

МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГОУ ВПО "Кубанский государственный аграрный университет"

Факультет прикладной информатики
Кафедра компьютерных технологий и систем

Лаптев В.Н.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Курс лекций
(для бакалавров специальности « Бизнес-информатика»)

Краснодар
2013

Лаптев В.Н.

Информационная безопасность и защита информации: Курс лекций (для бакалавров специальности « Бизнес-информатика»). – Краснодар: КубГАУ, 2013. - 198с.

Курс лекций по дисциплине "Информационная безопасность" разработан для бакалавров специальности « Бизнес-информатика» на кафедре компьютерных технологий и систем (КТС) факультета прикладной информатики (ФПИ) КубГАУ.

Рассмотрен и рекомендован к изданию на заседании кафедры компьютерных технологий и систем КубГАУ __ сентября 2012 г., протокол № 1.

Рекомендованы к печати:

- Советом факультета прикладной информатики Кубанского государственного аграрного университета __ сентября 2013 г., протокол № 1.

Содержание

ВВЕДЕНИЕ	4
I. ОСНОВНЫЕ ПОНЯТИЯ И ПОЛОЖЕНИЯ ИБ	5
Лекция 1. ПРЕДМЕТ И ОБЪЕКТ ЗАЩИТЫ	5
Лекция 2. КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	13
Лекция 3. УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В КС	23
II. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ В КОМПЬЮТЕРНЫХ СИСТЕМАХ	29
Лекция 4. НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	29
Лекция 5. ЗАЩИТА ИНФОРМАЦИИ ОТ СЛУЧАЙНЫХ УГРОЗ	57
Лекция 6. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ОТ ШПИОНАЖА И ДИВЕРСИЙ	65
Лекция 7. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ОТ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ И НАВОДОК	81
Лекция 8. МЕТОДЫ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ИЗМЕНЕНИЯ СТРУКТУР КС	97
Лекция 9. ЗАЩИТА В КС ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА	109
Лекция 10. КОМПЬЮТЕРНЫЕ ВИРУСЫ И МЕХАНИЗМЫ БОРЬБЫ С НИМИ	119
Лекция 11. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ	129
Лекция 12. ЗАЩИТА ИНФОРМАЦИИ В РАСПРЕДЕЛЕННЫХ КС	143
III. ПОСТРОЕНИЕ И ОРГАНИЗАЦИЯ ФУНКЦИОНИРОВАНИЯ КСЗИ В КС	159
Лекция 13. ПОСТРОЕНИЕ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ	159
Лекция 14. ПРОЕКТИРОВАНИЕ КОМПЛЕКСНЫХ СИСТЕМ	169
Лекция 15. ОРГАНИЗАЦИЯ ФУНКЦИОНИРОВАНИЯ КОМПЛЕКСНЫХ СИСТЕМ	177
ЗАКЛЮЧЕНИЕ	185
СПИСОК ПРИНЯТЫХ СОКРАЩЕНИЙ	188
СПИСОК ЛИТЕРАТУРЫ	189
ПРИЛОЖЕНИЯ.....	190
Приложение 1. Календарно-тематический план изучения дисциплины	190
Приложение 2. Программа самостоятельной работы студента по дисциплине	192
Приложение 3. Вопросы для подготовки к экзамену по дисциплине	197

ВВЕДЕНИЕ

Вступление человечества в XXI век знаменуется бурным развитием информационных технологий (ИТ) 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 (ИР).

Значимость обеспечения безопасности государства в информационной сфере подчеркнута в принятой в сентябре 2000 года "Доктрине информационной безопасности Российской Федерации". /Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 09.09.2000г. //Российская газета, 28 сентября 2000г./: "Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать".

Острогу 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.

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 ИТ, стремление криминальных структур противоправно использовать ИР, необходимость обеспечения прав граждан в информационной сфере, наличие множества случайных угроз вызывают острую необходимость обеспечения защиты информации (ЗИ) в компьютерных системах (КС), являющихся материальной основой информатизации общества.

Проблема обеспечения информационной безопасности (ИБ) на всех уровнях может быть успешно решена только в том случае, если создана и функционирует комплексная система защиты информации, (КСЗИ) охватывающая весь жизненный цикл КС от разработки до утилизации и всю технологическую цепочку сбора, хранения, обработки и выдачи информации. Вопросы построения и организации функционирования такой системы защиты информации (СЗИ) рассматриваются в настоящем курсе лекций. Он позволит выработать у студентов целостный, системный взгляд на проблему защиты информации в КС.

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

І. ОСНОВНЫЕ ПОНЯТИЯ И ПОЛОЖЕНИЯ ИБ

Лекция 1. ПРЕДМЕТ И ОБЪЕКТ ЗАЩИТЫ

Вопросы:

- 1.1. Предмет защиты
- 1.2. Объект защиты информации
- 1.3. Цель и задачи дисциплины

Литература:

1. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. – Логос, 201. – С.6-16.
2. Ярочкин В.И. Информационная безопасность: Учебнк для студентов вузов. – М.: Академический проект: Гаудеамус, 2004. – С.6-28.

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.

Не материальность 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 важно-*

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

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

где C_0 - ценность информации в момент ее возникновения (получения);

t - время от момента возникновения информации до момента определения ее стоимости;

τ - 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, авто гонщиков 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. Информация покупается и продается. 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 интересует 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 символа-

ми 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 P_i - вероятность появления в сообщении символа i ;

k - 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 копий информации. Действие этого закона можно проследить на примере пиратского распространения программных продуктов, видео продукции и т.п.

В качестве **предмета защиты** рассматривается информация, хранящаяся, обрабатываемая и передаваемая в компьютерных системах. Особенности 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 вычислительные системы, сети и телекоммуникации, т.е. компьютерная система (КС) или автоматизированная система обработки данных (АСОД) объекта, ее связи с другими удаленными КС, а также средства общения людей (коммуникации). В работах, посвященных защите информации (ЗИ) в автоматизированных информационных системах (АИС), 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 (сосредоточенный или распределенный), предназначенный для автоматизированного сбора, хранения, обработки, передачи и получения информации. В ряду с термином "информация" применительно к КС часто используют термин "данные". Обусловлено это тем, что до сих пор нет четкого понимания сходства и различия этих терминов.

А суть дела в следующем. Все объекты материального мира (в т.ч. и люди) находятся в состоянии непрерывного движения и развития, которое сопровождается обменом вещества и энергии, их переходом из одной формы в другую. Все виды такого обмена сопровождаются появлением электромагнитных **сигналов** – своеобразных дискретных переносчиков энергоматериальных порций - "квантов" (комплексов из них) между взаимодействующими объектами. При взаимодействии сигналов с конкретным объектом в нем возникают определенное изменение его свойств – это явление называется регистрацией сигналов. Такие, зафиксированные в объекте сигналы, можно наблюдать, измерять или фиксировать иными способами – при этом в объекте запоминаются зарегистрированные сигналы и возникают новые сигналы. Сигналы, зафиксированные объектами, т.е. хранящиеся на материальных носителях, и называются **данными**. Эти данные и возникающие при регистрации сигналы, наделяемые человеком, определенным смыслом (содержанием) и являются **информацией**, т.е. общепринятыми "сведениями о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления". Эти, наделенные смыслом данные и сигналы, т.е. информация и используются человеком в дальнейшем в его разнообразной деятельности.

Следовательно, человек работает ИНФОРМАЦИЕЙ (с данными и сигналами, имеющих определенный смысл), а компьютер с помощью программ и средства связи манипулируют с формализованными (числовыми) ДАННЫМИ и СИГНАЛАМИ (командами), смысловое содержание которых для них не определено.

В сфере защиты информации и данных используется и понятие - "информационные ресурсы". В соответствии с законом РФ "Об информации, информатизации и защите информации" под **информационными ресурсами** (ИР) 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 понятия компьютерная система объединяется одним понятием по двум причинам:

во-первых, для всех этих систем *основные проблемы защиты информации и данных являются общими;*

во-вторых, более мелкие системы являются элементами более крупных систем.

Если защита информации и данных в каких-либо системах имеет свои особенности, то они рассматриваются отдельно.

Предметом защиты в КС являются данные и информация. Материальной основой существования информации и данных в КС и средствах связи являются электронные и электромеханические устройства (подсистемы), а также машинные (бумажные) носители. С помощью устройств ввода информация преобразуется в числовые данные, которые хранятся в запоминающих устройствах (ЗУ) различных уровней, преобразуется (обрабатывается) процессорами (ПЦ), выводится из системы с помощью устройств вывода (преобразующих данные в информацию /в виде рисунков и текстов на экране монитора, видеопроектора или печатных документов) и систем передачи данных (СПД). Традиционные средства связи могут использоваться для передачи данных лишь при наличии модемов - преобразователей дискретных сигналов в аналоговые (непрерывные) и обратно. С помощью СПД и традиционной связи (использующей модемы) данные передаются (принимаются) в другие (из других) КС. В качестве машинных носителей данных и информации (данных со смыслом) используются бумага, магнитные ленты, диски различных типов. Ранее в качестве машинных носителей использовались бумажные перфокарты и перфоленты, магнитные барабаны и карты. Большинство типов машинных носителей являются съемными, т.е. могут сниматься с устройств и использоваться (бумага) или храниться (ленты, диски, бумага) отдельно от устройств.

Таким образом, для защиты данных (в т.ч. и данных, наделенных смыслом – информации), или для обеспечения безопасности данных и информации, в КС необходимо защищать аппаратно-программные средства, устройства (подсистемы) и машинные носители от несанкционированных (неразрешенных) воздействий на них. Компьютерные системы относятся к классу человеко-машинных систем. Они 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 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 и данные.

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 "информационная безопасность" (ИБ) или "безопасность информации" и "защищенные КС".

Информационная безопасность (ИБ) или (защищенность) информации в КС - это такое состояние всех компонент компьютерной системы, при котором обеспечивается защита информации и данных от возможных угроз на требуемом уровне. Компьютерные системы, в которых обеспечивается безопасность информации (и данных), называются **защищенными**.

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

ИБ достигается проведением руководством соответствующего уровня **политики информационной безопасности**. Основным документом, на основе которого проводится политика ИБ, является **программа информационной безопасности**. Этот документ разрабатывается и принимается как официальный руководящий документ высшими органами управления государством, ведомством, организацией. В документе приводятся цели политики информационной безопасности и основные направления решения задач защиты информации (ЗИ) в КС. В про-

граммах ИБ содержатся также общие требования и принципы построения систем защиты информации в КС.

Под системой защиты информации (СЗИ) 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.

1.3. Цель и задачи дисциплины

В ГОС ВПО подготовки бакалавра по специальности 080500.62 – Бизнес информатика приведены следующие требования к обязательному минимуму содержания учебной дисциплины "Информационная безопасность" для студентов-информатиков:

Индекс	Наименование дисциплины и ее основные разделы	Всего часов
СД.Ф.04	ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или "нарушителей". Понятия о видах вирусов. Три вида возможных нарушений информационной системы. Защита. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Использование защищенных компьютерных систем. Методы криптографии. Основные технологии построения защищенных ЭИС. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.	150

В соответствии с общей характеристикой и требованиями ГОС ВПО, утвержденными приказом Министерства образования Российской Федерации № 686 от 2 марта 2000 года, Положения об итоговой государственной аттестации выпускников вузов РФ, учебно-методической документации ФГОУ ВПО "Кубанский государственный аграрный университет", методических рекомендаций УМО по дисциплине "Информационная безопасность" поставлена следующая цель ее изучения.

Цель изучения ИБ заключается в том, чтобы познакомить студентов с новым научным направлением, которое изучает методы предотвращения случайного или преднамеренного копирования, искажения, блокирования или уничтожения информации.

После изучения данной дисциплины студент должен осуществлять профессиональную деятельность и уметь решать задачи, соответствующие его квалификации. Он должен:

обладать

- специальной подготовкой использования проблемно-ориентированных информационных систем (ПОИС) в предметной области (экономике/юриспруденции) с учетом использования современных средств и методов обеспечения их информационной безопасности (ИБ);
- знаниями перспективных ИТ, проектирования, создания, анализа и сопровождения защищенных ПОИС;

знать:

- принципы, средства и методы обеспечения ИБ и создания комплексных систем защиты информации (КСЗИ) в компьютерных системах (КС) своей предметной области;

уметь

- ставить задачу системного проектирования и комплексирования локальных и глобальных сетей обслуживания пользователей ИС с учетом соблюдения требований ИБ;
- ставить и решать задачи, связанные с организацией диалога между человеком и ИС в условиях возможных нарушений требований ИБ;

- формулировать основные технико-экономические требования к проектируемым ПОИС с учетом теоретических положений ИБ и практики использования СЗИ;

владеть

- методиками и методами системного анализа предметной области и проектирования защищенных ПОИС;

иметь опыт

- работы с основными объектами, явлениями и процессами, связанными с комплексной КСЗИ в КС, использованием методов их научного исследования.

Так как информатик (экономист/юрист) в большей степени имеет дело с профессионально-ориентированной оболочкой (он ее проектирует, создаёт и применяет), и в меньшей степени - с ядром информационной системы (разработкой комплекса вычислительных средств, операционной системы, систем управления базами данных и др.). Оболочка состоит из специальных программных средств, информационного обеспечения и организационных мероприятий поддержки функционирования конкретных процессов в предметной области (экономике /юриспруденции). Следовательно выпускники-информатики в целом специализируются на организационно-технологических и управленческих аспектах применения методов информатики, ИС и ИТ, в своей практической работе в основном анализируют, прогнозируют, моделируют и создают автоматизированные информационные процессы, реализует технологии их функционирования и развития в рамках ПОИС.

Во всех видах профессиональной деятельности от информатика требуется успешное решение следующих функциональных задач:

- 1) внедрения методов информатики (и математики) в предметной области;
- 2) развития адаптационных возможностей ПОИС на всех стадиях их жизненного цикла (создания информационно-логических моделей объектов, разработки нового программного и информационного обеспечения для ПОИС; стыковки ИС из разных предметных областей в связи с появляющимися новыми задачами; перевода систем на новые аппаратные и информационные платформы);
- 3) оптимизации информационных процессов автоматизированной обработки информации (рационального управления взаимосвязанными материальными, денежными и информационными потоками; постановки и решение оптимизационных задач; разработки имитационных моделей процессов; применение методов системного анализа и алгоритмов математического программирования при адаптации ИС);
- 4) унификации профессионально-ориентированного программного и информационного обеспечения в предметной области (сертификация программных продуктов, приведение их к требованиям действующих стандартов; использование международных стандартов обработки информации и обмена данными; создания интерфейсов для ИС, использующих разные стандарты);
- 5) использования международных информационных ресурсов (с учетом обеспечения ИБ функционирования ПОИС при их взаимодействии с информационными рынками по сетям или с использованием иных методов обмена данными, оценка эффективности приобретаемого программного обеспечения и информационных баз данных и т.п.).

При наличии конкретного объекта профессиональной деятельности информатик, используя свои знания, умения и навыки по защите информации, как минимум должен обеспечить нормальное функционирование обслуживаемой им ПОИС. Отсюда вытекают следующие задачи изучения дисциплины:

- изучение теоретических положений ИБ, ее средств и методов ЗИ, особенностей их использования в КС, перспектив их развития в ИТ, предметной и смежных с ней областях;
- повышения уровня профессиональной культуры и исполнительской дисциплины студентов, понимание необходимости использования СЗИ в КС в профессиональной деятельности по специальности;
- освоения основных средств и методов обеспечения ИБ, методик их результативного использования;

- изучения технических и программно-аппаратных средств ЗИ, их основных;
- приобретения умений и навыков работы с СЗИ.

Практические умения и навыки работы с КСЗИ студенты получают на лабораторных занятиях (ЛЗ) в дисплейных классах кафедры КТС КубГАУ. Для каждого студента, изучающего дисциплину, предусматривается не менее 40 часов машинного времени.

Качественное изучение дисциплины "Информационная безопасность" базируется на том, что студенты 5-го курса ФПИ ФГОУ ВПО КубГАУ уже имеют подготовку по дисциплинам:

- Теория систем и системного анализа (ТСиСА);
- Вычислительные системы, сети и телекоммуникации (ВССТ).

Контрольные вопросы

1. Охарактеризуйте суть информации и ее свойства.
2. Что является объектом и предметом защиты информации?
3. Объясните сходства и различие терминов, данные и информация.
4. Объясните суть термина сигнал.
5. Дайте характеристику основных понятий теории защиты информации.
6. Сформулируйте цель изучения дисциплины.
7. Перечислите задачи изучения дисциплины.

Лекция 2. КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Вопросы:

- 2.1. Основные положения системы защиты информации
- 2.2. Концептуальная модель информационной безопасности
- 2.3. Угрозы конфиденциальной информации
- 2.4. Действия, приводящие к неправомерному овладению информацией

Литература:

1. Завгородний В.И. комплексная защита информации в компьютерных системах: Учебное пособие. – Логос, 201. – С.6-16.
2. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. – М.: Академический проект: Гаудеамус, 2004. – С.6-28.

Что храним, то и имеем

"ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ - это состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государств".

Закон РФ "Об участии в международном информационном обмене"

Постулаты

1. Информация - это всеобщее свойство материи.
2. Любое взаимодействие в природе и обществе основано на информации.
3. Всякий процесс совершения работы есть процесс информационного взаимодействия.
4. Информация - продукт отражения действительности.
5. Действительность отражается в пространстве и времени.
6. Ничего не происходит из ничего.
7. Информация сохраняет свое значение в неизменном виде до тех пор, пока остается в неизменном виде носитель информации - ПАМЯТЬ.
8. Ничто не исчезает просто так.

Понятие "информация" сегодня употребляется весьма широко и разносторонне. Трудно найти такую область знаний, где бы оно не использовалось. Огромные информационные потоки буквально захлестывают людей. Объем научных знаний, например, по оценке специалистов, удваивается каждые пять лет. Такое положение приводит к заключению, что XXI век будет веком торжества теории и практики ИНФОРМАЦИИ - информационным веком.

Правомерно задать вопрос: что же такое информация? В литературе дается такое определение: информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. Известно, что информация может иметь различную форму, включая данные, заложенные в компьютерах, "синьки", кальки, письма или памятные записки, досье, формулы, чертежи, диаграммы, модели продукции и прототипы, диссертации, судебные документы и другое.

Как и всякий продукт, информация имеет потребителей, нуждающихся в ней, и потому обладает определенными потребительскими качествами, а также имеет и своих обладателей или производителей.

С точки зрения потребителя, качество используемой информации позволяет получать дополнительный экономический или моральный эффект.

С точки зрения обладателя - сохранение в тайне коммерчески важной информации позволяет успешно конкурировать на рынке производства и сбыта товаров и услуг. Это, естественно, требует определенных действий, направленных на защиту конфиденциальной информации (ЗКИ).

Понимая под безопасностью состояние защищенности жизненно важных интересов личности, предприятия, государства от внутренних и внешних угроз, можно выделить и компоненты безопасности - такие, как *персонал*, материальные и финансовые *средства* и *информацию*.

1.1. Основные положения системы защиты информации

Анализ состояния дел в сфере защиты информации показывает, что уже сложилась вполне сформировавшаяся концепция и структура защиты, основу которой составляют:

- весьма развитый арсенал технических средств защиты информации (ЗИ), производимых на промышленной основе;
- значительное число фирм, специализирующихся на решении вопросов ЗИ
- достаточно четко очерченная система взглядов на эту проблему;
- наличие значительного практического опыта и другое.

И, тем не менее, как свидетельствует отечественная и зарубежная печать, злоумышленные действия над информацией не только не уменьшаются, но и имеют достаточно устойчивую тенденцию к росту.

Опыт показывает, что для борьбы с этой тенденцией необходима стройная и целенаправленная организация процесса защиты информационных ресурсов (ИР). Причем в этом должны активно участвовать профессиональные специалисты, администрация, сотрудники и пользователи, что и определяет повышенную значимость организационной стороны вопроса.

Опыт также показывает, что:

- обеспечение информационной безопасности /ИБ/ (безопасности информации) не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования и развития системы защиты, непрерывном контроле ее состояния, выявлении ее узких и слабых мест и противоправных действий;
- безопасность информации может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты во всех структурных элементах производственной системы и на всех этапах технологического цикла обработки информации. Наибольший эффект достигается тогда, когда все используемые средства, методы и меры объединяются в единый целостный механизм систему защиты информации (СЗИ). При этом функционирование системы должно контролироваться обновляться и дополняться в зависимости от изменения внешних и внутренних условий;
- ни какая СЗИ не может обеспечить требуемого уровня безопасности информации без надлежащей подготовки пользователей и соблюдения ими всех установленных правил, направленных на ее защиту (рис.2.1).

БЕЗОПАСНОСТЬ - состояние защищенности жизненно важных интересов личности, предприятия, государства от внутренних и внешних угроз

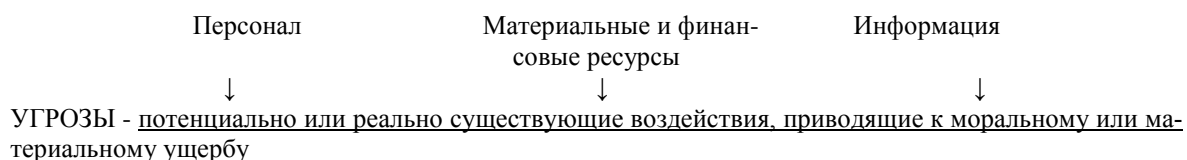


Рис.2.1. Безопасность объекта и угрозы ей

С учетом накопленного опыта можно определить СЗИ как организованную совокупность специальных органов, средств, методов и мероприятий, обеспечивающих защиту информации от внутренних и внешних угроз.

С позиций системного подхода к ЗИ предъявляются определенные требования. ЗИ должна быть:

- непрерывной. Это требование проистекает из того, что злоумышленники только и ищут возможность, как бы обойти защиту интересующей их информации;

- плановой. Планирование осуществляется путем разработки каждой службой детальных планов защиты информации в сфере ее компетенции с учетом общей цели предприятия (организации);

- целенаправленной. Защищается то, что должно защищаться в интересах конкретной цели, а не все подряд;

- конкретной. защите подлежат конкретные данные, объективно подлежащие охране, утрата которых может причинить организации определенный ущерб;

- активной. Защищать информацию необходимо с достаточной степенью настойчивости;

- надежной. Методы и формы защиты должны надежно перекрывать возможные пути неправомерного доступа к охраняемым секретам, независимо от формы их представления, языка выражения и вида физического носителя, на котором они закреплены;

- универсальной. Считается, что в зависимости от вида канала утечки или способа несанкционированного доступа его необходимо перекрывать, где бы он ни проявился, разумными и достаточными средствами, независимо от характера, формы и вида информации;

- комплексной. ДляЗИ во всем многообразии структурных элементов должны применяться все виды и формы защиты в полном объеме. Недопустимо применять лишь отдельные формы или технические средства (ТС). Комплексный характер защиты проистекает из того, что защита - это специфическое явление, представляющее собой сложную систему неразрывно взаимосвязанных и взаимозависимых процессов, каждый из которых в свою очередь имеет множество различных взаимообуславливающих друг друга сторон, свойств, тенденций.

Зарубежный и отечественный опыт показывает, что для обеспечения выполнения столь многогранных требований безопасности СЗИ должна удовлетворять определенным условиям:

- *охватывать весь технологический комплекс информационной деятельности;*

- *быть разнообразной по используемым средствам, многоуровневой с иерархической последовательностью доступа;*

- *быть открытой для изменения и дополнения мер обеспечения безопасности информации;*

- *быть нестандартной, разнообразной.* При выборе средств защиты нельзя рассчитывать на неосведомленность злоумышленников относительно ее возможностей;

- *быть простой для технического обслуживания и удобной для эксплуатации пользователями;*

- *быть надежной.* Любые поломки технических средств являются причиной появления неконтролируемых каналов утечки информации;

- *быть комплексной, обладать целостностью, означающей, что ни одна ее часть не может быть изъята без ущерба для всей системы.*

К системе ИБ предъявляются также определенные **требования**:

- *четкость* определения полномочий и прав пользователей на доступ к определенным видам информации;

- *предоставление* пользователю *минимальных полномочий*, необходимых ему для выполнения порученной работы;

- *сведение к минимуму* числа общих для нескольких пользователей *средств защиты*;

- *учет* случаев и попыток *несанкционированного доступа* к конфиденциальной информации;

- *обеспечение оценки* степени конфиденциальной информации;

- *обеспечение контроля целостности* средств защиты и *немедленное реагирование на их выход из строя.*

Система защиты информации (СЗИ), как любая система, должна иметь определенные виды собственного обеспечения, опираясь на которые она будет выполнять свою целевую функцию. С учетом этого СЗИ может иметь:

- *правовое обеспечение.* Сюда входят нормативные документы, положения, инструкции, руководства, требования которых являются обязательными в рамках сферы их действия;

- *организационное обеспечение.* Имеется в виду, что реализация защиты информации осуществляется определенными структурными единицами, такими как: служба защиты документов; служба режима, допуска, охраны; служба защиты информации техническими средствами; информационно-аналитическая деятельность и другими;

• *аппаратное обеспечение.* Предполагается широкое использование технических средств как для защиты информации, так и для обеспечения деятельности собственно СЗИ;

• *информационное обеспечение.* Оно включает в себя сведения, данные, показатели, параметры, лежащие в основе решения задач, обеспечивающих функционирование системы. Сюда могут входить как показатели доступа, учета, хранения, так и системы информационного обеспечения расчетных задач различного характера, связанных с деятельностью службы обеспечения безопасности;

• *программное обеспечение.* К нему относятся различные информационные, учетные, статистические и расчетные программы, обеспечивающие оценку наличия и опасности различных каналов утечки и путей несанкционированного проникновения к источникам конфиденциальной информации;

• *математическое обеспечение.* Предполагает использование математических методов для различных расчетов, связанных с оценкой опасности технических средств злоумышленников, зон и норм необходимой защиты;

• *лингвистическое обеспечение.* Совокупность специальных языковых средств общения специалистов и пользователей в сфере защиты информации;

• *нормативно-методическое обеспечение.* Сюда входят нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации, различного рода методики, обеспечивающие деятельность пользователей при выполнении своей работы в условиях жестких требований защиты информации.

Под системой безопасности (СБ) будем понимать организованную совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз (рис.2.2).

Как и любая система, система информационной безопасности (СИБ) имеет свои цели, задачи, методы и средства деятельности, которые согласовываются по месту и времени в зависимости от условий.

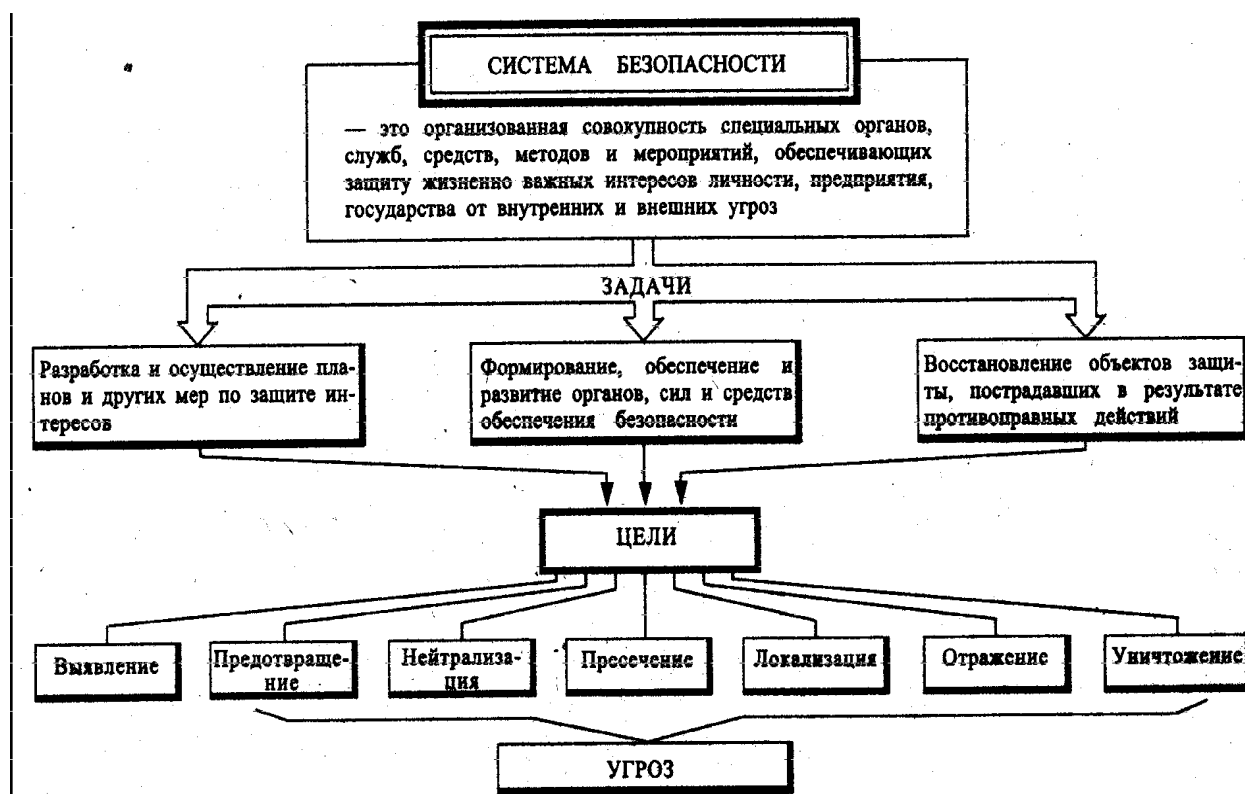


Рис.2.2. Система безопасности (СБ) объекта

Удовлетворить современные требования по обеспечению безопасности предприятия и защиты его конфиденциальной информации может только система безопасности.

1.2. Концептуальная модель информационной безопасности

Понимая информационную безопасность (ИБ) как "состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций", правомерно определить угрозы ИБ, источники этих угроз, способы их реализации и цели, а также иные условия и действия, нарушающие безопасность. При этом, естественно, следует рассматривать и меры защиты информации от неправомерных действий, приводящих к нанесению ущерба.

Практика показала, что для анализа такого значительного набора источников, объектов и действий целесообразно использовать **моделирование**, при котором вместо реальных ситуаций используется модель – ее "заместитель". При этом следует учитывать, что модель не копирует оригинал, она проще. Модель должна быть достаточно общей, чтобы описывать реальные действия с учетом их сложности.

Можно предложить компоненты модели информационной безопасности на первом уровне декомпозиции. По нашему мнению, такими компонентами концептуальной модели ИБ могут быть следующие:

- *объекты угроз;*
- *угрозы;*
- *источники угроз;*
- *цели угроз со стороны злоумышленников;*
- *источники информации;*
- *способы неправомерного овладения конфиденциальной информацией (способы доступа);*
- *направленияЗИ*
- *способыЗИ;*
- *средстваЗИ.*

Объектом угроз ИБ выступают сведения о составе, состоянии и деятельности объекта защиты (персонала, материальных и финансовых ценностей, информационных ресурсов).

Угрозы информации выражаются в нарушении ее целостности, конфиденциальности, полноты и доступности.

Источниками угроз выступают конкуренты, преступники, коррупционеры, административно-управленческие органы.

Источники угроз преследуют при этом следующие цели:

- *ознакомление с охраняемыми сведениями,*
- *их модификация в корыстных целях и*
- *уничтожение для нанесения прямого материального ущерба (рис.2.3).*

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ - состояние защищенности информационной среды общества от внутренних и внешних угроз, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства

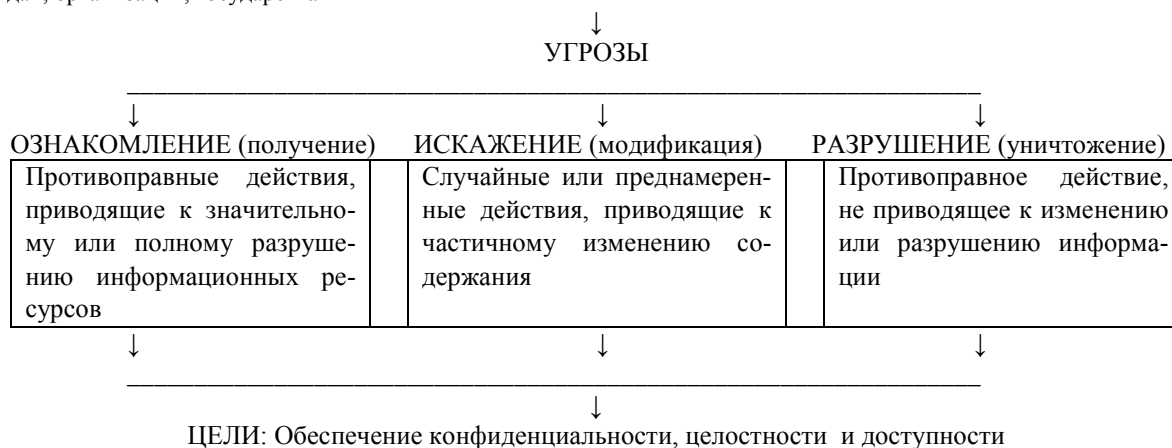


Рис.2.3. Цели источников угроз информационной безопасности

Неправомерное овладение конфиденциальной информацией возможно за счет ее разглашения источниками сведений, за счет утечки информации через технические средства и за счет несанкционированного доступа к охраняемым сведениям.

Источниками конфиденциальной информации являются люди, документы, публикации, технические носители информации, технические средства обеспечения производственной и трудовой деятельности, продукция и отходы производства.

Основными направлениями ЗИ являются *правовая, организационная и инженерно-техническая защиты информации* как выразители комплексного подхода к обеспечению информационной безопасности.

Средствами ЗИ являются физические средства, аппаратные средства, программные средства и криптографические методы. Последние могут быть реализованы как аппаратно, программно, так и смешанно программно-аппаратными средствами.

В качестве способов защиты выступают всевозможные меры, пути, способы и действия, обеспечивающие упреждение противоправных действий, их предотвращение, пресечение и противодействие несанкционированному доступу.

В обобщенном виде рассмотренные компоненты в виде концептуальной модели безопасности информации приведены на следующей схеме (рис.2.4).

Основные элементы концептуальной модели будут рассмотрены более подробно в следующих разделах книги.

Концепция безопасности является основным правовым документом, определяющим защищенность предприятия от внутренних и внешних угроз.

Информационная безопасность - это состояние защищенности ИР, технологии их формирования и использования, а также прав субъектов информационной деятельности

ОБЪЕКТЫ УГРОЗ Сведения о составе, состоянии и деятельности	СПОСОБЫ ДОСТУПА - за счет разглашения - за счет утечки - за счет НСД		НАПРАВЛЕНИЯ ЗАЩИТЫ - правовая - организационная - инженерно-техническая
УГРОЗЫ - целостности - конфиденциальности - полноте - доступности	ИНФОРМАЦИЯ		СРЕДСТВА ЗАЩИТЫ - физические - аппаратные - программные - криптографические
ИСТОЧНИКИ УГРОЗ - конкуренты - преступники - коррупционеры - административные органы	ЦЕЛИ - ознакомление - модификация - уничтожение	ИСТОЧНИКИ ИНФОРМАЦИИ - люди - документы - публикации - тех. носители - тех. средства - продукция отходы	СПОСОБЫ ЗАЩИТЫ - упреждение - предотвращение - пресечение - противодействие

Рис.2.4. Концептуальная модель безопасности информации

1.3. Угрозы конфиденциальной информации

Под **угрозами** конфиденциальной информации принято понимать потенциальные или реально возможные действия по отношению к информационным ресурсам, приводящие к неправомерному овладению охраняемыми сведениями.

Таковыми действиями являются:

- *ознакомление с конфиденциальной информацией* различными путями и способами *без нарушения ее целостности*;
- *модификация информации* в криминальных целях как частичное или значительное изменение состава и содержания сведений;
- *разрушение (уничтожение) информации* как акт вандализма с целью прямого нанесения материального ущерба.

В конечном итоге противоправные действия с информацией приводят к нарушению ее конфиденциальности, полноты, достоверности и доступности (рис.2.5), что в свою очередь приводит к нарушению как режима управления, так и его качества в условиях ложной или неполной информации.



Рис.2.5. Проявление угроз безопасности конфиденциальной информации

Каждая угроза влечет за собой определенный ущерб - моральный или материальный, а защита и противодействие угрозе призваны снизить его величину, в идеале - полностью, реально - значительно или хотя бы частично.

Но и это удается далеко не всегда.

С учетом этого угрозы могут быть классифицированы по следующим кластерам (рис.2.6):

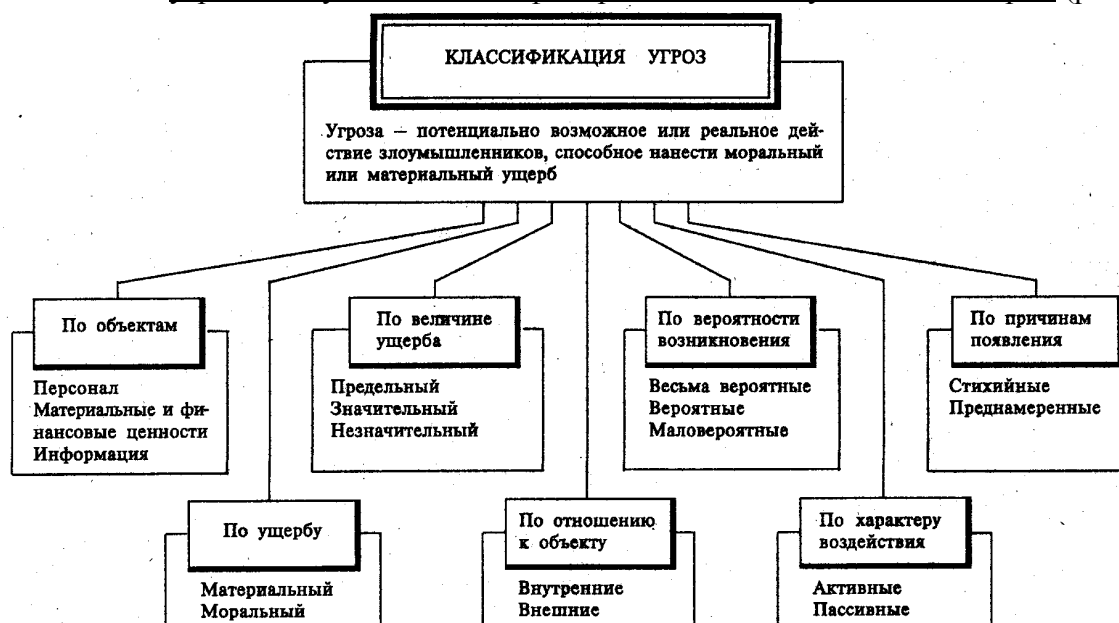


Рис.2.6. Классификация угроз

- по величине принесенного ущерба:

- предельный, после которого фирма может стать банкротом;
- значительный, но не приводящий к банкротству;
- незначительный, который фирма за какое-то время может компенсировать.

