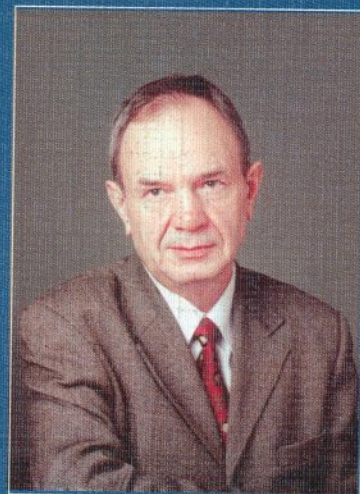




Мельников Виталий Викторович – системный аналитик в области обеспечения безопасности данных в автоматизированных информационных системах, кандидат технических наук, автор 45 научных трудов, в том числе хорошо известной специалистам книги “Защита информации в компьютерных системах” (М.: Финансы и статистика – Электронинформ, 1997). Разработчик перспективного концептуального подхода к построению защиты данных в автоматизированных системах. Более 25 лет посвятил разработке, изготовлению, испытаниям и сдаче в эксплуатацию упомянутых систем. В настоящее время В.В. Мельников – начальник сектора НИИ автоматической аппаратуры им. академика В.С. Семенихина.

В.В. МЕЛЬНИКОВ

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ



В.В. МЕЛЬНИКОВ БЕЗОПАСНОСТЬ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

ISBN 5-279-02560-7



9 785279 025602

В.В. МЕЛЬНИКОВ

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

2065



МОСКВА
"ФИНАНСЫ И СТАТИСТИКА"
2003

РЕЦЕНЗЕНТ

А.В. Петраков,
доктор технических наук, профессор,
Заслуженный деятель науки Российской Федерации,
заведующий кафедрой «Защита информации»
Московского технического университета связи и информатики

Мельников В.В.

М48 **Безопасность информации в автоматизированных системах.** –
М.: Финансы и статистика, 2003. – 368 с.: ил.
ISBN 5-279-02560-7

Изложены новые подход, концепция, методология и принципы построения защиты и расчета уровня безопасности данных в автоматизированных системах обработки информации и управления информационными процессами на основе построения замкнутой оболочки с количественными показателями ее прочности. Цель книги – показать возможность создания в указанных системах подсистемы безопасности информации с более высоким уровнем эффективности и качества.

Для специалистов в области безопасности информации в автоматизированных системах ее обработки, а также для разработчиков этих систем, пользователей, студентов и аспирантов.

М $\frac{2404000000 - 106}{010(01) - 2003}$ 318 – 2003

УДК 004.78.056
ББК 32.973.26-018.2

ISBN 5-279-02560-7

© В.В. Мельников, 2003

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ	7
ВВЕДЕНИЕ	11
1. АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ КАК ОБЪЕКТЫ ОБРАБОТКИ И ЗАЩИТЫ ИНФОРМАЦИИ	21
1.1. Предмет защиты	21
1.1.1. Свойства информации	21
1.1.2. Виды и формы представления информации	24
1.1.3. Машинное представление информации	24
1.1.4. Физическое представление информации и процессы ее обработки	27
1.1.5. Информация и ресурсы	30
1.1.6. Информация как объект права собственности	30
1.1.7. Информация как коммерческая тайна	33
1.1.8. Информация как рыночный продукт	35
1.2. Объекты обработки и защиты информации	38
1.2.1. Современное состояние классификации автоматизированных систем	38
1.2.2. Первые вычислительные системы	38
1.2.3. Архитектура «клиент-сервер»	40
1.2.4. Архитектура «клиент-сервер», основанная на Web-технологии	45
1.2.5. Эталонная модель OSI	48
1.2.6. Масштабирование компьютерных сетей	50
1.2.7. Топология простых локальных вычислительных сетей	57
1.2.8. Сегментация сложных локальных сетей	64
1.2.9. Региональные и глобальные сети	67
1.2.10. Виртуальные сети	77
1.2.11. Корпоративная сеть	80
1.2.12. Автоматизированные системы управления	82
1.2.13. Классификация автоматизированных систем	84
1.2.14. Организация проектирования автоматизированных систем	86
1.2.15. Условия и режимы эксплуатации автоматизированных систем	87
1.3. Потенциальные угрозы безопасности информации	88
1.3.1. Постановка задачи	88
1.3.2. Случайные угрозы	88
1.3.3. Преднамеренные угрозы	91
2. МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ	100
2.1. Краткий обзор современных методов защиты информации	100
2.1.1. Ограничение доступа	101
2.1.2. Разграничение доступа	103
2.1.3. Контроль доступа к аппаратуре	103

2.1.4. Разграничение и контроль доступа к информации	104
2.1.5. Разделение привилегий на доступ к информации	106
2.2. Идентификация и установление подлинности объекта (субъекта)	106
2.2.1. Объект идентификации и установления подлинности	106
2.2.2. Идентификация и установление подлинности личности	107
2.2.3. Идентификация и установление подлинности документов	110
2.2.4. Идентификация и установление подлинности информации на средствах ее отображения и печати	112
2.3. Криптографическое преобразование информации	112
2.3.1. Основные принципы и классификация методов криптографического преобразования информации	112
2.3.2. Краткий обзор методов шифрования	115
2.3.3. Выбор метода преобразования	124
2.4. Методы защиты информации от компьютерных вирусов	128
2.5. Защита информации от утечки за счет побочного электромагнитного излучения и наводок	135
2.5.1. Потенциальные угрозы	135
2.5.2. Методы и средства защиты информации от излучения	136
2.6. Методы и средства защиты информации от случайных воздействий	137
2.7. Методы защиты информации от аварийных ситуаций	147
2.8. Организационные мероприятия по защите информации	148
2.9. Законодательные меры по защите информации	150
3. ОСНОВЫ МЕТОДОЛОГИИ ПОСТРОЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ	152
3.1. Анализ и оценка действующей концепции защиты	152
3.2. Выбор концептуальной модели построения защиты	155
3.3. Исходные данные для постановки задачи	159
3.4. Основы теории построения защиты информации	163
3.4.1. Введение в проблему теории защиты информации	163
3.4.2. Общий методический подход	164
3.4.3. Основные принципы построения защитной оболочки	165
3.4.4. Модель элементарной защиты	166
3.4.5. Модель многоуровневой защиты	179
3.4.6. Многоуровневая защита	181
3.4.7. Некоторые особенности точности расчета прочности защиты	182
3.5. Метод построения защиты информации в системах с сосредоточенной обработкой данных	184
3.5.1. Объект исследования	184
3.5.2. Классификация возможных каналов НСД	185
3.5.3. Метод применения средств защиты	185
3.5.4. Построение системы безопасности информации КСА	188
3.5.5. Анализ средств и метод расчета прочности защиты	190
3.5.6. Технология проектирования защиты информации в КСА	193
3.6. Метод построения защиты информации в системах с распределенной обработкой данных	194
3.6.1. Объект исследования	194
3.6.2. Предмет защиты и потенциальные угрозы	195
3.6.3. Классификация возможных несанкционированных действий	195
3.6.4. Метод применения средств защиты	196
3.6.5. Построение системы безопасности информации АСУ и СПД	198

3.6.6. Анализ средств и метод расчета прочности защиты	202
3.6.7. Технология проектирования защиты информации АСУ	204
3.7. Основные принципы и порядок проектирования защиты	205
3.7.1. Основные принципы проектирования защиты	205
3.7.2. Порядок проектирования защиты	207
4. СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ С СОСРЕДОТОЧЕННОЙ ОБРАБОТКОЙ ДАННЫХ	210
4.1. Системы охранной сигнализации на территории и в помещениях объекта обработки информации	210
4.1.1. Требования к системам охранной сигнализации	211
4.1.2. Наружные системы охраны	213
4.1.3. Традиционные системы	215
4.1.4. Ультразвуковые системы	216
4.1.5. Системы прерывания луча	216
4.1.6. Телевизионные системы	217
4.1.7. Радиолокационные системы	217
4.1.8. Микроволновые системы	218
4.1.9. Беспроводные системы	220
4.2. Система контроля вскрытия аппаратуры	220
4.2.1. Требования, предъявляемые к системе контроля вскрытия аппаратуры	220
4.2.2. Принципы построения СКВА	223
4.3. Программы контроля и разграничения доступа к информации	230
4.3.1. Задачи и общие принципы построения программ контроля и разграничения доступа к информации	230
4.3.2. Выбор значений паролей (кодов паролей)	233
4.3.3. Разграничение полномочий пользователей	234
4.3.4. Концепция построения систем контроля и разграничения доступа	236
4.3.5. Средства перекрытия путей обхода программ контроля и разграничения доступа	237
4.3.6. Выбор носителей кодов паролей	239
4.3.7. Оценка программ контроля и разграничения доступа как средства защиты	243
4.4. Контроль целостности программного обеспечения и информации	244
4.5. Дублирование информации	248
4.6. Средства защиты программного обеспечения и информации от несанкционированной загрузки	251
4.7. Защита информации на машинных носителях	253
4.8. Защита остатков информации	254
4.9. Защита информации в линиях связи	255
4.10. Средства регистрации доступа к информации АС	256
4.11. Защита информации при документировании	258
4.12. Организационные мероприятия по защите информации в АС	258
5. СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ С РАСПРЕДЕЛЕННОЙ ОБРАБОТКОЙ	263
5.1. Линейное шифрование	263
5.2. Абонентское шифрование	264

5.3. Цифровая подпись	267
5.4. Средства идентификации и аутентификации	271
5.5. Средства контроля и разграничения доступа	275
5.6. Межсетевые экраны	275
5.6.1. Постановка задачи	275
5.6.2. Функции межсетевого экранирования	277
5.6.3. Фильтрация трафика	278
5.6.4. Выполнение функций посредничества	280
5.7. Средства защиты трафика	282
5.8. Особенности защиты информации в базах данных	283
6. МЕТОД ПОСТРОЕНИЯ СИСТЕМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ РАБОЧЕЙ СТАНЦИИ, ЛВС, ГЛОБАЛЬНОЙ СЕТИ И АСУ	288
6.1. Построение системы безопасности информации рабочей станции	288
6.1.1. Рабочая станция как объект обработки и защиты информации ..	288
6.1.2. Потенциальные угрозы информации, обрабатываемой в рабочих станциях	294
6.1.3. Система защиты информации от несанкционированного доступа в рабочей станции	296
6.1.4. Показатели прочности защиты информации рабочей станции ..	300
6.2. Построение системы безопасности информации локальной вычислительной сети	302
6.2.1. Локальная вычислительная сеть как объект обработки и защиты информации	302
6.2.2. Возможные каналы несанкционированного доступа	303
6.2.3. Построение системы безопасности информации в ЛВС	305
6.2.4. Показатели оценки прочности защиты информации ЛВС	309
6.3. Построение системы безопасности информации в глобальных АСУ и телекоммуникационных вычислительных сетях	310
6.3.1. Особенности построения защиты информации в АСУ	310
6.3.2. Особенности построения защиты информации в телекоммуникационных вычислительных сетях	312
7. МЕТОДЫ ОЦЕНКИ УРОВНЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ	317
7.1. Анализ современных методов оценки	317
7.2. Совершенствование методов оценки уровня безопасности информации в автоматизированных системах	320
ЗАКЛЮЧЕНИЕ	323
Приложение 1. Руководящий документ «Автоматизированные системы обработки и передачи данных». Система безопасности информации (Проект)	326
Приложение 2. Основные нормативные акты Российской Федерации по рассматриваемой тематике (по состоянию на 2000 г.)	354
Приложение 3. Пример расчета прочности оболочки защиты	356
ЛИТЕРАТУРА	358
СПИСОК СОКРАЩЕНИЙ	363
ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ	365

ПРЕДИСЛОВИЕ

Проблема безопасности информации продолжает оставаться весьма актуальной. В теории это выражается в различном понимании основных терминов и определений, отсутствии классификации объектов обработки и защиты информации, методов определения возможных каналов несанкционированного доступа к информации, отсутствии методов расчета прочности средств защиты, принципов построения системы защиты, гарантированных количественных показателей уровня прочности защиты как единого механизма в создаваемых автоматизированных системах, на практике – в достаточно успешных действиях нарушителей и весьма ощутимых потерях владельцев систем.

Решение названной проблемы, несмотря на большой объем проведенных исследований и выпуск международных стандартов, осложняется еще и тем, что в применяемой в настоящее время концепции защиты информации в автоматизированных системах отсутствует привязка к типовым объектам автоматизации процессов ввода-вывода, хранения, обработки и передачи информации, не разработаны принципы построения защитной оболочки. Отсутствие защитной оболочки означает наличие возможных путей обхода защиты.

Автор попытался решить данную проблему в книге «Защита информации в компьютерных системах» (М.: Финансы и статистика, 1997).

Новое издание отличается от вышеуказанного следующим:

- описанием новой классификации автоматизированных систем;
- разработкой концептуальной модели построения защиты;
- усовершенствованием методологии построения защиты в части локальных и глобальных вычислительных сетей.

Это позволило довести идею построения защитной оболочки до логического завершения и еще раз убедило автора в том, что он на правильном пути. В данной книге предлагаются разработанная автором методология и проект нового нормативного руководящего документа по созданию и сертификации защиты упомянутых систем. Принципиальное отличие описываемой в этом издании концепции от применяемой заключается в следующем:

- выборе информации в качестве предмета защиты (ресурсы тоже защищаются, но только в особых случаях) как объекта права собственности;
- использовании классификации автоматизированных систем по видам, принципам построения и обработки данных;
- сведении всех потенциальных угроз информации к трем событиям: утечке, модификации и утрате;
- применении различных подходов к случайным и преднамеренным угрозам информации;

- разработке простой модели ожидаемого поведения нарушителя и его классификации;
- определении в автоматизированных системах возможных каналов несанкционированного доступа к информации со стороны нарушителя того или иного класса;
- перекрытии возможных каналов несанкционированного доступа к информации автоматизированных систем средствами защиты, связанными расчетными соотношениями, образующими виртуальную защитную оболочку;
- разработке расчетных соотношений для построения средств и системы защиты с гарантированным уровнем прочности.

Образно говоря, разница между применяемым и предлагаемым подходами к построению защиты такая же, как если бы для защиты своих ценностей вы стали выбирать между множеством капканов и сейфом. Надеюсь, что последний вариант предпочтительнее, и значит, данное издание для вас, уважаемый читатель.

Книга состоит из семи разделов.

Термины и определения, отражающие новый подход к решению проблемы, приведены во введении.

В разделе 1 рассматривается информация как предмет защиты, ее свойства, виды и формы представления в автоматизированных системах. Приводятся классификация, состав технических средств и обобщенные свойства систем обработки данных как объектов, содержащих предмет защиты. Систематизируются потенциальные угрозы безопасности информации в автоматизированных системах и подводится база под постановку задачи.

В разделе 2 освещаются современные методы защиты информации, без которых книга была бы неполной. Материалы разделов 1 и 2 изложены с позиций новой концепции защиты информации.

В разделе 3 представлены основы методологии построения и принципы проектирования защиты информации. Приводятся анализ и оценка действующей концепции защиты, разработка новой модели защиты, основы теории и методология построения защиты информации в автоматизированных системах с сосредоточенной и распределенной обработкой данных.

В разделах 4 и 5 описываются средства защиты информации с сосредоточенной и распределенной обработкой данных.

В разделе 6 рассмотрены принципы построения и методы оценки ожидаемой эффективности системы безопасности информации на основе предлагаемой автором методологии, а также отражены особенности построения защиты в глобальных автоматизированных системах. Учитывая особенности современного развития вычислительной техники и принципов построения автоматизированных систем на основе получивших широкое распространение персональных компьютеров и локальных вычислительных сетей, показано, что к ним также применима предложенная концепция безопасности информации.

Раздел 7 посвящен методам оценки уровня безопасности информации. В нем используется разработанный автором целевой проект «Руководящего

документа по проектированию и оценке ожидаемой эффективности защиты информации в автоматизированных системах», приведенный в приложении 1. По этой причине в названии книги употреблен действующий сегодня термин «автоматизированные системы» – название конечных продуктов разработчика и производителя. Предполагается, что в случае признания специалистами новой концепции и методологии построения защиты проект может послужить основой при разработке новых стандартов по их сертификации.

В приложении 2 представлены основные нормативные акты Российской Федерации по рассматриваемой тематике (по состоянию на 2000 г.).

В приложении 3 дан пример расчета прочности оболочки защиты.

В конце издания приведены список сокращений и предметный указатель.

При написании книги автор придерживался ряда принципов.

Во-первых, это четкое ограничение предмета изложения.

Во-вторых, упоминаемые в книге отдельные средства защиты приводятся для примера и при необходимости могут быть заменены другими, более совершенными, так как издание не рассчитано на то, чтобы служить справочником по существующим средствам защиты: к моменту выхода книги вполне может случиться, что перечисленные средства морально устареют. Однако на выполнение поставленной в книге задачи это не влияет.

В-третьих, по мере возможности выдерживается доступный метод изложения, не требующий от читателя глубоких знаний в области вычислительной техники и программирования. Вместе с тем книга не является популярным рассказом на актуальную тему.

В-четвертых, учитывая нереальность широкого охвата всех вопросов безопасности информации в автоматизированных системах, а также наличие специальных работ, посвященных данной тематике, в книге дается лишь краткая информация по защите программного обеспечения, средствам защиты от побочных электромагнитных излучений и наводок информации, компьютерных вирусов, а также по криптографии. В нее намеренно не включены правовые вопросы, в принципе очень важные, но, по мнению автора, выходящие за рамки поставленной задачи. Законодательные меры упоминаются только как средство предупреждения и сдерживания потенциального нарушителя. По той же причине не освещаются вопросы защиты информации в организации-разработчике при проведении опытно-конструкторской разработки автоматизированной системы.

Предлагаемые концепция и принципы построения систем безопасности информации базируются на том, что до момента передачи автоматизированной системы ее владельцу никакие несанкционированные изменения и «потайные закладки» в нее не вносились. Решение этой задачи связано с созданием другой системы – системы безопасности информации в данной организации, в которой предметом защиты являются процессы и сведения по разработке, изготовлению и испытанию данной автоматизированной системы, а также ее тактико-технические характеристики.

Цель данного издания – показать возможность создания в автоматизированных системах защиты с более высокими качественными и количественными

ными показателями, с меньшими затратами за счет применения предложенной автором методологии построения, а также теории, методов расчета и оценки ожидаемой эффективности системы безопасности информации.

Книга предназначена для специалистов по безопасности информации в автоматизированных системах, для ее разработчиков, а также для студентов и аспирантов вузов соответствующих специальностей.

Автор приносит глубокую благодарность профессору, доктору технических наук, заведующему кафедрой «Защита информации» Московского технического университета связи и информатики, действительному члену Международной академии информатизации, Заслуженному деятелю науки РФ А.В. Петракову, чьи критические замечания позволили улучшить структуру книги, а также профессору, доктору технических наук Г.А. Оганяну, указавшему направление по совершенствованию и реализации идеи.

*Посвящается сыновьям
Александру и Роману*

ВВЕДЕНИЕ

Проблема защиты информации от постороннего доступа и нежелательных воздействий на нее возникла давно – с той поры, как человеку не захотелось делиться ею с другими людьми. С развитием общества, появлением частной собственности, государственного строя, борьбой за власть и дальнейшим расширением масштабов человеческой деятельности информация приобретает все большую цену, особенно та информация, обладание которой позволит ее владельцам получить какой-либо выигрыш: моральный, материальный, политический, военный и т.д.

В период существования примитивных носителей информации ее защита осуществлялась организационными методами, которые включали ограничение и разграничение доступа, определенные меры наказания за разглашение тайны. По свидетельству Геродота, уже в V в. до н.э. использовалось преобразование информации методом кодирования. Коды появились в глубокой древности в виде криптограмм (гр. *kryptos* тайный + *gramma* запись – тайнопись). Спартанцы имели специальный механический прибор, при помощи которого важные сообщения можно было писать особым способом, обеспечивающим сохранение тайны. Собственная секретная азбука была у Юлия Цезаря. В средние века и эпоху Возрождения над изобретением тайных шифров трудились многие выдающиеся люди, в их числе известный философ Фрэнсис Бэкон, математики Франсуа Виет, Джероламо Кардано, Джон Валлис [1].

С переходом на использование технических средств связи информация подвергается воздействию случайных процессов: неисправностям и сбоям оборудования, ошибкам операторов и т.д., которые могут привести к ее разрушению, изменению на ложную, а также создать предпосылки к доступу посторонних лиц. С дальнейшим усложнением и широким распространением технических средств связи возросли возможности для преднамеренного доступа к информации.

С появлением сложных автоматизированных систем управления (АСУ), связанных с автоматизированным вводом, хранением, обработкой и выводом информации, проблема ее защиты приобретает еще большее значение.

Индустрия обработки информации достигла высочайшего уровня. Открылась возможность выхода в глобальную вычислительную сеть с домашнего компьютера. Появление «электронных» денег (кредитных карточек) создало предпосылки для хищений крупных денежных сумм. В печати приведено множество конкретных примеров хищения информации из автоматизированных систем (АС) обработки данных, которые весьма убедительно иллюстрируют актуальность проблемы.

Новое удивительное порождение научно-технической революции – компьютерные злоумышленники: хакеры и крэкеры. Хакеры (англ. Hacker) – компьютерные хулиганы, проникающие в чужой компьютер, прекрасные знатоки информационной техники. С помощью телефона и домашних компьютеров они подключаются к сетям передачи данных, связанным почти со всеми крупными компьютерами в области экономики, научно-исследовательских центров, банков. Особая разновидность хакеров – крэкеры (англ. Cracker – вор-взломщик). Крэкеры, в отличие от хакеров, воруют информацию с помощью компьютера, выкачивая целые информационные банки данных.

По сообщению журнала COMPUTERWORLD, опубликованным 5 февраля 2002 г., полиции Италии удалось выследить шестерых участников хакерской группы, обвиняемой в атаках на тысячи сайтов в 62 странах. В США были взломаны сайты Пентагона, НАСА и многочисленных вузов, в том числе Гарвардского, Колумбийского и Корнеллского университетов. Были атакованы сайты в Англии, Китае, Швеции, Австралии, в странах Латинской Америки, на Филиппинах и в Пакистане. Группа начала атаки в июле 2001 г. в ходе саммита «большой восьмерки» в Генуе, сопровождавшегося выступлениями антиглобалистов, в число которых входила эта группа.

По данным М. Мур, руководителя отдела информационных технологий и рисков компании Ernst & Young, опрос более сотни компаний, работающих в России и других странах СНГ, показал, что многие из них не имеют четкого представления об уязвимых местах своих систем и о реальных рисках, которым они подвергаются. Оказалось, что 65% респондентов в течение года сталкивались с нарушением компьютерной безопасности, причем 43% инцидентов было связано с вирусными атаками. Остальные случаи – с внешними проникновениями в систему, несанкционированным доступом корпоративных пользователей и DOS-атаками, вызывающими отказы в обслуживании из-за перегрузки системы ложными запросами. Только в Москве ущерб от злонамеренных электронных действий достигает 15 млн долл. в месяц.

В последнее время широкое распространение получил новый вид компьютерного преступления – создание компьютерных вирусов, в качестве которых выступают специально разработанные программы, начинающие работать только по определенному сигналу. При этом вирус может размножаться, словно возбудитель болезни, когда соприкасается с другим программным обеспечением. Последствия от «заражения» программ подобными вирусами могут быть различными: от безобидных шуток в виде юмористических помех до разрушения программного обеспечения, восстановление которого может оказаться невозможным, а потери невосполнимыми.

«Только в августе этого года (2002 г. – Примеч. ред.) и только в одной Великобритании было зарегистрировано 5580 попыток взлома корпоративных информационных систем и хакерских атак. Общее же их число с начала года превысило 30 тыс.

Размеры убытков, нанесенных в прошлом году такими вирусами, как Code Red, Nimda и Sircam, оценивались миллиардами долларов»¹.

¹ Сазонов А. Трехглавый дракон Интернета // Деньги. – 2002. – №36 (391). – С. 108, 110.

Несмотря на то что специалисты отмечают снижение интереса к вирусоспирательству, вопрос по-прежнему остается актуальным.

«Помимо злодеев, которые угрожают целым странам и народам, существуют и вполне благопристойные компании, буквально терроризирующие всех, кто пользуется электронной почтой. Это спаммеры¹. Электронный спам стал настоящим бедствием для Интернета²».

Последствия несанкционированных воздействий и несанкционированного использования информации могут носить весьма серьезный характер, включая политический, связанный с опасностью возникновения войны в случаях появления ложной информации о нападении.

В связи с политическим аспектом проблемы уместно вспомнить о созданной в России автоматизированной системе управления «Выборы» и системе подсчета голосов в Госдуме. Если не уделить в них особого внимания гарантированной защите обрабатываемой информации от несанкционированного доступа, результаты голосования могут быть сфальсифицированными.

Полезно также отметить еще одну сторону проблемы – вопиющую безответственность пользователей данных. Специалисты приводят множество способов несанкционированного доступа к информации в системе обработки данных: просмотр; копирование и подмена данных; ввод ложных программ, команд и сообщений; подключение к линиям и каналам связи; использование отладочных и аварийных программ и устройств; чтение остатков информации; прием сигналов побочного электромагнитного излучения и наводок информации; использование неисправностей и сбоев аппаратуры, ошибок операторов и программистов и т.д.

Для того чтобы не повторять прошлых ошибок, перечислим основные вехи истории создания защиты от указанных угроз [16].

Главенствующей идеей первого этапа создания защиты (1960-е гг.) являлось намерение обеспечивать надежную защиту информации механизмами, содержащими в основном технические и программные средства.

«Техническими» были названы такие средства, которые реализуются в виде электрических, электромеханических и электронных устройств. Вся совокупность этих средств было принято делить на аппаратные и физические. Под аппаратными техническими средствами защиты понимали устройства, встраиваемые непосредственно в аппаратуру автоматизированной системы, или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу. Физическими средствами были названы такие, которые реализуются в виде автономных устройств и систем (электронно-механическое оборудование охранной сигнализации и наблюдения, замки на дверях, решетки на окнах и т.п.).

Отметим некорректность упомянутых терминов: «технические» средства – понятие более широкое, к ним можно отнести и аппаратные, и физические, и программные средства, а к «физическим» – аппаратные. Программные средства защиты – это программы, предназначенные для выполнения функций, связанных с защитой информации.

¹ Спам (англ. spam) здесь: бесполезная информация (обычно реклама), рассылаемая большому числу абонентов электронной почты. – Примеч. ред.

² Сазонов А. Трехглавый дракон Интернета // Деньги. – 2002. – №36 (391), С. 108, 110.

Указанные средства и составляли основу механизмов защиты на первом этапе. Господствовало убеждение, что основными средствами защиты являются программные средства, причем считалось, что программы защиты информации станут работать эффективнее, если будут включены в состав общесистемных компонентов программного обеспечения. Поэтому первоначально программные механизмы защиты включались в состав операционных систем или систем управления базами данных (например, операционная система фирмы IBM OS/360). Практика показала, что надежность механизмов защиты такого типа явно недостаточная.

Следующей попыткой расширения рамок и повышения эффективности программной защиты стала организация дифференцированного разграничения доступа пользователей к данным, находящимся в АС. Для этого идентифицировались все пользователи и все элементы защищаемых данных, устанавливалось соответствие между идентификаторами пользователей и идентификаторами элементов данных и строилась алгоритмическая процедура проверки лояльности каждого запроса пользователя. Одной из систем с такими механизмами была система MULTIC, испытания и углубленные исследования которой, проведенные в течение трех лет, выявили несколько путей обхода механизмов разграничения доступа [17].

Уникальной по своему содержанию была система безопасности ресурса (СБР) в операционной системе, разработанной под руководством фирмы IBM. Перед разработчиками стояла задача реализовать три основные функции защиты: изоляцию, контроль доступа и контроль уровня защиты. Кроме того, предполагалось, что программная защита будет дополнена комплексом организационных мер под руководством специального должностного лица – офицера безопасности. Всесторонние испытания СБР выявили в ней ряд серьезных недостатков. В итоге специалисты пришли к выводу, что концепция, основанная на концентрации механизмов защиты в рамках операционной системы, не отвечает требованиям надежной защиты информации, особенно в АС с повышенной секретностью.

Для преодоления указанных недостатков принимались следующие меры: 1) создание в механизмах защиты специального организующего элемента – ядра безопасности; 2) децентрализация механизмов защиты вплоть до создания элементов, находящихся под управлением пользователей АС; 3) расширение арсенала используемых средств защиты.

Развитие концепции, основанной на перечисленных решениях, и составило содержание второго этапа (1970-е гг.). Он характеризуется интенсивным развитием средств защиты, особенно технических и криптографических.

Однако, несмотря на принятые меры, надежная защита информации опять оказалась недостижимой, о чем красноречиво говорили факты злоумышленного доступа к ней. К тому же именно в это время была доказана теорема (ее иногда называют теоремой Харрисона) о невозможности решить для общего случая задачу о безопасности произвольной системы защиты при общем задании на доступ [86]. В этой связи в зарубежной печати все чаще стали появляться высказывания о том, что вообще нет предпосылок для надежного обеспечения безопасности информации.

Таким образом, второй период, начавшись с оптимистических надежд на реализацию надежного механизма защиты, закончился унылым пессимизмом. Поиски выхода из этого тупикового состояния и составляют содержание третьего этапа (1980-е гг.) развития концепций защиты информации. Генеральным направлением поисков стало неуклонное повышение системности подхода к самой проблеме защиты информации. Понятие «системность» интерпретировалось как создание соответствующих механизмов защиты, а также как регулярность процесса, осуществляемого на всех этапах жизненного цикла АС при комплексном использовании всех имеющихся средств защиты [87]. При этом все средства, методы и мероприятия, используемые для защиты информации, непременно объединяются в единый целостный механизм – систему защиты.

В этой системе должно быть, по крайней мере, четыре защитных пояса: внешний пояс, охватывающий всю территорию, на которой расположены сооружения АС; пояс сооружений, помещений или устройств АС; пояс компонентов системы (технических средств, программного обеспечения, элементов баз данных) и пояс технологических процессов обработки данных (ввод-вывод, внутренняя обработка и т. п.).

По сообщениям зарубежной печати [84], ярким примером практической реализации системного подхода к защите информации является проект системы защиты, разрабатываемый и реализуемый фирмой Honeywell Inc. по контракту с Министерством обороны США. В качестве исходных были приняты следующие три положения: 1) система защиты информации разрабатывается и внедряется одновременно с разработкой самой АС; 2) функции защиты реализуются преимущественно аппаратно; 3) обеспечение задаваемого уровня защиты должно быть строго доказано. Специалисты центра системных исследований фирмы Honeywell Inc. заявили, что ими разработан математический аппарат, позволяющий определять степень защищенности информации, создание которого будет иметь не меньшее значение, чем создание компьютера с высоким уровнем защиты. Этот математический аппарат разработан на основе дальнейшей разработки средств защиты информации для систем Multics и Scomp, а также при создании фирмой SRI International операционной системы с доказуемой защищенностью данных.

В 1985–1988 гг. проводились исследования по Проекту COST-11 Ter «Механизмы защиты вычислительных сетей» при поддержке Комиссии по европейским коммуникациям с участием европейских университетов, исследовательских институтов и фирм по производству вычислительных сетей. По результатам исследований составлен итоговый отчет, материалы которого легли в основу книги С. Мафтика [40]. В ней предложены отдельные механизмы защиты в нескольких взаимосвязанных областях: криптографии, средств коммуникации, баз данных, управления процессами и т.п. Попытку решить концептуальные вопросы построения защиты в вычислительных сетях в целом удачной назвать нельзя. В книге отмечается необходимость разработки модели защиты для распределенных вычислительных систем, функций управления защитой и высказывается сомнение в правильности определения защищенной вычислительной сети специалистами.

В 1990-х гг. вновь большое внимание стало уделяться проблемам защиты программного обеспечения АС, что обусловлено рядом обстоятельств. Во-первых, программное обеспечение играет решающую роль в качественной обработке информации. Во-вторых, программы становятся предметом коммерческой тайны и авторского права. В-третьих, программные средства являются одним из наиболее уязвимых компонентов АС. Распространение сетевых технологий превратило отдельные машины в локальные сети, совместно использующие общие ресурсы, а применение технологии клиент-сервер преобразовало такие сети в распределенные вычислительные среды. Безопасность такой сети зависит от безопасности составляющих ее компьютеров. Современные технологии телекоммуникации объединяли локальные сети в глобальные, что привело к появлению такого уникального явления, как Интернет. Возникновение Интернета создало огромные возможности для несанкционированного доступа к информации ее абонентов по всему миру. Особую тревогу вызывает все, что связано с компьютерным вирусом. В связи с этим в зарубежной печати снова стали появляться заявления о принципиальной невозможности построения надежной защиты информации в АС [16].

Параллельно с исследованиями до настоящего времени ведется работа по выпуску стандартов в области создания «защищенных» систем обработки информации. В США с 1983 г. опубликовано несколько книг так называемой радужной серии. Затем появились интерпретация «Оранжевой книги» для сетевых конфигураций, «Канадские критерии», «Гармонизированные критерии Европейских стран», «Федеральные критерии» и проект международного стандарта «Общие критерии безопасности» [59]. В России аналогичные стандарты вышли в 1992 г. и были дополнены в последующие годы. В рамках проекта «Общие критерии» в 1999 г. выпущен международный стандарт ИСО/МЭК 15408–99 «Критерии оценки безопасности информационных технологий» [68].

В перечисленных документах условия гарантий политики безопасности формулируются без доказательств. Критерием оценки «защищенности» служит выполнение заданного набора защитных функций без количественных показателей. Первое обстоятельство свидетельствует о том, что их до сих пор нет. Последнее наводит на мысль, что стандарту подвергается конструкция, не имеющая обозначенных границ, и нет ничего удивительного в том, что практически все системы защиты основаны на анализе результатов успешно состоявшихся атак на момент разработки этой системы, что предопределяет их отставание в будущем. В качестве примера можно привести ситуацию с закрытием «внезапно» обнаружившихся «дыр» в операционных системах UNIX, Windows или антивирусные средства, которые в основном обнаруживают и уничтожают только известные вирусы. Кроме того, применяемые средства защиты настроены на определенные аппаратные и программные платформы и в случае изменения последних перестают работать.

Анализ проблемы и путей ее решения, а также опыт разработки соответствующих систем и приведенные ниже исследования позволяют предположить следующие причины перечисленных недостатков. Это прежде всего отсутствие четких и ясных определений объектов и предмета защиты, оптимальных классификаций потенциальных угроз и возможных каналов несанкционирован-

ного доступа (НСД), отсутствие адекватных моделей объекта защиты информации и ожидаемой модели поведения нарушителя. Деление отдельных средств защиты на аппаратные, физические, программные, инженерные и прочие, т.е. по технологии исполнения (не по прямому назначению), положенное в основу принципов построения системы защиты, не учитывает их функциональные возможности по взаимодействию и создает предпосылки для образования «щелей» в защите.

При построении защиты часто не учитываются различие предметов защиты, возможных каналов НСД и соответствующих им средств защиты на этапах проектирования и эксплуатации АС.

Отсутствие четкой и обоснованной классификации объектов обработки и защиты информации по принципам построения не позволило найти единого подхода к территориально-сосредоточенным и глобальным АС.

Предполагаемой причиной неудач явилось также и то, что используемое представление потенциальных угроз не полностью учитывает их физическое происхождение и точки приложения в конкретной вычислительной системе (например, различную природу случайных и преднамеренных воздействий). В результате этого не точно определяются возможные подходы нарушителя к объекту защиты, что, в свою очередь, не позволяет установить соответствующие преграды.

Модель поведения нарушителя часто не проясняет его исходную позицию и не учитывает его стремление использовать наиболее слабое звено в защите. Практически полностью отсутствуют обоснование и реализация принципа равнопрочности звеньев защиты, вытекающего из необходимости создания вокруг предмета замкнутой оболочки защиты.

Почти не учитывается при разработке и не оценивается в количественном отношении принципиально важное свойство звеньев защиты – способность к своевременному обнаружению и блокировке несанкционированных действий нарушителя по аналогии с функциональным контролем вычислительной системы.

Выявленные недостатки и трудности решения проблемы дают основание искать их причины в анализе объектов обработки и защиты информации, потенциальных угроз и выборе другой концепции защиты информации.

Решение проблемы автор видит в пересмотре существующей парадигмы информационной безопасности: переходе от создания защитной среды к созданию защитной оболочки. Для того чтобы остановить нарушителя, необходимо уточнить предмет защиты, определить типовые объекты обработки данных, возможные точки приложения его усилий на автоматизированной системе и установить на его пути систему взаимосвязанных преград, образующих защитную оболочку необходимой прочности.

В заключение приведем список ключевых терминов, определяющих понятийный аппарат области исследования, что поможет нам однозначно воспринимать излагаемый ниже материал. Как советовал великий А.С. Пушкин: «Определяйте значения слов... и вы избавите свет от половины его заблуждений».

Администрация автоматизированной системы (АС) – должностные лица, наделенные владельцем автоматизированной системы правами по управлению процессами ввода-вывода, хранения, обработки и передачи информации.

Административные меры по защите информации – меры, принимаемые администрацией системы по обеспечению безопасности информации в организационном порядке согласно разработанной ею должностной инструкции и действующему законодательству в рамках наделенных полномочий.

Автоматизированное рабочее место (АРМ) – работающие автономно, в составе вычислительной сети или вычислительного комплекса персональная ЭВМ с прикладным программным обеспечением (ПО) или специально разработанное рабочее место на базе аппаратных стандартных вычислительных элементов и нестандартных общего и прикладного программного обеспечения.

Автоматизированная система управления (АСУ) – территориально распределенная региональная или глобальная вычислительная структура, состоящая из сети передачи данных и ее абонентов – комплексов средств автоматизации (КСА) с иерархической системой отношений и принадлежащая одной организации. В глобальную АСУ может входить несколько региональных структур.

Аутентификация – проверка подлинности субъекта или объекта.

Абонентское шифрование – шифрование информации в вычислительных сетях или АСУ в тракте передачи данных от пользователя к пользователю.

Аварийная ситуация – случайные воздействия на информацию в результате отказа функционирования вычислительной системы по причине аварий: энергопитания, жизнеобеспечения, пожаров, наводнений и других случайных событий подобного рода.

Безопасность информации – защита информации от утечки, модификации и утраты (предмет защиты – информация).

Безопасность АС – защита системы обработки информации от внешних несанкционированных преднамеренных и случайных воздействий на ее технические средства (предмет защиты – система обработки информации).

Верификация – проверка целостности и подлинности информации, программы, документа и т.д.

Вычислительный комплекс (ВК) – аппаратно-программная вычислительная структура, состоящая из дублирующих друг друга ЭВМ, работающая в составе информационного вычислительного комплекса (ИВК) или локальной вычислительной сети (ЛВС).

Защита информации от несанкционированного доступа (НСД) – см. *Безопасность информации*.

Информация – сведения о внутреннем и окружающем мире, событиях, процессах и т.д., воспринимаемые и передаваемые людьми устным, письменным или другим способом (с помощью условных сигналов, технических или вычислительных средств и т.д.).

Информационный вычислительный комплекс (ИВК) – автоматизированная система, состоящая из мощного универсального вычислительного комплекса с централизованной обработкой данных и внешних устройств, в числе которых могут быть рабочая станция (РС), АРМ, принтеры, табло отображения и т.д.

Идентификация – присвоение имени субъекту или объекту. Иногда используется для аутентификации.

Криптография – метод специального преобразования информации с целью защиты от ознакомления и модификации посторонним лицом.

Кодирование информации – представление информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и ввода-вывода. Иногда употребляется в значении «шифрование».

Комплекс средств автоматизации (КСА) – территориально сосредоточенная или распределенная автономная или являющаяся элементом региональной или глобальной вычислительной сети (АСУ) автоматизированная система, состоящая из одного (ой) или нескольких объединенных линиями связи и общими задачами АРМ, РС, ИВК и ЛВС.

Корпоративная сеть – некоторое наложенное (виртуальное) пространство с ограниченным (защищенным) доступом к передаче, обработке и хранению информации, принадлежащей корпорации (организации), реализованное как на ресурсах сетей связи общего пользования, так и на выделенных каналах связи и средствах коммутации организации.

Локальная вычислительная сеть (ЛВС) – автоматизированная система, состоящая из группы РС (АРМ) и вспомогательных технических средств (серверов, общего принтера, коммутатора и др.), соединенных между собой линиями связи и объединенных сетевым аппаратным и программным обеспечением в целях выполнения общей задачи на ограниченной территории.

Линейное шифрование – криптографическое преобразование информации при ее передаче по прямым каналам связи от одного элемента вычислительной сети (КСА) к другому.

Модификация информации – несанкционированное изменение информации, корректное по форме и содержанию, но отличное по смыслу.

Нарушитель в АС – посторонний человек или законный пользователь, предпринимающий попытку несанкционированного доступа к информации в корыстных интересах, для самоутверждения или развлечения.

Несанкционированный доступ к информации – действия нарушителя с целью похитить, разрушить, модифицировать информацию или ознакомиться с ее содержанием.

Объект обработки и защиты информации – автоматизированная система обработки данных, содержащая информацию, подлежащую защите.

Опознавание пользователя – см. *Аутентификация*.

Оперативная информация – информация прикладных функциональных задач АС.

Организационные мероприятия по защите информации – мероприятия с участием человека и административные меры, включаемые в должностную инструкцию пользователя.

Пользователь АС – владелец АС. Должностное лицо, работающее с прикладными задачами АС.

Программный вирус – специально разработанная программа-вредитель, имеющая способность разрушать программное обеспечение и информацию АС и воспроизводить себе подобных.

Предмет защиты в АС – информация, подлежащая защите по техническому заданию на АС.

Пароль – строка или последовательность символов, недоступных для посторонних, предназначенных для идентификации и аутентификации субъектов или объектов между собой.

Прочность защиты информации в АС – вероятность преодоления защиты (преграды) нарушителем за установленный промежуток времени.

ПЭМИН – побочное электромагнитное излучение информации и наводки на цепях питания, заземления, вспомогательного и сервисного оборудования.

Рабочая станция (РС) – работающий в составе вычислительной сети или вычислительного комплекса стандартный персональный компьютер (ПК) с сетевым аппаратным и программным обеспечением, а также пакетом прикладных программ.

Ресурсы АС – средства ввода-вывода, хранения, передачи и обработки информации в АС (программные и аппаратные).

Случайный НСД – случайные воздействия на информацию, приводящие к ее утрате, модификации и несанкционированному ознакомлению с ней посторонних лиц.

Система защиты информации АС – система, встроенная в структуру АС, представляющая собой регулируемый механизм, состоящий из системы взаимосвязанных централизованно управляемых преград, перекрывающих возможные каналы несанкционированного доступа к информации, подлежащей защите от НСД.

Секретность информации – уровень ответственности пользователя, работающего с этой информацией, и нарушителя за несанкционированный доступ к ней по закону или уставу частной организации.

Сеть передачи данных (СПД) – территориально распределенная региональная или глобальная вычислительная сеть, состоящая из одного или нескольких узлов коммутации, выполняющих задачи маршрутизации сообщений, каналов связи между ними и аппаратуры передачи данных КСА, являющихся одновременно ее абонентами и элементами АСУ.

Технологическая информация АС – информация, связанная с обеспечением функционирования аппаратных и программных средств АС.

Телекоммуникационная вычислительная сеть (ТВС) – территориально распределенная региональная или глобальная вычислительная сеть, состоящая из нескольких узлов коммутации, выполняющих задачи маршрутизации сообщений, каналов связи между ними и аппаратуры передачи данных КСА, являющихся ее абонентами. Данная сеть выполняет услуги по обмену данными и предоставлению своих данных.

Уровень безопасности информации в АС – группа показателей прочности защиты, соответствующая определенному классу защиты.

Утечка информации – ознакомление постороннего лица с содержанием секретной информации.

Утрата информации – потеря, хищение, разрушение или неполучение переданных данных.

Функциональный контроль – метод обеспечения контроля функционирования АС с целью обнаружения отказов, неисправностей, ошибок и сбоев аппаратуры, программного обеспечения и ошибок человека.

Целостность данных – неизменность данных.

Шифрование информации – криптографическое преобразование информации в целях ее защиты от ознакомления и модификации посторонними лицами.

Эффективность защиты информации – способность системы защиты информации обеспечить достаточный уровень своей безопасности.

АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ КАК ОБЪЕКТЫ ОБРАБОТКИ И ЗАЩИТЫ ИНФОРМАЦИИ

1

1.1. Предмет защиты

1.1.1. Свойства информации

Информация – это результат отражения и обработки в человеческом сознании многообразия внутреннего и окружающего мира, это сведения об окружающих человека предметах, явлениях природы, деятельности других людей и т.д., а также сведения о его внутреннем состоянии. Сведения, которыми человек обменивается через машину с другим человеком или с машиной и являются предметом защиты в автоматизированной системе. Однако защите подлежит не всякая информация, а только та, которая имеет цену.

Ценность информации является критерием при принятии любого решения о защите. Несмотря на то что было предпринято немало попыток формализовать этот процесс с использованием методов теории информации и анализа решений, критерий оценки до сих пор остается весьма субъективным. Для оценки требуется не только разделение информации на категории в соответствии с ее ценностью, но и важностью. Известно [69] следующее разделение информации по степени важности:

- жизненно важная незаменимая информация, наличие которой необходимо для функционирования организации;
- важная информация – информация, которая может быть заменена или восстановлена, но процесс восстановления очень труден и связан с большими затратами;
- полезная информация – информация, которую трудно восстановить, однако организация может эффективно функционировать и без нее;
- несущественная информация – информация, которая может быть больше не нужна организации.

На практике отнесение информации к одной из этих категорий представляет собой довольно трудную задачу, так как одна и та же информация может быть использована многими подразделениями организации, каждое из которых может отнести эту информацию к различным категориям важности. Категория важности, как и ценность информации, обычно изменяется со временем и зависит от отношения к ней различных групп потребителей и потенциальных нарушителей.

Существуют определенные группы лиц, связанных с обработкой информации: *держатель* – организация или лицо – обладатель информации; *источник* – организация или лицо, поставляющая информацию; *нарушитель* – отдельное лицо или организация, стремящийся получить, изменить или уничтожить эту информацию. Отношение этих групп к значимости идентичной информации может быть различным: для одной – важная, для другой – нет. Например:

- важная оперативная информация, такая, как список заказов на данную неделю и график производства, может иметь высокую ценность для держателя, тогда как для источника (например, заказчика) или нарушителя она низка;
- персональная информация, например медицинская, имеет значительно большую ценность для источника (лица, к которому относится информация), чем для ее держателя или нарушителя;
- информация, используемая руководством для выработки решений, например о перспективах развития рынка, может быть значительно более ценной для нарушителя, чем для источника или ее держателя, который уже завершил анализ этих данных.

Приведенные категории важности заслуживают внимания и могут быть применены к любой информации. Это также согласуется с существующим принципом деления информации по уровням секретности. Уровень секретности – это административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю конкретной секретной информации, регламентируемой специальным документом, с учетом государственных, военно-стратегических, коммерческих, служебных или частных интересов. Такой информацией может быть государственная, военная, коммерческая, служебная или личная тайна.

Практика показала, что защищать необходимо не только секретную информацию. Несекретная информация, подвергнутая несанкционированным изменениям (например, модификации команд управления), может привести к утечке или потере связанной с ней секретной информации, а также к невыполнению автоматизированной системой заданных функций по причине получения ложных данных, которые могут быть не обнаружены пользователем системы.

Суммарное количество или статистика несекретных данных в итоге могут оказаться секретными. Аналогично сводные данные одного уровня секретности в целом могут являться информацией более высокого уровня секретности. Для защиты от подобных ситуаций широко применяется разграничение доступа к информации по функциональному признаку. При одинаковой степени важности информации, обрабатываемой в системе обработки данных, информация делится в соответствии с функциональными обязанностями и полномочиями пользователей, устанавливаемыми администрацией организации-владельца АС.

Согласно приведенным принципам деления информации, обрабатываемую в АС, для иллюстрации можно представить в виде пирамиды, состоящей из нескольких уровней по вертикали по категориям важности и секретности. Вершиной пирамиды является наиболее важная информация, а фундаментом – несекретная информация, связанная с обработкой более важной (секретной)

информации. Каждый уровень данной пирамиды, поделенный на части по горизонтали, отражает принцип деления информации по функциональному признаку и полномочиям ($p_1, p_2 \dots p_n$) ее пользователей (рис. 1.1).

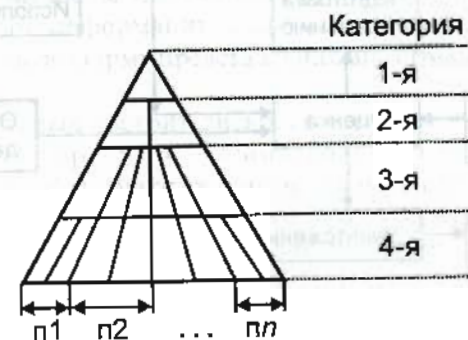


Рис. 1.1. Модель предмета защиты

Важной может быть не обязательно секретная информация, например статистические отчетные данные по результатам эксплуатации проданных изделий.

До последнего времени безопасность информации в АС понималась исключительно как опасность ее несанкционированного получения во все время нахождения в АС. В настоящее время безопасность интерпретируется еще и как безопасность действий, для осуществления которых используется информация. Соответствующие команды управления тоже относятся к информации. Принципиальные отличия расширенного толкования по сравнению с традиционным очень важны, так как вычислительная техника все больше используется для автоматизированного и автоматического управления высокоответственными информационными системами и процессами, в которых несанкционированные изменения запланированных алгоритмов могут иметь серьезные последствия.

У информации в АС есть свой жизненный цикл (рис. 1.2), описание которого приведено в работе В. Г. Журавлева¹.

Полученная системой информация оценивается на достоверность и полезность. Часть информации уничтожается, а остальная подготавливается к хранению (систематизируется, преобразуется в удобную для хранения форму, сортируется по массивам хранения). Из хранилища выбирается нужная в данный момент времени информация, обрабатывается и используется в определенных целях. Полученные отчетные данные проходят тот же цикл. При выборке могут уничтожаться сведения, потерявшие цену из-за их старения. Количественные оценки цены и времени старения информации, приводимые в литературе, по причине сложности задачи довольно трудны, неточны и противоречивы. Время жизни информации определяется ее владельцем в процессе эксплуатации АС в конкретных условиях.

¹ См.: Журавлев В. Г. Основы АСУ. – Кишинев: Штиинца, 1975.

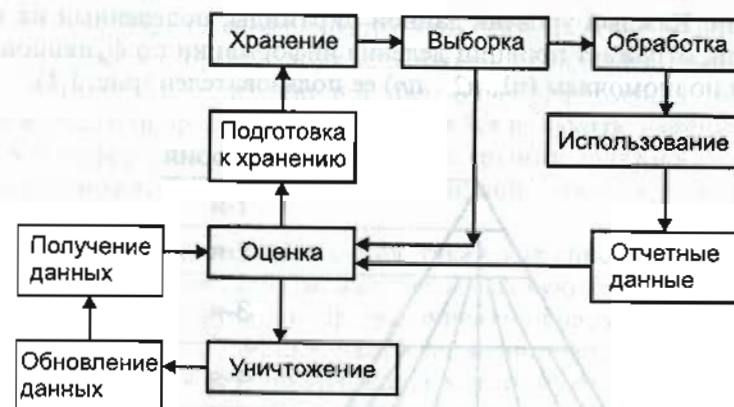


Рис. 1.2. Жизненный цикл информации

1.1.2. Виды и формы представления информации

Информация может быть представлена в следующем виде: букв, символов, цифр; слов; текста; рисунков; схем; формул; графиков; таблиц; планов; чертежей; карт географических, топографических и т.д.; технологических карт; алгоритмов и т.д., которые, в свою очередь, могут быть представлены в виде: постоянных или переменных данных; команд; сообщений; справок; решений; приказов; распоряжений; заданий; отчетов; ведомостей; инструкций; комментариев; писем и записок; телеграмм; чеков; массивов; файлов.

1.1.3. Машинное представление информации

Информация, воплощенная и зафиксированная в некоторой материальной форме, называется сообщением. Сообщения могут быть непрерывными и дискретными (цифровыми).

Непрерывное сообщение представляется определенной физической величиной (электрическим напряжением, током и т.д.), изменения которой отображают протекание рассматриваемого процесса. Физическая величина, передающая непрерывное сообщение, может принимать любые значения и изменяться в произвольные моменты времени. Таким образом, в непрерывном сообщении конечной длины может содержаться большое количество информации.

Для дискретных сообщений характерно наличие фиксированного набора отдельных элементов, из которых в дискретные моменты формируются различные последовательности элементов. Важным является не физическая природа элементов, а то обстоятельство, что набор элементов конечен, и потому любое дискретное сообщение конечной длины передает конечное чис-

ло значений некоторой величины, следовательно, количество информации в таком сообщении конечно.

При дискретной форме представления информации отдельным элементам ее могут быть присвоены числовые (цифровые) значения. В таких случаях говорят о цифровой информации, а вычислительные машины и системы, использующие цифровую форму представления информации, называются также цифровыми.

Элементы, из которых состоит дискретное сообщение, называют буквами, или символами. Набор этих букв (символов) образует алфавит. Здесь под буквами понимаются любые знаки (обычные буквы, цифры, знаки препинания, математические и прочие знаки, цвета сигнальных ламп и др.). Число символов в алфавите называется объемом алфавита. Объем алфавита определяет количество информации, доставляемой одним символом сообщения. Если алфавит имеет объем A и в любом месте в сообщении равновероятно появление любого символа, то доставляемое символом количество информации можно определить как [63]:

$$I_0 = \log_2 A \text{ [бит]}. \quad (1.1)$$

Дискретное сообщение можно разбить на группы символов и назвать эти группы словами. Длина слова определяется количеством содержащихся в нем символов.

