводок от средств электронно-вычислительной техники: домыслы и реальность. Защита информации. Конфидент. - 1994. - №2. - С.49-57.
26. Мафтик С. Механизмы защиты в сетях ЭВМ. - М.: Мир, 1993. - 216 с.
27. Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через INTERNET / Под научной редакцией проф. П.Д. Зегжды - СПб.: Мир и семья, 1997. - 296с.
28. Мельников В.В. Защита информации в компьютерных системах. - М: Финансы и статистика; Электронинформ, 1997. - 368 с.
29. Михайлов С.Ф., Петров В.А., Тимофеев Ю. А. Информационная безопасность. Защита информации в автоматизированных системах. Основные концепции: Учебное пособие. - М.: МИФИ, 1995. - 112 с.
30. Молчанов А.А. Моделирование и проектирование сложных систем. - К.: Выща шк. Головное издательство, 1988. - 359 с.
31. Особенности устройств съема информации и методы их блокировки. - Томск: НПП «Вихрь», 1996. - 32 с.
32. Пилюгин П.Л. Общие вопросы зашиты вычислительных систем и особенности защиты персональных компьютеров: Курс лекций. - М.: ИКСИ, 1997. - 84 с.
33. Положение о государственном лицензировании деятельности в области защиты информации (Решение Государственной технической комиссии России и ФАПСИ от 27.04.1994 г. №10). - М.: Гостехкомиссия РФ, 1994. - 16 с.
34. Положение о сертификации средств защиты информации (Постановление Правительства Российской Федерации от 26.06.95 г. № 608). - М., 1995. - 4 с.
35. Положение по аттестации объектов информатизации по требованиям безопасности информации (Утверждено Председателем Гостехкомиссии Российской Федерации 25.11. 1994г.). - М.: Гостехкомиссия РФ, 1994. - 16 с.
36. Портативный тепловизионный комплекс «Иртис-200». Паспорт. - М.: «Иртис», 1998.- 11 с.
37. Протоколы и методы управления в сетях передачи данных / Пер. с англ.;Под ред. Ф.Ф.Куо. - М.: Радио и связь, 1985.
38. Расторгуев С П. Программные методы защиты в компьютерных сетях. - М.: «Яхтсмен», 1993.-188 с.
39. Спесивцев А.В., Вегнер В.А., Крутяков А.Ю. и др. Защита информации в персональных ЭВМ. - М.: Радио и связь; МП «Веста», 1992. - 192 с.
40. Специальная техника защиты и контроля информации: Каталог. - М.: Маском, 1998.-44 с.

41. Специальная техника: Каталог. - М: НПО «Защита информации», **1998.** - 32 с.
42. Стенг Д.И., Мун С. Секреты безопасности сетей - К.: Диалектика, 1996.
43. Таили Э. Безопасность персонального компьютера. - Мн.: ООО «Попурри», 1997. - 480 с.
44. Технические системы защиты информации: Каталог. - М.: АОЗТ «Нелк», 1998.-56 с.
45. Технические системы защиты информации: Каталог. - М.: АОЗТ «Нелк», 1997. - 200 с.
46. Технические средства, применяемые в охранной деятельности: Учебное пособие. - М.: Школа охраны «Баярд», 1995. - 156с.
47. Тимец Б.В. Сделайте свой офис безопасней // Защита информации. Конфидент.- 1997,- №1.
48. Торокин А.А. Основы инженерно-технической защиты информации. -М.: Ось-89, 1998.-336 с.
49. Уолкер Б.Дж., Блейк Я.Ф. Безопасность ЭВМ и организация их защиты. - М.: Связь, 1980.-112 с.
50. Федеральный закон Российской Федерации «Об информации, информатизации и защите информации», 1995.
51. Филлипс Кен. Биометрия, о которой нельзя забыть // PC WEEK (RE). - 1998. - № 2.
52. Флорен М.В. Оборудование управления доступом в помещения. Система «Менуэт» в вопросах и ответах // Защита информации. Конфидент. - 1995. - №6.
53. Флорен М.В. Системы управления доступом // Защита информации. Конфидент. - 1995. - №5.
54. Фоменков Г.В. и др. Методы и средства обеспечения безопасности в сети Интернет: Научно-практическое пособие. -М.: ИКСИ, 1997. - 112 с.
55. Фролов А.В., Фролов Г.В. Осторожно: компьютерные вирусы. - М.:ДИАЛОГ-МИФИ,1996. - 256 с.
56. Хоффман Л.Дж. Современные методы защиты информации / Пер. с англ. - М: Сов. радио, 1980.
57. Цыганков В.Д., Лопатин В.Н. Психотронное оружие и безопасность России. Серия «Информатизация России на пороге XXI века». - М.: СИНТЕГ, 1999. -152 с.
58. Шелест СО. Методы и приборы для измерения параметров линии // Защита информации. Конфидент. - 1996. - № 4.
59. Шеннон К. Математическая теория связи. Работы по теории информации и кибернетике. - М.: ИИЛ, 1963. - 830с.
60. Шрейдер Ю.А. О семантических аспектах теории информации. Информация и кибернетика. - М.: Сов. радио, 1967.
61. Щербаков А.Ю. Защита от копирования. - М.: Эдэль, 1992.
62. Щербаков А. Разрушающие программные воздействия. - М.: Эдэль, 1993. - 64 с.
63. Щербаков Н.С. Достоверность работы цифровых устройств. - М.: Машиностроение, 1989.

64. Электромагнитная совместимость радиоэлектронных средств и непреднамеренные помехи. Пер. с англ. / Под ред. А.И.Саприга. - М.: Сов. радио, 1978. Вып. 2. - 272 с.
65. Audio Surveillance: Catalog. - Germany: PK Electronic International FRG, 1996. -44 p.
66. Datapro Reports on Information Security. 1990-1993.
67. Discrete surveillance. Navelties: Catalog. - Germany: Helling, 1996. - 13 p.
68. PC WEEK/RE. № 32, С 6.
69. Spence B. Biometrics in Physical Access Control Issues, Status and Trends // Web Recognition Systems. - 1998.
70. Stansfield E.V., Harmer D., Kerrigan M.F. Speech processing techniques for HF radio security. - IEEE Proceedings, Pt. I, 1989, February. V. 136, № 1. Pp. 25-46.

Учебное издание

Виктор Иванович Завгороднии

Комплексная защита информации в компьютерных системах

Учебное пособие

Редактор В.А. Якусевич
ПереплетД Коночкина
Корректор И Я Дабагян

Изд лиц ИД № 01670 от 24 04 2000
Налоговая льгота - общероссийский классификатор продукции ОК-005-93, том 2 953000

Подписано в печать 25.04.2001 Формат 60x90/16
Бумага офсетная. Печать офсетная
Печ. л. 16,5. Тираж 5000 экз. Заказ № 1284

Издательско-книготорговый дом «Логос»
105318, Москва, Измайловское ш., 4

Отпечатано с готовых диапозитивов
во ФГУП И ПК «Ульяновский Дом печати»
432980, г. Ульяновск, ул. Гончарова, 14

По вопросам приобретения литературы
обращаться по адресу:
105318, Москва, Измайловское ш., 4
Тел./факс: (095) 369-5819, 369-5668, 369-7727
Электронная почта: universitas@mail.ru
Интернет-магазин «Университетская книга»
http://www.chat.ru/-universitas/
Корпоративный пейджер: (095) 956-1956 (аб. 55032)