- по вероятности возникновения:

- весьма вероятная угроза;
- вероятная угроза;
- маловероятная угроза.

- по причинам появления:

- стихийные бедствия;
- преднамеренные действия.

- по характеру нанесенного ущерба:

- материальный;
- моральный;

- по характеру воздействия:

- активные;
- пассивные.

- по отношению к объекту:

- внутренние;
- внешние.

Источниками внешних угроз являются:

- * недобросовестные конкуренты;
- * преступные группировки и формирования;
- * отдельные лица и организации административно-управленческого аппарата.

Источниками внутренних угроз могут быть:

- ** администрация предприятия;
- ** персонал;
- ** технические средства обеспечения производственной и трудовой деятельности.

Соотношение внешних и внутренних угроз на усредненном уровне можно охарактеризовать так:

- 82% угроз совершается собственными сотрудниками фирмы при их прямом или опосредованном участии;
- 17% угроз совершается извне - внешние угрозы;
- 1% угроз совершается случайными лицами.

Угроза - это потенциальные или реальные действия, приводящие к моральному или материальному ущербу.

1.4. Действия, приводящие к неправомерному овладению информацией

Отношение объекта (фирма, организация) и субъекта (конкурент, злоумышленник) в информационном процессе с противоположными интересами можно рассматривать с позиции активного **взаимодействия, приводящего к овладению конфиденциальными сведениями**. В этом случае возможны такие ситуации:

- *владелец (источник)* не принимает никаких мер к сохранению конфиденциальной информации, что позволяет злоумышленнику легко получить интересующие его сведения;
- *источник информации* строго соблюдает меры ИБ, тогда злоумышленнику приходится прилагать значительные усилия к осуществлению доступа к охраняемым сведениям, используя для этого всю совокупность способов несанкционированного проникновения: легальное или нелегальное, заходное или беззаходное;
- *промежуточная ситуация* - это утечка информации по техническим каналам, при которой источник еще не знает об этом (иначе он принял бы меры защиты), а злоумышленник легко, без особых усилий может их использовать в своих интересах.

Факт получения охраняемых сведений злоумышленниками или конкурентами называют утечкой. Однако одновременно с этим в значительной части законодательных актов, законов, кодексов, официальных материалов используются и такие понятия, как **разглашение сведений** и **несанкционированный доступ к конфиденциальной информации** (рис.2.7).

1. Разглашение - это умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним.

Разглашение выражается в сообщении, передаче, предоставлении, пересылке, опубликовании, утере и в других формах обмена и действий с деловой и научной информацией. Реализуется разглашение по формальным и неформальным каналам распространения информации. К формальным коммуникациям относятся деловые встречи, совещания, переговоры и тому подобные формы общения: обмен официальными деловыми и научными документами средствами передачи официальной информации (почта, телефон, телеграф и т.д.). Неформальные коммуникации включают личное общение (встречи, переписка), выставки, семинары, конференции и другие массовые мероприятия, а также средства массовой информации (печать, газеты, интервью, радио, телевидение). Как правило, причиной разглашения конфиденциальной информации является недостаточное знание сотрудниками правил защиты коммерческих секретов и непонимание (или недопонимание) необходимости их тщательного соблюдения. Тут важно отметить, что субъектом в этом процессе выступает источник (владелец) охраняемых секретов.

Следует отметить информационные особенности этого действия. Информация содержательная, осмысленная, упорядоченная, аргументированная, объемная и доводится зачастую в реальном масштабе времени. Часто

имеется возможность диалога. Информация ориентирована в определенной тематической области и документирована. Для получения интересующей злоумышленника информации последний затрачивает практически минимальные усилия и использует простые легальные технические средства (диктофоны, видеомониторинг).



Рис.2.7. Действия, приводящие к незаконному овладению информацией

2. Утечка - это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена.

Утечка информации осуществляется по различным техническим каналам. Известно, что информация вообще переносится или передается либо энергией, либо веществом. Это либо акустическая волна (звук), либо электромагнитное излучение, либо лист бумаги (написанный текст) и др. С учетом этого можно утверждать, что по физической природе возможны следующие пути переноса информации: световые лучи, звуковые волны, электромагнитные волны, материалы и вещества. Соответственно этому классифицируются и каналы утечки информации на визуально-оптические, акустические, электромагнитные и материально-вещественные. Под каналом утечки информации принято понимать физический путь от источника конфиденциальной информации к злоумышленнику, посредством которого последний может получить доступ к охраняемым сведениям. Для образования канала утечки информации необходимы определенные пространственные, энергетические и временные условия, а также наличие на стороне злоумышленника соответствующей аппаратуры приема, обработки и фиксации информации.

3. Несанкционированный доступ (НСД)- это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам.

Несанкционированный доступ к источникам конфиденциальной информации реализуется различными способами: от инициативного сотрудничества, выражающегося в активном стремлении «продать» секреты, до использования различных средств проникновения к коммерческим секретам. Для реализации этих действий злоумышленнику приходится часто проникать на объект или создавать вблизи него специальные посты контроля и наблюдения - стационарных или в подвижном варианте, оборудованных самыми современными техническими средствами.

Если исходить из комплексного подхода к обеспечению информационной безопасности, то такое деление ориентирует на защиту информации, как от разглашения, так и от утечки по техническим каналам и от несанкционированного доступа к ней со стороны конкурентов и злоумышленников.

Такой подход к классификации действий, способствующих неправомерному овладению конфиденциальной информацией, показывает многогранность угроз и многоаспектность защитных мероприятий, необходимых для обеспечения комплексной ИБ.

С учетом изложенного отметим следующие условия способствующие неправомерному овладению конфиденциальной информацией:

- = *разглашение* (излишняя болтливость сотрудников) - 32%;
- = *несанкционированный доступ путем подкупа* и склонения к сотрудничеству со стороны конкурентов и преступных группировок - 24%;
- = *отсутствие* на фирме надлежащего *контроля* и жестких условий обеспечения информационной безопасности — 14%;
- = *традиционный обмен* производственным *опытом* - 12%;

= бесконтрольное использование ИС - 10%;

=наличие предпосылок возникновения, среди сотрудников *конфликтных ситуаций* - 8%;

а также *отсутствие* высокой трудовой дисциплины, *психологическая несовместимость*, *случайный подбор кадров*, *слабая работа службы кадров по сплочению коллектива*.

Среди форм и методов недобросовестной конкуренции находят наибольшее распространение:

- *экономическое подавление*, выражающееся в срыве сделок и иных соглашений (48%), парализации деятельности фирмы (31%), компрометации фирмы (11%), шантаже руководителей фирмы (10%);
- *физическое подавление*: ограбления и разбойные нападения на офисы, склады, грузы (73%), угрозы физической расправы над руководителями фирмы и ведущими специалистами (22%), убийства и захват заложников (5%);
- *информационное воздействие*: подкуп сотрудников (43%), копирование информации (24%), проникновение в базы данных (18%), продажа конфиденциальных документов (10%), подслушивание телефонных переговоров и переговоров в помещениях (5%), а также ограничение доступа к информации, дезинформация;
- *финансовое подавление* включает такие понятия, как инфляция, бюджетный дефицит, коррупция, хищение финансов, мошенничество;
- *психическое давление* может выражаться в виде хулиганских выходок, угрозы и шантажа, энергоинформационного воздействия.

Основными угрозами информации являются ее разглашение, утечка и НСД к ее источникам.

Каждому из условий неправомерного овладения конфиденциальной информацией можно поставить в соответствие определенные каналы, определенные способы защитных действий и определенные классы средств защиты или противодействия. Совокупность определений, каналов, способов и средств представляется в виде следующей схемы (рис.2.8).

УГРОЗЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ		
РАЗГЛАШЕНИЕ	УТЕЧКА	НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП
Каналы распространения	Каналы утечки	Каналы проникновения
Способы пресечения	Способы защиты	Способы противодействия
Средства пресечения	Средства защиты	Средства противодействия

Рис.2.8. Совокупность определений, каналов, способов и средств ЗИ

Выводы: Все изложенное в этой главе можно кратко сформулировать так.

1. Информация - это ресурс. Потеря конфиденциальной информации приносит моральный или материальный ущерб.
2. Условия, способствующие неправомерному овладению информацией, сводятся к ее разглашению, утечке и несанкционированному доступу к ее источникам.
3. В современных условиях безопасность ИР может быть обеспечена только комплексной системой защиты информации (КСЗИ).
4. КСЗИ должна быть: непрерывной, плановой, целенаправленной, конкретной, активной, надежной.
5. КСЗИ должна опираться на систему видов собственного обеспечения, способного реализовать ее функционирование не только в повседневных условиях, но и в критических ситуациях.

Контрольные вопросы

1. Сформулируйте понятие информационной безопасности (ИБ)
2. Определите объекты, угрозы и источники информации
3. Перечислите основные угрозы информации
4. Опишите классификации угроз ИБ

Лекция 3. УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В КС

Вопросы:

- 3.1. Классификация угроз
- 3.2. Случайные угрозы
- 3.3. Преднамеренные угрозы

Литература:

1. Завгородний В.И. комплексная защита информации в компьютерных системах: Учебное пособие. – Логос, 201. – С.16-28.
2. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. – М.: Академический проект: Гаудеамус, 2004. – С.18-28.

3.1. Классификация угроз.

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 потребления" в КС и выступает в виде центральной компоненты системы. ИБ 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, называемых 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 ИБ 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.3.1).

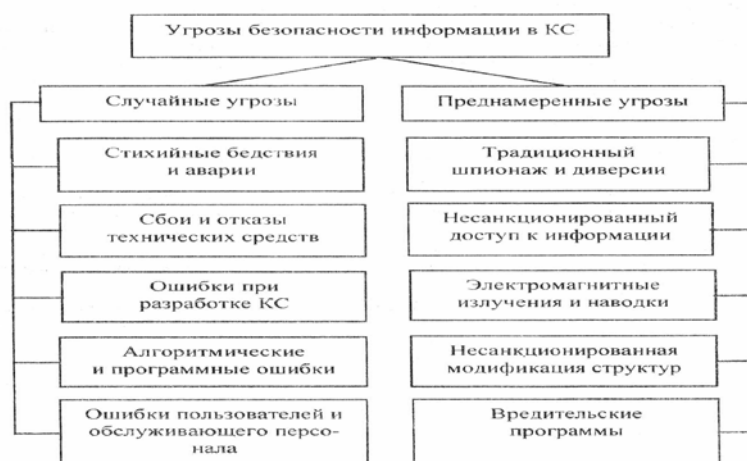


Рис.3.1. Угрозы безопасности информации в компьютерных системах

3.2. Случайные угрозы

Случайными (непреднамеренными) называют угрозы, которые не связаны с преднамеренными действиями злоумышленников и реализуются в случайные моменты времени.

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.

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 отдельных 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 защиты 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.

3.3. Преднамеренные угрозы

Преднамеренно создаваемые угрозы – это второй класс угроз безопасности информации в КС, которые обусловлены появлением угроз, связанных с деятельностью человека.

Данный класс угроз изучен недостаточно, очень динамичен и постоянно пополняется новыми видами угроз. Сегодня угрозы этого класса в соответствии с их физической сущностью и механизмами реализации могут быть распределены на пять групп:

- традиционный или универсальный шпионаж и диверсии;
- несанкционированный доступ к информации;
- электромагнитные излучения и наводки;
- модификация структур КС;
- вредительские программы.

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 традиционного 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.

Подслушивание. 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 окопном 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. Реальные расстояния 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]. Съём 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 проводным и радиоканалам не требует дорогостоящего оборудования и высокой квалификации злоумышленника.

Дистанционная видео-разведка для получения информации в КС малоприменима 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 микро-видеокамера весит 15 г)[68].

Хищение документов, машинных носителей, программ и атрибутов системы защиты прямо связано с вербовкой сотрудников. В этом случае злоумышленник все эти действия может делать чужими руками, вплоть до физического уничтожения объектов КС, применяя традиционные методы шпионажа и диверсий через "своих" людей.

Злоумышленник или его люди, имеющие доступ на объект КС, все это может делать сам, используя 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" ("радио-закладки") быстро устанавливаются, но также имеют демаскирующий признак - излучение в радио или оптическом диапазоне. "Радио-закладки" 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 к 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.

Сбор и анализ отходов машинных носителей информации, поджоги и взрывы (диверсии) злоумышленник также может делать сам, либо через завербованных им людей, работающих на предприятии.

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

2. Несанкционированный доступ к информации. Термин "несанкционированный доступ к информации" (НСДИ) определен как доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств и 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 иницируются 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 лекции 9.

НСД 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.

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 источника 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.

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 или 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".

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 утилит оказывают негативное воздействие на КС.

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

6. Классификация злоумышленников. Возможности осуществления вредительских воздействий в большей 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, находится 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 ЗИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Лекция 4. НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Вопросы:

- 4.1. Правовая защита
- 4.2. Организационная защита
- 4.3. Инженерно-техническая защита

Литература:

1. Завгородний В.И. комплексная защита информации в компьютерных системах: Учебное пособие. – Логос, 201. – С.16-28.
2. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. – М.: Академический проект: Гаудеамус, 2004. – С.18-28.

Подальше положишь - поближе возьмешь

Направления обеспечения информационной безопасности - это нормативно-правовые категории,

Постулаты Безопасности

1. Если не уверен в безопасности, считай, что опасность существует реально.
2. Безопасности бесплатной не бывает.
3. Безопасности не бывает много.
4. Безопасность должна быть только комплексной.
5. Комплексная безопасность может быть обеспечена только системой безопасности.
6. Никакая система безопасности не обеспечивает требуемого уровня без надлежащей подготовки руководителей, сотрудников и клиентов.
7. В безопасности должен быть заинтересован каждый.

Направления обеспечения безопасности - это нормативно-правовые категории, определяющие комплексные меры ЗИ на уровне: государства, предприятия и организации, личности. Они ориентированны на обеспечение комплексной ЗИ от внутренних и внешних угроз.

С учетом сложившейся практики обеспечения ИБ выделяют следующие направления ЗИ:

- правовая защита - это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
- организационная защита - это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба исполнителям;
- инженерно-техническая защита - это использование различных технических средств, препятствующих нанесению ущерба коммерческой деятельности (рис.4.1).



Рис.4.1. Направления обеспечения безопасности

Кроме этого, защитные действия, ориентированные на обеспечение ИБ, могут быть охарактеризованы целым рядом параметров, отражающих, помимо направлений, ориентацию на

объекты защиты, характер угроз, способы действий, их распространенность, охват и масштабность (рис.4.2).

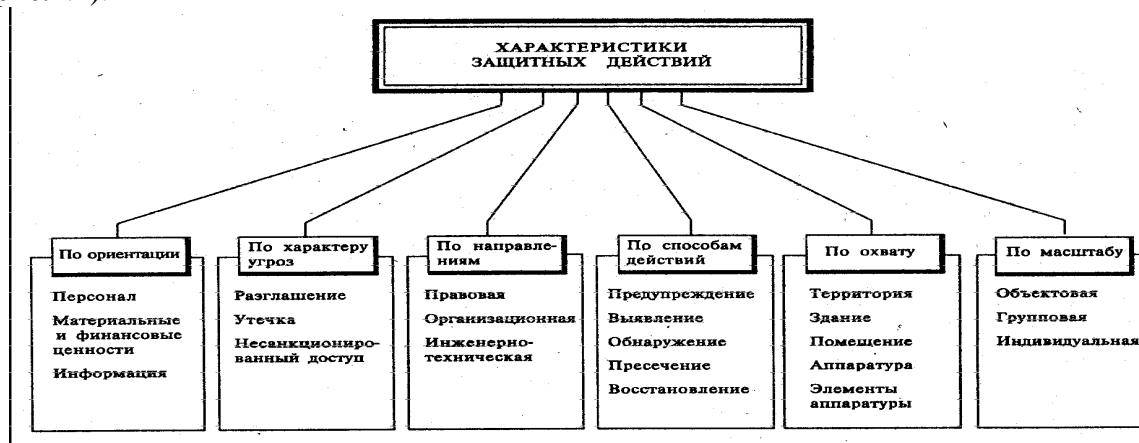


Рис.4.2. Характеристики защитных действий

Так, по характеру угроз защитные действия ориентированы на ЗИ от разглашения, утечки и несанкционированного доступа. По способам действий их можно подразделить на предупреждение, выявление, обнаружение, пресечение и восстановление ущерба или иных убытков. По охвату защитные действия могут быть ориентированы на территорию, здание, помещение, аппаратуру или отдельные элементы аппаратуры. Масштабность защитных мероприятий характеризуется как объектовая, групповая или индивидуальная защита. Например, защита автономной ПЭВМ в режиме индивидуального пользования.

4.1. Правовая защита

Как известно, **право** - это совокупность общеобязательных правил и норм поведения, установленных или санкционированных государством в отношении определенных сфер жизни и деятельности государственных органов, предприятий (организаций) и населения (отдельной личности).

Правовая ЗИ как ресурса признана на международном, государственном уровне и определяется межгосударственными договорами, конвенциями, декларациями и реализуется патентами, авторским правом и лицензиями на их защиту. На государственном уровне правовая защита регулируется государственными и ведомственными актами (рис.4.3.).

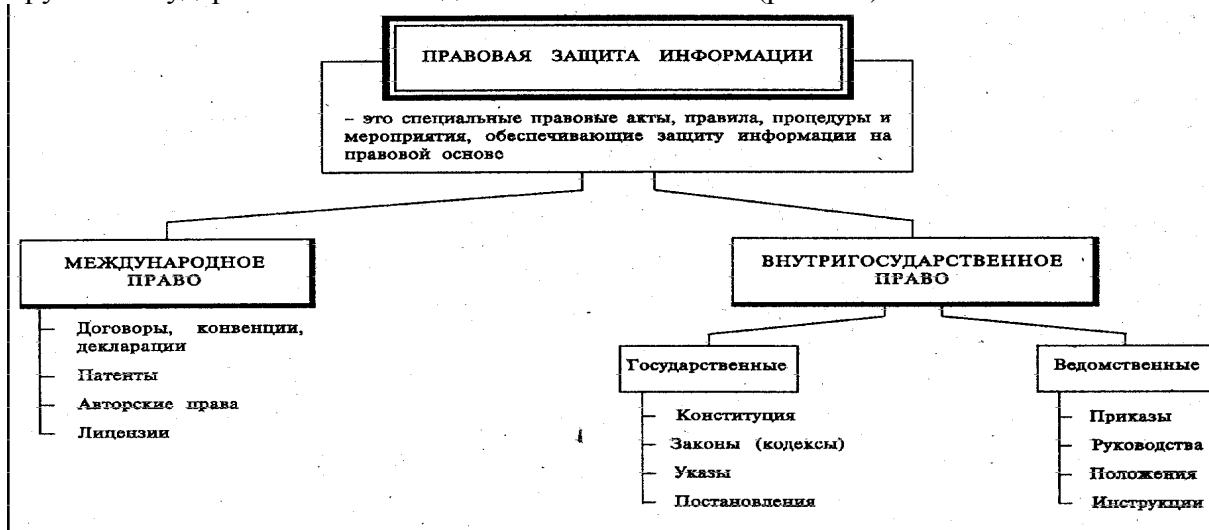


Рис.4.3. Правовая защита информации

В нашей стране такими правилами (актами, номами) являются Конституция, законы РФ, гражданское, административное, уголовное право, изложенные в соответствующих кодексах. Что касается ведомственных нормативных актов, то они определяются приказами, руководствами, положениями и инструкциями, издаваемыми ведомствами, организациями и предпри-

иятиями, действующими в рамках определенных структур (рис.4.5).

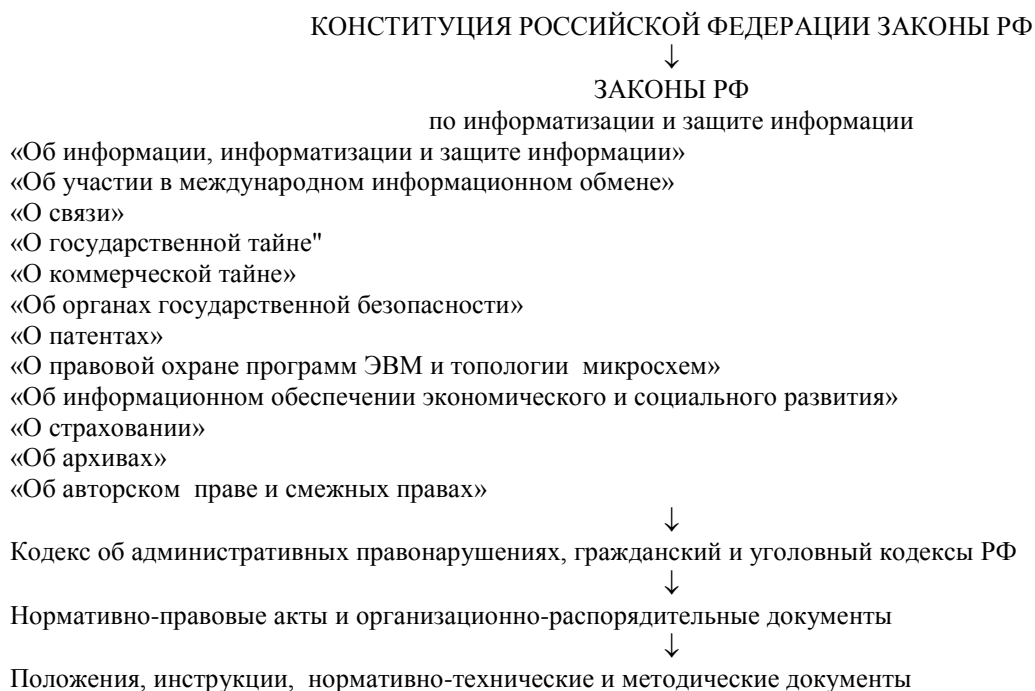


Рис.4.5. Структура законодательства России в области защиты информации

Современные условия требуют и определяют необходимость комплексного подхода к формированию законодательства по ЗИ, его состава и содержания, соотнесения его со всей системой законов и правовых актов РФ.

Требования ИБ должны органически включаться во все уровни законодательства, в том числе и в конституционное законодательство, основные общие законы, законы по организации государственной системы управления, специальные законы, ведомственные правовые акты и другие. В литературе приводится такая структура правовых актов, ориентированных на правовую защиту информации.

Первый блок - конституционное законодательство. Нормы, касающиеся вопросов информатизации и ЗИ, входят в него как составные элементы.

Второй блок - общие законы, кодексы (о собственности, о недрах, о земле, о правах граждан, о гражданстве, о налогах, об антимонопольной деятельности), которые включают нормы по вопросам информатизации и ИБ.

Третий блок - законы об организации управления, касающиеся отдельных структур хозяйства, экономики, системы государственных органов и определяющие их статус. Они включают отдельные нормы по вопросам ЗИ. Наряду с общими вопросами информационного обеспечения и ЗИ конкретного органа эти нормы должны устанавливать его обязанности по формированию, актуализации и безопасности информации, представляющей общегосударственный интерес.

Четвертый блок - специальные законы, полностью относящиеся к конкретным сферам отношений, отраслям хозяйства, процессам. В их число входит и Закон РФ "Об информации, информатизации и защите информации". Именно состав и содержание этого блока законов и создает специальное законодательство как основу правового обеспечения ИБ.

Пятый блок - законодательство субъектов РФ, касающееся ЗИ.

Шестой блок - подзаконные нормативные акты по ЗИ.

Седьмой блок - это правоохранительное законодательство России, содержащее нормы об ответственности за правонарушения в сфере информатизации.

Специальное законодательство в области ИБ может быть представлено совокупностью законов. В их составе особое место принадлежит базовому Закону "Об информации, информатизации и защите информации", который закладывает основы правового определения всех важнейших компонентов информационной деятельности:

- информации и ИС;
- субъектов - участников информационных процессов;

- и правоотношений производителей - потребителей информационной продукции;

- владельцев (обладателей, источников) информации - обработчиков и потребителей на основе отношений собственности при обеспечении гарантий интересов граждан и государства.

Этот закон определяет основы ЗИ в системах обработки и при ее использовании с учетом категорий доступа к открытой информации и к информации с ограниченным доступом. Он, кроме того, содержит общие нормы по организации и ведению информационных систем (ИС), включая банки данных (БД) государственного назначения, порядка государственной регистрации, лицензирования, сертификации, экспертизы, а также общие принципы защиты и гарантий прав участников информационного процесса.

В дополнение к базовому закону в мае 1992 г. были приняты Законы "О правовой охране программ для электронно-вычислительных машин и баз данных" и "О правовой охране топологии интегральных микросхем".

Оба закона устанавливают охрану соответствующих объектов с помощью норм авторского права, включая в перечень объектов авторского права наряду с традиционными базами данных топологии интегральных микросхем и программы для ЭВМ.

Вопросы правового режима информации с ограниченным доступом реализуются в двух самостоятельных законах о государственной и коммерческой (проект) тайнах. Кроме того, этот аспект раскрывается и в Гражданском кодексе РФ статьей 139 "Служебная и коммерческая тайна".

1. Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности. Сведения, которые не могут составлять служебную или коммерческую тайну, определяются законом и иными правовыми актами.

2. Информация, составляющая служебную или коммерческую тайну, защищается способами, предусмотренными настоящим кодексом и другими законами.

Вторая часть статьи 139 определяет правовые основы ответственности за несанкционированное получение информации или причинение ущерба. Звучит это так:

"Лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору".

Указ Президента РФ от 6 марта 1997г. № 188 определяет понятие и содержание конфиденциальной информации (см. таблицу 4.1).

Таблица 4.1. Понятие и содержание конфиденциальной информации

	КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ	Документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ
1	ЛИЧНАЯ	Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленном порядке
2	СУДЕБНО-СЛЕДСТВЕННАЯ	Сведения, составляющие тайну следствия и судопроизводства
3	СЛУЖЕБНАЯ	Служебные сведения, доступ к которым ограничен органами государственной власти (служебная тайна)
4	ПРОФЕССИОНАЛЬНАЯ	Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений и др.)
5	КОММЕРЧЕСКАЯ	Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен законами (коммерческая тайна)
6	ПРОИЗВОДСТВЕННАЯ	Сведения о сущности изобретения полезной модели или промышленного образца до официальной публикации информации о них

Таким образом, правовая ЗИ обеспечивается нормативно-законодательными актами, представляющими собой по уровню иерархическую систему от Конституции РФ до функциональных обязанностей и контракта отдельного конкретного исполнителя, определяющих перечень

сведений, подлежащих охране, и меры ответственности за их разглашение.

Одним из новых для нас направлений правовой защиты является страховое обеспечение. Оно предназначено для защиты собственника информации и средств ее обработки как от традиционных угроз (кражи, стихийные бедствия), так и от угроз, возникающих в ходе работы с информацией. К ним относятся: разглашение, утечка и несанкционированный доступ к конфиденциальной информации.

Целью страхования является обеспечение страховой защиты физических и юридических лиц от страховых рисков в виде полного или частичного возмещения ущерба и потерь, причиненных стихийными бедствиями, чрезвычайными происшествиями в различных областях деятельности, противоправными действиями со стороны конкурентов и злоумышленников, путем выплат денежной компенсации или оказания сервисных услуг (ремонт, восстановление) при наступлении страхового события.

Таблица 4.1. Понятие и содержание конфиденциальной информации

	КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ	Документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ
1	ЛИЧНАЯ	Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленном порядке
2	СУДЕБНО-СЛЕДСТВЕННАЯ	Сведения, составляющие тайну следствия и судопроизводства
3	СЛУЖЕБНАЯ	Служебные сведения, доступ к которым ограничен органами государственной власти (служебная тайна)
4	ПРОФЕССИОНАЛЬНАЯ	Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений и др.)
5	КОММЕРЧЕСКАЯ	Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен законами (коммерческая тайна)
6	ПРОИЗВОДСТВЕННАЯ	Сведения о сущности изобретения полезной модели или промышленного образца до официальной публикации информации о них

В основе российского страхового законодательства лежит Закон РФ "О страховании". Он призван гарантировать защиту интересов страхователей, определять единые положения по организации страхования и принципы государственного регулирования страховой деятельности.

Закон "О страховании" дает следующее понятие страхования:

"Страхование представляет собой отношения по защите имущественных интересов физических и юридических лиц при наступлении определенных событий (страховых случаев) за счет денежных фондов, формируемых из уплачиваемых ими страховых взносов".

Действия по защите информации от утечки по техническим каналам регламентируются следующими правовыми документами:

1. ГОСТ 29339-92 "Информационная технология. Защита информации от утечки за счет ПЭМИН при ее обработке СВТ" (ПЭМИН - побочные электромагнитные излучения и наводки.).
2. ГОСТ Р 50752 "Информационная технология. Защита информации от утечки за счет ПЭМИН при обработке средствами вычислительной техники. Методы испытаний".
3. Нормы эффективности и защиты АСУ и ЭВМ от утечки информации за счет ПЭМИН.
4. Специальные требования и рекомендации по защите объектов ЭВТ II и III категории от утечки информации за счет ПЭМИН.

Действия по ЗИ от несанкционированного доступа (НСД) регламентируют:

- Постановление Правительства РФ от 15.09.93 № 912-51 "Положение о государственной системе защиты информации от иностранной технической разведки и от утечки электрическим каналам)", а также
- Указы Президента:

"О создании государственной технической комиссии при Президенте РФ" (от 05.01.92 № 9);

"О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам связи" (от 08.05.93 № 644);

"О методах по соблюдению законности в области разработки, производства реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации" (от 03.04.95 № 334);

"Положение о государственной системе защиты информации Российской Федерации".

Правовыми документами являются и государственные стандарты на информационную деятельность с учетом обеспечения ее безопасности, в частности:

ГОСТ Р 50739-95 "СВТ. Защита от НСД к информации";

ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования";

ГОСТ Р.34.10-94 "Процедуры выработки и проверки электронной подписи на базе асимметричного криптографического ключа";

ГОСТ Р.34.11-94 "Функция хеширования";

ГОСТ Р.В 50170-92 "Противодействие ИТР. Термины и определения".

Опираясь на государственные правовые акты и учитывая ведомственные интересы на уровне конкретного предприятия (фирмы, организации), разрабатываются собственные нормативно-правовые документы, ориентированные на обеспечение ИБ.

К таким документам относятся:

- Положение о сохранении конфиденциальной информации;
- Перечень сведений, составляющих конфиденциальную информацию;
- Инструкция о порядке допуска сотрудников к сведениям, составляющим конфиденциальную информацию;
- Положение о специальном делопроизводстве и документообороте;
- Перечень сведений, разрешенных к опубликованию в открытой печати;
- Положение о работе с иностранными фирмами и их представителями;
- Обязательство сотрудника о сохранении конфиденциальной информации;
- Памятка сотруднику о сохранении коммерческой тайны.

Указанные нормативные акты направлены на предупреждение случаев неправомерного оглашения (разглашения) секретов на правовой основе, и в случае их нарушения должны приниматься соответствующие меры воздействия.

В зависимости от характера информации, ее доступности для заинтересованных потребителей, а также экономической целесообразности конкретных защитных мер могут быть избраны следующие формы ЗИ:

- патентование;
- авторское право;
- признание сведений конфиденциальными;
- товарные знаки;
- применение норм обязательственного права.

В таблице 4.2 приводятся некоторые характеристики этих форм и анализируется взаимосвязь между ними, а в таблице 4.3 приведены определения и основные параметры коммерческой тайны.

Таблица 4.2. Взаимосвязь патентов и коммерческой тайны

Характеристики	Патенты	Коммерческая тайна
Объект защиты	Специфический и четко определенный документ	Применима к широкому спектру интеллектуальной собственности и деловой информации
Требования к информации	Информация должна быть: полезной, новой, неочевидной	Информация должна быть: потенциально полезной, не должна быть общеизвестной, не обязательно должна быть новой и неочевидной
Степень определенности	Четко определена в заявке	Часто трудно четко определить
Необходимость опубликования	Строго необходима. Публикуется обязательно	Любое обнародование должно быть под контролем и ограничено в неизвестной степени (храниться в тайне)
Порядок защиты	Определяется узким, но четким статусом. Предоставляется монополия	Определяется в зависимости от обстоятельств. Реализуется только от недобросовестной конкуренции
Продолжительность защита	Продолжительность 15-20 лет с момента защиты опубликования	Практически не ограничена
Стоимость	По получению патента	Защита от утечки и использования информации другими лицами
Стоимость риска	Недействительность по истечении срока	Независимое открытие другими лицами

Существуют определенные различия между *авторским правом* и *коммерческой тайной*. **Авторское право защищает** только форму выражения идеи. **Коммерческая тайна относится** непосредственно к содержанию. Авторское право защищает от копирования независимо от конфиденциальных отношений с владельцем. К авторскому праву прибегают при широкой публикации своей информации, в то время как коммерческую тайну держат в секрете. Очевидно, что по сравнению с патентом и авторским правом, коммерческая и производственная тайны являются наиболее удобными, надежными и гибкими формами защиты информации.

Помимо вышеизложенных форм правовой защиты и права принадлежности информации находит широкое распространение официальная передача права на пользование ею в виде лицензии. **Лицензия** - это разрешение, выдаваемое государством на проведение некоторых видов хозяйственной деятельности, включая внешнеторговые операции (ввоз и вывоз) и предоставление права использовать защищенные патентами изобретения, технологии, методики. Лицензионные разрешения предоставляются на определенное время и на определенные виды товаров.

Таблица 4.3. Определение и основные параметры коммерческой тайны

Коммерческая тайна - не являющиеся государственными секретами сведения, связанные с производством, технологией, управлением, финансами и другой деятельностью, разглашение, утечка и несанкционированный доступ к которой может нанести ущерб их владельцам

Определения	Содержание
СУБЪЕКТ	Предприятия, организации, коллективы, граждане
ОБЪЕКТ	Понятие применимо к широкому спектру интеллектуальной и промышленной собственности
ХАРАКТЕРИСТИКИ	1. Активный ресурс 2. Конфиденциальная информация 3. Особая форма собственности 4. Товар рыночной новизны
ЦЕННОСТЬ	Реально (потенциально) создает преимущества в конкурентной борьбе
ТРЕБОВАНИЯ	1. Потенциально полезная 2. Не общеизвестная.
СРОК ДЕЙСТВИЯ	Определяется жизненным циклом товара
ЗАЩИТА	1. Правовая 2. Организационная 3. Инженерно-техническая

К коммерческой тайне не относятся:

- охраняемые государством сведения;
- общеизвестные на законных основаниях сведения;
- общедоступные сведения, патенты, товарные знаки;
- сведения о негативной стороне деятельности;
- учредительные документы и сведения о хозяйственной деятельности.

На все эти формы защиты интеллектуальной собственности имеются соответствующие законы РФ - закон о патентах, закон об авторском праве, проект закона о коммерческой тайне, закон о товарных знаках и другие.

Создавая систему ИБ, необходимо четко понимать, что без правового обеспечения ЗИ любые последующие претензии с вашей стороны к недобросовестному сотруднику, клиенту, конкуренту и должностному лицу окажутся просто беспочвенными.

Если перечень сведений конфиденциального характера не доведен своевременно до каждого сотрудника (естественно, если он допущен по должностным обязанностям) в письменном виде, то сотрудник, укравший важную информацию в нарушение установленного порядка работы с ней, скорее всего, разведет руками: мол, откуда мне это знать! В этом случае никакие инстанции, вплоть до судебных, не помогут Вам.

Правовые нормы обеспечения безопасности и **ЗИ на конкретном предприятии** (фирме, организации) **отражаются в совокупности** учредительных, организационных и функциональных документов.

Требования обеспечения безопасности и ЗИ отражаются в **Уставе** (учредительном договоре) в виде следующих положений:

- предприятие имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, требовать от своих сотрудников обеспечения их сохранности и защиты от внутренних и внешних угроз;
- предприятие обязано обеспечить сохранность конфиденциальной информации.

Такие требования дают право администрации предприятия:

- создавать организационные структуры по защите конфиденциальной информации;
- издавать нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизмы их защиты;
- включать требования по ЗИ в договоры по всем видам хозяйственной деятельности;
- требовать защиты интересов предприятия со стороны государственных и судебных инстанций;
- распоряжаться информацией, являющейся собственностью предприятия, в целях извлечения выгоды и недопущения экономического ущерба коллективу предприятия и собственнику средств производства;
- разработать "Перечень сведений конфиденциальной информации". Требования правовой обеспеченности ЗИ предусматриваются в коллективном договоре. Коллективный договор должен содержать следующие требования:

Раздел "Предмет договора"

Администрация предприятия (в том числе и администрация самостоятельных подразделений) обязуется обеспечить разработку и осуществление мероприятий по определению и защите конфиденциальной информации.

Трудовой коллектив принимает на себя обязательства по соблюдению установленных на предприятии требований по защите конфиденциальной информации.

Администрация обязана учесть требования защиты конфиденциальной информации в правилах внутреннего распорядка.

Раздел "Кадры. Обеспечение дисциплины труда"

Администрация обязуется: нарушителей требований по защите коммерческой тайны привлекать к административной и уголовной ответственности в соответствии с действующим законодательством.

Правила внутреннего трудового распорядка для рабочих и служащих предприятия целесообразно дополнить следующими требованиями.

Раздел "Порядок приема и увольнения рабочих и служащих"

• При поступлении рабочего или служащего на работу или переводе его в установленном порядке на другую работу, связанную с конфиденциальной информацией предприятия, а также при увольнении администрация обязана проинструктировать работника или служащего по правилам сохранения коммерческой тайны с оформлением письменного обязательства о ее неразглашении.

• Администрация предприятия вправе принимать решение об отстранении от работ лиц, которые нарушают установленные требования по защите конфиденциальной информации.

Раздел "Основные обязанности рабочих и служащих"

Рабочие и служащие обязаны соблюдать требования нормативных документов по защите конфиденциальной информации предприятия.

Раздел "Основные обязанности администрации"

Администрация предприятия, руководители подразделений обязаны:

- обеспечить строгое сохранение конфиденциальной информации, постоянно осуществлять организаторскую и воспитательно-профилактическую работу, направленную на защиту секретов предприятия;
- включить в должностные инструкции и положения обязанности по сохранению конфиденциальной информации;
- неуклонно выполнять требования Устава, коллективного договора, трудовых договоров, правил внутреннего трудового распорядка и других организационных и хозяйственных документов в части обеспечения экономической и информационной безопасности.

Обязательства конкретного сотрудника, рабочего или служащего в части ЗИ обязательно должны быть оговорены в трудовом договоре (контракте). В соответствии с КЗоТ (гл. III) при заключении трудового договора трудящийся обязуется выполнять определенные требования, действующие на данном предприятии. Независимо от формы заключения договора (устного или письменного) подпись трудящегося на приказе о приеме на работу подтверждает его согласие с условиями договора (КЗоТ РФ ст. 18).