В вычислительной технике широко используется однородное представление информации, при котором в вычислительной системе или отдельных ее частях все слова имеют определенную длину. Однородное представление информации упрощает обмен ею и конструкцию устройств вычислительной системы.

Известно, что в алфавите объемом A можно представить N различных слов длиной в количестве символов S , где

$$N = A^S. \quad (1.2)$$

Тогда количество информации, содержащейся в слове, равно:

$$I_1 = \log_2 N = S \cdot \log_2 A = S \cdot I_0. \quad (1.3)$$

Выражение (1.3) справедливо, если вероятность появления в сообщении любого слова (и символа) равна и не зависит от предшествующих слов (и символов).

Неравномерность появления символов, наличие взаимной зависимости символов в сообщении, как это имеет место, например, при передаче смысловых сообщений (текста), являются причиной того, что количество информации в одном символе уменьшается.

Связь между символами сообщения создает избыточность информации. В языке избыточность носит естественный характер. Однако в вычислительных системах широко применяется искусственная избыточность при

кодировании сообщений, которая позволяет контролировать и устранять ошибки при передаче информации по линиям связи, а также между отдельными устройствами вычислительной системы.

В вычислительных машинах и системах широко употребляется двоичный алфавит, имеющий лишь два символа 0 (нуль) и 1 (единица). Его применение упрощает техническую реализацию устройств вычислительной техники. Любое дискретное сообщение, выраженное в некотором алфавите, переводимо в двоичный алфавит, если длина двоичного слова отвечает формуле

$$S_2 > S_1 \log_2 A_1.$$

Современные вычислительные системы обрабатывают не только числовую, но и текстовую, иначе говоря, алфавитно-цифровую информацию, содержащую цифры, буквы, знаки препинания, математические и другие символы. Именно такой характер имеет экономическая, планово-производственная, учетная, бухгалтерская, статистическая и другая информация, содержащая наименование предметов, фамилии людей, числа и т.д.

Характер этой информации таков, что для ее представления требуются слова переменной длины. Применение для записи алгоритмов и автоматизация программирования алгоритмических языков делают необходимым ввод в машину и вывод наряду с общеупотребительными еще и ряд некоторых специальных символов.

Деловая информация в среднем содержит вдвое больше цифр, чем букв. Поэтому наряду с общей системой кодирования алфавитно-цифровых символов в ЭВМ сохраняют также отдельную систему кодирования для десятичных цифровых данных.

В последние годы наибольшее распространение получило представление информации посредством восьмиразрядного слога, называемого *байтом*.

При помощи байта можно кодировать 256 различных символов. Несколько байтов образуют слова.

Электронно-вычислительная машина производит обработку информации, состоящую в ее запоминании, передаче из одних устройств в другие, выполнении арифметических и логических преобразований. Процесс обработки информации автоматизирован при помощи программного управления. Программа представляет собой алгоритм переработки информации, записанной в виде последовательности команд, которые должны быть выполнены машиной для получения искомого результата.

Используемые человеком при расчетах, обработке экономической, планово-производственной и другой информации, при программировании задач натуральные формы представления и натуральные единицы информации существенно отличаются от форм представления и единиц информации в ЭВМ.

С целью ознакомления с систематизацией сведений по кодированию информации в ЭВМ рассмотрим иерархию натуральных и соответствующих машинных единиц информации (в порядке возрастания размеров единиц информации).

Поле – группа символов, имеющих определенное значение и подвергающихся обработке за одну и ту же арифметическую или логическую операцию. К ним относятся: многоразрядное число, команда, группа символов, обозначающих определенный признак-реквизит какого-либо объекта (например, фамилия или год рождения некоторого лица, наименование детали, вес и т.д.).

Запись – представляет собой группу полей, описывающих признаки (свойства, характеристики, параметры) некоторого объекта. Например, строка экзаменационной ведомости:

Фамилия	№ зачетной книжки	Дисциплина	Оценка
Степанов	27035	ЭВМ	5

Каждый из реквизитов (признаков) – фамилия, номер зачетной книжки и т.д. – является полем. Поля объединены тем, что относятся к определенному студенту.

Массив – объединение записей, описывающее некоторое множество объектов (например, экзаменационная ведомость или их совокупность).

Слово – группа символов (разрядов) в памяти ЭВМ, соответствующая некоторому полю. Обычно термин «машинное слово» относят к коду определенной длины, который считывается из оперативного запоминающего устройства (ОЗУ) или записывается в ОЗУ за одно обращение. Машинное слово может представлять собой двоичное число с плавающей или фиксированной запятой, команду, несколько слогов (байтов). Оно может также содержать дополнительные разряды (разряд контроля по четности, разряды защиты памяти и др.). Как правило, машинное слово, в частности команда, содержит целое число байтов.

Машинная единица информации, соответствующая натуральной единице – записи, называется *фразой* (или также *записью*). Она может занимать несколько машинных слов.

Блоком называют группу фраз (записей), расположенных компактно (без промежутков) на носителе внешнего запоминающего устройства (ЗУ) и записываемых на носитель из ОЗУ, а также считываемых с носителя в ЗУ одной командой. Среди натуральных единиц информации нет единицы, соответствующей блоку.

Информационному массиву соответствует машинная единица информации – *файл*. Он состоит в общем случае из нескольких блоков.

Томом называется машинная единица информации, соответствующая пакету дисков.

1.1.4. Физическое представление информации и процессы ее обработки

Как было показано выше, в вычислительных системах информация представляется в двоичном алфавите. Физическими аналогами знаков этого алфавита служат физические сигналы, способные принимать два хорошо

различимых значения, например электрическое напряжение (потенциал) высокого и низкого уровней, отсутствие и наличие импульса тока, противоположные по знаку значения напряженности магнитного поля и т.п.

Настоятельным требованием к физическим аналогам двоичного алфавита является возможность надежного распознавания двух различных значений сигнала, которые при описании законов функционирования схем обозначаются символами 0 и 1.

В схемах цифровых устройств переменные и соответствующие им сигналы изменяются и воспринимаются не непрерывно, а лишь в дискретные моменты времени – по тактовым импульсам.

В цифровых устройствах применяют три способа физического представления информации: потенциальный, импульсный и динамический. Слово может быть представлено последовательным или параллельным способом (кодом). Устройства последовательного действия работают медленнее, чем параллельного. Однако устройство параллельного действия требует большего объема аппаратуры. В вычислительной технике применяются оба способа в зависимости от требований, предъявляемых к конкретному изделию.

Информация в автоматизированной системе подвергается различным процессам: вводу-выводу, хранению, обработке и передаче.

Ввод информации в автоматизированную систему осуществляется с магнитных лент, дисков, с помощью универсальной и формализованной клавиатуры и т.д.

Хранение информации производится в запоминающих устройствах: кратковременное – в ОЗУ и в различных регистрах памяти, выполненных на полупроводниковых приборах, магнитных элементах; долговременное – во внешних запоминающих устройствах, выполненных на магнитных лентах, дисках (жестких типа «винчестер» и гибких магнитных дисках – ГМД), лазерных компакт-дисках с однократной и многократной записью и т.д.

Обработка информации в вычислительной системе производится в соответствии с принятой в данной системе системой команд, алгоритмами, определяемыми программным обеспечением и командами, поступающими с внешних устройств управления.

Вывод информации производится на внешние устройства связи и регистрации без ее визуального отображения (на перечисленные выше запоминающие устройства) и устройства с отображением: печатающие устройства, индикаторы, табло и другие устройства индивидуального и коллективного отображения. Выбор метода обработки информации определяется характером решаемых задач, особенностями используемой информации, а также параметрами технических средств автоматизации и возможностями программного обеспечения вычислительных средств.

Передача информации производится по линиям и каналам связи и узлам коммутации. В зависимости от назначения и сложности поставленных задач в автоматизированной системе происходят обработка и формирование документов различного рода и объемов.

Информационные процессы в системах обработки данных типа АСУ (корпоративной вычислительной сети) можно условно разделить на три группы [4]:

- информационно-справочное обеспечение должностных лиц органов управления;

- информационное обеспечение расчетных задач;
- обслуживание информационной базы АСУ.

Эти процессы реализуют должностные лица органов управления и обслуживающий персонал АСУ с помощью аппаратных средств автоматизации и связи, программного обеспечения и информационной базы АСУ.

По степени стабильности информацию делят на условно-постоянную и переменную. К условно-постоянной информации относятся данные, которые в течение длительного времени не меняются. По использованию в процессах управления вся информация делится на нормативную, справочную, плановую, оперативно-производственную, отчетную и аналитическую.

Обработанная информация выдается должностным лицам непосредственно на их автоматизированные средства управления и контроля (на устройства печати и отображения индивидуального пользования) либо на устройства выдачи информации коллективного пользования (печати, регистрации графической информации, табло отображения коллективного пользования).

На объектах АСУ накапливаются и хранятся большие объемы информации как документальной (в виде обычных документов), так и на машинных носителях.

Документальная информация содержит:

- ведомость учета хранимых документов;
- документы, прошедшие обработку на объекте АСУ;
- ведомость регистрации запросов должностных лиц и обслуживающего персонала на получение справок и решение задач;
- ведомость регистрации выдаваемой информации и другие документы.

На машинных носителях хранятся:

- информационные массивы общего информационного поля;
- архивные данные;
- программные блоки, файлы, тома.

Информационные массивы общего информационного поля используются для выдачи различных справок по запросам, а также для информационного обеспечения расчетных задач.

В состав архивных данных входит информация, которая в данный момент в работе системы не участвует, но может понадобиться для восстановления или замены массивов, документирования работы системы и т.д.

Информационное единство в АСУ обеспечивается следующими путями [4]:

- созданием системы классификации и кодирования информации;
- разработкой и внедрением унифицированных систем документации;
- унификацией принципов построения нормативов и их обновлением;
- унификацией системы показателей для обеспечения сопоставляемости во времени и по различным качественным и количественным признакам;
- регламентацией потоков информации по направленности, объему, периодичности, достоверности и срочности;
- унификацией порядка формирования и обработки данных.

1.1.5. Информация и ресурсы

Физическое представление информации и процессы ее обработки говорят о том, что реализация системы защиты может быть направлена также на защиту аппаратных и программных средств, составляющих автоматизированную систему обработки данных, т.е. ее ресурсов, имея в виду, что защита последних обеспечивает и защиту информации.

Понятие «ресурсы» в широком смысле слова подразумевает запасы чего-либо, возможности и т.д. В вычислительных системах под ресурсами понимают программные и аппаратные средства обработки, хранения и передачи информации, которых может хватить или не хватить вообще или в данный момент времени. Поэтому понятие «ресурсы» не могут иметь описанные выше свойства информации и некоторые свойства средств ее обработки. В этом случае предмет защиты выходит за рамки данного понятия. Некоторые специалисты, почувствовав это, ввели понятие «информационные ресурсы», еще более усугубив положение.

В буквальном смысле данное понятие с учетом сказанного выше приобретает значение информационных запасов. Информация не материальна и не может быть расходным материалом (исключение составляют «запасы знаний» – но это имеет совсем другой смысл). Некорректность употребления данного понятия очевидна.

Кроме того, информация может быть защищена без аппаратных и программных средств защиты с помощью криптографического преобразования. При этом нарушитель имеет доступ к аппаратным и программным средствам, а к информации доступа не имеет. Как показывает практика, законный пользователь, имеющий доступ к некоторым ресурсам АС, также может быть нарушителем. Информация, передаваемая по открытым каналам и линиям связи, по побочным электромагнитным излучениям может быть перехвачена нарушителем без физического доступа к ресурсам АС.

Информация – это предмет собственности. Она может быть собственностью владельца АС, государства, той или иной организации, фирмы, частной или общественной, личной собственностью человека, доверившего ее владельцу АС. Владельцами информации и ресурсов АС могут быть разные лица и организации. А там, где речь идет о праве собственности, должны быть четкость, ясность и определенность. Соблюдение гарантий этих прав обеспечивает безопасность информации.

Таким образом можно утверждать, что защита ресурсов не всегда гарантирует защиту информации. Поэтому предметом защиты в АС является прежде всего информация. Что обрабатываем, то и защищаем.

1.1.6. Информация как объект права собственности

По существу, сфера безопасности информации – не защита информации, а защита прав собственности на нее. Попробуем это показать на материалах работы [76].

Рассмотрим особенности информационной собственности.

Исторически традиционным объектом права собственности является материальный объект. Фактически право собственности до настоящего времени являлось вещным правом.

Как мы знаем, информация не является материальным объектом, тем не менее она неразрывно связана с материальным носителем. Это – человеческий мозг или отчужденные от человека материальные носители, такие, как книга, дискета и другие виды «памяти» (запоминающие устройства).

С философской точки зрения, видимо, можно говорить об информации как об абстрактной субстанции, существующей сама по себе, но для нас ни хранение, ни передача информации без материального носителя невозможны.

Информация как объект права собственности копируема (тиражируема) за счет материального носителя. Материальный объект права собственности не копируем. Действительно, если рассмотреть две одинаковые вещи, то они состоят из одинаковых структур, но материально разных молекул. А информация при копировании остается той же, это – то же знание, та же семантика.

Информация как объект права собственности легко перемещается к другому субъекту права собственности без очевидного (заметного) нарушения права собственности. Перемещение материального объекта к другому субъекту права собственности неизбежно и, как правило, влечет за собой утрату этого объекта первоначальным субъектом права собственности, т.е. происходит очевидное нарушение его права собственности.

Опасность копирования и перемещения информации усугубляется тем, что она, как правило, отчуждаема от собственника, т.е. хранится и обрабатывается в сфере доступности большого числа субъектов, не являющихся субъектами права собственности на эту информацию. Это, например, автоматизированные системы, в том числе и сети.

В остальном информация ничем не отличается от традиционных объектов права собственности.

Право собственности включает три правомочия собственника, составляющие содержание (элементы) права собственности: право распоряжения; право владения; право пользования.

Субъект права собственности на информацию может передать часть своих прав (распоряжение), не теряя их, другим субъектам, например «хранителю», т.е. владельцу материального носителя информации (это – владение или пользование) или пользователю (это – пользование и, может быть, владение).

Для информации право распоряжения подразумевает исключительное право (т.е. никто другой, кроме собственника) определять, кому эта информация может быть предоставлена (во владение и пользование).

Право владения подразумевает иметь эту информацию в неизменном виде. Право пользования – использовать эту информацию в своих интересах.

Таким образом, к информации, кроме субъекта права собственности на эту информацию, могут иметь доступ другие субъекты права собственности как законно, санкционированно (это – субъекты права на элементы собственности), так и незаконно, несанкционированно. Возникает сложная система взаимоотношений между этими субъектами права собственности.

Данные взаимоотношения должны регулироваться и охраняться, так как отклонения от них могут привести к перемещению информации, что влечет за собой нарушение права собственности субъекта на нее. Другими словами, речь идет о реализации права собственности на информацию. Под этим будем понимать государственную или частную (или государственно-частную) инфраструктуру, предотвращающую нарушение права собственности на информацию.

Как и любой объект собственности, такая инфраструктура состоит из цепочки: законодательная власть – судебная власть – исполнительная власть (закон – суд – наказание).

Закон должен предусматривать ответственность и полномочия субъектов права собственности (на элементы собственности). Каждый такой субъект в рамках предоставленных ему собственником полномочий несет перед ним ответственность за предусмотренное законом и подтвержденное судом превышение этих полномочий, которое привело или могло привести к нарушению права собственности собственника информации.

Итак, несмотря на ряд особенностей, информация наряду с традиционными материальными объектами может и должна рассматриваться законом как объект права собственности.

Любой закон о собственности должен, зафиксировав субъектов и объектов права собственности, регулировать отношения между субъектами, а также между субъектами и объектами права собственности в целях предотвращения нарушения, другими словами, защиты прав собственника, как, впрочем, и прав субъектов права на элементы собственности, например прав законных владельцев или законных пользователей объектов права собственности. Особенности регулирования этих отношений зависят от специфики объектов права собственности.

В рассматриваемом случае информационной собственности ввиду перечисленных выше особенностей информации как объекта права собственности (копируемость, перемещаемость, отчуждаемость) закон должен регулировать отношения субъектов, а также субъектов и объектов права собственности на информацию в целях защиты прав как собственника, так и законных владельцев и пользователей информации. Нарушение информационной собственности заключается в разглашении, несанкционированном изменении, разрушении, блокировке доступа и ознакомлении с ней путем копирования, модификации или уничтожения [76]. Учитывая возможность хищения информации вместе с ее носителем, необходимо указать и на эту угрозу, в результате осуществления которой могут также произойти утечка и утрата информации. Под модификацией информации понимается ее несанкционированное изменение, корректное по форме и содержанию, но отличное по смыслу.

Впервые в правовой практике России информация определяется в качестве объекта права в Гражданском кодексе РФ (ст. 128), принятом Государственной Думой 21.10.94 г. Федеральным законом «Об информации, информатизации и защите информации» от 20.02.95 г. определено, что информационные ресурсы, т.е. отдельные документы или массивы документов, в том числе и в информационных системах, являясь объектами отношений физических, юридических лиц и государства, подлежат обязательному

учету и защите как материальное имущество собственника (ст. 4.1, 6.1). Этим же законом впервые вводится понятие «документированная информация с ограниченным доступом» (ст. 10.2), которая подразделяет информацию на две категории: относящуюся к государственной тайне, и конфиденциальную (т.е. представляющую коммерческую, личную, служебную и другие тайны).

Таким образом можно определить цель обеспечения безопасности информации, которая заключается в защите прав собственности на нее, и задачи безопасности информации, которые состоят в ее защите от утечки, модификации и утраты.

1.1.7. Информация как коммерческая тайна

Понятие «коммерческая тайна» введено в нашу практику с 1 января 1991 г. статьей 33 Закона «О предприятиях в СССР», которая гласит:

«1. Под коммерческой тайной предприятия понимаются не являющиеся государственными секретами сведения, связанные с производством, технологией, управлением, финансами и другой деятельностью предприятия, разглашение (передача, утечка) которых могут нанести ущерб его интересам.

2. Состав и объем сведений, составляющих коммерческую тайну, определяются руководителем предприятия».

Для того чтобы иметь возможность контролировать деятельность предприятий, Правительство РФ выпустило 5 декабря 1991 г. постановление № 35 «О перечне сведений, которые не могут составлять коммерческую тайну».

Порядок защиты государственной тайны регулируется Законом РФ «О государственной тайне» и постановлением Правительства РФ «Об утверждении правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» от 04.09.95 г. № 870. Защита информации и прав субъектов в области информационных процессов и информатизации регулируются гл. 5 Федерального закона РФ «Об информации, информатизации и защите информации», принятого Государственной Думой 25 января 1995 г.

Поскольку проблема защиты государственной тайны хорошо рассмотрена и освещена в многочисленных источниках (например, в журналах «Вопросы защиты информации»), автор счел необходимым уделить внимание вопросу коммерческой тайны.

Сведения о коммерческой тайне сгруппированы по тематическому принципу. Предлагаемое разделение на группы носит рекомендательный характер и может быть изменено в зависимости от специфики сведений, составляющих коммерческую тайну конкретного предприятия (организации). Сведения, включенные в приведенный ниже перечень, могут быть коммерческой тайной только с учетом особенностей конкретного предприятия (организации).

1. Сведения о финансовой деятельности:

- прибыль, кредиты, товарооборот;
- финансовые отчеты и прогнозы;
- коммерческие проекты;
- фонд заработной платы;

- стоимость основных и оборотных средств;
 - кредитные условия платежа;
 - банковские счета;
 - плановые и отчетные калькуляции.
2. Информация о рынке:
- цены, скидки, условия договоров, спецификация продукции;
 - объем, история, тенденции производства и прогноз для конкретного продукта;
 - рыночная политика и планы;
 - маркетинг и стратегия цен;
 - отношения с потребителями и репутация;
 - численность и размещение торговых агентов;
 - каналы и методы сбыта;
 - политика сбыта;
 - программа рекламы.
3. Сведения о производстве и продукции:
- сведения о техническом уровне, технико-экономических характеристиках разрабатываемых изделий;
 - сведения о планируемых сроках создания разрабатываемых изделий;
 - сведения о применяемых и перспективных технологиях, технологических процессах, приемах и оборудовании;
 - сведения о модификации и модернизации ранее известных технологий, процессов, оборудования;
 - производственные мощности;
 - состояние основных и оборотных фондов;
 - организация производства;
 - размещение и размер производственных помещений и складов;
 - перспективные планы развития производства;
 - технические спецификации существующей и перспективной продукции;
 - схемы и чертежи отдельных узлов, готовых изделий, новых разработок;
 - сведения о состоянии программного и компьютерного обеспечения;
 - оценка качества и эффективности;
 - номенклатура изделий;
 - способ упаковки;
 - доставка.
4. Сведения о научно-исследовательских разработках (НИР):
- новые технологические методы, новые технические, технологические и физические принципы, планируемые к использованию в продукции предприятия;
 - программы НИР;
 - новые алгоритмы;
 - оригинальные программы.
5. Сведения о системе материально-технического обеспечения:
- сведения о составе торговых клиентов, представителей и посредников;
 - потребности в сырье, материалах, комплектующих узлах и деталях, источники удовлетворения этих потребностей;
 - транспортные и энергетические потребности.

6. Сведения о персонале предприятия:
- численность;
 - лица, принимающие решение.
7. Сведения о принципах управления предприятием:
- сведения о применяемых и перспективных методах управления производством;
 - сведения о фактах ведения переговоров, предметах и целях совещаний и заседаний органов управления;
 - сведения о планах предприятия по расширению производства;
 - условия продажи и слияния фирм.
8. Прочие сведения:
- важные элементы систем безопасности, кодов и процедур доступа к информационным сетям и центрам;
 - принципы организации защиты коммерческой тайны.

Законом РФ от 2 декабря 1990 г. «О банках и банковской деятельности» введено понятие «банковская тайна».

Под банковской тайной (БТ) подразумевается обязанность кредитного учреждения сохранять тайну по операциям, счетам и вкладам клиентов и корреспондентов, отражение банковских операций от ознакомления с ними посторонних лиц, прежде всего конкурентов того или иного клиента. Иначе банковскую тайну можно определить как личную тайну вкладчика банка. Таким образом, коммерческая тайна банка включает коммерческую тайну самого банка и личную тайну вкладчика.

1.1.8. Информация как рыночный продукт

1991 г. можно считать годом рождения информационного рынка в России, о чем свидетельствует появление ряда сетевых структур, информационных предприятий, предлагающих пользователям набор услуг, альтернативных услугам Министерства связи РФ. Это передача речи, обеспечение факсимильной связи, электронный обмен данными. Министерство связи перестало быть монополистом государственной телефонной сети, изменился и характер его работы, за ним остались только задачи регулирования развития отрасли (лицензирование, сертификация), а все подведомственные предприятия были переведены на хозяйственные отношения [63].

Появление и развитие информационного рынка в России, как и в других странах, обусловлены прежде всего созданием и распространением телекоммуникационных вычислительных сетей (ТВС). С другой стороны, потребности информационного рынка послужили основной побудительной причиной бурного развития и распространения ТВС. В отличие от Запада, где ранее системы компьютерной связи использовались главным образом научными кругами и только в 1970-х гг. начался и по настоящее время продолжается процесс коммерциализации ТВС, в нашей стране появляющиеся сетевые структуры инвестируются исключительно крупным бизнесом, поэтому они коммерциализованы изначально.

На характере развития отечественных сетевых структур отражаются общие мировые тенденции развития ТВС. Одна из них – тенденция объединения различных сетевых структур, обусловленная необходимостью предоставления пользователям возможности связи с компьютером, находящимся в любой точке планеты (в современном мире это важное условие конкурентной способности предприятия, оказывающего телекоммуникационные услуги) [63].

Процессу объединения сетей способствует развитие их архитектуры в направлении создания национальных и международных ассоциаций систем компьютерной связи, в которых используются ЭВМ, изготовленные различными производителями и управляемые различными операционными системами (ОС). Это стало возможно, так как в основу моделей и архитектуры сетей положены международные стандарты. В результате во всех развитых странах в настоящее время выпускаются разнообразные технические и программные средства территориальных и локальных сетей нового типа – открытых сетей [63].

Возможности и конкурентоспособность любой ТВС определяются прежде всего ее информационными ресурсами – знаниями, данными, программами, которые сеть предоставляет пользователям. Естественно, что эти ресурсы должны как можно шире охватывать те области, в которых работают пользователи сети, а также непрерывно обновляться и пополняться.

Современный информационный рынок можно разделить на четыре взаимодействующие области [63]:

- электронная информация;
- электронные сделки;
- системы сетевых коммуникаций;
- программное обеспечение.

Рынок электронной информации включает четыре сектора: деловая информация, юридическая информация, информация для специалистов, массовая, потребительская информация. Основными поставщиками информации на этом рынке выступают центры – генераторы баз данных, центры – распределители информации на основе базы данных (БД) и информационные брокеры.

Базы данных, представляющие собой организованную совокупность однородных записей в машиночитаемой форме, являются основой любых видов услуг, оказываемых на современном информационном рынке. Затраты на их создание окупаются в среднем за 3–5 лет при условии постоянного обновления информации в БД, ориентации на предоставление уникальной информации многим пользователям (для этого необходимо предусматривать разнообразные способы доступа к БД), применения новых технологий создания и распространения БД, тесного взаимодействия с разработчиками программного обеспечения, облегчающего и упрощающего использование каналов распространения информации. В отечественных сетях используются обе формы доступа пользователей к БД: диалоговый доступ (режим on-line) и разовые запросы в режиме off-line (например, через электронную оплату выдаваемой справки по результату информационного запроса, что связано с задержками по времени получения информации).

Сектор деловой информации (в рамках рынка электронной информации) охватывает:

- биржевую и финансовую информацию, генераторами которой являются банки, биржи, брокерские компании. Это информация о котировках ценных бумаг, валютных курсах, учетных ставках, рынке товаров и капиталов, инвестициях, ценах;
- экономическую и статистическую информацию (числовую экономическую, демографическую, социальную информацию в виде рядов динамики, программных моделей, оценок и т.д.);
- коммерческую информацию (информацию о предприятиях и фирмах, их продукции и ее цене, о руководителях предприятий и т.п.). В России крупные БД по отечественным предприятиям созданы государственными системами;
- информацию коммерческих предложений (информацию о купле/продаже по определенным товарным группам);
- деловые новости в области экономики и бизнеса.

Сектор юридической информации включает системы доступа к электронным сборникам указов, постановлений, инструкций и другим документам, выпущенным органами государственной и местной власти.

Сектор информации для специалистов охватывает:

- профессиональную информацию, дифференцированную по различным областям науки и техники;
- доступ к первоисточникам (библиографическую и реферативную информацию).

К наиболее распространенным услугам, предоставляемым современными ТВС, относятся [63]:

- телекоммуникационные услуги: обмен сообщениями в режиме «электронная почта» как между пользователями одной сети, так и между пользователями различных сетей; обмен сообщениями между участниками телеконференций и телесеминаров; организация электронных бюллетеней новостей (электронных досок объявлений); организация диалога и обмен сообщениями двух абонентов в режиме «запрос-ответ»; передача больших массивов файлов; размножение сообщений и передача их по заранее подготовленному списку; приоритетное обслуживание сообщений согласно категориям срочности; организация замкнутых групп абонентов (подсетей) для взаимного обмена информацией только в рамках группы; доставка факсимильных сообщений; переадресация сообщений в случае изменения адреса получателя информации; выдача копий сообщений по запросам абонентов и др.;
- информационные услуги: поиск информации по вопросам, интересующим абонентов;
- консультационные услуги по информационному и программному обеспечению сети; по технологии использования общесетевых ресурсов; обучение навыкам работы с компьютером и другими техническими средствами;
- технические услуги: установка программного обеспечения, установка и тестирование модемов и др.;
- рекламные услуги: размещение рекламы в электронных конференциях и семинарах.

1.2. Объекты обработки и защиты информации

1.2.1. Современное состояние классификации автоматизированных систем

Автоматизированные системы обработки информации, или автоматизированные системы обработки данных в широком смысле этих слов, в настоящее время получили различное воплощение. Деление и классификацию указанных систем по видам до настоящего времени нельзя считать завершенными. Однако для решения проблемы безопасности важно определить не только предмет защиты, но и условия, в которых он находится, т.е. объекты его ввода-вывода, обработки, хранения и передачи. Данные объекты имеют различные типовые технические решения.

Принципиально важным моментом постановки задачи построения защиты в общем виде является выбор такой классификации автоматизированных систем обработки информации, которая позволила бы ожидаемые результаты решения задачи в типовых системах распространить на частные случаи построения любой автоматизированной системы – от автоматизированного рабочего места до глобальной АС независимо от аппаратной и программной платформ, на базе которых они построены. Для этого воспользуемся материалами работ [28], наиболее подробно отражающими современное состояние вопроса.

1.2.2. Первые вычислительные системы

Первый этап эволюции вычислительных систем, который пришелся на 1950–1970 гг., относится к началу использования компьютеров после изобретения первой ЭВМ.

Каждая вычислительная система того времени была основана, как правило, на применении одного многопользовательского компьютера, так как персональные компьютеры еще не появились. Архитектура подобных вычислительных систем, функционирующих в автономном режиме, была централизованной, когда к одному центральному компьютеру подсоединялись алфавитно-цифровые терминалы (рис. 1.3).

Если компьютеры объединялись линиями связи в сеть, то такая сеть имела *одноранговую архитектуру*, при которой отсутствовали компьютеры, полностью предоставляющие свои ресурсы в общее пользование для других компьютеров сети.

Таким образом, централизованная архитектура относится к автономной вычислительной системе, основанной на использовании одного многопользовательского компьютера, а одноранговая архитектура – к компьютерной сети, состоящей из ЭВМ одного ранга.

Все ресурсы вычислительной системы при централизованной архитектуре, включая информацию, были сконцентрированы в центральной ЭВМ, называемой еще *мейнфреймом* (англ. main frame – центральный блок ЭВМ). В качестве основных средств доступа к компьютерным ресурсам использовались алфавитно-цифровые терминалы, которые соединялись с центральной ЭВМ кабелем. Поскольку терминал – устройство простое, от конечного пользователя не требовалось никаких специальных действий по настройке и конфигурированию программного обеспечения ввиду его отсутствия на терминале. Управление терминалами осуществлялось централизованно с компьютера. Все терминалы были однотипными. При этом гарантировалось, что программа, запущенная на компьютере, будет работать со всеми терминалами одинаково.

Основным достоинством централизованной архитектуры с точки зрения обеспечения безопасности хранения и обработки данных является относительная простота построения и администрирования системы защиты информации. Эта относительная простота определяется концентрацией компьютерных ресурсов в одном месте. Ведь защита любых объектов, находящихся в одной точке, реализуется намного проще, чем в случае их территориального распределения.



Рис. 1.3. Архитектура первых вычислительных систем

Наряду с достоинствами первые вычислительные системы обладали рядом недостатков, связанных с отсутствием гибкости, неудобством их использования конечными пользователями, а также дороговизной обслуживания.

В то время как вычислительные системы с описанной централизованной архитектурой применяются редко, одноранговые сети из-за своей дешевизны используются широко. Однако в настоящее время они, как правило, объединяют не многопользовательские ЭВМ, а персональные компьютеры. Главным признаком одноранговой сети по-прежнему является отсутствие компьютеров, полностью предоставляющих свои ресурсы в общее пользование.

К существенным недостаткам одноранговых сетей можно отнести усложнение решения задач безопасности информации, невысокую производительность и сложность администрирования. Кроме того, при увеличении количества узлов сети эти показатели постепенно ухудшаются. Поэтому одноранговую сетевую архитектуру целесообразно использовать при небольшом количестве объединяемых компьютеров и невысоких требованиях по безопасности и производительности обработки данных.

1.2.3. Архитектура «клиент-сервер»

Недостатки, свойственные первым вычислительным системам с централизованной архитектурой, а также одноранговым компьютерным сетям, устраняются при построении вычислительных систем по архитектуре «клиент-сервер». Эта архитектура появилась на втором этапе эволюции компьютерных технологий, наступившем в 1980-х годах. Особенности данного этапа состоят в децентрализации архитектуры автономных вычислительных систем и их объединении в глобальные компьютерные сети.

Децентрализация архитектуры первых вычислительных систем стала возможной в связи с появлением персональных компьютеров, к которым мигрировала часть функций центральных ЭВМ. В результате появились распределенные локальные и глобальные вычислительные системы, объединяющие персональные компьютеры и компьютеры, полностью предоставляющие свои ресурсы в общее пользование для других компьютеров сети. Компьютеры, предоставляющие те или иные общие ресурсы, были названы серверами, а компьютеры, использующие общие ресурсы, – клиентами. Соответственно архитектуру таких распределенных вычислительных систем стали называть архитектурой «клиент-сервер» (рис. 1.4). Персональные компьютеры, исполняющие роль клиентов, называют еще рабочими станциями сети.



Рис. 1.4. Типовая архитектура «клиент-сервер»

Конкретный сервер характеризуется видом ресурса, которым он владеет. Так, если ресурсом является только база данных, то речь идет о сервере базы данных, назначение которого – обслуживать запросы клиентов, связанные с обработкой данных; если ресурс – это файловая система, то говорят о файловом сервере, или файл-сервере. В настоящее время серверы, как правило, выделяют в общее пользование комплекс ресурсов – базы данных, файловые системы, различные сервисы, предоставляемые выполняемыми на сервере программами, а также внешние устройства, например принтеры.

Различают несколько моделей архитектуры «клиент-сервер», каждая из которых отражает соответствующее распределение компонентов программного обеспечения между компьютерами сети. Распределяемые программные компоненты выделяют по функциональному признаку.

Функции любого программного приложения могут быть разделены на три группы:

- функции ввода и отображения данных;
- прикладные функции, характерные для предметной области приложения;

- функции накопления информации и управления данными (базами данных, файлами).

Соответственно любое программное приложение можно представить как структуру из трех компонентов:

- компонент представления, реализующий интерфейс с пользователем;
- прикладной компонент, обеспечивающий выполнение прикладных функций;
- компонент доступа к информационным ресурсам или менеджер ресурсов, выполняющий накопление информации и управление данными.

Различают следующие модели архитектуры «клиент-сервер», соответствующие нижеприведенным типам распределения перечисленных компонентов между рабочей станцией и сервером сети:

- на сервере расположены только данные (рис. 1.5);

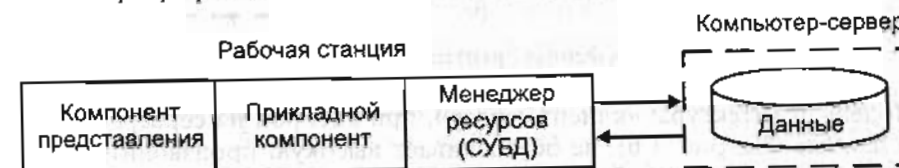


Рис. 1.5. Модель доступа к удаленным данным

- кроме данных на сервере расположен менеджер информационных ресурсов, например система управления базой данных (рис. 1.6);



Рис. 1.6. Модель сервера управления данными

- на сервере сконцентрированы как данные и менеджер ресурсов, так и прикладной компонент (рис. 1.7);



Рис. 1.7. Модель комплексного сервера

- на одном сервере расположен прикладной компонент, а на другом – данные и менеджер ресурсов (рис. 1.8).



Рис. 1.8. Трехзвенная архитектура «клиент-сервер»

Модель архитектуры «клиент-сервер», при которой на сервере расположены данные (см. рис. 1.6), не обеспечивает высокую производительность, так как вся информация обрабатывается на рабочих станциях, а файлы, содержащие эту информацию, для обработки должны быть переданы по сети с сервера. Передача же по сети больших объемов данных, возможно, избыточных, приводит к существенному снижению общей скорости информационного обмена. Это, в свою очередь, может привести к перегрузкам сети. По этим причинам модель доступа к удаленным данным может использоваться только для маленьких сетей.

При использовании модели сервера управления данными на сервере, кроме самой информации, расположен менеджер информационных ресурсов, например, система управления базой данных (см. рис. 1.6). Компонент представления и прикладной компонент совмещены и выполняются на компьютере-клиенте, который поддерживает как функции ввода и отображения данных, так и чисто прикладные функции. Доступ к информационным ресурсам обеспечивается, как правило, операторами специального языка (например, языка SQL, если речь идет о базах данных) или вызовами функций специализированных программных библиотек. Запросы к информационным ресурсам направляются по сети менеджеру ресурсов, например серверу базы данных. Последний обрабатывает запросы и возвращает клиенту блоки данных.

Главным преимуществом модели сервера управления данными перед моделью доступа к удаленным данным является снижение объема информации, передаваемой по сети, так как выборка требуемых информационных элементов из файлов выполняется не на рабочих станциях, а на сервере. Кроме того, в настоящее время существует множество инструментальных средств, обеспечивающих быстрое создание приложений с развитым интерфейсом, работающих с SQL-ориентированными СУБД. Это обеспечивает унификацию и широкий выбор средств разработки приложений. С использованием подавляющего большинства этих средств как раз и создаются программы, в которых совмещены прикладные функции и функции представления.

Основным недостатком модели сервера управления данными является отсутствие четкого разграничения между компонентом представления и

прикладным компонентом, что затрудняет дальнейшее совершенствование вычислительной системы, архитектура которой построена на основе данной модели.

Учитывая перечисленные достоинства и недостатки модели сервера управления данными, можно сделать вывод, что эту модель целесообразно использовать при построении вычислительных систем, ориентированных на обработку умеренных, не увеличивающихся со временем объемов информации. При этом сложность прикладного компонента приложения не должна быть высокой.

Модель комплексного сервера по сравнению с моделью сервера управления данными является более технологичной. Она строится в предположении, что процесс, выполняемый на компьютере-клиенте, ограничивается функциями представления, в то время как собственно прикладные функции и функции доступа к данным выполняются сервером (см. рис. 1.7). Прикладные функции могут быть реализованы в отдельных программах или в хранимых процедурах, которые называют также процедурами базы данных. Эти процедуры хранятся в самой базе данных и выполняются на компьютере-сервере, где функционирует и компонент, управляющий доступом к данным, т.е. ядро СУБД.

Преимущества модели комплексного сервера перед моделью сервера управления данными очевидны: это и более высокая производительность, и более совершенное централизованное администрирование, и соответственно экономия ресурсов сети. Следовательно, модель комплексного сервера является оптимальной для крупных сетей, ориентированных на обработку больших и увеличивающихся со временем объемов информации.

При существенном усложнении и увеличении ресурсоемкости прикладного компонента для него может быть выделен отдельный сервер, называемый сервером приложений. В этом случае говорят о трехзвенной архитектуре «клиент-сервер» (см. рис. 1.8), предполагающей наличие трех звеньев: первое звено – компьютер-клиент, второе – сервер приложений, а третье – сервер управления данными. Архитектуру «клиент-сервер», при которой прикладной компонент расположен на рабочей станции вместе с компонентом представления (см. рис. 1.5 и 1.6) или на сервере вместе с менеджером ресурсов и данными (см. рис. 1.7), называют двухзвенной архитектурой.

В рамках сервера приложений могут быть реализованы несколько прикладных функций, каждая из которых оформляется как отдельная служба, предоставляющая услуги всем программам. Серверов приложений может быть несколько, каждый из которых ориентирован на предоставление некоторого набора услуг. Любая программа, которая пользуется ими, рассматривается как клиент приложения. Детали реализации прикладных функций в сервере приложений полностью скрыты от клиента приложения. Запросы, поступающие от клиентов приложения, выстраиваются в очередь к процессу-серверу приложения, который извлекает, а затем передает их для обработки службе в соответствии с приоритетами.

Клиент приложения трактуется более широко, чем компонент представления. Он может поддерживать интерфейс с конечным пользователем (в таком случае он является компонентом представления), может обеспечивать поступление данных от некоторых устройств (например, датчиков), может,

наконец, быть сервером приложения. Последнее позволяет реализовать прикладную систему, содержащую серверы приложений нескольких уровней. Архитектура такой системы может выглядеть как ядро, окруженное concentрическими кольцами. Ядро состоит из серверов приложения, в которых реализованы базовые прикладные функции. Кольца символизируют наборы серверов приложения, являющихся клиентами по отношению к серверам внутреннего уровня. Число уровней серверов приложений не ограничено.

Четкое разграничение в архитектуре «клиент-сервер» компонентов программных приложений и рациональное их распределение между компьютерами сети позволяют достичь такого уровня гибкости, который недостижим в одноранговой архитектуре. Благодаря этому обеспечивается высокая эффективность использования компьютерных ресурсов, реализуются возможности расширения и дальнейшего совершенствования вычислительной системы.

Сетевую архитектуру «клиент-сервер», появившуюся на втором этапе эволюции компьютерных технологий, называют классической архитектурой «клиент-сервер». Ей присущи следующие особенности:

- на сервере порождается не конечная информация, а данные, подлежащие интерпретации компьютерами-клиентами;
- фрагменты прикладной системы распределены между компьютерами сети;
- для обмена данными между клиентами и сервером могут использоваться закрытые протоколы, не совместимые с открытым стандартом TCP/IP, применяемым в сети Интернет;
- каждый из компьютеров сети ориентирован на выполнение только своих локальных программ.

Последняя особенность способствует повышению информационно-компьютерной безопасности. В случае выполнения на каждом компьютере только своих локальных программ исключается миграция программ по сети при обработке серверами запросов со стороны клиентов. Соответственно снижается вероятность запуска на выполнение вредоносных программ и заражения компьютерными вирусами.

С точки зрения безопасности обработки и хранения данных архитектура «клиент-сервер» обладает рядом недостатков:

- территориальная распределенность компонентов программных приложений и неоднородность элементов вычислительной системы приводят к существенному усложнению построения и администрирования системы информационно-компьютерной безопасности;
- часть защищаемых информационных ресурсов может располагаться на персональных компьютерах, которые характеризуются повышенной уязвимостью;
- использование для обмена данными между компьютерами сети закрытых протоколов требует разработки уникальных средств защиты и соответственно повышенных затрат;
- при потере параметров настройки программного обеспечения какого-либо компьютера-клиента необходимо выполнение сложных процедур связывания и согласования этого компьютера с остальной частью вычислительной системы, что приводит к увеличению времени восстановления работоспособности компьютерной сети при возникновении отказов.

1.2.4. Архитектура «клиент-сервер», основанная на Web-технологии

Многие недостатки, присущие компьютерным сетям с классической архитектурой «клиент-сервер», отсутствуют в вычислительных системах новой архитектуры, которые сконцентрировали и объединили в себе лучшие качества централизованных систем и классических систем «клиент-сервер». Новая архитектура компьютерных сетей была названа интранет-архитектура. Ее часто называют также Web-архитектурой, или архитектурой «клиент-сервер», основанной на Web-технологии. Эта архитектура явилась итогом многолетних исследований и разработок в области приложения глобальных сетевых технологий Интернет к локальным сетям. Появление в 1993 г. архитектуры интранет относят к началу третьего этапа эволюции вычислительных систем.

Основной особенностью архитектуры интранет является возвращение к серверам ряда функций, которые были вынесены за пределы центральной ЭВМ на втором этапе эволюции вычислительных систем. Базисом новой архитектуры является Web-технология, пришедшая из Интернета.

В соответствии с Web-технологией на сервере размещаются так называемые Web-документы, которые визуализируются и интерпретируются программой навигации, функционирующей на рабочей станции (рис.1.9). Программу навигации называют еще Web-навигатором, или Web-браузером.

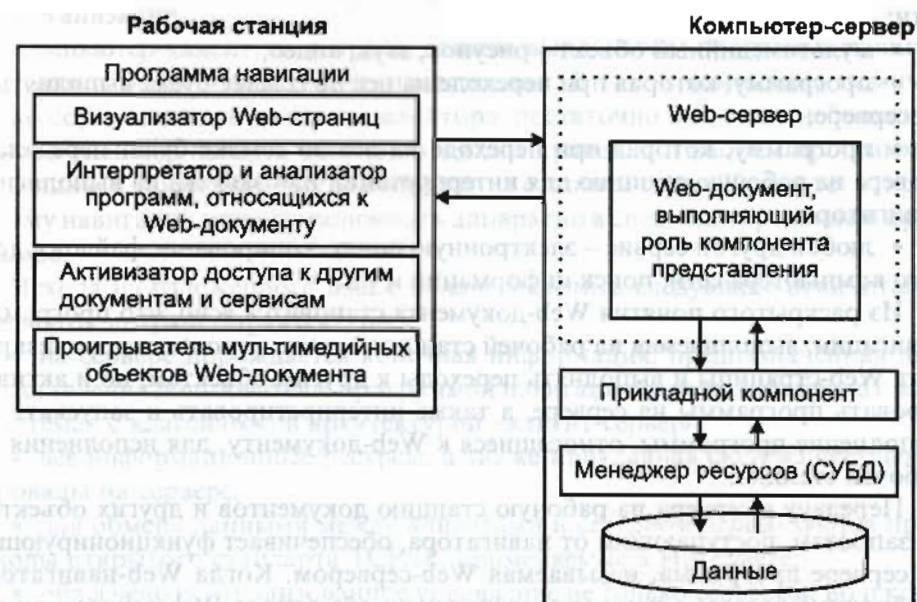


Рис. 1.9. Архитектура «клиент-сервер», основанная на Web-технологии

Логически Web-документ представляет собой гипермедийный документ, объединяющий ссылками различные Web-страницы, каждая из которых может содержать ссылки и на другие объекты. Физически Web-документ пред-

ставляет собой текстовый файл специального формата, содержащий ссылки на другие объекты и Web-документы, расположенные в любом узле сети. Web-документ реально включает только одну Web-страницу, но логически может объединять любое количество таких страниц, принадлежащих различным Web-документам.

Web-страница, являясь информационным аналогом страницы бумажного носителя, может включать как текст, так и рисунки. Но, в отличие от бумажной страницы, Web-страница может быть связана с компьютерными программами и содержать ссылки на другие объекты. Программа, связанная с Web-страницей, начинает автоматически выполняться при переходе по соответствующей ссылке или открытии Web-страницы. Любые ссылки, включенные в Web-страницу, выделяются другим цветом и/или подчеркиванием. Для перехода по ссылке достаточно щелкнуть по ней мышью.

Получаемая таким образом система гиперссылок основана на том, что некоторые выделенные участки одного документа, которыми могут быть части текста и рисунки, выступают в качестве ссылок на другие логически связанные с ними объекты. При этом объекты, на которые делаются ссылки, могут находиться на любом компьютере сети. В Web-страницу могут быть включены ссылки на следующие объекты:

- другую часть Web-документа;
- другой Web-документ или документ другого формата (например, документ Word или Excel), который может размещаться на любом компьютере сети;
- мультимедийный объект – рисунок, звук, видео;
- программу, которая при переходе на нее по ссылке будет выполняться на сервере;
- программу, которая при переходе на нее по ссылке будет передана с сервера на рабочую станцию для интерпретации или запуска на выполнение навигатором;
- любой другой сервис – электронную почту, копирование файлов с другого компьютера сети, поиск информации и т.д.

Из раскрытого понятия Web-документа становится ясно, что программа навигации, выполняемая на рабочей станции, может не только визуализировать Web-страницы и выполнять переходы к другим объектам, но и активизировать программы на сервере, а также интерпретировать и запускать на выполнение программы, относящиеся к Web-документу, для исполнения на рабочей станции.

Передачу с сервера на рабочую станцию документов и других объектов по запросам, поступающим от навигатора, обеспечивает функционирующая на сервере программа, называемая Web-сервером. Когда Web-навигатору необходимо получить документы или другие объекты от Web-сервера, он отправляет серверу соответствующий запрос. При достаточных правах доступа между сервером и навигатором устанавливается логическое соединение. Далее сервер обрабатывает запрос, передает Web-навигатору результаты обработки, например требуемый Web-документ, и разрывает установленное соединение.

Web-сервер выступает в качестве информационного концентратора, который доставляет информацию из разных источников, а потом однородным образом предоставляет ее пользователю. Навигатор, снабженный универсальным и естественным интерфейсом с человеком, позволяет последнему легко просматривать информацию вне зависимости от ее формата.

Таким образом, в рамках Web-документа может быть выполнена интеграция данных и программных объектов различных типов, расположенных в совершенно разных узлах компьютерной сети. Это позволяет рассредоточивать информацию в соответствии с естественным порядком ее создания и потребления, а также осуществлять единообразный доступ. Приставка Web здесь, а также в названии самой технологии (англ. web – паутина), как раз и отражает тот факт, что работа пользователя осуществляется на основе перехода по ссылкам, которые как нити паутины связывают разнотипные объекты, распределенные по узлам компьютерной сети.

Web-документы, помимо связывания распределенных и разнотипных данных, позволяют рассматривать информацию с нужной степенью детализации, что существенно упрощает анализ больших объемов информации. Можно сосредоточить внимание на главном, а затем изучить выбранный материал в подробностях. Можно эффективно реализовать многомодельный подход представления материала, создавая различные «взгляды» на требуемую предметную область, отражающие точки зрения той или иной группы сотрудников организации.

Компьютер-клиент, на котором должна выполняться программа навигации, может быть полностью стандартизован. В такой компьютер помимо процессора, основной памяти и монитора достаточно включить небольшой участок внешней памяти, необходимый для хранения и работы программы навигации, а также устройство сопряжения с линией связи. Кроме того, программу навигации можно реализовать аппаратно в специализированном процессоре.

Исходя из изложенного выше можно выделить следующие отличительные черты интранет-архитектуры:

- на сервере порождается конечная информация, предназначенная для представления пользователю программой навигации, а не полуфабрикат, как в системах с классической архитектурой «клиент-сервер»;
- все информационные ресурсы, а также прикладная система сконцентрированы на сервере;
- для обмена данными между клиентами и сервером используются протоколы открытого стандарта TCP/IP, применяемые в Интернете;
- облегчено централизованное управление не только сервером, но и компьютерами-клиентами, так как они стандартизованы с точки зрения программного обеспечения (на каждой рабочей станции достаточно наличия стандартной программы навигации);
- на рабочих станциях помимо своих программ могут выполняться программы с других компьютеров сети.

Предполагается, что перечисленные особенности, за исключением последней, способствуют решению проблемы информационно-компьютерной безопасности.

Концентрация на сервере информации и прикладной системы существенно упрощает построение и администрирование системы безопасности.

Использование для обмена данными между компьютерами сети протоколов открытого стандарта TCP/IP приводит к унификации всех способов взаимодействия между рабочими станциями и сервером. Не нужно решать задачу обеспечения безопасного информационного взаимодействия для множества приложений каждого компьютера. Решение по безопасности взаимодействия для одного компьютера и будет стандартным для всех. Кроме того, по отношению к протоколам открытого стандарта намного интенсивнее и шире публичное обсуждение вопросов информационной безопасности и богаче выбор защитных средств.

Облегченное централизованное управление сервером и компьютерами-клиентами снижает вероятность допущения непреднамеренных ошибок пользователями, операторами и администраторами. Такие ошибки являются одной из основных угроз безопасности информации и приводят к прямому ущербу. К ним относятся неправильно введенные данные или ошибки в программе, вызвавшие остановку либо разрушение системы. Эти ошибки также создают слабые места, которыми могут воспользоваться злоумышленники.

В интранет-архитектуре распределенная обработка информации предполагает возможность выполнения на рабочих станциях программ, полученных с сервера. Такой вид распределенной обработки позволил сконцентрировать всю прикладную систему на сервере. Однако возможность выполнения на рабочих станциях программ с сервера порождает новые угрозы безопасности информации, например появляется угроза подмены передаваемой с сервера программы [9]. Соответственно возможность миграции программ предъявляет дополнительные требования по поддержанию безопасности сетевого взаимодействия [28].

1.2.5. Эталонная модель OSI

Эталонная модель Международного стандарта на организацию архитектуры информационно-вычислительных сетей является базовой при организации взаимодействия открытых систем. Под системой в данном случае понимают автономную совокупность вычислительных средств, осуществляющих телеобработку данных прикладных процессов пользователей. При этом система считается открытой, если она выполняет стандартное множество функций технического взаимодействия, принятое в вычислительных сетях, т.е. не в смысле доступа к информации.

Область взаимодействия открытых систем определяется последовательно-параллельными или аппаратными средствами. Модули, образующие область взаимодействия прикладных процессов и физических средств соединения, делятся на семь иерархических уровней (рис. 1.10, табл. 1.1).



Рис. 1.10. Эталонная модель открытых систем:

X21 – интерфейс между окончанием оборудования данных и аппаратурой передачи данных;

HDLC – протокол канального уровня, обеспечивающий передачу последовательности пакетов через физический канал;

X25 – протокол, определяющий процедуры сетевого уровня управления передачей пакетов в интересах организации виртуальных каналов между абонентами и передачи по каналам последовательностей пакетов;

IP – межсетевой протокол

Таблица 1.1

Уровни взаимодействия открытых систем

Уровень	Наименование	Основная задача	Функции
1	Физический	Соприжение физического канала	Установление, поддержка и разъединение физического канала
2	Канальный	Управление передачей по информационному каналу	Управление передачей кадров, контроль данных, обеспечение прозрачности и проверка состояния информационного канала. Обрамление массивов служебными символами управления каналом
3	Сетевой	Маршрутизация пакетов	Управление коммуникационными ресурсами, маршрутизация пакетов, обрамление служебными символами управления сетью
4	Транспортный	Управление логическим каналом	Управление информационными потоками, организация логических каналов между процессами, обрамление служебными символами запроса и ответа
5	Сеансовый	Обеспечение сеансов связи	Организация поддержки и окончания сеансов связи, интерфейс с транспортным уровнем
6	Представительный	Параметрическое отображение данных	Генерация и интерпретация команд взаимодействия процессов. Представление данных программе пользователей
7	Прикладной	Выполнение процесса	Вспомогательные работы. Информационно-поисковые или справочные. Логическое преобразование информации пользователей

Как видно из табл. 1.1, каждый из уровней выполняет определенную функциональную задачу.