Требования по защите конфиденциальной информации могут быть оговорены в тексте договора, если договор заключается в письменной форме. Если же договор заключается в устной форме, то действуют требования по ЗИ, вытекающие из нормативно-правовых документов предприятия. При заключении трудового договора и оформлении приказа о приеме на работу нового сотрудника делается отметка об осведомленности его с порядком защиты информации предприятия. Это создает необходимый элемент включения данного лица в механизм обеспечения ИБ.

Использование договоров о неразглашении тайны - вовсе не самостоятельная мера по ее защите. Не следует думать, что после подписания такого соглашения с новым сотрудником тайна будет сохранена. Это только предупреждение сотруднику, что в дело вступает система мероприятий по ЗИ, и правовая основа к тому, чтобы пресечь его неверные или противоправные действия. Дальше задача - не допустить утраты коммерческих секретов.

Реализация правовых норм и актов, ориентированных на ЗИ на организационном уровне, опирается на те или иные организационно-правовые формы, к числу которых относятся соблюдение конфиденциальности работ и действий, договоры (соглашения) и различные формы обязательного права.

Конфиденциальность - это форма обращения со сведениями, составляющими коммерческую тайну, на основе организационных мероприятий, исключающих неправомерное овладение такими сведениями.

Договоры - это соглашения сторон (двух и более лиц) об установлении, изменении или прекращении взаимных обязательств.

Обязательство - гражданское правоотношение, в силу которого одна сторона (должник) обязана совершить в пользу другой стороны определенные действия (рис.4.6).

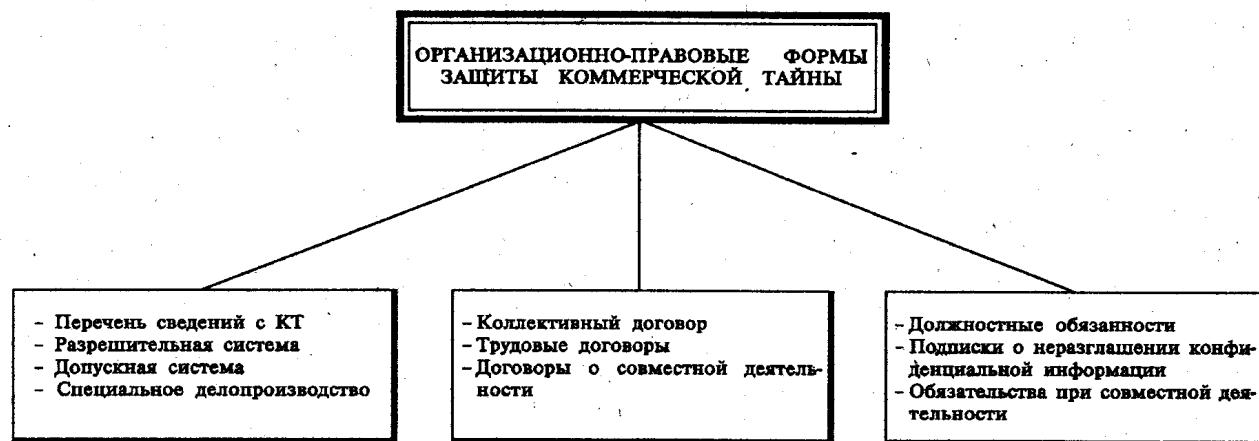


Рис.4.6. Организационно-правовые формы защиты коммерческой тайны

Правовое регулирование необходимо для совершенствования механизма предупреждения противоправных действий по отношению к информационным ресурсам, для уточнения и закрепления задач и правомочий отдельных субъектов в сфере предупредительной деятельности, охраны прав и законных интересов граждан и организаций.

Анализ законодательства, регулирующего деятельность субъектов в сфере ИБ, показывает наличие определенных недостатков. Существующие правовые нормы разбросаны по различным нормативным актам, издававшимся в разное время, в разных условиях и на разных уровнях. Действующее законодательство не систематизировано, что создает большие трудности в его использовании на практике.

Правовые меры обеспечения безопасности и ЗИ являются основой порядка деятельности и поведения сотрудников предприятия и определяют меры их ответственности за нарушение установленных норм.

4.2. Организационная защита

Организационная защита - это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз.

Организационная защита обеспечивает:

- организацию охраны, режима, работу с кадрами, с документами;
- использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз предпринимательской деятельности.

Организационные мероприятия играют существенную роль в создании надежного механизма ЗИ, так как возможности несанкционированного использования конфиденциальных сведений в значительной мере обуславливаются не техническими аспектами, а злоумышленными действиями, нерадивостью, небрежностью и халатностью пользователей или персонала защиты. Влияния этих аспектов практически невозможно избежать с помощью ТС. Для этого необходима совокупность организационно-правовых и организационно-технических мероприятий, которые исключали бы (или, по крайней мере, сводили бы к минимуму) возможность возникновения опасности конфиденциальной информации.

К основным организационным мероприятиям можно отнести:

- организацию режима и охраны. Их цель - исключение возможности тайного проникновения на территорию и в помещения посторонних лиц; обеспечение удобства контроля прохода и перемещения сотрудников и посетителей; создание отдельных производственных зон по типу конфиденциальных работ с самостоятельными системами доступа; контроль и соблюдение временного режима труда и пребывания на территории персонала фирмы; организация и поддержание надежного пропускного режима и контроля сотрудников и посетителей и др.;

- организацию работы с сотрудниками, которая предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил ЗИ и др.;

- организацию работы с документами и документированной информацией, включая организацию разработки и использования документов и носителей конфиденциальной информации, их учет, исполнение, возврат, хранение и уничтожение;

- организацию использования ТС средств сбора, обработки, накопления и хранения конфиденциальной информации;

- организацию работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению ее защиты;

- организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей (рис.4.7).

В каждом конкретном случае организационные мероприятия носят специфическую для данной организации форму и содержание, направленные на обеспечение ИБ в конкретных условиях.

Специфической областью организационных мер является организация защиты ПЭВМ, ИС и сетей. Организация защиты ПЭВМ, ИС и сетей определяет порядок и схему функционирования основных ее подсистем, использование устройств и ресурсов, взаимоотношения пользователей между собой в соответствии с нормативно-правовыми требованиями и правилами. ЗИ на основе организационных мер играет большую роль в обеспечении надежности и эффективности, так как несанкционированный доступ и утечка информации чаще всего обусловлены злоумышленными действиями, небрежностью пользователей или персонала. Эти факторы практически невозможно исключить или локализовать с помощью программно-аппаратных средств ЗИ (ПАЗИ), криптографии и физических средств защиты. Поэтому совокупность организационных, организационно-правовых и организационно-технических мероприятий, применяемых совместно с техническими методами, имеют цель исключить, уменьшить или полностью устранить потери при действии различных нарушающих факторов.

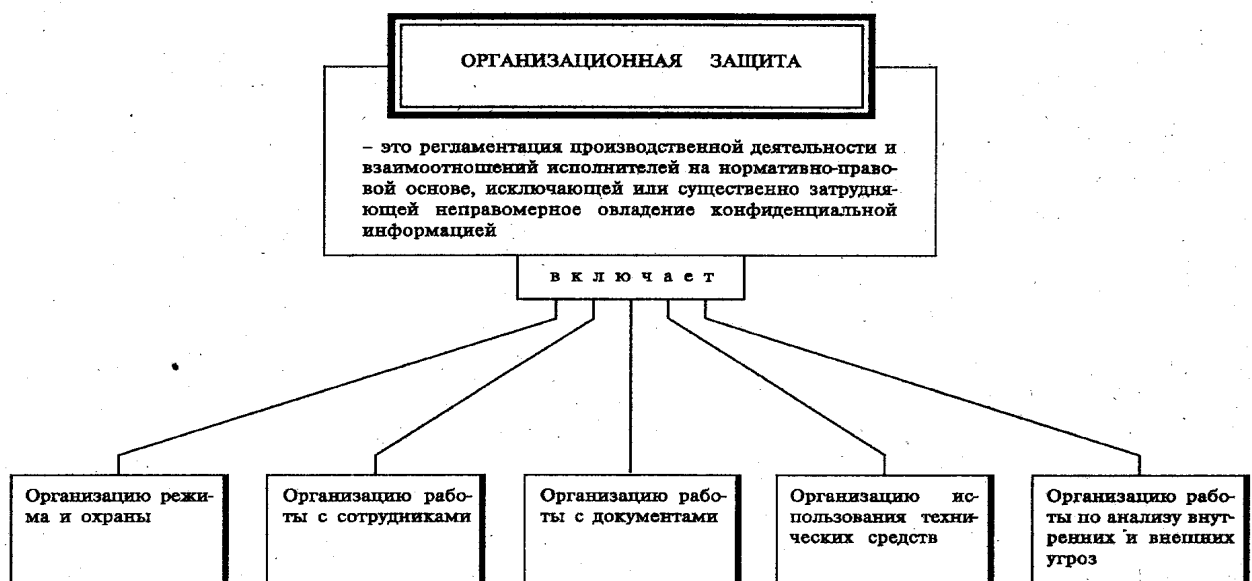


Рис.4.7. Организационная защита информации

Организационные средства защиты ПЭВМ и информационных сетей применяются:

- при проектировании, строительстве и оборудовании помещений, узлов сети и других объектов ИС, включающих влияние стихийных бедствий, возможность недозванного проникновения в помещения и др.;
- при подборе и подготовке персонала. В этом случае предусматриваются проверка принимаемых на работу, создание условий, при которых персонал был бы заинтересован в сохранности данных, обучение правилам работы с закрытой информацией, ознакомление с мерами ответственности за нарушение правил защиты и др.;
- при хранении и использовании документов и других носителей (маркировка, регистрация, определение правил выдачи и возвращения, ведение документации и др.);
- при соблюдении надежного пропускного режима к ТС, ПЭВМ и ИС при сменной работе (выделение ответственных за ЗИ в сменах, контроль за работой персонала, ведение (возможно и автоматизированное) журналов работы, уничтожение в установленном порядке закрытых производственных документов);
- при внесении изменений в программное обеспечение (строгое санкционирование, рассмотрение и утверждение проектов изменений, проверка их на удовлетворение требованиям защиты, документальное оформление изменений и др.);
- при подготовке и контроле работы пользователей.

Одним из важнейших организационных мероприятий является создание специальных штатных служб ЗИ в закрытых ИС (ЗИС) в виде администратора безопасности сети и администратора распределенных баз и банков данных, содержащих сведения конфиденциального характера.

Очевидно, что организационные мероприятия должны четко планироваться, направляться и осуществляться какой-то организационной структурой, каким-то специально созданным для этих целей структурным подразделением, укомплектованным соответствующими специалистами по безопасности предпринимательской деятельности и ЗИ.

Зачастую таким структурным подразделением является служба безопасности предприятия (фирмы, организации), на которую возлагаются следующие общие функции:

- организация и обеспечение охраны персонала, материальных и финансовых ценностей и защиты конфиденциальной информации;
- обеспечение пропускного и внутри объектового режима на территории, в зданиях и помещениях, контроль соблюдения требований режима сотрудниками, смежниками, партнерами и посетителями;
- руководство работами по правовому и организационному регулированию отношений по защите информации;
- участие в разработке основополагающих документов с целью закрепления в них требований обеспечения безопасности и защиты информации, а также положений о подразделениях, трудовых договоров, соглашений, подрядов, должностных инструкций и обязанностей руководства, специалистов, рабочих и служащих;
- разработка и осуществление совместно с другими подразделениями мероприятий по обеспечению работы с документами, содержащими конфиденциальные сведения; при всех видах работ организация и контроль выполнения требований «Инструкции по защите конфиденциальной информации»;
- изучение всех сторон производственной, коммерческой, финансовой и другой деятельности для выявления и последующего противодействия любым попыткам нанесения ущерба, ведения учета и анализа нарушений режима безопасности, накопление и анализ данных о злоумышленных устремлениях конкурентной и других организаций, о деятельности предприятия и его клиентов, партнеров, смежников;
- организация и проведение служебных расследований по фактам разглашения сведений, утрат документов, утечки конфиденциальной информации и других нарушений безопасности предприятия;
- разработка, ведение, обновление и пополнение «Перечня сведений конфиденциального характера» и других нормативных актов, регламентирующих порядок обеспечения безопасности и защиты информации;
- обеспечение строгого выполнения требований нормативных документов по защите производственных секретов предприятия;
- осуществление руководства службами и подразделениями безопасности подведомственных предприятий, организаций, учреждений и другими структурами в части оговоренных в договорах условий по защите конфиденциальной информации;
- организация и регулярное проведение учета сотрудников предприятия и службы безопасности по всем направлениям защиты информации и обеспечения безопасности производственной деятельности;
- ведение учета и строгого контроля выделенных для конфиденциальной работы помещений, технических средств в них, обладающих потенциальными каналами утечки информации и каналами проникновения к источникам охраняемых секретов;
- обеспечение проведения всех необходимых мероприятий по пресечению попыток нанесения морального и материального ущерба со стороны внутренних и внешних угроз;

- поддержание контактов с правоохранительными органами и службами безопасности соседних предприятий в интересах изучения криминогенной обстановки в районе (зоне) и оказания взаимной помощи в кризисных ситуациях.

Служба безопасности является самостоятельной организационной единицей предприятия, подчиняющейся непосредственно руководителю предприятия. Возглавляет службу безопасности начальник службы в должности заместителя руководителя предприятия по безопасности.

Организационно служба безопасности состоит из следующих структурных единиц:

- подразделения режима и охраны;
- специального подразделения обработки документов конфиденциального характера;
- инженерно-технических подразделений;
- информационно-аналитических подразделений.

В таком составе служба безопасности способна обеспечить защиту конфиденциальной информации от любых угроз.

К задачам службы безопасности предприятия относятся:

- определение круга лиц, которые в силу занимаемого служебного положения на предприятии прямо или косвенно имеют доступ к сведениям конфиденциального характера;
- определение участков сосредоточения конфиденциальных сведений;
- определение круга сторонних предприятий, связанных с данным предприятием кооперативными связями, на которых в силу производственных отношений возможен выход из-под контроля сведений конфиденциального характера;
- выявление круга лиц, не допущенных к конфиденциальной информации, но проявляющих повышенный интерес к таким сведениям;
- выявление круга предприятий, в том числе и иностранных, заинтересованных в овладении охраняемыми сведениями с целью нанесения экономического ущерба данному предприятию, устранения экономического конкурента либо его компрометации;
- разработка системы защиты документов, содержащих сведения конфиденциального характера;
- определение на предприятии участков, уязвимых в аварийном отношении, выход из строя которых может нанести материальный ущерб предприятию и сорвать поставки готовой продукции или комплектующих предприятиям, связанным с ним кооперацией;
- определение на предприятии технологического оборудования, выход (или вывод) которого из строя может привести к большим экономическим потерям;
- определение уязвимых мест в технологии производственного цикла, несанкционированное изменение в которой может привести к утрате качества выпускаемой продукции и нанести материальный или моральный ущерб предприятию (потеря конкурентоспособности);
- определение мест на предприятии, несанкционированное посещение которых может привести к изъятию (краже) готовой продукции или полуфабрикатов, заготовок и др. и организация их физической защиты и охраны;
- определение и обоснование мер правовой, организационной и инженерно-технической защиты предприятия, персонала, продукции и информации;
- разработка необходимых мероприятий, направленных на совершенствование системы экономической, социальной и информационной безопасности предприятия;
- внедрение в деятельность предприятия новейших достижений науки и техники, передового опыта в области обеспечения экономической и ИБ;
- организация обучения сотрудников службы безопасности в соответствии с их функциональными обязанностями;
- изучение, анализ и оценка состояния обеспечения экономической и ИБ предприятия и разработка предложений и рекомендаций для их совершенствования; разработка технико-экономических обоснований, направленных на приобретение технических средств, получение консультации у специалистов, разработку необходимой документации в целях совершенствования системы мер по обеспечению экономической и информационной безопасности.

Организационные меры являются решающим звеном формирования и реализации комплексной защиты информации и создания системы безопасности предприятия.

4.3. Инженерно-техническая защита

На вооружении промышленных шпионов, недобросовестных конкурентов и просто злоумышленников находятся самые разнообразные средства проникновения на объекты противоправных интересов и получения конфиденциальной информации. В этих условиях в интересах обеспечения ИБ необходимы адекватные по ориентации, функциональному назначению и другим характеристикам технические средства защиты охраняемых секретов.

1. Инженерно-техническая защита (ИТЗ) - это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации.

Многообразие целей, задач, объектов защиты и проводимых мероприятий предполагает рассмотрение некоторой системы классификации средств по виду, ориентации и другим характеристикам.

Например, средства ИТЗ можно рассматривать по объектам их воздействия. В этом плане они могут применяться для защиты людей, материальных средств, финансов, информации.

Примерная классификационная структура инженерно-технической защиты приведена на рис.4.8.



Рис.4.8. Классификационная структура ИТЗ

Многообразие классификационных характеристик позволяет рассматривать инженерно-технические средства по объектам воздействия, характеру мероприятий, способам реализации, масштабу охвата, классу средств злоумышленников, которым оказывается противодействие со стороны службы безопасности.

По функциональному назначению средства ИТЗ защиты делятся на следующие группы:

- **физические средства**, включающие различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям конфиденциальной информации (рис.4.9) и осуществляющие защиту персонала, материальных средств, финансов и информации от противоправных воздействий;



Рис.4.9. Классификация ИТЗ

- **аппаратные средства**. Сюда входят приборы, устройства, приспособления и другие технические решения, используемые в интересах ЗИ. В практике деятельности предприятия находит широкое применение самая различная аппаратура, начиная с телефонного аппарата до совершенных автоматизированных систем, обеспечивающих

производственную деятельность. Основная задача аппаратных средств - обеспечение стойкой ЗИ от разглашения, утечки и несанкционированного доступа через ТС обеспечения производственной деятельности;

- программные средства, охватывающие специальные программы, программные комплексы и системы ЗИ в ИС различного назначения и средствах обработки (сбора, накопления, хранения, обработки и передачи) данных;
- криптографические средства - это специальные математические и алгоритмические средства ЗИ, передаваемой по системам и сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования.

Аппаратные средства и методы защиты распространены достаточно широко. Однако из-за того, что они не обладают достаточной гибкостью, часто теряют свои защитные свойства при раскрытии их принципов действия и в дальнейшем не могут быть используемы.

Программные средства и методы защиты надежны и период их гарантированного использования без перепрограммирования значительно больше, чем аппаратных.

Криптографические методы занимают важное место и выступают надежным средством обеспечения защиты информации на длительные периоды.

Очевидно, что такое деление средств ЗИ достаточно условно, так как на практике очень часто они и взаимодействуют и реализуются в комплексе в виде программно-аппаратных модулей с широким использованием алгоритмов закрытия информации.

2. Физические средства защиты - это разнообразные устройства, приспособления, конструкции, аппараты, изделия, предназначенные для создания препятствий на пути движения злоумышленников.

К физическим средствам относятся механические, электромеханические, электронные, электронно-оптические, радио- и радиотехнические и другие устройства для воспрепятствования несанкционированного доступа (входа, выхода), проноса (выноса) средств и материалов и других возможных видов преступных действий (рис.4.10).

Эти средства применяются для решения следующих задач:

- 1) охрана территории предприятия и наблюдение за ней;
- 2) охрана зданий, внутренних помещений и контроль за ними;
- 3) охрана оборудования, продукции, финансов и информации;
- 4) осуществление контролируемого доступа в здания и помещения.

Все физические средства защиты объектов можно разделить на три категории:

- средства предупреждения,
- средства обнаружения и
- системы ликвидации угроз.



Рис.4.10. Физические средства защиты

Охранная сигнализация и охранное телевидение, например, относятся к средствам обнаружения угроз; заборы вокруг объектов - это средства предупреждения несанкционированного проникновения на территорию, а усиленные двери, стены, потолки, решетки на окнах и другие

меры служат защитой и от проникновения, и от других преступных действий (подслушивание, обстрел, бросание гранат и взрывпакетов и т.д.).

Средства пожаротушения относятся к системам ликвидации угроз. В общем плане по физической природе и функциональному назначению все средства этой категории можно разделить на следующие группы:

- охранные и охранно-пожарные системы;
- охранные телевидение;
- охранные освещение;
- средства физической защиты.

Охранные системы. Охранные системы и средства охранной сигнализации предназначены для обнаружения различных видов угроз: попыток проникновения на объект защиты. В охраняемые зоны и помещения, попыток проноса (выноса) оружия, средств промышленного шпионажа, краж материальных и финансовых ценностей и других действий; оповещения сотрудников охраны или персонала объекта о появлении угроз и необходимости усиления контроля доступа на объект, территорию, в здания и помещения.

Важнейшими элементами охранных систем являются датчики, обнаруживающие появление угрозы. Характеристики и принципы работы датчиков определяют основные параметры и практические возможности охранных систем.

Уже разработано и широко используется значительное количество самых разнообразных датчиков как по принципам обнаружения различных физических полей, так и по тактическому использованию.

Эффективность работы системы охраны и охранной сигнализации в основном определяется параметрами и принципом работы датчиков. На сегодня известны датчики следующих типов: механические выключатели, проволока с выключателем, магнитный выключатель, ртутный выключатель, коврики давления, металлическая фольга, проволоочная сетка, шифровольный датчик, ультразвуковой датчик, инфракрасный датчик, фотоэлектрический датчик, акустический датчик, вибрационный датчик, индуктивный датчик, емкостный датчик и другие.

Каждый тип датчика реализует определенный вид защиты: точечная защита, защита по линии, защита по площади или защита по объему. Механические датчики ориентированы на защиту линии, коврики давления - на точечное обнаружение, а инфракрасные находят широкое применение по площади и по объему.

Датчики посредством тех или иных каналов связи соединены с контрольно-приемным устройством пункта (или поста) охраны и средствами тревожного оповещения.

Каналами связи в системах охранной сигнализации могут быть специально проложенные проводные или кабельные линии, телефонные линии объекта, линии связи трансляции, системы освещения или радиоканалы. Выбор каналов определяется возможностями объекта.

Важным объектом охранной системы являются средства тревожного оповещения: звонки, лампочки, сирены, подающие постоянные или прерываемые сигналы о появлении угрозы.

По тактическому назначению охранные системы подразделяются на системы охраны:

- периметров объектов;
- помещений и проходов в служебных и складских зданиях;
- сейфов, оборудования, основных и вспомогательных технических средств;
- автотранспорта;
- персонала, в том числе и личного состава охраны, и другие.

К средствам физической защиты относятся:

- естественные и искусственные барьеры;
- особые конструкции периметров, проходов, оконных и дверных переплетов, помещений, сейфов, хранилищ;
- зоны безопасности.

Естественные и искусственные барьеры служат для противодействия незаконному проникновению на территорию объекта. Однако основная защитная нагрузка ложится все-таки на искусственные барьеры - такие, как заборы и другие виды ограждений. Практика показывает, что ограждения сложной конфигурации способны задер-

жать злоумышленника на достаточно большое время. На сегодня насчитывается значительный арсенал таких средств: от простых сетчатых до сложных комбинированных ограждений, оказывающих определенное отпугивающее воздействие на нарушителя.

Особые конструкции периметров, проходов, оконных переплетов, помещений, сейфов, хранилищ являются обязательными с точки зрения безопасности для любых организаций и предприятий. Эти конструкции должны противостоять любым способам физического воздействия со стороны криминальных элементов: механическим деформациям, разрушению сверлением, термическому и механическому резанию, взрыву; несанкционированному доступу путем подделки ключей, угадывания кода и т. д. Одним из главных технических средств защиты проходов, помещений, сейфов и хранилищ являются замки. Они бывают простыми (с ключами), кодовыми (в том числе и с временной задержкой на открывание) и с программными устройствами, открывающие двери и сейфы только в определенные часы.

Зоны безопасности. Важнейшим средством физической защиты является планировка объекта, его зданий и помещений по зонам безопасности, которые учитывают степень важности различных частей объекта с точки зрения нанесения ущерба от различного вида угроз. Оптимальное расположение зон безопасности и размещение в них эффективных технических средств обнаружения, отражения и ликвидации последствий противоправных действий составляет основу концепции инженерно-технической защиты объекта.

Зоны безопасности должны располагаться на объекте последовательно, от забора вокруг территории объекта до хранилищ ценностей, создавая цепь чередующихся друг за другом препятствий (рубежей), которые придется преодолевать злоумышленнику. Чем сложнее и надежнее препятствие на его пути, тем больше времени потребуются на преодоление каждой зоны и тем больше вероятность того, что расположенные в каждой зоне средства обнаружения (охранные посты, охранная сигнализация и охранное телевидение) выявят наличие нарушителя и подадут сигнал тревоги.

Основу планировки и оборудования зон безопасности объекта составляет принцип равнопрочности границ зон безопасности. Суммарная прочность зон безопасности будет оцениваться наименьшей из них.

Охранное телевидение. Одним из распространенных средств охраны является охранное телевидение. Привлекательной особенностью охранного телевидения является возможность не только отметить нарушение режима охраны объекта, но и контролировать обстановку вокруг него в динамике ее развития, определять опасность действий, вести скрытое наблюдение и производить видеозапись для последующего анализа правонарушения как с целью анализа, так и для привлечения к ответственности нарушителя.

Источниками изображения (датчиками) в системах охранного телевидения являются видеокамеры. Через объектив изображение злоумышленника попадает на светочувствительный элемент камеры, в котором оно преобразуется в электрический сигнал, поступающий затем по специальному коаксиальному кабелю на монитор и при необходимости - на видеомагнитофон.

Видеокамера является наиболее важным элементом системы охранного телевидения, так как от ее характеристик зависит эффективность и результативность всей системы контроля и наблюдения. В настоящее время разработаны и выпускаются самые разнообразные модели, различающиеся как по габаритам, так и по возможностям и по конструктивному исполнению.

Вторым по значимости элементом системы охранного телевидения является монитор. Он должен быть согласован по параметрам с видеокамерой. Часто используется один монитор с несколькими камерами, подключаемыми к нему поочередно средствами автоматического переключения по определенному регламенту.

В некоторых системах телевизионного наблюдения предусматривается возможность автоматического подключения камеры, в зоне обзора которой произошло нарушение. Используется и более сложное оборудование, включающее средства автоматизации, „ устройства одно-временного вывода нескольких изображений, детекторы движения для подачи сигнала тревоги при выявлении каких-либо изменений в изображении.

Охранное освещение является обязательной составной частью системы защиты любого объекта является охранное освещение. Различают два вида охранного освещения - дежурное и тревожное.

Дежурное освещение предназначается для постоянного использования в нерабочие часы, в вечернее и ночное время, как на территории объекта, так и внутри здания.

Тревожное освещение включается при поступлении сигнала тревоги от средства охранной сигнализации. Кроме того, по сигналу тревоги в дополнение к освещению могут включаться и звуковые приборы (звонки, сирены и пр.).

Сигнализация и дежурное освещение должны иметь резервное электропитание на случай аварии или выключения электросети.

В последние годы большое внимание уделяется созданию систем физической защиты, совмещенных с системами сигнализации.

Так, известна электронная система сигнализации для использования с проволочным ограждением. Система состоит из электронных датчиков и микропроцессора, управляющего блоком обработки данных. Ограждение длиной до 100 м может устанавливаться на открытой местности или размещаться на стенах, чердаках и имеющихся оградах. Устойчивые к воздействию окружающей среды датчики монтируются на стойках, кронштейнах. Проволочное ограждение состоит из 32 горизонтально натянутых стальных нитей, в средней части каждой из которых крепится электромеханический датчик, преобразующий изменение натяжения нитей в электрический сигнал.

Превышение пороговой величины напряжения, программируемое по амплитуде для каждого датчика отдельно, вызывает сигнал тревоги. Связь системы с центральным пунктом управления и контроля осуществляется с помощью мультимплексора. Микропроцессор автоматически через определенные интервалы времени проверяет работу компонентов аппаратуры и программных средств и - в случае установления отклонений - подает соответствующий сигнал.

Подобные и ряд других аналогичных систем физической защиты могут использоваться для защиты объектов по периметру в целях обнаружения вторжения на территорию объекта.

Используются системы из сетки двух волоконно-оптических кабелей, по которым передаются кодированные сигналы инфракрасного диапазона. Если в сетке нет повреждений, то сигналы поступают на приемное устройство без искажений. Попытки повреждения сетки приводят к обрывам или деформации кабелей, что вызывает сигнал тревоги. Оптические системы отличаются низким уровнем ложных тревог, вызванных воздействием на нее мелких животных, птиц, изменением погодных условий и высокой вероятностью обнаружения попыток вторжения.

Защита элементов зданий и помещений является следующим видом физической защиты. Хорошую физическую защиту оконных проемов помещений обеспечивают традиционные металлические решетки, а также специальное остекление на основе пластических масс, армированных стальной проволокой. Двери и окна охраняемого помещения оборудуются датчиками, срабатывающими при разрушении стекол, дверей, но не реагирующими на их колебания, вызванные другими причинами. Срабатывание датчиков вызывает сигнал тревоги.

Среди средств физической защиты особо следует отметить средства защиты ПЭВМ от хищения и проникновения к их внутренним компонентам.

Для этого используют металлические конструкции с клейкой подставкой, которая обеспечивает сцепление с поверхностью стола с силой в 2500-2700 кг/см. Это исключает изъятие или перемещение ПЭВМ без нарушения целостности поверхности стола. Перемещение ПЭВМ возможно только с использованием специальных ключей и инструментов.

Запирающие устройства и специальные шкафы занимают особое место в системах ограничения доступа, поскольку они несут в себе признаки, как систем физической защиты, так и устройств контроля доступа. Они отличаются большим разнообразием и предназначены для защиты документов, материалов, магнитных и фото носителей и даже ТС: ПЭВМ, калькуляторов, принтеров, ксероксов и других.

Выпускаются специальные металлические шкафы для хранения ПЭВМ и другой техники. Такие шкафы снабжаются надежной двойной системой запирания: замком ключевого типа и трех - пятизначным комбинированным замком. Фирмы утверждают, что такие шкафы обладают прочностью и надежностью, достаточными для защиты от промышленного шпионажа.

Выпускаются замки с программируемым временем открывания с помощью механических или электронных часов.

Системы контроля доступа осуществляет регулирование доступа в помещения или здания посредством опознавания службой охраны или ТС. Контролируемый доступ предполагает ограничение круга лиц, допускаемых в определенные защищаемые зоны, здания, помещения, и отслеживает передвижением этих лиц внутри них.

Основанием допуска служит определенный метод опознавания и сравнения с разрешительными параметрами системы. Имеется весьма широкий спектр методов опознавания уполномоченных лиц на право их доступа в помещения, здания, зоны.

На основе опознавания принимается решение о допуске лиц, имеющих на это право, или запрещение - для лиц не имеющих его. Наибольшее распространение получили атрибутивные и персональные методы опознавания.

К атрибутивным способам относятся средства подтверждения полномочий. Такие, в частности, как документы (паспорт, удостоверение), карты (фотокарточки, карты с магнитными, электрическими, механическими идентификаторами и т.д.) и иные средства (ключи, сигнальные элементы и т.д.). Заметим, что эти средства в значительной мере подвержены различного рода подделкам и мошенничеству.

Персональные методы - это методы определения лица по его независимым показателям: отпечаткам пальцев, геометрии рук, особенностям глаз. Персональные характеристики бывают *статические* и *динамические*.

К последним характеристикам относятся пульс, давление, кардиограммы, речь, почерк и другие.

Персональные способы наиболее привлекательные.

Во-первых, они полно описывают каждого отдельного человека.

Во-вторых, невозможно или крайне трудно подделать индивидуальные характеристики.

Статические способы включают анализ физических характеристик - таких, как отпечатки пальцев, особенности геометрии рук и другие. Они достаточно достоверны и обладают малой вероятностью ошибок.

Динамические же способы используют изменяющиеся во времени опознавательные характеристики.

Характеристики, зависящие от привычек и навыков, являются не только наиболее простыми для подделок, но и наиболее дешевыми с точки зрения практической реализации.

Способы опознавания, основанные на чем-либо запоминаемом (код, пароль), могут применяться в случаях наиболее низких требований к безопасности, так как часто эта информация записывается пользователями на различных бумажках, в записных книжках и других носителях, что при их доступности другим может свести на нет все усилия по безопасности. Кроме того, имеется реальная возможность подсмотреть, подслушать или получить эту информацию другим путем (насилие, кража и т.д.).

Способ опознавания человеком (вахтер, часовая) не всегда надежен из-за так называемого "человеческого фактора", заключающегося в том, что человек подвержен влиянию многих внешних условий (усталость, плохое самочувствие, эмоциональный стресс, подкуп). В противовес этому находят широкое применение технические средства опознавания, такие, например, как идентификационные карты, опознавание по голосу, почерку, пальцам и др.

Простейший и наиболее распространенный метод идентификации использует различные карты и карточки, на которых помещается кодированная или открытая информация о владельце, его полномочиях и другое.

Обычно это пластиковые карты типа пропусков или жетонов. Карты вводятся в читающее устройство каждый раз, когда требуется войти или выйти из охраняемого помещения или получить доступ к чему-нибудь (сейфу, камере, терминалу).

Существует много разновидностей устройств опознавания и идентификации личности, использующих подобные карты. Одни из них оптическим путем сличают фотографии и другие идентификационные элементы, другие - магнитные поля.

Системы опознавания по отпечаткам пальцев реализуют идентификации личности путем сравнения относительного положения окончаний и разветвлений линий отпечатка.

Поисковая система ищет на текущем изображении контрольные элементы, определенные при исследовании эталонного образца. Для идентификации одного человека считается достаточным определение координат 12 точек. Эти системы, естественно, весьма сложны и рекомендуются к использованию на объектах, требующих надежной защиты.

Системы опознавания по голосу обеспечивают выделения характерных признаков речи человека: анализ кратковременных сегментов, контрольный анализ, выделение статистических характеристик.

Следует отметить, что теоретически вопросы идентификации по голосу разработаны достаточно полно, но промышленное производство пока налажено слабо.

Системы опознавания по почерку считаются наиболее удобными для пользователя. Основным принципом идентификации по почерку является постоянство подписи каждого индивидуума, хотя абсолютного совпадения не бывает.

Система опознавания по геометрии рук анализирует при идентификации комбинации линий сгибов пальцев и ладони, линий складок, длины и толщины пальцев и других.

Технически это реализуется путем наложения руки на матрицу фото-ячеек. Рука освещается мощной лампой, производится регистрация сигналов с ячеек, несущих информацию о геометрии.

Все устройства идентификации человека могут работать как отдельно, так и в комплексе. Комплекс может быть узкоспециальным или многоцелевым, при котором система выполняет функции охраны, контроля, регистрации и сигнализации. Такие системы являются уже комплексными.

Комплексные системы обеспечивают:

- допуск на территорию предприятия по карточке (пропуску), содержащей индивидуальный машинный код;

- блокирование прохода при попытках несанкционированного прохода (проход без пропуска, проход в спецподразделения сотрудников, не имеющих допуска);
- возможность блокирования прохода для нарушителей графика работы (опоздание, преждевременный уход и т.д.);
- открытие зоны прохода для свободного выхода по команде вахтера;
- проверку кодов пропусков на задержание их предъявителей на КПП по указанию оператора системы;
- регистрацию времени пересечения проходной и сохранение его в базе данных персональной ЭВМ;
- обработку полученных данных и формирование различных документов (табель рабочего времени, суточный рапорт, ведомость нарушителей трудовой дисциплины и т. д.), что позволяет иметь оперативную информацию о нарушителях трудовой дисциплины, отработанном времени;
- оперативную корректировку информации базы данных с доступом по паролю;
- распечатку табелей рабочего времени по произвольной группе сотрудников (предприятие в целом, структурное подразделение, отдельно выбранные сотрудники);
- распечатку списков нарушителей графика рабочего времени с конкретными данными о нарушении;
- текущий и ретроспективный анализ посещения сотрудниками подразделений, передвижения сотрудников через КПП, выдачу списочного состава присутствовавших или отсутствовавших в подразделении или на предприятии для произвольно выбранного момента времени (при условии хранения баз данных за прошлые периоды);
- получение оперативной информации абонентами локальной сети в случае сетевой реализации системы.

Физические средства являются первой преградой для злоумышленника при реализации им заходных методов доступа.

3. Аппаратные средства защиты - это самые различные по принципу действия, устройству и возможностям технические конструкции, обеспечивающие пресечение разглашения, защиту от утечки и противодействие несанкционированному доступу к источникам конфиденциальной информации.

Аппаратные средства ЗИ применяются для решения следующих задач:

- проведение специальных исследований технических средств обеспечения производственной деятельности на наличие возможных каналов утечки информации;
- выявление каналов утечки информации на разных объектах и в помещениях;
- локализация каналов утечки информации;
- поиск и обнаружение средств промышленного шпионажа;
- противодействие несанкционированному доступу к источникам конфиденциальной информации и другим действиям.

По функциональному назначению аппаратные средства могут быть классифицированы на средства обнаружения, средства поиска и детальных измерений, средства активного и пассивного противодействия. При этом по своим техническим возможностям СЗИ могут быть

- приборы (комплексы) общего назначения, рассчитанные на использование непрофессионалами с целью получения предварительных (общих) оценок, и
- профессиональные комплексы, позволяющие проводить тщательный поиск, обнаружение и прецизионные измерения всех характеристик средств промышленного шпионажа.

В качестве *СЗИ общего назначения* можно рассмотреть группу индикаторов электромагнитных излучений типа ИП, обладающих широким спектром принимаемых сигналов и довольно низкой чувствительностью.

В качестве *профессиональных СЗИ* - комплекс для обнаружения и пеленгования радио-закладок, предназначенный для автоматического обнаружения и определения местонахождения радиопередатчиков, радио-микрофонов, телефонных закладок и сетевых радиопередатчиков. Это уже сложный современный поисково-обнаружительный профессиональный комплекс. Таким является, например, комплекс "Дельта", который обеспечивает:

- достоверное обнаружение практически любых из имеющихся в продаже радио-микрофонов, радиостетоскопов, сетевых и телефонных передатчиков, в том числе и с инверсией спектра;
- автоматическое определение места расположения микрофонов в объеме контролируемого помещения.

В состав комплекса входит радиоприемное устройство AR-3000 и ПЭВМ (рис.4.11).

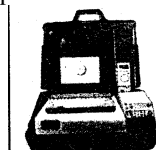


Рис.4.11. Разведывательно-поисковый комплекс «Дельта»

Поисковую аппаратуру можно подразделить на аппаратуру

- 1) поиска средств съема информации и

2) исследования каналов ее утечки.

Аппаратура первого типа направлена на поиск и локализацию уже внедренных злоумышленниками средств несанкционированного доступа.

Аппаратура второго типа предназначена для выявления каналов утечки информации. Примером такого комплекса может служить комплекс «Зарница», обеспечивающий измерение параметров побочных электромагнитных излучений в диапазоне частот от 10 КГц до 1 ГГц. Обработка результатов измерений осуществляется на ПЭВМ в соответствии с действующими нормативно-методическими Документами Гостехкомиссии при Президенте РФ (рис.4.12).

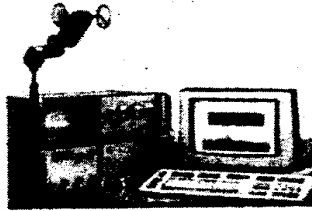


Рис.4.12. Комплекс обнаружения и измерения «Зарница»

Определяющими для такого рода систем являются оперативность исследования и надежность полученных результатов.

Использование профессиональной поисковой аппаратуры требует высокой квалификации оператора. Как в любой области техники, универсальность той или иной аппаратуры приводит к снижению ее параметров по каждой отдельной характеристике.

С другой стороны, существует огромное количество различных по физической природе каналов утечки информации, а также физических принципов, на основе которых работают системы несанкционированного доступа. Эти факторы обуславливают многообразие поисковой аппаратуры, а ее сложность определяет высокую стоимость каждого прибора. В связи с этим достаточный комплекс поискового оборудования могут позволить себе иметь структуры, постоянно проводящие соответствующие обследования. Это либо крупные службы безопасности, либо специализированные фирмы, оказывающие услуги сторонним организациям.

Конечно, описанное выше не является аргументом для отказа от использования средств поиска самостоятельно. Но эти средства в большинстве случаев достаточно просты и позволяют проводить профилактические мероприятия в промежутке между серьезными поисковыми обследованиями.

В особую группу выделяются **аппаратные средства защиты ЭВМ и коммуникационных систем** на их базе.

Аппаратные средства защиты применяются как в отдельных ПЭВМ, так и на различных уровнях и участках сети: в центральных процессорах ЭВМ, в их оперативных ЗУ (ОЗУ), контроллерах ввода-вывода, внешних ЗУ, терминалах и т.д.

Для защиты центральных процессоров (ЦП) применяется кодовое резервирование - создание дополнительных битов в форматах машинных команд (разрядов секретности) и резервных регистров (в устройствах ЦП). Одновременно предусматриваются два возможных режима работы процессора, которые отделяют вспомогательные операции от операций непосредственного решения задач пользователя. Для этого служит специальная система прерывания, реализуемая аппаратными средствами.

Одной из мер аппаратной защиты ЭВМ и информационных сетей является ограничение доступа к оперативной памяти с помощью установления границ или полей. Для этого создаются регистры контроля и регистры защиты данных. Применяются также дополнительные биты четности - разновидность метода кодового резервирования.

Для обозначения степени конфиденциальности программ и данных, категорий пользователей используются биты, называемые битами конфиденциальности (это два-три дополнительных разряда, с помощью которых кодируются категории секретности пользователей, программ и данных).

Программы и данные, загружаемые в ОЗУ, нуждаются в защите, гарантирующей их от несанкционированного доступа. Часто используются биты четности, ключи, постоянная специальная память. При считывании из ОЗУ необходимо, чтобы программы не могли быть уничтожены несанкционированными действиями пользователей или вследствие выхода аппаратуры из строя. Отказы должны своевременно выявляться и устраняться, чтобы предотвратить исполнение искаженной команды ЦП и потери информации.

Для предотвращения считывания оставшихся после обработки данных в ОЗУ применяется специальная схема стирания. В этом случае формируется команда на стирание ОЗУ и указывается адрес блока памяти, который должен быть освобожден от информации. Эта схема записывает нули или какую-нибудь другую последовательность символов во все ячейки данного блока памяти, обеспечивая надежное стирание ранее загруженных данных.

Аппаратные средства защиты применяются и в терминалах пользователей. Для предотвращения утечки информации при подключении незарегистрированного терминала необходимо перед выдачей запрашиваемых данных осуществить идентификацию (автоматическое опреде-

ление кода или номера) терминала, с которого поступил запрос. В многопользовательском режиме этого терминала идентификации его недостаточно. Необходимо осуществить аутентификацию пользователя, то есть установить его подлинность и полномочия. Это необходимо и потому, что разные пользователи, зарегистрированные в системе, могут иметь доступ только к отдельным файлам и строго ограниченные полномочия их использования.

Для идентификации терминала чаще всего применяется генератор кода, включенный в аппаратуру терминала, а для аутентификации пользователя - такие аппаратные средства, как ключи, персональные кодовые карты, персональный идентификатор, устройства распознавания голоса пользователя или формы его пальцев. Но наиболее распространенными средствами аутентификации являются пароли, проверяемые не аппаратными, а программными средствами опознавания.

Аппаратные средства защиты информации - это различные технические устройства, системы и сооружения, предназначенные для защиты информации от разглашения, утечки и несанкционированного доступа.

4. Программные средства защиты

Системы защиты компьютера от чужого вторжения весьма разнообразны и классифицируются, как:

- средства собственной защиты, предусмотренные общим программным обеспечением;
- средства защиты в составе вычислительной системы;
- средства защиты с запросом информации;
- средства пассивной защиты и другие.

Более подробно эти группы защиты представлены на рис.4.12.

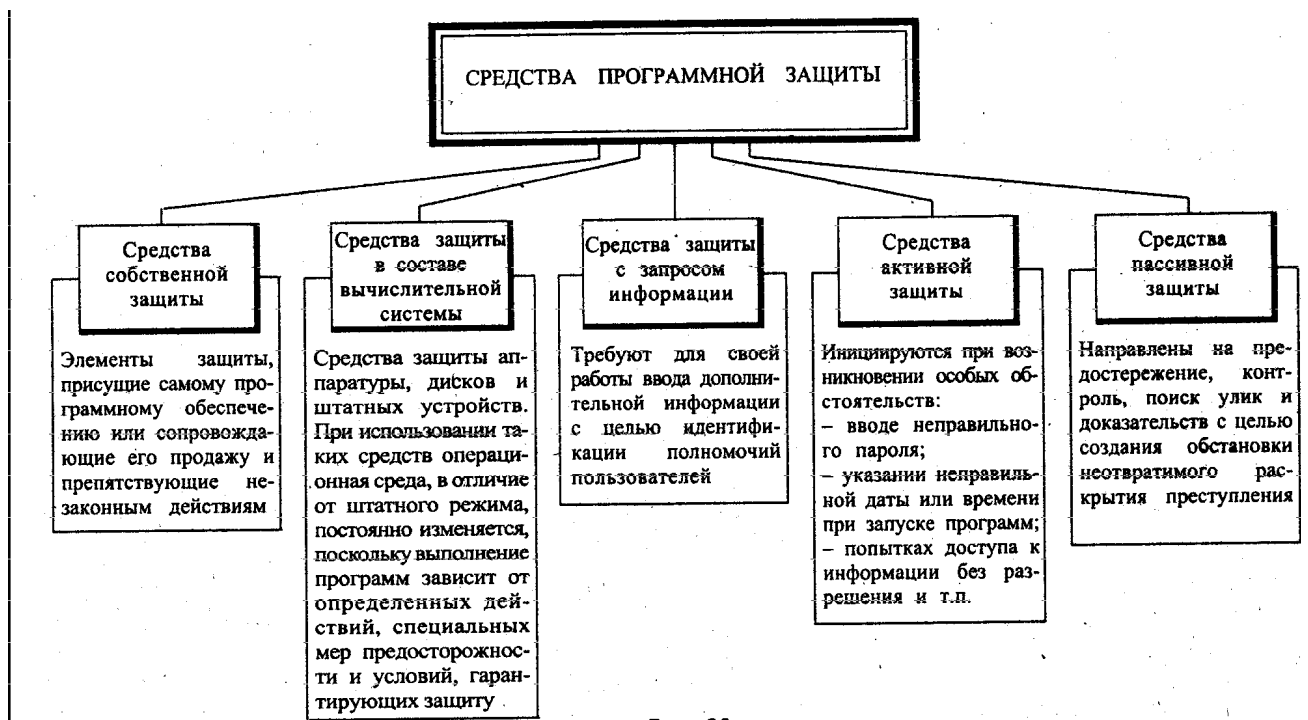


Рис.4.12. Средства программной защиты

Основные направления использования программной ЗИ.

- защита информации от несанкционированного доступа;
- защита информации от копирования;
- защита программ от копирования;
- защита программ от вирусов;
- защита информации от вирусов;
- программная защита каналов связи.

По каждому из указанных направлений имеется, достаточное количество качественных, разработанных профессиональными организациями и распространяемых на рынках программных продуктов (рис.4.13).

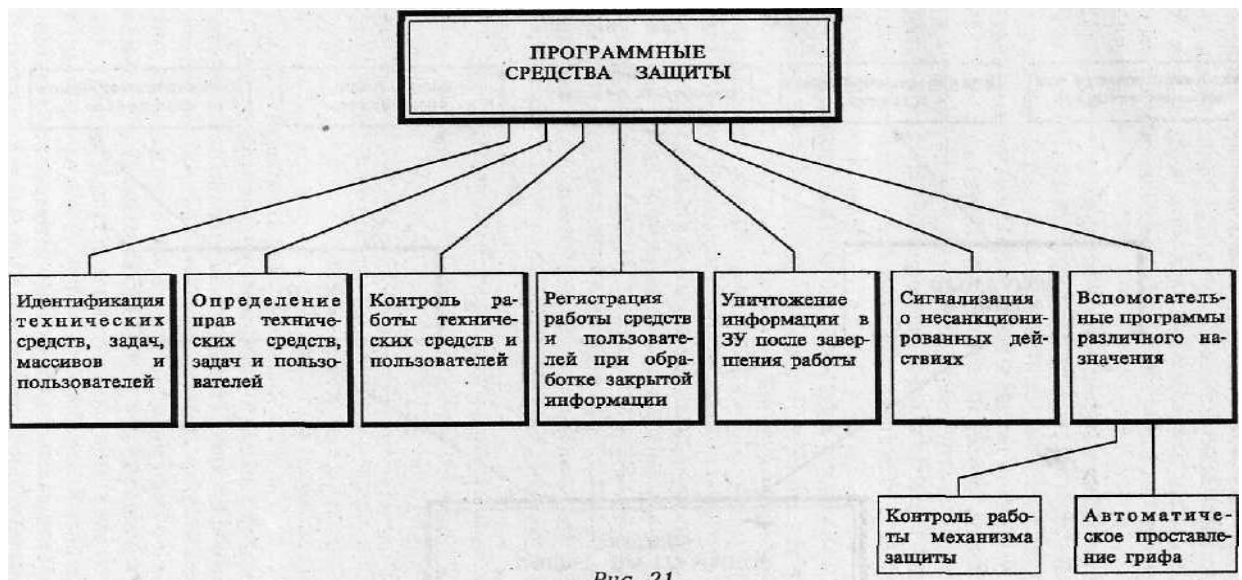


Рис. 21

Рис.4.13. Программные защитные средства

Программные средства защиты имеют следующие разновидности специальных программ:

- идентификации технических средств, файлов и аутентификации пользователей;
- регистрации и контроля работы технических средств и пользователей;
- обслуживания режимов обработки информации ограниченного пользования;
- защиты операционных средств ЭВМ и прикладных программ пользователей;
- уничтожения информации в защитные устройства после использования;
- сигнализирующих нарушения использования ресурсов;
- вспомогательных программ защиты различного назначения (рис.2.14).

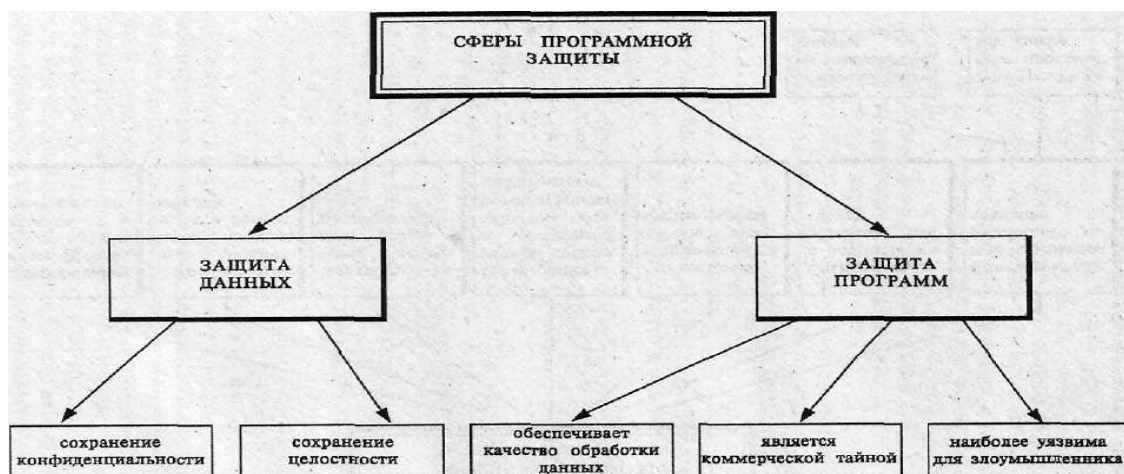


Рис.4.14. Сферы программной защиты

Идентификация ТС и файлов, осуществляемая программно, делается на основе анализа регистрационных номеров различных компонентов и объектов информационной системы и сопоставления их со значениями адресов и паролей, хранящихся в защитном устройстве системы управления.

Для обеспечения надежности защиты с помощью паролей работа системы защиты организуется таким образом, чтобы вероятность раскрытия секретного пароля и установления соответствия тому или иному идентификатору файла или терминала была как можно меньше. Для этого надо периодически менять пароль, а число символов в нем установить достаточно большим.

Эффективным способом идентификации адресуемых элементов и аутентификации пользователей является алгоритм запросно-ответного типа, в соответствии с которым система защиты выдает пользователю запрос на пароль, после чего он должен дать на него определенный

ответ. Так как моменты ввода запроса и ответа на него непредсказуемы, это затрудняет процесс отгадывания пароля, обеспечивая тем самым более высокую надежность защиты.

Получение разрешения на доступ к тем или иным ресурсам можно осуществить не только на основе использования секретного пароля и последующих процедур аутентификации и идентификации. Это можно сделать более детальным способом, учитывающим различные особенности режимов работы пользователей, их полномочия, категории запрашиваемых данных и ресурсов. Этот способ реализуется специальными программами, анализирующими соответствующие характеристики пользователей, содержание заданий, параметры технических и программных средств, устройств памяти.

Поступающие в систему защиты конкретные данные, относящиеся к запросу, сравниваются в процессе работы программ защиты с данными, занесенными в регистрационные секретные таблицы (матрицы). Эти таблицы, а также программы их формирования и обработки хранятся в зашифрованном виде и находятся под особым контролем администратора (администраторов) безопасности информационной сети.

Для разграничения обращения отдельных пользователей к вполне определенной категории информации применяются индивидуальные меры секретности этих файлов и особый контроль доступа к ним пользователей.

Гриф секретности может формироваться в виде трехразрядных кодовых слов, которые хранятся в самом файле или в специальной таблице. В этой же таблице записываются идентификатор пользователя, создавшего данный файл, идентификаторы терминалов, с которых может быть осуществлен доступ к файлу, идентификаторы пользователей, которым разрешен доступ к данному файлу, а также их права на пользование файлом (считывание, редактирование, стирание, обновление, исполнение и т.д.). Важно не допустить взаимовлияния пользователей в процессе обращения к файлам. Если, например, одну и ту же запись имеют право редактировать несколько пользователей, то каждому из них необходимо сохранить именно его вариант редакции (делается несколько копий записей с целью возможного анализа и установления полномочий).

ЗИ от несанкционированного доступа обеспечивает защиту от чужого вторжения. Ее основные функции, осуществляемые программными средствами, это:

- идентификация субъектов и объектов;
- разграничение (иногда и полная изоляция) доступа к вычислительным ресурсам и информации;
- контроль и регистрация действий с информацией и программами.

Процедура Идентификации и подтверждения подлинности предполагает проверку, является ли субъект, осуществляющий доступ (или объект, к которому осуществляется доступ), тем, за кого себя выдает. Подобные проверки могут быть одноразовыми или периодическими (особенно в случаях продолжительных сеансов работы).

В процедурах идентификации используются различные методы:

- простые, сложные или одноразовые пароли;
- обмен вопросами и ответами с администратором;
- ключи, магнитные карты, значки, жетоны;
- средства анализа индивидуальных характеристик (голоса, отпечатков пальцев, геометрических параметров рук, лица);
- специальные идентификаторы или контрольные суммы для аппаратуры, программ, данных.

Наиболее распространенным методом идентификации является парольная идентификация.

Практика показала, что парольная защита данных является слабым звеном, так как пароль можно подслушать или подсмотреть, пароль можно перехватить, а то и просто разгадать.

Для защиты самого пароля выработаны определенные рекомендации, как сделать пароль надежным:

- пароль должен содержать, по крайней мере, восемь символов. Чем меньше символов содержит пароль, тем легче его разгадать;
- не используйте в качестве пароля очевидный набор символов, например ваше имя, дату рождения, имена близких или наименования ваших программ. Лучше всего использовать для этих целей неизвестную формулу или цитату;
- если криптографическая программа позволяет, введите в пароль, по крайней мере один пробел, небуквенный символ или прописную букву;
- не называйте никому ваш пароль, не записывайте его. Если вам пришлось нарушить эти правила, спрячьте листок в запираемый ящик;
- чаще меняйте пароль;
- не вводите пароль в процедуру установления диалога или макрокоманду.

Помните, что набранный на клавиатуре пароль часто сохраняется в последовательности команд автоматического входа в систему.

Для идентификации программ и данных часто прибегают к подсчету контрольных сумм,

однако, как и в случае парольной идентификации, важно исключить возможность подделки при сохранении правильной контрольной суммы. Это достигается путем использования сложных методов контрольного суммирования на основе криптографических алгоритмов. Обеспечить защиту данных от подделки (имитостойкость) можно, применяя различные методы шифрования и методы цифровой подписи на основе криптографических систем с открытым ключом.

После выполнения процедур идентификации и установления подлинности пользователь получает доступ к вычислительной системе, и ЗИ осуществляется на трех уровнях:

- аппаратуры;
- программного обеспечения;
- данных.

Защита на уровне аппаратуры и программного обеспечения предусматривает управление доступом к вычислительным ресурсам: отдельным устройствам, оперативной памяти, операционной системе, специальным служебным или личным программам пользователя.

ЗИ на уровне данных направлена:

- на ЗИ при обращении к ней в процессе работы на ПЭВМ и выполнении только разрешенных операций над ними;
 - на ЗИ при ее передаче по каналам связи между различными ЭВМ.
- Управление доступом к информации позволяет ответить на вопросы:
- кто может выполнять и какие операции;
 - над какими данными разрешается выполнять операции.

Объектом, доступ к которому контролируется, может быть файл, запись в файле или отдельное поле записи файла, а в качестве факторов, определяющих порядок доступа, - определенное событие, значения данных, состояние системы, полномочия пользователя, предыстория обращения и другие данные.

Доступ, управляемый событием, предусматривает блокировку обращения пользователя. Например, в определенные интервалы времени или при обращении с определенного терминала. Доступ, зависящий от состояния, осуществляется в зависимости от текущего состояния вычислительной системы, управляющих программ и системы защиты.

Что касается доступа, зависящего от полномочий, то он предусматривает обращение пользователя к программам, данным, оборудованию в зависимости от предоставленного режима. Такими режимами могут быть "только читать", "читать и писать", "только выполнять" и другие.

В основе большинства средств контроля доступа лежит то или иное представление матрицы доступа.

Другой подход к построению средств защиты доступа основан на контроле информационных потоков и разделении субъектов и объектов доступа на классы конфиденциальности.

Средства регистрации, как и средства контроля доступа, относятся к эффективным мерам защиты от несанкционированных действий. Однако, если средства контроля доступа предназначены для предотвращения таких действий, то задача регистрации - обнаружить уже совершенные действия или их попытки.

Комплекс программно-технических средств и организованных (процедурных) решений по ЗИ от НСД реализуется следующими действиями:

- управлением доступом;
- регистрацией и учетом;
- применением криптографических средств;
- обеспечением целостности информации.

Можно отметить следующие формы контроля и разграничения доступа, нашедшие широкое применение на практике:

1. Предотвращение доступа:
 - к жесткому диску;
 - к отдельным разделам;
 - к отдельным файлам;
 - к каталогам;
 - к гибким дискам;
 - к сменным носителям информации.
2. Установка привилегий доступа к группе файлов,
3. Защита от модификации:
 - файлов;
 - каталогов.

4. Защита от уничтожения:

- файлов;
- каталогов.

5. Предотвращение копирования:

- файлов;
- каталогов;
- прикладных программ.

6. Затемнение экрана по истечении времени, установленного пользователем.

В обобщенном виде средства защиты данных приведены на рис.2.15.

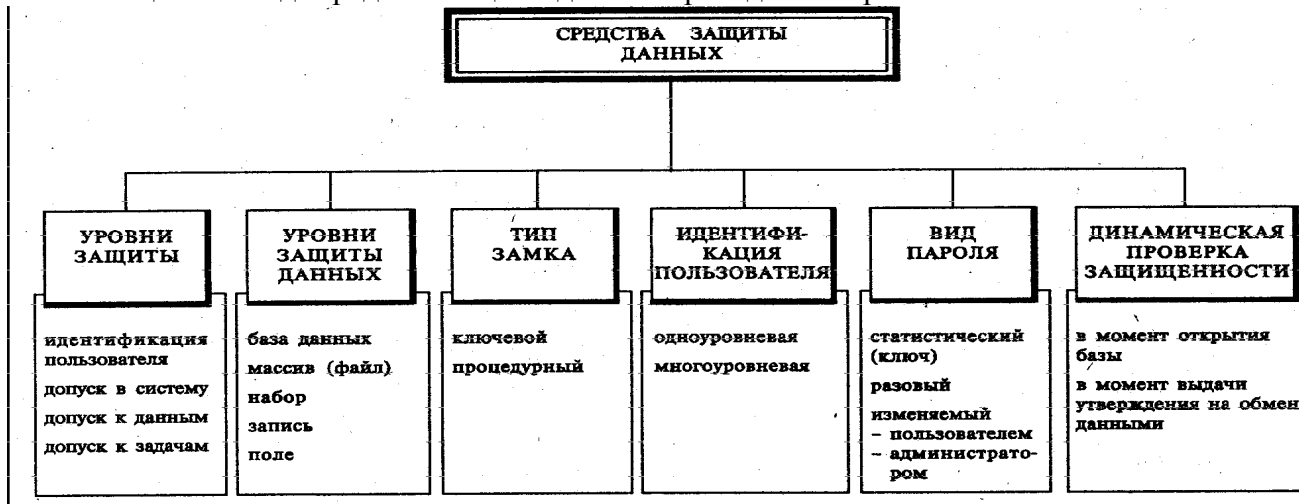


Рис.2.15. Классификация средств защиты данных

Защита от копирования. Средства защиты от копирования предотвращают использование ворованных копий программного обеспечения и являются в настоящее время единственно надежным средством - как защищающим авторское право программистов-разработчиков, так и стимулирующим развитие рынка. Под средствами защиты от копирования понимаются средства, обеспечивающие выполнение программой своих функций только при опознании некоторого уникального не копируемого элемента. Таким элементом (называемым ключевым) может быть дискета, определенная часть компьютера или специальное устройство, подключаемое к ПЭВМ. Защита от копирования реализуется выполнением ряда функций, являющихся общими для всех систем защиты:

- идентификация среды, из которой будет запускаться программа;
- аутентификация среды, из которой запущена программа;
- реакция на запуск из несанкционированной среды;
- регистрация санкционированного копирования;
- противодействие изучению алгоритмов работы системы.

Под средой, из которой будет запускаться программа, подразумевается либо дискета, либо ПЭВМ (если установка происходит на НЖМД). Идентификация среды заключается в том, чтобы некоторым образом поименовать среду с целью дальнейшей ее аутентификации. Идентифицировать среду - значит закрепить за ней некоторые специально созданные или измеренные редко повторяющиеся и трудно подделываемые характеристики - идентификаторы.

Идентификация дискет может быть проведена двумя способами.

Первый основан на нанесении повреждений на некоторую часть поверхности дискеты. Распространенный способ такой идентификации - "черная дыра". При таком способе дискета прожигается в некотором месте лазерным лучом. Очевидно, что сделать точно такую же дырку в дискете-копии и в том же самом месте, как и на дискете-оригинале, достаточно сложно.

Второй способ идентификации основан на нестандартном форматировании дискеты.

Реакция на запуск из несанкционированной среды обычно сводится к выдаче соответствующего сообщения.

ЗИ от разрушения при использовании ПЭВМ предназначена для ЗИ от разрушения, которое может произойти при подготовке и осуществлении различных восстановительных меро-

приятый (резервировании, создании и обновлении страховочного фонда, ведении архивов информации и других).

Так как причины разрушения информации весьма разнообразны (несанкционированные действия, ошибки программ и оборудования, компьютерные вирусы и пр.), то проведение страховочных мероприятий обязательно для всех, кто пользуется персональными ЭВМ.

Необходимо специально отметить опасность компьютерных вирусов. Многие пользователи ЭВМ (ПЭВМ), о них хорошо знают, а тот, кто с ними еще не знаком, скоро познакомится. Вирус компьютерный - небольшая, достаточно сложная, тщательно составленная и опасная программа, которая может самостоятельно размножаться, переносить себя на диски, прикрепляться к чужим программам и передаваться по информационным сетям.

Вирус обычно создается для нарушения работы компьютера различными способами - от "безобидной" выдачи какого-либо сообщения до стирания, разрушения файлов. Основную массу вирусов создают люди, хулиганствующие программисты, в основном, чтобы потешить свое самолюбие или заработать деньги на продаже антивирусов.

Антивирус - программа, обнаруживающая или обнаруживающая и удаляющая вирусы.

Такие программы бывают специализированными и универсальными. Чем отличается универсальный антивирус от специализированного?

Специализированный антивирус способен бороться только с уже написанными, работающими вирусами, а универсальный антивирус - и с еще не написанными.

К специализированным относится большинство антивирусных программ: AIDSTEST, VDEATH, SERUM-3, ANTI-KOT, SCAN и сотни других. Каждая из них распознает один или несколько конкретных вирусов, никак не реагируя на присутствие остальных.

Универсальные антивирусы предназначены для борьбы с целыми классами вирусов. По назначению антивирусы универсального действия бывают довольно различны. Широкое применение находят резидентные антивирусы и программы-ревизоры.

И те и другие антивирусные программы обладают определенными возможностями, положительными и отрицательными (недостатки) характеристиками. Специализированные при своей простоте слишком узко специализированы. При значительном разнообразии вирусов требуется такое же многообразие антивирусов.

Помимо использования в интересах защиты от вирусов антивирусных программ широко используют и организационные меры безопасности. Для уменьшения опасности вирусных актов возможно предпринять определенные действия, которые для каждого конкретного случая могут быть сокращены или расширены. Вот некоторые из таких действий:

1. Информировать всех сотрудников предприятия об опасности и возможном ущербе от вирусных атак.
2. Не осуществлять официальные связи с другими предприятиями по обмену (получению) программным обеспечением. Запретить сотрудникам приносить программы "со стороны" для установки их в системы обработки информации. Должны использоваться только официально распространяемые программы.
3. Запретить сотрудникам использовать компьютерные игры на ПЭВМ, обрабатывающих конфиденциальную информацию.
4. Для выхода на сторонние информационные сети выделить отдельное специальное место.
5. Создать архив копий программ и данных.
6. Периодически проводить проверку контрольным суммированием или сравнением с "чистыми" программами.
7. Установить системы защиты информации на особо важных ПЭВМ. Применять антивирусные средства.

Программная защита информации - это система специальных программ, включаемых в состав программного обеспечения, реализующих функции защиты информации.

5. Криптографические средства защиты. Криптография как средство защиты (закрытия) информации приобретает все более важное значение в мире коммерческой деятельности.

Криптография имеет достаточно давнюю историю. Вначале она применялась главным образом в области военной и дипломатической связи. Теперь она необходима в производственной и коммерческой деятельности. Если учесть, что сегодня по каналам шифрованной связи только у нас в стране передаются сотни миллионов сообщений, телефонных переговоров, огромные объемы компьютерных и телеметрических данных, и все это, что называется, не для чужих глаз и ушей, становится ясным: сохранение тайны этой переписки крайне необходимо.

Что же такое криптография? Она включает в себя несколько разделов современной математики, а также специальные отрасли физики, радиоэлектроники, связи и некоторых других смежных отраслей. Ее задачей является преобразование математическими методами передаваемого по каналам связи секретного сообщения, телефонного разговора или компьютерных данных таким образом, что они становятся совершенно непонятными для посторонних лиц. То есть криптография должна обеспечить такую защиту секретной (или любой другой) информации, что даже в случае ее перехвата посторонними лицами и обработки любыми способами с использованием самых быстродействующих ЭВМ и последних достижений науки и техники, она не должна быть дешифрована в течение

нескольких десятков лет. Для такого преобразования информации используются различные шифровальные средства - такие, как средства шифрования документов, в том числе и портативного исполнения, средства шифрования речи (телефонных и радиопереговоров), средства шифрования телеграфных сообщений и передачи данных.

Общая технология шифрования. Исходная информация, которая передается по каналам связи, может представлять собой речь, данные, видеосигналы, называется незашифрованными сообщениями P (рис.4.14).

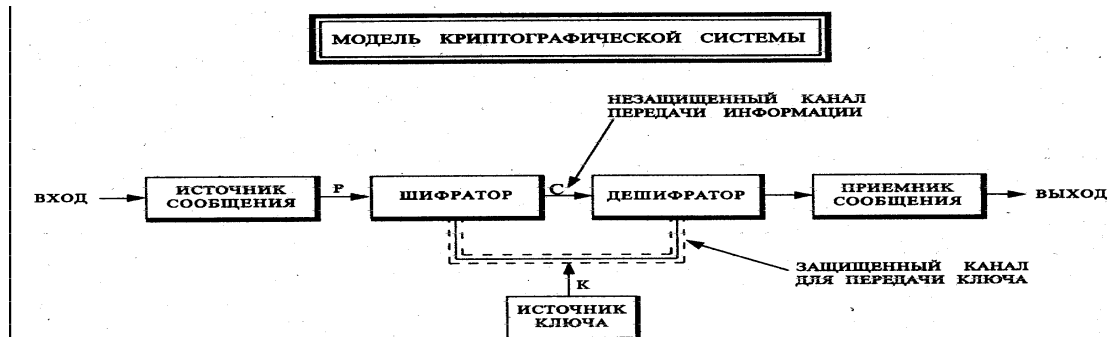


Рис.4.14. Модель криптографической системы

В устройстве шифрования сообщение P шифруется (преобразуется в сообщение C) и передается по "незакрытому" каналу связи. На приемной стороне сообщение C дешифруется для восстановления исходного значения сообщения P .

Параметр, который может быть применен для извлечения отдельной информации, называется ключом.

В современной криптографии рассматриваются два типа криптографических алгоритмов (ключей):

- классические криптографические алгоритмы, основанные на использовании секретных ключей, и
- новые криптографические алгоритмы с открытым ключом, основанные на использовании ключей двух типов: секретного (закрытого) и открытого.

В криптографии с открытым ключом имеются, по крайней мере, два ключа, один из которых невозможно вычислить из другого. Если ключ расшифрования вычислительными методами невозможно получить из ключа зашифрования, то секретность информации, зашифрованной с помощью несекретного (открытого) ключа, будет обеспечена. Однако этот ключ должен быть защищен от подмены или модификации. Ключ расшифрования также должен быть секретным и защищен от подмены или модификации.

Если, наоборот, вычислительными методами невозможно получить ключ зашифрования из ключа расшифрования, то ключ расшифрования может быть не секретным.

Разделение функций зашифрования и расшифрования посредством разделения на две части дополнительной информации, требуемой для выполнения операций, является той ценной идеей, которая лежит в основе криптографии с открытым ключом.

Технология шифрования речи. Наиболее распространенным способом шифрования аналогового речевого сигнала является разделение его на части.

В этом случае входной речевой сигнал поступает в полосовые фильтры для выделения полос шифруемого спектра. Выходной сигнал каждого фильтра в процессе шифрования подвергается либо перестановке по частоте, либо перевороту спектра (инверсия), либо и тому и другому одновременно. Затем синтезируется полный шифровальный выходной сигнал.

По этому принципу работает система AVPS (Analog Voice Privided System) - речевой шифратор (скремблер), который осуществляет перестановку отдельных «вырезок» входного сигнала с помощью полосового фильтра - анализатора. Система имеет 12 ключей шифрования, обусловленных возможными перестановками, что обеспечивает надежность используемого метода.

Система AVPS используется в реальном времени с любыми унифицированными телефонами. Качество шифрования речи высокое, сохраняется узнаваемость абонента.

Находят очень широкое распространение цифровые системы шифрования речевых сигналов. Эти системы обеспечивают высокую надежность шифрования.

В системах шифрования данных используются в основном две элементарные системы:

1. Перестановка (биты или подблоки внутри каждого блока входных данных переставляются).
2. Замещение (биты или подблоки внутри каждого блока входных данных заменяются).

Разработано большое число алгоритмов шифрования. К числу наиболее эффективных относится алгоритм DES (Data Encryption Standart) - стандарт шифрования данных. Американское

национальное бюро по стандартизации NBS узаконило алгоритм DES в качестве стандарта для систем связи. Механизм шифрования в этом алгоритме основывается на использовании ключа длиной 56 бит.

Для защиты промышленной и коммерческой информации на международном и отечественном рынке предлагаются различные технические устройства и комплекты профессиональной аппаратуры шифрования и криптозащиты телефонных и радиопереговоров, деловой переписки и пр.

Широкое распространение получили скремблеры и маскираторы, заменяющие речевой сигнал цифровой передачей данных. Производятся средства защиты телетайпов, телексов и факсов. Для этих целей используются шифраторы, выполняемые в виде отдельных устройств, в виде приставок к аппаратам или встраиваемые в конструкцию телефонов, факс-модемов и других аппаратов связи (радиостанции и другие).

Распространенность шифрования как средства обеспечения безопасности теми или иными средствами можно характеризовать следующими данными (рис.4.13).



Специализированное программное обеспечение 18%

Рис.4.13. Распространенность шифрования как средства ЗИ

Аппаратные, программные, программно-аппаратные и криптографические средства реализуют те или иные услуги ИБ различными механизмами ЗИ, обеспечивающими соблюдение конфиденциальности, целостности, полноты и доступности.

Инженерно-техническая ЗИ использует физические, аппаратные, программные и криптографические средства.

Выводы

1. Комплексная безопасность информационных ресурсов достигается использованием правовых актов государственного и ведомственного уровня, организационных мер и технических средств ЗИ от различных внутренних и внешних угроз.

2. Правовые меры обеспечения безопасности и ЗИ являются основой порядка деятельности и поведения сотрудников всех уровней и степени их ответственности за нарушения установленных норм и правил работы по обеспечению сохранности секретов.

3. Организационные меры являются решающим звеном в формировании и реализации комплексных мер ЗИ. Они, в первую очередь, выражаются в создании службы безопасности предприятия и обеспечении ее нормального функционирования.

4. ИТЗ - это использование различных ТС в интересах обеспечения ИТ.

Контрольные вопросы

1. Перечислите направления обеспечения ИБ.
2. Определите понятие правовой защиты. Перечислите уровни правовой защиты
3. Где отражаются правовые нормы ИБ на конкретном предприятии?
4. Дайте определение понятию организационной защите. Каковы функции и структура службы безопасности предприятия
5. В чем состоит суть инженерно-технической защиты (ИТЗ)? Перечислите средства ИТЗ

Лекция 5. ЗАЩИТА ИНФОРМАЦИИ ОТ СЛУЧАЙНЫХ УГРОЗ

Вопросы:

5.1. Задачи ЗИ от случайных угроз

5.2. Повышение надежности и отказоустойчивости КС, блокировка ошибочных операций

5.3. Оптимизация взаимодействия пользователей и персонала с КС, минимизация ущерба от аварий и стихийных бедствий

Литература:

1. Завгородний В.И. комплексная защита информации в компьютерных системах: Учебное пособие. – Логос, 201. – С.38-53.

5.1. Задачи ЗИ от случайных угроз

Для блокирования (парирования) случайных угроз ИБ в КС должен быть решен следующий комплекс задач (рис.5.1):



Рис.5.1. Задачи защиты информации в КС от случайных угроз

- дублирования информации; повышения
- повышения надежности компьютерных систем (КС);
- создания отказоустойчивых КС;
- блокировки ошибочных операций;
- оптимизации взаимодействия человека с КС;
- минимизации ущерба от аварий и стихийных бедствий.

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 и 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.

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 дублируются таким образом, чтобы они были размещены на цилиндра 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 использование блоков (накопителей на магнитных дисках) для записи файлов. Дублирование не используется.

Зеркальное дублирование предусматривается на 1-м уровне RAID.

На 2-м уровне биты информации поочередно размещаются на дисках. Данные размещаются на дисках с дублированием.

Начиная с 3-го уровня, для восстановления информации используется не дублирование данных, а контрольная информация. Восстановление возможно при отказе одного диска. На 3-м уровне байты данных поочередно записываются на диски. Контрольная информация записывается на один выделенный диск.

Начиная с 4-го уровня, поочередная запись на диски ведется блоками. На 4-м уровне для записи контрольной информации отводится выделенный диск. Подсистема 4-го уровня допускает параллельное выполнение запросов на чтение, но запись осуществляется последовательно, так как контрольная информация записывается на один диск.

На 5-м уровне осуществляется поочередная запись на диски, как блоков данных, так и контрольной информации. На этом уровне, возможно, осуществлять одновременно несколько операций чтения или записи. В случае отказа одного диска, последний восстанавливается с помощью контрольной информации. Для восстановления информации с отказавшего диска требуется до 10 минут времени.

Блочная конструкция подсистем RAID позволяет наращивать число дисков. Реальные подсистемы поддерживают несколько уровней. Последние выбираются пользователем с учетом требований, предъявляемых к внешним запоминающим устройствам (ВЗУ) конкретной КС.

В подсистемах RAID, как правило, используются резервные источники питания, что существенно повышает отказоустойчивость таких подсистем.

Для дублирования информации используются также накопители на магнитных лентах. Такие устройства обладают большой емкостью, но значительно уступают накопителям на магнитных дисках по времени доступа к информации.

В настоящее время для хранения дублирующей информации используются устройства, получившие название *ленточные системы* с автоматической сменой кассет (их называют также библиотеками). Такие системы состоят из одного или нескольких лентопротяжных механизмов, механизма перемещения кассет и магазина для кассет. На одной кассете может храниться 10 Гбайт в сжатой или 4 Гбайта несжатой информации. Если учесть, что в магазине системы может находиться до 60 кассет (Spectra Logic 4655), то емкость таких систем позволяет хранить огромные массивы данных. Наряду с такими мощными системами могут использоваться и компактные системы с емкостью магазина в несколько кассет. Например, ленточная система Conner Peripherals 4586 NP имеет магазин емкостью 4 кассеты. С учетом возможности замены кассет такие системы позволяют дублировать на ленте объемы информации, ограниченные только наличием свободных кассет. Они используются для неоперативного дублирования, поэтому информация на ленты обычно записывается в сжатом виде. С помощью этих устройств осуществляется полное, частичное и комбинированное копирование с созданием копий различных уровней.