Три верхних уровня (5–7) вместе с прикладными процессами образуют область обработки данных, в которой выполняются информационные процессы системы. Процессы этой области используют сервис по транспортировке данных уровня 4, который осуществляет процедуры передачи информации от системы-отправителя к системе-адресату: прикладной реализует решение информационно-вычислительных задач прикладных процессов пользователей; представительный интерпретирует информационный обмен между прикладными процессами в форматах данных программ пользователей; сеансовый реализует диалог или монолог между прикладными процессами в режиме организуемых сеансов связи; транспортный осуществляет управление передачей информационных потоков между сеансовыми объектами пользователей.

Три нижних уровня (1–3) образуют область передачи данных между множеством взаимодействующих систем, выполняют коммуникационные процессы по транспортировке данных: сетевой обеспечивает маршрутизацию и мультиплексирование потоков данных в транспортной среде пользователей; канальный управляет передачей данных через устанавливаемые физические средства соединения; физический сопрягает физические каналы передачи данных в синхронном или асинхронном режиме.

Область взаимодействия открытых систем характеризуется семиуровневой иерархией протоколов, обеспечивающих взаимодействие абонентских систем сети, путем передачи данных между ними. Каждый из блоков данных состоит из заголовка, информационного поля данных и концевого.

Заголовок содержит информацию, связанную с управлением передачей информационных потоков. Данные центральной части блока представляют собой информационное поле, передаваемое между прикладными процессами взаимодействующих абонентских систем. Основная задача концевого – проверка информационного поля путем формирования проверочного блока данных.

1.2.6. Масштабирование компьютерных сетей

В зависимости от масштаба, территориального расположения и принадлежности компьютерные сети разделяют на локальные, региональные и глобальные.

Локальная вычислительная сеть представляет собой группу компьютеров, сопряженных друг с другом линиями связи и размещенных в пределах нескольких компактно расположенных зданий на ограниченной территории, принадлежащей одной организации.

Локальная сеть может быть разделена на отдельные сегменты. Под каждым *сетевым сегментом* понимается часть локальной сети, за пределы которой распространяются только те пакеты сообщений, которые адресованы не входящим в этот сегмент компьютерам. В пределах сегмента локальной сети реализуется метод множественного доступа, когда отправляемый компьюте-

ром сегмента пакет сообщения доставляется всем остальным компьютерам в этом сегменте, а принимается только тем компьютером, которому он адресован. Остальные компьютеры этот пакет сообщения в штатном режиме работы должны игнорировать.

Разделение локальной сети на сегменты улучшает ее производительность, сокращая трафик. Это связано с тем, что пакеты отдельных компьютеров сегмента, адресат которых находится в этом же сегменте, не распространяются по всей сети. Однако следует учитывать, что улучшение производительности локальной сети путем ее разбиения на сегменты будет обеспечено только в том случае, если выделенные сегменты соответствуют рабочим группам, в пределах которых осуществляется интенсивный обмен информацией. При отсутствии разделения локальной сети на сегменты считается, что данная сеть состоит из одного сетевого сегмента.

Корпоративная, региональная, а также глобальная сеть объединяет с помощью каналов связи территориально распределенные локальные сети. В качестве основного признака корпоративной сети выступает принадлежность одной организации, региональной – охват какого-либо региона, например одного города, а глобальной – охват глобальных территориальных областей, например стран и континентов. Большая региональная сеть может объединять более мелкие региональные и корпоративные сети, а глобальная – любые виды компьютерных сетей. Региональные и глобальные сети, в отличие от корпоративной, часто не принадлежат какой-либо одной организации. Ярким примером глобальной сети является сеть Интернет, которая не имеет владельца, входящие в ее состав компьютерные сети принадлежат различным организациям.

Для наращивания, а также интеграции вычислительных сетей используются различные типы аппаратно-программных устройств:

- повторители, обеспечивающие усиление и при необходимости разветвление электрического сигнала для увеличения размера сегмента локальной сети;
- мосты и коммутаторы, предназначенные для разбиения локальной сети на сегменты, а также для объединения полученных сегментов и небольших локальных сетей;
- маршрутизаторы, служащие для подключения к глобальным сетям, а также для объединения локальных сетей и их больших частей;
- шлюзы, выполняющие функции маршрутизации и предназначенные для объединения компьютерных сетей, функционирующих по несовместимым протоколам информационного взаимодействия;
- концентраторы – устройства, связывающие несколько устройств.

Перечисленные устройства функционируют на различных уровнях эталонной модели сетевого взаимодействия.

Повторители, позволяющие увеличить размер сетевого сегмента за счет усиления и разветвления электрического сигнала, функционируют на физическом уровне модели OSI (рис. 1.11). В настоящее время начинают применяться повторители, расширяющие сферу своего влияния и на канальный уровень с целью обеспечения безопасного использования сетевых адресов физического уровня, о чем будет идти речь ниже.

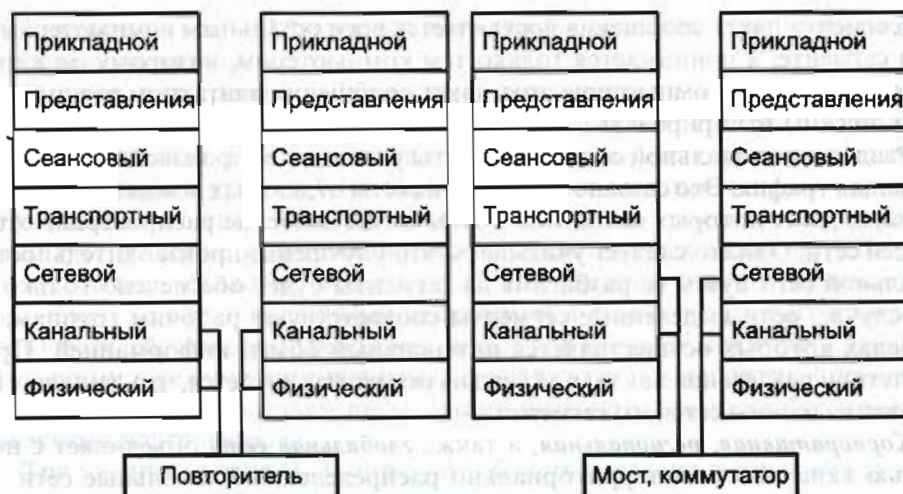


Рис. 1.11. Уровни модели OSI, на которых функционируют повторители и мосты

Мосты и коммутаторы, используемые для объединения сегментов локальной сети, а также небольших локальных сетей, работают на канальном уровне модели OSI (см. рис. 1.11). Объединяемые сегменты и локальные сети должны функционировать по одинаковым протоколам среднего и высокого уровней эталонной модели (с сетевого по прикладной уровень). Протоколы канального и физического уровней могут отличаться. Соответственно мосты и коммутаторы обеспечивают объединение сегментов и локальных сетей с разной топологией, например Ethernet и Token Ring.

Отдельные мосты и коммутаторы, например маршрутизирующий мост (routing bridge), помимо своих функций поддерживают некоторые функции сетевого уровня эталонной модели для оптимизации передачи данных. Современные коммутаторы позволяют объединять сегменты и локальные сети с различными протоколами не только физического и канального уровней, но и сетевого уровня, например с протоколами IP и IPX.

Маршрутизаторы, служащие для объединения локальных сетей и их больших частей, а также подключения локальных сетей к глобальным, функционируют на сетевом уровне модели OSI (рис. 1.12). Отдельные интеллектуальные маршрутизаторы, поддерживающие усовершенствованные функции фильтрации пакетов сообщений, могут обрабатывать пакеты транспортного уровня модели OSI.

В отличие от мостов и коммутаторов, маршрутизаторы обеспечивают поиск оптимального маршрута при передаче пакетов сообщений между сегментами сети или локальными сетями. Мосты и коммутаторы не реализуют функцию выбора оптимального маршрута, а лишь пересылают пакеты сообщений из одного сегмента локальной сети в другой или из одной локальной сети в другую.

Существуют также комбинированные сетевые устройства типа *мост/маршрутизатор* (brouter или bridge/router), которые в нормальном режиме работают как многопротокольные маршрутизаторы, а при получении пакета с неизвестным сетевым протоколом обрабатывают его как мост.



Рис. 1.12. Уровни модели OSI, на которых функционируют маршрутизаторы и шлюзы

Если локальные сети построены по протоколам, отличающимся не только на физическом, канальном и сетевом уровнях модели OSI, но и на более высоких уровнях, то для объединения таких сетей или сегментов сети должны использоваться специализированные компьютеры, называемые *шлюзами*. Шлюзы обычно работают на прикладном уровне модели OSI (рис. 1.13), обеспечивая маршрутизацию передаваемой информации и протокольное преобразование для всех уровней эталонной модели сетевого взаимодействия. Например, шлюзы необходимы для подсоединения к современным локальным сетям устаревших больших ЭВМ (мейнфреймов), имеющих централизованную архитектуру. Обычно шлюзы позволяют пользователям объединенных систем воспользоваться такими сервисами, как электронная почта, пересылка файлов и доступ к базе данных.

В современных сетевых топологиях, таких как Fast Ethernet и Token Ring, сегменты локальной сети соединяются с мостом, коммутатором или маршрутизатором только через повторители (рис. 1.13).



Рис. 1.13. Схема подключения сетевых сегментов

При кольцеобразной и звездообразной топологии, например в сетях Token Ring и Fast Ethernet, роль повторителей выполняют *активные концентраторы*, или, как их еще называют, *хабы*, объединяющие группы компьютеров в сетевом сегменте. Функции повторителей выполняют также и современные коммутаторы.

Вспомним, что активные концентраторы реализуют как функции коммутации, так и функции усиления сигнала. *Пассивные концентраторы* реализуют только функции разветвления. Соответственно к активным концентраторам может быть подсоединено большее количество компьютеров, например 16 или 32, а кабельные соединения могут иметь большую длину, например от 45 до 200 м в зависимости от типа кабеля. Пассивный концентратор используется в дополнение к активному и обеспечивает подключение только нескольких компьютеров, например трех. При этом максимально возможная длина кабеля, соединяющего компьютер с пассивным концентратором, не должна превышать несколько десятков метров.

При топологии «общая шина», например в сетях Ethernet типа 10-Base5, повторители применяют для подключения отдельных участков с общей шиной, а также увеличения длины одного участка. В последнем случае участки общей шины с максимально возможной длиной соединяются друг с другом через повторители.

Повторители для топологии «общая шина» называют линейными повторителями, так как содержат один входной и один выходной порт. В активных концентраторах все имеющиеся порты являются и входными, и выходными.

Повторители относятся к прозрачным и неадресуемым сетевым устройствам, работающим с той же скоростью, что и связываемые ими участки сети. Помимо усиления и разветвления электрического сигнала повторители обеспечивают выполнение функций *обработки ошибок* и *восстановления сигналов*. Если сигналы являются искаженными и/или зашумленными, но все еще различимыми для повторителя, то перед ретрансляцией другим портам повторитель эти сигналы восстанавливает. В случае же, когда на какой-либо порт повторителя поступают ошибочные сигналы, то повторитель блокирует их дальнейшее распространение.

В настоящее время начинают использовать повторители, работающие не только на физическом, но и на канальном уровне модели OSI с целью обеспечения безопасного применения сетевых адресов физического уровня, называемых MAC-адресами (MAC – Media Access Control). MAC-адрес, состоящий обычно из 48 бит, уникален для каждого узла локальной сети и присваивается сетевому адаптеру во время его изготовления. Все сетевые адаптеры имеют различные MAC-адреса. Исключением является только локальная сеть ArcNet, адаптеры которой имеют 8-битовые адреса, присваиваемые сетевым администратором.

Объединяемые сегменты локальной сети подсоединяются к портам моста (рис. 1.14), в качестве которых выступают сетевые адаптеры. Каждый связываемый сетевой сегмент подсоединяется к сетевому адаптеру, тип которого совпадает с типом этого сегмента. Мост чаще всего имеет от двух до четырех портов.

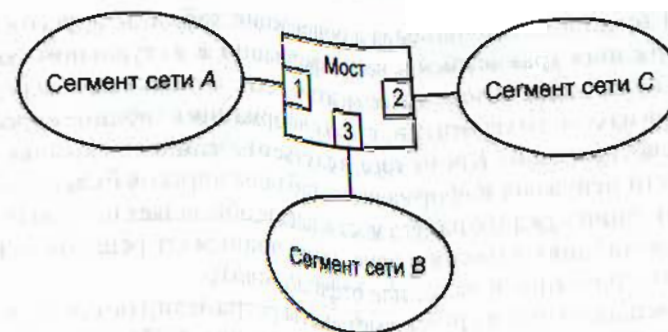


Рис. 1.14. Схема подключения сегментов локальной сети к мосту

Любой пакет, отправленный компьютером какого-либо сегмента сети, приходит в порт моста, к которому этот сегмент подключен. Если получатель данного пакета находится в другом сегменте сети, то мост направляет этот пакет в порт, к которому подсоединен сегмент с получателем. Этот процесс называется *ретрансляцией* (forwarding). Говорят, что пакет ретранслирован, если он получен одним портом моста и передан через другой. В случае когда принятый портом моста пакет имеет адрес получателя, находящегося в пределах подсоединенного к этому порту сегмента, данный пакет не ретранслируется. Этот процесс называется *фильтрацией* (filtering). Говорят, что кадр отфильтрован, если он получен одним портом моста и не ретранслирован другим.

Принятие мостом решения о том, ретранслировать полученный пакет или отфильтровать, основано на запоминании MAC-адресов компьютеров, входящих в подсоединенные к портам моста сегменты. Данные адреса хранятся в памяти моста в виде таблицы, ставящей в соответствие MAC-адресу каждого компьютера номер порта, к которому подсоединен сегмент с этим компьютером.

Заполнение таблицы адресов мост осуществляет сам. После первого подключения к сети мост в течение короткого промежутка времени, как правило нескольких секунд, запоминает адреса всех активных узлов, входящих в подсоединенные к мосту сегменты. В случае поступления на какой-либо порт пакета с неизвестным мосту MAC-адресом получателя мост ретранслирует этот пакет всем другим портам.

Для каждого MAC-адреса таблица адресов имеет три поля: сам адрес, номер порта, на котором адрес наблюдался в последний раз, а также возраст MAC-адреса.

При получении каждого пакета с неизвестным MAC-адресом отправителя мост регистрирует сам адрес, номер принявшего пакет порта, а также устанавливает значение возраста зарегистрированного адреса в 0. Возраст адреса в таблице увеличивается на единицу каждую секунду. При достижении определенного значения, называемого *границей возраста* (age limit), информация об этом MAC-адресе стирается из таблицы. Этот процесс называется старением. Поле возраста каждого MAC-адреса обнуляется, когда мост получает пакет с таким же MAC-адресом отправителя. При этом выполняется также обновление соответствующего этому MAC-адресу порта.

Данная технология заполнения и обновления таблицы адресов гарантирует поддержание хранящейся в ней информации в актуальном состоянии. При добавлении компьютеров к сегментам сети, а также при перемещении компьютеров из одного сегмента в другой информация в таблице адресов будет обновлена своевременно. Кроме того, в случае отсоединения компьютеров от сегментов сети ненужная информация из таблицы адресов будет удалена.

При получении каждого пакета мост вначале обновляет по описанной технологии свою таблицу адресов и лишь затем принимает решение о том, ретранслировать полученный пакет или отфильтровать.

Широковещательные и групповые пакеты ретранслируются во все порты моста, за исключением порта, принявшего этот пакет. Такая ретрансляция групповых пакетов выполняется по той причине, что мост не может узнать, каким узлам они предназначены. Эта информация доступна только на сетевом уровне компьютерам-получателям. В связи с тем что мосты и коммутаторы прозрачно пропускают широковещательные пакеты во всех направлениях, локальная сеть или ее часть, образованная объединением сегментов, мостами и коммутаторами, называется *широковещательной областью*.

Если на мост поступает однопунктовый пакет, то осуществляется поиск и анализ соответствующей строки в таблице адресов по MAC-адресу получателя этого пакета. Принимаемое решение о ретрансляции, зависящее от результатов поиска и анализа, представлено ниже.

Результат поиска и анализа	Решение
Адрес в таблице не обнаружен	Пакет ретранслируется во все порты, за исключением порта, на который он поступил
Адрес в таблице найден и соответствующий ему номер порта не совпадает с номером порта, принявшего пакет	Пакет ретранслируется только в порт, номер которого указан в таблице адресов
Адрес в таблице имеется и соответствующий ему номер порта совпадает с номером порта, принявшего пакет	Пакет отфильтровывается и ни в один из портов не ретранслируется

По описанной технологии работают все мосты. Однако некоторые из них могут принимать решение о ретрансляции на основе более сложных правил. Многие мосты допускают ручную настройку отдельных элементов таблицы адресов, так называемых статических элементов, которые никогда не удаляются из таблицы. Подобная настройка требуется для пассивных устройств, например для сетевого принтера, который может «молчать» в течение более продолжительного времени, чем допустимый максимальный возраст его MAC-адреса. При возникновении необходимости что-либо напечатать принтеру будет послан пакет, и в случае удаления из таблицы адресов информации о MAC-адресе принтера мост должен будет ретранслировать этот пакет на все порты.

Мосты имеют достаточно простую архитектуру и представляют собой специализированный компьютер с двумя или более сетевыми адаптерами, выступающими в качестве портов моста (рис. 1.15). Каждый порт принимает все поступающие к нему пакеты сообщений. Специализированное программное обеспечение проверяет каждый принятый пакет, заполняет и обновляет

ет таблицу адресов и принимает решение о ретрансляции. Мосты, включающие один процессор, могут одновременно обрабатывать только один пакет. Соответственно такие мосты, чтобы поддерживать высокую скорость обработки поступающих пакетов, имеют, как правило, не более четырех портов. Многопроцессорные мосты имеют большее количество портов, но стоят существенно дороже.

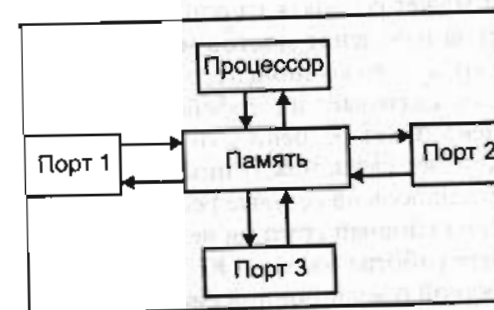


Рис. 1.15. Упрощенная архитектура моста с тремя портами

Функции моста может выполнять и обычный подсоединенный к сети компьютер со специальным программным обеспечением и несколькими сетевыми адаптерами, каждый из которых предназначен для одного из связываемых сегментов сети. Если в качестве моста используется сервер, то такой мост называют внутренним, а если рабочая станция — внешним. При использовании в качестве моста рабочей станции эту станцию не следует применять для других функций, так как любой отказ запущенной на ней пользовательской программы может привести к нарушению информационного обмена в сети.

1.2.7. Топология простых локальных вычислительных сетей

Локальная вычислительная сеть (ЛВС) позволяет прозрачно распределять ресурсы: каталоги дисков и принтеры, а также адаптеры модемов и факсов, отсутствующие на рабочих станциях. Подсоединившись к таким ресурсам, вы можете распоряжаться ими как собственными. Тот факт, что многие пользователи сети имеют доступ к одним и тем же ресурсам, упрощает распространение информации в пределах ЛВС, так как не требует осваивать новые методы передачи данных.

Существуют особые сетевые программы, использующие ЛВС для передачи информации: электронная почта, программа планирования, групповое ПО. Однако самое основное свойство локальной сети — простой доступ к сетевым ресурсам. Конечно, за этой простотой стоит многое, о чем пользователь рабочей станции может и не подозревать. Для доступа к сетевым ресурсам применяется целый ряд аппаратных и программных компонентов. Аппаратура — сетевая интерфейсная плата — электрически подсоединяет РС к локальной сети. Она устанавливается в пустое расширительное гнездо персонального компь-

ютера либо подключается к параллельному порту ПК-блокнота (или в гнездо PCMCIA).

Сетевое программное обеспечение делится на три категории:

- управления сетевой платой;
- выполняющее правила (или протокол) общения в сети;
- сетевой операционной системы.

Первый компонент может состоять из одной или нескольких небольших программ. Он отвечает за наведение мостов между сетевой платой и стеком протокола. Стек протокола – это компонент, осведомленный о правилах движения данных по сети, он связывает интерфейсную плату с оболочкой. Оболочка, или сетевой клиент, знает особенности используемых в сети операционных систем и осуществляет связь между ними. Оболочка отвечает за передачу и удовлетворение запросов на сетевые ресурсы.

Операционная система рабочей станции не единственная ОС в локальной сети. На файловом сервере работает особая ОС, называемая сетевой ОС (COC).

На вопрос о том, с какой операционной системой работает пользователь ПЭВМ чаще всего указывает название, например, NetWare. Однако все может быть гораздо сложнее. Если вы работаете с Windows for Workgroups и связаны с сервером NetWare, вы эксплуатируете две COC, так как Windows for Workgroups также представляет собой сетевую операционную систему – NOS (Network Operating System).

Информационные свойства локальной сети во многом зависят от состава поддерживаемых ею операционных систем, которые функционируют в РС и серверах. Если ЛВС поддерживает только одну операционную систему, т.е. имеет однородный состав узлов (компьютер или сервер с установленными в них сетевыми адаптерами), то такая локальная сеть называется гомогенной (или однородной). В противном случае – гетерогенной (или разнородной).

Локальные вычислительные сети бывают двух основных типов: равноправные (или одноранговые) и с выделенным сервером. В равноправной локальной сети все узлы равноправны: любая РС может выступать по отношению к другой как клиент или как сервер. В сети с выделенным сервером все клиенты общаются с центральным сервером.

Одноранговые сети обычно легко устанавливать, и для их ОС не требуется выделять особый компьютер. С другой стороны, эти сети обладают меньшими функциональными возможностями по сравнению с сетями на основе выделенного сервера. В частности, проблемы централизованной защиты ресурсов и данных в таких сетях часто неразрешимы, так как каждый пользователь сам контролирует доступ к своей системе. По мере роста размеров таких сетей они быстро становятся неуправляемыми.

И все же простая сеть с равноправными узлами может стать оптимальным решением, если необходимо объединить всего несколько машин. Windows for Workgroups – это Windows со встроенной одноранговой сетевой ОС. Windows NT Workstation тоже содержит встроенную равноправную COC. Другой пример популярной одноранговой сети – LANtastik фирмы Artisoft. В ней грань между сетью с равноправными узлами и сетью с выделенным сервером стирается, так как она позволяет отводить системы для работы в качестве серверов. Novell также предлагает продукт этого класса – Personal NetWare.

Равноправные COC хороши для мелких сетей и идеальны в случае необходимости объединения лишь нескольких машин в целях коллективного применения специальных файлов и принтеров, когда не требуется централизованного администрирования. Но иногда доступ к некоторым ресурсам должен быть предоставлен лишь определенным пользователям, и администратору требуется управлять такими ресурсами. Например, к определенному ресурсу должен быть организован централизованный доступ, в частности для организации «общего котла» модемов или принтеров. В этих случаях лучше обратиться к сети с выделенным сервером. В таких сетях один или несколько компьютеров организуют централизованный доступ к своим ресурсам. Все запросы от РС проходят через серверы. Компьютер, используемый в качестве сервера, должен быть как можно более мощным и надежным.

Программы сервера обеспечивают возможность централизованного администрирования и защиты и управляют доступом к ресурсам с помощью реконфигурируемых бюджетов пользователей. Администратор сети контролирует эти бюджеты и определяет, что должен видеть и делать пользователь, зарегистрированный в сети. Локальные сети с выделенным сервером обычно сложнее в установке по сравнению с одноранговыми, но они мощнее, функционально многообразнее и поддерживают крупные сетевые системы.

Наиболее популярным сетевым ПО с выделенным сервером является ОС Novell NetWare, используемая, по некоторым оценкам, в 70% локальных сетей. К числу других широко известных COC этого класса относятся Banyan Vines, IDM LAN Serve для OS/2, DEC Pathworks для VAX и Windows NT, а также Microsoft Windows NT Server.

Типичными методами доступа к передающей среде, влияющими на топологию в современных ЛВС, являются [63]:

- множественный доступ с контролем несущей и обнаружением конфликтов (CSMA/CD), иначе называемый методом доступа Ethernet, так как именно в этой сети получил наибольшее распространение;
- маркерное кольцо (метод доступа Token Ring);
- маркерная шина (метод доступа Arcnet).

Указанные методы доступа реализованы соответственно на стандартах IEEE802.3, IEEE802.4, IEEE802.5.

Метод доступа Ethernet (метод случайного доступа) разработан фирмой Xerox в 1975 г. и используется в ЛВС с шинной топологией (рис. 1.16), обеспечивает высокую скорость передачи данных и надежность. Это метод множественного доступа с прослушиванием несущей и разрешением конфликтов (коллизий). Каждая РС перед началом передачи определяет, свободен канал или занят. Если канал свободен, РС начинает передачу данных, осуществляемую пакетами, упакованными в кадры. Из-за различных системных задержек могут возникнуть коллизии. В этом случае станция задерживает передачу на определенное время. Для каждой РС устанавливается свое время ожидания перед повторной передачей кадра. Коллизии приводят к снижению быстродействия сети только при сравнительно большом количестве активных РС (до 80–100).



Рис. 1.16. Схема локальной вычислительной сети с общей шиной и выделенными серверами

Метод доступа *Token Ring* разработан фирмой IBM и рассчитан на кольцевую топологию сети (рис. 1.17). Это селективный метод доступа в кольцевой моноканал, именуемый «маркерное кольцо». В качестве маркера используется уникальная последовательность битов. Маркер не имеет адреса и может находиться в одном из двух состояний – свободном или занятом. Если ни одна РС не готова к передаче данных, свободный маркер циркулирует по кольцу. Станция, имеющая кадр для передачи, ждет подхода свободного маркера, захватывает его, изменяет состояние маркера на «занятый» и добавляет к нему кадр. Занятый маркер с кадром перемещается по кольцу и возвращается к станции-отправителю, причем при прохождении через узел назначения снимается копия кадра. Станция-отправитель удаляет свой кадр из кольца, изменяет состояние маркера на «свободный» и передает его дальше по кольцу. С этого момента любая станция может изменить состояние маркера на «занятый» и начать передачу данных. Описанная процедура характерна для сети, в которой все станции имеют одинаковый приоритет. В рамках метода «маркерное кольцо» предусматривается возможность передачи кадров станциями с учетом их приоритетов. Тогда станции с низким приоритетом могут захватывать кольцо в случае неактивности станций с более высоким приоритетом.



Рис. 1.17. Локальная сеть с кольцевой топологией

Метод доступа *Arcnet* разработан фирмой Datapoint Corp и используется в ЛВС с топологией «звезда» (рис. 1.18) и «общая шина». Это селективный метод доступа в моноканал, называемый «маркерная шина». Маркер создается одной из станций сети и имеет адресное поле, где указывается номер (адрес) станции, владеющей маркером. Передачу производит только та станция, которая в данный момент владеет маркером (эстафетной палочкой). Остальные станции работают на прием. Последовательность передачи маркера от одной станции к другой задается управляющей станцией сети. Станции, последовательно получающие маркер для передачи кадров, образуют «логическое кольцо». Станция, получившая маркер (полномочия на передачу информации), передает свой подготовленный кадр в шину. Если кадра для передачи нет, она сразу посылает маркер другой станции согласно установленному порядку передачи полномочий. Так продолжается до тех пор, пока управляющая станция не инициирует новую последовательность передач маркера. Станция назначения, получившая маркер с кадром, «отцепляет» кадр от маркера и передает маркер следующей станции в установленной последовательности передач. При таком методе доступа в моноканал имеется возможность обеспечить приоритетное обслуживание абонентов, например в течение одного цикла, когда маркер совершает полный оборот по «логическому кольцу», станции с более высоким приоритетом получают маркер не один раз, а несколько.



Рис. 1.18. Локальная сеть с топологией «звезда»

В качестве примера приведем структуру пакета по стандарту IEEE 802.3 с указанием длины каждого поля в байтах (табл. 1.2).

Таблица 1.2

Структура пакета по стандарту IEEE 802.3

Преамбула	Признак начала пакета	Назначение	Источник	Длина	Данные	Набивка	CRC-сумма
7	1	2 или 6	2 или 6	2	0–1500	?	4

Преамбула – это поле, содержащее семь одинаковых байтов 10101010, предназначенных для синхронизации.

Признак начала пакета – однобайтовое поле для обозначения начала пакета.

Назначение – поле длиной 2 или 6 байт (в зависимости от типа ЛВС) указывает, для какой РС данный пакет предназначен.

Источник – в этом поле содержится адрес отправителя пакета.

Длина – здесь содержится информация о длине данных в пакете.

Данные – в это поле записываются данные, составляющие передаваемое сообщение.

Набивка – сюда вставляют пустые символы для доведения длины пакета до минимально допустимой величины. При достаточно большой длине поля данных поле набивки может отсутствовать.

CRC-сумма – здесь содержится контрольное число, используемое на приемном пункте для выявления ошибок в данных принятого пакета. В качестве контрольного числа применяется остаток избыточной циклической суммы, вычисленный с помощью полиномов типа CRC-32. На приемном пункте также производится вычисление этого остатка и затем его сравнение с содержимым рассматриваемого поля с целью обнаружения ошибок в принятых данных.

Общая длина пакета стандарта IEEE 802.3 находится в диапазоне от 64 до 1518 байт, не считая преамбулы и признака начала пакета [63].

В последнее время в локальных сетях все больше используется протокол FDDI (определяемый Комитетом X3T9.5 ANSI), который используется либо в качестве высокоскоростных базовых сетей, либо для подключения моделей высокопроизводительных рабочих станций и суперсерверов.

По сравнению с популярными сетями Ethernet сети FDDI имеют более высокую производительность, обладают большей надежностью и безопасностью.

Все варианты стандарта FDDI (для разных типов передающей среды – оптоволоконного кабеля и витой пары медных проводов) обеспечивают скорость передачи 100 Мбит/с, что в 10 раз выше скорости Ethernet и в 6 раз выше максимальной скорости Token Ring (16 Мбит/с). На рынке высокоскоростных технологий ЛВС FDDI-технология проверена временем, а ее стандартизация достигла степени развития, позволяющей обеспечить совместимость устройств FDDI разных производителей. При этом сегодня нет нужды полностью отказываться от сетей Ethernet, так как возможны варианты одновременного использования FDDI и сетей других типов, если применять такие ТС, как коммутаторы и мосты/маршрутизаторы.

Отказоустойчивость сети FDDI обеспечивается применением двух колец передачи данных. В нормальном состоянии данные передаются только по основному кольцу. При одиночном физическом разрыве основного кольца (обрыв кабеля, выход из строя рабочей станции) станции обнаруживают по обе стороны места разрыва неисправность и автоматически переключают поток данных на резервное кольцо в направлении, противоположном направлению передачи по основному кольцу.

В стандарте FDDI определены также методы восстановления после серьезного нарушения целостности кольца (две станции с одним адресом и др.) – требуется вмешательство администратора сети. Знание места аварии позволяет администратору сети предпринять действия по восстановлению кольца.

При использовании оптоволоконного кабеля реализуются другие преимущества технологии FDDI:

• большое расстояние между узлами, так как стандарт FDDI определяет, что станции могут находиться на расстоянии до 2 км друг от друга, а общая длина кольца – достигать 100 км при числе станций до 500;

• нечувствительность к электромагнитным помехам, вызываемым электродвигателями и другими излучающими приборами;

• большая степень безопасности благодаря тому, что оптоволоконный кабель практически не излучает в радиодиапазоне, а передаваемую по нему информацию трудно перехватить удаленными приборами;

• гальваническая развязка в каждом сетевом узле, что значительно снижает электрические помехи и наводки за счет сокращения длинных электрических цепей.

Существуют также и другие топологии локальных вычислительных сетей с применением вспомогательного оборудования: коммутаторов, повторителей, концентраторов, маршрутизаторов и т.д. Однако в их основе лежат указанные выше топологии.

Существуют два типа межкомпьютерного обмена данными – датаграммы и сеансы. *Датаграмма* – это сообщение, которое не требует подтверждения о приеме от принимающей стороны. Если такое подтверждение необходимо, то адресат должен сам послать специальное сообщение. Для осуществления обмена этим способом принимающая и передающая стороны должны придерживаться определенного протокола во избежание недоразумений. Каждая датаграмма является самостоятельным сообщением, и при наличии нескольких датаграмм в ЛВС порядок их доставки не гарантируется. В некоторых случаях максимальный размер датаграмм гораздо меньше, чем длина сообщений в сеансах. Зато в большинстве ЛВС скорость передачи датаграмм гораздо выше, чем сообщений в сеансах.

В противоположность датаграммам в *сеансе* предполагается создание логической связи для обмена сообщениями между рабочими станциями и гарантируется получение сообщений. В то время как датаграммы могут передаваться в произвольные моменты времени, в сеансе для передачи сообщений сначала необходимо выполнить некоторую подготовительную работу: сеанс должен быть установлен, после этого происходит обмен сообщениями и, наконец, после окончания обмена данными сеанс должен быть закрыт.

Требования на обмен сообщениями, поступающие от модулей сетевой ОС, выполняющих перенаправление файлов, или от прикладных программ (таких как электронная почта), попадают на уровень NetBIOS. Эти требования можно разделить на четыре категории.

• *Поддержка имен.* Каждая из рабочих станций в ЛВС имеет одно или несколько имен. Эти имена хранятся NetBIOS в таблице, в первом столбце которой записывается уникальное и неизменное имя сетевого адаптера. Дополнительные имена пользователей (например, BARRY) могут быть добавлены в таблицу для удобства идентификации каждой рабочей станции. Пользовательские имена могут быть уникальными или, в специальных случаях, относиться к группе пользователей.

• *Поддержка сеанса.* NetBIOS осуществляет управление процессами установления связи, обмена и окончания связи между любыми двумя узлами (рабочими станциями) в ЛВС. Это происходит следующим образом. Сначала

одна станция начинает прослушивать сеть в ожидании вызова. Другая станция ее вызывает. Устанавливается сеанс, в течение которого оба компьютера на равных основаниях посылают и принимают сообщения. Закончив, обе станции извещают друг друга об этом и закрывают сеанс.

- *Поддержка датаграмм.* Сообщения могут передаваться для какого-то имени, группе имен или всем именам в ЛВС. Диалога между двумя машинами при этом не устанавливается, и прием сообщений не гарантируется.

- *Статус адаптера/сеанса.* С помощью NetBIOS прикладная программа имеет возможность получить информацию о локальном сетевом адаптере, о других адаптерах в сети и обо всех текущих сеансах в ЛВС.

1.2.8. Сегментация сложных локальных сетей

Если локальная сеть достаточно велика, то чаще всего для ее разбиения на сегменты и объединения этих сегментов между собой одного моста будет недостаточно. Прозрачность мостов позволяет создавать весьма сложные сети, в которых можно предусмотреть резервные маршруты между сетевыми сегментами в случае выхода из строя промежуточных сегментов сети. Например, на рис. 1.19 показана схема сети с несколькими мостами и резервным маршрутом между сегментами *A* и *D*. При выходе сегмента *C* из строя связь между группами сегментов {*A*, *B*} и {*D*, *E*, *F*} не будет нарушена, так как сработает альтернативный путь, образованный мостом с номером 3.

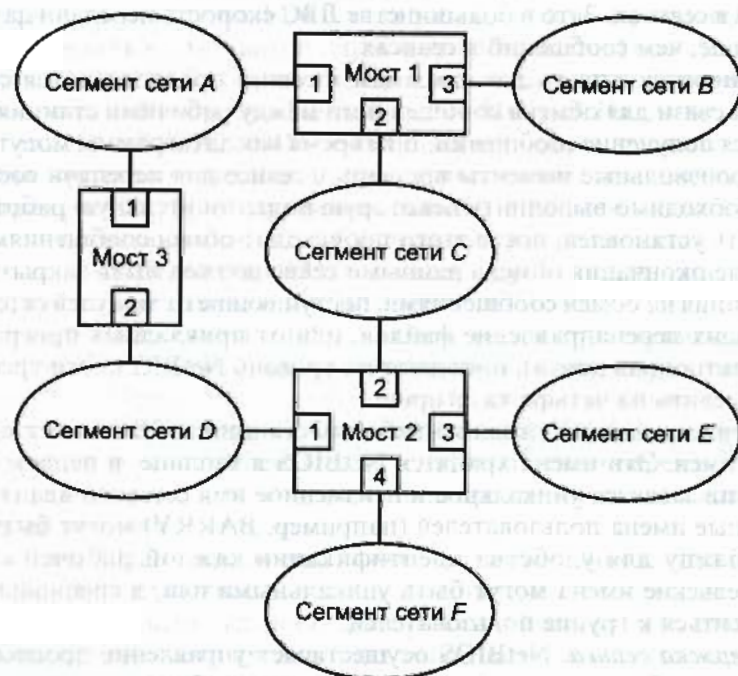


Рис. 1.19. Схема сети с несколькими мостами и резервным маршрутом

Однако в локальной сети между любыми двумя узлами должен существовать единственный путь. В противном случае при множестве путей между двумя узлами, которое называется петлей, могут возникнуть следующие нежелательные последствия:

- широковещательные штормы;
- размножение однопунктовых пакетов;
- проблемы с запоминанием.

Без принятия соответствующих мер широковещательные штормы приводят сеть к полному выводу из строя. Данный эффект возникает при наличии петель в структуре сети, когда мост ретранслирует широковещательный пакет. В результате этот же пакет, размноженный мостами по альтернативным путям, возвращается по петле к исходному мосту, который опять ретранслирует полученные одинаковые широковещательные пакеты.

Сетевые протоколы компьютеров разработаны таким образом, чтобы получать каждый пакет один раз. Получение размноженного пакета воспринимается как ошибка, после которой отсылается запрос отправителю размноженного пакета на повторную передачу. В конечном итоге повторно передаваемые и многократно размноженные пакеты займут полосы пропускания всех сегментов. Однопунктовые пакеты также будут размножаться, но с меньшей интенсивностью. В процессе движения широковещательного пакета по сети каждый мост петли будет наблюдать один и тот же адрес отправителя на нескольких принимающих портах. Это приведет к запоминанию в таблице адресов ложной информации о номере порта, к которому подсоединен отправитель широковещательного пакета. В результате возникнет путаница, так как однопунктовые пакеты будут направляться не в те порты.

Для недопущения описанных эффектов, приводящих к нарушениям работоспособности локальных сетей, современные мосты позволяют своевременно обнаруживать и блокировать эти эффекты, а также автоматически преобразовывать сеть с петлями в сеть с правильной структурой, предполагающей наличие между любыми двумя узлами единственного пути. Такое автоматическое преобразование выполняется на основе множества специальных управляющих сообщений, посредством которых мосты взаимодействуют друг с другом и изучают топологию сети. При обнаружении петель мосты начинают совместно отключать некоторые из своих портов. В результате петли уничтожаются, и достигается топология дерева, соединяющая любые два узла единственным путем.

Когда любая связь, имеющая резервную, выходит из строя, мосты автоматически изменяют топологию сети, активизируя резервный путь. Например, при работоспособности всех сегментов сети, представленной на рис. 1.20, порты моста с номером 3 будут отключены. В случае же выхода сегмента *C* из строя мост с номером 3 автоматически включит свои порты и связь между группами сегментов {*A*, *B*} и {*D*, *E*, *F*} будет восстановлена.

Если имеющиеся мосты не поддерживают функцию автоматического преобразования сети с петлями в сеть с правильной структурой, то изначально

необходимо сконфигурировать сеть в виде дерева, соединяющего любые два узла сети единственным путем.

Особенности сетевой коммутации. В отличие от мостов коммутаторы содержат большее количество портов, имеют более высокую производительность и могут не только разделять сеть на сегменты, но и разграничивать потоки сообщений между различными узлами сети друг от друга.

Первые коммутаторы имели лишь 6 или 8 портов. С развитием технологии появились коммутаторы с 16, 24 и более портами. Большое количество портов позволяет сегментировать локальную сеть на меньшие части, что существенно повышает ее пропускную способность. Кроме того, большое количество портов обеспечивает возможность подключения к портам не только сетевых сегментов, но и отдельных компьютеров локальной сети. Коммутаторы позволяют организовать подключенные компьютеры в сегменты сети и легко перегруппировывать их, когда это необходимо.

Конструктивно коммутатор выполнен в виде сетевого концентратора. Несмотря на то что коммутаторы подобны высокоскоростным многопортовым мостам, их внутренняя архитектура существенно отличается от архитектуры мостов. Коммутатор может обрабатывать много пакетов одновременно. Он проверяет пакеты, управляет таблицей адресов и принимает решение об одновременной или параллельной ретрансляции для всех своих портов.

Каждый порт коммутатора, подобно порту сетевого адаптера, имеет принимающую и передающую части. Каждая часть порта логически связана с перекрестной матрицей, реализованной аппаратным способом на основе микросхем ASIC (Application-Specific Integrated Circuit – специализированная интегральная схема). Принимающая часть каждого порта соединена с горизонтальной линейкой перекрестной матрицы, а передающая – с вертикальной (рис. 1.20). Когда горизонтальная линейка соединяется с вертикальной, создается путь от принимающей части одного порта к передающей части другого. Таким способом можно соединить любую пару портов. Например, если соединены пары портов 2 и 4, а также 3 и 5, то два пакета могут быть одновременно получены на портах 2 и 3 и переданы в порты 4 и 5. Как только порт получает пакет, коммутатор считывает адрес получателя и на основе таблицы адресов принимает решение о ретрансляции. Если пакет нуждается в ретрансляции, то создается связь с нужным портом.

Поскольку между портами коммутатора может быть много логических путей, то одновременно можно ретранслировать много кадров. Однопунктовые пакеты с неизвестным адресом, а также многопунктовые и широковещательные пакеты-коммутаторы, как и мосты, ретранслируют на все порты, за исключением тех портов, на которые эти пакеты поступили.

Описанная технология называется коммутацией пакетов, или коммутацией кадров, и используется в локальных сетях Ethernet и Token Ring. Каждый пакет обрабатывается ближайшим коммутатором и передается далее по сети непосредственно получателю. В результате сеть превращается как бы в совокупность параллельно работающих высокоскоростных прямых каналов [28].

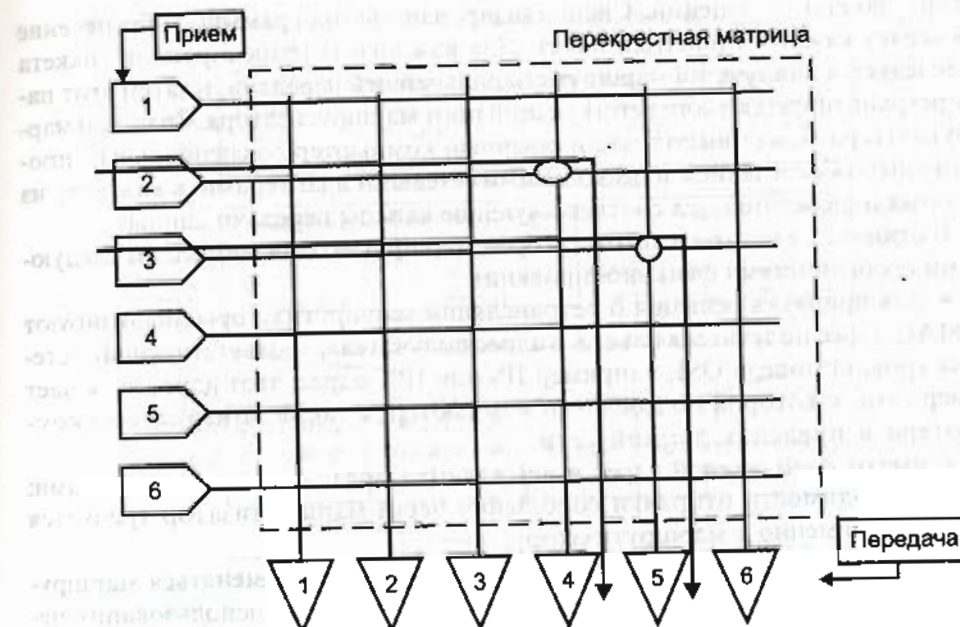


Рис. 1.20. Логическая схема коммутатора

1.2.9. Региональные и глобальные сети

Мосты и коммутаторы, предназначенные для разбиения локальной сети на сегменты, а также объединения полученных сегментов и небольших локальных сетей, не реализуют функцию выбора оптимального маршрута, а лишь пересылают пакеты сообщений из одного сегмента локальной сети в другой или из одной локальной сети в другую. Кроме того, данные устройства не в силах защитить сеть от лавин широковещательных пакетов, которые приводят к непроизводительной загрузке сети. По этим причинам мосты и коммутаторы не могут эффективно использоваться для подключения к глобальным сетям, а также объединения локальных сетей и их больших частей. Данные функции возложены на маршрутизаторы, функционирующие на сетевом уровне эталонной модели OSI.

Маршрутизаторы имеют особо важное значение для объединенных и глобальных сетей, в которых используются удаленные коммуникации. Маршрутизаторы обеспечивают оптимальный трафик по сложным маршрутам в разветвленных объединенных сетях, имеющих избыточные связи. В дополнение они отфильтровывают ненужный здесь поток широковещательных сообщений, повышая таким образом пропускную способность каналов связи. Последняя функция наиболее важна при соединении локальных сетей каналами с низкой пропускной способностью.

Маршрутизатор, как и мост, представляет собой специализированный компьютер с двумя или более сетевыми адаптерами, выступающими в качестве портов маршрутизатора. Порты принимают поступающие к маршрути-

затому пакеты сообщений. Специализированное программное обеспечение проверяет каждый принятый пакет. Для каждого ретранслируемого пакета определяется наилучший маршрут его дальнейшей передачи, и затем этот пакет ретранслируется в соответствующий порт маршрутизатора. Функции маршрутизатора может выполнять и обычный компьютер со специальным программным обеспечением и несколькими сетевыми адаптерами, к каждому из которых подсоединяются соответствующие каналы передачи данных.

В отличие от мостов и коммутаторов маршрутизаторы обладают следующими особенностями функционирования:

- для принятия решения о ретрансляции маршрутизаторы анализируют не MAC-адрес получателя пакета, а адрес получателя, соответствующий сетевому уровню модели OSI, например IP- или IPX-адрес; этот адрес включает номер сети, к которой подсоединен компьютер, а также номер самого компьютера в пределах данной сети;
- имеют свой сетевой адрес и не являются прозрачными устройствами; при необходимости отправки сообщения через маршрутизатор требуется обратиться именно к маршрутизатору;
- при использовании маршрутизаторов должны применяться маршрутизируемые протоколы, такие, как IP или IPX; в случае использования немаршрутизируемого протокола, например, NetBIOS, пакеты которого не включают информацию об адресе сети, передаваемые через маршрутизатор пакеты должны инкапсулироваться в пакеты маршрутизируемого протокола, например, IP или IPX.

Рассмотрим первые две особенности более подробно.

Повторители работают с пакетами физического уровня модели OSI (рис. 1.21) и не анализируют поле данных этих пакетов. Исключением являются повторители, ориентированные на выполнение функций *избирательного шифрования пакетов канального уровня*, а также *фильтрации MAC-адресов*. В этом случае обрабатываются служебные данные, соответствующие пакетам канального уровня.

Мосты и коммутаторы работают с пакетами канального уровня эталонной модели (см. рис. 1.21), анализируя для принятия решений о ретрансляции MAC-адреса их отправителя и получателя. Отдельные мосты и коммутаторы с целью оптимизации передачи данных позволяют обрабатывать и пакеты сетевого уровня. Например, многие производители стали встраивать в коммутаторы функции маршрутизации, которые в дополнение позволяют организовать виртуальные сети на основе анализа адресов сетевого уровня.

Маршрутизаторы работают с пакетами сетевого уровня модели OSI, анализируя не MAC-адреса, а сетевые адреса получателей, каждый из которых, в отличие от MAC-адреса, включает номер сети, к которой подсоединен компьютер, а также номер самого компьютера в пределах данной сети. Маршрутизаторы могут поддерживать и усовершенствованные функции фильтрации, обрабатывая также пакеты транспортного уровня эталонной модели. Например, возможна фильтрация не только по адресам отправителя и получателя из заголовков пакетов сетевого уровня, но и по видам приложений источника и получателя из заголовков пакетов транспортного уровня.

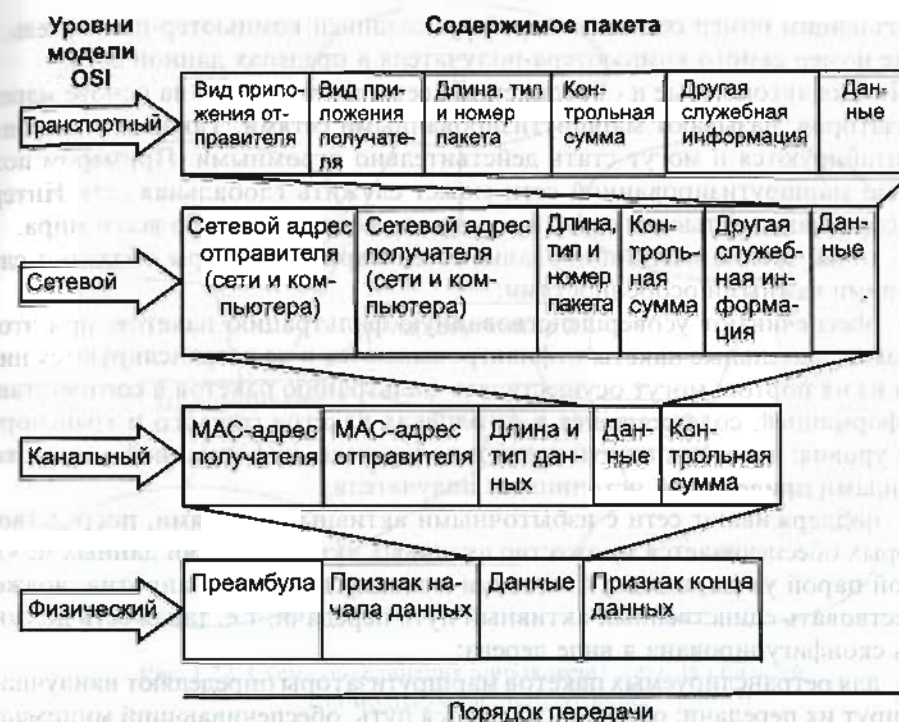


Рис. 1.21. Схема инкапсуляции передаваемого пакета

При отправке сообщения узел сети помещает в заголовки пакетов сетевого уровня адреса отправителя и получателя, каждый из которых состоит из соответствующих номеров сети и компьютера. В случае использования в сети маршрутизатора перед формированием пакетов канального уровня узел должен установить, может ли он отправить эти пакеты непосредственно получателю или же их нужно переслать маршрутизатору.

Пакеты могут быть отправлены непосредственно получателю, если номер сети отправителя совпадает с номером сети получателя. Это означает, что отправитель и получатель находятся в одной широковещательной области.

Напомним, что под широковещательной областью понимается локальная сеть или ее часть, образованная сетевыми сегментами, объединенными мостами и коммутаторами. Широковещательные пакеты в пределах такой области доставляются всем сетевым узлам.

Для отправления пакетов непосредственно получателю необходимо на канальном уровне в качестве MAC-адреса получателя этих пакетов указать действительный MAC-адрес компьютера-получателя.

Если же номер сети отправителя не совпадает с номером сети получателя, то передающий узел должен направить эти пакеты маршрутизатору. Для этого на канальном уровне в качестве MAC-адреса получателя данных пакетов следует указать MAC-адрес маршрутизатора. После получения пакетов маршрутизатор возьмет на себя заботу об их доставке получателю. Получатель для маршрутизатора будет идентифицироваться адресом сетевого уровня,

включающим номер сети, к которой подсоединен компьютер-получатель, а также номер самого компьютера-получателя в пределах данной сети.

Любые автономные и объединенные сети, построенные на основе маршрутизаторов, называют маршрутизированными сетями. Такие сети хорошо масштабируются и могут стать действительно огромными. Примером полностью маршрутизированной сети может служить глобальная сеть Интернет, соединяющая тысячи сетей и миллионы компьютеров со всего мира.

С точки зрения масштабирования сетей маршрутизаторы обладают следующими важными особенностями:

- обеспечивают усовершенствованную фильтрацию пакетов; при этом широковещательные пакеты отфильтровываются и не ретранслируются ни в один из их портов; могут осуществлять фильтрацию пакетов в соответствии с информацией, содержащейся в заголовках пакетов сетевого и транспортного уровня: адресами отправителя и получателя, информацией о протоколе, видами приложений источника и получателя;
- поддерживают сети с избыточными активными связями, посредством которых обеспечивается множество активных путей передачи данных между любой парой узлов; в сетях с мостами и коммутаторами, напротив, должен существовать единственный активный путь передачи, т.е. такая сеть должна быть сконфигурирована в виде дерева;
- для ретранслируемых пакетов маршрутизаторы определяют наилучший маршрут их передачи; обычно избирается путь, обеспечивающий минимальное время доставки при максимальной надежности; в качестве такого пути может выступать путь с минимальным числом транзитных узлов, предусматривающий возможность обхода загруженных участков сети.

Подобно тому, как мосты и коммутаторы разбивают сети на области множественного доступа, маршрутизаторы выполняют разделение сетей на широковещательные области и поддерживают между ними множественные активные связи (рис. 1.22). При этом широковещательная область ограничивает также область множественного доступа, что характерно для случая, когда широковещательная область состоит из одного сегмента. Любой узел маршрутизированной сети может взаимодействовать с любым другим. Однако широковещательные пакеты никогда не покидают своей широковещательной области и не используют полосы пропускания каналов связи, расположенных вне ее. Множественные активные связи между широковещательными областями повышают безопасность и производительность компьютерных сетей за счет:

- наличия запасных путей на случай перегрузки или выхода из строя основного пути;
- возможности расширения полосы пропускания между широковещательными областями в результате распределения трафика между имеющимися путями.

Например, между широковещательными областями В, С и Е на рис. 1.22 существует несколько альтернативных путей. Это обеспечивает наличие резервных связей и возможность равномерного распределения трафика альтернативных путей с учетом текущей загрузки используемых каналов связи.

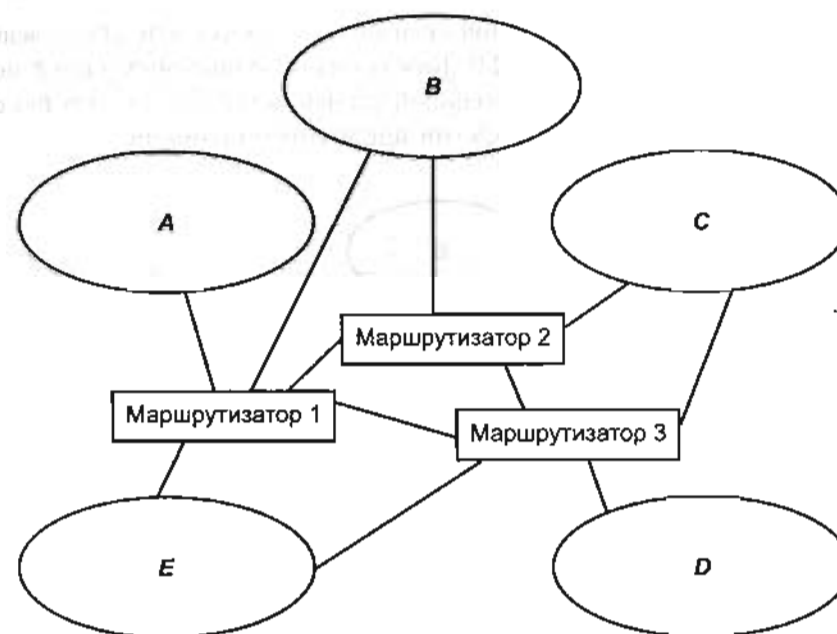


Рис. 1.22. Схема объединения широковещательных областей с помощью маршрутизаторов

A, B, C, D, E – локальная сеть или часть сети, образующая широковещательную область

Пересылка пакетов осуществляется маршрутизаторами всегда по наилучшим путям из всех возможных. Определение наилучших путей выполняется на основе таблиц маршрутизации в соответствии с используемыми протоколами. Изначальное заполнение таблиц маршрутизации может выполняться как вручную, так и автоматически. Для поддержки этих таблиц в актуальном состоянии маршрутизаторы взаимодействуют друг с другом путем передачи различных сообщений и осуществляют контроль состояния подключенных к ним каналов связи. На основе полученной информации каждый маршрутизатор обновляет детальные сведения о топологии сети, хранящиеся в его таблице.

Наличие в маршрутизированной сети множественных активных связей порождает такую особенность, как возможность передачи получателю пакетов по различным путям. Если первый пакет передается по медленному или перегруженному пути, то следующий может быть направлен по более быстрому пути и достичь получателя раньше первого. Несоответствие порядка принятых пакетов порядку их отправления устраняется на транспортном уровне модели OSI.

Использование маршрутизаторов вместо мостов и коммутаторов для объединения больших частей и сегментов локальной сети целесообразно в том случае, когда широковещательная область локальной сети становится слишком большой или существенно увеличивается количество сетевых сегментов и сложность сети. В этом случае части локальной сети, разграниченные и объединенные маршрутизатором, легче обслуживаются, так как на сетевом уровне модели OSI каждая из этих логических подсетей имеет свой отдельный номер, входящий и в адрес сетевых узлов.

Объединяемые части локальной сети подключаются непосредственно к портам маршрутизатора (рис. 1.23). Каждая из объединяемых частей может представлять собой отдельный большой сегмент сети или множество сетевых сегментов, объединенных мостами и/или коммутаторами.

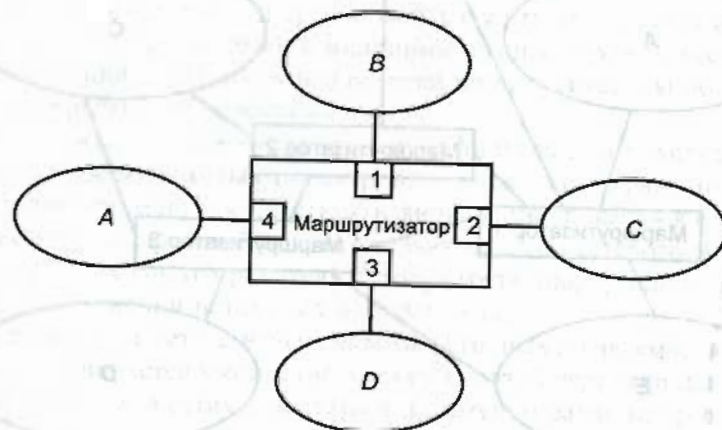


Рис. 1.23. Схема объединения частей крупной сети:
A, B, C, D — большой сегмент или часть локальной сети

В очень большой локальной сети для объединения ее частей разумно использовать несколько маршрутизаторов с образованием избыточных активных связей между ширококестельными областями, как показано на рис. 1.22.

Для объединения больших частей и сегментов локальной сети могут использоваться также комбинированные устройства, получившие название мостов-маршрутизаторов (brouter или bridge/router), которые подобно многопротокольным маршрутизаторам поддерживают работу с несколькими протоколами. Данные устройства обрабатывают пакеты сообщений одного вида как маршрутизаторы, а другого — как мосты. Для того чтобы определить, какую функцию необходимо выполнить, используются фильтрующие маски, настраиваемые администратором. Например, в нормальном режиме эти устройства работают как многопротокольные маршрутизаторы, а при получении пакета с неизвестным сетевым протоколом обрабатывают его как мост.

Следует учитывать, что маршрутизаторы для объединения частей локальной сети, в отличие от маршрутизаторов, используемых для объединения сетей и подключения к опорным сетям, должны быть производительнее. Это связано с более высокой пропускной способностью каналов связи в пределах локальной сети.

Объединение локальных сетей выполняют путем их подключения через маршрутизаторы к опорным сетям (рис. 1.24, а), в качестве которых выступает корпоративная, региональная или глобальная сеть.



Рис. 1.24. Схемы подключения к опорной сети:

а — объединение ЛВС через опорную сеть;

б — объединение ЛВС через специальный маршрутизатор (мост, коммутатор)

Опорные сети, в отличие от сегментов локальных сетей, реализуют не множественный, а избирательный доступ к устройствам, непосредственно подключенным к этим сетям. В качестве таких устройств используются маршрутизаторы. При обмене информацией между двумя компьютерами через опорную сеть маршрутизаторы устанавливают друг с другом двухточечные соединения. В результате пакеты сообщений в пределах опорной сети курсируют по строгим маршрутам, которые определяют маршрутизаторы. Когда же пакеты сообщений поступают в сегмент локальной сети получателя, то в рамках этого сегмента реализуется множественный доступ, при котором полученные пакеты доставляются всем узлам сегмента, но принимаются только теми узлами, которым они адресованы.

Многие мосты и коммутаторы также поддерживают каналы опорных сетей, но в этом случае ширококестельные пакеты сообщений, которые не отфильтровываются данными устройствами, снижают пропускную способность опорной сети.

При объединении локальных сетей следует учитывать правило, согласно которому интенсивность графика внутри локальной сети по отношению к интенсивности межсетевых графиков не должна быть ниже соотношения 80/20. В противном случае локальные сети с интенсивным межсетевым графиком необходимо объединить каналами связи с высокой пропускной способностью напрямую через высокопроизводительный маршрутизатор, мост или коммутатор, оставив соединение через опорную сеть в качестве резервного (рис. 1.24, б). Такой способ объединения позволит снизить нагрузку на опорную сеть и повысить скорость информационного обмена между связанными напрямую локальными сетями.

В качестве корпоративной опорной сети часто используется кольцо FDDI (Fiber Distributed Data Interface — распределенный интерфейс передачи данных по волоконно-оптическим каналам), называемое маршрутизируемым кольцом (рис. 1.25). Маршрутизаторы, используемые подобным образом, называют краевыми маршрутизаторами.

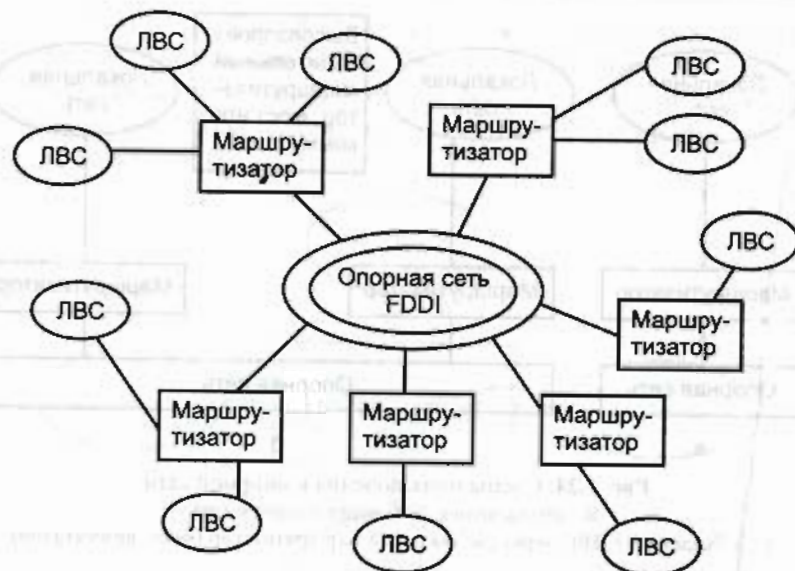


Рис. 1.25. Опорная сеть в виде маршрутизируемого кольца

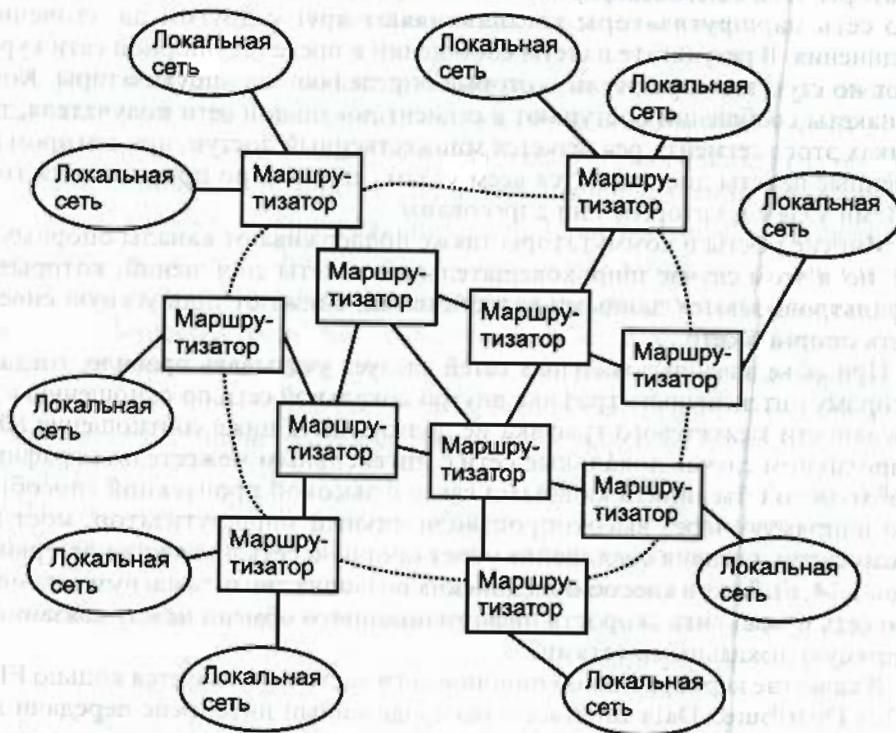


Рис. 1.26. Опорная сеть в виде маршрутизируемого облака

Региональные и глобальные опорные сети чаще всего имеют другую структуру (рис. 1.26), называемую *маршрутизируемым облаком*. Краевые маршрутизаторы объединяют локальные сети в маршрутизированную сеть, а внутренние маршрутизаторы обеспечивают связь уровня опорной сети. Для связи маршрутизаторов друг с другом могут использоваться любые каналы передачи данных, начиная от медленных аналоговых и цифровых телефонных линий и заканчивая скоростными каналами оптоволоконной и спутниковой связи.

При использовании различных каналов принцип маршрутизации не меняется, а изменяются лишь типы сетевых адаптеров. Типы сетевых адаптеров каждого маршрутизатора должны соответствовать типам подключаемых к этим адаптерам каналов передачи данных.

Например, если маршрутизатор связывает локальную сеть Ethernet с цифровой телефонной линией ISDN опорной сети, то один порт этого маршрутизатора должен представлять собой сетевой адаптер Ethernet, а другой – адаптер ISDN. Поставщик услуг Интернета может иметь маршрутизаторы, поддерживающие сотни модемов для передачи данных по аналоговым телефонным линиям.

Маршрутизаторы согласовывают подключенные к ним медленные и быстрые каналы связи друг с другом, например аналоговые телефонные линии с каналами ISDN. При передаче информации из быстрых каналов в медленные маршрутизаторы выполняют буферизацию данных, что предотвращает возможную перегрузку медленных линий связи.

Маршрутизаторы позволяют объединять локальные сети и сетевые сегменты, отличающиеся друг от друга по используемым протоколам физического и канального уровней модели OSI, например сети Ethernet, Token Ring, FDDI и ArcNet. Известно, что максимальный размер кадра в сети Token Ring составляет 4 Кбайта, а в FDDI – 64 Кбайта. В сети же Ethernet длина кадра не превышает 1500 байт. В случае использования протокола IP маршрутизатор может фрагментировать большие IP-пакеты, полученные из локальной сети Token Ring или FDDI, на несколько пакетов сети Ethernet. Такой прием называется IP-фрагментацией.

Многопротокольные маршрутизаторы обеспечивают объединение сегментов и сетей, функционирующих по разным протоколам сетевого уровня, например по протоколам IP и IPX. Они выполняют независимую обработку IP- и IPX-пакетов, передавая их затем соответствующим сегментам или локальным сетям.

При подключении локальной сети к Интернету, а также другим общественным опорным сетям появляются угрозы несанкционированного вторжения в локальную сеть из глобальной, а также угрозы несанкционированного доступа из локальной сети к ресурсам глобальной. Защита от реализации данных угроз основана на использовании программно-аппаратных комплексов, поддерживающих функции маршрутизации и называемых межсетевыми экранами или брандмауэрами. Межсетевой экран, как и маршрутизатор, устанавливается на стыке между локальной и опорной сетью. Он поддерживает безопасность локальной сети на основе фильтрации двустороннего потока сообщений и аутентификации участников обмена информацией. Брандмауэр может заменять функции маршрутизатора, а может использоваться совместно с маршрутизатором, обеспечивая более надежную защиту (рис. 1.27).



Рис. 1.27. Схема безопасного подключения к глобальной сети

Роль простейшего межсетевого экрана может выполнять и современный маршрутизатор, обеспечивающий фильтрацию пакетов сетевого и транспортного уровней модели OSI. Более совершенные межсетевые экраны подобно шлюзу работают на прикладном уровне модели OSI. Они обеспечивают фильтрацию информации не только на сетевом и транспортном, но и на более высоких уровнях эталонной модели [28].

Алгоритмы маршрутизации. Современные протоколы маршрутизации предусматривают автоматическое формирование таблиц маршрутизации и поддержание их в актуальном состоянии на основе взаимодействия маршрутизаторов друг с другом. На каждом маршрутизаторе функционируют программы опроса и прослушивания, с помощью которых он обменивается информацией с другими маршрутизаторами. Полученная информация используется для построения и обновления таблицы маршрутизации.

Таблица маршрутизации, иногда называемая базой данных маршрутизации, включает набор оптимальных путей, используемых маршрутизатором при передаче пакетов в данный момент времени. Каждая строка этой таблицы содержит по крайней мере такую информацию:

- сетевой адрес получателя;
- адрес следующего маршрутизатора, пересылка к которому соответствует оптимальному пути до пункта назначения;
- характеристику пути, например, пропускную способность канала связи и отметку времени, когда эта характеристика была определена;
- информацию о способе пересылки, например номер выходного порта.

В одной строке таблицы могут храниться данные о нескольких возможных следующих транзитных маршрутизаторах, задающих различные критерии оптимальности пути. Способ выбора транзитного маршрутизатора зависит от используемой схемы протокола маршрутизации.

Определение оптимальности путей при формировании и обновлении таблицы маршрутизации может производиться в соответствии с такими критериями или их комбинациями, как:

- длина маршрута, измеряемая количеством маршрутизаторов, через которые необходимо пройти до пункта назначения;
- пропускная способность канала связи;
- прогнозируемое суммарное время пересылки;
- стоимость канала связи.

При наличии таблицы маршрутизации функцию передачи пакетов по оптимальным путям маршрутизатор реализует достаточно просто. Для

отправки пакета через маршрутизатор узел локальной сети помещает в заголовок пакета на сетевом уровне модели OSI адрес действительного получателя, а на канальном уровне — MAC-адрес маршрутизатора. После получения очередного пакета маршрутизатор выполняет следующие действия:

- считывает из заголовка пакета, соответствующего сетевому уровню модели OSI, адрес назначения, т.е. сетевой адрес получателя;
- по таблице маршрутизации определяет адрес следующего транзитного маршрутизатора, пересылка к которому соответствует оптимальному пути до пункта назначения;
- заменяет в заголовке пакета, соответствующего канальному уровню модели OSI, свой MAC-адрес на MAC-адрес выбранного транзитного маршрутизатора;
- отсылает пакет выбранному транзитному маршрутизатору.

По мере того как пакет продвигается через сеть, физический адрес (MAC-адрес) его получателя меняется, но логический адрес пункта назначения, соответствующий сетевому уровню модели OSI, остается без изменений [28].

1.2.10. Виртуальные сети

Коммутаторы, имея большое количество портов, позволяют подключить к своим портам отдельные компьютеры, а также распределить подключенные компьютеры по сетевым сегментам (рис. 1.28) и легко перегруппировать их, когда это необходимо. В результате появляется возможность территориального перемещения компьютеров сети при сохранении ими своих мест в логической сетевой структуре.

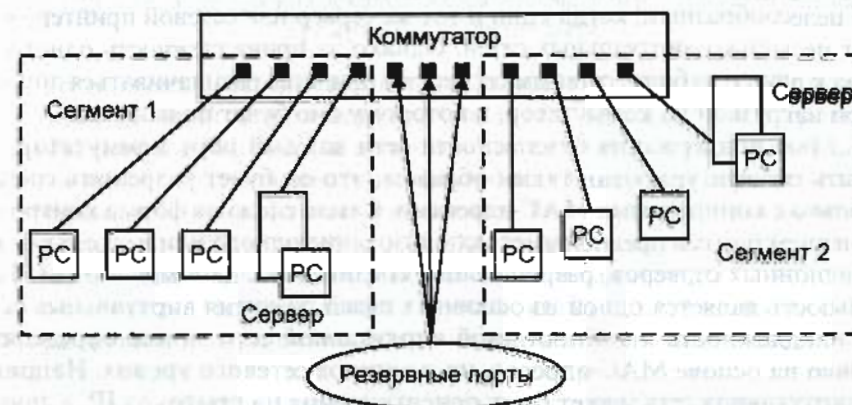


Рис. 1.28. Пример коммутации

Логическая структура сети отражает разбиение сети на рабочие группы, образуемые сетевыми сегментами. В пределах сегмента сети реализуется метод множественного доступа, когда отправляемый компьютером сегмента пакет сообщения доставляется всем остальным компьютерам в этом сегменте, а принимается только тем компьютером, которому он адресован. Сегмен-

ты локальной сети, аппаратно-программное обеспечение которой позволяет отделить ее логическую структуру от физической, называют *виртуальными сетями* (Virtual Local Area Network – VLAN).

Современные коммутаторы поддерживают несколько видов виртуальных сетей (сетевых сегментов), конфигурируемых программным способом:

- виртуальные сети, принадлежность к которым определяется физическими портами коммутаторов;
- виртуальные сети, принадлежность к которым определяется не физическими портами коммутаторов, а MAC-адресами подключенных к коммутаторам устройств;
- виртуальные сети, принадлежность к которым определяется не только MAC-адресами, но и адресами сетевого уровня подключенных к коммутаторам устройств, например адресами протокола IP или IPX.

В первом случае сегменты локальной сети, образующие виртуальные сети, создаются посредством логического соединения портов внутри физической инфраструктуры коммутатора. Например, одни порты коммутатора приписываются к первому сегменту сети, а другие – ко второму. Недостаток такого метода организации виртуальных сетей состоит в том, что все станции, подключенные к одному и тому же порту, должны принадлежать одному и тому же сегменту сети.

Другой метод создания виртуальных сетей базируется на MAC-адресах подсоединенных устройств. При таком способе организации виртуальной сети любой сотрудник сможет подключать свой компьютер, например Notebook, к любому порту коммутатора и коммутатор автоматически определит принадлежность этого компьютера к тому или иному сетевому сегменту на основе его MAC-адреса. Такой метод разрешает также компьютерам, подключенным к одному порту коммутатора, принадлежать разным сегментам сети. Это оказывается целесообразным, когда один и тот же сервер или сетевой принтер обслуживает несколько виртуальных сетей. Однако за принадлежность одного устройства к двум или более сетевым сегментам придется расплачиваться дополнительной нагрузкой на коммутатор, к которому оно будет подключено.

С целью поддержания безопасности сети каждый порт коммутатора может быть сконфигурирован таким образом, что он будет разрешать соединения только с конкретными MAC-адресами. Самая сложная форма контроля за назначением портов предполагает использование одного или нескольких конфигурационных серверов, разрешающих соединения с данным портом. Такая мобильность является одной из основных целей развития виртуальных сетей.

Принадлежность к той или иной виртуальной сети может определяться не только на основе MAC-адресов, но и адресов сетевого уровня. Например, одна виртуальная сеть может быть ориентирована на протокол IP, а другая – на протокол IPX. Система управления виртуальными сетями дает пользователям обеих виртуальных сетей возможность организовывать доступ к серверам, поддерживающим соответствующие протоколы (IP или IPX). В этом случае система разграничит серверы по отдельным сетевым сегментам. Согласно данному способу каждое подсоединенное к коммутатору устройство, например сервер или сетевой принтер, также может входить в несколько виртуальных сетей.

Организация виртуальных сетей на основе адресов сетевого уровня возможна лишь в случае использования маршрутизируемых протоколов, например IP или IPX. В противном случае, например при использовании протокола NetBIOS, виртуальные сети придется организовывать только на основе портов и MAC-адресов.

Описанные способы построения виртуальных сетей особенно эффективны при использовании иерархии территориально распределенных коммутаторов, управляемых централизованным образом (рис. 1.29). Коммутаторы иерархии могут быть распределены, например, между отдельными этажами здания. Для обеспечения устойчивости к сбоям и отказам сети вводятся дополнительные связи между коммутаторами на этажах, которые при нормальной работе сети запрещены, но в случае обрыва любой рабочей линии связи будут задействованы автоматически. В случае необходимости использования одного сервера на всю локальную сеть его необходимо подключить к корневому коммутатору.

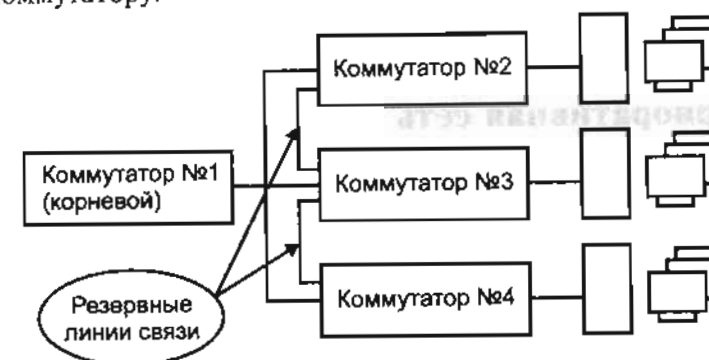


Рис. 1.29. Схема построения локальной сети на основе иерархии коммутаторов с резервными линиями связи

При всех своих достоинствах коммутаторы, как и мосты, имеют один существенный недостаток: они не в силах защитить сеть от лавин широковедаемых пакетов, а это ведет к непроизводительной загрузке сети. Маршрутизаторы могут контролировать и фильтровать ненужный широковедаемый трафик, но они работают медленнее. Типичная производительность маршрутизатора составляет около 10 000 пакетов в секунду, а это не идет ни в какое сравнение с аналогичным показателем коммутатора – около 600 000 пакетов в секунду. Поэтому многие производители стали встраивать в коммутаторы функции маршрутизации, которые в дополнение позволяют организовать виртуальные сети на основе анализа адресов сетевого уровня.

В настоящее время технологии сетевой коммутации интенсивно развиваются. Параллельно с завершением создания универсального стандарта виртуальных сетей производители коммутаторов активно работают над повышением их возможностей автоматической переконфигурации. Ближайшая цель – полностью динамические виртуальные сети, в которых подключение компьютера к порту коммутатора автоматически отслеживается центральным приложением управления, передающим коммутатору всю необходимую для конфигурации сети информацию без малейшего вмешательства администратора.

Конечной целью в стратегических планах производителей является создание виртуальных сетей с внутренней политикой. Поскольку уровень автоматизации управления виртуальными сетями будет очень высоким, администраторы должны будут иметь возможность задавать внутреннюю политику работы сети. Здесь под политикой понимается набор специфических параметров, определяющих правила доступа к сетевым ресурсам, а также правила их использования. По заявлениям производителей, такие виртуальные сети возьмут на себя многие функции сетевых операционных систем, оставив на их долю только предоставление пользователям требуемых сервисов.

Предполагается, что создание виртуальных сетей с внутренней политикой позволит снять с сервера ряд управляющих функций, а также существенно повысит степень безопасности информации. Ведь злоумышленнику, прежде чем добраться до сетевых ресурсов, придется преодолевать уровни защиты, реализуемые коммутаторами. При достижении этой цели сетевые операционные системы могут лишиться многих своих функций по управлению сетью и защите ее ресурсов [28].

1.2.11. Корпоративная сеть

Под корпоративной сетью понимается некоторое наложенное (виртуальное) сетевое пространство с ограниченным (защищенным) доступом к ресурсам передачи, обработки и хранения информации, принадлежащей корпорации (организации), реализованное как на ресурсах сетей связи общего пользования, так и на выделенных каналах связи и средствах коммутации организации [81].

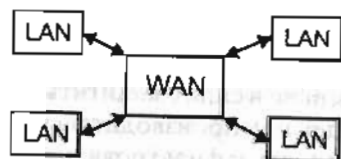


Рис. 1.30. Структура корпоративной сети

Обобщенная структура корпоративной сети приведена на рис. 1.30. Здесь единое сетевое пространство – глобальная сеть (либо сети) – WAN предоставляет виртуальные каналы для взаимодействия между собой локальных вычислительных сетей (LAN) организации. Последние объединяют в себе два типа станций – рабочие станции пользователей и необходимые им сетевые ресурсы (сервер печати и др.), а также информационные серверы, служащие для хранения и обработки информации (файл-сервер, коммуникационный сервер и др.), которые в общем случае распределены на всем сетевом пространстве. В зависимости от иерархии задач обработки информации в корпоративной сети должна быть реализована и иерархия подсетей (LAN), представленная, например, на рис. 1.31. Из сказанного можно сделать следующие выводы [81].



Рис. 1.31. Иерархия подсетей

1. В общем случае корпоративная сеть имеет ярко выраженную типовую структуру, состоящую в объединении различных LAN в единое сетевое пространство на технических средствах WAN общего пользования и на выделенных каналах связи.

2. К структурным особенностям сети организации относится функциональная иерархия локальных вычислительных сетей связи.

В настоящее время применяются следующие типовые архитектурные решения, нашедшие широкое применение в корпоративных сетях [81]:

- межсетевой протокол IP – признанный на сегодняшний день протокол, обеспечивающий возможность объединения в единое сетевое пространство различных сетевых технологий. Это обязательное требование построения большинства корпоративных сетей;
 - транспортные протоколы TCP, UDP, поддерживающие все современные информационные технологии;
 - фиксированный набор команд Интернета, обеспечивающий передачу и обработку сообщений, поддерживаемый протоколами TCP (UDP)/IP, таких как FTP, Telnet и т.д.;
 - технология «клиент–сервер» при взаимодействии рабочих станций сети с информационными серверами;
 - произвольные топологии ЛВС, функционирующие, как правило, под стеком протоколов TCP/IP (прежде всего, Ethernet и FDDI);
 - современные СУБД на информационных серверах, прежде всего Oracle и Informix;
 - современные ОС; многопользовательские ОС UNIX на информационных серверах и ОС Windows на рабочих станциях;
 - неоднородность трафика, содержащего как конфиденциальную, так и открытую информацию;
 - предсказуемость для сети организации трафика как по нагрузке, так и по фиксированности маршрутов передачи информации.
- К задачам по формированию наложенной сети организации на сетевом пространстве общего пользования относятся [81]:
- формирование иерархии технических средств (в частности, подсетей), входящих в состав организации;
 - формирование и выделение технических средств, обеспечивающих обработку и хранение информации организации;
 - реализация разграничения прав доступа пользователей к информационным ресурсам организации;

- реализация ограниченного взаимодействия пользователей организации с внешними по отношению к ней абонентами того же сетевого пространства;
- решение задач администрирования в рамках корпоративной сети, включающее управление безопасностью, эффективностью и надежностью функционирования корпоративной сети.

1.2.12. Автоматизированные системы управления

Автоматизированные системы управления (АСУ) в сложившемся в настоящее время понимании отличаются от вычислительных сетей наличием средств, решающих задачи управления каким-либо процессом. Например, процессом производства каких-либо изделий, процессом управления какой-либо организацией, предприятием, коммерческой структурой и т.д.

Различают системы управления техническими устройствами, производственными процессами и системы административно-организационного управления. В первых и вторых объектами управления являются различные технические устройства (самолет, станок, домна, ракета и т.д.), в третьих – коллективы людей.

АСУ административно-организационного управления предназначены для комплексной автоматизации всех или большинства основных функций органов управления: сбора и анализа информации, планирования и принятия решений, доведения решений до исполнителей и контроля исполнения. Этим они отличаются от автономного использования технических средств или автоматизации отдельных подсистем управления.

АСУ административно-организационного управления представляют собой сложные комплексы коллективов специалистов, технических средств, математического, программного, информационного и лингвистического обеспечения, предназначенных для сбора, переработки и выдачи информации. Общая структура таких автоматизированных систем обычно соответствует иерархической структуре органов управления и принятым в них процессам управления. Обычно автоматизированные системы административно-организационного управления представляют собой ряд автоматизированных объектов при органах управления различных уровней (производственный участок, цех, завод и т.д.), объединенных единой системой обмена данными – автоматизированной системой связи. Каждый автоматизированный объект в свою очередь включает информационно-вычислительный комплекс объекта, значительное число автоматизированных рабочих мест административных работников с устройствами формирования запросов, ввода и выдачи информации, средства математического обеспечения и технические устройства, обеспечивающие процесс функционирования объекта.

Объекты АСУ условно разделяются на основные и вспомогательные. К основным относятся управляющие объекты и объекты управления. Управляющий объект является источником управляющего воздействия, направленного на достижение поставленной цели управления. Объект управления является исполнителем управляющих воздействий, получаемых от управляющего объекта.

Вспомогательные объекты служат для автоматизации обработки и передачи информации, циркулирующей в системе. К ним относятся вычислительные центры, узлы коммутации сообщений, объекты связи и т.п. Вычислительные центры, на которых реализуются информационно-расчетные процессы в интересах органов управления системы, территориально могут размещаться как на основных объектах, так и на некотором удалении от них. Центры коммутации сообщений и другие объекты связи совместно с каналами связи предназначены для обеспечения автоматизации обмена информацией между объектами системы.

Наиболее распространенные структурные конфигурации АСУ:

- централизованная с непосредственным подчинением объектов центральному пункту управления;
- централизованная с автономными подсистемами;
- иерархическая с последовательными связями;
- иерархическая с последовательно-параллельными связями.

Поскольку последняя структура АСУ содержит указанные выше варианты структур, она представлена на рис. 1.32. Указанные на рисунке объекты связаны между собой или по прямым каналам связи, или через узлы коммутации сети обмена данными (на рисунке не показано). Поскольку в больших АСУ объекты системы территориально могут быть удалены друг от друга на большие расстояния (до сотен и тысяч километров), преимущественно используются узлы коммутации сообщений и пакетов, которые обеспечивают доведение команд с верхнего управляющего объекта до исполнителя в нижней ступени иерархии системы, а также с нижней ступени до верхней.

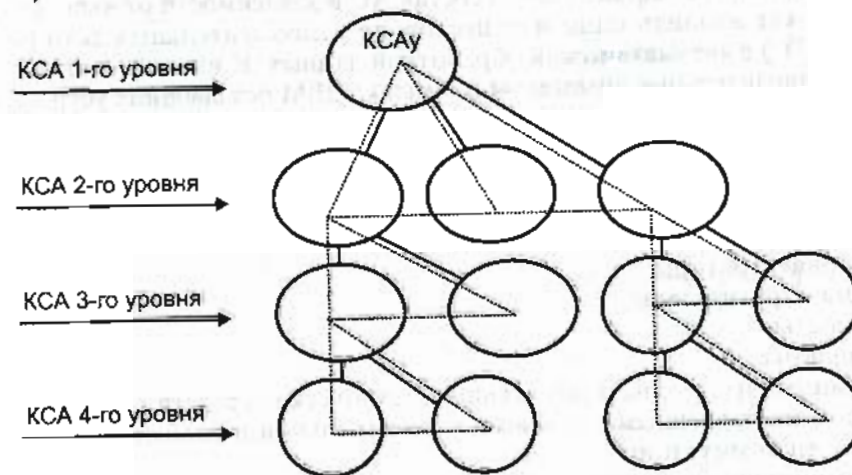


Рис. 1.32. Структурная схема многоступенчатой АСУ

Системотехнически управляющие, управляемые объекты и передача данных АСУ реализуются на тех же решениях, что и вычислительные сети. Они представляют собой в зависимости от выполняемых задач различного масштаба системы с централизованной и распределенной обработкой данных, основные принципы построения которых приведены выше. Помимо приклад-

ных задач АСУ отличает от вычислительных сетей наличие иерархических отношений ее абонентов, реализация которых обеспечивается в настоящее время за счет средств цифровой подписи, абонентского шифрования и организационных мероприятий службы безопасности информации АСУ.

В настоящее время в АСУ используются современные аппаратные, программные и системотехнические решения вычислительных сетей, в том числе в виде корпоративной сети.

1.2.13. Классификация автоматизированных систем

Анализ указанных выше материалов по принципам построения автоматизированных систем позволяет определить типовые системы (см. Введение), к которым относятся: автоматизированное рабочее место; рабочая станция; информационный вычислительный комплекс; локальная вычислительная сеть; комплекс средств автоматизации; телекоммуникационная вычислительная сеть; сеть передачи данных; автоматизированная система управления.

Корпоративную сеть можно отнести к АСУ, реализованной программными средствами, наложенными на готовую телекоммуникационную сеть общего пользования, в которой ее абоненты связаны между собой системными отношениями, реализующими задачи какой-либо организации, предприятия, корпорации и т.д.

Данные виды АС могут быть не только законченными самостоятельными структурами, способными выполнять свои задачи, но и являться элементами более сложной АС. Кроме того, в состав АС в зависимости от выполняемых задач может входить один или несколько вспомогательных технических средств (ТС) с автоматической обработкой данных. К ним относятся:

- вычислительные комплексы (комплекс ЭВМ без внешних устройств);
- серверы;
- табло коллективного пользования;
- аппаратура передачи данных, модемы;
- повторители;
- коммутаторы;
- концентраторы;
- маршрутизаторы;
- мосты;
- шлюзы.

Комплекс из группы перечисленных технических средств в составе, определенном поставленными задачами в региональной и глобальной сети, образует узел коммутации.

Перечисленные технические средства во время нормального функционирования АС не требуют вмешательства человека. С позиций безопасности информации достаточно того, что доступ к ним (кроме табло) будет закрыт механически корпусом и крышками с датчиками вскрытия, находящимися под централизованным контролем службы безопасности.

Среди них с позиций безопасности информации необходимо выделить специальные вычислительные комплексы, серверы и табло. Специальные вычислительные комплексы могут решать некоторое множество специальных

функциональных задач. Серверы являются накопителями больших объемов данных различного назначения и важности, с которыми также могут работать пользователи, обращаясь к ним по линиям связи. Табло по определению является средством коллективного отображения информации, доступ к которой может быть ограничен только отдельным помещением.

Учитывая изложенное выше, можно предложить следующую классификацию АС обработки информации по видам (рис. 1.33). На рисунке представлены виды АС как законченные аппаратно-программные изделия, прошедшие все этапы создания и имеющие своего владельца. Поэтому на рисунке не показаны персональный компьютер, виртуальные сети и сеть Интернет. Первый – как не имеющий прикладных программ АС, вторая – как сеть, являющаяся составной частью АС, третья – как сеть, не имеющая единого владельца. С технической точки зрения Интернет – объединение транснациональных компьютерных сетей, работающих по самым разнообразным протоколам, связывающим всевозможные типы компьютеров, физически передающих данные по телефонным и оптоволоконным линиям связи, через спутники и радиомодемы. С административной точки зрения сеть Интернет – не более чем терминологическая удобная условность. Координацию сети осуществляет Центр информационных сетей при Стэнфордском университете в Менло-парке (шт. Калифорния, США) [63].

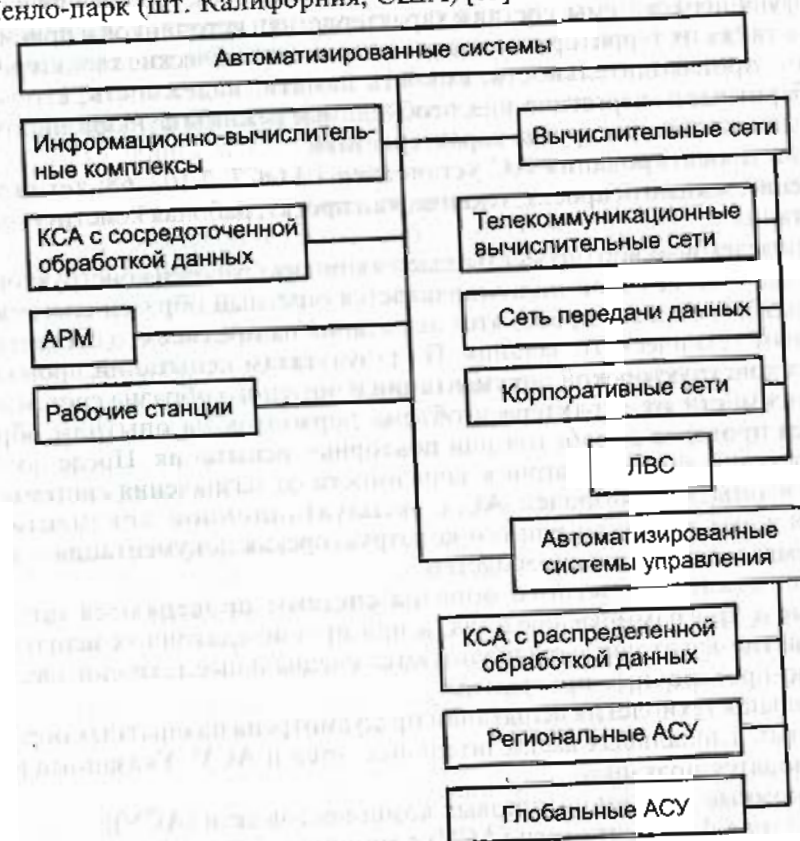


Рис. 1.33. Классификация автоматизированных систем

Столь широкий диапазон рассматриваемых систем выбран не только по причине общей проблемы защиты информации, но и потому, что все перечисленные виды АС могут входить в состав одной и той же региональной или глобальной вычислительной сети или АСУ. Очевидно, что концепция безопасности информации, теория и основные принципы построения ее защиты в них должны быть едиными. Такому подходу способствует также и то, что ввод-вывод, хранение, обработка и передача информации во всех видах АС строятся на базе типовых методов и средств. Поиск подобных методов и средств обеспечения безопасности информации также является основной задачей при проектировании АС.

1.2.14. Организация проектирования автоматизированных систем

Проектирование автоматизированных систем обработки данных – это создание комплекта конструкторской и программной документации, необходимой для производства, испытаний и эксплуатации. Цель проектирования, назначение проектируемой системы, исходные данные и технические требования устанавливаются техническим заданием. В нем задаются: требования к выполняемым функциям системы, состав и характеристики источников и приемников данных, а также их территориальное размещение; технические характеристики системы – производительность, емкость памяти, надежность, стоимость, массогабаритные и энергетические; необходимые режимы функционирования; условия эксплуатации и другие характеристики.

Стадии проектирования АС установлены ГОСТ 2.103–68: техническое предложение, эскизный проект, технический проект, рабочая конструкторская документация.

На основе технического проекта создается комплект рабочей конструкторской документации, по которой подготавливается опытный образец системы.

На опытном образце проводятся испытания на предмет его соответствия требованиям технического задания. По результатам испытаний проводится доработка конструкторской документации и опытного образца системы. Далее в зависимости от характера и объема доработок на опытном образце проводятся проверка доработок или повторные испытания. После положительных результатов испытаний в зависимости от назначения системы и ее сложности опытный образец АС с эксплуатационной документацией передается в эксплуатацию или его конструкторская документация – на запуск системы в серийное производство.

При испытаниях опытного образца системы проверяются штатные аппаратные и программные средства, а при приемо-сдаточных испытаниях на предприятии-изготовителе используются специальные технологические и контрольно-проверочные программы.

Специальная технология испытаний предусмотрена на опытных образцах региональных, глобальных вычислительных сетей и АСУ. Указанные испытания проводятся поэтапно:

- 1) автономные испытания типовых компонентов сети (АСУ);
- 2) испытания фрагмента сети (АСУ) с минимальной конфигурацией, позволяющей проверить основные функции системы;

3) доработки сети (АСУ) по результатам испытаний;

4) испытания сети (АСУ) в полном составе.

Автоматизированная система считается законченным и годным к эксплуатации изделием, если она прошла испытания на соответствие требованиям технического задания (предварительные и государственные для госзаказчика и аналогичные испытания для частного заказчика), имеет соответствующие конструкторскую и эксплуатационную документацию, технические условия (ТУ), паспорт или формуляр, а также акты приемки и передачи в эксплуатацию заказчику.

Региональные и глобальные АС по договоренности с заказчиком могут сдаваться в эксплуатацию фрагментами, сначала в опытную, а затем в рабочую.

1.2.15. Условия и режимы эксплуатации автоматизированных систем

Эксплуатация автоматизированной системы состоит из технического и системотехнического обслуживания и использования ее по прямому назначению.

Техническое обслуживание заключается в обеспечении работоспособности системы путем создания требуемых условий эксплуатации и проведения согласно инструкции по эксплуатации профилактических и ремонтно-восстановительных работ. Для повышения эффективности технического обслуживания в системах предусматриваются средства накопления данных об ошибках, сбоях и отказах. Данные накапливаются путем регистрации состояния системы в момент ошибки, обнаруживаемой встроенными средствами контроля или программами. Регистрация данных производится операционной системой в специальном системном журнале – области накопителя на магнитных дисках. Данные из системного журнала периодически или при необходимости выводятся на печать и используются обслуживающим персоналом для выявления источников ошибок, сбоев и отказов с целью проведения профилактических и ремонтно-восстановительных работ.

Системотехническое обслуживание заключается в обеспечении эффективности использования системы с целью снижения стоимости обработки данных, повышения производительности системы, качества обслуживания пользователей и др.

В зависимости от назначения и характера задач по обработке информации можно выделить три основных вида эксплуатации автоматизированных систем, имеющих принципиальное значение для состава должностных лиц и характера доступа к информации:

1) с закрытым доступом; организация-потребитель использует автоматизированную систему полностью в своих интересах; при этом обслуживающий персонал, включая технический и оперативный состав, являются сотрудниками данной организации. Например, АСУ по управлению предприятием;

2) с ограниченным доступом; организация-потребитель вычислительной системы сочетает свои интересы с интересами других организаций и частных лиц. Например, вычислительный центр;

3) с открытым доступом; организация-потребитель вычислительной сети (АСУ) оказывает услуги населению. Например, банковская финансово-кредитная автоматизированная система. Название «Система с открытым доступом» условно в том смысле, что любой человек может воспользоваться услугами данной системы. На самом же деле каждая АС имеет и внутреннюю часть, касающуюся обработки ее собственной информации, которая может быть закрыта для посторонних лиц. Банки и подобные им финансовые структуры несут также юридическую ответственность за информацию, доверяемую им клиентами.

По истечении некоторого времени в процессе эксплуатации сложных АС могут потребоваться ремонт и доработки принципиального характера.

1.3. Потенциальные угрозы безопасности информации

1.3.1. Постановка задачи

Исследование и анализ многочисленных случаев воздействий на информацию и несанкционированного доступа к ней показывают, что их можно разделить на случайные и преднамеренные. Преднамеренные угрозы часто путем их систематического применения могут быть приведены в исполнение через случайные путем долговременной массовой атаки несанкционированными запросами или вирусами.

Последствия, к которым приводит реализация угроз, следующие: разрушение (утрата) информации, модификация (изменение информации на ложную, которая корректна по форме и содержанию, но имеет другой смысл) и ознакомление с ней посторонних лиц. Цена указанных событий может составлять сотни тысяч долларов и более. Предупреждение означенных последствий в автоматизированной системе и есть основная цель создания системы безопасности информации.

Перед проектированием новых и выбором готовых средств защиты информации необходимо определить природу угроз, формы, места и пути их возможного проявления и осуществления в автоматизированной системе. Для решения поставленной задачи приведем все многообразие угроз и путей их воздействия к простейшим видам и формам, которые были бы адекватны их множеству в автоматизированной системе.

1.3.2. Случайные угрозы

Исследования опыта проектирования, изготовления, испытаний и эксплуатации автоматизированных систем говорят о том, что информация в процессе ввода, хранения, обработки, вывода и передачи подвергается

различным случайным воздействиям. В результате таких воздействий на аппаратном уровне происходят физические изменения уровней сигналов в цифровых кодах, несущих информацию.

При этом наблюдаются в одном, двух, трех и т.д. разрядах изменение 1 на 0, или 0 на 1, или то и другое вместе, но в разных разрядах, следствием чего в итоге является изменение значения кода. Если применяемые для этой цели средства функционального контроля способны обнаружить эти изменения (например, контроль по модулю 2 легко обнаруживает однократную ошибку), производится браковка данного кода, а устройство, блок, модуль или микросхема, участвующие в обработке, объявляются неисправными. Если функциональный контроль отсутствует или не способен обнаружить неисправность на данном этапе обработки, процесс обработки продолжается по ложному пути, т.е. происходит модификация информации. В процессе дальнейшей обработки в зависимости от содержания и назначения ложной команды возможны либо пересылка информации по ложному адресу, либо передача ложной информации адресату, либо стирание или запись другой информации в ОЗУ или долговременное запоминающее устройство (ДЗУ) и т.д., что провоцирует нежелательные события: разрушение (утрату), модификацию и утечку информации.

На программном уровне в результате случайных воздействий может произойти изменение алгоритма обработки информации на непредусмотренный, характер которого тоже может быть различным: в лучшем случае – остановка вычислительного процесса, а в худшем – его модификация. Если средства функционального контроля изменения не обнаруживают, последствия модификации алгоритма или данных могут пройти незамеченными или привести также к разрушению информации, а при перепутывании адреса устройства – к утечке информации. При программных ошибках могут подключаться программы ввода-вывода и передачи их на запрещенные устройства.

Причинами случайных воздействий при эксплуатации автоматизированной системы могут быть:

- отказы и сбои аппаратуры;
- помехи на линиях связи от воздействий внешней среды;
- ошибки человека как звена системы;
- схемные и системотехнические ошибки разработчиков;
- структурные, алгоритмические и программные ошибки;
- аварийные ситуации и другие воздействия.

Частота отказов и сбоев аппаратуры увеличивается с выбором при проектировании системы недостаточно надежной в отношении функционирования аппаратуры. Помехи на линиях связи зависят от правильности выбора места размещения технических средств АС относительно друг друга и по отношению к аппаратуре и агрегатам соседних систем.

При разработке сложных автоматизированных систем увеличивается число схемных, системотехнических, структурных, алгоритмических и программных ошибок. На их количество в процессе проектирования оказывают большое влияние квалификация разработчиков, условия их работы, наличие опыта и другие обстоятельства.

На этапах изготовления и испытаний на качество входящей в АС аппаратуры влияют полнота и качество документации, технологическая дисциплина и другие факторы.

К ошибкам человека как звена системы следует относить ошибки человека как источника информации, человека-оператора, неправильные действия обслуживающего персонала и ошибки человека как звена, принимающего решения.

Ошибки человека могут подразделяться на логические (неправильно принятые решения), сенсорные (неправильное восприятие оператором информации) и оперативные, или моторные (неправильная реализация решения). Интенсивность ошибок человека может колебаться в широких пределах: от 1–2 до 15–40% и выше общего числа операций, выполняемых при решении задачи [54].

Несмотря на то что человек как элемент системы обладает по сравнению с техническими средствами рядом преимуществ (адаптируемостью, обучаемостью, эвристичностью, избирательностью, способностью к работе в конфликтных ситуациях), он в то же время имеет ряд недостатков, основными из которых являются: утомляемость, зависимость психологических параметров от возраста, чувствительность к изменениям окружающей среды, зависимость качества работы от физического состояния, эмоциональность.

Для расчета достоверности выходной информации важны статистические данные по уровню ошибок человека как звена системы. Данные [54] показывают, что интенсивность ошибок человека-оператора составляет $2 \cdot 10^{-2}$ – $4 \cdot 10^{-3}$. Исследования, проведенные Мейстером [54] по выявлению количества ошибок при работе человека-оператора, показали, что вероятность ошибок зависит от общего количества кнопок, количества кнопок в ряду, числа кнопок, которые необходимо нажимать одновременно, и расстояния между кнопками.

Громадное значение имеют также ошибки человека как звена системы, принимающего решение. Особенно важное значение приобретает проблема борьбы с ошибками такого рода в автоматизированных системах управления административного типа. Некоторые вопросы, связанные с психологическими аспектами принятия решения, рассмотрены в книге У.Морриса¹.

Вопросы, связанные с выбором критериев, стимулирующих деятельность человека в АСУ, можно найти в работах академика В.А. Трапезникова².

Ошибки человека как звена системы, принимающего решение, вызваны неадекватным восприятием реальной ситуации и свойством действовать по заранее намеченной программе. Например, руководитель, будучи уверен, что мастер зависил требуемое количество дефицитного материала, уменьшает соответствующую заявку и тем самым вводит в АСУ ошибочные данные.

Другой важной особенностью человека является стремление к построению упрощенной модели рассматриваемой ситуации. Чрезмерное упрощение конкретной ситуации, исключение из нее важных моментов и принятое при этом решение могут оказаться ошибочными.

¹ См.: Моррис У. Наука об управлении. Байесовский подход. – М.: Мир, 1971.

² См.: Трапезников В.А. Человек в системе управления // Наука и жизнь. – 1972. – №2.

К угрозам случайного характера следует также отнести аварийные ситуации, которые могут возникнуть на объекте размещения автоматизированной системы:

- отказ функционирования АС в целом; например, выход из строя электропитания и освещения;
- стихийные бедствия: пожар, наводнение, землетрясение, ураганы, удары молнии, обвалы и т.д.;
- отказ системы жизнеобеспечения на объекте эксплуатации АС.

Вероятность этих событий связана прежде всего с правильным выбором места размещения АС, включая географическое положение, и организацией противопожарных мероприятий.

1.3.3. Преднамеренные угрозы

Преднамеренные угрозы связаны с действиями человека, причинами которых могут быть недовольство жизненной ситуацией, выполнение по долгу службы задач разведчика, диверсанта и провокатора, сугубо материальный интерес или развлечение, цель которого самоутверждение, как у хакеров, или желание получить удовольствие от того, что кому-то «крупно насолил», и т.д. Оговоримся сразу, что изучение мотивов поведения нарушителя не является нашей задачей. Наша задача – предупреждение, обнаружение и блокировка его возможных действий в АС. Потенциальные угрозы с этой стороны будем рассматривать только в техническом аспекте.

Потенциальные угрозы необходимо анализировать с учетом этапа создания и эксплуатации АС, исходной позиции и ожидаемой модели поведения нарушителя.

На этапе создания (проектирования, изготовления и испытаний) АС наиболее опасными являются:

- ошибки разработчиков программного обеспечения;
- выбор и применение готовых программных продуктов, имеющих ошибки и недоработки;
- преднамеренные аппаратные закладки, позволяющие считывать и передавать по радиозифиру информацию в заданные момент и промежутки времени;
- преднамеренные программные закладки типа вирусов, «троянских коней», «люков» и др.

Ошибки, как уже было указано, относятся к разряду случайных событий. Но на этапе эксплуатации указанными ошибками может с успехом воспользоваться нарушитель. Напомним, что ввиду ограниченного объема данной книги защита от перечисленных выше угроз в ней не рассматривается. Считается, что перед сдачей АС в эксплуатацию такая работа была проведена с положительными результатами. Рассмотрим потенциальные угрозы информации АС на этапе эксплуатации.

Исходная позиция нарушителя зависит от того, является ли он посторонним человеком или законным пользователем АС. В последнем случае нарушитель уже имеет санкционированный доступ к информации и ресурсам АС

в рамках данных ему полномочий, если в системе существуют средства разграничения доступа, которые он попытается преодолеть. Ожидаемая модель поведения нарушителя определяется его исходной позицией, квалификацией, степенью владения объемом информации о принципах построения системы и ее защиты.

Посторонний человек попытается проникнуть в систему, используя незащищенные каналы и линии связи, а также прибегнув к нижеследующим методам, которые рассмотрим по материалам [3].