Съемные машинные носители могут использоваться для дублирования информации без использования специальных аппаратных средств. Для этих целей используются, как правило, гибкие магнитные диски, оптоэлектронные диски, а также жесткие съемные магнитные диски и магнитные ленты.

Методы использования съемных носителей информации сходны с методами использования ленточных систем с автоматической сменой кассет.

При использовании многоуровневого дублирования может быть реализован следующий подход к созданию и использованию копий. В качестве эталона верхнего уровня используется

редко изменяемая информация (программы, постоянные исходные данные). Эталон первого уровня используется только для восстановления информации, если ее невозможно восстановить с эталонов более низкого уровня, а также при изменениях информации и при периодическом контроле. Эталон второго уровня получается путем полного копирования информации с определенной периодичностью, например, один раз в сутки. На эталон первого уровня осуществляется инкрементное копирование либо по времени (раз в смену), либо после существенных и важных изменений. Например, получение важных сообщений по сети или результатов выполнения программ.

Распределенное копирование достижимо в компьютерных сетях и является практически единственным способом обеспечения целостности и доступности информации при стихийных бедствиях и крупных авариях.

5.2. Повышение надежности и отказоустойчивости КС, блокировка ошибочных операций

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 совместной 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 повышения 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.

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 самоустраниющихся 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.

Блокировка ошибочных операций. Ошибочные операции или действия могут вызывать отказы 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 диски.

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

5.3. Оптимизация взаимодействия пользователей и персонала с КС, минимизация ущерба от аварий и стихийных бедствий

1. Оптимизация взаимодействия пользователей и обслуживающего персонала с КС - Одно из основных направлений ЗИ в КС от непреднамеренных угроз. По сути дела она сводится к сокращению 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 (НОТ) предполагает:

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

Рабочее место пользователя или специалиста из числа обслуживающего 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 общения 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 талонов существенно снимает нагрузку на нервную систему, сокращает число ошибок, повышает работоспособность человека и производительность системы в целом.

Воспитание и обучение пользователей корпоративных КС и персонала является одним из центральных вопросов обеспечения ИБ в КС от всех классов угроз (в том числе и от преднамеренных). 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.

Анализ и совершенствование процессов взаимодействия человека с КС – важная задача оптимизации взаимодействия человека с КС, где применяются средства и методы ИБ. 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.

2. 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 удастся 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 системами 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 и 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?

Лекция 6. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ОТ ШПИОНАЖА И ДИВЕРСИЙ

Вопросы:

- 6.1. Система охраны объекта КС
- 6.2. Организация работ с конфиденциальной информацией и противодействие наблюдению в оптическом диапазоне
- 6.3. Противодействие подслушиванию и средства борьбы с закладными подслушивающими устройствами
- 6.4. Защита от злоумышленных действий обслуживающего персонала и пользователей

Литература:

1. Завгородний В.И. комплексная защита информации в компьютерных системах: Учебное пособие. – Логос, 201. – С.53-85.

6.1. 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.

1. 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 ограждений 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 металлическим 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 звенья 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 необходимости 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 полужакаленного 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 "заминированных" 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]. Пленки состоят 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.

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

- 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.6.1.



Рис.6.1. 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 полосы фольги. Они бывают электроконтактными, магнитоконтактными, ударно-контактными 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.

Ударно-контактные 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 возгорании изменяется акустический фон, что и фиксируется датчиком. Активные акустические (ультразвуковые) датчики (ДУЗ-4, ДУЗ-5, ДУЗ-12, "Фигус-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 человека 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°C 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 радио лучевые и радиотехнические датчики. В *радио лучевых 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 радио лучевые датчики: "Радий-1", "Радий-2", "Пион-Т", "Риф-РЛ", "Гарус", "Лена-2", "Протва", "Витим" и др.

Радиотехническими датчиками 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 видеомонитора.

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, радио лучевые и радиотехнические датчики. В системе "Гоби" применяются комплексно радио лучевые, вибрационные, контактные и емкостные датчики. Комбинированное использование датчиков различных типов значительно снижает вероятность бесконтрольного проникновения злоумышленника на территорию объекта КС. Основными направлениями 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 охраняемыми системами, включая систему пожарной безопасности, в одном устройстве управления комплексной системой охраны объекта. Такое устройство выполняется на базе ПЭВМ [46].

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. Их называют также телевизионными системами видеоконтроля (ТСВ).

Телевизионная система видеоконтроля обеспечивает:

- автоматизированное видео наблюдение за рубежами защиты;
- контроль за действиями персонала организации;
- видеозапись действий злоумышленников;
- режим видео охраны.

В режиме видео охраны ТСВ выполняет функции охранной сигнализации. Оператор ТСВ оповещается о движении в зоне наблюдения. В общем случае телевизионная система видеоконтроля включает следующие устройства (рис.6.2):

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

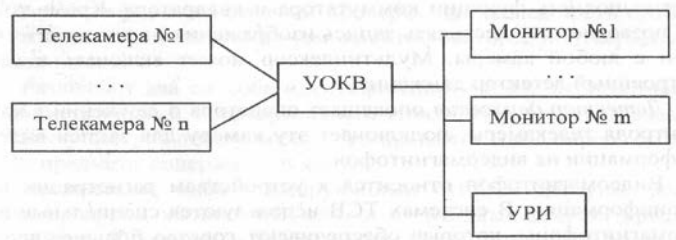


Рис.6.2.. Структурная схема телевизионной системы видеоконтроля

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

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

Коммутаторы позволяют подключить к одному монитору от 1 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 может выполнять функции коммутатора и квадратора. Кроме того, он позволяет осуществлять запись изображения на видеоманитофон 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 видеоманитофон.

Видеоманитофон относится к устройствам регистрации видеоинформации. В системах ТСВ используются специальные видеоманитофоны, которые обеспечивают гораздо большее

время записи (от 24 часов до 40 суток), чем бытовые видеомэгнитофоны. 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 - видео принтер.

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.

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 геометрический. **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. Контактные 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;
- запахи 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", DAL-LAS Bio-95 [70].

По надежности и затратам времени метод идентификации *по узорам сетчатки глаз* сопоставим с дактилоскопическим методом [69]. С помощью высококачественной телекамеры осу-

ществляется 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 узору сетчатки глаза. Объясняется это значительно меньшей стабильностью 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 помещениях. 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. 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.

6.2. Организация работ с конфиденциальной информацией и противодействие наблюдению в оптическом диапазоне

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.

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 прочесть 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.

6.3. Противодействие подслушиванию и средства борьбы с закладными подслушивающими устройствами

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 частотной инверсии сигнала низкие частоты преобразуются в высокие, и наоборот (рис.6).

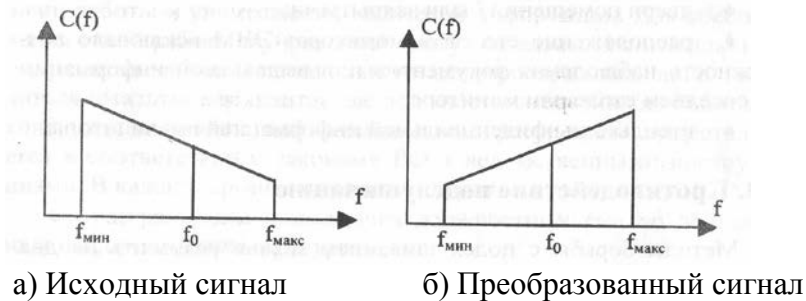


Рис.6. Частотная инверсия сигнала

Такой способ скремблирования обеспечивает невысокий уровень защиты, так как частота f_0 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).

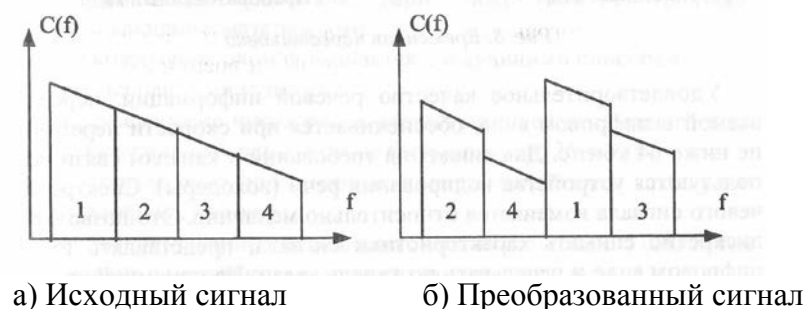


Рис.7. Частотная перестановка сигнала

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.

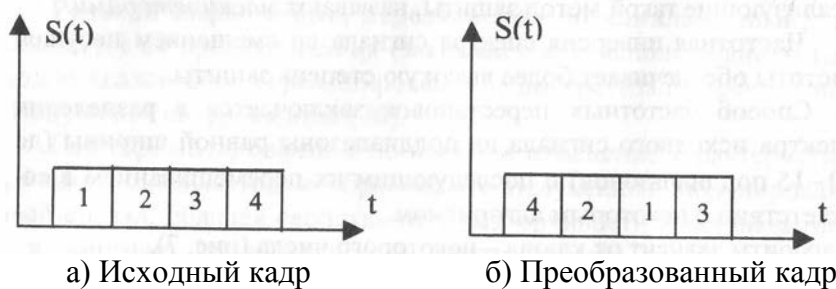


Рис.8. Временная перестановка

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 преобразования данных в КС. Методы шифрования подробно рассматриваются в лекции 10.

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 пористо-волокнутого 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 большом 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", "Буря") [44] действуют на расстоянии до 3 метров и способны непрерывно работать до 2 часов. Устройство "Буря-2" является мобильным и размещается в портфеле ("дипломате").

Средства борьбы с закладными подслушивающими устройствами

1. Средства радио контроля 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 радио контроля помещений;
- средства поиска неизлучающих закладок;
- средства подавления закладных устройств. Для осуществления радио контроля 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 фоновое. 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 радио-закладка 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 радио-закладок 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 радио-закладок 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].

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 (ССГО-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 , $2f_0$, $3f_0$ 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 $2f_0$ 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 i 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 $0,05^\circ\text{C}$ (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 МДЗ 11" 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.

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 радио-закладок.

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.

6.4. 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.

Лекция 7. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ОТ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ И НАВОДОК

Вопросы:

- 7.1. Пассивные методы защиты от побочных электромагнитных излучений и наводок
- 7.2. Активные методы защиты от ПЭМИН
- 7.3. Средства выявления и защиты от ПЭМИН

Литература:

1. Завгородний В.И. комплексная защита информации в компьютерных системах: Учебное пособие. – Логос, 201. – С.91-115.
2. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. – М.: Академический проект: Гаудеамус, 2004. – С.130-181

Широкое использование самых различных ТС обеспечения производственной и научной деятельности и автоматизированной обработки информации привело к появлению технических каналов утечки информации. Переносчиками информации в них выступают побочные электромагнитные излучения и наводки (ПЭМИН) различного происхождения. ПЭМИН присущи любым электронным устройствам, системам, изделиям по самой природе проявления (рис.7.1).



Рис.7.1. Побочные электромагнитные излучения и наводки (ПЭМИН)

Защита информации от утечки по электромагнитным каналам - это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет электромагнитных полей побочного характера и наводок.

Известны следующие электромагнитные каналы утечки информации:

- микрофонный эффект элементов электронных схем;
- электромагнитное излучение низкой и высокой частоты;
- возникновение паразитной генерации усилителей различного назначения;
- цепи питания и цепи заземления электронных схем;
- взаимное влияние проводов и линий связи;
- высокочастотное навязывание;
- волоконно-оптические системы.

Физические явления, лежащие в основе появления опасных излучений, имеют различный характер, тем не менее, в общем виде утечка информации за счет ПЭМИН может рассматриваться как непреднамеренная передача охраняемой информации по некоторой «побочной» системе связи.

Кроме того, технические средства (ТС) и системы могут не только непосредственно излучать в пространство сигналы, содержащие обрабатываемую информацию, но и улавливать за

счет своих микрофонных или антенных свойств акустические или магнитные (электромагнитные) излучения, преобразовывать их в электрические сигналы и передавать по своим линиям связи, как правило, бесконтрольно. Это в еще большей степени повышает опасность утечки информации за счет ПЭМИН.

Отдельные ТС имеют в своем составе помимо подобных "микрофонов" и "антенн" высокочастотные или импульсные генераторы, излучения которых могут быть промодулированы различными сигналами, содержащими конфиденциальную информацию. Опасный "микрофонный эффект" (образование паразитного электрического сигнала) возникает в некоторых телефонных аппаратах даже при положенной микрофонной трубке. Электромагнитные излучения могут образовываться и при самовозбуждении на радиочастотах звуковоспроизводящей и звукоусилительной аппаратуры.

Анализ условий и причин образования источников появления ПЭМИН показал, что для этого имеется ряд причин и условий. К ним можно отнести (рис.7.2).

- несовершенство схемных решений, принятых для данной категории технических средств, и
- эксплуатационный износ элементов изделия

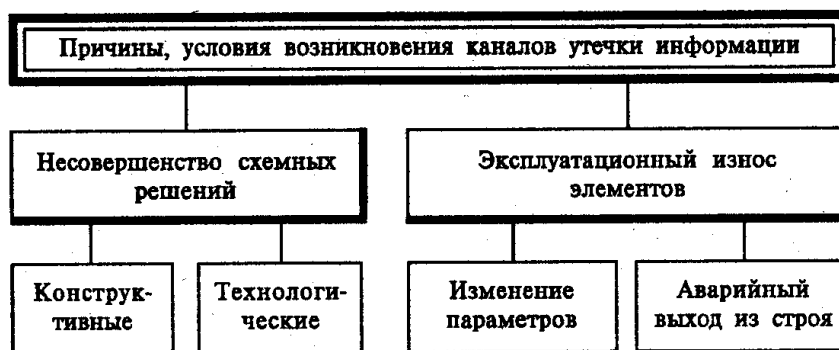


Рис.7.2 . Причины возникновения технических каналов утечки информации

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

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

Активные методы защиты направлены на создание помех в каналах ПЭМИН, 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.

7.1. Пассивные методы защиты от побочных электромагнитных излучений и наводок

Пассивные методы защиты от ПЭМИН могут быть разбиты на три группы (рис.7.3):

- экранирование;
- снижение мощности излучений и наводок;
- снижение информативности сигналов.

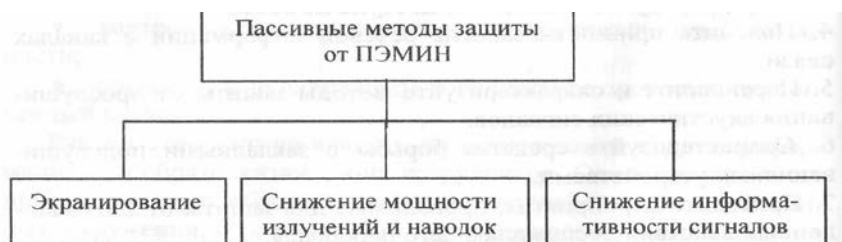


Рис.7.3. Классификация пассивных методов защиты от ПЭМИН

Экранирование - одним из самых 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 ε . При этом поле ослабляется в ε раз [64].

Экранирование магнитных полей включает в себя экранирование *низкочастотных* (до 10 кГц) и *высокочастотных магнитных полей*.

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 высокочастотных 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.

Экранирование электромагнитного поля (излучения) и его блокированию методами высокочастотного электрического и магнитного экранирования. Это 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.

С уровня *блоков* до уровня *устройств* экранирование осуществляется с помощью конструкций из листовой стали, металлических сеток и напыления.

Экранирование *кабелей* осуществляется 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 склеиванием 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 металлизирован 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, и позволяет уменьшить влияние электромагнитных шумов на работу устройств.

Снижение мощности излучений и наводок обеспечивает снижения уровня излучения и взаимного влияния элементов КС. К данной группе пассивных методов защиты от ПЭМИН относятся 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.

Использование оптических каналов связи является перспективным направлением борьбы с ПЭМИН. 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 неподвержены воздействию электромагнитных помех.

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

Использование фильтров [64] - один 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.

Гальваническая развязка в системе питания полностью исключается попадание побочных наведенных сигналов во внешнюю цепь электропитания. Наличие генераторов питания в первичной цепи обеспечивают *гальваническую развязку* между первичной и вторичной цепями, а также позволяет подавать во вторичную 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.

Снижение информативности сигналов ПЭМИН обеспечивает затрудняющее их использование при перехвате.

Оно осуществляется с помощью использования:

- *специальных схемных решений;*
- *кодирования информации.*

Специальные схемные решения – это использование не традиционных схем, например, таких 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.

Кодирование информации чаще всего осуществляется путем использования криптографических преобразований данных. Это предотвращает утечку информации, т.е. ее невозможно использовать без расшифровки.

7.2. 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 пространственное 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.

7.3. Средства выявления и защиты от ПЭМИН

7.3.1. Защита от утечки за счет микрофонного эффекта. Акустическая энергия, возникающая при разговоре, вызывает соответствующие колебания элементов электронной аппаратуры, что в свою очередь приводит к появлению электромагнитного излучения или электрического тока. Наиболее чувствительными элементами электронной аппаратуры к акустическим воздействиям являются катушки индуктивности, конденсаторы переменной емкости, пьезо- и оптические преобразователи. Микрофонным эффектом обладают:

- отдельные типы телефонных аппаратов,
- вторичные электрические часы системы часофикации,
- громкоговорители (динамики) систем радиофикации и громкоговорящей связи и др.

Там, где имеются такие элементы, возможно появление микрофонного эффекта.

Защита телефонного аппарата от утечки информации за счет микрофонного эффекта может быть обеспечена организационными или техническими мерами.

Организационные меры могут быть следующие:

- выключить телефонный аппарат из розетки (этим исключается источник, образования микрофонного эффекта);
- заменить аппарат на защищенный (выпускаются Пермским телефонным заводом).

Технические меры сводятся к включению в телефонную линию специальных устройств локализации микрофонного эффекта.

Так, электромеханический звонок колокольного типа является источником возникновения микрофонного эффекта в телефонном аппарате. Под воздействием на него акустических колебаний на выходе его катушки возникает ЭДС микрофонного эффекта (Емэ). Для защитных от Емэ используются схемы ее подавления (они представлены на рис.7.4-7.5).

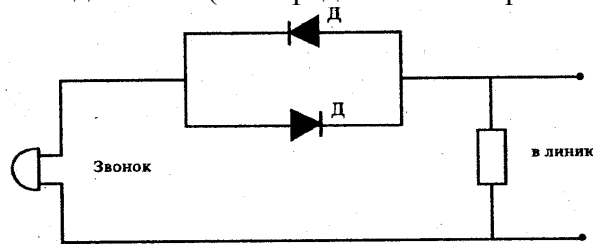


Рис.7.4. Схема подавления ЭДС микрофонного эффекта Емэ звонковой цепи ТА

Первая схема представляет автоматический клапан: малую ЭДС блокирует, а речевой сигнал разговора абонента пропускает. В ней в звонковую цепь включаются два диода, образующие схему подавления Емэ. Для малых значений Емэ такая схема представляет собой большое сопротивление, а для речевого сигнала, значительно большего по величине, схема открывается и речевой сигнал свободно проходит в линию.

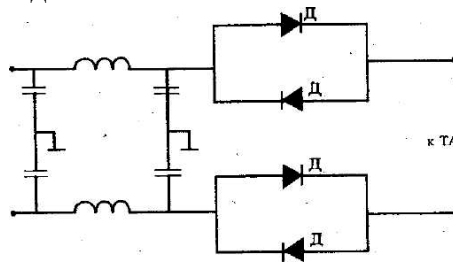


Рис.7.5. Более сложная схема подавления ЭДС

Во второй, более сложной схеме используется две пары диодов и высокочастотный фильтр. Обе схемы предотвращают возможность образования утечки информации за счет микрофонного эффекта телефонного аппарата с положенной на рычаг телефонной трубкой. В последнее время схемы подавления микрофонного эффекта стали выполняться в виде различных по конструкции аппаратных решений (например, в виде телефонной розетки, что позволяет скрывать их наличие от "любопытных" глаз).

Защита абонентского громкоговорителя радиовещательной сети или сети диспетчерского вещания осуществляется включением в разрыв сигнальной линии специального буферного усилителя, нагрузкой которого является однопрограммный абонентский громкоговоритель /динамик/ (рис.7.6).

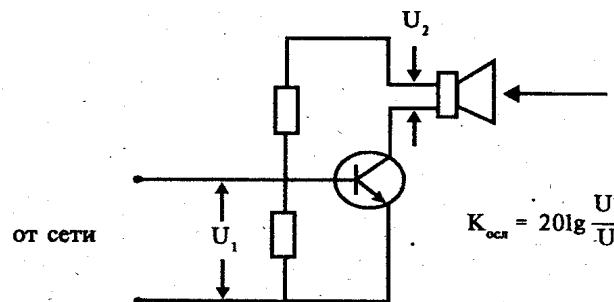


Рис.7.6. Вариант буферного усилителя

Такой усилитель обеспечивает ослабление Емэ на выходе громкоговорителя порядка 120 дБ. (такое акустическое подавление позволяет говорить перед громкоговорителем с любой громкостью). Для трехпрограммных громкоговорителей такое устройство необходимо только для низкочастотного (прямого) канала вещания, для остальных (высокочастотных) роль буфера будет выполнять усилитель преобразователя.

Блокирование канала утечки информации за счет микрофонного эффекта вторичных электрочасов системы централизованной часофикации осуществляется с помощью фильтров звуковых частот, обладающих очень сильным ослаблением частот в диапазоне 700-3400 Гц. Как правило, стремятся использовать фильтры с коэффициентом ослабления не менее 120 дБ.

Вывод: Микрофонный эффект присущ самым различным ТС и прежде чем приступать к использованию защитных мер, очевидно, следует как-то узнать, имеется ли в данном конкретном устройстве этот самый эффект.

Испытания и исследование ТС на наличие в них микрофонного эффекта проводится на специальных испытательных стендах с использованием высококачественной испытательной аппаратуры. Комплект такой аппаратуры используется при разработке, испытаниях и контроле качества электроакустических и электромеханических преобразователей: телефонных аппаратов, громкоговорителей, микрофонов, наушников, слуховых аппаратов и т.д. На рис.7.7. представлена примерная схема испытаний телефонного аппарата (ТА) на таком комплексе.

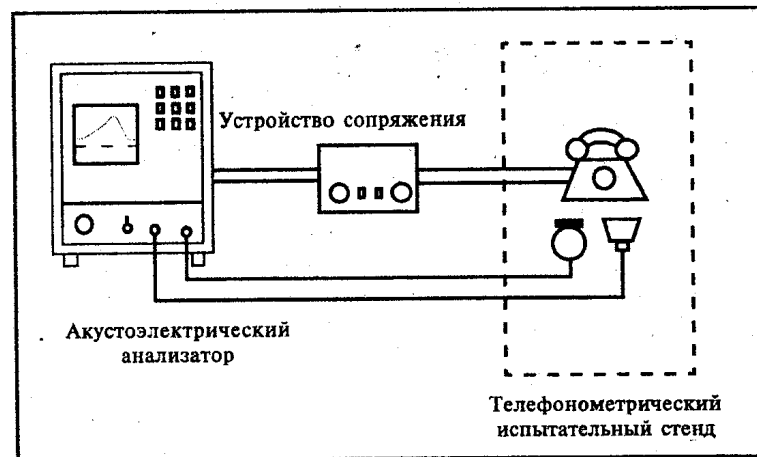


Рис.7.7. Примерная схема испытаний телефонного аппарата (ТА)

Комплекс позволяет определить передаточные характеристики исследуемых ТС, их эквивалентные схемы, характеристики микрофонного эффекта и другие параметры и обеспечивает измерение характеристик приема, передача и слышимости собственного микрофона, а также обратные потери, шум и искажения.

7.3.2. Защита от утечки за счет электромагнитного излучение низкой и высокой частоты. Электронные и радиоэлектронные ТС, особенно средства электросвязи, обладают большим электромагнитным излучением, специально вырабатываемым для передачи информации, и нежелательными излучениями, образующимися по тем или иным причинам конструкторско-технологического характера.

Нежелательные электромагнитные излучения низкой и высокой частоты подразделяются на опасные для ИБ побочные электромагнитные излучения и наводки (ПЭМИН), внеполосные и шумовые. Особенно опасны ПЭМИН - главный источник образования электромагнитных каналов утечки информации.

Каждое электронное устройство является источником электромагнитных полей широкого частотного спектра, характер которых определяется назначением и схемными решениями, мощностью устройства, материалами, из которых оно изготовлено, и его конструкцией. Характеристики любого электромагнитного поля изменяется в зависимости от дальности его приема. Это расстояние делится на две зоны: *ближнюю* и *дальнюю*. Для ближней зоны расстояние r значительно меньше длины волны ($r \ll \lambda$) и поле имеет ярко выраженный магнитный характер, а для дальней - ($r \gg \lambda$) поле носит явный электромагнитный характер и распространяется в виде

плоской волны, энергия которой делится поровну между электрическим и магнитным компонентами. Следовательно, можно считать возможным образование канала утечки в ближней зоне за счет магнитной плоя, а в дальней - за счет электромагнитного излучения.

В результате перекрестного влияния электромагнитных полей одно- или разнородного радио- и электротехнического оборудования в энергетическом помещении создается помехоустойчивое поле, обладающее магнитной и электрической напряженностью. Значение (величина) и фазовая направленность этой напряженности определяется числом и интенсивностью источников электромагнитных полей; размерами помещения, в котором размещается оборудование; материалами, из которых изготовлены элементы оборудования и помещения. Очевидно, чем ближе расположено оборудование относительно друг друга, чем меньше размеры помещения, тем больше напряженность электромагнитного поля.

В отношении энергетического помещения необходимо рассматривать две области распространения поля:

- внутри энергетического помещения (ближнее поле);
- за пределами помещения (дальнее поле).

Ближнее поле определяет электромагнитную обстановку в энергетическом помещении, а дальнее электромагнитное поле - распространение, дальность действия которого определяется диапазоном радиоволн.

Ближнее поле воздействует путем наведения электромагнитных полей в линиях электропитания, связи и других кабельных магистралях.

Суммарное электромагнитное поле имеет свою структуру, величину, фазовые углы напряженности, зоны максимальной интенсивности. Эти характеристики присущи как ближнему, так и дальнему полю.

В настоящее время напряженность внешних электромагнитных полей определяется с большой точностью: разработаны как аналитические, так и инструментальные методы. А вот напряженность суммарного поля, определяющая электромагнитную обстановку в энергетическом помещении, рассчитывается не достаточно строго. Нет пока четких методик расчета и методов инструментального измерения.

Таким образом, электромагнитную обстановку в помещении определяют следующие факторы:

- размеры и формы помещений;
- количество, мощность, режим работы и одновременность использования аппаратуры;
- материалы, из которых изготовлены элементы помещений и технические средства.

В качестве методов защиты и ослабления электромагнитных полей энергетического помещения используется

- установка электрических фильтров,
- пассивные и активные экранирующие устройства и
- специальное размещение аппаратуры и оборудования.

Установка экранирующих устройств может производиться либо в непосредственной близости от источника излучения, либо на самом источнике, либо, наконец, экранируется помещение, в котором размещены источники электромагнитных сигналов.

Рациональное размещение аппаратуры и технических средств в энергетическом помещении может существенно повлиять как на результирующую напряженность электромагнитного поля внутри помещения, так и на результирующее электромагнитное поле за его пределами. Рациональное размещение предполагает перестановку отдельных элементов оборудования помещений или отдельных групп аппаратов и ТС с тем, чтобы новое расположение приводило к взаимокompенсации напряженности электромагнитных полей опасных сигналов в заданных зонах. Такое размещение аппаратуры в отдельных случаях может оказаться определяющим.

Для реализации мероприятий по рациональному размещению аппаратуры и иного оборудования энергетических помещений с точки зрения ослабления ПЭМИН необходимо:

- иметь методику расчета электромагнитных полей группы источников опасных сигналов;

• иметь методы формализации и алгоритмы решения оптимизационных задач размещения аппаратуры.

Мероприятия по защите информации от ее утечки за счет электромагнитных излучений включают в себя мероприятия по

- воспрепятствованию возможности выхода этих сигналов за пределы зоны
- уменьшению их доступности.

Развернутая структура и краткое содержание этих мероприятий приведены на рис.7.8.

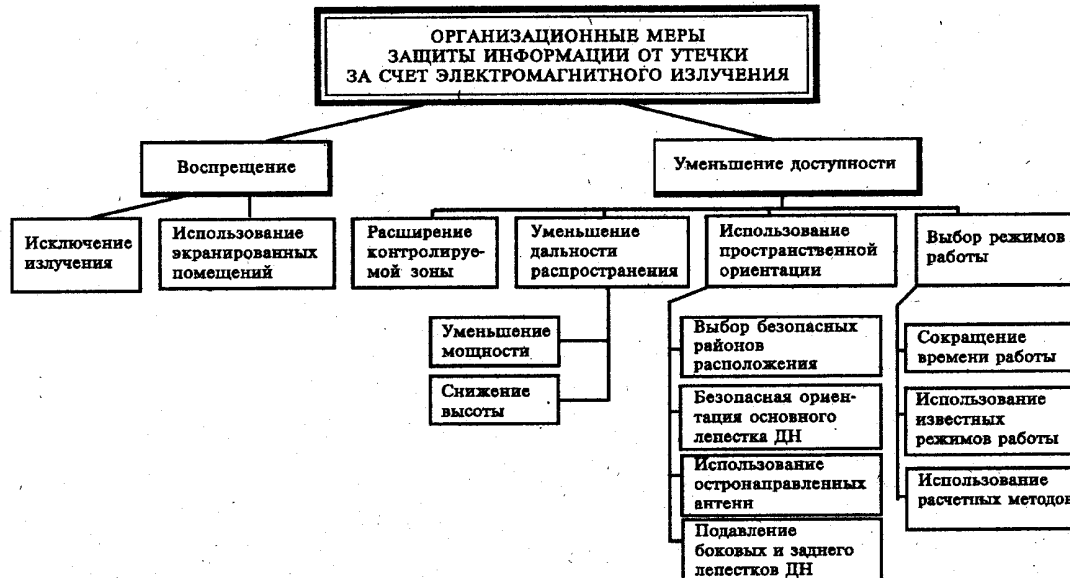


Рис.7.8. Организационные меры ЗИ от утечки за счет электромагнитного излучения

Учет электромагнитных излучений (волн) очень важен при реализации мероприятий по ЗИ. Особенности их распространения в пространстве по направлению и по дальности определяются диапазоном частот (длин волн) и мощностью излучения. Дальность и направленность излучения определяются физической природой распространения соответствующего вида волн и пространственным расположением источника опасного сигнала и средств его приема.

Учитывая особенности распространения электромагнитных колебаний, определяющихся прежде всего мощностью излучения, особенностями распространения и величинами поглощения энергии в среде распространения, правомерно ставить вопрос об установлении их предельно допустимых интенсивностей (мощностей), потенциально возможных для приема средствами злоумышленников. Эти допустимые значения интенсивностей принято называть нормами или допустимыми значениями.

Процесс определения или выработки норм называется нормированием, которое включает прежде всего, собственно, выбор критерия нормирования, выбор и обоснование нормируемого параметра и определение его предельно допустимого значения.

Нормы могут быть международные, федеральные и отраслевые. Не исключается наличие специальных норм для конкретных изделий и предприятий.

ЗИ от утечки за счет ПЭМИН самого различного характера предполагает:

- размещение источников и средств на максимально возможном удалении от границы охраняемой(контролируемой) зоны;
- экранирование зданий, помещений, средств кабельных коммуникаций;
- использование локальных систем, не имеющих выхода за пределы охраняемой территории (в том числе систем вторичной часофикации, радиофикации, телефонных систем внутреннего пользования, диспетчерских систем, систем энергоснабжения и т.д.);
- развязку по цепям питания и заземления, размещенных в границах охраняемой зоны;
- использование подавляющих фильтров в информационных цепях, цепях питания и заземления.

Для обнаружения и измерения основных характеристик ПЭМИН используются:

- измерительные приемники;
- селективные вольтметры;
- анализаторы спектра;
- измерители мощности и другие специальные устройства.

В таблице 7.1. приведены характеристики отдельных измерительных приемников и селективных вольтметров (табл. 6). С их помощью измеряют мощность (или напряженность) излучения на границе контролируемой зоны, определяют соответствие ее допустимым нормам. Если нормы не выполняются, то принимают меры по ослаблению мощности излучения.

Таблица 7.1. Характеристики измерительных приемников и селективных вольтметров

Тип	Диапазон частот	Пределы измерения мощности
П5-34	8,24-12,05 ГГц	3 10 ⁻¹² -10 ⁻⁴ Вт
П5-14	16,6-25,8 ГГц	10 ⁻¹² -10 ⁻⁶ Вт
В6-9	20 Гц — 200 кГц	1 мкВ — 1 В
В6-10	0,1~30 МГц	1 мкВ — 1 В
SMV-II	0,01-30 МГц	0,3 мкВ — 0,6 В

Например, программно-аппаратный комплекс "Зарница" (измерительный приемник) обеспечивает автоматизацию измерений при проведении исследований и контроля ТС ЭВТ, а именно:

- измерение параметров ПЭМИН,
- обработку результатов измерений,
- выполнение необходимых расчетов и
- выпуск отчетной документации при проведении исследований и контроля ТС.

Его достоинства:

- повышение достоверности и эффективности проведения (специальных) исследований за счет автоматизации процессов измерения,
- выявления информативных сигналов,
- обработки полученных результатов в соответствии с действующими нормативно-методическими документами,
- выпуска отчетной документации;
- снижение трудозатрат на проведение исследований.

При адаптации программного обеспечения комплекс может быть использован для решения задач в области электромагнитной совместимости (ЭМС), радионаблюдения и анализа электромагнитной обстановки при проведении испытаний.

Технические данные комплекса:

- измерение напряженности электромагнитного поля ПЭМИ от технических средств ЭВТ;
- работа в диапазоне частот:
 - а) при измерении напряженности магнитной составляющей поля ПЭМИ от 0,01 до 30 МГц;
 - б) при измерении напряженности электрической составляющей поля ПЭМИ от 0,01 до 1000 МГц;
- одновременное независимое управление анализаторами спектра СК4-59 и СК4-61;
- вывод на экран монитора и принтер результатов регистрации протоколов расчетов;
- обработка результатов измерений и проведение расчетов в соответствии с действующими нормативно-методическими документами.

Гарантийный срок эксплуатации - 1 год (за исключением изделий внешней поставки).

Состав комплекса:

- ПЭВМ типа IBM PC/AT - 1 шт.;
- Анализатор спектра СК4-59 - 1 шт.;
- Анализатор спектра СК4-61 - 1 шт.;
- Комплект входных преобразователей «АМУР-М» - 1 шт.;

- Контроллер управления АС - 2 шт.;
- Пакет прикладных программ - 1 комп.

7.3.3. Защита от утечки за счет паразитической генерации усилителей различного назначения. Паразитная генерация усилителей возникает из-за неконтролируемой положительной обратной связи за счет конструктивных особенностей схемы или за счет старения элементов.

Самовозбуждение может возникнуть и при отрицательной обратной связи из-за того, что на частоты, где усилитель вместе с цепью обратной связи вносит сдвиг фазы на 180° , отрицательная обратная связь превращается в положительную.

Самовозбуждение усилителей обычно происходит на высоких частотах, выходящих за пределы рабочей полосы частот (вплоть до КВ и УКВ диапазонов).

Частота самовозбуждения модулируется акустическим сигналом, поступающим на усилитель, и излучается в эфир как обычным радиопередатчиком. Дальность распространения такого сигнала определяется мощностью усилителя (т.е. передатчика) и особенностями диапазона радиоволн.

Защитные меры - контроль усилителей на самовозбуждение с помощью радиоприемников типа индикаторов поля, работающих в достаточно широком диапазоне частот, что обеспечивает поиск опасного сигнала.

7.3.4. Защита от утечки по цепям питания. Циркулирующая в тех или иных ТС конфиденциальная информация может попасть в цепи и сети электрического питания и через них выйти за пределы контролируемой зоны. На рис.7.9. приведен пример передачи высокой частоты в линию электропитания за счет паразитных емкостей трансформаторов блоков питания.

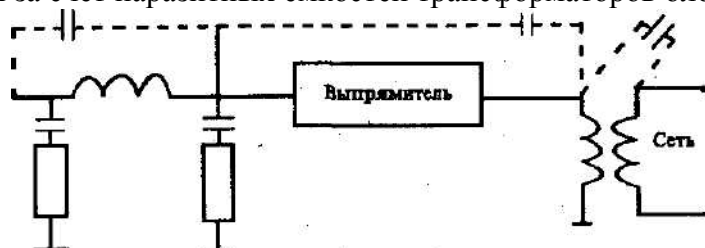


Рис.7.9. Схема утечки информации по цепям питания

Защита: Использование методов развязки (разводки) цепей питания с помощью отдельных стабилизаторов, преобразователей, сетевых фильтров для отдельных средств или помещений. Возможно использование отдельных трансформаторных узлов для всего энергоснабжения объекта защиты, расположенного в пределах контролируемой территории. Это более надежное решение локализации данного канала утечки.

5.4.5. Защита от утечки по цепям заземления. Правильное оборудование цепям заземления – одно из важных условий ЗИ. **Заземление** - это устройство, состоящее из заземлителей-проводников, соединяющих заземлители с электронными и электрическими установками, приборами, машинами. Как правило, заземлители имеет формы трубы, стержня, полосы, листа. Они выполняют защитную функцию и предназначены для соединения с землей приборов защиты. Отношение потенциала заземлителя к стекающему с него току называется сопротивлением заземления. Величина заземления зависит от удельного сопротивления грунта и площади соприкосновения заземления с землей (рис.7.10).

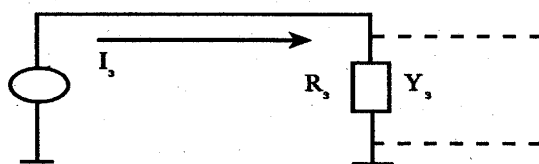


Рис.7.10. Эквивалентная схема заземления

Сопротивление заземления одного контура не должно быть более 1 ома. Если заземление состоит из металлической пластины радиуса r , расположенной непосредственно у поверхности земли, то сопротивление заземления рассчитывается по формуле:

$$R_3 = \rho/4r,$$

где ρ - удельное сопротивление грунта, Ом/см³;

r - радиус пластины, см;

R_3 - сопротивление заземлителя, Ом.

Для практических расчетов удельное сопротивление грунтов можно выбрать из табл.7.2. При устройстве заземления в качестве заземлителей чаще всего применяются стальные трубы длиной 2-3 м и диаметром 25-50 мм и стальные полосы сечением 50 - 100 мм². Заземлители следует соединять между собой шинами с помощью сварки. Сечение шин и магистралей заземления по условиям механической прочности и получения достаточной проводимости рекомендуется брать не менее 24 x 4 мм².

Таблица 7.2. Удельное сопротивление грунтов

Грунт	ρ - Ом/см ³ X 10 ³
Смешанный	1
Чернозем	30
Глина	40
Супесок	30
Суглинок	10
Песок влажный	50
Песок сухой	2500

Магистраль заземления вне здания надо прокладывать на глубине около 1,5 м, а внутри здания - по стенам или специальным каналам таким образом, чтобы их можно было внешне осматривать на целостность и на наличие контактного подключения. Не рекомендуется использовать в качестве заземления металлические конструкции зданий и сооружений, имеющих соединения с землей (отопление, водоснабжение).

7.3.6. Защита от утечки за счет взаимного влияние проводов и линий связи. Элементы, цепи, тракты, соединительные провода и линии связи любых электронных систем и схем постоянно находятся под воздействием собственных (внутренних) и сторонних (внешних) электромагнитных полей различного происхождения, индуцирующих или наводящих в них значительные напряжения. Такое электромагнитным влиянием (влияние) на элементы цепи образует непредусмотренные связями, т.е. паразитные (вредные) связи и наводки. Последние могут привести к образованию каналов утечки информации.

Основными видами паразитных связей в схемах электронных устройств являются емкостные, индуктивные, электромагнитные, электромеханические связи, связи через источники питания и заземления радиоэлектронных средств.

Паразитные емкостные связи обусловлены электрической емкостью между элементами, деталями и проводниками устройств, несущих потенциал сигнала, так как сопротивление емкости, создающей паразитную емкостную связь, падает с ростом частоты ($X_c = 1/\omega c$).

Паразитные индуктивные связи обусловлены наличием взаимоиндукции между проводниками и деталями аппаратуры, главным образом между его трансформаторами. Паразитная индуктивная обратная связь между трансформаторами усилителя, например, между входным и выходным трансформаторами, может вызвать режим самовозбуждения в области рабочих частот и гармониках.

Паразитные электромагнитные связи обычно возникают между выводными проводниками усилительных элементов, образующими колебательную систему с распределенными параметрами и резонансной частотой определенного порядка.

Взаимные влияния в линиях связи. Рассмотрим, какое влияние друг на друга оказывают параллельно проложенные линии связи.

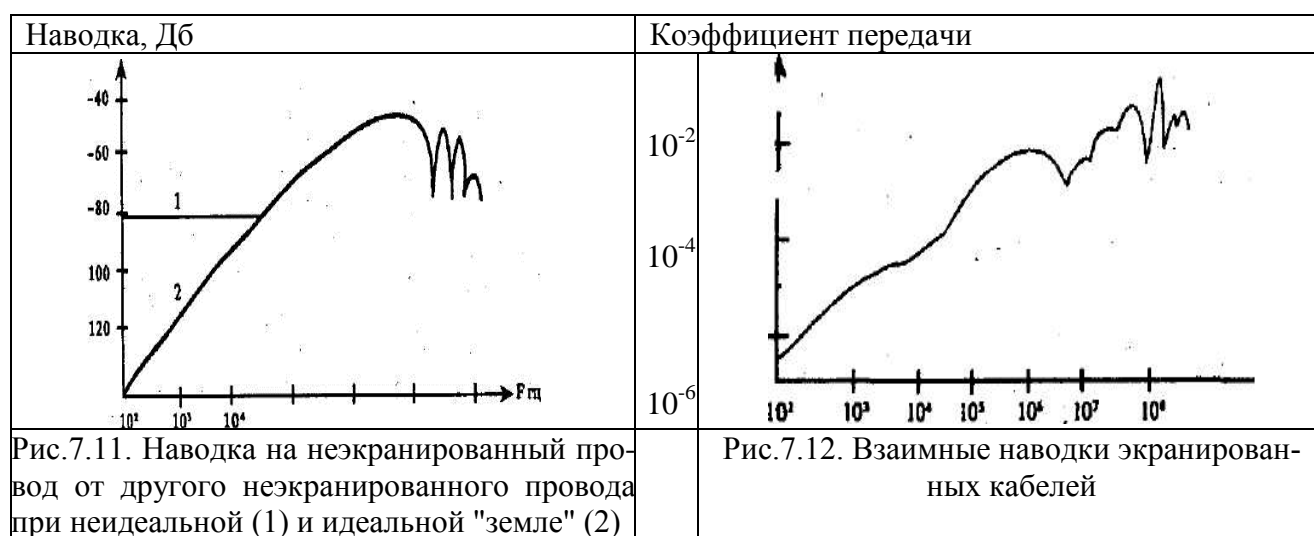
В теории взаимных влияний между цепями линий связи приняты следующие основные определения:

- влияющая цепь - цепь, создающая первичное влияющее электромагнитное поле;
- цепь, подверженная влиянию, - цепь, на которую воздействует влияющее электромагнитное поле;
- непосредственное влияние - сигналы, индуцируемые непосредственно электромагнитным полем влияющей цепи в цепь, подверженную влиянию.

Помимо непосредственного влияния имеют место косвенные влияния вторичными полями за счет отражений.

В зависимости от структуры влияющего электромагнитного поля и конструкции цепи, подверженной влиянию, различают систематические и случайные влияния.

К *систематическим* влияниям относят взаимные наводки, возникающие по всей длине линии, а к *случайным* - влияния, возникающие вследствие ряда случайных причин, не поддающихся точной оценке. Существуют реальные условия наводок с одного неэкранированного провода на другой, параллельный ему провод той же длины, когда оба они расположены над "землей". На рис.7.11-7.12 приведены характеристики взаимных наводок неэкранированных и экранированных кабелей.



В реальных условиях имеют место наводки и от экранированных кабелей на экранированные кабели и от неэкранированных кабелей на экранированные.

Вывод: 1. Излучения и наводки от различных ТС, экранированных и неэкранированных кабельных сетей далеко не безопасны. Для последних требуется хорошее состояние экрана и качественное заземление. На практике кабели не всегда полностью экранированы. Неисправные или покрытые коррозией соединители могут быть причиной значительных излучений.

2 Используя узкополосные (полоса менее 1 кГц) приемники, можно зарегистрировать напряженности поля 0,1 мкВ на поверхности кабеля. Это позволяет обнаружить сигнал 1 мкВ на расстоянии 3 м от кабеля. Даже на расстоянии 300 м сигналы, имеющие значение 1 мВ на поверхности кабеля, могут быть обнаружены.

Основные меры защиты цепей и трактов линий связи и проводов от взаимных влияний.

1. Массовое применение систем передачи и типов линий связи, обеспечивающих малые значения взаимных влияний. Так, применение коаксиальных кабелей и волоконно-оптических линий практически полностью решает проблему защиты цепей и трактов линий связи от взаимного влияния.

2. Рациональный выбор кабелей для различных систем передачи.

3. Взаимная компенсация наводок и помех между цепями симметричных линий связи, наводимых на различных участках за счет скрещивания цепей воздушных линий связи или симметричных кабельных линий и соответствующего подбора шагов скрутки цепей симметричного кабеля.

4. Экранирование цепей кабельных линий гибкими (чулок) или жесткими (трубы) экранами. Защита от взаимного влияния в этом случае достигается путем ослабления интенсивности влияющего электромагнитного поля в экране.

В таблице 7.3 приведены данные взаимного влияния типов линий и меры их защиты.

Таблица 7.3. Взаимное влияние различных линий связи и меры защиты

Тип линии	Преобладающее влияние	Меры защиты
Воздушные линии связи	Систематическое влияние, возрастающее с увеличением частоты сигнала	Скрещивание цепей, оптимальное расположение цепей
Коаксиальный кабель	Систематическое влияние через третьи цепи. С повышением частоты влияние убывает вследствие поверхностного эффекта	Экранирование и ограничение диапазона рабочих частот снизу
Симметричный кабель	Систематическое и случайное влияния, возрастающие с частотой	Оптимизация шагов скрутки и конструкции кабеля; пространственное разделение цепей, экранирование
Оптический кабель	Систематическое и случайное влияния от частоты сигнала практически не зависят	Экранирование оптических волокон, пространственное разделение оптических волокон, защита от акустического воздействия

7.3.7. Защита от утечки за счет высокочастотного (ВЧ) навязывания. Любое электронное устройство под воздействием высокочастотного электромагнитного поля становится как бы перемещенным излучателем, вторичным источником излучения высокочастотных колебаний. Такой сигнал принято называть интермодуляционным излучением, а в практике специалистов бытует понятие "высокочастотное навязывание". Интермодуляционное излучение - это побочное радиоизлучение, возникающее в результате воздействия на нелинейный элемент высокочастотного электромагнитного поля и электромагнитного поля электронного устройства.

Интермодуляционное излучение в последующем может быть переизлучено на гармониках 2 и 3 порядка или наведено на провода и линии связи. Но в любом случае оно способно выйти за пределы контролируемой зоны в виде электромагнитного излучения.

В качестве источника навязываемого ВЧ сигнала могут выступать (рис.7.12):

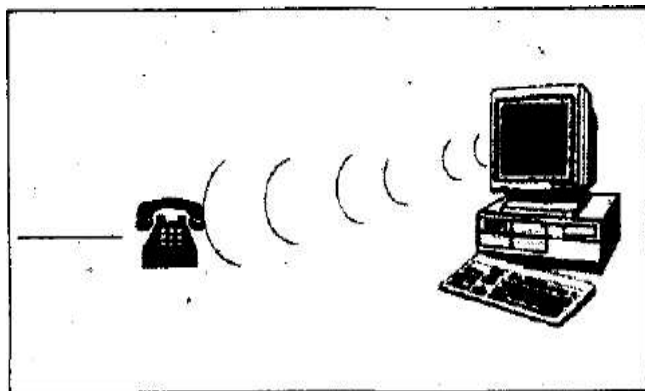


Рис.7.12. Вариант ВЧ навязывания

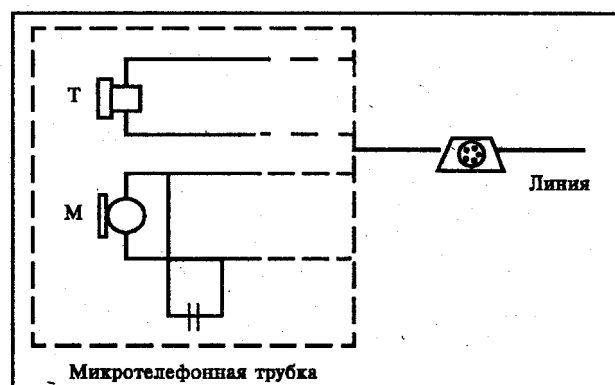


Рис.7.13. Шунтирование микрофона телефона при ВЧ навязывании

- радиовещательные станции, находящиеся вблизи объекта защиты;
- персональные ЭВМ, электромагнитное поле которых может воздействовать на телефонные и факсимильные аппараты, с выходом опасного сигнала по проводам за пределы помещений и здания.

При воздействии ВЧ навязывания на телефонный аппарат его модулирующим элементом является микрофон. Следовательно, нужно воспрепятствовать прохождению ВЧ тока через него. Это достигается путем подключения параллельно микрофону постоянного конденсатора емкостью порядка 0,01-0,05 мкФ. В этом случае ВЧ составляющая сигнала будет проходить через конденсатор, минуя микрофон (рис.7.13). Глубина модуляции при такой защите уменьшается более чем

в 10 000 раз, что практически исключает последующую демодуляцию сигнала на приемной стороне.

Более сложной защитой является использование фильтров подавления ВЧ сигналов на входе телефонного аппарата. При угрозе ВЧ навязывания лучше всего выключить телефонный аппарат на период ведения конфиденциальных переговоров.

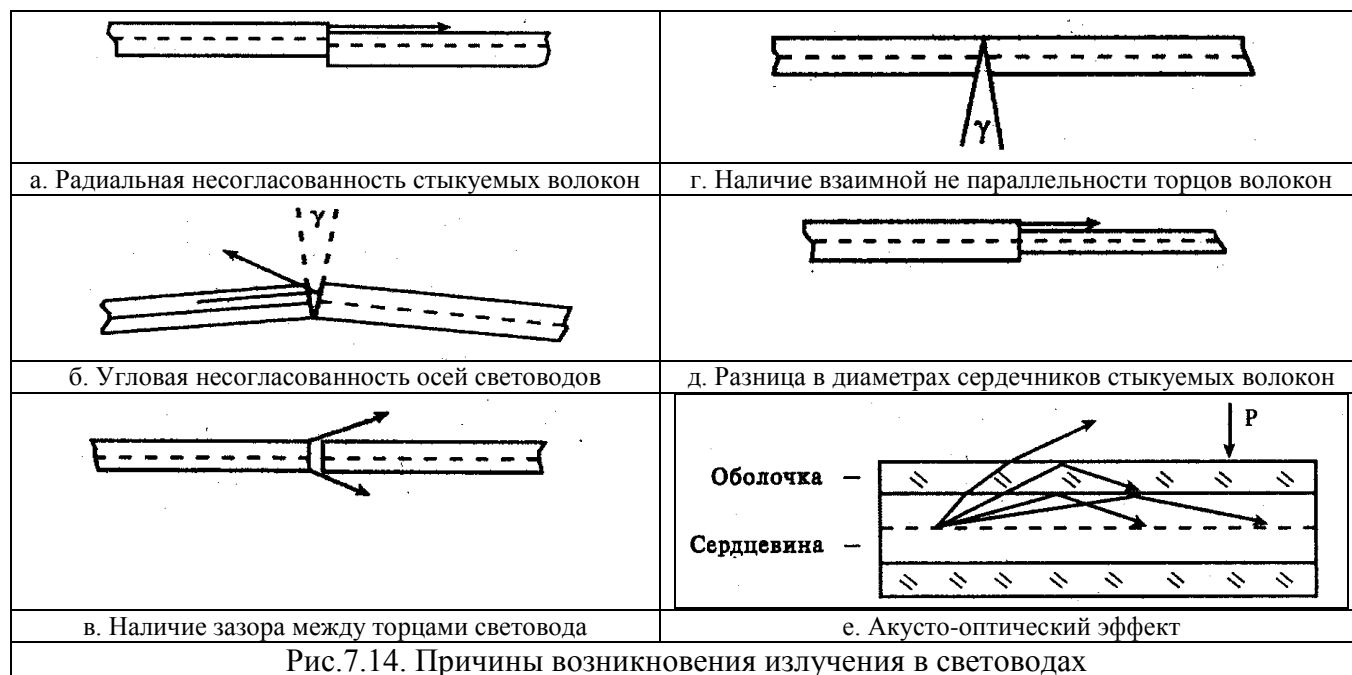
7.3.8. Защита от утечки в волоконно-оптических линиях и системах связи. Волоконно-оптические линии связи обладают оптическими каналами утечки информации и акусто-оптическим эффектом, также образующим канал утечки акустической информации.

Причинами возникновения излучения (утечка световой информации) в разъемных соединениях волоконных световодов являются:

- радиальная несогласованность стыкуемых волокон (рис.7.14а);
- угловая несогласованность осей световодов (рис.7.14б);
- наличие зазора между торцами световода (рис.7.14в);
- наличие взаимной не параллельности поверхностей торцов волокон (рис.7.14г);
- разница в диаметрах сердечников стыкуемых волокон (рис.7.14д).

Все эти причины приводят к излучению световых сигналов в окружающее пространство.

Акусто-оптический эффект проявляется в модуляции светового сигнала за счет изменения толщины волновода под воздействием акустического давления P на волновод (рис.7.14е).



Меры защиты: Определяются физической природой возникновения и распространения света. Она требует ограждения волноводов от акустического воздействия на него, за счет наружного покрытие оптического волокна соответствующим материалом, повышающим или понижающим чувствительность световодов к действию давления P . С одной стороны, акустическая чувствительность волоконного световода с полимерным покрытием может значительно превышать чувствительность оптического волокна без защитного покрытия.

С другой стороны, можно значительно уменьшить чувствительность волоконно-оптического кабеля к действию акустического поля, если волокно перед его заделкой в кабель покрыть слоем вещества с высоким значением объемного модуля упругости.

Это может быть достигнуто, например, нанесением непосредственно на поверхность оптического волокна слоя никеля толщиной около 13 мкм, алюминия толщиной около 95 мкм или стекла, содержащего алюминат кальция, толщиной около 70 мкм.

Применяя метод гальванического покрытия, можно получать на оптическом волокне относительно толстую и прочную пленку.

Зависимость чувствительности световодов к акустическому давлению при различных покрытиях эластомерами приведена на рис.7.15

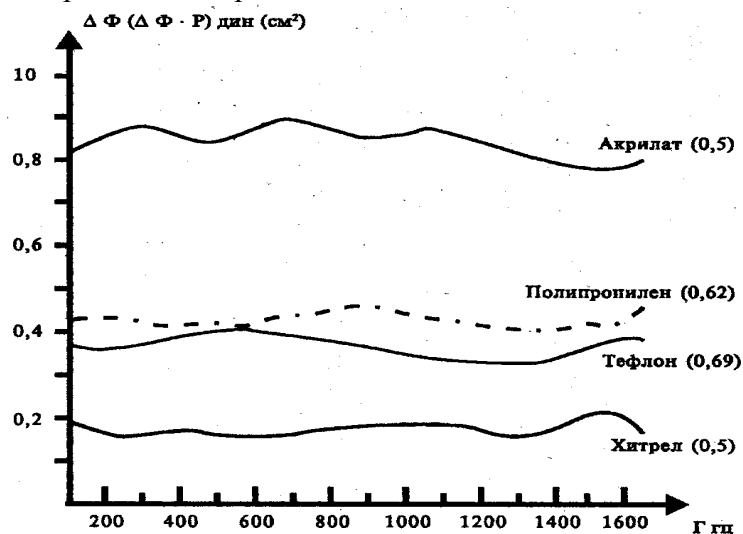


Рис.7.15. Чувствительность световодов к оптическому давлению P при его покрытии различными эластомерами (в скобках указана толщина слоя покрытия в мм)

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.

Лекция 8. МЕТОДЫ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ИЗМЕНЕНИЯ СТРУКТУР КС

Вопросы:

- 8.1. Общие требования к защищенности КС от несанкционированного изменения структур
- 8.2. Защита от закладок при разработке программ
- 8.3. Защита от внедрения аппаратных закладок на этапе разработки и производства
- 8.4. Защита от несанкционированного изменения структур КС в процессе эксплуатации

Литература:

1. Завгородний В.И. комплексная защита информации в компьютерных системах: Учебное пособие. – Логос, 201. – С.85-91.

8.1. 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.8.1).

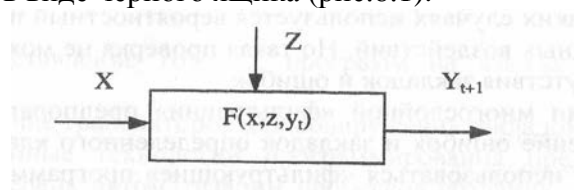


Рис.8.1. Графическое представление блока

Блок осуществляет преобразование вектора \mathbf{X} входных воздействий при наличии вектора внешних условий \mathbf{Z} и с учетом состояния блока \mathbf{Y}_t . Функциональное преобразование $\mathbf{F}(\mathbf{x}, \mathbf{z}, \mathbf{y}_t)$ переводит блок в состояние, характеризуемое состоянием \mathbf{Y}_{t+1} , где $\mathbf{x} \in \mathbf{X}$, $\mathbf{z} \in \mathbf{Z}$, $\mathbf{y} \in \mathbf{Y}$.

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, приемосдаточные 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.

8.2. Защита от закладок при разработке программ

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.

1. 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 отдельную 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, само документируемых модулей описаний классов и множество модулей реализации тел методов. Такое представление программ упрощает их семантический анализ и контроль на наличие в них закладок.

2. Автоматизированная система (АС) разработки программных средств. АС 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 опок-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 может сам внедрить закладку, так как у него нет права на модификацию программ, разрабатываемых программистами.

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 моделей 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.8.2):



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

Рис.8.2. Структурная схема контрольно-испытательного стенда

- 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 ша
- модель внешних воздействий, предназначенная для учета воздействий, внешних по отношению к моделируемой системе;
- модуль анализа результатов тестирования.

4. Представление готовых программ на языках высокого уровня. 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.

5. Наличие трансляторов для обнаружения закладок, проверенных на отсутствие ошибок и закладок, из любой 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.

8.3. 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.

8.4. Защита от несанкционированного изменения структур КС в процессе эксплуатации

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 лекции 6.

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. лекцию 6);
- механические ключи.

Практически во всех 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 необходимо 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 $S \geq 9$ символов.
3. Пароли должны периодически меняться. Безопасное время использования пароля (T_δ) может быть рассчитано по формуле [54]:

$$T_\delta = (A^S t)/2,$$

где t - время, необходимое на ввод слова длиной s ;

s - длина пароля;

A - количество символов, из которых может быть составлен пароль.

Время t определяется из соотношения:

$$t = E/R,$$

где E - число символов в сообщении, содержащем пароль;

R - скорость передачи символов пароля (симв./мин.).

Величина E зависит от длины пароля и количества служебных символов.

В приведенной формуле расчета величины T_δ 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 T_δ . 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 *съёмный 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 SecurID 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 закрываться 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.

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.

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.

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 $mod 2$, 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 $n-1$, где n - 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 $R_A(x)$ действия выполняются по правилам деления полиномов, заменяя операцию вычитания операцией сложения по модулю 2:

$$\begin{array}{r} x^9 + x^7 + x^4 \\ \oplus \quad \begin{array}{l} | \frac{x^3 + x + 1}{x^6 + x^3 + 1} \\ x^9 + x^7 + x^6 \\ \hline x^6 + x^4 \\ \oplus \quad x^6 + x^4 + x^3 \\ \hline x^3 \\ \oplus \quad x^3 + x + 1 \\ \hline x + 1 \end{array} \end{array}$$

- остаток $R_A(x)$

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

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 делиться на порождающий полином без остатка:

$$\begin{array}{r}
 x^9 + x^7 + x^3 + x + 1 \\
 \oplus \quad \frac{x^3 + x + 1}{x^6 + x^3 + 1} \\
 \hline
 x^9 + x^7 + x^6 \\
 \hline
 x^6 + x^4 + x + 1 \\
 \oplus \\
 x^6 + x^4 + x^3 \\
 \hline
 x^3 + x + 1 \\
 \oplus \\
 x^3 + x + 1 \\
 \hline
 0
 \end{array}$$

- остаток $R_A(x)$

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 $mod 2$ 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 последовательности 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?

Лекция 9.ЗИ В КС ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Вопросы:

- 9.1. Система разграничения доступа к информации в КС
- 9.2. Система защиты программных средств от копирования и исследования

Литература:

1. Завгородний В.И. комплексная защита информации в компьютерных системах: Учебное пособие. – Логос, 201. – С.114-133.

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 системы 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.

9.1. Система разграничения доступа к информации в КС

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 O_j , а субъекту доступа - строка S_i . На пересечении столбцов и строк записываются операция или операции, которые допускается выполнять субъекту доступа i с объектом доступа j (рис.9.1).

	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.9.1. Матрица доступа

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 такой метод контроля доступа к информации называется дискреционным.

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.9.2) 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.

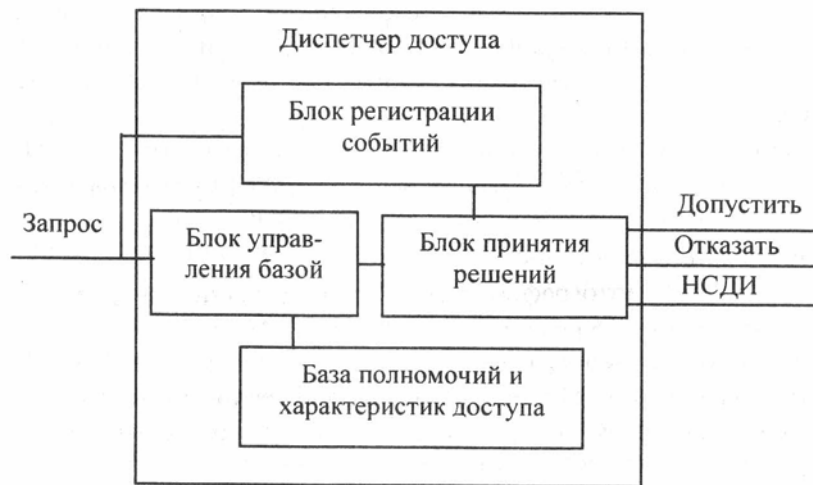


Рис.9.2. Диспетчер доступа

Блок криптографического преобразования информации при ее хранении и передаче является надежным способом защиты от НСДИ в распределенных КС. Обусловлено это тем, что криптографическое закрытие информации сегодня одним из самых надежных средств ЗИ. Сущность его изложена в лекции 11.

Блок очистки памяти в СРД должен реализовать функцию очистки оперативной памяти и рабочих областей на ВЗУ 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.

3. Концепция построения систем разграничения доступа. В основе построения СРД лежит концепция разработки защищенной универсальной ОС на базе ядра безопасности [6]. Под **яд-**

ром безопасности понимают локализованную, минимизированную, четко ограниченную и надежно изолированную совокупность 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 фон-неймановской 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 использование 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.

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 Wipehifo, 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 СЗИ в качестве идентификатора используют, как правило, только пароль. Пароль может быть перехвачен 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. Причем 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 бес-

смысленной. 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.

9.2. Система защиты программных средств от копирования и исследования

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 позволяет 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 сбоя.

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. Ес-

ли 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 диске 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.

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 передается 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.

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 работы 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.

Использование самогенерируемых кодов, заключается в том, что исполняемые коды программы 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.

"Обманом" дизассемблера – это 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 современных 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.

Изменением среды функционирования понимается – это 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.

Модифицирующиеся (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?

Лекция 10. КОМПЬЮТЕРНЫЕ ВИРУСЫ И МЕХАНИЗМЫ БОРЬБЫ С НИМИ

Вопросы:

- 10.1. Классификация компьютерных вирусов
- 10.2. Методы и средства борьбы с вирусами
- 10.3 Профилактика заражения вирусами компьютерных систем

Литература:

1. Завгородний В.И. комплексная защита информации в компьютерных системах: Учебное пособие. – Логос, 201. – С.159-179.

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, используя, 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 нарушению целостности и конфиденциальности информации, хранящейся в запоминающих устройствах. Последствия таких вирусов могут 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 выполнения программ, перезагрузки операционной системы или повторной передачи данных по каналам связи и т.п.

Очень опасными следует считать вирусы, вызывающие нарушение 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 пользователей. 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 электромагнитических 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 видеoinформации 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 телевидению. 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" (*companion*);
- 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;
- "стелс" - 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.

"Стелс" - 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. "Стелс"- 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, осуществляется 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.

1. Файловые вирусы

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). Макро вирусы могут внедряться и в другие файлы, содержащие макрокоманды.

Файловые вирусы могут размещаться в начале, середине и конце заражаемого файла (рис.10.1).

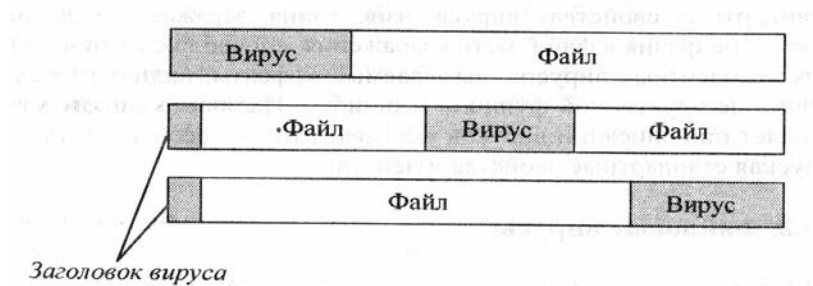


Рис.10.1. Варианты размещения вирусов в файлах

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.

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.

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.

2. 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.

3. Загрузочные вирусы

Загрузочные вирусы заражают загрузочные (Boot) сектора гибких дисков и Boot-сектора или Master Boot Record (MBR) жестких дисков (рис.10.2).

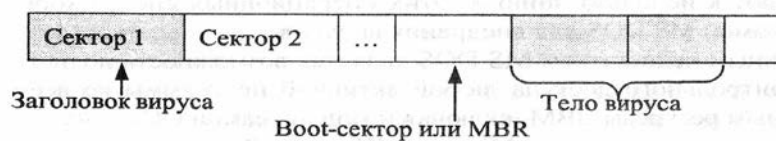


Рис.10.2. Размещение загрузочного вируса на диске

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 ОП, 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.

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.

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 IBM 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 ограничен. Сохраняют работоспособность и загрузочные вирусы, разработанные для MS DOS, так как они получают управление еще до загрузки Microsoft Windows 3.1 и в 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 IBM 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.

10.2. 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.

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 Aidtest Дмитрия Лозинского.

Метод обнаружения изменений 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 "стелс" - 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 вирусом 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 необходимо 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 "стелс"-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.

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.

10.3 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. Копируется 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).

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.

Лекция 11. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Вопросы:

- 11.1. Классификация методов криптографического преобразования информации
- 11.2. Стандарты шифрования
- 11.3. Перспективы использования криптозащиты информации в КС

Литература:

1. Завгородний В.И. комплексная защита информации в компьютерных системах: Учебное пособие. – Логос, 201. – С.159-179.

11.1. 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.11.1).

Процесс **шифрования** заключается в проведении обратимых математических, логических, комбинаторных и других преобразований исходной информации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов и двоичных кодов.



Рис.11.1. Классификация методов криптографического преобразования информации

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 обра-

ботке 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 шифрованию. Для сокращения времени целесообразно совмещать процесс сжатия и шифрования информации.

11.1.1. 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 обнаружено 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 Programmable 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 технологию 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.11.2 [8].



Рис.11.2. Классификация методов шифрования

11.1.3. Методы шифрования с симметричным ключом

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 s_{0i} , исходного алфавита A_0 , с помощью которых записывается исходная информация, однозначно ставятся в соответствие символы s_{1i} , шифрующего алфавита A_1 . В простейшем случае оба алфавита могут состо-

ять 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. T_0 , длиной - K символов, по определенному алгоритму.

Алгоритм моно алфавитной замены может быть представлен в виде последовательности шагов.

Шаг 1. Формирование числового кортежа L_{0h} путем замены каждого символа $s_{0i} \in T_0$ ($i = 1, K$), представленного в исходном алфавите A_0 размера $[1 \times R]$, на число $h_{0i}(s_{0i})$, соответствующее порядковому номеру символа s_{0i} в алфавите A_0 .

Шаг 2. Формирование числового кортежа L_{1h} путем замены каждого числа кортежа L_{0h} на соответствующее число h_{1i} кортежа L_{1h} , вычисляемое по формуле:

$$h_{1i} = (k_1 \times h_{0i}(s_{0i}) + k_2) \pmod{R},$$

где k_1 - десятичный коэффициент;

k_2 - коэффициент сдвига.

Выбранные коэффициенты k_1, k_2 должны обеспечивать однозначное соответствие чисел h_{0i} и h_{1i} ; а при получении $h_{1i} = 0$ выполнить замену $h_{1i} = R$.

Шаг 3. Получение шифртекста T_1 путем замены каждого числа $h_{1i}(s_{1i})$ кортежа L_{1h} соответствующим символом $s_{1i} \in T_1$ ($i = 1, K$) алфавита шифрования A_1 размера $[1 \times R]$.

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

Пример. Исходными данными для шифрования являются:

$T_0 = \langle \text{МЕТОД ШИФРОВАНИЯ} \rangle$;

$A_0 = \langle \text{АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ_} \rangle$;

$A_1 = \langle \text{ОРЩЪЯТЭ_ЖМЧХАВДЫФКСЕЗПИЦГНЛЪШБУО} \rangle$;

$K=32$; $k_1=3$; $k_2=15$, $b=4$.

Пошаговое выполнение алгоритма приводит к получению следующих результатов.

Шаг 1. $L_{0h} = \langle 12, 6, 18, 14, 5, 32, 24, 9, 20, 16, 14, 3, 13, 9, 31 \rangle$.

Шаг 2. $L_{1h} = \langle 19, 1, 5, 25, 30, 15, 23, 10, 11, 31, 25, 24, 18, 22, 10, 12 \rangle$.

Шаг 3. $T_1 = \langle \text{СОЯГБДИМЧУГЦКПМХ} \rangle$.

Шаг 4. $T_2 = \langle \text{СОЯГ БДИМ ЧУГЦ КПМХ} \rangle$.

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

$$k_1 h_{0i} + k_2 = n R + h_{1i},$$

При известных целых величинах k_1, k_2, h_{1i} и R величина h_{0i} вычисляется методом перебора n .

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_{0i} таблицы. Если произошло

Шаг 5. Полученная зашифрованная последовательность разбивается на блоки определенной длины, например, по четыре символа. Последний блок дополняется, при необходимости, случайными 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 s_{1r} из шифртекста и соответствующие символы ключа k_m . В матрице T_{III} определяется строка i , для которой выполняется условие $k_m = b_{i1}$. В строке i определяется элемент $b_{ij} = s_{1r}$. В расшифрованный текст на позицию r помещается символ b_{1ij} .

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

Пример.

Требуется с помощью ключа $K = \langle \text{ЗОНД} \rangle$ зашифровать исходный текст $T = \langle \text{БЕЗОБЛАЧНОЕ_НЕБО} \rangle$. Механизмы зашифрования и расшифрования представлены на рис.11.5.

Исходный текст	БЕЗОБЛАЧНОЕ_НЕБО
Ключ	ЗОНДЗОНДЗОНДЗОНД
Текст после замены	ИУФТИШНЫФЫТГФУОТ
Шифртекст	ИУФТ ИШНЫ ФЫТГ ФУОТ
Ключ	ЗОНД ЗОНД ЗОНД ЗОНД
Расшифрованный текст	БЕЗО БЛАЧ НОЕ_ НЕБО
Исходный текст	БЕЗОБЛАЧНОЕ_НЕБО

Рис.11.5. 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 π , e и другие. Очередной n -й символ исходного текста заменяется соответствующим символом из строки матрицы шифрования, номер которой совпадает с n -й цифрой бесконечного числа.

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 8×8) возможны $1,6 \times 10^9$ комбинаций ключа. Для блока длиной 256 символов (матрица размерностью 16×16) 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.11.6).

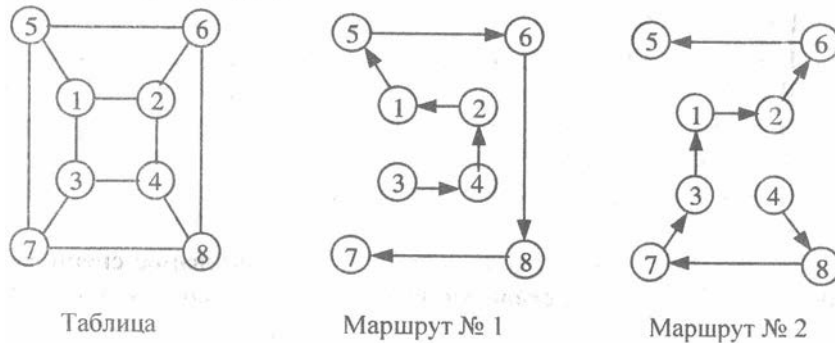


Рис.11.6. Вариант 8-элементной таблицы и маршрутов Гамильтона

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 К.

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.

Из таблицы символы считываются в порядке следования номеров элементов. Ниже приводится пример шифрования информации с использованием маршрутов Гамильтона.

Пусть требуется зашифровать исходный текст $T_0 = \langle \text{МЕТОДЫ_ПЕРЕСТАНОВКИ} \rangle$. Ключ и длина зашифрованных блоков соответственно равны: $K = \langle 2, 1, 1 \rangle$, $L = 4$. Для шифрования используются таблица и два маршрута, представленные на рис.11.5. Для заданных условий маршруты с заполненными матрицами имеют вид, показанный на рис.11.6.

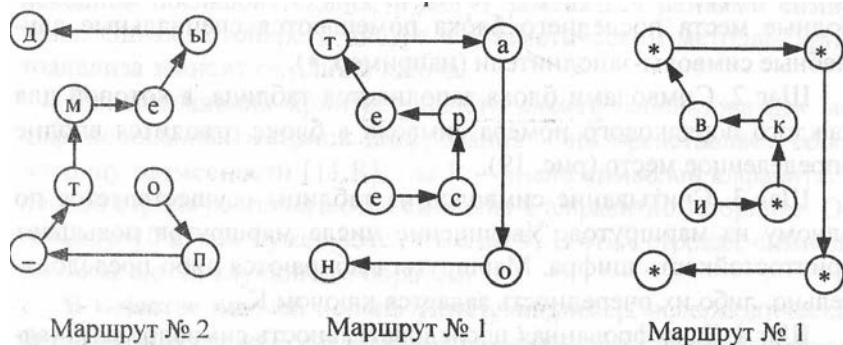


Рис.11.6. Пример шифрования с помощью маршрутов Гамильтона

Шаг 1. Исходный текст разбивается на три блока:

$B1 = \langle \text{МЕТОДЫ_П} \rangle$;

$B2 = \langle \text{ЕРЕСТАНО} \rangle$;

$B3 = \langle \text{ВКИ*****} \rangle$.

Шаг 2. Заполняются три матрицы с маршрутами 2,1,1 (рис.20).

Шаг 3. Получение шифртекста путем расстановки символов в соответствии с маршрута-ми.

$T_i = \langle \text{ОП_ТМЕЫДЕСРЕТАОНИ*КВ****} \rangle$.

Шаг 4. Разбиение на блоки шифртекста

$T_1 = \langle \text{ОП_Т М ЕЫД Е СРЕ Т А О Н И*К В ****} \rangle$.

В практике большое значение имеет использование специальных аппаратных схем, реализующих метод перестановок (рис.11.7).

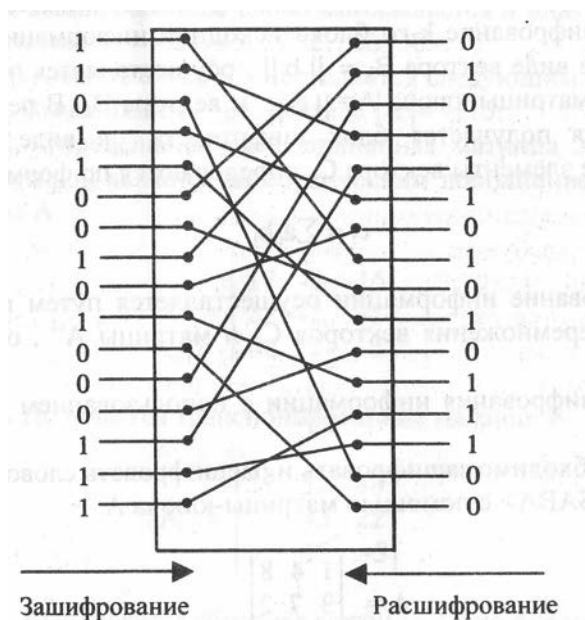


Рис.11.7. Схема перестановок

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 криптоаналитику для раскрытия шифра достаточно направить в систему шифрования $K-1$ блок тестовой информации, в которых все символы за исключением одного одинаковы.