В общем случае программное обеспечение любой универсальной компьютерной системы состоит из трех основных компонентов: операционной системы, сетевого программного обеспечения (СПО) и системы управления базами данных (СУБД). Поэтому все попытки взлома защиты компьютерных систем можно разделить на три группы:

- атаки на уровне операционной системы;
- атаки на уровне сетевого программного обеспечения;
- атаки на уровне систем управления базами данных.

Защита СУБД является одной из самых простых задач. Это связано с тем, что СУБД имеют строго определенную внутреннюю структуру, и операции над элементами СУБД заданы довольно четко. Есть четыре основных действия – поиск, вставка, удаление и замена элемента. Другие операции являются вспомогательными и применяются достаточно редко. Наличие строгой структуры и четко определенных операций упрощает решение задачи защиты СУБД. В большинстве случаев хакеры предпочитают взламывать защиту на уровне операционной системы и получать доступ к файлам СУБД с помощью средств операционной системы. Однако в случае, если используется СУБД, не имеющая достаточно надежных защитных механизмов, или плохо протестированная версия СУБД, содержащая ошибки, или если при определении политики безопасности администратором СУБД были допущены ошибки, то становится вполне вероятным, что хакер может преодолеть защиту, реализуемую на уровне СУБД.

Кроме того, имеются два специфических сценария атаки на СУБД, для защиты от которых требуются специальные методы. В первом случае результаты арифметических операций над числовыми полями СУБД округляются в меньшую сторону, а разница суммируется в некоторой другой записи СУБД (как правило, эта запись содержит личный счет хакера в банке, а округляемые числовые поля относятся к счетам других клиентов банка). Во втором случае хакер получает доступ к полям записей СУБД, для которых доступной является только статистическая информация. Идея хакерской атаки на СУБД – так хитро сформулировать запрос, чтобы множество записей, для которых собирается статистика, состояло только из одной записи.

Защищать операционную систему, в отличие от СУБД, гораздо сложнее. Дело в том, что внутренняя структура современных операционных систем чрезвычайно сложна, и поэтому соблюдение адекватной политики безопасности является более трудной задачей. Среди людей несведущих бытует мнение, что самые эффективные атаки на операционные системы могут быть организованы только с помощью сложнейших средств, основанных на самых последних достижениях науки и техники, а хакер должен быть программистом высочайшей квалификации. Это не совсем так.

Никто не спорит с тем, что пользователю следует быть в курсе всех новинок в области компьютерной техники. Да и высокая квалификация – совсем не лишнее. Однако искусство хакера состоит отнюдь не в том, чтобы взламывать любую самую «крутую» компьютерную защиту. Нужно просто суметь найти слабое место в конкретной системе защиты. При этом простейшие методы взлома оказываются ничуть не хуже самых изощренных, поскольку чем проще алгоритм атаки, тем выше вероятность ее завершения без ошибок и сбоев, особенно если возможности предварительного тестирования этого алгоритма в условиях, приближенных к «боевым», весьма ограничены.

Успех реализации того или иного алгоритма хакерской атаки на практике в значительной степени зависит от архитектуры и конфигурации конкретной операционной системы, являющейся объектом этой атаки. Однако имеются атаки, которым может быть подвергнута практически любая операционная система [3]. К ним относятся:

- кража пароля;
- подглядывание за пользователем, когда тот вводит пароль, дающий право на работу с операционной системой (даже если во время ввода пароль не высвечивается на экране дисплея, хакер может легко узнать пароль, следя за перемещением пальцев пользователя по клавиатуре);
- получение пароля из файла, в котором этот пароль был сохранен пользователем, не желающим затруднять себя вводом пароля при подключении к сети (как правило, такой пароль хранится в файле в незашифрованном виде);
- поиск пароля, который пользователи, чтобы не забыть, записывают на календарях, в записных книжках или на обратной стороне компьютерных клавиатур (особенно часто подобная ситуация встречается, если администраторы заставляют пользователей применять труднозапоминаемые пароли);
- кража внешнего носителя парольной информации (дискеты или электронного ключа, на которых хранится пароль пользователя, предназначенный для входа в операционную систему);
- полный перебор всех возможных вариантов пароля;
- подбор пароля по частоте встречаемости символов и биграмм, с помощью словарей наиболее часто применяемых паролей, с привлечением знаний о конкретном пользователе – его имени, фамилии, номера телефона, даты рождения и т.д., с использованием сведений о существовании эквивалентных паролей, при этом из каждого класса опробуется всего один пароль, что может значительно сократить время перебора;
- сканирование жестких дисков компьютера (хакер последовательно пытается обратиться к каждому файлу, хранимому на жестких дисках компьютерной системы; если объем дискового пространства достаточно велик, можно быть уверенным, что при описании доступа к файлам и каталогам администратор допустил хотя бы одну ошибку, в результате чего все такие каталоги и файлы будут прочитаны хакером; для сокрытия следов хакер может организовать эту атаку под чужим именем, например, под именем пользователя, пароль которого известен хакеру);
- сбор «мусора» (если средства операционной системы позволяют восстанавливать ранее удаленные объекты, хакер может воспользоваться этой возможностью, чтобы получить доступ к объектам, удаленным другими пользователями, например, просмотрев содержимое их «мусорных» корзин);

- превышение полномочий (используя ошибки в программном обеспечении или в администрировании операционной системы, хакер получает полномочия, превышающие полномочия, предоставленные ему согласно действующей политике безопасности);
- запуск программы от имени пользователя, имеющего необходимые полномочия, или в качестве системной программы (драйвера, сервиса, демона и т.д.);
- подмена динамически загружаемой библиотеки, используемой системными программами, или изменение переменных среды, описывающих путь к таким библиотекам;
- модификация кода или данных подсистемы защиты самой операционной системы;
- отказ в обслуживании (целью этой атаки является частичный или полный вывод из строя операционной системы);
- захват ресурсов (хакерская программа производит захват всех имеющихся в операционной системе ресурсов, а затем входит в бесконечный цикл);
- бомбардировка запросами (хакерская программа постоянно направляет операционной системе запросы, реакция на которые требует привлечения значительных ресурсов компьютера);
- использование ошибок в программном обеспечении или администрировании.

Если в программном обеспечении компьютерной системы нет ошибок и ее администратор строго соблюдает политику безопасности, рекомендованную разработчиками операционной системы, то атаки всех перечисленных типов малоэффективны. Дополнительные меры, которые должны быть предприняты для повышения уровня безопасности, в значительной степени зависят от конкретной операционной системы, под управлением которой работает данная компьютерная система. Тем не менее приходится признать, что полностью устранить угрозу взлома компьютерной системы на уровне операционной системы невозможно. Поэтому политика обеспечения безопасности должна быть направлена на то, чтобы вероятность проникновения нарушителя в операционную систему была минимальной.

Сетевое программное обеспечение является наиболее уязвимым, потому что канал связи, по которому передаются сообщения, чаще всего не защищен, и всякий, кто имеет доступ к этому каналу, соответственно может перехватывать сообщения и отправлять свои собственные. Поэтому на уровне СПО возможны следующие хакерские атаки [3]:

- прослушивание сегмента локальной сети (в пределах одного и того же сегмента локальной сети любой подключенный к нему компьютер в состоянии принимать сообщения, адресованные другим компьютерам сегмента, а следовательно, если компьютер хакера подсоединен к некоторому сегменту локальной сети, то ему становится доступен весь информационный обмен между компьютерами этого сегмента);
- перехват сообщений на маршрутизаторе (если хакер имеет привилегированный доступ к сетевому маршрутизатору, то он получает возможность перехватывать все сообщения, проходящие через этот маршрутизатор, и хотя тотальный перехват невозможен из-за слишком большого объема, чрезвычай-

чайно привлекательным для хакера является выборочный перехват сообщений, содержащих пароли пользователей и их электронную почту);

- создание ложного маршрутизатора (путем отправки в сеть сообщений специального вида хакер добивается, чтобы его компьютер стал маршрутизатором сети, после чего получает доступ ко всем проходящим через него сообщениям);

• навязывание сообщений (отправляя в сеть сообщения с ложным обратным сетевым адресом, хакер переключает на свой компьютер уже установленные сетевые соединения и в результате получает права пользователей, чьи соединения обманным путем были переключены на компьютер хакера);

- отказ в обслуживании (хакер отправляет в сеть сообщения специального вида, после чего одна или несколько компьютерных систем, подключенных к сети, полностью или частично выходят из строя).

Для конкретизации задачи проанализируем объект обработки информации на предмет ввода-вывода, хранения, ее обработки и возможностей нарушителя по доступу к информации при отсутствии средств защиты в данной автоматизированной системе.

В качестве объекта исследования согласно приведенной выше классификации АС (рис. 1.33) выбираем вначале информационно-вычислительный комплекс, который является системой с сосредоточенной обработкой данных и может быть элементом вычислительной сети или АСУ. Для вычислительных систем в этом случае характерны следующие штатные (законные) каналы доступа к информации:

- терминалы пользователей;
- терминал администратора системы;
- терминал оператора функционального контроля;
- средства отображения информации;
- средства документирования информации;
- средства загрузки программного обеспечения в вычислительный комплекс;
- носители информации (ОЗУ, ЖМД, ГМД, НМЛ, CD, бумажные носители);
- внешние каналы связи.

Имея в виду, что при отсутствии защиты нарушитель может воспользоваться как штатными, так и другими физическими каналами доступа, назовем возможные каналы несанкционированного доступа (ВКНСД) в вычислительной системе, через которые можно получить доступ к аппаратуре, ПО и осуществить хищение, разрушение, модификацию информации и ознакомление с ней. К ним относятся:

- все перечисленные выше штатные средства при их использовании законными пользователями не по назначению и за пределами своих полномочий;
- все перечисленные выше штатные средства при их использовании посторонними лицами;
- технологические пульты управления;
- внутренний монтаж аппаратуры;
- линии связи между аппаратными средствами данной вычислительной системы;

- ремонтируемые запоминающие устройства с остатками информации;
- побочное электромагнитное излучение информации с аппаратуры системы;
- побочные наводки информации по сети электропитания и заземления аппаратуры;
- побочные наводки информации на вспомогательных и посторонних коммуникациях;
- отходы обработки информации в виде бумажных и магнитных носителей, брошенные в мусорную корзину.

Очевидно, что при отсутствии законного пользователя, контроля и разграничения доступа к терминалу квалифицированный нарушитель легко воспользуется его функциональными возможностями для несанкционированного доступа к информации путем ввода соответствующих запросов или команд. При наличии свободного доступа в помещения можно визуально наблюдать информацию на средствах отображения и документирования, а на последних похитить бумажный носитель, снять лишнюю копию, а также похитить другие носители с информацией: листинги, магнитные ленты, диски. Особую опасность представляет бесконтрольная загрузка программного обеспечения в ЭВМ, в которой могут быть изменены данные, алгоритмы или введена программа «троянский конь» – программа, выполняющая дополнительные незаконные функции: запись информации на посторонний носитель, передачу в каналы связи другого абонента вычислительной сети, внесение в систему компьютерного вируса и т.д. При отсутствии разграничения и контроля доступа к технологической и оперативной информации возможен доступ к оперативной информации со стороны терминала функционального контроля. Очень опасна ситуация, когда нарушителем является пользователь вычислительной системы, который по своим функциональным обязанностям имеет законный доступ к одной части информации, а обращается к другой за пределами своих полномочий.

У законного пользователя имеется много способов нарушать работу вычислительной системы, злоупотреблять ею, извлекать, модифицировать или уничтожать информацию. Для этой цели могут быть использованы привилегированные команды ввода-вывода, отсутствие контроля законности запроса и обращений к адресам памяти ОЗУ, ДЗУ и т.д. Свободный доступ позволит ему обращаться к чужим файлам и банкам данных и изменить их случайно или преднамеренно.

При техническом обслуживании (профилактике и ремонте) аппаратуры могут быть обнаружены остатки информации на магнитной ленте, поверхностях дисков и других носителях информации. Стирание информации обычными методами не всегда эффективно. Ее остатки могут быть легко прочитаны. При транспортировании носителя по неохраняемой территории существует опасность его перехвата и последующего ознакомления посторонних лиц с секретной информацией.

Не имеет смысла создание системы контроля и разграничения доступа к информации на программном уровне, если не контролируется доступ к управлению ЭВМ, внутреннему монтажу аппаратуры, кабельным соединениям.

Нарушитель может стать незаконным пользователем системы в режиме разделения времени, определив порядок работы законного пользователя либо

работая вслед за ним по одним и тем же линиям связи. Он может также использовать метод проб и ошибок и реализовать «дыры» в операционной системе, прочесть пароли. Без знания паролей он постарается осуществить «селективное» включение в линию связи между терминалом и процессором ЭВМ; без прерывания работы законного пользователя может продлить ее от его имени, аннулировав сигналы отключения законного пользователя.

Процессы обработки, передачи и хранения информации аппаратными средствами автоматизированной системы обеспечиваются срабатыванием логических элементов, построенных на базе полупроводниковых приборов, выполненных чаще всего в виде интегральных схем. Срабатывание логических элементов обусловлено высокочастотным изменением уровней напряжений и токов, что приводит к возникновению в эфире, цепях питания и заземления, а также в параллельно расположенных цепях и индуктивностях посторонней аппаратуры, электромагнитных полей и наводок, несущих в амплитуде, фазе и частоте своих колебаний признаки обрабатываемой информации. Использование нарушителем различных примесей может привести к утечке информации. С уменьшением расстояния между приемником нарушителя и аппаратными средствами вероятность приема сигналов такого рода увеличивается.

Непосредственное подключение нарушителем примесной аппаратуры и специальных датчиков к цепям электропитания и заземления, к каналам связи также позволяет совершать несанкционированное ознакомление с информацией, а несанкционированное подключение к каналам связи передающей аппаратуры может привести и к модификации информации.

Особо следует отметить угрозы, которым могут подвергаться АС на каналах и линиях связи.

Предположим, что нарушитель может располагаться в некоторой точке сети, через которую должна проходить вся интересующая его информация. Например, в межсетевых условиях нарушитель может подключить аппаратуру в виде шлюза в некоторой промежуточной сети, которая обеспечивает единственный путь соединения между двумя процессами, являющимися конечными интересующего нарушителя соединения. В общем случае предполагается, что нарушитель занимает позицию, позволяющую осуществлять пассивный и активный перехват данных.

В случае пассивного перехвата нарушитель только следит за сообщениями, передаваемыми по соединению, без вмешательства в их поток. Наблюдение нарушителя за данными (прикладного уровня) в сообщении позволяет раскрыть содержание сообщений. Нарушитель может также следить за заголовками сообщений, даже если данные непонятны ему, с целью определения места размещения и идентификаторов процессов, участвующих в передаче данных. Нарушитель может определить длины сообщений и частоту их передачи для определения характера передаваемых данных, т.е. провести анализ потока сообщений.

Нарушитель может также заниматься активным перехватом, выполняя множество действий над сообщениями, передаваемыми по соединению. Эти сообщения могут быть выборочно изменены, уничтожены, задержаны, переупорядочены, сдублированы и введены в соединение в более поздний момент

времени. Нарушитель может создавать поддельные сообщения и вводить их в соединение. Подобные действия можно определить как изменение потока и содержания сообщений.

Кроме того, нарушитель может сбрасывать все сообщения или задерживать их. Подобные действия можно классифицировать как прерывание передачи сообщений.

Попытки использования записи предыдущих последовательностей сообщений по инициированию соединений классифицируются как инициирование ложного соединения.

За последнее время в разных странах проведено большое количество исследовательских работ с целью обнаружения потенциальных каналов несанкционированного доступа к информации в вычислительных сетях. При этом рассматривались не только возможности нарушителя, получившего законный доступ к сетевому оборудованию, но и воздействия, обусловленные ошибками программного обеспечения или свойствами используемых сетевых протоколов [72]. Несмотря на то что изучение каналов несанкционированного доступа продолжается до сих пор, уже в начале 1980-х гг. были сформулированы 5 основных категорий угроз безопасности данных в вычислительных сетях [72]:

- 1) раскрытие содержания передаваемых сообщений;
- 2) анализ трафика, позволяющий определить принадлежность отправителя и получателя данных к одной из групп пользователей сети, связанных общей задачей;
- 3) изменение потока сообщений, что может привести к нарушению режима работы какого-либо объекта, управляемого из удаленной ЭВМ;
- 4) неправомерный отказ в предоставлении услуг;
- 5) несанкционированное установление соединения.

Данная классификация угроз не противоречит определению термина «безопасность информации» и делению потенциальных угроз на утечку, модификацию и утрату информации. Угрозы 1-ю и 2-ю можно отнести к утечке информации, угрозы 3-ю и 5-ю – к ее модификации, а угрозу 4-ю – к нарушению процесса обмена информацией, т.е. к ее потере для получателя. Согласно исследованиям [23] в вычислительных сетях нарушитель может применять следующие стратегии:

- 1) получить несанкционированный доступ к секретной информации;
- 2) выдать себя за другого пользователя, чтобы снять с себя ответственность или же использовать его полномочия с целью формирования ложной информации, изменения законной информации, применения ложного удостоверения личности, санкционирования ложных обменов информацией или же их подтверждения;
- 3) отказаться от факта формирования переданной информации;
- 4) утверждать, что информация получена от некоторого пользователя, хотя на самом деле она сформирована самим же нарушителем;
- 5) утверждать, что получателю в определенный момент времени была послана информация, которая на самом деле не посылалась (или посылалась в другой момент времени);

6) отказаться от факта получения информации, которая на самом деле была получена, или утверждать о другом времени ее получения;

7) незаконно расширить свои полномочия по доступу к информации и ее обработке и т.д.;

8) незаконно изменить полномочия других пользователей (расширить или ограничить, вывести или ввести других лиц);

9) скрыть факт наличия некоторой информации в другой информации (скрытая передача одной в содержании другой информации);

10) подключиться к линии связи между другими пользователями в качестве активного ретранслятора;

11) изучить, кто, когда и к какой информации получает доступ (даже если сама информация остается недоступной);

12) заявить о сомнительности протокола обеспечения информации из-за раскрытия некоторой информации, которая согласно условиям протокола должна оставаться секретной;

13) модифицировать программное обеспечение путем исключения или добавления новых функций;

14) преднамеренно изменить протокол обмена информацией с целью его нарушения или подрыва доверия к нему;

15) помешать обмену сообщениями между другими пользователями путем введения помех с целью нарушения аутентификации сообщений.

Анализ последних возможных стратегий нарушителя в вычислительных сетях говорит о том, насколько важно знать, кого считать нарушителем. При этом в качестве нарушителя рассматривается не только постороннее лицо, но и законный пользователь. По-видимому, эти задачи следует разбирать отдельно. С этих позиций приведенные выше 5 видов угроз характерны для поведения постороннего нарушителя. Тогда из числа последних угроз можно отнести к пяти упомянутым выше видам следующие: 1-ю, 10-ю, 11-ю, 15-ю.

Анализ остальных угроз свидетельствует о том, что задачу защиты можно условно разделить на задачи двух уровней: пользователей и элементов сети, с которыми работают пользователи сети. К уровню элемента сети можно отнести угрозы под номерами 2, 7, 8, 13 и 14. Уровень взаимоотношений пользователей называется уровнем доверия одного пользователя другому. Для обеспечения гарантий этого доверия, очевидно, потребуются специальные средства и критерии оценки их эффективности.

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

2

2.1. Краткий обзор современных методов защиты информации

Возвращаясь к истории вопроса, напомним, что при наличии простых средств хранения и передачи информации существовали и не утратили своего значения до настоящего времени следующие методы ее защиты от преднамеренного доступа:

- ограничение доступа;
- разграничение доступа;
- разделение доступа (привилегий);
- криптографическое преобразование информации;
- контроль, обнаружение и регистрация доступа;
- законодательные меры.

Указанные методы осуществлялись чисто организационно или с помощью технических средств.

С появлением автоматизированной обработки информации изменился и дополнился новыми видами физический носитель информации и усложнились технические средства ее обработки.

С усложнением обработки, увеличением количества технических средств, участвующих в ней, умножаются количество и виды случайных воздействий, а также возможные каналы несанкционированного доступа. С возрастанием объемов, сосредоточением информации, увеличением количества пользователей и другими указанными выше причинами увеличивается вероятность преднамеренного несанкционированного доступа к информации. В связи с этим развиваются старые и возникают новые дополнительные методы защиты информации в вычислительных системах:

- методы функционального контроля, обеспечивающие обнаружение и диагностику отказов, сбоев аппаратуры и ошибок человека, а также программные ошибки;
- методы повышения достоверности информации;
- методы защиты информации от аварийных ситуаций;
- методы контроля доступа к внутреннему монтажу аппаратуры, линиям связи и технологическим органам управления;
- методы разграничения и контроля доступа к информации;

- методы идентификации и аутентификации пользователей, технических средств, носителей информации и документов;
- методы защиты от побочного излучения и наводок информации.

Рассмотрим каждый из методов подробнее и оценим его возможности в плане дальнейшего использования при проектировании конкретных средств защиты информации в автоматизированных системах.

2.1.1. Ограничение доступа

Ограничение доступа заключается в создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом обработки и защиты по своим функциональным обязанностям.

Ограничение доступа к автоматизированной системе обработки информации заключается:

- в выделении специальной территории для размещения КСА;
- в сооружении по периметру зоны специальных ограждений с охранной сигнализацией;
- в сооружении специальных зданий или других построек;
- в выделении специальных помещений в здании;
- в создании контрольно-пропускного режима на территории, в зданиях и помещениях.

Задача средств ограничения доступа – исключить случайный и преднамеренный доступ посторонних лиц на территорию размещения КСА и непосредственно к аппаратуре. В указанных целях создается защитный контур, замыкаемый двумя видами преград: физической и контрольно-пропускной. Такие преграды часто называют системой охранной сигнализации и системой контроля доступа.

Традиционные средства контроля доступа в защищаемую зону: изготовление и выдача допущенным лицам специальных пропусков с фотографией владельца и сведений о нем. Данные пропуска могут храниться у владельца или непосредственно в пропускной кабине охраны. В последнем случае допущенное лицо называет фамилию и свой номер либо набирает его на специальной панели кабины при проходе через турникет; пропускное удостоверение выпадает из ячейки и поступает в руки работника охраны, который визуально сверяет личность владельца с изображением на фотографии, названную фамилию с фамилией на пропуске. Эффективность защиты данной системы выше первой. При этом исключается: потеря пропуска, его перехват и подделка. Кроме того, есть резерв в повышении эффективности защиты с помощью увеличения количества проверяемых параметров. Однако основная нагрузка по контролю при этом ложится на человека, а он, как известно, может ошибаться.

В зарубежной литературе имеются сообщения о применении биометрических методов аутентификации человека, когда в качестве идентификаторов используются отпечатки пальцев, ладони, голоса, личной подписи. Однако перечисленные методы пока не получили широкого распространения и вряд ли получат.

Совершенствование контрольно-пропускной системы в настоящее время ведется также в направлении улучшения конструкции пропуска-удостоверения личности путем записи кодовых значений паролей и других данных, размещаемых на носителе типа смарт-карты. Подробнее эти вопросы рассмотрены ниже.

Физическая преграда защитного контура, размещаемая по периметру охраняемой зоны, снабжается охранной сигнализацией.

В настоящее время ряд предприятий выпускает электронные системы для защиты государственных и частных объектов от проникновения посторонних лиц. Гарантировать эффективность системы охранной сигнализации можно только в том случае, если обеспечена надежность всех ее составных элементов и их согласованное функционирование. При этом имеют значение тип датчика, способ оповещения или контроля, помехоустойчивость, а также реакция на сигнал тревоги. Местная звуковая или световая сигнализация может оказаться недостаточной, поэтому данные устройства охраны целесообразно подключить к специализированным средствам централизованного управления, которые при получении сигнала тревоги высылают специальную группу быстрого реагирования.

Следить за состоянием датчиков может автоматическая система, расположенная в центре управления, или сотрудник охраны, который находится на объекте и при световом или звуковом сигнале принимает соответствующие меры. В первом случае местные охранные устройства подключаются к центру через телефонные линии, а специализированное цифровое устройство осуществляет периодический опрос состояния датчиков, автоматически набирая номер приемоответчика, расположенного на охраняемом объекте. При поступлении в центр сигнала тревоги автоматическая система включает сигнал оповещения.

Датчики сигналов устанавливаются на различного рода ограждениях, внутри помещений, непосредственно на сейфах и т.д.

При разработке комплексной системы охраны конкретного объекта с целью исключения возможности обхода создаваемой преграды учитывают его специфику: внутреннюю планировку здания, окон, входной двери, размещение наиболее важных технических средств.

Все эти факторы влияют на выбор типа датчиков, их положение и определяют ряд других особенностей данной системы. По принципу действия системы тревожной сигнализации можно классифицировать следующим образом:

- традиционные (обычные), основанные на использовании цепей сигнализации и индикации в комплексе с различными контактными датчиками;
- ультразвуковые;
- системы прерывания луча;
- телевизионные;
- радиолокационные;
- микроволновые;
- прочие.

2.1.2. Разграничение доступа

Автоматизированная система в зависимости от ее сложности и выполняемых задач может размещаться в одной, двух, трех и т.д. помещениях, этажах, зданиях. В силу различия функциональных обязанностей и работы с разными документами необходимо обеспечить разграничение доступа пользователей к их рабочим местам, аппаратуре и информации. Это обеспечивается размещением рабочих мест пользователей в отдельных помещениях, закрываемых разного рода замками на входных дверях с устанавливаемыми на них датчиками охранной сигнализации или применением специальной автоматической системы контроля доступа в помещения по жетонам или карточкам с индивидуальным кодом ее владельца, записанным в ее память.

2.1.3. Контроль доступа к аппаратуре

К сожалению, предоставить отдельное помещение каждому оператору-пользователю с его аппаратурой (рабочей станцией, АРМом) удастся редко. Кроме того, следует учитывать другую категорию специалистов, занятых техническим обслуживанием этой аппаратуры, сервисного оборудования и коммуникаций жизнеобеспечения людей в данном помещении. Данные специалисты не должны быть допущены к оперативной информации. Все это требует дополнительного разграничения доступа.

В целях контроля доступа к внутреннему монтажу технических средств, линиям связи и технологическим органам управления используется система контроля вскрытия аппаратуры. Это означает, что внутренний монтаж аппаратуры и технологические органы и пульты управления закрыты крышками, дверцами или кожухами, на которых установлены датчики. Датчики срабатывают при вскрытии аппаратуры и выдают электрические сигналы, которые по цепям сбора поступают на централизованное устройство контроля. Установка такой системы имеет смысл при наиболее полном перекрытии всех технологических подходов к аппаратуре, включая средства загрузки программного обеспечения, пульт управления ЭВМ и внешние кабельные соединители технических средств, входящие в состав вычислительной системы.

В идеальном случае для систем с повышенными требованиями к эффективности защиты информации целесообразно закрывать крышками под механический замок с датчиком или ставить под контроль включение также штатных средств входа в систему – терминалов пользователей.

Контроль вскрытия аппаратуры необходим не только в интересах защиты информации от НСД, но и для соблюдения технологической дисциплины в целях обеспечения нормального функционирования вычислительной системы, потому что часто при эксплуатации параллельно решению основных задач производится ремонт или профилактика аппаратуры, и может оказаться, что случайно забыли подключить кабель или с пульта ЭВМ изменили программу обработки информации. С позиций защиты информации от

несанкционированного доступа контроль вскрытия аппаратуры предохраняет от следующих действий:

- изменения и разрушения принципиальной схемы вычислительной системы и аппаратуры;
- подключения постороннего устройства;
- изменения алгоритма работы вычислительной системы путем использования технологических пультов и органов управления;
- загрузки посторонних программ и внесения программных «вирусов» в систему;
- использования терминалов посторонними лицами и т.д.

Основная задача систем контроля вскрытия аппаратуры – перекрытие на период эксплуатации всех нештатных и технологических подходов к аппаратуре. Если последние потребуются в процессе эксплуатации системы, выводимая на ремонт или профилактику перед началом работ оперативная информация на выводимом техническом средстве удаляется, аппаратура отключается от рабочего контура обмена информацией, подлежащей защите, и вводится в рабочий контур под наблюдением и контролем лиц, ответственных за безопасность информации.

Доступ к штатным входам в систему – терминалам проверяется с помощью контроля выдачи механических ключей пользователям. Доступ к информации – с помощью системы контроля и разграничения доступа, включающей применение кодов паролей, соответствующие функциональные задачи программного обеспечения и специального терминала службы безопасности информации, которые будут рассмотрены отдельно.

Указанные терминал и устройство контроля вскрытия аппаратуры входят в состав рабочего места службы безопасности информации, с которого осуществляются централизованный контроль доступа к аппаратуре и информации и управление ее защитой на данной автоматизированной системе.

2.1.4. Разграничение и контроль доступа к информации

Разграничение доступа в автоматизированной системе заключается в разделении информации, циркулирующей в ней, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями. Задача такого разграничения доступа к информации: сокращение количества должностных лиц, не имеющих к ней отношения при выполнении своих функций, т.е. защита информации от нарушителя среди законных пользователей.

Принимая во внимание, что доступ осуществляется с различных технических средств, начинать разграничение можно путем разграничения доступа к техническим средствам, разместив их в отдельных помещениях. Все подготовительные функции технического обслуживания аппаратуры, ее ремонта, профилактики, перезагрузки программного обеспечения и другие должны быть технически и организационно отделены от основных задач системы. Комплекс средств автоматизации и организация его обслуживания должны быть построены следующим образом:

• техническое обслуживание КСА в процессе эксплуатации должно выполняться специальным техническим персоналом без доступа к информации, подлежащей защите;

• перезагрузка программного обеспечения и его изменения должны производиться выделенным для этой цели проверенным специалистом;

• функции обеспечения безопасности информации должны выполняться специальным подразделением в организации-владельце КСА, вычислительной сети или АСУ;

• организация доступа пользователей к памяти КСА должна обеспечивать возможность разграничения доступа к информации, хранящейся в ней, с достаточной степенью детализации и в соответствии с заданными уровнями полномочий пользователей;

• регистрация и документирование технологической и оперативной информации должны быть разделены.

Разграничение доступа пользователей потребителя КСА может осуществляться также по следующим параметрам:

- виду, характеру, назначению, степени важности и секретности информации;
- способам ее обработки: считать, записать, внести изменения, выполнить команду;
- условному номеру терминала;
- времени обработки и др.

Принципиальная возможность разграничения по указанным параметрам должна быть обеспечена проектом КСА. А конкретное разграничение при эксплуатации КСА устанавливается потребителем и вводится в систему его подразделением, отвечающим за безопасность информации.

В указанных целях при проектировании вычислительных средств для построения КСА проводятся:

- разработка операционной системы с возможностью реализации разграничения доступа к информации, хранящейся в памяти ЭВМ, ПК, сервера;
- изоляция областей доступа;
- разделение базы данных на группы;
- процедуры контроля перечисленных функций.

При проектировании КСА и информационной системы АСУ (сети) на их базе производятся:

- разработка и реализация функциональных задач по разграничению и контролю доступа к аппаратуре и информации как в рамках данного КСА, так и АСУ (сети) в целом;
- разработка аппаратных средств идентификации и аутентификации пользователя;
- разработка программных средств контроля и управления разграничением доступа;
- разработка отдельной эксплуатационной документации на средства идентификации, аутентификации, разграничения и контроля доступа.

В качестве идентификаторов личности для реализации разграничения широко распространено применение кодов паролей, которые хранятся в памяти пользователя и КСА. В помощь пользователю в системах с повышенными требованиями большие значения кодов паролей записываются на специальные носители – электронные ключи, жетоны, смарт-карты и т.д.

2.1.5. Разделение привилегий на доступ к информации

Разделение привилегий на доступ к информации заключается в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы.

Задача указанного метода – существенно затруднить преднамеренный перехват информации нарушителем. Примером такого доступа может быть сейф с несколькими ключами, замок которого открывается только при наличии всех ключей. Аналогично в АС может быть предусмотрен механизм разделения привилегий при доступе к особо важным данным с помощью кодов паролей.

Данный метод несколько усложняет процедуру, но обладает высокой эффективностью защиты. На его принципах можно организовать доступ к данным с санкции вышестоящего лица по запросу или без него.

Сочетание двойного криптографического преобразования информации и метода разделения привилегий позволяет обеспечить высокоэффективную защиту информации от преднамеренного НСД.

Кроме того, при наличии дефицита в средствах, а также в целях постоянного контроля доступа к ценной информации со стороны администрации потребителя АСУ в некоторых случаях возможен вариант использования права на доступ к информации нижестоящего руководителя только при наличии его идентификатора и идентификатора его заместителя или представителя службы безопасности информации. При этом информация выдается на монитор только руководителю, а на монитор подчиненного – только информация о факте ее вызова.

2.2. Идентификация и установление подлинности объекта (субъекта)

2.2.1. Объект идентификации и установления подлинности

Идентификация – это присвоение какому-либо объекту или субъекту уникального образа, имени или числа. Установление подлинности (*аутентификация*) заключается в проверке, является ли проверяемый объект (субъект) в самом деле тем, за кого себя выдает [78].

Конечная цель идентификации и установления подлинности объекта в автоматизированной системе – допуск его к информации ограниченного пользования в случае положительного исхода проверки или отказ в допуске в случае отрицательного исхода проверки.

Объектами идентификации и установления подлинности в автоматизированной системе могут быть:

- человек (оператор, пользователь, должностное лицо);
- техническое средство (терминал, АРМ, РС, ЭВМ, КСА);
- документы (распечатки, листинги и др.);
- носители информации (магнитные ленты, диски и др.);
- информация на дисплее, табло и т.д.

Установление подлинности объекта может производиться человеком, аппаратным устройством, программой, вычислительной системой и т.д.

В вычислительных системах применение указанных методов в целях защиты информации при ее обмене предполагает конфиденциальность образов и имен объектов.

При обмене информацией между человеком и ЭВМ абонентам в сети рекомендуется предусмотреть взаимную проверку подлинности полномочий объекта или субъекта (а при удаленных связях – обязательно). В указанных целях необходимо, чтобы каждый из объектов (субъектов) хранил в своей памяти, не доступной для посторонних, список образов (имен) объектов (субъектов), с которыми производится обмен информацией, подлежащей защите.

2.2.2. Идентификация и установление подлинности личности

В повседневной жизни идентификатором личности является ее внешний вид: фигура, форма головы, черты лица, характер, привычки, поведение и другие, свойственные данному человеку признаки, которые создают образ данного человека и которые сознательно или подсознательно мы отмечаем в процессе общения с ним и храним в своей памяти. При появлении человека по этим признакам мы узнаем или не узнаем в нем своего знакомого. С течением времени те или иные признаки стираются из нашей памяти. У каждого человека эти признаки формируют различные образы одного и того же человека, в чем-то совпадающие или не совпадающие. Со временем меняется также сам человек – объект идентификации. Изложенные обстоятельства и технические трудности реализации средств идентификации указанных признаков в вычислительной технике заставляют искать другие пути решения задачи.

Известно, что отпечатки пальцев и очертания ладони, тембр голоса, личная подпись и другие элементы личности носят индивидуальный характер и сохраняются на протяжении всей жизни человека. В настоящее время в этом направлении ведутся поиски технических решений и достигнуты определенные успехи, но они пока носят рекламный характер и не получили широкого распространения. В разработанных для этой цели системах наблюдаются достаточно частые случаи отказа в санкционированном доступе и открытии доступа случайному пользователю. Не располагая подробными отчетами о проделанной работе, можно все же на уровне постановки задачи указать на предполагаемые причины этих неудач. Они кроются, как нам кажется, в недооценке задачи. Дело в том, что для выполнения процедуры установления подлинности необходимо совпадение образа, снимаемого с личности пользователя, с образом, хранящимся в памяти вычислительной системы, а для от-

каза в доступе система должна обладать способностью отличать похожие образы. Здесь возникают две задачи, которые необходимо решить одновременно. Для выполнения первой задачи (допуска) не требуется большого объема информации об образе (скажем даже, что чем меньше, тем лучше), а для выполнения второй (отказа) – информацию об образе необходимо увеличить на максимально возможную величину.

Пока возможности техники были ограничены и память систем распознавания хранила небольшой объем информации об образе, преобладали случаи допуска лица, не предусмотренного системой.

С развитием техники и увеличением объема информации об образе (с целью наиболее точной проверки личности и наибольшего количества ее параметров) возрастает вероятность изменений параметров личности во времени и несовпадения с параметрами образа, хранимого системой проверки, т.е. увеличивается вероятность отказа в доступе лицу, имеющему на это право.

Отправной точкой при разработке систем распознавания образов было естественное стремление повысить точность воспроизведения образа с целью отобрать автоматически из множества потенциальных образов единственный, хранящийся в памяти системы. Но при этом, по-видимому, не принималась во внимание величина этого множества, а она приближается к бесконечности (населению, жившему, живущему и рождающемуся на Земле). Какова должна быть точность воспроизведения образа? Какова должна быть разница между образом разрешенной к доступу личности и образом потенциального нарушителя? Какова вероятность появления нарушителя, образ которого приближается к образу, хранимому в памяти вычислительной системы? На эти вопросы ответов нет. Следовательно, работы по системам распознавания образов в целях широкого применения для защиты информации в вычислительных системах нецелесообразны. Не стоит также забывать о том, что стремление человека копировать природу не всегда приносило положительный результат. Достаточно вспомнить историю создания летательных аппаратов с машущими крыльями и близкий нам пример создания «мыслящей» ЭВМ.

Кроме того, системы идентификации и установления подлинности личности, основанные на антропометрических и физиологических данных человека, не отвечают самому важному требованию: конфиденциальности, так как записанные на физические носители данные хранятся постоянно и фактически являются ключом к информации, подлежащей защите, а постоянный ключ в конце концов становится доступным. Данный аргумент, по мнению автора, является решающим при ответе на вопрос о применении такого метода.

Типичным примером простой и распространенной системы аутентификации является система «ключ-замок», в которой владелец ключа является объектом установления подлинности. Но ключ можно потерять, похитить или снять с него копию, так как идентификатор личности физически от нее отделен. Система «ключ-замок» имеет локальное применение. Однако в сочетании с другими системами аутентификации и в условиях пониженных требований применяется до сих пор. В электромеханическом замке вместо ключа может использоваться код.

Одним из распространенных методов аутентификации является присвоение лицу или другому объекту уникального имени или числа – пароля и хранение его значения в вычислительной системе. При входе в вычислительную систе-

му пользователь вводит через терминал свой код пароля, вычислительная система сравнивает его значение со значением, хранящимся в своей памяти, и при совпадении кодов открывает доступ к разрешенной функциональной задаче, а при несовпадении – отказывает в нем.

Наиболее высокий уровень безопасности входа в систему достигается разделением кода пароля на две части: одну, запоминаемую пользователем и вводимую вручную, и вторую, размещаемую на специальном носителе – карточке, устанавливаемой пользователем на специальное считывающее устройство терминала. В этом случае идентификатор связан с личностью пользователя, размер пароля может быть легко запоминаемым и при хищении карточки у пользователя будет время для замены кода пароля и получения новой карточки.

На случай защиты запоминаемой части пароля от получения ее нарушителем путем физического принуждения пользователя, возможно, будет полезно в вычислительной системе предусмотреть механизм тревожной сигнализации, основанной на применении ложного пароля. Ложный пароль запоминается пользователем одновременно с действительным и сообщается преступнику в вышеупомянутой ситуации.

Однако, учитывая опасность, которой подвергается жизнь пользователя, необходимо в вычислительной системе одновременно со скрытой сигнализацией предусмотреть механизм обязательного выполнения требований преступника, воспользовавшегося средствами аутентификации законного пользователя.

Кроме указанных методов паролей в вычислительных системах в качестве средств аутентификации применяют методы «запрос-ответ» и «рукопожатия».

В методе «запрос-ответ» набор ответов на «*m*» стандартных и «*n*» ориентированных на пользователя вопросов хранится в ЭВМ и управляется операционной системой. Когда пользователь делает попытку включиться в работу, операционная система случайным образом выбирает и задает ему некоторые (или все) из этих вопросов. Правильные ответы пользователя на указанные вопросы открывают доступ к системе.

Для исключения некоторых недостатков описанных выше методов операционная система может потребовать, чтобы пользователь доказал свою подлинность с помощью корректной обработки алгоритмов. Эту часть называют процедурой в режиме «рукопожатия», она может быть выполнена как между двумя ЭВМ, так и между пользователем и ЭВМ.

Методы «запрос-ответ» и «рукопожатия» в некоторых случаях обеспечивают большую степень безопасности, но вместе с тем являются более сложными и требующими дополнительных затрат времени. Как обычно, здесь нужно найти компромисс между требуемой степенью безопасности и простотой применения. При сложном применении пользователь будет искать путь упрощения процедуры и в итоге найдет его, но за счет снижения эффективности средства защиты.

Следует, однако, при этом учитывать расстояние между субъектами (объектами) аутентификации. При удаленной аутентификации возможен перехват значений пароля нарушителем. На этот случай существуют специальные алгоритмы аутентификации с применением одноразовых паролей и криптографических преобразований с помощью шифрования, цифровой подписи

и необратимой функции. В этом алгоритме может принимать участие и информация, передаваемая вместе с аутентификационными данными во время сеанса связи.

Подробнее эти вопросы будут рассмотрены в разд. 5 данной книги.

2.2.3. Идентификация и установление подлинности документов

В вычислительных системах в качестве документов, являющихся продуктом информационной системы и содержащих секретную информацию, могут быть распечатки с печатающих устройств, магнитные ленты, диски и другие долговременные постоянные запоминающие устройства в виде физических носителей.

Здесь подлинность документа необходимо рассматривать с двух позиций:

- получения документа, сформированного непосредственно данной вычислительной системой и на аппаратуре ее документирования;
- получения готового документа с удаленных объектов вычислительной сети или АСУ.

В первом случае подлинность документа гарантируется автоматизированной системой, имеющей средства защиты информации от НСД, а также физическими характеристиками печатающих устройств, присущими только данному устройству. Однако в особых случаях этого может оказаться недостаточно. Применение криптографического преобразования информации является более эффективным средством. Информация, закрытая шифрованием с кодом ключа, известным лишь передающему ее лицу и получателю, не вызывает сомнения в ее подлинности. Если код пароля, применяемый в данном случае, используется только передающим лицом и вводится им лично, можно утверждать, что ключ является его личной подписью.

Криптографическое преобразование информации для идентификации и установления подлинности документа во втором случае, когда документ транспортировался по неохраняемой территории с территориально удаленного объекта или продолжительное время находился на хранении, также является наиболее эффективным средством. Однако при отсутствии необходимого для этой цели оборудования невысокие требования к защите информации иногда позволяют использовать более простые средства идентификации и установления подлинности документов: опечатывание и опломбирование носителей документов с обеспечением их охраны. При этом к носителю должны прилагаться сопроводительные документы с подписями ответственных должностных лиц, заверенными соответствующими печатями.

При неавтоматизированном обмене информацией подлинность документа удостоверяется личной подписью руки человека, автора (авторов) документа. Проверка подлинности документа в этом случае обычно заключается в визуальной проверке совпадения изображения подписи на документе с образцом подлинника. Подпись располагается на одном листе вместе с текстом или частью текста документа, подтверждая тем самым подлинность текста. В особых случаях в криминалистической экспертизе проверяются и другие параметры подлинности документа.

При автоматизированной передаче документов по каналам связи, расположенным на неконтролируемой территории, меняются условия передачи документов. В этих условиях, даже если сделать аппаратуру, воспринимающую и передающую изображение подписи автора документа, его получатель получит не подлинник, а всего лишь копию подписи, которая в процессе передачи может быть подвергнута повторному копированию для использования при передаче ложного документа. Поэтому при передаче документов по каналам связи в вычислительной сети применяется криптографическое преобразование информации по специальному алгоритму цифровой подписи. Передаваемый документ может быть в открытом или зашифрованном виде. В последнем варианте дополнительно используется шифрование информации.

Область применения цифровой подписи чрезвычайно широка: от проведения финансовых и банковских операций до контроля за выполнением международных договоров и охраны авторских прав. Исследования специалистов по проблеме цифровой подписи изложены в [19, 65] и других источниках. При этом отмечается, что участники обмена документами нуждаются в защите от следующих преднамеренных несанкционированных действий:

- отказа отправителя от переданного сообщения;
- фальсификации (подделки) получателем полученного сообщения;
- изменения получателем полученного сообщения;
- маскировки отправителя под другого абонента.

Обеспечение защиты каждой стороны, участвующей в обмене, осуществляется с помощью введения специальных протоколов. Для верификации сообщения протокол должен содержать следующие обязательные положения:

- отправитель вносит в передаваемое сообщение свою цифровую подпись, представляющую собой дополнительную информацию, зависящую от передаваемых данных, имени получателя сообщения и некоторой закрытой информации, которой обладает только отправитель;
- получатель сообщения должен иметь возможность удостовериться, что полученная в составе сообщения подпись есть правильная подпись отправителя;
- получение правильной подписи отправителя возможно лишь при использовании закрытой информации, которой обладает только отправитель;
- для исключения возможности повторного использования устаревших сообщений последние должны быть привязаны ко времени.

Подпись сообщения представляет собой способ шифрования сообщения с помощью криптографического преобразования. Закрываемым элементом в преобразовании является код ключа. Если ключ подписи принадлежит конечному множеству ключей, если это множество достаточно велико, а ключ подписи определен методом случайного выбора, то полная проверка ключей подписи для пар сообщение-получатель эквивалентна поиску ключа. Практически подпись является паролем, зависящим от отправителя, получателя и содержания передаваемого сообщения. Для предупреждения повторного использования подпись должна меняться от сообщения к сообщению. Получатель сообщения, несмотря на неспособность составить правильную подпись отправителя, тем не менее должен иметь возможность удостовериться для себя ее правильность или неправильность [19, 65]. Поскольку вопрос обеспечения подлинности передаваемых документов и сообщений

более актуален для территориально рассредоточенных АС и тесно связан с принципами построения в них системы защиты информации, его решение рассмотрено в разд. 5 данной книги.

2.2.4. Идентификация и установление подлинности информации на средствах ее отображения и печати

В автоматизированных системах с централизованной обработкой информации и относительно невысокими требованиями к защите установление ее подлинности на технических средствах отображения и печати гарантируется наличием системы защиты информации. Однако с усложнением автоматизированных систем вероятность возникновения несанкционированного доступа к информации и ее модификации существенно увеличивается. Поэтому в ответственных случаях отдельные сообщения или блоки информации подвергаются специальной защите, которая заключается в применении средств повышения достоверности или криптографического преобразования информации. Установление подлинности полученной информации, включая отображение на табло и терминалах, заключается в контроле положительных результатов обеспечения достоверности информации и результатов дешифрования полученной информации до отображения ее на экране и печати. Подлинность информации на средствах ее отображения тесно связана с подлинностью документов. Поэтому все положения, приведенные в подразд. 2.2.3, справедливы и для обеспечения подлинности ее отображения.

Достоверность информации на средствах отображения и печати в случае применения указанных средств защиты зависит от надежности функционирования средств, доставляющих информацию на поле отображения после окончания процедур проверки ее достоверности. Чем ближе к полю отображения (бумажному носителю) эта процедура, тем достовернее отображаемая информация.

2.3. Криптографическое преобразование информации

2.3.1. Основные принципы и классификация методов криптографического преобразования информации

Защита информации методом криптографического преобразования заключается в преобразовании ее составных частей (слов, букв, слогов, цифр) с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении ее к неясному виду. Для ознакомления с шифрованной

информацией применяется обратный процесс: декодирование (дешифрование). Использование криптографии является одним из распространенных методов, значительно повышающих безопасность передачи данных в сетях ЭВМ, данных, хранящихся в удаленных устройствах памяти, и при обмене информацией между удаленными объектами. Современный взгляд на эту проблему представлен подробно в [3, 65, 26].

Для преобразования (шифрования) обычно используется некоторый алгоритм или устройство, реализующие заданный алгоритм, которые могут быть известны широкому кругу лиц. Управление процессом шифрования осуществляется с помощью периодически меняющегося кода ключа, обеспечивающего каждый раз оригинальное представление информации при использовании одного и того же алгоритма или устройства. Знание ключа позволяет просто и надежно расшифровать текст. Однако без знания ключа эта процедура может быть практически невыполнима даже при известном алгоритме шифрования.

Даже простое преобразование информации является весьма эффективным средством, дающим возможность скрыть ее смысл от большинства неквалифицированных нарушителей. Структурная схема шифрования информации представлена на рис. 2.1.



Рис. 2.1. Схема шифрования информации

Коды и шифры использовались в течение многих веков задолго до появления ЭВМ. Между кодированием и шифрованием не существует ощутимой разницы. Заметим только, что в последнее время на практике слово «кодирование» употребляют, когда речь идет о цифровом представлении информации при ее обработке на технических средствах, а «шифрование» относится к преобразованию информации в целях защиты от НСД. В настоящее время некоторые методы шифрования хорошо проработаны и являются классическими. Классификация криптографических методов преобразования информации приведена на рис. 2.2 [15].

Для построения средств защиты информации от НСД необходимо иметь представление о некоторых традиционных методах шифрования: подстановки, перестановки, гаммирования, аналитических, комбинированных и др.

Зарубежными специалистами сформирована следующая система требований к алгоритму шифрования [16]:

- зашифрованный текст должен поддаваться чтению только при наличии ключа шифрования;
- число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного текста и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;

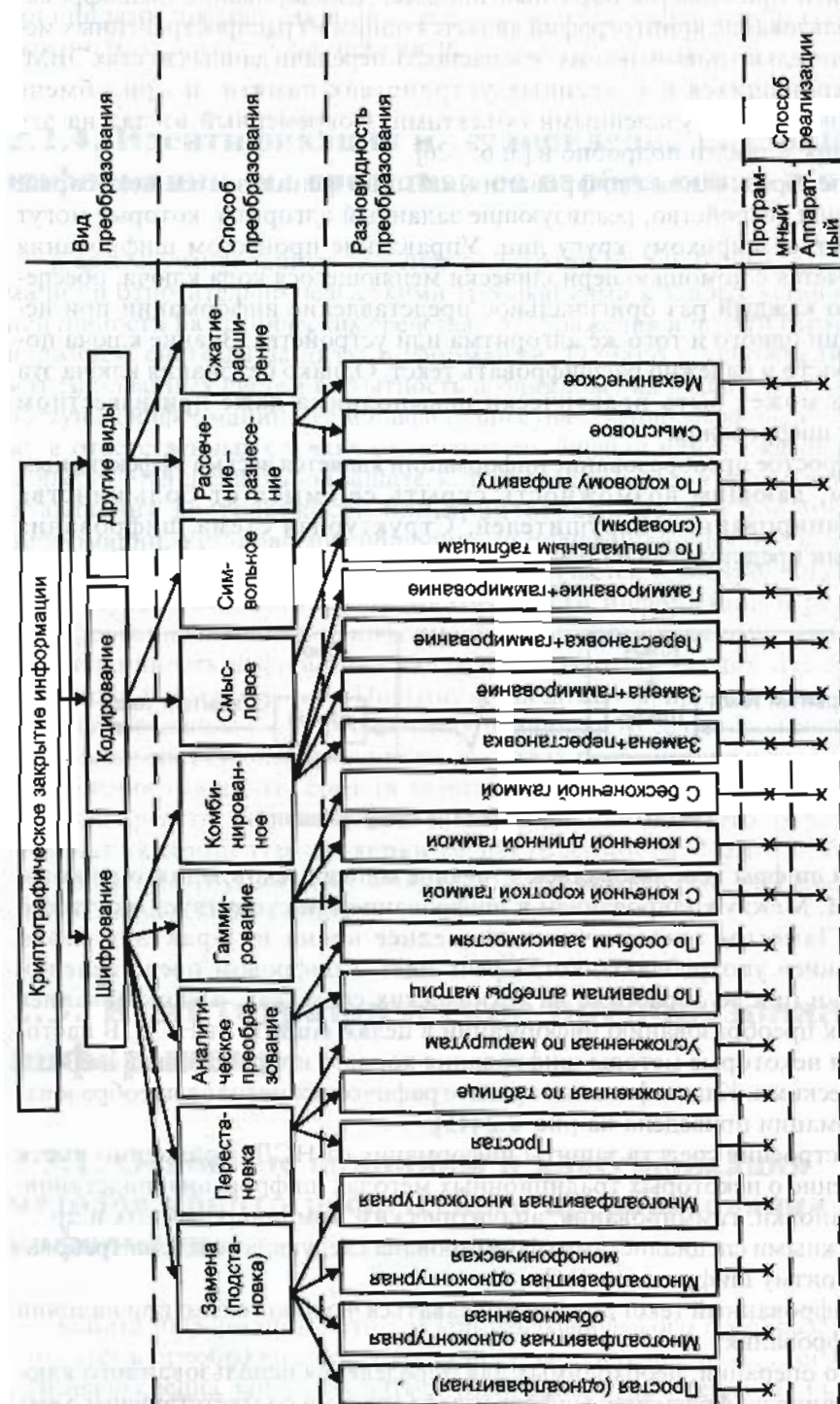


Рис. 2.2. Классификация криптографических методов преобразования информации

- знание алгоритма шифрования не должно влиять на надежность защиты;
- незначительные изменения ключа шифрования должны приводить к существенному изменению вида зашифрованного текста;
- незначительные изменения шифруемого текста должны приводить к существенному изменению вида зашифрованного текста даже при использовании одного и того же ключа;
- структурные элементы алгоритма шифрования должны быть неизменными;
- в процессе шифрования должен осуществляться постоянный контроль за шифруемыми данными и ключом шифрования;
- дополнительные биты, вводимые в текст в процессе шифрования, должны быть полностью и надежно скрыты в шифрованном тексте;
- длина шифрованного текста должна быть равной длине исходного открытого текста;
- не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемых в процессе шифрования;
- любой ключ из множества возможных должен обеспечивать надежную защиту информации;
- алгоритм должен допускать как программную, так и аппаратную реализацию; при этом изменение длины ключа не должно вести к ухудшению характеристик алгоритма.