11.1.3.3. 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 $B_k = \|b_j\|$, осуществляется путем перемножения матрицы-ключа $A = \|a_{ij}\|$ и вектора B_k . В результате перемножения получается блок шифртекста в виде вектора $C_k = \|c_i\|$, где элементы вектора C_k определяются по формуле:

$$c_i = \sum_j a_{ij} b_j.$$

Расшифрование информации осуществляется путем последовательного перемножения векторов C_k и матрицы A^{-1} , обратной матрице A .

Пример шифрования информации с использованием алгебры матриц.

Пусть необходимо зашифровать и расшифровать слово

$T_0 = \langle \text{ЗАБАВА} \rangle$ с помощью матрицы-ключа A :

$$A = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \end{vmatrix}$$

$$| 6 \ 9 \ 5 |$$

Для **зашифрования** исходного слова необходимо выполнить следующие шаги.

Шаг 1. Определяется числовой эквивалент исходного слова как последовательность соответствующих порядковых номеров букв слова T_3 :

$$T_3 = \langle 8, 1, 2, 1, 3, 1 \rangle.$$

Шаг 2. Умножение матрицы A на векторы $B_1 = \{8, 1, 2\}$ и $B_2 = \{1, 3, 1\}$.

$$C_1 = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \end{vmatrix} \cdot \begin{vmatrix} 8 \\ 1 \\ 2 \end{vmatrix} = \begin{vmatrix} 28 \\ 35 \end{vmatrix};$$

$$\begin{vmatrix} 6 & 9 & 5 \end{vmatrix} \cdot \begin{vmatrix} 2 \end{vmatrix} = \begin{vmatrix} 67 \end{vmatrix}$$

$$C_1 = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \end{vmatrix} \cdot \begin{vmatrix} 1 \\ 3 \\ 1 \end{vmatrix} = \begin{vmatrix} 21 \\ 26 \end{vmatrix}.$$

$$\begin{vmatrix} 6 & 9 & 5 \end{vmatrix} \cdot \begin{vmatrix} 1 \end{vmatrix} = \begin{vmatrix} 38 \end{vmatrix}$$

Шаг 3. Зашифрованное слово записывается в виде последовательности чисел $T_1 = \langle 28, 35, 67, 21, 26, 38 \rangle$.

Расшифрование слова осуществляется следующим образом.

Шаг 1. Вычисляется определитель $|A| = -115$.

Шаг 2. Определяется присоединенная матрица A^* , каждый элемент которой является алгебраическим дополнением элемента a_{ij} матрицы A

$$A^* = \begin{vmatrix} 17 & -3 & -15 \\ 52 & -43 & 15 \end{vmatrix}$$

$$\begin{vmatrix} -48 & 22 & -5 \end{vmatrix}$$

Шаг 3. Получается транспонированная матрица A

$$A^T = \begin{vmatrix} 17 & 52 & -48 \\ -3 & -43 & 22 \end{vmatrix}$$

$$\begin{vmatrix} -15 & 15 & -5 \end{vmatrix}$$

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 5. Определяются векторы B_1 и B_2 :

$$B_1 = A^{-1} C_1; \quad B_2 = A^{-1} C_2.$$

$$B_1 = \begin{vmatrix} 17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix} \cdot \begin{vmatrix} 28 \\ 35 \\ 67 \end{vmatrix} = \begin{vmatrix} 8 \\ 1 \\ 2 \end{vmatrix}$$

$$B_2 = \begin{vmatrix} 17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix} \cdot \begin{vmatrix} 21 \\ 26 \\ 38 \end{vmatrix} = \begin{vmatrix} 1 \\ 3 \\ 1 \end{vmatrix}$$

Шаг 6. Числовой эквивалент расшифрованного слова $T_3 = \langle 8, 1, 2, 1, 3, 1 \rangle$ заменяется символами, в результате чего получается исходное слово $T_0 = \langle \text{ЗАБАВА} \rangle$.

11.1.3.4. Аддитивные методы шифрования

Сущность аддитивных методов шифрования заключается в последовательном суммировании цифровых кодов, соответствующих символам исходной информации, с последовательно-

стью 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 π , e и других.

На практике самыми эффективными и распространенными являются аддитивные методы, в основу которых положено использование *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

$$T(i+1) = (a T(i) + c) \bmod m,$$

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 $a \bmod 4 = 1$ [39]: Такой генератор может быть сравнительно легко создан как аппаратными средствами, так и программно.

11.1.4. 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 потайной ход. Эти функции с параметром z обладают следующими свойствами. Для определенного z могут быть найдены алгоритмы E_z и D_z . С помощью E_z легко получить функцию $f(x)$ для всех x из области определения. Так же просто с помощью алгоритма D_z получается и обратная функция $x = f^{-1}(y)$ 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 $f^{-1}(x)$ при помощи вычислений невозможно даже при известном E_z . 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-Гамала и Мак-Элиса. В настоящее время наиболее эффективным и распространенным алгоритмом шифрования с открытым ключом

чом 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 :

$$n = p \cdot q.$$

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: $e \cdot d = 1 \pmod{f(p, q)}$.

Данное условие означает, что остаток от деления (вычет) произведения $e \cdot d$ 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: $L \geq \log_2(n+1)$. Каждый блок рассматривается как целое положительное число $X(i)$, принадлежащее интервалу $[0, n-1]$. Таким образом, исходная информация представляется последовательностью чисел $X(i)$, $i=1, I$. 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:

$$X(i) = (Y(i))^d \pmod{n}.$$

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 $n = 3 \cdot 11 = 33$.

Шаг 3. Определяется функция Эйлера

$$f(p, q) = (3-1) \cdot (11-1) = 20.$$

Шаг 4. В качестве взаимно простого числа выбирается число $d=3$.

Шаг 5. Выбирается такое число e , которое удовлетворяло бы соотношению: $(e \cdot 3) \pmod{20} = 1$. 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 n). Исходная информация в двоичном коде имеет вид:

$$000100000001001001.$$

Длина блока L определяется как минимальное число из целых чисел, удовлетворяющих условию: $L \geq \log_2(n+1) = \log_2(33+1)$, так как $n = 33$. Отсюда $L=6$. Тогда исходный текст представляется в виде кортежа $X(i) = \langle 4, 1, 9 \rangle$.

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 $Y(i) = \langle 16, 1, 15 \rangle$.

Шаг 8. Расшифровка сообщения $Y(i) = \langle 16, 1, 15 \rangle$ 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 $X(i) = \langle 4, 1, 9 \rangle$ заменяется исходным текстом «ГАЗ».

Система Эль-Гамала основана на сложности вычисления дискретных логарифмов в конечных полях [22]. Основным недостатком систем RSA и Эль-Гамала 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.

11.2. Стандарты шифрования

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 деление 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 А и В по 32 разряда. Слово А образуют младшие биты, а слово В - старшие биты блока. Эти слова подвергаются итерационной обработке с числом итераций равным $i=32$. Слово, находящееся на месте младших бит блока, (А на первой итерации) суммируется по $\text{mod } 2^{32}$ 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 заменяется на другой вектор (4 бита); полученные векторы объединяются в 32-разрядное слово, которое циклически сдвигается влево на 32 разряда и суммируется по $\text{mod } 2$ с другим 32-разрядным словом из 64-разрядного блока (слово В на первой итерации).

После выполнения первой итерации в блоке на месте младших бит будет расположено слово В, а слева преобразованное слово А.

На следующих итерациях операции над словами повторяются.

На каждой итерации i 32-разрядное слово ключа j (всего их 8) выбирается по следующему правилу:

$$j = \begin{cases} (i-1) \bmod 8, & \text{при } 1 \leq i \leq 24; \\ 32-i, & \text{при } i \geq 25; \\ 0, & \text{при } i=32. \end{cases}$$

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 k бит. Значение параметра k выбирается с учетом вероятности навязывания ложной информации P_H , которая связана с параметром k соотношением:

$$P_H = 1/2^k.$$

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 бита. Первый блок $T(1)$ 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 $T(2)$. Результат суммирования подвергается тем же итерационным преобразованиям, что и блок $T(1)$, а на завершающем этапе суммируется по mod 2 с третьим блоком $T(3)$. Эти действия повторяются для $m-1$ блоков исходной информации. Если последний блок $T(m)$ не полный, то он дополняется соответствующим числом нулей до 64 разрядов. Этот блок суммируется по mod 2 с результатом, полученным при обработке $T(m-1)$ блока, и подвергается преобразованию в соответствии с первыми 16-ю итерациями алгоритма простой замены. Из полученного 64-разрядного блока выделяется слово длиной k 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.

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 IBM. 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.

11.3. 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 криптостойкость 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?

Лекция 12. ЗАЩИТА ИНФОРМАЦИИ В РАСПРЕДЕЛЕННЫХ КС

Вопросы:

12.1. Архитектура распределенных КС и особенности ЗИ в РКС

12.3. Обеспечение ИБ в пользовательской подсистеме и специализированных коммуникационных КС

12.3. Защита информации на уровне подсистемы управления РКС

Литература:

1. Завгородний В.И. комплексная защита информации в компьютерных системах: Учебное пособие. – Логос, 201. – С.180-246.

12.1. Архитектура распределенных КС и особенности ЗИ в РКС

Под распределенными компьютерными системами 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.12.1).

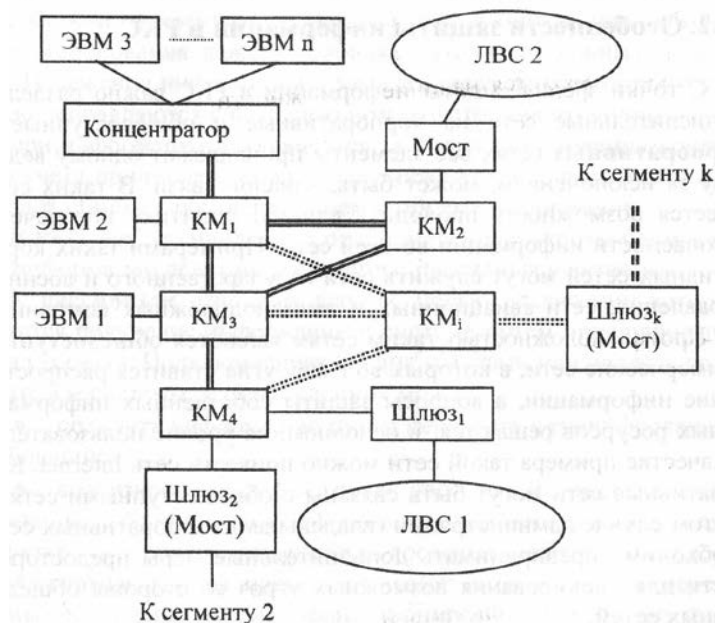


Рис.12.1. Фрагмент распределенной компьютерной системы

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 предназначена для удовлетворения потребностей пользователей в хранении, обработке и получении информации.

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.

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 ЗИ 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 отдельными абонентами, 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 несанкционированного доступа к информационным ресурсам удаленного объекта КС, осуществления несанкционированного изменения программной структуры КС путем внедрения вредительских программ.

Анализируя приведенные особенности потенциальных угроз ИБ в РКС, можно сделать вывод, что все они связаны с передачей информации по каналам связи, с территориальной разобщенностью объектов системы. Таким образом, в РКС наряду с мерами, предпринимаемыми для обеспечения ИБ в сосредоточенных КС, реализуется ряд механизмов дляЗИ 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;
- ЗИ на уровне подсистемы управления сетью;
- ЗИ в каналах связи;
- обеспечение контроля подлинности взаимодействующих процессов.

12.2. Обеспечение ИБ в пользовательской подсистеме и специализированных коммуникационных КС

Обеспечение ИБ 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 коммуникационные 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 относятся 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 полсети, 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 предназначены 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.

12.3. 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/IP** 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 TCP/IP насчитывается 5 уровней (рис.12.2).



Рис.12.2. Уровневые модели протоколов

Протокол X.25 позволяет обеспечить более надежное взаимодействие удаленных процессов. Достоинствами протокола TCP/IP являются сравнительно низкая стоимость и простота подключения к сети.

Задачи обеспечения безопасности информации в сети решаются на всех уровнях. Выполнение протоколов организуется с помощью подсистемы управления. Наряду с другими на уровне подсистемы управления решаются следующие проблемы защиты информации в РКС.

1. Создание единого центра управления сетью, в котором решались 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 графика (потока сообщений в сети), контроль соблюдения правил работы абонентами, оперативное реагирование на нарушения.

6. Организация восстановления работоспособности элементов сети при нарушении процесса их функционирования.

ЗИ 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 графику 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.

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 эффективнее, 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 межсетевого экран (Firewall) (рис.12.3). Как правило, межсетевой экран реализуется на выделенной ЭВМ, через которую защищенная РКС (ее фрагмент) подключается к общедоступной сети.



Рис.12.3. 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 выбора 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 агенты* (прокси-серверы), которые являются программами-посредниками и обеспечивают установление соединения между субъектом и объектом доступа, а затем пересылают информацию, осуществляя контроль и регистрацию. Дополнительной функцией экранирующего агента является сокрытие от субъекта

доступа истинного объекта. Действия экранирующего агента являются прозрачными для участников взаимодействия.

Функция *трансляции адресов* межсетевого экрана предназначена для скрытия от внешних абонентов истинных внутренних адресов. Это позволяет скрыть топологию сети и использовать большее число адресов, если их выделено недостаточно для защищенной сети.

Межсетевой экран выполняет *регистрацию событий* 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.

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 отправляет ее процессу B .

Шаг 2. Процесс B по секретному алгоритму вычисляет функцию $y = f(x)$ и отправляет 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 взаимодействия 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.12.4).

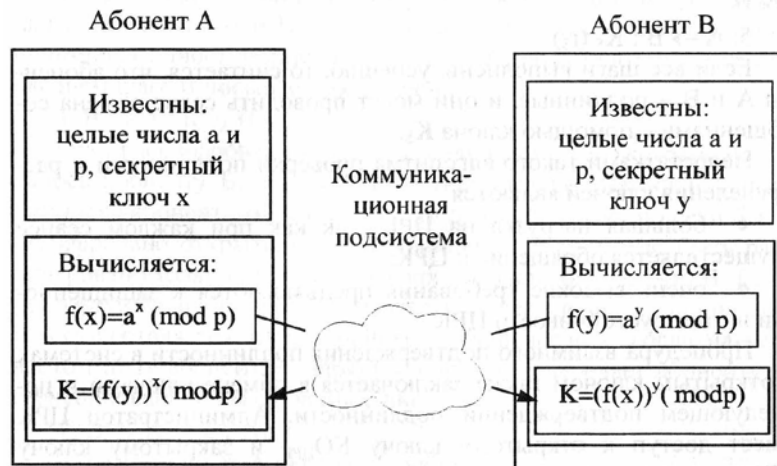


Рис.12.4. Схема получения секретного сеансового ключа K

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 распределения 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 случае организации прямого обмена сеансовыми ключами возникают сложности в проверке подлинности процессов или абонентов.

Распределение ключей совмещается с процедурой проверки 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 A , а вызываемый - через B . Оба процесса (абонента) имеют идентификаторы I_A и I_B . Абоненты имеют также мастер-ключи KM_A KM_B , известные только соответственно A и B , а также ЦРК. Мастер-ключи распределяются между абонентами вне РКС. Это может быть специальная почта, другие автоматизированные системы и т.п.

Абонент A посылает в ЦРК в открытом виде идентификатор I_A и зашифрованные на KM_A идентификатор I_B , случайное число r_1 и просьбу обеспечить связь с B [26]:

1. $A \rightarrow \text{ЦРК} : I_A, KM_A(I_B, r_1, \text{"Прошу установить связь с B"})$. По открытому идентификатору I_A соответствующая процедура обеспечивает выбор мастер-ключа KM_A , расшифровывает сообщение, а затем генерируется сеансовый ключ K_S и отсылается зашифрованное сообщение A :

2. $\text{ЦРК} \rightarrow A : KM_A(r_1, K_S, I_B, KM_B(K_S, I_A))$

Это сообщение может расшифровать только абонент A , имеющий ключ KM_A . Случайное число r_1 подтверждает, что полученное сообщение не является повторным, а выдано ЦРК в ответ на сообщение A . Абонент A оставляет у себя K_S , генерирует случайное число r_2 и отправляет сообщение абоненту B :

3. $A \rightarrow B : KM_B(K_S, I_A), K_S(r_2)$.

Сообщение может расшифровать только В. Полученный идентификатор I_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 K_S случайное число r_2 . Если используется односторонняя процедура подтверждения подлинности, то абонент В передает абоненту А сообщение:

4. $B \rightarrow A : K_S(f(r_2))$.

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 K_S . 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. $B \rightarrow A : K_S(r_2, r_3)$, где r_3 - случайное число.

В ответ А передает сообщение, подтверждающее его подлинность:

5. $A \rightarrow B : K_S(r_3)$.

Если все шаги выполнены успешно, то считается, что абоненты А и В - подлинны, и они могут проводить сеанс обмена сообщениями с помощью ключа K_S .

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 $KO_{ЦРК}$ и закрытому ключу $KЗ_{ЦРК}$, 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. $A \rightarrow ЦРК : I_A, I_B, \text{"Вышлите ключи"}$.

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. $ЦРК \rightarrow A : KЗ_{ЦРК}(KO_A, I_A), KЗ_{ЦРК}(KO_B, I_B)$.

Абонент А расшифровывает сообщение с помощью открытого ключа $KЗ_{ЦРК}$, который доставлен ему надежным путем. Полученные идентификаторы абонентов А и В подтверждают, что ЦРК правильно воспринял запрос и KO_B - открытый ключ абонента В.

На следующем шаге процедуры абонент А посылает абоненту В сообщение, в котором сгенерированное число r_1 и идентификатор I_A зашифрованы открытым ключом KO_B , а открытый ключ KO_A и идентификатор I_A зашифрованы закрытым ключом ЦРК.

3. $A \rightarrow B : KO_B(r_1, I_A), KЗ_{ЦРК}(KO_A, I_A)$.

Абонент В расшифровывает первую часть сообщения с помощью своего закрытого ключа $KЗ_B$, а вторую часть - с помощью открытого ключа $KO_{ЦРК}$. 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 $KЗ_{ЦРК}$. 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. $B \rightarrow A : KO_A(f(r_1))$.

Если расшифрованное число r_1 совпадает с тем, которое посылалось абоненту В, то абонент А получает подтверждение подлинности абонента В, так как число r_1 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 под-

линности, то осуществляется трехстороннее "рукопожатие". Тогда на четвертом шаге абонент В, наряду с числом r_1 , передает абоненту А сгенерированное им случайное число r_2 .

4. $B \rightarrow A : KO_A(r_1, r_2)$.

В ответ абонент А передает сообщение:

5. $A \rightarrow B : KO_B(r_2)$.

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 c и сервера s реализуется следующей последовательностью шагов.

1. Клиент $c \rightarrow$ Kerberos: $I_C, s_1, \text{timeexp}, r_1$.

Клиент c передает Kerberos в открытом виде свой идентификатор I_C , запрашиваемый сервис s_1 , срок годности билета timeexp и случайное число r_1 .

2. Kerberos \rightarrow клиент c : $K_C(K_{CS}, \text{timeexp}, r_1); K_S(K_{CS})$.

Kerberos возвращает сеансовый ключ K_{CS} , идентификатор сервера I_S , атрибуты timeexp и r_1 , зашифрованные ключом клиента, а также сеансовый ключ K_{CS} , зашифрованный ключом сервера c .

3. Клиент c - сервер s : $K_{CS}(I_C, ts, ck); K_S(K_{CS})$.

Клиент посылает серверу свой идентификатор I_C , временной штамп ts и контрольную сумму ck , зашифрованные сеансовым ключом, а также пересылает без изменений зашифрованный ключ $K_S(K_{CS})$, который называется билетом.

4. Сервер $s \rightarrow$ клиент c : $K_{CS}(I_S, ts)$.

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 K_{AB} полученный ранее (вне РКС). Процедура выполняется за три шага.

1. $A \rightarrow B : I_A, r_1$.

На первом шаге инициатор обмена абонент А передает в открытом виде абоненту В свой идентификатор I_A и случайное число r_1 . Это сообщение могло быть послано любым абонентом сети.

2. $B \rightarrow A : K_{AB}(f(r_1), I_B, r_2, K_S)$.

На шаге 2 абонент В генерирует случайное число r_2 и сеансовый ключ K_S , посылает А сообщение, зашифрованное общим секретным ключом K_{AB} . Абонент может быть уверен, что сообщение пришло от В, т. к. только ему известен ключ K_{AB} . Функция $f(r_1)$ подтверждает, что сообщение получено в ответ на сообщение 1, а не является повтором старого сообщения.

3. $A \rightarrow B : K_S(f(r_2))$.

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. $A \rightarrow B : KO_B(r_1, I_A)$.

На первом шаге абонент зашифровывает сообщение для В с помощью открытого ключа КОВ. Случайное число r_1 и идентификатор абонента А может прочесть только абонент В с помощью секретного личного ключа.

2. $B \rightarrow A : KO_A(f(r_1), r_2, I_B, K_S)$.

На втором шаге абонент вычисляет функцию $f(r_1)$, генерирует случайное число r_2 и сеансовый ключ K_S и зашифровывает все сообщение с помощью открытого ключа абонента А. Абонент А делает вывод, что сообщение 1 получено абонентом В.

3. $A \rightarrow B : K_S(f(r_2))$.

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.

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 представляемых 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-Гамала 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-Гамала 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 $0 < x < p-2$. Число k генерируется в процессе получения подписи сообщения, является секретным и должно быть уничтожено после выработки подписи.

Упрощенный алгоритм процедуры выработки подписи включает следующие шаги.

1. Вычисление хэш-функции $h(M)$ от сообщения M .
2. Получение целого числа k , $0 < k < p-1$.
3. Вычисление значений $r = a^k \pmod{p}$ и $r' = r \pmod{g}$. Если $r' = 0$, перейти к шагу 2.
4. Вычисление значения $s = (xr' + kh \pmod{p}) \pmod{g}$. Если $s = 0$, то переход к шагу 2, иначе

конец работы алгоритма. Цифровой подписью сообщения M является вектор $\langle r' \rangle_{256} \| \langle s \rangle_{256}$, 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: $0 < s < g$ и $0 < r' < g$. Если хотя бы одно условие не выполнено, то подпись считается недействительной.
2. Определяется хэш-функция $h(M_1)$ от полученного сообщения M_1 .
3. Вычисляется значение $v = (h(M_1))^{g-2} \pmod{g}$.
4. Вычисляются значения $z_1 = sv \pmod{g}$, $z_2 = (g-r')v \pmod{g}$.
5. Вычисление значения $u = (a^{z_1} y^{z_2} \pmod{p}) \pmod{g}$.
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.

Особенности защиты информации в базах данных. БД 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 **СУБД** понимаются программные или аппаратно-программные средства, реализующие функции управления данными, такие как: просмотр, сортировка, выборка, модификация, выполнение операций определения статистических характеристик и т.п. БД размещаются:

- на компьютерной системе пользователя;
- на специально выделенной ЭВМ (сервере). Как правило, на компьютерной системе пользователя размещаются личные или персональные БД, которые обслуживают процессы одного пользователя.

В вычислительных сетях БД 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 БД проще решаются проблемы ЗИ от преднамеренных угроз, поддержания актуальности и непротиворечивости данных. Достоинством распределенных БД, при условии дублирования данных, является их высокая защищенность от стихийных бедствий, аварий, сбоев технических средств, а также диверсий.

ЗИ в БД, 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 БД 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 БД 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. Современные СУБД обеспечивают такую логическую целостность и непротиворечивость на этапе описания модели данных.

В БД, работающих с конфиденциальной информацией, необходимо дополнительно использовать криптографические средства ЗИ. 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 БД. 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 БД необходимо учитывать ряд специфических угроз ИБ, связанных с концентрацией в БД большого количества разнообразной информации, а также с возможностью использования сложных запросов обработки данных. К таким угрозам относятся:

- инференция;
- агрегирование;
- комбинация разрешенных запросов для получения закрытых данных.

Под инференцией понимается получение конфиденциальной информации из сведений с меньшей степенью конфиденциальности 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 получают 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 БД. 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 опера-

ции 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 информацию 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 БД;
- 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 БД 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 БД 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.) к элементам БД (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 ЗИ в БД 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 ЗИ в РКС.
2. Каким образом обеспечивается ЗИ в пользовательских подсистемах и специализированных коммуникационных КС?
3. Приведите основные особенности ЗИ в подсистемах распределенных КС.
4. В чем заключается сущность межсетевое экранирования?
5. Охарактеризуйте ЗИ в базах данных.

III. ПОСТРОЕНИЕ И ОРГАНИЗАЦИЯ ФУНКЦИОНИРОВАНИЯ КСЗИ В КС

Лекция 13. ПОСТРОЕНИЕ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Вопросы:

- 13.1. Концепция создания защищенных КС
- 13.2. Методология проектирования КСЗИ
- 13.3. Моделирование КСЗИ

Литература:

1. Завгородний В.И. комплексная защита информации в компьютерных системах: Учебное пособие. – Логос, 201. – С.211-228.

13.1. 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 информа-

ции: 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.13.1).

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.

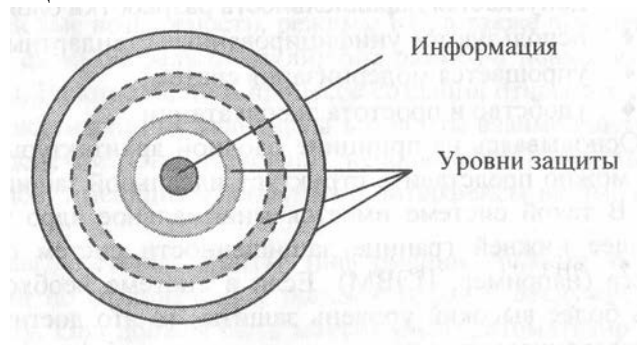


Рис.13.1. Многоуровневая КСЗИ

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 развивающимися 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.

13.2. Методология проектирования КСЗИ

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.

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.13.2).

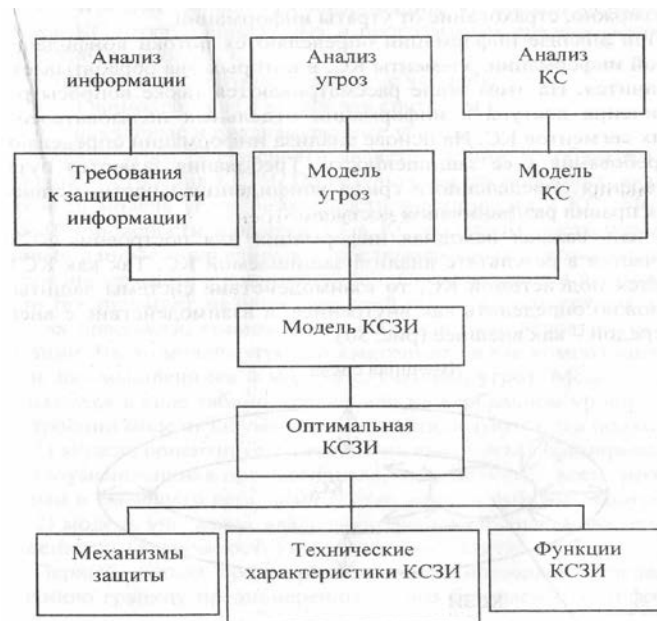


Рис.13.2. Последовательность и содержание научно-исследовательской разработки КСЗИ

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.

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.13.3).

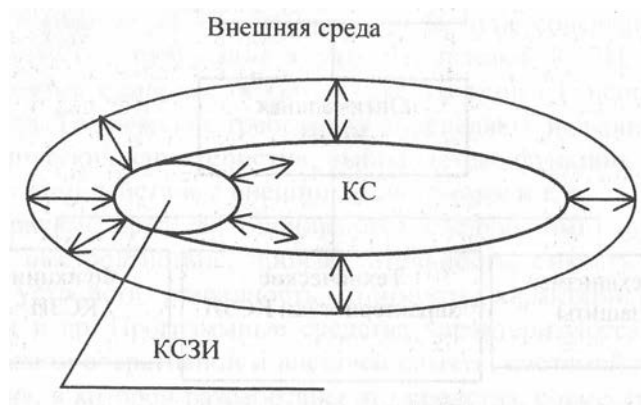


Рис.13.3. Схема взаимодействия КСЗИ

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.

13.3. 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, разностные 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:

- *специальные методы неформального моделирования;*
- *декомпозиция общей задачи на ряд частных задач;*
- *макромоделирование.*

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 принципов 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 решений 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, развивающийся 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 преодоления 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 отсекаания 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 получают 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.

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:

$$P(t) = 1 - P_{\text{отк}}(t),$$

где $P_{\text{отк}}(t)$ - вероятность отказа системы за время t .

Величина $P_{\text{отк}}(t)$, в свою очередь, определяется в соответствии с известным выражением:

$$P_{\text{отк}}(t) = e^{-\lambda t},$$

где λ - 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:

$$T = A^S t/2,$$

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 оп-

тимизации комплексной системы защиты приходится всякий раз учитывать общий лимит веса оборудования.

3. Макро моделирование. При оценке сложных систем используется также макро моделирование. Такое моделирование осуществляется для общей оценки системы. Задача при этом упрощается за счет использования при построении модели только основных характеристик. К макро моделированию прибегают в основном для получения предварительных оценок систем.

В качестве макро модели можно рассматривать модель КСЗИ, представленной на рис.30. Если в КСЗИ используется k 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 k уровней защиты, чтобы получить доступ к информации. Для такого злоумышленника вероятность получения несанкционированного доступа к информации $P_{НСД}$ может быть рассчитана по формуле:

$$P_{НСД} = \prod_{i=1}^k P_i,$$

где P_i - вероятность преодоления злоумышленником i -го уровня защиты.

На макро уровне 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.

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 макро моделирования.
5. Выполните сравнительный анализ подходов к оценке эффективности КСЗИ.

Лекция 14. ПРОЕКТИРОВАНИЕ КОМПЛЕКСНЫХ СЗИ

Вопросы:

- 14.1. Выбор показателей эффективности и критериев оптимальности КСЗИ
- 14.2. Математическая постановка задачи разработки КСЗИ и ее оценки
- 14.3. Этапы создания организационной структуры КСЗИ

Литература:

1. Завгородний В.И. комплексная защита информации в компьютерных системах: Учебное пособие. – Логос, 201. – С.228-246.

14.1. 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 ;

$$y_k = f(x_1, x_2, \dots, x_n), \quad k=\overline{1, K}, \quad n=\overline{1, N},$$

где K - мощность множества показателей эффективности системы,

N - мощность множества характеристик системы.

Характеристиками системы x_1, x_2, \dots, 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 k 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:

$$P_{H3} = P_{H3}^{max},$$

при $C < C_{ооп}$, $G < G_{ооп}$,

где P_{H3} - вероятность не преодоления злоумышленником системы защиты за определенное время,

C 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 Y_1 .

Определяется допустимая величина изменения показателя Y_1 , которая называется уступкой. Измененная величина показателя:

$$Y_1 = Y_1 \pm \Delta_1 \quad (\Delta_1 - \text{величина уступки}) \text{ фиксируется.}$$

Определяется оптимальная величина показателя Y_2 при фиксированном значении Y'_1 , выбирается уступка Δ_2 и процесс повторяется до получения Y_{K-1} .

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_{Π}, Z_C). Показатели, используемые в обобщенных показателях, называют *частными* (y_i, y_j).

Если в произведение (сумму) включается часть показателей, то остальные частные показатели включаются в ограничения. Показатели, образующие произведение (сумму), могут иметь весовые коэффициенты k_i (k_j). В общем виде эти методы можно представить следующим образом:

$$Z_{\Pi} = \text{extr} \prod_i k_i y_i; \quad Z_C = \text{extr} \sum_j k_j y_j$$

4. Оценка эффективности СЗИ может осуществляться также **методом Парето**. Сущность метода заключается в следующем. При использовании p показателей эффективности системе соответствует 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.

14.2. Математическая постановка задачи разработки КСЗИ и ее оценки

После выбора показателей эффективности и критерия эффективности может быть осуществлена математическая постановка задачи разработки КСЗИ. На этом этапе уже известны:

- $F = \{f_1, f_2, \dots, f_n\}$ - функции, которые должна выполнять КСЗИ;
- $M = \{m_1, m_2, \dots, m_k\}$ - возможные механизмы защиты;
- $U = \{u_1, u_2, \dots, u_p\}$ - способы управления КСЗИ.
- $Y = \{y_1, y_2, \dots, y_w\}$ - показатели эффективности КСЗИ;

Показатели эффективности зависят от выполняемых функций, механизмов защиты и способов управления КСЗИ: $Y = \Phi(F, M, U)$.

Критерий эффективности получается с использованием показателей эффективности: $K = E(Y)$. Тогда математическая постановка задачи разработки КСЗИ в общем случае может быть представлена в следующем виде:

найти $\text{extr} S(F, M^*, U^*)$, при $M^* \in M, U^* \in U$, которым соответствуют $Y^* \in Y_d$, где Y_d - множество допустимых значений показателей эффективности КСЗИ.

То есть, требуется создать или выбрать такие механизмы ЗИ 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 КСЗИ.

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*.

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.

2. Официальный подход. Большую практическую значимость имеет подход к определению эффективности КСЗИ, который условно можно назвать официальным. Политика безопасности ИТ 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 ЗИ, которые необходимо иметь в КС, чтобы она соответствовала определенному классу защиты. Используя такие документы, 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 Defense 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 A (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 B (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 C (избирательная защита) представляет избирательную защиту подсистем с контролем доступа к ним пользователей. В этой группе выделены классы безопасности *C1* и *C2*.

Класс C1 (избирательная защита информации) предусматривает разделение в КС пользователей и данных. Этот класс обеспечивает самый низкий уровень защиты КС.

Класс C2 (защита через управляемый или контролируемый доступ) обеспечивается отдельным доступом пользователей к данным.

Группу D (минимальной безопасности) составляют КС, проверенные на безопасность, но которые не могут быть отнесены к классам *A, B* или *C*.

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 *E0* до *E6*.

В РФ 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 (таблица 14.1). Самый низкий класс - седьмой, самый высокий - первый.

Таблица 14.1. 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.

Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты:

- 1 группа содержит только один седьмой класс;
- 2 группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
- 3 группа характеризуется мандатной защитой и содержит 4, 3 и 2 классы;
- 4 группа характеризуется верифицированной защитой и содержит только 1 класс.
- 7 класс присваивают СВТ, к которым предъявлялись требования по защите от НСД к информации, но при оценке защищенности 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 таблице 14.2.

Таблица 14.2. Требования к защищенности автоматизированных систем

Подсистемы и требования									
	ЗБ	ЗА	ЗБ	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				+		+	+	+	+
- 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 субъектам 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 ВТ 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 1В.

В подсистеме управления доступом АС 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 обеспечения;
- 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 ТС и специального персонала, строгий пропускной режим, специальное оборудование помещений АС;
- наличие администратора (службы) ЗИ, 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 ИС с применением ЭВМ общего пользования (main frame) и мини-ЭВМ. Для персональных ЭВМ (ПК) и локальных сетей ПК требования безопасности должны быть несколько иными. Такие требования изложены [42] в стандарте The Trusted Network Interpretation of Department of Defense 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.

3. Экспериментальный подход. Под экспериментальным подходом понимается организация процесса определения эффективности существующих КСЗИ путем 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.)

14.3. Этапы создания 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 объектах 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 этом 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 ЗИ, которые представляют собой действия, выполняемые сотрудниками служб безопасности, органов ОБИ, обслуживающим персоналом и пользователями, 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 СЗИ 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.15.2.

Имея полный перечень организационных мероприятий защиты и зная их характеристики, можно определить в общих чертах организационно-штатную структуру подразделения ОБИ. Организационно-штатная структура подразделения ОБИ уточняется в процессе анализа степени автоматизации системы защиты, а также режимов функционирования КС. При этом решается

вопрос о 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 пульта 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 макро моделирования.
5. Выполните сравнительный анализ подходов к оценке эффективности КСЗИ.

Лекция 15. ОРГАНИЗАЦИЯ ФУНКЦИОНИРОВАНИЯ КОМПЛЕКСНЫХ СЗИ

Вопросы:

15.1. Организация доступа к ресурсам КС

15.2. Обеспечение целостности и доступности информации в КС

15.3 Техническая эксплуатация КСЗИ

Литература:

1. Завгородний В.И. комплексная защита информации в компьютерных системах: Учебное пособие. – Логос, 201. – С.246-258.

15.1. Организация доступа к ресурсам КС

Функционирование комплексных систем защиты информации (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.15.1).

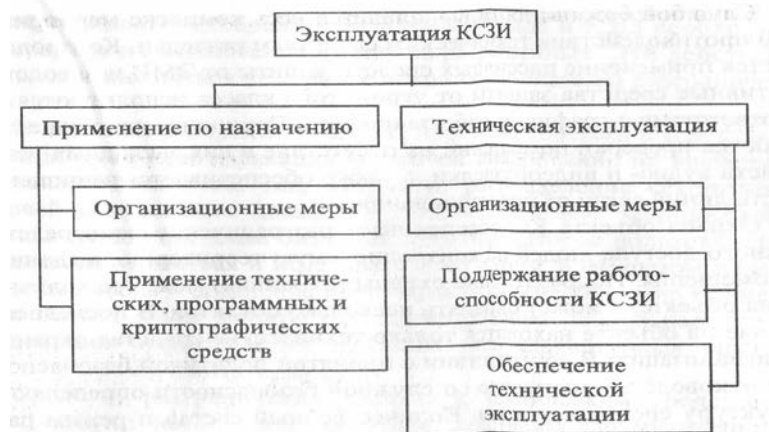


Рис. 15.1. Содержание процесса эксплуатации КСЗИ

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*.

Права должностных лиц по доступу к ресурсам КС **устанавливаются руководством организации**, в интересах которой используется КС.

Каждому должностному лицу определяются:

- технические ресурсы для использования (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 обеспечение безопасности информации (ОБИ) в компьютерной системе (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 видео-разведки, а также обеспечивается защищенность линий связи от прослушивания.