Современные методы защитных преобразований можно классифицировать на группы: перестановка, замена (подстановки), аддитивные, аналитические и комбинированные методы.

Методы перестановки и подстановки обычно характеризуются короткой длиной ключа, а их надежность защиты определяется сложностью алгоритмов преобразования.

Для аддитивных методов характерны простые алгоритмы преобразования, а их надежность основана на увеличении длины ключа.

Все перечисленные методы относятся к так называемому симметричному шифрованию: один и тот же ключ используется для шифрования и дешифрования.

В последнее время появились методы несимметричного шифрования: один ключ для шифрования (открытый), второй – для дешифрования (закрытый).

2.3.2. Краткий обзор методов шифрования

Суть методов перестановки состоит в том, что входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов [78].

Перестановки в классической криптографии обычно получают в результате записи исходного текста и чтения шифрованного текста по разным путям геометрической фигуры.

Простейшим примером перестановки является запись исходного текста по строкам некоторой матрицы и чтение его по столбцам этой матрицы. Пос-

последовательность заполнения строк и чтение столбцов может быть любой и задается ключом. Таким образом, для матрицы размерностью 8×8 (длина блока 64 символа) возможно $1,6 \times 10^9$ ключей, что позволяет на современных ЭВМ путем перебора расшифровать заданный текст. Однако для матрицы размерностью 16×16 (длина блока 256 символов) имеется $1,4 \times 10^{26}$ ключей, и перебор их с помощью современных средств весьма затруднителен.

Примером применения метода перестановки может быть также восьми-элементная схема (рис. 2.3), обладающая совокупностью маршрутов, носящих название маршрутов Гамильтона.

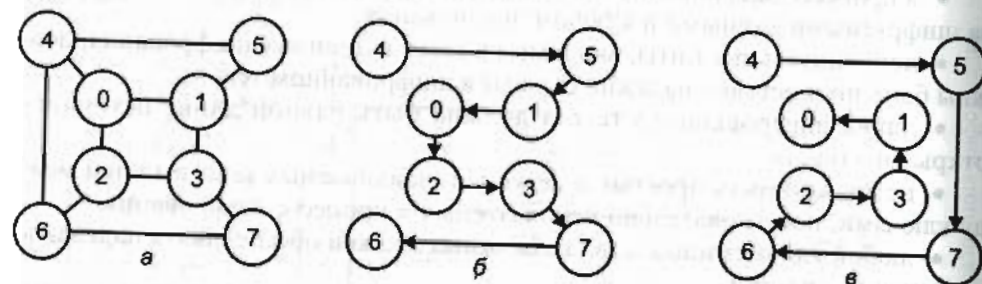


Рис. 2.3. Вариант схемы маршрутов:
а – общий вид; б – маршрут 1; в – маршрут 2

Последовательность заполнения схемы каждый раз соответствует нумерации ее элементов. Если длина шифруемого текста не кратна числу элементов, то при последнем заполнении в свободные элементы заносится произвольный символ. Выборка из таблицы для каждого заполнения может выполняться по своему маршруту, при этом маршруты могут использоваться как последовательно, так и в порядке, задаваемом ключом.

Для методов перестановки характерны простота алгоритма, возможность программной реализации и низкий уровень защиты, так как при большой длине исходного текста в зашифрованном тексте проявляются статистические закономерности ключа, что и позволяет его быстро раскрыть. Другой недостаток этих методов – легкое раскрытие, если удастся направить в систему для шифрования несколько специально подобранных сообщений. Так, если длина блока в исходном тексте равна K символам, то для раскрытия ключа достаточно пропустить через шифровальную систему $K-1$ блоков исходного текста, в которых все символы, кроме одного, одинаковы.

Существуют и другие способы перестановки, которые можно реализовать программным и аппаратным путем. Например, реализованный аппаратным путем блок перестановки для преобразования информации использует электрические цепи, по которым она передается параллельным способом. Преобразование текста заключается в «перепутывании» порядка разрядов в цифровой кодограмме путем изменения электрического монтажа схемы в блоке. Для дешифрации на приемном пункте устанавливается другой блок, восстанавливающий порядок цепей.

Методы шифрования заменой (подстановкой) заключаются в том, что символы исходного текста (блока), записанные в одном алфавите, заменяют-

ся символами другого алфавита в соответствии с принятым ключом преобразования [78].

Одним из простейших методов является прямая замена исходных символов их эквивалентом из вектора замен. Для очередного символа исходного текста отыскивается его местоположение в исходном алфавите. Эквивалент из вектора замены выбирается как отстоящий на полученное смещение от начала алфавита. При дешифровании поиск производится в векторе замен, а эквивалент выбирается из исходного алфавита. Полученный таким способом текст имеет сравнительно низкий уровень защиты, так как исходный и зашифрованный тексты имеют одинаковые статистические характеристики.

Более стойкой к раскрытию является схема шифрования, основанная на использовании таблицы Вижинера (рис. 2.4). Таблица представляет собой квадратную матрицу с числом элементов K , где K – количество символов в алфавите. В первой строке матрицы записываются буквы в порядке очередности их в алфавите, во второй – та же последовательность букв, но со сдвигом влево на одну позицию, в третьей – со сдвигом на две позиции и т.д. Освободившиеся места справа заполняются вытесненными влево буквами, записываемыми в порядке очередности.

АБВГДЕ.....	ЭЮЯ
БВГДЕЖ.....	ЮЯА
ВГДЕЖЗ.....	ЯАБ
ГДЕЖЗИ.....	АБВ
ДЕЖЗИК.....	БВГ
.....	
.....	
ЯАБВГД.....	БЭЮ

Рис. 2.4. Таблица шифрования

Для шифрования текста устанавливается ключ, представляющий собой некоторое слово или набор букв. Далее из полной матрицы выбирается подматрица шифрования, включающая, например, первую строку и строку матрицы, начальной буквой которой являются последовательно буквы ключа (рис. 2.5), например МОРЕ.

ШИФРУЕМЫЙ ТЕКСТ	ЗАЩИТА ИНФОРМАЦИИ
КЛЮЧ	МОРЕ МОРЕ МОРЕ МОРЕ
ТЕКСТ ПОСЛЕ ЗАМЕНЫ	У О И О З О Ш Т Я Я Я С М Г Ш О
ЗАШИФРОВАННЫЙ ТЕКСТ	У О И О З О Ш Т Я Я Я С М Г Ш О

Рис. 2.5. Механизм шифрования заменой

Процесс шифрования включает следующую последовательность действий (рис. 2.6):

АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ
 МНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛ
 ОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛМН
 РСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛМНОП
 ЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГД

Рис. 2.6. Ключ шифрования

- под каждой буквой шифруемого текста записываются буквы ключа, повторяющие ключ требуемое число раз;
- шифруемый текст по подматрице заменяется буквами, расположенными на пересечениях линий, соединяющих буквы текста первой строки подматрицы и буквы ключа, находящейся под ней.

Так, под первой буквой шифруемого текста «З» оказалась буква «М» ключа. В первой строке подматрицы находим букву «З» и выбираем из данной колонки подматрицы букву в той строке, которая соответствует букве «М» ключа. Такой буквой оказалась буква «У».

Далее выполняется замена исходной буквы «З» на «У» в выходном тексте. Выходной текст делится на группы, например, по четыре знака.

Для этого алгоритма может быть составлена программа ЭВМ.

Раскрыть текст, полученный по данному алгоритму, только на основе статистических характеристик языка невозможно, так как одни и те же символы открытого текста могут быть заменены различными символами шифрованного текста. С другой стороны, различные буквы открытого текста могут быть заменены одинаковыми знаками шифрованного текста.

Для дешифрования необходимо знать ключ, который может быть введен пользователем со своего терминала или хранится в памяти ЭВМ в зашифрованном виде. Для шифрования ключа можно использовать другую систему шифрования.

Дешифрование текста выполняется в следующей последовательности (рис. 2.7):

КЛЮЧ	МОРЕ МОРЕ МОРЕ МОРЕ
ЗАШИФРОВАННЫЙ ТЕКСТ	УОЮО ЭОШТ ЯЫАС МГШО
РАСШИФРОВАННЫЙ ТЕКСТ	ЗАШИ ТАИН ФОРМ АЦИИ
ИСХОДНЫЙ ТЕКСТ	ЗАЩИТА ИНФОРМАЦИИ

Рис. 2.7. Механизм дешифрования

Над буквами шифрованного текста сверху последовательно записываются буквы ключа.

В строке подматрицы таблицы Вижинера для каждой буквы ключа отыскивается буква, соответствующая знаку шифрованного текста. Находящаяся над ней буква первой строки и будет знаком расшифрованного текста.

Полученный текст группируется в слова по смыслу.

Один из недостатков шифрования по таблице Вижинера – это низкая стойкость при небольшой длине ключа и сложность формирования длинных ключей. Поскольку в ключе не допускается повторение букв (в противном случае шифрование будет неоднозначным), а сам ключ должен легко запоминаться; последовательность букв, не имеющих определенного смысла, запомнить трудно.

С целью повышения надежности шифрования текста предлагается [78] усовершенствованный вариант таблицы Вижинера, который заключается в следующем:

- во всех (кроме первой) строках таблицы буквы алфавита располагаются в произвольном порядке;
- выбирается десять (не считая первой) строк, пронумерованных натуральными числами от 0 до 9;
- в качестве ключа используются величины, выраженные бесконечным рядом чисел (например, основание натуральных логарифмов $e = 2,7182818285...$, число $\eta = 3,14159...$).

Шифрование и дешифрование осуществляются в той же последовательности, что и в случае простой таблицы Вижинера.

Частным случаем метода замены, обеспечивающим надежное шифрование информации, является использование алгебры матриц (например, правила умножения матрицы на вектор). Это правило, как известно, заключается в следующем:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} a_{11}b_1 + a_{12}b_2 + a_{13}b_3 \\ a_{21}b_1 + a_{22}b_2 + a_{23}b_3 \\ a_{31}b_1 + a_{32}b_2 + a_{33}b_3 \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix}$$

В соответствии с этим правилом матрицу можно использовать в качестве основы для шифрования, знаками вектора b_i могут быть символы шифруемого текста, а знаками вектора результата c_i – символы зашифрованного текста.

Для шифрования буквенных сообщений необходимо прежде всего заменить знаки алфавита их цифровыми эквивалентами, которыми могут быть порядковые номера буквы в алфавите.

Для дешифрования используются те же правила умножения матрицы на вектор, только в качестве основы берется обратная матрица, а в качестве умножаемого вектора – соответствующее количество чисел шифрованного текста. Цифрами вектора-результата будут цифровые эквиваленты знаков исходного текста.

Нетрудно видеть, что процедуры шифрования и дешифрования строго формализованы, что позволяет сравнительно легко запрограммировать их для автоматической реализации в ЭВМ. Причем важно, что шифрование и дешифрование осуществляются по одной и той же процедуре умножения матрицы на вектор, т.е. для них может использоваться одна и та же программа. Недостатком же является то, что для шифрования и дешифрования каждой буквы требуется выполнить несколько арифметических действий, что увеличивает время обработки информации.

Существуют и другие методы подстановки. Приведенные выше методы подстановки относятся к моноалфавитным подстановкам, которые можно представить как числовые преобразования букв исходного текста, рассматриваемых как числа. Каждая буква в тексте умножается на некоторое число (называемое десятичным коэффициентом) и прибавляется к некоторому другому числу (коэффициенту сдвига)

$$C = (aP + \delta) \bmod A,$$

где a – десятичный коэффициент;
 δ – коэффициент сдвига.

Получающееся число уменьшается по правилу вычитания модуля A , где A – размер алфавита, и зашифрованный текст формируется из соответствующих ему алфавитных эквивалентов [78].

В целях маскировки естественной частотной статистики исходного языка применяется многоалфавитная подстановка, которая также бывает нескольких видов.

Аддитивные методы [80]. В качестве ключа в аддитивных методах используется некоторая последовательность букв того же алфавита и такой же длины, что и в исходном тексте. Шифрование выполняется путем сложения символов исходного текста и ключа по модулю, равному числу букв в алфавите (так, если используется двоичный алфавит, то производится сложение по модулю 2).

Разновидностью аддитивного метода является **гаммирование** – наложение на исходный текст некоторой последовательности кодов, называемых гаммой. Процесс наложения осуществляется следующим образом:

- символы исходного текста и гамма представляются в двоичном коде и располагаются один под другим;
- каждая пара двоичных знаков заменяется одним двоичным знаком шифрованного текста в соответствии с принятым алгоритмом;
- полученная последовательность двоичных знаков шифрованного текста заменяется символами алфавита в соответствии с выбранным кодом.

Если ключ шифрования выбирается случайным образом, например формируется с помощью датчика псевдослучайных чисел, то раскрыть информацию, не зная ключа, практически невозможно.

Однако на практике длина ключа ограничена возможностями вычислительной техники и аппаратуры обмена данными, а именно выделяемыми объемами памяти, временем обработки сообщения, а также возможностями аппаратуры подготовки и записи кодов ключей.

Эффективным методом шифрования является **комбинированный**. Комбинация основных методов шифрования – перестановки и подстановки – дает в результате сложное преобразование, называемое производным шифром. Этот шифр обладает большими криптографическими возможностями по сравнению с отдельной перестановкой и подстановкой. Он используется в федеральном стандарте NBS США, называемом также стандартом DES, и отечественном – ГОСТ 28147-89, введенном в действие с июля 1990 г.

Стандарт DES построен на комбинированном использовании перестановки, замены и гаммирования, причем каждый блок шифруемых данных длиной 32 бита последовательно подвергается 15-кратному преобразованию, а в качестве ключа, который служит для генерирования последовательности знаков случайной гаммы, используется последовательность в 56 бит. Такой ключ дает 10^{16} различных комбинаций гаммы. Однако по последним сообщениям¹, данный алгоритм шифрования 17 июня 1997 г. за 140 дней был «взломан» по причине малой длины ключа шифрования. Для стойкости шифртекста при использовании алгоритма DES текст шифруется 3 раза с разными ключами, т.е. длина ключа возрастает до 168 бит (56×3). В настоящее время за рубежом популярен алгоритм PGP и другие алгоритмы.

¹ См.: Семьянов П. Почему криптосистемы ненадежны / www.cd.boom.com.

В России действует стандарт шифрования ГОСТ 28147-89, обязательный для использования государственными организациями, предприятиями и учреждениями при защите информации. Его алгоритм предусматривает работу с 256-битовым ключом и может быть реализован аппаратным и программным путями. Алгоритм производит:

- шифрование данных в режиме простой замены;
- шифрование данных в режиме гаммирования;
- шифрование данных в режиме гаммирования с обратной связью;
- выработку имитовставки.

Имитовставка – это блок данных, который вырабатывается в результате обработки открытых данных по определенному алгоритму с использованием ключа и затем добавляется к зашифрованным данным для обеспечения их защиты от навязывания ложной информации.

Последним достижением криптографии стала **система шифрования с открытым ключом**.

В криптографии с открытым ключом предусмотрены два ключа, каждый из которых невозможно вычислить из другого. Один ключ (открытый) используется отправителем для шифрования информации, другой (закрытый) – служит для расшифрования получателем полученного шифртекста.

Криптографические системы с открытым ключом используют необратимые или односторонние функции, которые обладают следующими свойствами: при заданном значении X относительно просто вычислить значение $f(X)$, однако если $Y = f(X)$, то нет простого пути для вычисления значения X . Другими словами, чрезвычайно трудно рассчитать значение обратной функции $f^{-1}(Y)$.

Исследование необратимых функций проводилось в основном по трем направлениям: 1) дискретное возведение в степень; 2) умножение простых чисел; 3) комбинаторные задачи, в частности задача об укладке ранца.

Диффи и Хеллман исследовали функцию дискретного возведения в степень, в результате чего получили новый алгоритм криптографического закрытия информации, позволяющий применять два ключа: открытый для шифрования, закрытый для расшифрования информации. Система открытого ключа позволила решить проблему рассылки ключей пользователям при одновременном выполнении требований по стойкости защиты [6].

Р. Л. Ривестом, А. Шамиром и Л. Адельманом предложен метод с ключом общего пользования для более высокой степени защиты, основанный на применении необратимой функции с потайным ходом, которая определяется как семейство обратимых функций [6].

Криптография с открытым ключом наиболее эффективна при шифровании передаваемых данных, а не данных, хранящихся в ЗУ. Кроме того, она прекрасно подходит для замены обычной подписи электронной, так называемой **цифровой подписью**, применяемой в системах электронных платежей и при передаче сообщений с помощью устройств телесвязи.

Несмотря на все преимущества криптосистем с открытым ключом и схем вероятностного шифрования, ни одна из них до настоящего времени не может конкурировать по **быстродействию** с такими криптосистемами с секретным ключом, как, например, DES. Когда необходимо передавать большое количество информации, то может случиться, что применение RSA будет се-

решительно замедлять работу, тогда как использование DES по каким-то причинам либо окажется невозможным (например, из-за отсутствия совместного секретного ключа), либо перестанет отвечать необходимым требованиям секретности.

В такой ситуации очень полезным может быть использование гибридной криптосистемы, в которой один раз перед началом каждого сеанса передачи шифрованных сообщений с помощью криптосистемы с открытым ключом формируется небольшая (совместная и секретная для других) часть информации, а затем в последующей передаче используется в качестве ключа к шифратору (и дешифратору) для тех текущих сообщений открытого текста, которые будут зашифровываться (и расшифровываться) при помощи криптосистемы с секретным ключом.

Если передаваемое сообщение является достаточно длинным, то лучше всего в течение каждой передачи использовать криптосистему с открытым ключом по нескольку раз, с тем чтобы секретные ключи можно было почаще менять. Не вызывая особого замедления протокола, это значительно повысит стойкость гибридной системы по двум причинам: во-первых, при атаке на основе только шифртекста, являющейся единственным типом атаки, которая имеет смысл в данной ситуации, криптосистему с секретным ключом легче раскрыть, если доступен большой шифртекст, и, во-вторых, даже если криптоаналитику и удастся определить какой-нибудь один из секретных ключей, то он сможет расшифровать лишь соответствующую ему часть сообщения.

В числе последних достижений криптографии следует также назвать вероятностное (Ш. Гольдвассер и С. Микэли) и квантовое (С. Уиснер) шифрование [7].

Основное техническое различие между вероятностным шифрованием и системами с открытым ключом состоит в том, что естественные алгоритмы шифрования являются при этом вероятностными, а не детерминированными: одно и то же сообщение открытого текста может привести к возникновению большого числа различных шифртекстов. В результате криптоаналитик, имеющий, по его предположению, истинный открытый текст, не сможет долго проверять свою догадку посредством шифрования этого открытого текста (с помощью естественного алгоритма его законного получателя) и последующего сравнения полученного результата с перехваченным шифртекстом.

Формально система вероятностного шифрования состоит из пространства ключей K и для каждого $k \in K$, из пространства открытых текстов M_k сообщений, пространства шифртекстов C_k , вероятностного пространства R_k и пары функций $E_k: M_k \cdot R_k \rightarrow C_k$ и $D_k: C_k \rightarrow M_k$, таких, что $D_k(E_k(m, r)) = m$ для любого сообщения открытого текста $m \in M_k$ и случайного числа $r \in R_k$. С помощью любого $k \in K$ должны легко получаться эффективные естественные алгоритмы для вычисления как E_k , так и D_k , но построение какого-либо эффективного алгоритма вычисления D_k на основе только естественных алгоритмов вычисления E_k должно быть практически невозможно.

Использование системы вероятностного шифрования очень похоже на использование систем с открытым ключом. Каждый пользователь раз и навсегда выбирает для себя ключ $k \in K$, который используется для получения обоих естественных алгоритмов вычисления E_k и D_k . Он делает алгоритм шиф-

рования E_k общедоступным, но сохраняет в секрете алгоритм дешифрования D_k . В том случае, когда другой пользователь захочет послать ему свое сообщение m , он находит E_k в справочнике, случайно выбирает некоторое $r \in R_k$ и вычисляет шифртекст $c = E_k(m, r)$. При этом только законный получатель, используя свою секретную лазейку, может легко определить m из c .

Весьма перспективным методом, по мнению специалистов, является квантовое шифрование. Когда для пересылки информации применяются такие элементарные квантовые системы, как поляризованные фотоны, то использование принципа неопределенности Гейзенберга позволяет достичь совершенно нового криптографического феномена, который абсолютно недостижим для обычных средств передачи информации. В традиционной теории информации и криптографии считается не требующим доказательств то, что цифровая связь может всегда пассивно просматриваться или копироваться даже лицом, которое не осведомлено об информации, которая передается. Это может быть полезно, например, тому, кто надеется вычислить (или разузнать) секретный ключ по прошествии какого-то времени, возможно, после того, как будет накоплен достаточный объем шифртекста. В противоположность этому, когда информация закодирована в неортогональных квантовых состояниях, например, в одиночных фотонах с направлениями поляризации 0° , 45° , 90° и 135° , то получается такой канал связи, что почта в нем даже в принципе не может с достоверностью ни читаться, ни копироваться нарушителем, не знаящим некую информации о ключе, которая используется при формировании пересылаемого сообщения. Нарушитель не может извлечь никакой частичной информации об этой пересылке, позволяющей отличить ее от случайной, и таким способом, который не поддавался бы контролю и который не смогли бы обнаружить законные пользователи канала [7].

Стеганография – это метод организации связи, который собственно скрывает само наличие связи. В отличие от криптографии, где неприятель точно может определить, является ли передаваемое сообщение зашифрованным текстом, методы стеганографии позволяют встраивать секретные сообщения в безобидные послания так, чтобы невозможно было заподозрить существование встроенного тайного послания.

К стеганографии относится огромное множество секретных средств связи, таких, как невидимые чернила, микрофотоснимки, условное расположение знаков, тайные каналы, средства связи на плавающих частотах и т.д.

Стеганография занимает свою нишу в обеспечении безопасности: она не заменяет, а дополняет криптографию. Соккрытие сообщения методами стеганографии значительно снижает вероятность обнаружения самого факта передачи сообщения. А если это сообщение к тому же зашифровано, то оно имеет еще один, дополнительный, уровень защиты.

В настоящее время в связи с бурным развитием вычислительной техники и новых каналов передачи информации появились новые стеганографические методы, в основе которых лежат особенности представления информации в компьютерных файлах, вычислительных сетях и т.п. Это дает нам возможность говорить о становлении нового направления – компьютерной стеганографии.

Обобщенная модель стегосистемы представлена на рис. 2.8.



Рис. 2.8. Модель стегосистемы

В качестве данных может использоваться любая информация: текст, сообщение, изображение и т.п.

В общем же случае целесообразно употреблять слово «сообщение», поскольку сообщениями могут быть как текст или изображение, так и, например, аудиоданные. *Контейнер* – любая информация, предназначенная для сокрытия тайных сообщений. *Пустой контейнер* – контейнер без встроенного сообщения; заполненный контейнер или *стегоконтейнер*, содержащий встроенную информацию. *Встроенное (скрытое) сообщение* – сообщение, встраиваемое в контейнер.

В зависимости от количества уровней защиты (например, встраивание предварительно зашифрованного сообщения) в стегосистеме может быть один или несколько стегоключей. По аналогии с криптографией, по типу стегоключа стегосистемы можно подразделить на два типа: с секретным ключом и с открытым ключом [20, 66].

2.3.3. Выбор метода преобразования

Изложенные сведения по методам шифрования информации не претендуют на глубокий анализ и полноту описания, так как это не является задачей данной книги. Введение в проблему требует также ознакомления с некоторыми методами оценки криптостойкости и сравнения методов шифрования.

Большинство искусственных языков (и все естественные языки) имеют характерное частотное распределение букв и других знаков. Например, *e* – наиболее часто встречающаяся буква в английском языке, а *z* – наиболее редкая. Это вовсе не говорит о том, что не будут попадаться английские (исходные) сообщения, в которых другая буква будет встречаться чаще, чем *e*, и реже, чем *z*. Но для очень большого числа сообщений могут быть установлены определенные характерные частоты. Многие сообщения, зашифрованные методом перестановки, или одноалфавитной подстановки, сохраняют характерные частотные распределения и, таким образом, указывают криптоаналитику путь к раскрытию шифра.

Криптоаналитики часто используют индекс соответствия (ИС) для определения того, находятся ли они на правильном пути. Теоретически ожидаемое значение ИС для английского языка определяется выражением

$$\frac{N-m}{m(N-1)} 0,066 + 0,038 \frac{N(m-1)}{m(N-1)},$$

где N – длина сообщения в буквах;
 m – число алфавитов.

Шифровки, которые дают значения ИС, большие, чем 0,066 (для английского языка), сами сообщают о том, что, вероятно, использовалась одноалфавитная подстановка, предоставляя, таким образом, криптоаналитикам превосходный инструмент для разгадки шифра.

Если ИС находится между значениями 0,052 и 0,066, то, возможно, был использован двухалфавитный шифр подстановки, если между 0,052 и 0,047 – трехалфавитный и т.д. Криптоаналитик берет наиболее часто встречающийся символ и предполагает, что это пробел, затем берет следующий наиболее часто встречающийся символ и предполагает, что это «e», и т.д. С помощью ЭВМ это делается быстро и аккуратно.

Дело осложняется, когда криптоаналитик сталкивается с равномерным распределением символов (ИС = 0,038 для английского языка $1/26 = 0,038$, где 26 – число букв в английском алфавите), которое получается при использовании многоалфавитной подстановки [78].

Принципиальное значение для надежности шифрования имеет длина кода ключа, т.е. отношение его длины к длине закрываемого им текста. Чем больше оно приближается к единице, тем надежнее шифрование. Следует иметь в виду, что это отношение распространяется не только на данное сообщение, переданное однократно по назначению, но и на все остальные сообщения, закрытые этим же кодом ключа и передаваемые постоянно и периодически в течение времени его существования до замены новым значением. Это объясняется тем, что мы не знаем времени подключения нарушителя к линии связи и поэтому заранее предполагаем наиболее опасный вариант, когда он подключен постоянно. В этом случае при многократном повторении кода ключа по всей длине текста существует опасность его раскрытия статистическим методом. Вероятность этого события зависит не только от указанного выше отношения, но и от выбранного метода шифрования.

Поясним это на примере цифрового текста, закрытого цифровым кодом ключа методом гаммирования.

1. Закрытое многозначное число 1001 1000 1011 1010 1101 1100 получено путем поразрядного сложения по модулю 2 числа $X_1 X_2 X_3 X_4 X_5 X_6$ с однозначным числом K , т.е. шифрование числа $X_1 X_2 X_3 X_4 X_5 X_6$ ключом K можно представить в виде системы уравнений:

$$\begin{aligned} X_1 \oplus K &= 1001, \\ X_2 \oplus K &= 1000, \\ X_3 \oplus K &= 1011, \\ X_4 \oplus K &= 1010, \\ X_5 \oplus K &= 1101, \\ X_6 \oplus K &= 1100. \end{aligned}$$

2. Исходя из условия, что X принимает десятичные значения от 0 до 9, для поиска неизвестного K определим все возможные значения X_i и K , сумма которых по модулю 2 приводит к результату 1001:

$$\begin{array}{r}
 X_1 = 0000\ 0001\ 0010\ 0011\ 0100\ 0101\ 0110\ 0111\ 1000\ 1001 \\
 \oplus \\
 1001\ 1001\ 1001\ 1001\ 1001\ 1001\ 1001\ 1001\ 1001\ 1001 \\
 \hline
 K = 1001\ 1000\ 1011\ 1010\ 1101\ 1100\ 1111\ 1110\ 0001\ 0000.
 \end{array}$$

3. Аналогично определим K для чисел 1000, 1011, 1101 и 1100.

4. Анализируя полученные значения K для каждого из чисел и исключая значения более 9, определим значение, которое присутствует в каждом из десятков результатов.

Это значение будет равно 1001, т.е. в десятичном счислении 9. Следовательно, код ключа $K = 9$, а искомое число – 012345.

Приведенный пример говорит о низкой эффективности метода гаммирования при малой длине кода ключа. Другие методы наложения также могут быть не стойкими, так как в этом случае лишь усложняется математическое уравнение системы с несколькими неизвестными и увеличивается объем вычислений при их решении. Но эти преграды легко преодолеть с помощью современной математики и вычислительной техники.

Для повышения эффективности шифрования рекомендуется «длинный» ключ; «двойной» ключ, где два ключа добавлялись по модулю 2 к исходному тексту; шифрование псевдослучайным ключом, где ключ так изменяется с каждым словом, как это обеспечивалось генератором псевдослучайных чисел. Применяются и другие методы использования ключей.

Интересным и эффективным способом является применение уравнения – генератора псевдослучайных чисел (ПСЧ) [78]. Современные достижения математики позволяют с помощью этого уравнения получить шифр с «бесконечным» ключевым словом, располагая относительно малой длиной самого ключа. Реализация этого метода заключается в том, что в вычислительную систему закладывается специальный алгоритм, который при получении кода ключа (порождающего числа T) вырабатывает по определенному закону (уравнению) с каждым тактом новое псевдослучайное число, цепочка из которых накладывается на закрываемый текст, и таким образом из «короткого» ключа получается «длинный» и жестко связанный с ним второй ключ. Например, если использованное порождающее число было 4372, то последовательность будет выглядеть следующим образом:

$T_0 = 4372$ Двумя средними числами являются 3 и 7.
 Квадрат 37 – число 1369.
 $T_1 = 1369$ Двумя средними цифрами являются 3 и 6.
 Квадрат 36 – число 1296.
 $T_2 = 1296$ Двумя средними цифрами являются 2 и 9.
 Квадрат 29 – число 841.
 $T_3 = 0841$...
 И т.д.

Это выглядит достаточно убедительно, пока не будет обнаружено, что из 100 возможных чисел, которые могут быть возведены в квадрат:

62 вырабатывают последовательности, которые вырождаются в 00, 00, 00, ...;

19 – вырабатывают последовательности, которые вырождаются в 10, 10, 10, ...;

15 – вырабатывают последовательности, которые вырождаются в 60, 60, 60, ...;

3 – вырабатывают последовательности, которые вырождаются в 24, 57, 24, 57, 24, 57, ...;

1 – вырабатывает последовательность, которая вырождается в 50, 50, 50, ...

Для нас важно, чтобы генераторы ПСЧ были воспроизводимыми, хотя в то же время они должны вырабатывать числа, которые «кажутся случайными». На основе теории групп было разработано несколько типов таких генераторов. В настоящее время наиболее доступными являются конгруэнтные генераторы. На основе их строгого определения можно сделать математически корректное заключение о том, какими свойствами должны обладать выходные сигналы этих генераторов с учетом периодичности и случайности.

Одним из хороших конгруэнтных генераторов является линейный конгруэнтный генератор ПСЧ. Этот генератор вырабатывает последовательность псевдослучайных чисел $T_1, T_2, T_3, \dots, T_m, \dots$, используя соотношение

$$T_i + 1 = (aT + c) \bmod m,$$

где T_i – исходная величина, выбранная в качестве порождающего числа;
 a и c – константы.

Указанное уравнение генерирует псевдослучайные числа с определенным периодом повторения, зависящим от выбранных значений a и c . Значение m обычно устанавливается равным 2^{b-1} или 2^b , где b – длина слова ЭВМ в битах [78].

Сам процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно, однако аппаратная реализация обладает по сравнению с программной рядом преимуществ: высокой производительностью, упрощенной организацией обработки информации и т.д.

Дальнейшее развитие симметричных систем шифрования привело к появлению нового алгоритма IDEA (International Data Encryption Algorithm), разработанного в Швейцарии. Он может стать одним из наиболее криптоустойчивых алгоритмов, доступных для широкого применения. Это алгоритм блочного шифрования, оперирующий с блоками открытого текста длиной 64 бита и преобразующий их в блоки шифртекста такой же длины. Длина ключа шифрования 128 бит. Один и тот же алгоритм используется для шифрования и дешифрования данных [85].

Pretty Good Privacy (PGP) – это программный пакет, разработанный Ф. Циммерманом, который обеспечивает шифровку почты и файлов. Циммерман взял существующие криптосистемы и криптографические протоколы и разработал бесплатную (freeware) программу для различных платформ. Она обеспечивает шифрование сообщений, цифровые подписи (digital signatures) и совместимую почту (e-mail compatibility).

Алгоритмы, используемые для шифрования сообщений, – это RSA для передачи ключа и IDEA для самого шифрования сообщений. Стойкость цифровой подписи достигается при применении RSA для подписи и MD5 для вычисления message digest. PGP использует ZIP-компрессию, а также маскирует координаты и данные отправителя, что немного осложняет процесс анализа трафика. Совместимость почты достигается путем использования Radix-64 конвертации (conversion).

PGP проверена огромным количеством людей, ее исходные тексты опубликованы в Интернете, но поскольку в ней используется RSA, то степень защиты сообщения зависит от длины ключа (чем больше, тем лучше).

MIT PGP версии 2.6 и последующие версии – это вполне легальная бесплатная программа для некоммерческого использования. Viascrypt версии 2.7 и последующие версии уже коммерческий продукт.

PGP – программа, служащая для кодирования и/или подписывания сообщений, файлов и любой другой информации, представленной в электронном виде. В основе работы PGP лежит алгоритм RSA (Rivest-Shamir-Adelman), основанный на наличии двух ключей – открытого и секретного. Открытый ключ распространяется максимальному количеству людей (через KeyServer'a, лично и т.п.), а секретный должен находиться только у владельца (рекомендуется использовать ключи не менее 1024 бит) [www.cd boom. com].

За рубежом существует много блочных симметричных алгоритмов: IDEA, AES, RC2, RC5, RC6 и другие, поточных симметричных алгоритмов, таких, как SEAL, WAKE, PIKE, GOAL и другие, асимметричных алгоритмов шифрования DH, DSA, а также большой класс алгоритмов, использующих хэш-функцию: MD2, MD5, SHA, RIPEMD, MDC2. Все они могут быть выполнены как в программном, так и в аппаратном варианте.

2.4. Методы защиты информации от компьютерных вирусов

Защита информации от компьютерных вирусов – особая область исследований, которой занимаются специалисты-профессионалы [30, 32, 57, 75]. Рассмотрим проблему с помощью материалов работы [27].

Вредительские программы и прежде всего вирусы представляют серьезную опасность для информации в АС. Недооценка этой опасности может иметь серьезные последствия для информации пользователей. Вредит использованию всех возможностей АС и чрезмерное преувеличение роли 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 1980-х гг. Малые размеры, способность быстро распространяться, размножаясь и внедряясь в объекты (заражая их), негативное воздействие на сис-

тему – все эти признаки биологических вирусов присущи и вредительским программам, получившим по этой причине название компьютерные вирусы. Вместе с термином «вирус» в вычислительной технике употребляются 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 АС. Вирусы могут изменять или уничтожать программное обеспечение или данные, хранящиеся в АС. В процессе распространения вирусы могут себя модифицировать.

Программы-вирусы создаются для ЭВМ определенного типа, работающих с конкретными ОС. Для одних ОС созданы тысячи вирусов, например ОС MS DOS.

Для ОС Unix, OS/2, Windows и некоторых других операционных систем известно незначительное количество вирусов. Привлекательность ОС для создателей вирусов обуславливается следующими факторами:

- распространенностью ОС;
- отсутствием встроенных антивирусных механизмов;
- относительной простотой;
- продолжительностью 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.

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 вероятность 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.

Массовое распространение вирусов, серьезность последствий их воздействия на ресурсы АС вызвали необходимость разработки и использования

специальных антивирусных средств и методов их применения. Антивирусные средства используются для решения следующих задач [75]:

- обнаружения вирусов в АС;
- блокирования работы программ-вирусов;
- устранения последствий воздействия вирусов.

Обнаружение вирусов желательно осуществлять на стадии их внедрения или, по крайней мере, до начала осуществления их деструктивных функций. Следует 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 обнаружения вируса по отношению к началу деструктивных действий. Восстановление информации без 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 предусматривают изменение информации.

Для борьбы с вирусами используются программные и аппаратно-программные средства, которые применяются в определенной последовательности и комбинации. Можно выделить методы обнаружения и удаления вирусов.

Известны следующие методы обнаружения вирусов [32]:

- сканирование;
- установление наличия изменений;
- эвристический анализ;
- использование резидентных сторожей;
- вакцинирование программ;
- аппаратно-программная защита от вирусов.

Сканирование – один из самых простых методов обнаружения вирусов. Оно осуществляется программой-сканером, которая просматривает файлы в поисках опознавательной части вируса – сигнатуры. Программа фиксирует наличие уже известных вирусов, за исключением полиморфных, которые применяют шифрование тела вируса, изменяя при этом каждый раз и сигнатуру. Программы-сканеры могут хранить не сигнатуры известных вирусов, а их контрольные суммы. Программы-сканеры часто могут удалять обнаруженные вирусы. Такие программы называются полифагами.

Метод сканирования применим для обнаружения вирусов, сигнатуры которых уже выделены и являются постоянными. Для эффективного использования метода необходимо регулярное обновление сведений о новых вирусах.

Самой известной программой-сканером в России является Aidstest Д. Позинского.

Метод обнаружения изменений базируется на использовании программ-ревизоров. Эти программы определяют и запоминают характеристики всех областей на дисках, в которых обычно размещаются вирусы. При периоди-

ческом 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. 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 вирусу области памяти.

Имеются у этого метода и недостатки. С помощью программ-ревизоров невозможно определить вирус в файлах, которые поступают в систему уже зараженными. Вирусы будут обнаружены только после размножения в системе.

Программы-ревизоры не пригодны для обнаружения заражения макро-вирусами, 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 выявления в них команд (групп команд), характерных для вирусов. Такими командами могут быть команды создания резидентных модулей в оперативной памяти, команды прямого обращения к дискам, мнущая 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 раздраже-

ние и желание отказаться от резидентных сторожей. Примером резидентного сторожа может служить программа Vsafe, входящая в состав MS DOS.

Под *вакцинацией программ* понимается создание специального модуля для контроля их 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 неизвестные, за исключением «стелс»-вирусов.

Самым надежным методом защиты от вирусов является использование *аппаратно-программных антивирусных средств*. В настоящее время для защиты ПК применяются 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.

В процессе удаления последствий заражения вирусами осуществляется удаление вирусов, а также восстановление файлов и областей памяти, в которых находился вирус. Существуют 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 сведения об общих принципах работы вирусов, осуществляется восстановление файлов. Если вирус подверг файл необратимым изменениям, то восстановление возможно только с 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 полезно сначала расшифровать информацию на диске. Для этого необходимо знать механизм действия вируса.

Для защиты от воздействия вирусов пользователь должен иметь представление о механизме действия вирусов, чтобы адекватно оценивать возможность и последствия заражения АС. Главным же условием безопасной работы в АС 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. Копируются 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 (Aidtest 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, проводящими эвристический анализ (Aidtest, Doctor Web, AntiVirus). При первом выполнении исполняемого файла применяются 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. Для этого надо использовать автоматизированное рабочее место администратора системы или лица, отвечающего за безопасность ин-

формации. 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 дисках 3,5 дюйма для этого достаточно открыть квадратное отверстие.

Неукоснительное 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).

Даже при скрупулезном выполнении всех правил профилактики возможность заражения АС компьютерными вирусами полностью исключить нельзя. И если вирус все же попал в АС, то последствия его пребывания можно свести к минимуму, придерживаясь определенной последовательности действий.

О наличии вируса в АС пользователь может судить по следующим событиям:

- появлению сообщений антивирусных средств о заражении или о предполагаемом заражении;
- явным проявлениям присутствия вируса, таким, как сообщения, выдаваемые на монитор или принтер, звуковые эффекты, уничтожение файлов, и другим аналогичным действиям, однозначно указывающим на наличие вируса в АС;
- неявным проявлениям заражения, которые могут быть вызваны и другими причинами, например сбоями или отказами аппаратных и программных средств АС.

К неявным проявлениям наличия вирусов в АС можно отнести «зависания» системы, замедление выполнения определенных действий, нарушение адресации, сбой устройств и т.п.

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 необходимо выполнить следующую последовательность шагов.

Шаг 1-й. Выключить ЭВМ для уничтожения резидентных вирусов.

Шаг 2-й. Осуществить загрузку эталонной операционной системы со сменного носителя информации, в которой отсутствуют вирусы.

Шаг 3-й. Сохранить на сменных носителях информации важные для вас файлы, которые не имеют резервных копий.

Шаг 4-й. Использовать антивирусные средства для удаления вирусов и восстановления файлов, областей памяти. Если работоспособность ЭВМ восстановлена, то осуществляется переход к шагу 8, если работоспособность ЭВМ не восстановлена – к шагу 5.

Шаг 5-й. Осуществить полное стирание и разметку (форматирование) несъемных внешних запоминающих устройств. В ПК 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 [81]. 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-й. Восстановить ОС, другие программные системы и файлы с дистрибутивов и резервных копий, созданных до заражения.

Шаг 7-й. Тщательно проверить файлы, сохраненные после обнаружения заражения, и при необходимости удалить вирусы и восстановить файлы.

Шаг 8-й. Завершить восстановление информации всесторонней проверкой ЭВМ с помощью имеющихся на данный момент антивирусных средств.

Постоянно обновлять антивирусные средства.

При выполнении рекомендаций по профилактике заражения компьютерными вирусами, а также при умелых и своевременных действиях в случае заражения вирусами ущерб информационным ресурсам АС может быть сведен к минимуму. Защита от заражения вирусами способствуют средства контроля и разграничения доступа, о которых пойдет речь в подразделах, посвященных построению системы безопасности информации АС.

2.5. Защита информации от утечки за счет побочного электромагнитного излучения и наводок

2.5.1. Потенциальные угрозы

Работа средств вычислительной техники сопровождается электромагнитными излучениями и наводками (ПЭМИН) на соединительные проводные линии, цепи «питания», «земля», возникающими вследствие электромагнитных воздействий в ближней зоне излучения, в которую могут попадать также провода вспомогательной и посторонней аппаратуры. Электромагнитные излучения, даже если они отвечают техническим нормам, не являются безопасными с точки зрения утечки секретной информации и несанкционированного доступа к ней.

В некоторых случаях информацию, обрабатываемую средствами ЭВТ, можно восстановить путем анализа электромагнитных излучений и наводок. Для этого необходимы их прием и декодирование. Одно время считалось очень трудным расшифровать информацию, содержащуюся в излучении, и бытовало мнение, что восстановление информации после приема под силу только профессионалам, располагающим очень сложной аппаратурой обнаружения и декодирования. Однако исследования показали, что восстановление информации от некоторых средств ЭВТ возможно с помощью общедоступных радиоэлектронных средств. В частности, при восстановлении информации с мониторов можно использовать обычный черно-белый телевизор, в котором проведены незначительные усовершенствования. Если монитор является элементом вычислительной системы, то он может оказаться самым слабым ее звеном, которое сведет на нет все меры по увеличению безопасности излучений, принятые в остальных частях системы.

Применение в средствах ЭВТ импульсных сигналов прямоугольной формы и высокочастотной коммутации приводит к тому, что в спектре излучений будут компоненты с частотами вплоть до сверхвысоких. Хотя энергетический спектр сигналов убывает с ростом частоты, эффективность излучения при этом увеличивается, и уровень излучений может оставаться постоянным до частот в несколько гигагерц. Резонансы из-за паразитных связей могут вызывать усиление излучения сигналов на некоторых частотах спектра [17, 38].

2.5.2. Методы и средства защиты информации от излучения

В целях защиты секретной информации от утечки за счет ПЭМИН производится измерение уровня опасных сигналов на расстоянии от источника (монитора, печатающего устройства, кабеля и т.д.). Замеры производят в нескольких точках на разных расстояниях от источника с помощью специальной приемной аппаратуры (например, анализатора спектра НР 8586 А в диапазоне 30...100 МГц в режиме с полосой пропускания 10 кГц и пиковым детектированием). Если уровень сигнала на границе установленной зоны превысил допустимые значения, применяют защитные меры.

Защитные меры могут носить различный характер в зависимости от сложности, стоимости и времени их реализации, которые определяются при создании конкретной автоматизированной системы. Такими мерами могут быть: доработка аппаратуры с целью уменьшения уровня сигналов, установка специальных фильтров, параллельно работающих аппаратных генераторов шума, специальных экранов и др. В числе этих мер большие надежды возлагаются на применение в линиях и каналах связи волоконно-оптических кабелей, которые обладают следующими преимуществами: отсутствием электромагнитного излучения во внешнюю среду, устойчивостью к внешним электромагнитным излучениям, большой помехозащищенностью, скрытностью передачи, малыми габаритами (что позволяет прокладывать их рядом с уже существующими кабельными линиями), устойчивостью к воздействиям агрессивной среды.

С точки зрения защиты информации волоконно-оптические кабели имеют еще одно преимущество: подключение к ним с целью перехвата передаваемых данных представляет собой значительно более сложную задачу, чем подключение к обычному проводу или кабелю с помощью индуктивных датчиков и прямого подключения [17]. Однако замена одного кабеля другим связана с введением электрооптических и оптико-электрических преобразователей, на которые и перекладывается проблема обеспечения безопасности информации. Решение этой проблемы находится в упомянутой выше области.

Беспроводная передача данных с помощью ИК-системы может быть особенно полезна в учреждениях с большим общим рабочим залом. Среди главных преимуществ такой системы следует указать невосприимчивость ИК-каналов передачи данных к электромагнитным излучениям работающего в том

же помещении оборудования. Специалисты считают, что использование этой системы почти полностью устраняет возможность просачивания электромагнитного излучения за пределы вычислительного центра [17, 38]. Однако из соображений безопасности американские ядерщики решили прекратить использование беспроводных компьютерных сетей¹.

2.6. Методы и средства защиты информации от случайных воздействий

В целях защиты АС от случайных воздействий применяются уже известные средства повышения надежности аппаратуры и программного обеспечения КСА, а для защиты информации – средства повышения ее достоверности. Для предотвращения аварийной ситуации применяются специальные меры.

Методы и средства повышения надежности вычислительных систем и достоверности информации в настоящее время достаточно хорошо разработаны [35, 39, 54, 79, 83]. Первые методы и средства косвенным образом помогают существенно сократить влияние случайных воздействий и на информацию.

Мы лишь кратко рассмотрим проблему и основные ее моменты, имеющие непосредственное отношение к защите информации в рамках поставленной задачи и необходимых для анализа и выработки нового подхода к средствам повышения надежности с позиций безопасности информации, обрабатываемой в АС.

Проблема надежности автоматизированных систем решается тремя путями:

- повышения надежности деталей и узлов;
- построения надежных систем из менее надежных элементов за счет структурной избыточности (дублирование, утроение элементов, устройств, подсистем и т.п.);
- применения функционального контроля с диагностикой отказа, увеличивающего надежность функционирования системы за счет сокращения времени восстановления отказавшей аппаратуры.

Задачами функционального контроля (ФК) системы являются: своевременное обнаружение сбоев, неисправностей и программных ошибок, исключение их влияния на дальнейший процесс обработки информации и указание места отказавшего элемента, блока программы с целью последующего быстрого восстановления системы.

Существующие методы функционального контроля вычислительных систем могут быть разделены на программный, аппаратный и комбинированный (сочетание программного с аппаратным) [35].

Сравнительная характеристика методов ФК учитывает следующие факторы:

- надежность обнаружения;
- возможность исправления ошибок после сбоев без вмешательства оператора;
- время, затрачиваемое на устранение случайных ошибок;

¹ www.Netoscope.ru.

- количество дополнительного оборудования;
- способы применения: параллельно или с прерыванием обработки информации;
- влияние контроля на быстродействие вычислительной системы или ее производительность;
- указание места неисправности с необходимой точностью.

Программный контроль делится на программно-логический, алгоритмический и тестовый.

Наиболее распространенная форма программно-логического контроля – это двойной счет со сравнением полученных результатов.

Программно-логический контроль позволяет надежно обнаруживать сбои, и для его проведения не требуется дополнительного оборудования. Однако при нем более чем вдвое снижается производительность ЭВМ, не обнаруживаются систематические сбои, нельзя указать место отказа и тем более сбоя, требуется дополнительная емкость памяти для программы вычислений. Алгоритмический контроль заключается в том, что задача, решенная по какому-либо алгоритму, проверяется повторно по сокращенному алгоритму с достаточной степенью точности. При алгоритмическом контроле производительность ЭВМ выше, в остальном он обладает теми же недостатками и, кроме того, имеет ограниченное применение, так как не всегда удается найти для основного алгоритма сокращенный.

Тестовый контроль, как правило, применяется для проверки работоспособности комплекса средств автоматизации с помощью испытательных программ.

Тестовый контроль в отличие от программно-логического проверяет не процесс переработки информации, а пребывание КСА или его части в работоспособном состоянии. Кроме того, тестовый контроль не всегда обнаруживает сбои и во время проверки не может решать задачи по рабочей программе.

Аппаратный контроль в отличие от программного может обеспечивать указание о наличии сбоя или неисправности непосредственно в момент его возникновения. Аппаратный контроль в КСА делится на контроль по модулю, контроль при дублировании оборудования и контроль при троировании оборудования с использованием мажоритарных элементов.

Контроль по модулю основывается на следующих принципах. Из теории чисел известно, что целое положительное число можно представить в виде сравнения [35]:

$$A \equiv r_a \pmod{M} \quad (2.1)$$

(считается: A сравнимо с остатком r_a модуля M), которое устанавливает следующее соотношение между числами A , r и M :

$$A \equiv Ml + r_a,$$

где A , M , l и r_a – целые числа;
 A – любое контролируемое n -разрядное число;
 M – модуль или делитель;
 l – частное;
 r_a – остаток от деления A на модуль M (контрольный код числа A).

При данном методе контроля каждому контролируемому члену придается еще m дополнительных разрядов, в которые записывается контрольный код, т.е. остаток r_a . Если записать все числа в виде сравнения (2.1), то после этого их можно будет складывать, перемножать, а результаты записывать в виде подобных сравнений [35]:

$$\sum_{i=1}^p A_i \equiv \sum_{i=1}^p r_{a_i} \pmod{M}, \quad (2.2)$$

$$\prod_{i=1}^p A_i \equiv \prod_{i=1}^p r_{a_i} \pmod{M}. \quad (2.3)$$

Данные выражения означают, что сумма (произведение) чисел сравнима с суммой (произведением) остатков этих чисел по модулю M .

Техническая реализация контроля по модулю заключается в разработке специальных схем, которые в технической литературе получили название «свертки». Эффективность контроля повышается с увеличением модуля. Однако с увеличением M непропорционально возрастает количество дополнительного оборудования и усложняются схемы контроля [35]. Широкое распространение в вычислительных схемах получил контроль по модулю 2.

Дублирование оборудования позволяет путем сравнения выходных сигналов обнаружить отказ аппаратуры. Высокая эффективность такого контроля основывается на том, что вероятность одновременного отказа двух одинаковых элементов исчезающе мала. Недостатком этого метода является не всегда имеющаяся возможность определить, какой из каналов исправен и поэтому, чтобы процесс функционирования протекал нормально, приходится одновременно в каждом из каналов применять методы контроля, например контроль по модулю.

Троирование оборудования с элементами «голосования» позволяет наряду с увеличением вероятности безотказной работы увеличить и достоверность функционирования с помощью мажоритарных элементов. Данный метод требует, разумеется, увеличения объемов оборудования.

В настоящее время существуют разнообразные методы контроля, имеющие в зависимости от конкретных требований и условий различную степень применимости. Некоторые из этих методов являются специализированными для определенных типов устройств и систем. Другие – приспособлены для проверки определенных видов операций и применяются в различных типах устройств.

Поскольку результат воздействия на информацию зависит от количества ошибок в данный момент, рассмотрим вероятность появления этих событий.

Ввод, хранение и обработка информации в КСА осуществляется с помощью кодов чисел и слов по определенному алгоритму. Появление сбоев приводит к тому, что в коде может возникнуть одиночная или групповая ошибка (двукратная, трехкратная и т.д.). Ошибка может считаться одиночной, если она возникла в одном разряде кода числа или слова [35].

Считая ошибки в каждом разряде кода независимыми, можно определить вероятность появления ошибки i -й кратности при известной вероятности искажения одного разряда двоичного кода. В этом случае ошибки в каждом из разрядов подчиняются биномиальному распределению вероятностей. Согласно [35] вероятность появления однократной ошибки в n -разрядном двоичном коде может быть определена из выражения

$$P_1 = n \cdot q (1 - q)^{n-1},$$

где q – вероятность появления ошибки в отдельном разряде в течение одной операции.

Вероятность появления двукратной ошибки

$$P_2 = \frac{n(n-1)}{2} q^2 (1-q)^{n-2}.$$

Вероятность появления ошибок i -й кратности:

$$P_i = C_n^i q^i (1-q)^{n-i}.$$

Однако оценка значения P_i аналитическим путем связана с трудностями, которые зависят от причин, вызывающих сбои. Получение статистического материала о сбоях каждого разряда также является сложным вопросом. Поэтому в [35] показано, что P_i может быть получено по более удобной формуле

$$P_i = \frac{n \cdot \mu_p \cdot t_{\text{оп}}}{i!} e^{-n \cdot \mu_p \cdot t_{\text{оп}}},$$

где μ_p – интенсивность отказов оборудования, участвующего в передаче и хранении каждого разряда двоичного кода;
 $t_{\text{оп}}$ – длительность одной операции.

В [35] также отмечается, что с увеличением кратности ошибки вероятность ее появления уменьшается. Вероятность появления ошибки с кратностью $i = 4$ пренебрежимо мала. Для оценки эффективности аппаратного контроля необходимо знать вероятность обнаружения (пропуска) ошибок различной кратности при выбранном методе контроля. В связи с этим общая вероятность пропуска ошибки

$$P_{\text{пр}} = \sum_{i=1}^n P_i \cdot P_{M_{\text{пр},i}},$$

где P_i – вероятность появления ошибки i -й кратности;
 $P_{M_{\text{пр},i}}$ – вероятность пропуска ошибки i -й кратности при выбранном методе аппаратного контроля.

В настоящее время имеется достаточно работ по вероятности обнаружения ошибок различной кратности при аппаратном контроле по модулю [35]. Вероятность обнаружения дополняет до единицы вероятность пропуска ошибок, т.е. $P_{M_{\text{пр},i}} = 1 - P_{\text{обн},i}$. Например, вероятность появления двукратной ошибки можно вычислить по формуле [35]:

$$P_2 = \frac{n^2 \cdot \mu_p^2 \cdot t_{\text{оп}}^2}{2} e^{-n \mu_p t_{\text{оп}}}.$$

Вероятность пропуска двукратной ошибки при контроле по модулю 3 вычисляется по формуле [35]:

$$P_{\text{пр}} = 0,25 \cdot n^2 \cdot \mu_p^2 \cdot t_{\text{оп}}^2 (1 + 0,166 \cdot n \cdot \mu_p \cdot t_{\text{оп}}).$$

Способность средств ФК обеспечить своевременно (до начала последующей обработки) обнаружение и блокировку ошибок заданной кратности определяет уровень достоверности контроля обработки информации. Существенную роль для качества ФК играет плотность распределения его средств обнаружения ошибок по всей «площади» контролируемой вычислительной системы, т.е. полнота ее охвата функциональным контролем. В связи с этим при создании вычислительных систем используются следующие показатели качества ФК:

1) время обнаружения и локализации отказов аппаратуры с точностью до съемного элемента

$$T_{\text{обн}} = \frac{\sum_{i=1}^m t_{\text{обн},i}}{m},$$

где m – число экспериментов;
 i – номер эксперимента;
 $t_{\text{обн},i}$ – время обнаружения отказа в i -м эксперименте;

2) полнота контроля функционирования вычислительной системы

$$K_{\text{п}} = \frac{\lambda_{\text{к}}}{\lambda_0},$$

где $\lambda_{\text{к}}$ – суммарная интенсивность появления отказов составных частей, охваченных контролем;
 λ_0 – суммарная интенсивность отказов всех составных частей вычислительной системы;

3) достоверность контроля

$$K_d = \frac{n_{\text{обн}}}{n_{\text{пр}}},$$

где $n_{\text{обн}}$ – общее число отказов, обнаруженных данной системой ФК;
 $n_{\text{пр}}$ – общее число отказов проведения ФК при условии появления или искусственного введения отказов в каждом опыте.

Одним из основных условий эффективного функционирования автоматизированной системы является обеспечение требуемого уровня достоверности информации. Под достоверностью информации в АС понимают некоторую функцию вероятности ошибки, т.е. события, заключающегося в том, что реальная информация в системе о некотором параметре не совпадает в пределах заданной точности с истинным значением [39].

Необходимая достоверность достигается использованием различных методов, реализация которых требует введения в системы обработки данных информационной, временной или структурной избыточности. Достоверность при обработке данных достигается путем контроля и выявления ошибок в исходных и выводимых данных, их локализации и исправления. Условие повышения достоверности – снижение доли ошибок до допустимого уровня. В конкретных АС требуемая достоверность устанавливается с учетом нежелательных последствий, к которым может привести возникшая ошибка, и тех затрат, которые необходимы для ее предотвращения.

Методы контроля при обработке информации в АС классифицируют по различным параметрам: по количеству операций, охватываемых контролем, – единичный (одна операция), групповой (группа последовательных операций), комплексный (контролируется, например, процесс сбора данных); по частоте контроля – непрерывный, циклический, периодический, разовый, выборочный, по отклонениям; по времени контроля – до выполнения основных операций, одновременно с ними, в промежутках между основными операциями, после них; по виду оборудования контроля – встроенный, контроль с помощью дополнительных технических средств, безаппаратный; по уровню автоматизации – «ручной», автоматизированный, автоматический [39].

Различают системные, программные и аппаратные методы контроля достоверности.

Системные методы включают: оптимизацию структуры обработки; поддержание характеристик оборудования в заданных пределах; повышение культуры обработки; обучение и стимулирование обслуживающего персонала; создание оптимального числа копий и (или) предыстории программ исходных и текущих данных; определение оптимальной величины пакетов данных и скорости первичной обработки, процедур доступа к массивам данных и др.

Программные методы повышения достоверности информации состоят в том, что при составлении процедур обработки данных в них предусматривают дополнительные операции, имеющие математическую или логическую связь

с алгоритмом обработки данных. Сравнение результатов этих дополнительных операций с результатами обработки данных позволяет установить с определенной вероятностью наличие или отсутствие ошибок. На основании этого сравнения, как правило, появляется возможность исправить обнаруженную ошибку.

Аппаратные методы контроля и обнаружения ошибок могут выполнять практически те же функции, что и программные. Аппаратными методами обнаруживают ошибки быстрее и ближе к месту их возникновения, а также ошибки, не доступные для программных методов.

Все перечисленные методы контроля обработки данных базируются на использовании определенной избыточности. При этом различают методы контроля со структурной, временной и информационной избыточностью [39].

Структурная избыточность требует введения в состав АС дополнительных элементов (резервирование информационных массивов и программных модулей, реализация одних и тех же функций различными программами, схемный контроль в технических средствах АС и т.д.).

Временная избыточность связана с возможностью неоднократного повторения определенного контролируемого этапа обработки данных. Обычно этап обработки повторяют неоднократно и результаты обработки сравнивают между собой. В случае обнаружения ошибки производят исправления и повторную обработку.

Информационная избыточность может быть естественной и искусственной. Естественная информационная избыточность отражает объективно существующие связи между элементами обработки, наличие которых позволяет судить о достоверности информации. Искусственная информационная избыточность характеризуется введением дополнительных информационных разрядов в цифровой представлении обрабатываемых данных и дополнительных операций в процедуре их обработки, имеющих математическую или логическую связь с алгоритмом обработки данных. На основании анализа результатов дополнительных операций и процедур обработки данных, а также дополнительных информационных разрядов выявляются наличие или отсутствие ошибок определенного типа, а также возможности их исправления.

В работах по повышению достоверности информации рассматриваются совместно помехоустойчивость и надежность систем передачи и обработки информации с позиций качества таких систем.

По характеру информации, особенностей алгоритмов системы, а также по задачам, стоящим перед ее адресатами, можно установить следующие зависимости содержания информации от ошибок при ее передаче [54]:

- смысловой объем информации в сообщении уменьшается пропорционально числу искаженных разрядов в кодовой комбинации данного сообщения;
- искажение одного или нескольких разрядов приводит почти к полной потере остальной части информации, содержащейся в смысловом отрезке информации в сообщении.

Проанализируем способность средств ФК и повышения достоверности информации к защите от случайных разрушений, модификации и утечки информации.

Известно, что отказы, сбои в аппаратуре и ошибки в программном обеспечении могут привести к нарушению функционирования вычислительной системы и изменению информации на ложную. Анализ принятого в современных автоматизированных системах представления информации в цифровом виде показывает, что на один байт приходится одна буква, цифра или символ. Одно слово может занимать в русском языке от 1 до 20 букв. Каждой букве, цифре и символу присвоены двоичные коды. Таблица кодов [74] составлена так, что пропадание или появление одной единицы в разрядах приводит к изменению одной буквы (символа, цифры) на другую. В этом случае имеет место однократная ошибка, которая относительно легко обнаруживается простыми средствами аппаратного контроля (например, контролем по модулю 2). В случае же появления двукратной ошибки в байте измениться могут два разряда. Контроль по модулю 2 этого не обнаруживает, что уже может привести к незаметному изменению одной буквы на другую. В русском языке существуют слова, которые меняют свой смысл на другой при замене одной буквы на другую. Это и есть модификация информации. При трехкратной ошибке вероятность этого события, естественно, увеличивается. Правда, вероятность появления трехкратной ошибки меньше по сравнению с двукратной, но это слабый аргумент, так как ее величина при большом количестве аппаратных средств, интенсивности и накоплении их отказов может быть весьма ощутимой на большом отрезке времени работы вычислительной системы.

Если рассматривать искажение информации (без ее модификации) как разрушение, условием его возникновения может считаться однократная ошибка, несмотря на то, что пропадание одной буквы не всегда ведет к потере информации.

Для возникновения случайной утечки информации при ее обработке в вычислительной системе необходимо, чтобы в результате случайных воздействий был перепутан адрес получателя или в правильный адрес была выдана другая информация, для него не предназначенная. В первом случае, например, заменилась одна из букв другой (модификация), во втором – адресация ячеек памяти ОЗУ, из которого считывалась информация до ее передачи получателю (тоже модификация).

Таким образом, в нашем случае утечка информации – это частный случай ее модификации. Следовательно, средства ФК в принципе защищают информацию от случайных разрушений, модификации и утечки. Рассматривая вероятность появления этих событий при отсутствии ФК, заметим, что для разрушения информации (какой-то ее части) достаточно однократной ошибки, для модификации и утечки требуются дополнительные условия. Для наступления события, выражающегося в случайной распечатке или отображении информации на средствах, не предназначенных для этой цели, необходимо, чтобы из потока ошибок появилась такая, при которой какая-либо команда изменилась на команду «печатать» или «отображение», и по санкционированной команде информация была бы взята не по тому адресу из памяти или была направлена не на то техническое средство системы. Возможны и другие ситуации. Для наступления события, выражающегося в модификации информации, необходимо, чтобы из потока ошибок появилась такая ошибка или

группа ошибок, благодаря которым действительная информация изменилась бы на ложную, была бы не обнаружена и подверглась бы дальнейшей обработке.

Вероятность указанных событий зависит от многих факторов, но, анализируя приведенные выше относительные условия их наступления, можно дать им некоторую сравнительную оценку. Вероятность разрушения информации от случайных воздействий больше, чем ее модификации, а вероятность модификации информации больше вероятности ее утечки. Эта оценка необходима для выработки подхода к функциональному контролю с позиций защиты информации, который выражается в предъявлении к средствам ФК дополнительных требований, выполнение которых может потребовать дополнительных средств. Дополнительные требования заключаются в реализации уменьшения вероятности модификации и утечки информации существующими средствами повышения надежности и достоверности информации. Для выполнения этой задачи применяются специальные системотехнические решения:

- изоляция областей доступа к информации;
- специальная организация работы с данными, хранящимися в памяти вычислительной системы.

Изоляция областей доступа к информации вычислительной системы осуществляется также в целях поддержки разграничения санкционированного доступа.

Для исключения несанкционированного обмена между пользователями рекомендуется при проектировании сводить к минимуму число общих для них параметров и характеристик механизма защиты. Несмотря на то что функции операционной системы и системы разрешения доступа перекрываются, система разрешения доступа должна конструироваться как изолированный программный модуль, т.е. защита должна быть отделена от функций управления данными. Выполнение этого принципа позволяет программировать систему разрешения доступа как автономный пакет программ с последующей независимой отладкой и проверкой. Данный пакет программ должен размещаться в защищенном поле памяти, чтобы обеспечить системную локализацию попыток проникновения извне. Всякая попытка проникновения со стороны, в том числе операционной системы, должна автоматически фиксироваться, документироваться и отвергаться, если вызов не предусмотрен. Естественно, реализация обособленного механизма защиты потребует увеличения объемов программ. При этом может возникнуть дублирование управляющих и вспомогательных программ, а также необходимость в разработке самостоятельных вызываемых функций.

Информация, содержащаяся в вычислительной системе, может быть поделена между пользователями, что требует размещения ее в непересекающихся областях, отведенных для ее хранения. В каждой из этих областей хранится совокупность информационных объектов, подлежащих защите в равной степени. В процессе эксплуатации системы необходимо обеспечить надежное разграничение доступа к информации. Для этой цели, помимо организации доступа с помощью системы паролей, в систему при проектировании закладываются дополнительные меры по изоляции областей доступа, нарушение которых по причине отказов и программных ошибок не приводило бы к

несанкционированному доступу к информации. К таким мерам относится организация обращений процессора к памяти через регистр дескриптора, содержимое которого определяет границы доступной в данный момент области памяти путем задания адресов ее начала и конца. Таким образом, содержимое регистра является описанием (дескриптором) программы, так как она задает расположение объекта в памяти. Благодаря тому, что все обращения к памяти проходят через блок проверки дескрипторов, создается некоторый барьер.

В случае наличия в системе общего поля памяти, которое необходимо для решения поставленных задач, схемы защиты допускают обмен информацией между пользователями. Тогда применяются списковые и мандатные схемы защиты. В списковых схемах система безопасности снабжается списком всех лиц, имеющих право доступа к информации (для получения права доступа достаточно предъявить свой идентификатор). В мандатных схемах система реализует только один вид мандата, а пользователь должен иметь набор мандатов для доступа к каждому из необходимых ему объектов.

В списковой схеме при каждом обращении просмотр списка повторяется, т.е. доступ сопряжен с процедурой ассоциативного поиска. В мандатных схемах пользователь сам решает, какой объект ему нужен, и выбирает необходимый мандат или некоторое их количество, из тех, к которым он допущен.

Раздельный подход к защите информации от преднамеренных и случайных НСД, предлагаемый в данной работе (концепция защиты изложена ниже), предполагает отнести многие уже известные отдельные специальные технические решения по защите к средствам защиты от случайных воздействий. К ним можно отнести специальные средства защиты операционной системы и памяти, приведенные выше.

Анализ изложенного позволяет отметить следующие особенности требований к средствам ФК и повышению достоверности с позиций защиты информации от НСД:

- определенная целенаправленность мероприятий по ФК и повышению достоверности, выраженная в увязке технического представления информации с ее смыслом и содержанием;
- определение зависимости безопасности информации от кратности ошибок при ее обработке.

Наибольшую опасность представляют многократные ошибки, приводящие к модификации самой информации и команд, осуществляющих ее обработку. При этом уровень безопасности информации находится в прямой зависимости от количества одновременно возникающих ошибок. Способность средств функционального контроля к их обнаружению и определяет уровень безопасности информации. Поскольку вероятность появления четырехкратной ошибки относительно мала, то вероятность обнаружения дву- и трехкратных ошибок и будет мерой безопасности информации от отказов аппаратуры. Сложнее обстоит с программными ошибками, заложенными еще на этапе проектирования программного обеспечения. Это область будущих исследований.

Анализ приведенных средств ФК и повышения достоверности информации, а также специальных технических решений показывает, что с увеличе-

нием количества байтов в слове вероятность его модификации от случайных воздействий уменьшается, так как увеличивается кодовое расстояние по отношению к другим словам, командам, сообщениям. В этом смысле наименее устойчивы короткие слова и особенно цифры. Приведенный метод защиты от переадресации памяти по сути одному адресу присваивает дополнительную специальную процедуру и код, что естественно уменьшает вероятность случайного формирования такой процедуры и обращений по этому адресу других процедур и команд. Поэтому в целях повышения безопасности информации, а следовательно, и надежности вычислительной системы, может быть, следует пересмотреть методы кодирования символов, команд и адресов (включая адреса устройств и процессов) на предмет увеличения кодового расстояния между ними и уменьшения вероятности превращения одной команды или адреса в другие, предусмотренные в данной системе для других целей, что позволит не разрабатывать некоторые сложные специальные программы, которые не устраняют причины и условия появления случайных событий, а лишь обнаруживают их, да и то не всегда и в неподходящее время, т.е. когда событие уже произошло и основная задача по его предупреждению не выполнена.

Проблема защиты информации в АС от случайных воздействий достойна отдельных и более глубоких исследований. Пока же на уровне КСА она решается косвенным путем за счет повышения надежности работы аппаратных средств, их резервирования и применения тестирующих программ. Средствами, решающими непосредственно эту задачу, являются лишь средства повышения достоверности информации при ее передаче по каналам связи между удаленными объектами. На объектах автоматизации применяется специальное резервирование информации, которое рассмотрено ниже.

2.7. Методы защиты информации от аварийных ситуаций

Защита информации от аварийных ситуаций заключается в создании средств предупреждения, контроля и организационных мер по исключению НСД на комплексе средств автоматизации в условиях отказов его функционирования, отказов системы защиты информации, систем жизнеобеспечения людей на объекте размещения и при возникновении стихийных бедствий.

Практика показывает, что, хотя аварийная ситуация – событие редкое (вероятность его появления обусловлена многими причинами, в том числе не зависящими от человека, и эти причины могут быть взаимосвязаны), защита от нее необходима, так как последствия в результате ее воздействия, как правило, могут оказаться весьма тяжелыми, а потери – безвозвратными. Затраты на защиту от аварийных ситуаций могут быть относительно малы, а эффект в случае аварии – большим.

Отказ функционирования КСА может повлечь за собой отказ системы защиты информации, может открыться доступ к ее носителям: магнитным лентам, дискам и т.д., что может привести к преднамеренному разрушению,

хищению или подмене носителя. Несанкционированный доступ к внутреннему монтажу аппаратуры может привести к подключению посторонней аппаратуры, разрушению или изменению принципиальной электрической схемы.

Отказ системы жизнеобеспечения может привести к выводу из строя обслуживающего и контролирующего персонала. Стихийные бедствия: пожар, наводнение, землетрясение, удары молнии и т.д. – могут также привести к указанным выше последствиям. Аварийная ситуация может быть создана преднамеренно нарушителем. В последнем случае применяются организационные мероприятия.

На случай отказа функционирования КСА подсистема контроля вскрытия аппаратуры снабжается автономным источником питания. Для исключения безвозвратной потери информации носители информации дублируются и хранятся в отдельном удаленном и безопасном месте. Для защиты от утечки и модификации информация должна храниться в закрытом криптографическим способом виде. В целях своевременного принятия мер по защите системы жизнеобеспечения устанавливаются соответствующие датчики, сигналы с которых поступают на централизованные системы контроля и сигнализации.

Наиболее частой и типичной естественной угрозой является пожар. Он может возникнуть по вине обслуживающего персонала, при отказе аппаратуры, а также в результате стихийного бедствия.

Более подробно вопросы защиты информации от стихийных бедствий рассмотрены в специальной литературе, например в [69].

2.8. Организационные мероприятия по защите информации

Организационные мероприятия по защите информации в АС заключаются в разработке и реализации административных и организационно-технических мер при подготовке к эксплуатации системы.

По мнению зарубежных специалистов, организационные меры, невзирая на постоянное совершенствование технических мер, составляют значительную часть. Они применяются, когда вычислительная система не может непосредственно контролировать использование информации. Кроме того, в некоторых особых случаях в целях повышения эффективности защиты полезно технические меры продублировать организационными.

Организационные меры по защите систем в процессе их функционирования и подготовки к нему охватывают решения и процедуры, принимаемые руководством организации-потребителя системы. Несмотря на то что некоторые из них могут определяться внешними факторами, например законами или правительственными постановлениями, львиная доля проблем решается внутри организации в конкретных условиях.

В большинстве исследований, посвященных защите информации, и в зарубежных публикациях основное внимание уделялось либо правовому ас-

пекту и связанным с ним социальным и законодательным проблемам, либо техническим приемам решения специфических проблем защиты. По сравнению с ними организационным вопросам недоставало той четкой постановки, которая присуща техническим проблемам, и той эмоциональной окраски, которая свойственна правовым вопросам.

Предлагаемые организационные мероприятия часто не учитывают этапы: проектирования, разработки, изготовления и эксплуатации системы, а организационные меры иногда перепутаны с принципами построения.

Составной частью любого плана мероприятий должны быть четкое указание целей, распределение ответственности и перечень организационных мер защиты. Конкретное распределение ответственности и функций по реализации защиты от организации к организации может изменяться, но тщательное планирование и точное распределение ответственности являются необходимыми условиями создания эффективной и жизнеспособной системы защиты.

Организационные меры по защите информации в АС должны охватывать этапы проектирования, разработки, изготовления, испытаний, подготовки к эксплуатации и эксплуатации системы.

В соответствии с требованиями технического задания в организации-проектировщике наряду с техническими средствами разрабатываются и внедряются организационные мероприятия по защите информации на этапе создания системы. Под этапом создания понимаются проектирование, разработка, изготовление и испытание системы. При этом следует отличать мероприятия по защите информации, проводимые организацией-проектировщиком, разработчиком и изготовителем в процессе создания системы и рассчитанные на защиту от утечки информации в данной организации, и мероприятия, закладываемые в проект и разрабатываемую документацию на систему, которые касаются принципов организации защиты в самой системе и из которых вытекают организационные мероприятия, рекомендуемые в эксплуатационной документации организацией-разработчиком, на период ввода и эксплуатации системы. Выполнение этих рекомендаций есть определенная гарантия защиты информации в АС.

К организационным мероприятиям по защите информации в процессе создания системы относятся:

- введение на необходимых участках проведения работ режима секретности;
- разработка должностных инструкций по обеспечению режима секретности в соответствии с действующими в стране инструкциями и положениями;
- при необходимости выделение отдельных помещений с охранной сигнализацией и пропускной системой;
- разграничение задач, касающихся исполнителей и выпуска документации;
- присвоение грифа секретности материалам, документации, аппаратуре и хранение их под охраной в отдельных помещениях с учетом и контролем доступа исполнителей;

- постоянный контроль соблюдения исполнителями режима и соответствующих инструкций;
- установление и распределение ответственных лиц за утечку информации;
- другие меры, устанавливаемые главным конструктором при создании конкретной системы.

Организационные мероприятия, вносимые в инструкцию по эксплуатации на систему и рекомендуемые потребителю, должны быть предусмотрены на периоды подготовки, эксплуатации и завершения эксплуатации системы. Указанные мероприятия как метод защиты информации предполагают систему организационных мер, дополняющих и объединяющих перечисленные выше технические меры в единую систему безопасности информации. Поскольку организационные меры являются неотъемлемой частью системы защиты информации в автоматизированной системе, дальнейшее их описание приведено ниже в соответствующих разделах.

2.9. Законодательные меры по защите информации

Законодательные меры по защите информации от НСД заключаются в исполнении существующих в стране или введении новых законов, положений, постановлений и инструкций, регулирующих юридическую ответственность должностных лиц-пользователей и обслуживающего технического персонала за утечку, потерю или модификацию доверенной ему информации, подлежащей защите, в том числе за попытки выполнить аналогичные действия за пределами своих полномочий, а также ответственность посторонних лиц за попытку и совершение преднамеренного несанкционированного доступа к аппаратуре и информации.

Гражданский кодекс РФ (1994 г.) в части 1 в статье 139 определяет права на служебную и коммерческую тайну следующим образом:

«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.

Лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших слу-

жебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору».

Попутно с позиций, предлагаемых в данной книге, отметим, что при ознакомлении со статьей ГК, к сожалению, возникают вопросы.

Почему речь идет о третьих лицах, а о вторых – нет?

Почему рассматривается только утечка информации, а модификация, утрата (разрушение, хищение и блокировка доступа) – нет? Ведь эти действия также нарушают права собственности владельца информации.

Назревшая необходимость восстановления ответственности за правонарушения, совершаемые в области компьютерных технологий, предопределила соответствующие законодательные инициативы. В частности, Уголовный кодекс РФ 1996 г. содержит принципиально новые для отечественного уголовного законодательства виды преступлений, объединенные в самостоятельную главу 28 «Преступления в сфере компьютерной информации». Такой подход, несомненно, верен и соответствует мировым правовым тенденциям.

Основные нормативные правовые документы, регламентирующие (на 01.06.98 г.) в России вопросы государственной тайны, приведены в приложении 2.

Цель законодательных мер – предупреждение и сдерживание потенциальных нарушителей. Отсутствие в нашей стране опыта правового регулирования отношений в области компьютерных технологий позволяет оставлять многие преступления, совершаемые в информационном пространстве, практически безнаказанными.



ОСНОВЫ МЕТОДОЛОГИИ ПОСТРОЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

3

3.1. Анализ и оценка действующей концепции защиты

Из обзора технической литературы по данной проблеме видно, что в настоящее время при построении защиты информации сложился подход, основанный на представлении обработки информации в виде абстрактной вычислительной среды, в которой работает множество «субъектов» (пользователей и процессов) со множеством «объектов» (ресурсами и наборами данных). При этом построение защиты заключается в создании защитной среды в виде некоторого множества ограничений и процедур, способных под управлением ядра безопасности запретить несанкционированный и реализовать санкционированный доступ «субъектов» к «объектам» и защиту последних от множества преднамеренных и случайных внешних и внутренних угроз (рис.3.1).

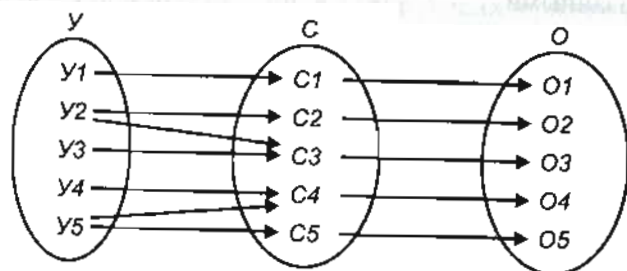


Рис. 3.1. Модель защиты информации по действующей концепции:
У – множество субъектов (угроз); С – множество защитных функций;
О – множество объектов защиты

Данный подход опирается на теоретические модели безопасности: АДЕПТ-50 Хартсона, Бела-Лападулы, MMS Лендвера и Мак-Лина, Биба, Кларка-Вилсона и др. [22, 71]. Считается, что данные модели являются инструментарием при разработке определенных политик безопасности, определяющих некоторое множество требований, которые должны быть выполнены в конкретной реализации системы. На практике разработчикам чрезвычайно сложно реализовать эти модели, и поэтому они рекомендуются лишь для анализа и оценки уровня безопасности автоматизированных систем, а руководствоваться при разработке им предлагается специально разработан-

ными на основе упомянутых подхода и моделей стандартами [14, 29, 31, 34, 64, 73].

Следует также назвать новый международный стандарт ИСО/МЭК 15408-99 «Критерии оценки безопасности информационных технологий» [Criteria for Information Technology Security Evaluation], разработанный в рамках проекта «Общие критерии». В данном стандарте обобщен опыт использования вышеперечисленных стандартов, но базовый подход, приведенный выше, сохранился. Тот же подход используется в стандартах России [12, 67]. В настоящее время планируется применить упомянутый стандарт и в России.

В указанных документах (с некоторыми различиями) приводится совокупность требований к набору и содержанию защитных функций, выполнение которых должно обеспечить «защищенность» создаваемых систем от известных на момент создания документов угроз случайного и преднамеренного характера. Данную технологию можно отнести к способу построения защиты. Полнота выполнения упомянутых требований оценивается экспертами и определяет класс «защищенности» по стандарту. Чем больше количество функций и сложнее их выполнение, тем выше класс.

Однако такому подходу и способу присущи принципиальные недостатки, приводящие к низкому уровню безопасности обрабатываемой информации. Суть их заключается в неопределенности постановки задачи и вытекающей из нее сложности ее решения. В разрабатываемой системе сложно определить:

- предмет защиты (множество «объектов» доступа);
- виды и количество угроз;
- «субъекты» доступа (множество процессов);
- возможные механизмы взаимодействия «субъектов» с «объектами» (в стандартах отсутствует физическая «привязка» функций защиты к видам автоматизированных систем).

Если число штатных «объектов» и «субъектов» (кроме процессов) доступа на конкретной системе можно как-то еще определить, то виды и количество процессов, преднамеренных несанкционированных и случайных воздействий, особенно в региональных, глобальных сетях учету не поддаются. Проверить стойкость защиты по каждой ожидаемой угрозе вообще не представляется возможным.

Особенно следует отметить невозможность объективной оценки степени приближения полученных результатов прочности защиты к истинному значению, так как в стандартах отсутствует механизм создания замкнутой защитной оболочки и расчетных соотношений ее прочности. Отсутствие механизма создания защитной оболочки приводит к наличию «дыр» в защите, а отсутствие расчетных соотношений прочности – к существенному отклонению точности получаемых результатов оценки ожидаемой эффективности защиты.

Создаваемая защитная среда носит сугубо фрагментарный характер, так как не определяются ее границы и плотность. На практике защитная среда реализуется в виде определенного нормативными документами набора функций, в котором отсутствуют количественные показатели прочности защиты и используется «лукавый» термин «защищенность». Данные функции определены лишь на основе опыта работы режимных служб. Достаточность

набора и уровня исполнения этих функций для обеспечения защиты нигде и никем не доказана.

При отсутствии необходимых функций защиты наблюдаются избыточные функции. С позиций предлагаемой в данной работе концепции, например в [12], по мнению автора данной книги, избыточными функциями являются:

- «мандатный доступ», так как он значительно усложняет проектирование и работу системы, а для защиты малоэффективен, если он необходим, его можно реализовать при задании дискреционного доступа;
- «взаимодействие пользователя с комплексом средств защиты» по причине сложности его проверки на СВТ и необходимости его реализации на этапе создания АС в рамках разграничения доступа.

«Гарантии архитектуры» и «требования к документации» функции защиты не выполняют и имеют отношение только к качеству ее изготовления, те же требования можно предъявить ко всей создаваемой системе обработки информации.

В некоторых классах защищенности автоматизированных систем, приведенных в [12], отсутствует требование сигнализации о НСД, а там, где оно указано, отсутствует самый важный параметр – время доведения сигнала. Период просмотра результатов регистрации события не задан. В подсистеме обеспечения целостности отсутствуют период контроля, в классах 1Д и 1Г отсутствует администратор безопасности или должностное лицо, исполняющее его обязанности, и т.д. Перечень недостатков, вытекающих из примененной концепции в нормативных документах, можно продолжить.

Исходя из изложенного, можно сделать вывод о том, что в основу проектирования защиты уже закладываются пути ее обхода, и может случиться, что получение сертификата о наличии защиты не означает, что она есть.

Следствием такого подхода являются также противоречия и различное толкование основных терминов и определений, появление которых в некоторых работах и нормативных документах при отсутствии работающей единой и общепринятой теории безопасности информации можно считать преждевременным (например, термины «защищенная СВТ», «защищенная АС», «защищенная сеть»). Под этими терминами обычно понимается создание вокруг СВТ, АС, сети защитной оболочки. Но это, как известно, поставленной задачи не решает и не всегда возможно (например, в глобальной сети и АСУ). Кроме того, как показала практика, основной задачей защиты информации является защита от нарушителей-пользователей. Они обладают определенными полномочиями и имеют доступ к информации и ресурсам внутри автоматизированной системы, т.е. указанные термины не соответствуют своему значению. Поэтому целесообразно при их определении сделать акцент на безопасной обработке информации как внутренних свойствах АС, таких, как надежность и устойчивость ее функционирования. В этих случаях термин «безопасная АС» будет выглядеть предпочтительнее.

Защищенной СВТ в принципе быть не может, так как СВТ согласно определению действующего стандарта [12] не является законченной автоматизированной системой. В этой связи отметим некорректность применения термина «защищенная СУБД» и других подобных терминов, применяемых к элементам вычислительной техники, не имеющих самостоятельного применения.

Подобные средства, содержащие какой-либо набор средств защиты, до применения их в АС не могут называться защищенными, так как информация, подлежащая защите, в СВТ появляется лишь после его установки. О завершении создания защиты можно говорить лишь тогда, когда в данной АС создана и принята заказчиком система безопасности информации, жестко связанная с определенной информационной технологией, с ее индивидуальной обработкой и управлением в организации-потребителе. Изложенное выше позволяет сделать вывод о нецелесообразности выпуска стандарта по СВТ и необходимости проведения сертификации средств защиты по техническим условиям их разработчика. Потребительские свойства средств защиты оценил разработчик АС, выбрав такие из них, которые позволят ему построить защиту информации, отвечающую требованиям технического задания и стандарта на АС.

Возвращаясь к предмету защиты и термину «информационные ресурсы», напомним, что под ресурсами согласно энциклопедическому словарю (М.: Русский язык, 1985) понимаются запасы чего-либо: объемов памяти, времени функционирования, быстроедействия и т.д. В работе [40] в состав ресурсов включены все компоненты вычислительной сети, ее аппаратное и программное обеспечение, а также процедуры, протоколы, управляющие структуры и т.п. В «Толковом словаре по вычислительной технике и программированию» А.П. Заморина и А.С. Маркова (М.: Русский язык, 1987) под информационными ресурсами понимается «информация, которая представляет ценность для предприятия и может быть оценена подобно материальным ресурсам». Как видно, добавление к слову «ресурсы» прилагательного меняет его первоначальный смысл. Поскольку уже существует нормальное выражение нового смысла в старом слове «информация», то предлагается его и применять, чтобы строго и четко обозначить предмет защиты и чтобы больше не появлялись такие выражения, как «тело обозначения ресурса» и «данные, вводимые пользователем, передаются как тело ресурса» (Computerworld. – №4, 26.09.95, с. 22). Однако это абсолютно не означает, что при решении задачи защиты информации не потребуются защита ресурсов вычислительной системы, но только в тех случаях, когда информацию непосредственно защитить сложно и когда защита ресурсов вычислительной системы существенно повышает уровень ее безопасности. Наконец, решающим аргументом в пользу изложенного является тезис: информация – это категория собственности, право владельца на которую мы защищаем (см. подразд. 1.1.6).

3.2. Выбор концептуальной модели построения защиты

Вспомним, что решение любой проблемы в науке и в повседневной жизни начинается с поиска уже готовых решений в похожих ситуациях. В нашем случае такое решение известно всем: для защиты какого-либо ценного пред-

мета вокруг него сооружается некая физическая и (или) интеллектуальная замкнутая преграда, преодоление которой в достаточной мере не по силам потенциальному нарушителю. Этот принцип используется, например, в системах охранной сигнализации вокруг локальной вычислительной сети. Но дальше в самой вычислительной сети принцип создания защитной оболочки реализовать не удалось по указанным выше причинам.

Однако такая возможность существует, если изменить подход к постановке задачи – внести определенность в ответы на вопросы: 1) Что? 2) Где? 3) От чего? 5) От кого? 6) Когда подлежит защите? Предполагаемый дальнейший путь к решению задачи заключается в представлении множества автоматизированных систем и комплексов типовыми структурами, разработке сначала для них общих методов и решений, а затем уже – и для более сложных структур.

Ответ на первый вопрос дан в подразд. 1.1, на второй – в подразд. 1.2, на третий и четвертый – в подразд. 1.3. На пятый и шестой вопросы ответы можно найти на этапах создания и эксплуатации АС. Это разные задачи и разные решения. Специалисты эти задачи, к сожалению, часто объединяют.

Проблема безопасности информации охватывает широкий спектр автоматизированных систем ее обработки: от персонального компьютера и больших вычислительных комплексов до глобальных вычислительных сетей и АСУ различного назначения. Наряду с известными и необходимыми для выполнения своих прямых задач характеристиками, такими, как надежность функционирования, устойчивость к внешним воздействиям и скорость обработки данных, каждая из этих систем должна обеспечивать гарантированную безопасность обрабатываемой информации. Как показал накопленный опыт, данная характеристика или свойство системы по своему значению не уступает приведенным характеристикам и часто даже *превосходит* их. Это видно хотя бы из того, что при отказе функционирования системы ценная информация в ней должна быть сохранена, т.е. не должна претерпеть никаких изменений, не быть разрушенной или похищенной и не быть доступной посторонним лицам.

Быстрое развитие и совершенствование информационных технологий повлияло и на представления специалистов о классификации автоматизированных систем. В настоящее время у них пока еще не сложилось единого мнения по этому вопросу. В данной книге *под автоматизированными системами* понимается широкий класс аппаратно-программных структур, обеспечивающих с помощью вычислительной техники с заданными требованиями и в заданных условиях возможность автоматизированного ввода (вывода), хранения, обработки и передачи данных с обеспечением их целостности, подлинности, недоступности посторонним лицам.

Принципиально важным моментом постановки задачи в общем виде с позиций построения защиты является выбор такой *модели автоматизированной системы обработки информации*, которая позволила бы ожидаемые результаты ее решения распространить на частные случаи построения любой автоматизированной системы: от автоматизированного рабочего места до глобальной АС независимо от аппаратной и программной платформ, на базе которых они построены.

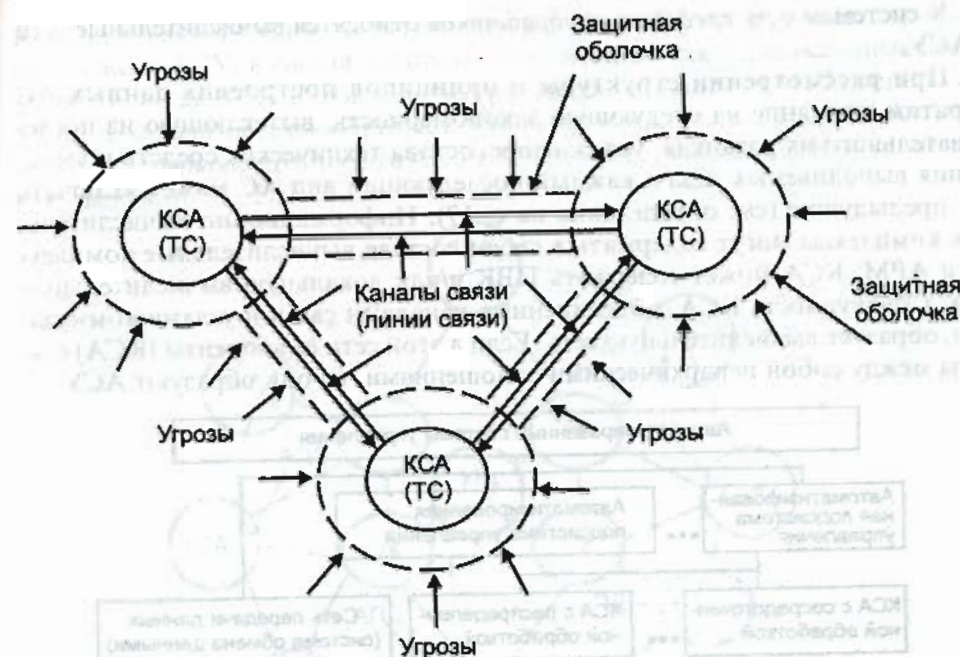


Рис. 3.2. Модель защиты информации по предлагаемой концепции:
КСА – комплекс средств автоматизации обработки информации;
ТС – техническое средство обработки информации

В целях выработки общего подхода к решению этой задачи для всех видов АС рассмотрим их классификацию по видам (рис. 3.2), принципам построения, приведенную в обобщенной структуре АСУ (рис. 3.3), а также схемы сетей, приведенные на рис. 1.4, 1.5, 1.26 и 1.27.

Анализ принципов построения и классификации автоматизированных систем, приведенных на рисунках, позволяет их условно разделить на два вида: с сосредоточенной и распределенной обработкой данных.

АС с *сосредоточенной обработкой* будем считать такие системы, в которых информация обрабатывается на одном обрабатывающем центре.

Системами с *распределенной обработкой* данных называем такие системы, в которых обработка информации распределена по нескольким узлам объекта автоматизации – элементам этой системы, которые связаны между собой локальной вычислительной сетью передачи данных или территориальной сетью обмена данными.

К системам с *сосредоточенной обработкой* относятся также КСА, технические средства которого территориально размещаются на одном объекте автоматизации на контролируемой его владельцем территории. К ним также относим структуры с централизованной обработкой данных: информационно-вычислительные комплексы (ИВК), узлы коммутации (УК) сообщений и пакетов, рабочие станции (РС), автоматизированные рабочие места (АРМ) и вспомогательные технические средства: вычислительные комплексы, серверы, маршрутизаторы, концентраторы, коммутаторы и др.

К системам с *распределенной обработкой* относятся вычислительные сети и АСУ.

При рассмотрении структуры и принципов построения данных АС обратим внимание на следующую закономерность, вытекающую из последовательного их развития, усложнения состава технических средств и умножения выполняемых задач: каждый последующий вид АС может включать все предыдущие (см. определения на с. 17). Информационно-вычислительные комплексы могут содержать в своем составе вычислительные комплексы и АРМ; КСА может содержать ИВК и/или локальную вычислительную сеть. Совокупность КСА, объединенных каналами связи и узлами коммутации, образует вычислительную сеть. Если в этой сети ее абоненты (КСА) связаны между собой иерархическими отношениями, то они образуют АСУ.



Рис. 3.3. Обобщенная структура автоматизированной системы управления:

АС с распределенной обработкой данных:
АСУ, АПУ, СПД, ЛВС, КСА с распределенной обработкой

Таким образом, комплекс средств автоматизации с позиций безопасности информации можно рассматривать как некий базовый элемент вычислительной сети и АСУ. Для решения поставленной задачи представляется целесообразным рассмотреть сначала структуру с сосредоточенной и распределенной обработкой данных. При этом в качестве первой выделим комплекс средств автоматизации (КСА) с сосредоточенной обработкой данных, а вторую представим в виде АС, обобщенная схема которой представлена на рис. 3.4, как их совокупность, объединенная каналами связи, где с позиций обеспечения безопасности не важен характер штатной обработки информации в

КСА и узел коммутации рассматриваем в статусе «КСА». В данном варианте изображена АСУ, в состав которой могут входить все перечисленные выше виды АС и где КСА (УК), аппаратура передачи данных (АПД) остальных КСА_{асу} с каналами связи образуют сеть передачи данных (СПД), КСА_{асу}(УК) является управляющим звеном АСУ (СПД), остальные КСА(УК) – управляемые звенья АСУ(СПД).

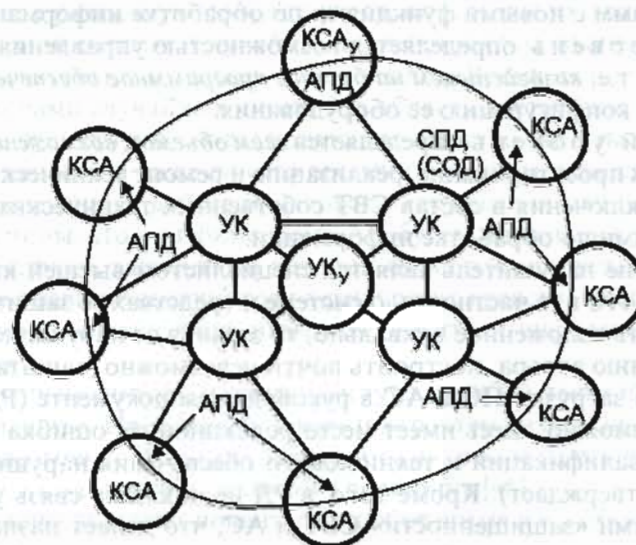


Рис. 3.4. Обобщенная функциональная схема АСУ:

АПД – аппаратура передачи данных; УК – управляющий узел коммутации;
КСА – комплекс средств автоматизации; СПД – сеть передачи данных

Локальную вычислительную сеть можно представить как совокупность технических средств, объединенных линиями связи.

Изложенное позволяет с позиций проектирования защиты информации АС построить **концептуальную модель защиты**, приведенную на рис. 3.2.

Данная модель помогает, как будет показано ниже, реализовать общий подход к разработке методов обеспечения безопасности информации сначала в АС с сосредоточенной обработкой данных (технических средствах, КСА), а затем развить и распространить его на АС с распределенной обработкой (вычислительные сети и АСУ).

3.3. Исходные данные для постановки задачи

Согласно действующей концепции [12] случайные и преднамеренные угрозы с позиций безопасности информации рассматриваются как один поток событий. Однако для защиты от преднамеренных угроз приводится модель нарушителя, являющегося законным пользователем. Нарушители классифи-

цируются по уровню возможностей, предоставляемых им штатными средствами. Выделяются четыре уровня таких возможностей.

«Первый уровень»¹ определяет самый низкий уровень возможностей ведения диалога в АС – запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.

Второй уровень определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации.

Третий уровень определяется возможностью управления функционированием АС, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования.

Четвертый уровень определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации.

В своем уровне нарушитель является специалистом высшей квалификации, знает все об АС и, в частности, о системе и средствах ее защиты».

Если понимать изложенное буквально, то защиту от нарушителей 2–4-го уровней, по мнению автора, построить почти невозможно (защита от несанкционированной загрузки ПО в АС в руководящем документе (РД) не предусмотрена). Возможно, здесь имеет место редакционная ошибка и имелись в виду уровни квалификации и технического обеспечения нарушителей (но п. 4.3 это не подтверждает). Кроме того, в РД не показана связь указанных уровней с классами «защищенности» СВТ и АС, что делает назначение такой классификации непонятной.

Учитывая изложенное, в данной работе предлагается другой подход.

Угрозы информации определяются условиями сохранения права собственности на нее (см. подразд. 1.1). Это утечка, модификация и утрата информации. При этом под *утечкой* информации понимается несанкционированное ознакомление с ней постороннего лица; под *модификацией* – несанкционированное изменение информации на корректную по форме и содержанию, но другую по смыслу; под *утратой* – хищение, искажение с потерей смысла, уничтожение, недоведение информации до адресата или блокировка доступа к ней ее владельца и его доверенного лица.

Все остальные угрозы – это способы достижения целей, которые в конечном итоге сводятся к этим трем событиям. Эти события могут произойти случайно по причине ошибок пользователя, сбоев или отказов аппаратуры, алгоритмических или программных ошибок, аварийных ситуаций, стихийных бедствий и других или созданы нарушителем преднамеренно. Техника исполнения последних имеет множество вариантов.

Нарушителем может быть человек: посторонний; законный пользователь или из числа лиц обслуживающего персонала. Квалификация его также может быть различной. Он может обладать и не обладать определенным набором технических средств, работать в комфортных условиях или в условиях риска; быть пойманным; быть единственным или в составе организованной группы, имеющей доступ к компьютерной системе. Не следует впадать в дру-

¹ Разрядка автора книги.

гую крайность – считать всех, работающих с системой, потенциальными нарушителями. Круг доверенных лиц, очевидно, будет зависеть от важности обрабатываемой информации и выполняемых задач. В эти исходные данные тоже следует внести определенность. Такими лицами должны быть по меньшей мере системные администраторы, руководители работ и должностные лица службы безопасности.

Учитывая различную природу угроз, определим их точки приложения к проектируемой системе. Случайные воздействия (см. выше) возможны в любой точке системы, т.е. на всей ее «площади». Время их наступления определяется законами случайных чисел. Эта область достаточно хорошо исследована и уже существуют соответствующие средства защиты и методы оценки их эффективности и даже до сего времени действует отраслевой стандарт.

Преднамеренные действия человека-нарушителя начинаются на «периметре» системы. Под «периметром» АС будем понимать ее внешнюю физическую оболочку, элементами которой являются корпуса, крышки, дверцы, свободные внешние соединители технических средств, средства управления, отображения, печати, ввода и вывода, носители информации и кабельные соединения.

Нарушением считаем попытку доступа к любой части информации, подлежащей защите. Предсказать время и характер возможных действий нарушителя невозможно. Поэтому целесообразно рассмотреть наиболее опасную для системы модель его возможного поведения [48]:

- а) нарушитель может появиться в любое время и в любой точке «периметра» системы;
- б) для достижения своей цели он выберет наиболее слабое звено в защите;
- в) квалификация и осведомленность нарушителя будет соответствовать важности защищаемой информации;
- г) постоянно хранимая информация о принципах работы системы, включая секретную, нарушителю известна;
- д) нарушителем может быть не только постороннее лицо, но и законный пользователь системы.

К перечисленным условиям целесообразно добавить не самую опасную ситуацию, когда нарушитель действует один без сообщников, имеющих доступ к данной системе. Защита от организованной группы нарушителей – значительно более сложная задача, решить которую можно, решив только более простую. Однако это не означает, что если последняя будет решена, то она не будет работать против группы не связанных между собой нарушителей. Поэтому дополним:

- е) нарушитель действует в единственном числе, однако их может быть несколько, но действия их не согласованы между собой.

Примечание. На неконтролируемых средствах защиты возможные действия организованной группы нарушителей все же будут учтены в расчетных соотношениях, будет рассмотрена в этом направлении также и прочность контролируемых средств.

Из данных условий вытекают следующие исходные положения:

1. Согласно п. «а» вокруг предмета защиты необходимо строить замкнутую оболочку (контур) защиты.

2. Согласно п. «б» прочность защиты определяется ее слабым звеном.
3. Согласно п. «в» прочность защиты должна соответствовать квалификации нарушителя.
4. Согласно п. «г» информация для входа в систему должна быть переменной.
5. Согласно п. «д» при наличии множества пользователей необходимо обеспечить разграничение доступа.

Риск нарушителя, очевидно, определится величиной вероятности обнаружения его действий. Однако для различных по назначению, виду и ценности обрабатываемой информации в АС «опасная» квалификация нарушителя будет также отличаться.

На основании изложенного в выборе исходной модели потенциального нарушителя целесообразен дифференцированный подход в соответствии с назначением АС и ценностью информации, обрабатываемой в ней. Поскольку модель нарушителя – понятие относительное и приближенное, предлагается за основу принять пока всего четыре класса потенциальных нарушителей:

- 1) высококвалифицированный нарушитель-профессионал (специалист по вычислительной технике, специально подготовленный к несанкционированному доступу к информации);
- 2) квалифицированный нарушитель – непрофессионал (специалист по вычислительной технике, не подготовленный к несанкционированному доступу к информации);
- 3) неквалифицированный нарушитель-непрофессионал;
- 4) прочие нарушители.

В соответствии с данной классификацией предлагается ввести и классификацию уровней безопасности информации в создаваемых АС.

I класс рекомендуется для защиты жизненно важной информации, утечка, модификация или утрата которой могут привести к невосполнимым потерям для ее владельца. Прочность защиты должна быть рассчитана на нарушителя-профессионала.

II класс рекомендуется использовать для защиты важной информации, утечка, модификация или утрата которой может привести к значительным потерям для ее владельца. Прочность защиты должна быть рассчитана на нарушителя высокой квалификации, но не на взломщика-профессионала.

III класс рекомендуется для защиты относительно ценной информации, утечка, модификация или утрата которой может привести к незначительным потерям для ее владельца или постоянный несанкционированный доступ к которой путем ее накопления может привести к утечке и более ценной информации. Прочность защиты при этом должна быть рассчитана на относительно квалифицированного нарушителя-непрофессионала.

IV класс рекомендуется для защиты прочей информации, не представляющей интереса для серьезных нарушителей. Однако необходимость его диктуется соблюдением технологической дисциплины учета и обработки информации служебного пользования в целях защиты от случайных нарушений и подстраховки от случаев преднамеренного несанкционированного доступа.

Очевидно, что количество возможных каналов НСД в АС для нарушителей различных классов тоже будет различным.

Реализация перечисленных уровней безопасности должна обеспечиваться совокупностью средств защиты, перекрывающих возможные каналы НСД

в АС со стороны ее «периметра» в количестве, соответствующем ожидаемой модели поведения потенциального нарушителя. Данная совокупность средств, связанных расчетными соотношениями прочности, должна образовывать виртуальную оболочку защиты. Уровень безопасности защиты внутри класса должен обеспечиваться количественной оценкой прочности защитного контура (оболочки) защиты.

В связи с тем что в технической литературе специалисты часто объединяют совершенно разные задачи: защиту информации в процессе проектирования системы и задачу проектирования самой защиты, считаем, что в данной работе рассматривается проблема создания встроенной в автоматизированную систему защиты, которая должна работать с момента эксплуатации системы потребителем. При этом допускаем, что на этапе ее проектирования, изготовления и испытаний обеспечивается режим ограничения и разграничения доступа к документации, программному обеспечению и аппаратуре; *несанкционированные аппаратные и программные закладки отсутствуют*. Однако это не означает, что при эксплуатации защита от последних построена не будет. Кроме того, считаем, что в законченной и годной к эксплуатации автоматизированной системе обработки информации *должны отсутствовать средства программирования и отладочные средства* за исключением тестовых программ, предусмотренных конструкторской документацией на эту систему. Всякие доработки АС без проведения испытаний и согласования с главным конструктором во время ее эксплуатации недопустимы. Недопустимо также использование АС для целей и задач, не предусмотренных ее техническими условиями. Несоблюдение данных требований лишает потребителя всех гарантий на нормальное функционирование системы, включая обеспечение безопасности информации.

3.4. Основы теории построения защиты информации

3.4.1. Введение в проблему теории защиты информации

Анализ технической литературы и работ специалистов в области защиты информации в автоматизированных системах ее обработки показывает, что вопросам теории было посвящено достаточно много научных трудов. Наиболее полно они обобщены и систематизированы в отечественных работах [22, 25, 71, 82]. Данные работы опираются на работы зарубежных специалистов – теоретические модели безопасности: АДЕПТ-50 Хартсона, Бела-Лападулы, MMS Лендвера и Мак-Лина, Биба, Кларка-Вилсона и др. Как было показано во введении к книге, практического применения по причине неопределенности постановки задачи, отсутствия механизма создания защитной оболочки и высокого уровня абстракции данные модели не нашли.

Попытки разработки новой теории защиты отечественными специалистами приведены в работах [8, 15, 58].

В [15] предложен формальный подход к решению задачи, отличающийся от приведенных, но постановка задачи по своей сути осталась прежней, в результате были получены другие расчетные соотношения, которые, как оказалось, так же далеки от практического использования. В [8] рассмотрен вопрос периода замены пароля и предложена несколько иная модель нарушителя, в которой преднамеренный несанкционированный доступ считается случайным процессом и период контроля событий не учитывается, что приводит к результатам, не соответствующим полной картине событий и неточным выводам. В [58] предлагается схема моделирования, использующая абстрагирование для упрощения анализа системы защиты с учетом деталей ее поведения. Представленный в этой работе подход использует модель машины состояний (ИМС) со свойством выводимости, приведенной в книге [7] Бела и Лападулы (1974 г.). Однако по выводу самого автора учесть факт физического нарушения безопасности в рамках ИМС не удается.

По причинам сложности и высокого уровня абстракции приведенных теорий и моделей построить защиту и получить количественные показатели ее прочности на их основе в конкретных системах до настоящего времени не удалось. Разработчику при проектировании системы приходится руководствоваться стандартами [12, 14, 29, 31, 34, 64, 73, 68], в которых задан лишь набор защитных функций и сформулированы требования к их реализации. Научное обоснование достаточности этого набора никем и нигде не проведено. Количество указанных функций и полнота выполнения требований являются критерием экспертной оценки соответствия защиты тому или иному классу. Методики оценки в указанных стандартах отсутствуют. Такие критерии и методы оценки обладают весьма низкой точностью результата. Кроме того, как было показано во введении к данной книге, стандартный набор требований, построенный на базе концепции защиты вычислительной среды, имеет фрагментарный характер, т.е. не содержит механизма создания замкнутой защитной оболочки, что с самого начала существенно снижает прочность защиты.