Охрана объекта в КСЗИ 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 неправомерных 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 ме-

ры 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

- *шифрование файлов*, хранящихся на внешних запоминающих устройствах,
- *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 неправомерных 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.

Дежурный администратор

- 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.

15.2. 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.

Дублирование информации является одним из главных условий обеспечения целостности и доступности информации в КС. *Стратегия* дублирования выбирается с учетом важности информации, требований к непрерывности работы КС, трудоемкости восстановления данных. Дублирование информации обеспечивается дежурным администратором КС.

Повышение отказоустойчивости КС обеспечивается с помощью

- 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.

Противодействие перегрузкам и "зависаниям" системы. В сложных КС практически невозможно избежать ситуаций, приводящих к перегрузке и "зависаниям" систем или их фрагментов. В результате сбоев аппаратных или программных средств, алгоритмических ошибок, допущенных на этапе разработки, ошибок операторов в системе происходят заикливания программ, непредусмотренные остановки 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.

Использование строго определенного множества программ. В защищенной КС используется 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, расположенных 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 хеширования (стартовый вектор хеширования).

Контроль состава программного обеспечения и целостности (неизменности) программ осуществляется

- при плановых проверках комиссиями и должностными лицами, а также
- дежурным оператором 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.

Контроль целостности информации. 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.

Обусловлено это тем, что на время проведения таких специальных работ отключаются (или находятся в неработоспособном состоянии) многие технические и программные средства защиты, а их отсутствие компенсируется системой организационных мероприятий:

- *подготовки КС* к выполнению работ;
- *допуска* к выполнению работ только *специалистов*;
- *четкой организацией работ* на объекте;
- *завершением работ*.

Подготовка КС к проведению работ по ее техническому обслуживанию, восстановлению работоспособности, ликвидации аварий и модернизации состоит в выполнении следующих шагов:

- отключить фрагмент КС, на котором необходимо выполнять работы, от функционирующей КС;
- снять носители информации с устройств;
- стереть информацию 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. Они должны 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 невозможности 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.

Четкая организация работ на объекте. 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.

Завершением работ. 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 оформляются 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.

15.3 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. Приведем 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.

Организация дежурства предназначено для непрерывного выполнения организационных мер защиты, и эксплуатации всех механизмов защиты. 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 кадрами – это работа с обслуживающим персоналом и пользователями. По сути она сводится к

- к подбору кадров,
- их обучению,
- воспитанию,
- к созданию условий для высокоэффективного труда.

Работа с документами. 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.

Поддержание работоспособности КСЗИ 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;
- безопасность 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.

Безопасность эксплуатации нацелена на важно обеспечение безопасности 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?

ЗАКЛЮЧЕНИЕ

Опыт показывает, что для достижения удачных решений по ИБ необходимо сочетание правовых, организационных и технических мер. Это сочетание определяется конфиденциальностью защищаемой информации, характером опасности и наличием средств защиты. Общие меры защиты необходимо применять комплексно, не упускать ни одну из них нельзя. Каждая мера дополняет другую, и недостаток или отсутствие любого способа приведет к нарушению защищенности объекта.

Работы по комплексной СЗИ (КСЗИ) включают в себя следующие этапы:

- анализ состава и содержания конфиденциальной информации, циркулирующей на конкретном объекте защиты;
- анализ ценности информации для предприятия (организации) с позиций возможного ущерба от ее получения конкурентами;
- оценка уязвимости информации, доступности ее для средств злоумышленника;
- исследование действующей СЗИ на объекте;
- оценка затрат на разработку новой (или совершенствование действующей) системы;
- организация мер ЗИ;
- закрепление персональной ответственности за ЗИ;
- реализация новой технологии ЗИ;
- создание обстановки сознательного отношения к ЗИ;
- контроль результатов разработки и прием в эксплуатацию новой системы защиты.

Изложенные этапы можно считать типовыми для процесса разработки комплексной СЗИ, так как они в значительной мере охватывают практически весь объем работ на организационном уровне.

Исходным шагом, направленным на развертывание работ по созданию или совершенствованию КСЗИ, является разработка приказа руководителя организации (предприятия) на проведение работ с указанием конкретного должностного лица, ответственного за создание СЗИ в целом. В приказе излагаются цели и задачи создания КСЗИ в данной организации, определяются этапы и сроки их выполнения, назначаются конкретные должностные лица, ответственные за отдельные этапы, отдельные виды работ, а также определяется подразделение или временный творческий (научно-технический) коллектив, который будет вести работы по созданию (совершенствованию) системы. Если к работе по созданию КСЗИ будут привлекаться сторонние организации, в приказе оговаривается способ взаимодействия с ними, а также даются необходимые поручения по его обеспечению.

В соответствии со сложившейся практикой разработки сложных систем устанавливаются следующие стадии:

- предпроектирование работ (обследование и разработка технического задания);
- проектирование (разработка технического, рабочего или технорбочего проектов);
- ввод КСЗИ в эксплуатацию.

Окончательное решение о стадийности проектирования разработки КСЗИ определяется на стадии предпроектных работ при разработке ТЗ исходя из производственно-технических условий, экономических возможностей, особенностей КСЗИ и используемых технических средств.

В ходе выполнения работ формируется:

- проектная документация - технический, рабочий или технорбочий проект (этап реализации технологии КСЗИ);
- организационно-распорядительная документация (разрабатывается по всем этапам).

Одной из ответственных работ является обследование объекта защиты. На этой стадии:

- определяется категория объекта с позиций степени конфиденциальности его информации по важности, ценности и секретности;
- обследуются все информационные потоки по виду и важности информации;
- оцениваются режимы и технология обработки, передачи и хранения подлежащей защите информации;

- оцениваются технические средства обработки информации на всем технологическом цикле на предмет их опасности и наличия ПЭМИН;
- определяются состав и содержание организационных, организационно-технических и технических мер, реализующих защитные мероприятия.

В результате проведения этих работ должны быть разработаны: информационная модель организации, структура информационных потоков, классификаторы потенциальных каналов утечки информации и аналитический обзор действующей системы защиты с оценкой ее эффективности, надежности и обеспечения ею необходимой безопасности.

Комплексный анализ полученных результатов в сочетании с инструментальным обследованием ТС обработки информации с использованием контрольно-измерительной аппаратуры позволит выявить возможные каналы утечки информации за счет ПЭМИН, оценить способы несанкционированного доступа к техническим средствам и документам.

На этапе разработки определяются организационно-функциональная схема КСЗИ, порядок и правила заботы сотрудников в новых условиях. Предлагаемый к внедрению проект КСЗИ подлежит изучению руководством организации и последующей его защите. После этого принимается решение о внедрении разработки в практику деятельности организации. Эту работу обычно выполняет группа ревизии, приема и контроля.

По завершении всех конструкторских работ КСЗИ принимается в опытную эксплуатацию.

Опытная эксплуатация КСЗИ имеет целью отработку взаимодействия подразделений и служб в условиях новой технологии, отладку технологического процесса обработки информации и проверку соответствия реализованных решений требованиям технического проекта. Опытная эксплуатация проводится на реальных информационных потоках в соответствии с установленным регламентом.

Завершающей стадией является прием КСЗИ в промышленную эксплуатацию. Для этого создается специальная приемная комиссия. Комиссия составляет акт приемки, в котором дается характеристика средствам и мерам защиты, фиксируется их полнота и достаточность, обеспечивающая требуемую степень безопасности. Акт утверждается руководством. На основании акта готовится приказ по организации на ввод КСЗИ в промышленную эксплуатацию.

Порядок действий по обеспечению безопасности информации с детальным изложением решаемых вопросов, ответственности по их решениям, необходимых мероприятий, учитывающих специфические особенности и содержание конкретных разрабатываемых документов по основным этапам разработки КСЗИ, описывается в нормативных документах защищаемого объекта.

Независимо от того, насколько хорошо разработаны технические и организационные меры безопасности, они, в конце концов, основываются на человеческой деятельности, в которой возможны ошибки и злой умысел. Если отдельный сотрудник обманет доверие, то никакая система безопасности и секретности не сможет предотвратить неправомерное овладение информацией.

Для обеспечения уверенности в том, что на защищаемом объекте успешно работает КСЗИ, применяются различные методы проверки. Это регулярные независимые инспекции и ревизии, а также проверочные комиссии, включающие представителей всех участвующих в работе с конфиденциальной информацией.

Так как ни одна из форм не является идеальной, то общий контроль за деятельностью системы защиты и ее функционированием должен осуществлять высший орган руководства организации (предприятия) через специальные подразделения обеспечения безопасности.

Оценка эффективности защиты должна осуществляться в соответствии с принципом комплексности и включать:

- установление на основе комплексного подхода состава проверяемых мер и средств: воспрещения, исключения несанкционированного доступа, режим;
- проверку организационно-режимных мероприятий;
- проверку категории объекта;
- проверку эффективности защиты информации;

- проверку воспреещения несанкционированного доступа;
- составление акта комплексной проверки;
- разработку рекомендаций по совершенствованию защиты (устранению установленных в процессе контроля недостатков).

На конкретных объектах при контроле эффективности ИБ, обеспечиваемой КСЗИ, может иметь место значительное разнообразие задач проверки. Так, на одном объекте может быть достаточно осуществить проверку эффективности экранирования, на другом - проверить эффективность шумовой защиты, а на третьем - необходимо убедиться, что излучения ПЭМИН могут быть приняты за пределами охраняемой территории организации (предприятия). То же имеет место и при проверке эффективности ЗИ от несанкционированного доступа (НСД): на этом объекте используется, например, монополярный режим обработки подлежащей ЗИ, а на другом - программная СЗИ. Все это означает, что работа по контролю эффективности защиты должна начинаться с определения состава проверяемых мер и средств. Кроме того, организационно-режимные средства и мероприятия должны иметь преимущественное значение по отношению к другим мерам и средствам защиты, поскольку их состав и эффективность оказывают определяющее действие на эффективность защиты от НСД. Это связано с тем, что при неправильном определении степени конфиденциальности защищаемой информации может оказаться неэффективным как воспреещение, так и защита от НСД. Иначе говоря, необходимо начинать контроль эффективности защиты с контроля организационно-режимных мер и средств защиты. Далее последовательность проверки может быть произвольной. Работы по проверке эффективности противодействия и защиты от НСД проводятся параллельно, поскольку на практике могут осуществляться только разными группами специалистов.

Организация и проведение контроля организационных мероприятий осуществляется с целью выявления нарушений требований соответствующей инструкции по обеспечению режима, которая действует на данном объекте, а также того, как данная инструкция и действующие по ней исполнители предотвращают возникновение нарушений. При подготовке к проверке целесообразно на основе анализа составить перечень возможных нарушений, что может оказать существенную помощь в организации контроля.

Эффективность защиты объекта обеспечивается, как известно, в соответствии с категорией его важности. В свою очередь, категория важности определяется в соответствии с грифом защищаемой информации. Поэтому после проведения организационно-режимных мероприятий (работ по проверке точности установления грифа защищаемой информации) можно провести проверку правильности категорирования объекта. Если при этом категория объекта оказалась неправильно определенной (заниженной), а защита на объекте реализована в точном соответствии с категорией, то защиту следует считать неэффективной.

Контроль эффективности ИБ от утечки за счет ПЭМИН предусматривает проведение работ с использованием определенной контрольно-измерительной аппаратуры в соответствии с существующими методиками. Этот контроль имеет целью определить наличие каналов утечки информации и их уровень за пределами охраняемой территории объекта.

Особое внимание при оценке эффективности системы защиты ТС необходимо обратить на их надежность и безотказность. При их эксплуатации имеют место поломки, сбои, отказы, вследствие чего они не обеспечивают выполнение задачи защиты. Отсюда задача обеспечения надлежащей надежности ТС обретает значительную важность, так как уровень, качество и безопасность защиты находятся в прямой зависимости от надежности технических средств.

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
ЗИ – защита информации
ЗУ - запоминающее устройство
ИБ – информационная безопасность
КМ - коммуникационный модуль
КПП - контрольно-пропускной пункт
КС - компьютерная система
КСЗИ - комплексная система защиты информации
ЛВС - локальная вычислительная сеть
НИС - несанкционированное изменение структур
НСД - 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

СПИСОК ЛИТЕРАТУРЫ

1. Основная:

1. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. – М.: Логос, 2001. – 264с.
2. Нечаев В.И. Основы теории защиты информации. – М.: Наука, 2001. – 212с.
3. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. – М.: Академический проект; Гаудеамус, 2004, - 544с.

2. Дополнительная:

4. Варфоломеев А., Пеленицын М. Методы криптографии и их применение в банковских технологиях. - М.: МИФИ, 1998.
5. Государственный стандарт Российской Федерации ГОСТ Р 50922-96. Защита информации. Основные термины и определения. Издание официальное Госстандарта России. – М.: Госстандарт РФ, 1996.
6. Девянин П.Н., Михальский Д.И., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности /Уч. пособие для вузов. – М.: Радио и связь, 2000. – 192с.
7. Доктрина информационной безопасности РФ. – М.: Госстандарт РФ, 2000.
8. Жельников В. Криптография от папируса до компьютера. – М.: АБФ, 1997.
9. Закон РФ "О государственной тайне" № 5486-1 от 21 июля 1993г.
10. Закон РФ "Об информации, информатизации и защите информации" № 24-ФЗ от 20 февраля 1995 г.
11. Зегжда П. и др. Теория и практика обеспечения информационной безопасности. – М.: Яхтсмен, 1998.
12. Зегжда Д., Ивашко А. Как построить защищенную информационную систему. –СПб.: Мир и семья, 1999.
13. Зима В., Молдовян А., Молдовян Н. Компьютерные сети и защита передаваемой информации. – СПб.: СПбГУ, 1998.
14. Мельников В. Защита информации в компьютерных системах. – М.: Финансы и статистика, 1997. – 157с.
15. Николаев Н. Проектирование защищенных информационных технологий. Часть первая. Введение в проблему проектирования распределенных вычислительных систем. – СПб.: СПбГТУ, 1997. – 312 с.
16. Пашков Ю., Казеннов В. Организация защиты информации от несанкционированного доступа в автоматизированных системах. - СПб.: Лаборатория ППШ, 1998.
17. Расторгуев С. Программные методы защиты информации в компьютерах и сетях. - М.: Яхтсмен, 1998.
18. Расторгуев С. Информационная война. - М.: Радио и связь, 1998. - 416с.
19. Сборник руководящих документов Гостехкомиссии РФ. – М.: ГТК, 1996.
20. Трубачев А.П. и др. Оценка безопасности информационных технологий. - М.: Издательство СИП РИА, 2001. - 356с.

ПРИЛОЖЕНИЯ

Приложение 1. Календарно-тематический план изучения дисциплины

"ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ"

П1.1. План лекций

Номер			Разделы, темы и основные вопросы лекции
не- дели	лек- ции	темы по РІ	
I. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ ИБ			
23	1	1	<u>Объект и предмет защиты. Цели и задачи дисциплины ИБ</u> 1.1. Объект и предмет защиты 1.2. Обоснование функций и задач защиты информации на государственном уровне 1.3. Цели и задачи дисциплины
24	2	1	<u>Концептуальная модель информационной безопасности (ИБ)</u> 2.1. Основные руководящие нормативные документы, касающиеся государственной тайны и ИБ 2.2. Основные положения систем защиты информации (СЗИ) 2.3. Концептуальная модель ИБ
25	3	1	<u>Угрозы конфиденциальной информации</u> 3.1. Анализ и оценки угроз конфиденциальной информации 3.2. Возможные виды нарушений ИБ и классификация противников («нарушителей») 3.3. Действия, приводящие к неправомерному овладению конфиденциальной информацией
II. МЕТОДЫ И СРЕДСТВА КОМПЬЮТЕРНЫХ СЗИ			
26	4	2	<u>Направления обеспечения ИБ</u> 4.1. Организационно-правовые аспекты ИБ 4.2. Инженерно-техническая защита 4.3. Программно-аппаратная защита информации
27	5	2	<u>Системы защиты информации (СЗИ) от случайных угроз</u> 5.1. Принципы защиты от случайных угроз 5.2. Программно-аппаратные методы защиты от случайных угроз 5.3. Минимизация ущерба от аварий и стихийных бедствий
28	6	2	<u>СЗИ от традиционного шпионажа и диверсий</u> 6.1. Система охраны объектов 6.2. ЗИ от утечки по техническим каналам 6.3. Противодействие НСД к источникам конфиденциальной информации
29	7	2	<u>СЗИ от электромагнитных излучений и закладок</u> 7.1. Пассивные методы защиты от побочных электромагнитных излучений и наводок (ПЭМИН) 7.2. Активные методы защиты от ПЭМИН 7.3. Средства выявления и защиты от ПЭМИН
30	8	2	<u>ЗИ от несанкционированного изменения структур</u> 8.1. Общие требования к защищенности КС от несанкционированного изменения структур 8.2. Защита от программных и аппаратных закладок 8.3. Защита от несанкционированного изменения структур КС в процессе эксплуатации
31	9	2	<u>ЗИ от несанкционированного доступа (НСД)</u> 9.1. Система разграничения доступа к информации в компьютерных системах 9.2. Требования к системам и средствам ЗИ от НСД 9.3. Защита программных средств от копирования и исследования
26	10	2	<u>Компьютерные вирусы (КВ) и механизмы борьбы с ними</u> 10.1. Сущность и классификация компьютерных вирусов. 10.2. Методы и средства борьбы с компьютерными вирусами. 10.3. Профилактика заражения КВ и действия пользователя при заражении ЭВМ вирусами
27	11	2	<u>Принципы криптографической ЗИ и ее применение в КС</u> 11.1. Классификация методов криптографического преобразования информации 11.2. Методы и стандарты шифрования 11.3. Перспективы использования криптозащиты информации в компьютерных системах
28	12	2	<u>ЗИ в распределенных компьютерных системах (КС)</u> 12.1. Международные стандарты информационного обмена 12.2. Архитектуры распределенных КС и особенности ЗИ в них 12.3. ИБ в условиях функционирования в России глобальных вычислительных систем

Номер			Разделы, темы и основные вопросы лекции
не- дели	лек- ции	темы по РГ	
III. ПОСТРОЕНИЕ И ОРГАНИЗАЦИЯ ФУНКЦИОНИРОВАНИЯ КОМПЬЮТЕРНЫХ СЗИ			
29	13	3	<u>Теория создания компьютерных систем защиты информации (СЗИ)</u> 13.1. Концепция создания защищенных компьютерных систем (КС) 13.2. Методология проектирования компьютерных СЗИ 13.3. Моделирование компьютерных СЗИ и их оценка
30	14	3	<u>Проектирование компьютерных СЗИ</u> 14.1. Выбор показателей эффективности и критерия оптимальности компьютерной СЗИ 14.2. Этапы создания комплексной СЗИ 14.3. Создание организационной структуры компьютерной СЗИ
31	15	3	<u>Организация функционирования компьютерных СЗИ</u> 15.1. Применение компьютерных СЗИ в экономике 15.2. Применение компьютерных СЗИ в юриспруденции 15.3. Техническая эксплуатация компьютерных СЗИ

3П1.2. План лабораторных занятий (ЛЗ)

Номер недели	Тема лабораторного занятия и отрабатываемые вопросы	Количе- ство часов	Вид от- чётности по ЛЗ
23-24	<u>ЛЗ-1. Разработка модели разграничения доступа к информации. Разграни- чение доступа к информации в среде Windows NT</u> 1. Разработать перечень защищаемых ресурсов и их критичности 2. Определить категории персонала и программно-аппаратных средств, на которые рас- пространяется политика ИБ 3. Установить особенности расположения, функционирования и построения средств КС и выявить угрозы безопасности информации и класс ее защищенности 4. Определить уязвимые места КС и формировать требования к построению СЗИ 5. Выбрать средства ЗИ для исследуемой КС 6. Разграничение доступа к информации в ОС Windows NT	4	Оп, От
25-26	<u>ЛЗ-2. Контроль за состоянием безопасности информации. Исследование проблем очистки магнитных носителей</u> 1. Средства ведения и анализа системных журналов ОС Windows 2. Анализ настройки разграничения доступа в ОС Windows. Восстановление файлов. 3. Средства освобождения областей оперативной памяти внешних носителей	4	Оп, От
27-28	<u>ЛЗ-3. СЗИ от разрушающих программных воздействий (РПВ). Примене- ние программных антивирусных комплексов</u> 1. Средства анализа программ. Дизассемблирование программ и исследование их кода 2. Настройка антивирусных программных комплексов 3. Применение антивирусных программных комплексов	4	Оп, От
29-30	<u>ЛЗ-4. Исследование программных средств борьбы с компьютерными ви- русами (КВ). Аппаратные средства опознавания пользователей</u> 1. Исследование результатов воздействия КВ на программы в среде ОС 2. Исследование результатов работы антивирусных программ 3. Аппаратные средства опознавания пользователей СЗИ (электронный замок «Соболь»)	4	Оп, От
31-32	<u>ЛЗ-5. Построение СЗИ на основе криптографических преобразований. Исследование уязвимостей ПО криптографической защиты</u> 1. Построение СЗИ "CriptonLITE" 2. Защита файлов и дисков. Шифрованные логические диски 3. Исследование криптографической стойкости WinZip и текстового редактора MS Word	4	Оп, От
34-35	<u>ЛЗ-6. Средства защиты от несанкционированного копирования информа- ции. Исследование программ, защищенных от копирования</u> 1. Привязка программ к гибким и жестким МД. Программные средства защиты от НМД 2. Средства анализа и копирования защищенных дискет и взламывания защиты программ 3. Исследование программ и дискет защищенных от копирования	4	Кз, От

Номер недели	Тема лабораторного занятия и отрабатываемые вопросы	Количество часов	Вид отчетности по ЛЗ
34-35	<u>ЛЗ-7. Защита программ от изучения. Системы ЭЦП</u> 1. Защита файлов от изменений, способы обеспечения целостности информации 2. Алгоритмы электронной цифровой подписи (ЭЦП), системы ЭЦП 3. Реализация ЭЦП в СКЗИ "Верба-OW"	4	Кз, От
34-35	<u>ЛЗ-8. Устройство и принципы функционирования СЗИ от НСД в ПК Работа в среде СЗИ от НСД «Secret Net»</u> 1. Работа пользователей ПЭВМ в защищенной среде. Установка СЗИ «Secret Net» и. Работа администратора при использовании СЗИ от НСД «Secret Net» 2. Защита информации в локальной вычислительной сети. Работа администратора ЛВС NetWare по управлению пользователями, доступом пользователей и процессов к ресурсам системы	4	Кз, От
34-35	<u>ЛЗ-10. Контроль знаний студентов по дисциплине с помощью АСК "Контроль" и прием отчетов по ЛЗ.</u> 1. Проверка знаний по дисциплине с помощью АСК "Контроль". 2. Прием отчетов по лабораторным занятиям дисциплины	2	КПЗ, От
Итого:		34	

Примечания. При выполнении ЛЗ предусмотрены следующие виды отчетности:

КПЗ – контрольно-проверочное занятие

Оп - опрос студентов перед выполнением лабораторного занятия (ЛЗ);

От - приём отчётов по ЛЗ;

Кз - контроль выполнения домашних заданий и приём отчётов по ЛЗ.

Приложение 2. Программа самостоятельной работы студента по дисциплине "ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ" 5 курс (9 семестр)

П2.1. Содержание самостоятельной работы

Самостоятельная работа студента (СРС) по дисциплине осуществляется путем освоения будущими информатиками-экономистами и информатиками-юристами тем и вопросов дисциплины, не включенных в лекционный курс и лабораторные занятия.

При выполнении заданий СРС студент обязан самостоятельно изучить дополнительные методические материалы по информационной безопасности в предметной области, подготовленные ведущими преподавателями с учетом особенностей специальности 230201.65 – "Информационные системы и технологии".

Цель СРС – самостоятельное изучение будущим информатиками-экономистами и информатиками-юристами теоретических, организационно-правовых, программно-аппаратных и технологических разделов ИБ, дающих углубленное представление о механизмах эффективного применения защищенных ПОИС и ИТ в соответствующей предметной области.

Задачи СРС – самостоятельное освоение студентом под руководством преподавателя перечисленных ниже вопросов-заданий по тематике дисциплины.

В результате самостоятельного выполнения этой работы студенты должны:

знать

- функциональные информационные процессы предметной области, подлежащие приоритетной защите;

- средства, способы и методы ЗИ, обеспечивающие создание и применение защищенной технологии сбора, хранения, анализа, обработки и передачи информации по областям;

уметь

- применять полученные знания по ЗИ в автоматизированном управлении процессами решения функциональных задач и обработке информации в предметной области;

обладать навыками

- работы с антивирусными программами и СЗИ;

- выполнения расчетов и подготовки необходимой документации в рамках своей профессиональной деятельности на компьютере;
- поиска необходимой информации в отраслевых, национальных и мировых базах знаний и данных.

П2.2. Виды и объём самостоятельной работы студента

Вид самостоятельной работы	Всего часов	Форма контроля
1. Самостоятельное изучение отдельных тем (вопросов)	56	От, ТК
2. Подготовка рефератов по индивидуальным заданиям	4	Зр, Дк
3. Подготовка докладов на семинары и конференции	4	Зр, Дк
4. Проведение патентного поиска по тематике НИРС, дисциплины и пр.	4	Пп, ТК
5. Выполнение студенческой научной работы (по тематике дисциплины)	4	Зр, Дк
6. Подготовка и защита курсового проекта (работы)	4	Зкр,
7. Другие виды самостоятельной работы (по инициативе студента)	4	С
Общий объём:	80	

Примечание. При проведении практических занятий используются следующие виды отчетности студентов:

Дк – выступление с докладом, рефератом, научной статьей;

Зкр – защита курсовой работы;

Зр – защита реферата, представление доклада, научной работы по НИРС;

От – отчет студента по самостоятельно отрабатываемому вопросу (теме);

Пп – представление результатов патентного поиска;

С – собеседование;

ТК – текущий контроль.

П2.3. Темы (вопросы), выносимые на СРС и рекомендуемая литература

№ п/п	Тема (вопрос), выносимый на самостоятельную работу студентов	Литература	
		основная	дополн.
1	Цели и задачи курса. Концепция ИБ	[1]	[4], [7]
2	Основные положения теории ИБ информационных систем	[2-3]	[14]-[16]
3	Необходимость ЗИ. Задачи по защите информации в КС	[1-3]	[6]
4	Разработка модели разграничения доступа к информации	[2]	[5], [9]
5	Разграничение доступа к информации	[1-2]	[7-8]
6	Разграничение доступа к информации в среде Windows NT	[1]	[4],[8]
7	Требования к системам и средствам защиты информации от НСД	[1-3]	[8-9],[12]
8	Контроль за состоянием безопасности информации	[2]	[11-13]
9	Задачи контроля в обеспечении безопасности информации	[1], [4]	[7],[12]
10	Исследование проблем очистки магнитных носителей	[3]	[15],
11	Понятие разрушающего программного воздействия (РПВ)	[1], [3]	[13] [14],
12	Средства ЗИ от разрушающих программных воздействий	[1], [3]	[15]
13	Принципы и методы защиты от РПВ	[3]	[16]
14	Применение программных антивирусных комплексов	[1]-[2]	[8-9],[12]
15	Исследование антивирусных программных средств	[2]	[13-14]
16	Обеспечение целостности информации	[2]	[13-14]
17	Криптографические средства обеспечения целостности информации	[2-3]	[10],[13]
18	Построение СЗИ на основе криптографических преобразований	[1-2]	[15],
19	Основные принципы криптографической защиты информации в КС	[2]	[13] [14],
20	Исследование уязвимостей криптографических программных средств	[1-2]	[14]
21	Применение криптографических средств ЗИ в КС	[3]	[14]
22	Аппаратные средства опознавания пользователей	[1-2]	[10],[15]
23	Построение системы защиты от НСД для ПЭВМ.	[1]	[18-19]
24	Средства защиты от несанкционированного копирования информации	[1-2]	[17],[20]
25	Исследование программ, защищенных от копирования	[1]	[15],
26	Защита программ от изучения	[1-2]	[13] [14],
27	Системы ЭЦП	[1-2]	[14]
28	Устройство и принципы функционирования СЗИ от НСД в ПЭВМ	[2]	[14]
29	Работа в среде СЗИ от НСД "Secret Net"	[2]	[8-9],[15]
30	Защита информации в локальной вычислительной сети	[2]	[15-16]

Темы рефератов

1. Модификация автоматизированных обучающих систем (АОС) с учетом требований ИБ.

2. Перспективные направления повышения эффективности ИБ на базе ИТ.
3. Информационные технологии в высшей школе и их защита.
4. Перспективные электронные ИС и ИТ, их защита НСД.
5. Программно-аппаратная защиты информации: состояние и перспективы развития.
6. Состояние и перспективы развития СЗИ.

Темы докладов

1. Модернизация электронных программно-методических комплексов (ЭПМК) с учетом современных требований к защите авторских прав и информации.
2. Разработка и создание защищенных АИСС по диссертациям, защищенных в ФГОУ ВПО КубГАУ.
3. Обеспечение ИБ корпоративной ЛВС ФГОУ ВПО КубГАУ.
4. Перспективные СЗИ для ИПС и БД в экономике (юриспруденции).
5. Проблемно-ориентированный информационный консалтинг по ИБ.

Направления патентного поиска

1. Автоматизированные обучающие системы и ЗИ в них.
2. Современные методы и средства защиты компьютерной информации.
3. Криптографические методы ЗИ.
4. Аппаратные и программные средства защиты компьютерной информации.
5. Методы защиты информации в компьютерных системах и сетях.

Темы научно-исследовательских работ студентов (НИРС)

1. Разработка мультимедийных компьютерных практикумов по информационной безопасности (совместно с преподавателями):
2. Использование Internet-технологий в качестве теоретического и практического источника совершенствования защиты информации в корпоративной ЛВС ФГОУ ВПО КубГАУ.
3. Анализ и переработка лабораторных занятий по информационной безопасности.
4. Подготовка мультимедийных лекций по информационной безопасности.
5. Разработка программных средств (приложений), обеспечивающих защиту информации в учебных аудиториях и на кафедрах.

Литература к СРС:

1. Алексеенко В.Н., Сокольский Б.В. Система защиты коммерческих объектов. Технические средства защиты. Практическое пособие для предпринимателей и руководителей служб безопасности. М., 1992. - 94с.
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.: РЕ, 1991. -416с.
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 криптографическая. Алгоритм криптографического преобразования.
10. ГОСТ Р 34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.
11. ГОСТ Р 34.11-94. Функция хеширования.

12. Гостехкомиссия РФ. Руководящий документ. Защита информации. Специальные 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.: Яхтсмен, 1996. - 192с.
17. Закон Российской Федерации "О государственной тайне". 21.07.1993.
18. Защита программного обеспечения. / Пер. с англ. Д. Гроувер, Р. Сатер, Дж. Фипс и др.; Под ред. Д. Гроувера. - М.: Мир, 1992. - 286с.
19. Информационно-безопасные системы. Анализ проблемы: Учеб. пособие. / Алешин И.В. и др.: Под ред. В.Н. Козлова - СПб.: СПбГТУ, 1996. - 69с.
20. Касперский Е. Компьютерные вирусы в MS-DOS. - М.: Эдэль, 1992. - 176с.
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. - М.: Энергоатомиздат, 1986. - 304с.
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. - 216с.
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. - 368с.
29. Михайлов С.Ф., Петров В.А., Тимофеев Ю. А. Информационная безопасность. Защита информации в автоматизированных системах. Основные концепции: Учебное пособие. - М.: МИФИ, 1995. - 112с.
30. Молчанов А.А. Моделирование и проектирование сложных систем. - К.: Выща шк. Головное издательство, 1988. - 359с.
31. Особенности устройств съема информации и методы их блокировки. - Томск: НПП "Вихрь", 1996. - 32с.
32. Пилюгин П.Л. Общие вопросы защиты вычислительных систем и особенности защиты персональных компьютеров: Курс лекций. - М.: ИКСИ, 1997. - 84с.
33. Положение о государственном лицензировании деятельности в области защиты информации (Решение Государственной технической комиссии России и ФАПСИ от 27.04.94 г. №10). - М.: Гостехкомиссия РФ, 1994. - 16с.
34. Положение о сертификации средств защиты информации (Постановление Правительства Российской Федерации от 26.06.95 г. № 608). - М., 1995. - 4с.
35. Положение по аттестации объектов информатизации по требованиям безопасности информации (Утверждено Председателем Гостехкомиссии Российской Федерации 25.11. 1994 г.). - М.: Гостехкомиссия РФ, 1994. - 16с.

36. Портативный тепловизионный комплекс "Иртис-200". Паспорт. - М.: "Иртис", 1998. - 11с.
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.: "Яхтмен", 1993. - 188с.
39. Спесивцев А.В., Вегнер В.А., Крутяков А.Ю. и др. Защита информации в персональных ЭВМ. - М.: Радио и связь; МП «Веста», 1992. - 192с.
40. Специальная техника защиты и контроля информации: Каталог. - М.: Маском, 1998. - 44с.
41. Специальная техника: Каталог. - М.: НПО "Защита информации", 1998. - 32с.
42. Стенг Д.И., Мун С. Секреты безопасности сетей - К.: Диалектика, 1996.
43. Таили Э. Безопасность персонального компьютера. - Мн.: ООО "Попурри", 1997. - 480с.
44. Технические системы защиты информации: Каталог. - М.: АОЗТ "Нелк", 1998. - 56с.
45. Технические системы защиты информации: Каталог. - М.: АОЗТ "Нелк", 1997. - 200с.
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. - 112с.
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. - 112с.
55. Фролов А.В., Фролов Г.В. Осторожно: компьютерные вирусы. - М.: ДИАЛОГ-МИФИ, 1996. - 256с.
56. Хоффман Л.Дж. Современные методы защиты информации. / Пер. с англ. - М.: Сов. радио, 1980.
57. Цыганков В.Д., Лопатин В.Н. Психотропное оружие и безопасность России. Серия "Информатизация России на пороге XXI века". - М.: СИНТЕГ, 1999. - 152с.
58. Шелест С.О. 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.Ю. Разрушающие программные воздействия. - М.: Эдэль, 1993. - 64с.
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. - 272с.
65. Audio Surveillance: Catalog. - Germany: PK Electronic International FRG 1996 - 44p.

66. Datapro Reports on Information Security. 1990-1993.
67. Discrete surveillance. Navelties: Catalog. - Germany: Helling 1996 - 13p.
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 HFradio security. - IEEE Proceedings, Pt. I, 1989, February, V 136 № 1, pp.25-46.

Приложение 3. Вопросы для подготовки к экзамену по дисциплине "ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ"

5 курс (9 семестр)

ПЗ.1. Теоретические вопросы:

1. Международные стандарты информационного обмена.
2. Концепция информационной безопасности (ИБ).
3. Место ИБ экономических (правовых) систем в национальной безопасности страны.
4. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
5. Таксономия нарушений ИБ вычислительной системы
6. Три вида возможных нарушений ИС
7. Актуальность проблемыЗИ.
8. Модели безопасности и их применение.
9. Классификация средств, методов и механизмовЗИ от НСД.
10. Государственные требования к построению СЗИ.
11. Особые требования к криптографическим средствам СЗИ от НСД.
12. Показатели защищенности СВТ от НСД.
13. Классификация КС и требования поЗИ, использованиеЗКС.
14. Методы контроля доступа к ресурсам компьютерной системы.
15. Структура и функции подсистемы контроля доступа программ и пользователей.
16. Средства активного аудита КС.
17. Идентификация и аутентификация субъектов и объектов КС.
18. Идентифицирующая информация и протоколы идентификации.
19. Основные подходы к защите данных от НСД.
20. Доступ к данным со стороны процесса.
21. Понятие скрытого доступа.
22. Модели управления доступом.
23. Дискреционная (избирательная) и мандатная (полномочная) модель управления доступом.
24. Защита алгоритма шифрования и программно-аппаратные средства шифрования.
25. Построение аппаратных компонент криптозащиты данных.
26. Взаимодействие прикладных программ и программы-злоумышленника.
27. Классификация разрушающих программных воздействий (РПВ) и их воздействий.
28. Компьютерные вирусы как особый класс РПС. Их классификация.
29. Необходимые и достаточные условия недопущения РПВ; понятие изолированной программной среды.
30. Роль морально-этических факторов в устранении угрозы РПВ.
31. Проблема обеспечения целостности информации.
32. Защита файлов от изменений. Способы обеспечения целостности информации.
33. Электронная цифровая подпись. Криптографические хэш-функции и их вычисления.
34. Методы криптографии и задачи, решаемые ими в КС.
35. Алгоритмы криптографических преобразований и их характеристики.
36. Методы и средства ограничения доступа к компонентам ЭВМ.

37. Построение средств защиты информации для ПЭВМ.
38. Перечень и краткая характеристика сертифицированных программно-аппаратных систем защиты информации (СЗИ) от НСД для ПЭВМ.
39. Особенности ЗИ в вычислительных сетях.
40. Механизмы реализации атак на ВС, защита сетевого файлового ресурса.

П3.2. Практические вопросы:

41. Определение перечня защищаемых ресурсов и их критичности.
42. Определение категорий персонала и программно-аппаратных средств, на которые распространяется политика безопасности.
43. Определение угроз ИБ.
44. Формирование требований к построению СЗИ.
45. Определение уязвимости КС и выбор средств ЗИ.
46. Создание учетных записей пользователей и групп.
47. Организация общего доступа к папкам.
48. Активный контроль состояния безопасности КС.
49. Средства ведения и анализа системных журналов ОС Windows NT.
50. Централизованное управление пользователями и контроль их действий.
51. Средства контроля вычислительных процессов.
52. Свойства процессов и управление ими.
53. Восстановление удаленных файлов и отформатированных дискет.
54. Средства гарантированного удаления информации.
55. Средства анализа программ.
56. Дизассемблирование программ и исследование кода.
57. Антивирусные программные комплексы. Настройка и применение.
58. Исследование результатов работы антивирусных программ.
59. Алгоритмы ЭЦП. Реализация ЭЦП.
60. Защита файлов и каталогов. Шифрованные логические диски.
61. Исследование временной стойкости криптосистемы архиватора WinZip.
62. Исследование уязвимостей криптосистемы архиватора Arj.
63. Построение аппаратных средств СЗИ "Аккорд" и управление пользователями в ней.
64. Средства анализа и копирования защищенных дискет и взламывания защиты программ.
65. Средства простановки ключевых меток и защиты программ от копирования.
66. Исследование дискет, защищенных от копирования
67. Исследование программ с защитой от копирования.
68. Защита программ от отладки и трассировки.
69. Работа пользователей ПК в защищенной среде.
70. Работа администратора ЛВС: управление пользователями, их доступом к процессам и ресурсам системы.

Лаптев Владимир Николаевич

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Курс лекций

(для бакалавров специальности 080500.62 – Бизнес информатика)

Подписано в печать	Формат 60х84
Бумага офсетная	Офсетная печать
Печ.л. 4,0	Заказ №
Тираж экз.	