Предлагаемый в данной работе вывод расчетных соотношений опирается на новую модель защиты, постановку задачи, приведенную в подразд. 3.1, а также на новый подход и принципы.

В конечном итоге сегодня специалисты вынуждены признать, что формальные подходы к решению задачи оценки защищенности из-за трудностей, связанных с формализацией, широкого распространения не получили¹.

3.4.2. Общий методический подход

Общий подход к построению защиты отражает ее модель, приведенную на рис. 3.2. Данная модель защиты в обобщенном виде содержит функциональные элементы АС и возможные средства взаимодействия между ними (на уровне АС: КСА – каналы связи, на уровне ЛВС: технические средства –

¹ См.: Астахов А. Анализ защищенности корпоративных систем // Открытые системы. – 2002. – № 7–8.

линии связи), она также отражает концептуальный подход к построению защиты. Анализ модели и функциональной схемы АС (см. рис. 3.4) объясняет выбор при постановке задачи объектов исследования: КСА с сосредоточенной и АС с распределенной обработкой данных.

Безопасность информации в АС заключается в создании на время эксплуатации таких условий автоматизации ввода (вывода), хранения, обработки и передачи информации, при которых в достаточной степени гарантируется защита ее от утечки, модификации и утраты, а также свободный доступ к ней только ее владельца и его доверенных лиц.

По причине различной природы и законов происхождения случайных и преднамеренных событий, связанных с НСД к информации, методы и средства их контроля и предупреждения тоже различны (см. подразд. 1.3). Это средства повышения надежности функционирования автоматизированных систем, средства повышения достоверности и резервирования информации. Для защиты информации от случайных воздействий анализируется достаточность и ожидаемая эффективность этих средств по [35, 39, 66, 79, 83].

При проектировании защиты от *преднамеренного* НСД выполняется *определенная последовательность* действий, вытекающих из указанной выше постановки задачи.

Определяются *перечень и классификация по характеру, размещению, важности и времени жизни данных*, подлежащих защите в заданной АС. В соответствии с характером и важностью этих данных выбирается ожидаемая квалификация и модель поведения *потенциального нарушителя*.

В соответствии с моделью нарушителя в проектируемой системе выявляются виды и количество *возможных каналов несанкционированного доступа* (ВК НСД) к защищаемым данным. Данные каналы делятся на технически контролируемые и неконтролируемые. Например, вход в систему со стороны клавиатуры терминала может контролироваться специальной программой, а каналы связи территориально-распределенной системы – не всегда. На основе анализа каналов выбираются готовые или создаются новые средства защиты с целью их *перекрытия*.

С целью создания *единого постоянно действующего механизма* защиты указанные средства защиты с помощью специально выделенных средств централизованного управления объединяются в одну автоматизированную *систему безопасности информации* (СБИ), которая путем анализа ее состава и принципов построения проверяется на предмет наличия возможных путей ее обхода. Если таковые обнаруживаются, то они перекрываются соответствующими средствами, которые также включаются в состав защитной оболочки.

3.4.3. Основные принципы построения защитной оболочки

При расчете прочности средства защиты, выбранного для перекрытия возможного канала НСД к информации АС, путем анализа принципов его построения определяется возможность путей его обхода. Если таковые имеются, то данное средство дорабатывается. Если путь его обхода перекрывается другим средством, переходим к расчету прочности последнего и так до тех пор,

пока не будет обеспечено полное перекрытие всех возможных каналов НСД и путей обхода средств защиты в создаваемой системе. В результате в ней таким образом будет построена замкнутая виртуальная оболочка защиты информации [42].

Степень защиты определяется полнотой перекрытия этих каналов и возможных путей обхода средств защиты, а также прочностью защиты. Согласно принятой модели поведения нарушителя прочность защитной оболочки определяется прочностью средства защиты с наименьшим значением из числа средств, составляющих эту оболочку [42].

Под прочностью защиты (преграды) понимается величина вероятности ее преодоления нарушителем [42].

Прочность защитной преграды является достаточной, если ожидаемое время преодоления ее нарушителем больше времени жизни предмета защиты или больше времени обнаружения и блокировки его доступа при отсутствии путей обхода этой преграды.

Защитная оболочка должна состоять из средств защиты, построенных по одному принципу (контроля или предупреждения НСД) и размещаемых на каналах НСД одного типа (технически контролируемых или неконтролируемых). На контролируемых каналах нарушитель рискует быть пойманным, а на неконтролируемых – он может работать в комфортных условиях, не ограниченных во времени и средствах. Прочность защиты во втором случае должна быть значительно выше. Поэтому целесообразно в автоматизированной системе иметь отдельные виртуальные защитные оболочки: контролируемую и превентивную [42].

Кроме того, необходимо учитывать применение организационных мероприятий, эффективность которых имеет место и которые в своей совокупности могут образовать свою защитную оболочку. Однако, учитывая ее низкую по отношению к технической оболочке эффективность, в ответственных системах рекомендуется ее применять только в качестве дублирующей.

Стратегия и тактика защиты от преднамеренного НСД заключается в применении на возможных каналах НСД к информации АС средств контроля, блокировки и предупреждения событий. Средства контроля и блокировки устанавливаются на возможных каналах НСД, на которых это возможно технически или организационно, а средства предупреждения (превентивные средства) применяются там, где такие возможности отсутствуют.

При расчете прочности средства защиты используется временной фактор, позволяющий получить количественную оценку его прочности – ожидаемую величину вероятности преодоления средства потенциальным нарушителем [42]. Метод расчета и получения этой величины приведен ниже.

На приведенных выше исходных данных, постановке задачи, положениях и принципах основывается вывод нижеприведенных расчетных соотношений для прочности отдельных средств и оболочек защиты информации в АС.

3.4.4. Модель элементарной защиты

Вывод общих расчетных соотношений. В общем случае простейшая модель элементарной защиты любого предмета может быть в виде, представленном на рис. 3.5.



Рис 3.5. Модель элементарной защиты

Предмет защиты помещен в замкнутую однородную защитную оболочку, называемую преградой. Прочность защиты зависит от свойств преграды. Принципиальную роль играет способность преграды противостоять попыткам преодоления ее нарушителем. Свойство предмета защиты – способность привлекать его владельца и потенциального нарушителя. Привлекательность предмета защиты заключается в его цене. Это свойство предмета защиты используется при оценке защищенности информации в вычислительных системах. При этом считается, что прочность созданной преграды достаточна, если стоимость ожидаемых затрат на ее преодоление потенциальным нарушителем превышает стоимость защищаемой информации. Однако оценка того и другого оказалась непростой задачей, и до настоящего времени не существует какой-либо универсальной методики ее проведения на практике для конкретных вычислительных систем. Поэтому в данной работе предлагается другой подход.

Если обозначить вероятность преодоления преграды нарушителем через $P_{сзн}$, вероятность преодоления преграды нарушителем через $P_{пр}$, то согласно теории вероятности [11] сумма вероятностей двух противоположных событий равна 1, т.е. $P_{сзн} + P_{пр} = 1$. Отсюда $P_{сзн} = (1 - P_{пр})$.

В реальном случае у преграды могут быть пути ее обхода. Обозначим вероятность обхода преграды нарушителем через $P_{обх}$. Нарушитель, действующий один, выберет один из путей: преодоление преграды или обходной вариант. Тогда, учитывая несовместимость событий, формальное выражение для прочности преграды можно представить в виде

$$P_{сзн} = \min\{(1 - P_{пр}), (1 - P_{обх})\}.$$

Выбор прямого или обходного пути будет зависеть от трудностей, которые ожидают нарушителя на каждом из них. В целях подстраховки мы выберем наиболее опасный случай, когда нарушитель знает и выберет наиболее легкий путь, т.е. путь с наибольшей вероятностью преодоления его трудностей. Какой из них? – ответ зависит от конкретной реализации преграды. Это обстоятельство позволяет предположить, что прочность преграды определяется вероятностью ее преодоления или обхода потенциальным нарушителем по пути с наибольшим значением этой вероятности. Другими словами: в случае единственного нарушителя прочность защиты определяется ее слабейшим звеном.

Логично предположить, что у преграды может быть несколько путей обхода. Тогда последнее выражение примет вид

$$P_{сзн} = \min\{(1 - P_{пр}), (1 - P_{обх1}), (1 - P_{обх2}), (1 - P_{обх3}), \dots, (1 - P_{обхk})\}, \quad (3.1)$$

где k – количество путей обхода.

Для случая, когда нарушителей более одного и они действуют одновременно (организованная группа) по каждому пути, это выражение с учетом совместимости событий будет выглядеть как

$$P_{\text{сзн}} = (1 - P_{\text{нр}}) (1 - P_{\text{обх1}}) (1 - P_{\text{обх2}}) (1 - P_{\text{обх3}}) \dots (1 - P_{\text{обхk}}). \quad (3.2)$$

В этом случае прочность преграды будет определяться произведением результатов вычитания из единицы значений вероятностей доступа нарушителей к предмету защиты по каждому возможному пути преодоления этой преграды.

Расчетные соотношения для контролируемой преграды. Когда к предмету защиты, имеющему постоянную ценность, необходимо и технически возможно обеспечить контроль доступа, обычно применяется постоянно действующая преграда, обладающая свойствами обнаружения и блокировки доступа нарушителя к предмету или объекту защиты. В качестве такой защиты могут быть применены человек, специальная или встроенная в АС автоматизированная система контроля под управлением человека.

Принцип работы автоматизированной преграды основан на том, что в ней блоком управления производится периодический контроль датчиков обнаружения нарушителя. Результаты контроля наблюдаются человеком на средствах централизованного управления. Периодичность опроса датчиков автоматом может достигать тысячных долей секунды и менее. В этом случае ожидаемое время преодоления преграды нарушителем значительно превышает период опроса датчиков. Поэтому такой контроль часто считают постоянным. Но для обнаружения нарушителя человеком, управляющим автоматом контроля, только малого периода опроса датчиков недостаточно.

Необходимо еще и время на выработку и передачу сигнала тревожной сигнализации на блок отображения средств управления, т.е. время срабатывания автомата, так как оно часто значительно превышает период опроса датчиков и тем самым увеличивает время обнаружения нарушителя. Практика показывает, что обычно сигнала тревожной сигнализации достаточно для приостановки действий нарушителя, если этот сигнал до него дошел. Но поскольку физический доступ к объекту защиты пока еще открыт, дальнейшие действия охраны сводятся к определению места и организации блокировки доступа нарушителя, на что также потребуется время.

Для анализа ситуации рассмотрим временную диаграмму процесса контроля и обнаружения НСД, приведенную на рис. 3.6.

Из рис. 3.6 следует, что нарушитель может быть не обнаружен в двух случаях:

а) когда $t_{\text{нр}} < T$;

б) когда $T < t_{\text{нр}} < T_{\text{обл}}$.

В случае а) требуется дополнительное условие – попадание интервала времени $t_{\text{нр}}$ в интервал T , т.е. необходима синхронизация действий нарушителя с частотой опроса датчиков обнаружения. Для решения этой задачи нарушителю придется скрытно подключить измерительную аппаратуру в момент выполнения несанкционированного доступа к информации, что является довольно сложной задачей для постороннего человека. Поэтому считаем, что свои

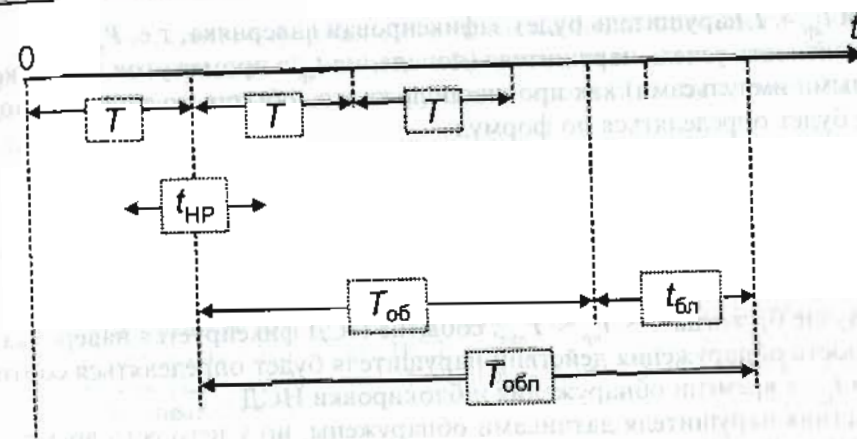


Рис. 3.6. Временная диаграмма процесса контроля НСД:

T – период опроса датчиков; $T_{\text{об}}$ – время передачи сигнала и обнаружения НСД;
 $t_{\text{бл}}$ – время блокировки доступа

действия с частотой опроса датчиков он синхронизировать не сможет и может рассчитывать лишь на некоторую вероятность успеха, выражающуюся в вероятности попадания отрезка времени $t_{\text{нр}}$ в промежуток времени между импульсами опроса датчиков, равный T .

При $t_{\text{нр}} > T$ действия нарушителя наверняка будут зафиксированы датчиком системы контроля.

Формально эту задачу можно представить следующим образом.

Есть бесконечно последовательное множество событий в виде контрольных импульсов с расстоянием T между ними и есть определенное множество элементарных событий в виде отрезка длиной $t_{\text{нр}}$ в тех же единицах времени, который случайным образом накладывается на первое множество. Задача состоит в определении вероятности попадания отрезка $t_{\text{нр}}$ на контрольный импульс, если $t_{\text{нр}} < T$.

Нетрудно заметить, что с увеличением отрезка $t_{\text{нр}}$ вероятность этого события увеличивается, при уменьшении – уменьшается, т.е. имеется прямая зависимость. При увеличении T вероятность попадания отрезка на контрольный импульс уменьшается, при уменьшении T – увеличивается, т.е. имеется обратная зависимость. Если обозначить вероятность попадания отрезка на контрольный импульс через P_{ϕ} (фиксации события в контрольной точке), мы вправе считать, что

$$P_{\phi} = \frac{t_{\text{нр}}}{T}. \quad (3.3)$$

Следует также отметить, что эта формула справедлива также и для организационной меры защиты в виде периодического контроля заданного объекта человеком. При этом полагаем, что обнаружение, определение места НСД и его блокировка происходят в одно время – в момент контроля объекта человеком, т.е. $T_{\text{обл}} = T$, где T – период контроля человеком объекта защиты.

При $t_{\text{пр}} > T$ нарушитель будет зафиксирован наверняка, т.е. $P_{\text{ф}} = 1$.
Вероятность успеха нарушителя (попадания $t_{\text{пр}}$ в промежуток между контрольными импульсами) как противоположного события по теории вероятностей будет определяться по формуле

$$P_{\text{пр}} = 1 - \frac{t_{\text{пр}}}{T}. \quad (3.4)$$

В случае б), когда $T < t_{\text{пр}} < T_{\text{обл}}$, событие НСД фиксируется наверняка, и вероятность обнаружения действий нарушителя будет определяться соотношением $t_{\text{пр}}$, а времени обнаружения и блокировки НСД — $T_{\text{обл}}$.

Действия нарушителя датчиками обнаружены, но у него есть время для завершения своей «работы». Однако этот успех относителен, так как нарушение зарегистрировано и через некоторое время будет определен источник нарушения, а для нарушителя возникает опасность быть пойманным, если он не покинет места нарушения до прибытия группы захвата.

В модели потенциального нарушителя мы условились, что ему известны значения T и $T_{\text{обл}}$. Следовательно, на нарушение он идет, зная о возможной такого рода ситуации, но только при определенных условиях: при доступе к достаточно ценной информации и при значительном превышении времени обнаружения и блокировки над затратами времени на НСД, так как ему необходимо дополнительное время, чтобы скрыться от преследования и иметь запас времени на случай неточности своих расчетов. Величина ожидаемого $t_{\text{пр}}$ в конкретной АС зависит от многих факторов:

- характера поставленной задачи нарушения;
- метода и способа нарушения;
- технических возможностей и квалификации нарушителя;
- технических возможностей автоматизированной системы.

Поэтому можно говорить о вероятностном характере величины $t_{\text{пр}}$ по отношению к $T_{\text{обл}}$. Чем больше время нарушителя, тем больше вероятность его поимки. Чем больше время его обнаружения и блокировки, тем меньше вероятность его поимки. Следовательно, если обозначить вероятность обнаружения и блокировки НСД в этом случае через $P_{\text{обл}}$, целесообразно считать, что

$$P_{\text{обл}} = \frac{t_{\text{пр}}}{T_{\text{обл}}}. \quad (3.5)$$

Вероятность успеха нарушителя будет определяться как противоположное событие:

$$P_{\text{пр}} = 1 - \frac{t_{\text{пр}}}{T_{\text{обл}}}. \quad (3.6)$$

Для более полного формального представления прочности преграды в виде автоматизированной системы обнаружения и блокировки НСД необходимо учитывать надежность ее функционирования и пути возможного обхода ее нарушителем.

Вероятность отказа системы определяется по известной формуле

$$P_{\text{отк}}(t) = e^{-\lambda t}, \quad (3.7)$$

где λ — интенсивность отказов группы технических средств, составляющих систему обнаружения и блокировки НСД;

t — рассматриваемый интервал времени функционирования системы обнаружения и блокировки НСД.

Исходя из наиболее опасной ситуации, считаем, что отказ системы контроля и НСД могут быть совместимыми событиями. Поэтому с учетом этой ситуации формула прочности контролируемой преграды (3.2) примет вид

$$P_{\text{сник}} = \min \{ P_{\text{обл}} (1 - P_{\text{отк}}), (1 - P_{\text{обл}1}), (1 - P_{\text{обл}2}), \dots, (1 - P_{\text{обл}k}) \}, \quad (3.8)$$

где $P_{\text{обл}}$ и $P_{\text{отк}}$ определяются соответственно по формулам (3.5) и (3.7).

$P_{\text{обл}}$ и количество путей обхода k определяются экспертным путем на основе анализа принципов построения конкретной системы контроля и блокировки НСД. Поскольку нашей задачей является не разработка этой системы, а лишь ее методологии, ограничимся отдельными типовыми примерами.

Например, для аппаратной схемы контроля контактных датчиков, приведенной на рис. 3.7, одним из возможных путей обхода может быть отключение устройства контроля путем преднамеренного обрыва цепи датчика Д1 или короткого замыкания цепи датчика Д2. В данных случаях очевидно, что $P_{\text{обл}} = 1$. Специалисты это знают и рекомендуют в этих случаях скрытые установки датчиков и прокладку цепей, а также механическую защиту, например металлическую трубу. Оценка $P_{\text{обл}}$ в этом случае проводится экспертным путем на основе анализа конструкции защиты. Такая защита рассчитана на не квалифицированного нарушителя-непрофессионала.

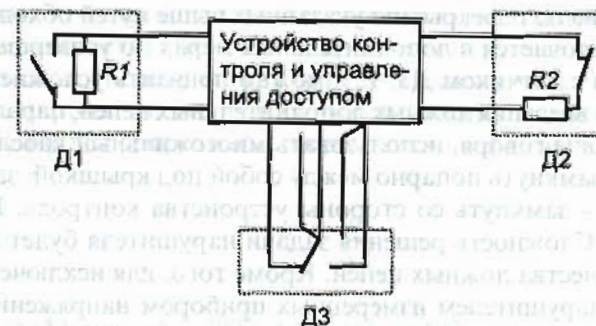


Рис. 3.7. Варианты схем подключения датчиков контроля

Значения $P_{обх1}, P_{обх2}, \dots, P_{обхk}$ в этом случае определяются в пределах от 0 до 1 экспертным путем на основе опыта специалистов. При экспертной оценке вероятности наступления того или иного события ($P_{пр}$, $P_{обх}$ и т.д.) предлагается в целях унификации метода принять за основу следующие градации значений:

$P = 0$ – событие невозможно;

$P = 0,2$ – событие маловероятно;

$P = 0,5$ – событие вероятно наполовину;

$P = 0,8$ – событие вполне вероятно;

$P = 0,95$ – вероятность события высокая;

$P \approx 1$ – событие произойдет наверняка.

Более высокая защита от нарушителя такого же уровня получится при применении датчика ДЗ. Это позволит получить точные значения вероятностей обхода системы. Для этого в датчике применяется группа контактов на переключение, при срабатывании которой на устройство контроля по двум цепям поступают два сигнала: прямой и инверсный.

Для необнаруживаемого отключения цепей контроля нарушителю необходимо в одной из трех угадать свободную цепь, оборвать ее, затем замкнуть оставшиеся две цепи. Вероятность этого события, т.е. $P_{обх}$, согласно теории вероятности равно одной трети. Но для квалифицированного нарушителя, владеющего обыкновенным мультиметром, позволяющим измерить полярность напряжения на контрольных цепях и определить замкнутую и разомкнутую цепи, $P_{обх}$ становится близким к единице.

Применяется также другое, на первый взгляд простое решение: установка в датчике Д2 резистора последовательно с нормально замкнутым контактом или в датчике Д1 – параллельно разомкнутому контакту. Это позволяет выйти на фиксированное значение тока в цепи контроля, и любые отклонения от него считаются нарушением и регистрируются устройством контроля. Но эти отклонения могут быть естественными по причине допустимого изменения электрических параметров устройства контроля (входящих радиоэлементов и электропитания), а также окружающей среды, т.е. такое решение выдвигает требования к помехоустойчивости и настройке конкретной системы в конкретных условиях эксплуатации. Вероятности обхода по указанным выше путям здесь значительно ниже, но методы ее оценки потребуют специальных исследований. Однако такие исследования могут не понадобиться, если применить другое решение.

Другое решение по перекрытию указанных выше путей обхода цепей контроля доступа заключается в дополнительных мерах по усовершенствованию схемы соединений с датчиком ДЗ. $P_{обх}$ можно понизить усложнением задачи нарушителя путем введения ложных дополнительных цепей, параллельных цепям контроля, проще говоря, использовать многожильный кабель. При этом часть жил можно замкнуть попарно между собой под крышкой, закрывающей датчик, а другую – замкнуть со стороны устройства контроля. Возможны и другие варианты. Сложность решения задачи нарушителя будет возрастать с увеличением количества ложных цепей. Кроме того, для исключения возможности сравнения нарушителем измеренных прибором напряжений на вскрытых проводах кабеля в устройстве контроля между выходами и коммутатором сигналов можно установить электронные переключатели, позволяющие пере-

одически с тактовой частотой устройства менять местами полярность напряжения на сигнальных цепях.

Таким образом получится закодированный монтаж цепей контроля. Если в первом случае нарушитель может предварительно использовать измерительный прибор и вероятность его успеха будет равна 1, то во втором и прибор не поможет, а вероятность его успеха сведется к решению задачи вытаскивания шаров заданного количества, цвета и номера с первой попытки из известного числа шаров двух цветов, помещенных в темный мешок.

Очевидно, что приведенный пример передачи тревожных сигналов в виде потенциальных уровней касается не столько контактных датчиков, сколько контрольных цепей, т.е. передачи прямого и инверсного сигналов. Кроме того, в зависимости от конкретного монтажа датчиков системы могут появиться и другие пути обхода защиты в местах отсутствия датчиков. Оценка вероятности такого рода события потребует специального исследования объекта размещения системы. Приведенный пример распространяется на системы охранной сигнализации, контроля доступа в помещения и вскрытия аппаратуры.

Другим примером контролируемой преграды может быть программа контроля идентификации и аутентификации пользователя при доступе его к операционной системе рабочей станции ЛВС. В данной программе в роли датчика выступают средства аутентификации пароля пользователя. Если вводимый им пароль совпал с хранимым в ЭВМ значением, доступ к ПО для него открыт, и событие просто регистрируется в специальном журнале. Если пароль не совпал, доступ не состоялся, событие регистрируется как НСД и соответствующее сообщение должно поступать на рабочую станцию администратора службы безопасности, который дает указания своим исполнителям по выяснению ситуации и поимке нарушителя. В данном случае важным будем считать момент обнаружения НСД, так как последующие события выходят за пределы нашей технической задачи.

Защита штатного входа в систему. Известно, что при построении защиты в вычислительных системах должен выдерживаться принцип: «все запрещено, кроме того, что разрешено». Это означает, что для нарушителя вход в систему должен быть с самого начала заблокирован. В этом случае необходимость учета времени блокировки в формуле расчета прочности контролируемой преграды отпадает, т.е. время обнаружения и блокировки сокращается до времени обнаружения ($T_{обл}$ в формулах заменяется на $T_{об}$, а $P_{обл}$ – на $P_{об}$).

Для анализа прочности данного средства защиты возьмем за основу формулу (3.1). Вероятность преодоления преграды нарушителем $P_{пр}$ со стороны законного входа в систему может определяться путем оценки вероятности подбора кода пароля, с помощью которого можно преодолеть эту преграду. Согласно [78] эту величину можно определить по формуле

$$P_{пр} = \frac{n}{A^s}, \quad (3.9)$$

где n – количество попыток подбора кода, как правило, равно 3;

A – число символов в выбранном алфавите кода пароля (ключа);

s – длина кода пароля (ключа) в количестве символов.

Например, при $n = 3$, $A = 42$ (русский алфавит + 10 цифр), $s = 8$,

$$P_{\text{нр}} < 3 \cdot 10^{-13}.$$

О мере достаточности этой величины можно также судить по времени, которое затратит нарушитель путем тривиального подбора пароля с неограниченным числом попыток. Тогда его «работа» займет время, определяемое согласно [78] по формуле

$$t_{\text{нр}} = \frac{A^s \cdot t}{2}, \quad (3.10)$$

где t – время, требуемое для того, чтобы попробовать каждый пароль из последовательности запросов.

Например, при $A = 42$, $s = 8$, $t = 1$ с (наборе на клавиатуре и попытке подобрать пароль этой же рабочей станции) время, необходимое нарушителю, составит:

$$t_{\text{нр1}} = 0,5 \cdot 10^{13} \text{ с} = 0,5 \cdot 2 \cdot 10^4 \text{ лет} = 10^5 \text{ лет}.$$

При попытке подобрать такой же пароль удаленной рабочей станции с помощью генератора случайных чисел используется [20] формула

$$t_{\text{нр2}} = \frac{A^s \cdot E}{2R}, \quad (3.11)$$

где R – скорость передачи сообщения в линии связи, симв/мин;

E – число символов в передаваемом сообщении при попытке получить доступ (включая пароль и служебные символы).

Анализ формулы показывает, что с уменьшением алфавита и количества символов в пароле уменьшается время нарушителя и т.д.

Например, при $A = 42$, $s = 8$, $E = 512$ символов, $R = 60$ млн симв/мин,

$$t_{\text{нр1}} = 3 \cdot 10^{13} \cdot \frac{512}{60000000} \cdot 0,5 \approx 15 \cdot 10^7 \text{ мин} \approx 10^5 \text{ дней} \approx 274 \text{ года}.$$

Для сравнения тот же пример, но при $A = 10$ (цифры):

$$t_{\text{нр2}} = 3 \cdot 10^8 \cdot \frac{512}{60000000} \cdot 0,5 \approx 15 \cdot 10^2 \text{ мин} = 25 \text{ ч};$$

при $s = 4$

$$t_{\text{нр3}} = 3 \cdot 42^4 \cdot \frac{512}{60000000} \cdot 0,5 \approx 9 \cdot 10 \cdot 0,5 \text{ мин} = 45 \text{ мин}.$$

Возможность получения достаточно большой величины этого времени расположила разработчиков к применению лишь только средств регистрации события, а нарушители типа хакеров продолжают эту работу на всякий случай – а вдруг повезет, так как эти данные составляют среднюю величину. Кроме того, зная слабость некоторых пользователей применять в качестве паролей имена своих ближайших родственников и знакомых и другие известные данные, нарушитель увеличит свои шансы на успех.

В любом случае, кроме средств регистрации, должны быть средства автоматического доведения информации о факте нарушения до средств отображения рабочей станции (РС) службы безопасности информации в кратчайший срок, так как при небольших величинах длины и алфавита пароля и достаточно большом времени обнаружения события (несовпадения пароля) у нарушителя есть вероятность, не обращая внимания на регистрацию его действий, войти в систему путем подбора пароля. Поэтому необходимо вовремя принять соответствующие меры.

Прочность защиты со стороны законного входа заставляет искать пути ее обхода, и такие пути существуют. Их виды зависят от исходной позиции нарушителя и конкретной реализации рабочей станции и ЛВС.

Таковыми путями могут быть: доступ к информации, минуя программу аутентификации, и попытка узнать действительные значения пароля.

В первом случае такой путь, например, возможен через дисковод с помощью специальной дискеты с программой, позволяющей изменить конфигурацию ОПО, установить свою программу аутентификации, узнать параметры существующей программы или отключить защиту. Во втором случае нарушитель может наблюдать, например, на экране значения пароля, набираемого пользователем.

Вероятность обхода преграды $P_{\text{обх}}$ оцениваем как вероятность преодоления нарушителем установленных на обнаруженных путях обхода средств защиты. Такими средствами могут быть применение в РС персональной ЭВМ без дисковода и размещение РС в отдельном помещении с контролируемым доступом. В первом случае вероятность обхода преграды по указанному пути приближается к нулю, во втором – определяется значением прочности системы контроля доступа в помещение, о которой говорилось выше.

Но на практике отдельных помещений на каждую РС не хватает и для защиты паролей от наблюдения на экране вводится блокировка их отображения. Кроме того, для исключения случайного доступа к действительным значениям паролей, хранящимся в памяти РС, применяется криптографическое преобразование перед их записью на жесткий диск. Оценка вероятности преодоления такой защиты приводится ниже.

Расчетные соотношения для неконтролируемой преграды. В АС неконтролируемыми возможными каналами НСД могут быть носители информации,

съемные запоминающие устройства, линии и каналы связи. Современные машинные носители имеют малые габариты и могут быть легко похищены. В брошенных в мусорную корзину носителях и ремонтируемых накопителях на жестких дисках может оставаться секретная информация. Линии и каналы связи могут быть проложены в местах, легко доступных для посторонних лиц, и т.д.

Известно, что информация со временем теряет свою привлекательность и начинает устаревать, а в отдельных случаях ее цена может упасть до нуля. Тогда за условие достаточности защиты можно принять превышение затрат времени на преодоление преграды нарушителем над временем жизни информации. Формально, если обозначить время жизни информации через $t_{ж}$, то

$$P_{сж} = (1 - P_{нр}) = 1, \text{ если } t_{ж} > t_{нр}. \quad (3.12)$$

В качестве такой защиты может быть применено криптографическое преобразование информации. Для этой цели используются различные алгоритмы симметричного (одноключевого) и несимметричного (двухключевого) шифрования и необратимого преобразования информации, например ГОСТ 28147-89. Системы обработки информации. Защита криптографического преобразования, стандарт шифрования; ГОСТ 34.10.94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи; ГОСТ 34.11.94 Информационная технология. Криптографическая защита информации. Функции хэширования; зарубежные аналогичные стандарты DES, RSA, DSA, SNA.

Указанные средства позволяют защититься от утечки и модификации информации. Формально криптографическая система – это однопараметрическое семейство обратимых преобразований из пространства сообщений открытого текста в пространство шифрованных текстов, где параметром является ключ, выбираемый из их конечного множества.

Преобразование шифрования может быть симметричным или ассиметричным относительно преобразования расшифрования. Это важное свойство определяет два класса криптосистем: симметричные (одноключевые) и ассиметричные (двухключевые с одним открытым ключом).

Если считать, что нарушителю известны применяемый алгоритм шифрования и шифр-текст сообщения, прочность такого рода защиты зависит от следующих параметров:

- стойкости алгоритма к криптоанализу;
- длины ключа шифрования;
- вычислительных мощностей нарушителя;
- способов защиты действительных значений ключей шифрования при хранении и передаче;
- выбора действительного значения ключа (оно должно быть случайным).

Чтобы гарантировать стойкость алгоритма к криптоанализу, разработчики автоматизированных систем применяют готовые, прошедшие специальные испытания и проверенные временем алгоритмы, предлагаемые специалистами в этой области. К их числу относятся вышеупомянутые алгоритмы.

Длина ключа определяет стойкость преобразования к автоматизированному подбору значения ключа с помощью быстродействующих ЭВМ. Согласно данным [62], если при такой попытке раскрыть шифр-текст, предпо-

ложить, что генерация ключа происходит за один такт ее работы, а операция дешифрования – мгновенно, то, определив отношение количества возможных ключей к быстродействию самого мощного компьютера, мы получим нижнюю оценку сложности дешифрования сообщения для идеального алгоритма. Результаты этих расчетов приведены в табл. 3.1. По теории вероятностей средним временем расшифровки сообщения (математическим ожиданием времени дешифрования) следует считать половину приведенного в табл. 3.1 времени (указано в скобках).

Таблица 3.1

Наименование машины	Мощность, оп/с	56 бит = $7,2 \cdot 10^{16}$ ключей	64 бита = $1,8 \cdot 10^{19}$ ключей	70 бит = $1,18 \cdot 10^{21}$ ключей	75 бит = $3,78 \cdot 10^{22}$ ключей
Intel ASCI Red	$1,068 \cdot 10^{12}$	0,002 г. (8,6 ч.)	0,534 г. (3,2 мес.)	35 лет (17,5 лет)	1122 г. (561 год)
Hitachi/Tsukuba CP-PAKS	$3,68 \cdot 10^{11}$	0,006 г. (25,8 ч.)	1,55 г. (9,3 мес.)	102 г. (51 год)	3257 лет (1628 лет)
SGL/Cray T3E	$2,65 \cdot 10^{11}$	0,008 г. (34,6 ч.)	2,15 г. (1,08 г.)	141 год (70,5 лет)	4523 г. (2261 год)
Fujitsu Numerikal Wind Tunnel	$2,3 \cdot 10^{11}$	0,0099 г. (1,7 сот)	2,48 г. (1,24 г.)	162 г. (81 год)	5211 лет (2605 лет)
Hitachi SR2201	$2,2 \cdot 10^{11}$	0,0103 г. (1,8 сот)	2,56 г. (1,28 г.)	170 лет (85 лет)	5448 лет (2724 года)

Однако приведенные в таблице данные рассчитаны на производительность современных вычислительных машин, т.е. необходима поправка данных на перспективное развитие этой техники. В работе [62] такая возможность рассматривается и приводятся обоснованные расчетные данные, которые заключаются в том, что производительность компьютера, деленная на его стоимость, увеличивается через каждые 5 лет в 10 раз. Кроме того, при расчетах оказалось, что, если начало дешифрования перехваченного шифр-текста выбрать с учетом данного обстоятельства, время на эту работу независимо от длины ключа составляет 2,17 г., а от длины ключа зависит лишь оптимальное для нарушителя время начала дешифрования. Если взять за точку отсчета быстродействие первых ЭВМ в 1946 г., равное 100 оп/с, то в результате расчетов [62] получаются данные, приведенные в табл. 3.2.

Таблица 3.2

Длина ключа, бит	Оптимальное время начала дешифрования, г.	Время окончания дешифрования, г.
64	2001,6	2003,77
70	2010,7	2012,87
90	2040,8	2042,87
128	2098	2100,17
137	2111,5	2113,69
256	2290,6	2292,77

Таким образом, зная время жизни информации, к которой по неконтролируемому каналу может добраться нарушитель, и данные табл. 2, можно выбрать алгоритм ее шифрования с длиной ключа, обеспечивающей превышение времени его доступа к открытому тексту, подлежащему защите.

Формально таким способом мы обеспечиваем нулевую вероятность преодоления преграды нарушителем путем перебора значений ключа, т.е. в формулах (3.1) и (3.2) $P_{\text{пр}} = 0$. Для защиты информации от нарушителя-профессионала целесообразно выбрать последнюю по причине отсутствия возможности контролировать ситуацию. Возможными путями обхода криптографической преграды, например, могут быть:

- криптоанализ исходного текста зашифрованного сообщения;
- доступ к действительным значениям ключей шифрования при хранении и передаче.

Возможны и другие пути обхода, известные только специалистам в этой области, например [10, 36, 56].

В первом случае это может быть, например, попытка анализа частоты букв в тексте сообщения. В каждом языке она разная. Существуют и другие методы. Защиту в этом случае обычно содержит сам аттестованный алгоритм шифрования. Поэтому ответственность в этом случае ложится на разработчиков алгоритма. Мы же считаем, что вероятность обхода преграды по этому пути равна нулю.

Во втором случае выбранный способ хранения и передачи ключей зависит от разработчика АС. Обычно в системе они не хранятся, а если хранятся и передаются, то в преобразованном криптографическом способе виде. Оценку защиты производим изложенным выше методом.

К неконтролируемым возможным каналам НСД к информации следует также отнести ремонтируемые запоминающие устройства, машинные и бумажные носители с остатками информации. Для защиты информации от нарушителя-непрофессионала, очевидно, будут достаточны обычные средства контроля стирания информации и уничтожения носителей. Для более ответственных – необходимы дополнительные средства: многократного наложения записи случайной последовательности символов на остатки информации и специальные сертифицированные устройства уничтожения носителей.

Оценка данных средств защиты и разработка соответствующих методик потребует специальных исследований. В настоящее время целесообразно воспользоваться методом экспертных оценок, приведенным выше.

На основании изложенного подводим некоторые итоги и делаем вывод о том, что защитные преграды бывают двух видов: контролируемые и не контролируемые человеком. Прочность *неконтролируемой* преграды рассчитывается по формулам (3.1) и (3.2), а *контролируемой* – по формуле (3.8). Анализ данных формул позволяет сформулировать первое правило защиты любого предмета:

Прочность защитной преграды является достаточной, если ожидаемое время преодоления ее нарушителем больше времени жизни предмета защиты или больше времени обнаружения и блокировки его доступа при отсутствии путей обхода этой преграды.

3.4.5. Модель многозвенной защиты

На практике в большинстве случаев защитный контур (оболочка) состоит из нескольких «соединенных» между собой преград с различной прочностью. Модель такой защиты из нескольких звеньев представлена на рис. 3.8.

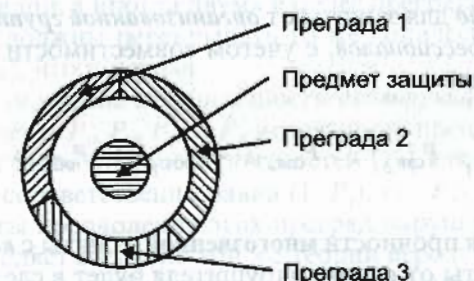


Рис. 3.8. Модель многозвенной защиты

Примером такого вида защиты может служить помещение, в котором хранится аппаратура. В качестве преград с различной прочностью здесь могут служить стены, потолок, пол, окна и замок на двери.

Для вычислительной системы «соединение» преград (замыкание оболочки защиты) имеет тот же смысл, но иную реализацию. Например, система контроля вскрытия аппаратуры и система опознавания и разграничения доступа, контролирующая доступ к периметру вычислительной системы, на первый взгляд образуют замкнутый защитный контур, но доступ к средствам отображения и документирования, побочному электромагнитному излучению и наводкам, носителям информации и другим возможным каналам НСД к информации не перекрывают и, следовательно, таковыми не являются. Таким образом, в контур защиты в качестве его звеньев войдут еще система контроля доступа в помещения, средства защиты от ПЭМИН, шифрование и т.д. Это не означает, что система контроля доступа в помещение не может быть замкнутым защитным контуром для другого предмета защиты (например, для технических средств вычислительной системы). Все дело в точке отсчета, в данном случае в предмете защиты, т.е. оболочка (контур) защиты не будет замкнутой до тех пор, пока существует какая-либо возможность несанкционированного доступа к одному и тому же предмету защиты.

Формальное описание прочности многозвенной оболочки защиты практически полностью совпадает с выражениями (3.1), (3.2) и (3.8), так как наличие нескольких путей обхода одной преграды, не удовлетворяющих заданным требованиям, потребует их перекрытия другими соответствующими преградами, которые в конечном итоге образуют многозвенную оболочку защиты.

Тогда выражение прочности многозвенной защиты из неконтролируемых преград, построенной для противостояния одному нарушителю, может быть представлено в виде

$$P_{зи} = \min \{P_{сзи1}, P_{сзи2}, \dots, P_{сзиi} (1 - P_{обх1}), (1 - P_{обх2}), \dots, (1 - P_{обхk})\}, \quad (3.14)$$

где $P_{сзи}$ – прочность i -й преграды;
 $P_{обх}$ – вероятность обхода преграды по k -му пути.

Выражение для прочности *многозвенной защиты, построенной из неконтролируемых преград* для защиты от *организованной группы квалифицированных нарушителей-профессионалов*, с учетом совместимости событий может быть представлено в виде

$$P_{зи0} = P_{сзи1} \cdot P_{сзи2} \cdot \dots \cdot P_{сзиi} \cdot (1 - P_{обх1}) (1 - P_{обх2}) \cdot \dots \cdot (1 - P_{обхk}). \quad (3.15)$$

Выражение для прочности *многозвенной защиты с контролируемыми преградами* для защиты от одного нарушителя будет в следующем виде

$$P_{зиk} = \min \{P_{сзиk1}, P_{сзиk2}, \dots, P_{сзиkni} (1 - P_{обх1}), (1 - P_{обх2}), \dots, (1 - P_{обхj})\}, \quad (3.16)$$

где $P_{сзиkn}$ – прочность n -й преграды;
 $P_{обхj}$ – вероятность обхода преграды по j -му пути.

Для защиты от *организованной группы нарушителей* аналогично подходу к выражению (3.15), т.е. считая действия нарушителей одновременными, преобразуем формулу (3.16) и получаем формулу для расчета прочности защитной оболочки с *контролируемыми преградами* в виде

$$P_{зиk0} = P_{сзиk1} \cdot P_{сзиk2} \cdot \dots \cdot P_{сзиkni} \cdot (1 - P_{обх1}) (1 - P_{обх2}) \cdot \dots \cdot (1 - P_{обхj}). \quad (3.17)$$

Изложенное позволяет сформулировать нижеследующие правила построения защитной оболочки.

Прочность многозвенной защитной оболочки от одного нарушителя равна прочности ее слабейшего звена. Это правило справедливо и для защиты от неорганизованной группы нарушителей, действующих самостоятельно.

Прочность многозвенной защиты от организованной группы нарушителей равна произведению вероятностей непреодоления потенциальным нарушителем каждого из звеньев, составляющих эту защиту.

Здесь следует подчеркнуть, что расчеты итоговых прочностей защиты для неконтролируемых и контролируемых преград должны быть отдельными, поскольку исходные данные для них различны и, следовательно, на разные задачи должны быть разные решения – две разные оболочки защиты одного уровня. Кроме того, недопустимо при расчете оболочки пользоваться одновременно двумя формулами, т.е. строить одну оболочку для защиты от разных нарушителей. Если существует какая-нибудь опасность проявления к предмету защиты интереса организованной группы нарушителей-профессионалов, необходимо для расчета выбрать формулы (3.15) и (3.17).

Если прочность слабейшего звена защиты удовлетворяет предъявленным требованиям оболочки защиты в целом, возникает вопрос об избыточности прочности на остальных звеньях данной оболочки. Отсюда следует, что *экономически целесообразно применять в многозвенной оболочке защиты равнопрочные преграды.*

Если звено защиты не удовлетворяет предъявленным требованиям, преграду в этом звене заменяем на более прочную или данная преграда дублируется еще одной преградой, а иногда двумя и более преградами. Но все дополнительные преграды должны перекрывать то же количество или более возможных каналов НСД, что и первая.

В этом случае, если обозначить прочность *дублирующих друг друга преград* соответственно через $P_1, P_2, P_3, \dots, P_r$, вероятность преодоления каждой из них нарушителем согласно теории вероятностей [21] как противоположное событие может быть соответственно равна $(1 - P_1), (1 - P_2), (1 - P_3), \dots, (1 - P_r)$.

Считаем, что факты преодоления этих преград нарушителем события совместимые. Это позволяет согласно той же теории вероятность преодоления суммарной преграды нарушителем формально представить в виде формулы

$$P_{нр} = (1 - P_1)(1 - P_2)(1 - P_3) \dots (1 - P_r).$$

Следовательно, вероятность непреодоления *дублирующих преград (прочность суммарной преграды)* как противоположное событие будет определяться выражением, приведенным в [48]:

$$P = 1 - P_{нр} = 1 - (1 - P_1)(1 - P_2)(1 - P_3) \dots (1 - P_r), \quad (3.18)$$

где i – порядковый номер преграды;
 P_i – прочность i -й преграды.

Излишне говорить о том, что эта формула справедлива для любых преград.

Иногда участок защитного контура (оболочки) с параллельными (с дублируемыми) преградами ошибочно называют *многоуровневой защитой*. В вычислительной системе защитные преграды часто перекрывают друг друга и по причине, указанной выше, и когда специфика возможного канала НСД требует применения такого средства защиты (например, системы контроля доступа в помещения, охранной сигнализации и контрольно-пропускного пункта на территории объекта защиты). Это означает, что прочность отдельной преграды P_i , попадающей под защиту второй, третьей и т.д. преграды, должна пересчитываться с учетом этих преград по формуле (3.18). Соответственно может измениться и прочность слабейшей преграды, определяющей итоговую прочность защитной оболочки в целом. Пример расчета см. в Приложении 3.

3.4.6. Многоуровневая защита

В ответственных случаях при повышенных требованиях к защите применяется многоуровневая защита, модель которой представлена на рис. 3.9.

Многоуровневой защитой будем называть защиту, построенную из нескольких замыкающих друг друга защитных оболочек.

При расчете суммарной прочности нескольких оболочек (контуров) защиты в формулу (3.18) вместо P_i включается P_{ki} – прочность каждой оболочки (контура), значение которой определяется по одной из формул (3.14), (3.15) и (3.16), т.е. для контролируемых и неконтролируемых преград опять расчеты должны быть раздельными и производиться для разных оболочек (контуров), образующих каждый по отдельности свою многоуровневую защиту. При $P_{ki} = 0$ данная оболочка (контур) в расчет не принимается. При $P_{ki} = 1$ остальные оболочки защиты являются избыточными. Подчеркнем также, что данная модель справедлива лишь для замкнутых оболочек защиты, перекрывающих одни и те же каналы несанкционированного доступа к одному и тому же предмету защиты.



Рис. 3.9. Модель многоуровневой защиты

3.4.7. Некоторые особенности точности расчета прочности защиты

Реализация контролируемых преград на аппаратных и программных средствах дает гарантированные результаты, которые с определенной степенью достоверности могут приближаться к действительным значениям. Степень приближения к этим значениям зависит в основном от надежности функционирования указанных средств. Однако с уверенностью можно утверждать, что ожидаемые отклонения в отрицательную сторону наверняка будут перекрываться запасом прочности защиты, рассчитанной на наиболее опасную модель поведения нарушителя. Но это справедливо лишь для защитной оболочки, построенной полностью на автоматике. Известно, что гарантированные результаты дает только техника. По этой причине защита жизненно важной информации в системах ее хранения, обработки и передачи должна строиться на такой основе.

На практике дополнительно к техническим средствам широко применяются организационные мероприятия, которыми перекрываются некоторые ВК НСД, т.е. они включаются в защитную оболочку. Данные меры также должны получить количественную оценку. Пока такие методики отсутствуют, целесообразно воспользоваться методом экспертных оценок.

Полученные результаты будут отличаться невысокой точностью и при расчете общей прочности защитной оболочки могут оказаться согласно определению определяющей величиной как самое слабое звено защиты и свести на нет высокие показатели технических средств, составляющих эту защитную оболочку. Все это необходимо учитывать. Для менее ответственных систем целесообразно задавать показатели прочности технических и организационных средств защиты отдельно, а их соотношение отразить в коэффициенте автоматизации средств защиты, который должен вычисляться по формуле

$$K_{\text{авт}} = \frac{N_{\text{авт}}}{N},$$

где $K_{\text{авт}}$ – коэффициент автоматизации;
 $N_{\text{авт}}$ – количество в одной оболочке средств защиты с автоматической подачей сигнала и блокировкой НСД;
 N – общее количество средств защиты в данной оболочке защиты.

Значение этого коэффициента должно указываться в техническом задании на АС. Его величина должна увеличиваться при увеличении важности и цены обрабатываемой информации, подлежащей защите. В ответственных системах он должен приближаться к 1.

На основе вышеизложенного можно сделать следующие выводы.

1. Данный метод расчета защиты данных от преднамеренного доступа дает возможность получения расчетных соотношений для элементарной однозвенной, многозвенной и многоуровневой защиты, которые позволят рассчитать и построить в автоматизированных системах обработки информации как отдельные средства защиты, так и защитную оболочку в целом.
2. Использование в расчете прочности защиты временного фактора представляется более удачным, чем фактор стоимости. Известно, что оценка стоимости информации может быть весьма приблизительной, и пока до настоящего времени практических методик для этой цели не существует. Для больших систем подобная работа, учитывая динамику движения и цены обрабатываемой информации, вообще вряд ли целесообразна. Известно, что временной фактор уже используется при оценке стойкости криптографических средств защиты, что говорит в пользу принятого решения. В результате получаем возможность применения общей для всех средств защиты одной широко известной единицы измерения – вероятности наступления события.
3. Применение данного метода расчета позволит:
 - создать научно обоснованную замкнутую оболочку защиты с количественными показателями ее прочности;
 - применить единую для всех АС теорию защиты информации от НСД;
 - сократить количество экспертных оценок эффективности средств защиты и упростить их методику;
 - на основе более точных расчетов прочности средств защиты и создания защитной оболочки получить значительное повышение уровня безопасности информации в разрабатываемых АС.

4. Полученные расчетные соотношения по своей сути являются основой теории построения системы защиты и контроля доступа не только к информации в вычислительных объектах, но и к другим объектам защиты.

3.5. Метод построения защиты информации в системах с сосредоточенной обработкой данных

3.5.1. Объект исследования

В качестве типового объекта исследования согласно вышеприведенной структуре и классификации АС (см. рис. 3.3) можно выбрать рабочую станцию, сервер, АРМ, вычислительный комплекс и т.д. Для более наглядного представления метода целесообразно рассмотреть более сложную систему – комплекс средств автоматизации с сосредоточенной обработкой данных, структурная схема которого приведена на рис. 1.3.

Для КСА такого рода характерны следующие штатные (законные) каналы доступа к информации:

- устройства ввода (вывода) информации;
- средства отображения информации;
- средства документирования информации;
- средства загрузки программного обеспечения;
- машинные носители информации;
- бумажные носители информации;
- внешние каналы связи.

Имея в виду, что при отсутствии защиты нарушитель может воспользоваться как штатными, так и нештатными каналами доступа, можно назвать возможными каналами несанкционированного доступа следующие каналы:

- все перечисленные выше штатные средства при их использовании законными пользователями не по назначению и за пределами своих полномочий;
- все перечисленные выше штатные средства при их использовании посторонними лицами;
- технологические пульты и средства управления;
- внутренний монтаж аппаратуры;
- линии связи между аппаратными средствами данной вычислительной системы;
- побочное электромагнитное излучение информации с аппаратуры технических средств;
- побочные наводки информации по сети электропитания и шинах заземления аппаратуры;
- побочные наводки информации на вспомогательных и посторонних коммуникациях, сервисном оборудовании;

- отходы в виде бумажных и машинных носителей информации, брошенных в мусорную корзину;
- ремонтируемые запоминающие устройства, содержащие остаточную информацию.

К перечисленным возможным каналам НСД следует также добавить людей: законных пользователей, операторов, лиц из числа технического обслуживающего персонала и других, которые при определенных условиях могут быть источником информации. Эта проблема в данной работе не рассматривается, так как она выходит за рамки поставленной задачи. В работе учтена только возможность непосредственного контакта с информацией этих людей. Такая возможность отражена в модели потенциального нарушителя, приведенной в подразд. 1.3.

3.5.2. Классификация возможных каналов НСД

При меньшей номенклатуре и количестве технических средств КСА, а также выборе модели поведения менее квалифицированного нарушителя количество возможных каналов НСД (ВК НСД) к информации уменьшается, уменьшаются соответственно количество и прочность применяемых средств защиты.

Поэтому вполне целесообразно предложить следующее распределение упомянутых каналов по указанным выше (см. подразд. 1.3) классам нарушителей:

I класс – все ВК НСД, известные на момент разработки системы;

II класс – все ВК НСД, кроме ПЭМИН;

III класс – все ВК НСД, кроме ремонтируемой аппаратуры, носителей информации, перемещаемых в пределах контролируемой зоны, остатков информации в запоминающих устройствах, аппаратуры передачи данных и внутренних линий связи, мусорной корзины;

IV класс – произвольное количество ВК НСД устанавливается разработчиком и заказчиком системы с целью обеспечения технологической дисциплины обработки информации и профилактики случаев ее утраты.

3.5.3. Метод применения средств защиты

Предлагаемая в данной книге методология не исключает применения уже имеющихся в настоящее время средств защиты информации в АС. Автор исходит из того, что данные элементы являются «кирпичиками» создаваемой защиты, из которых можно построить различные «здания», прочность которых зависит не только от их качества, но и от того, по какому проекту они сложены. Предлагаемая методология и есть этот проект. Проект предусматривает новые требования к этим «кирпичикам», на которые раньше не обращали внимания и которые позволяют связать их между собой настолько, насколько это необходимо, чтобы построить здание защиты заданной прочности. В отличие от привычного подхода к построению защиты предлагается исходить из того, что защита уже есть, но в ней имеются каналы несанкционированного доступа к предмету защиты, количество которых соответствует ожидаемой модели поведения потенциального нарушителя.

Подробный анализ и описание известных средств защиты не являются задачей данной работы. Рассмотрим только в качестве примера распределение известных средств защиты по возможным каналам НСД в КСА с централизованной обработкой информации. Это распределение может быть представлено в табл. 3.3.

Таблица 3.3

№ п/п	Наименование ВК НСД	Класс защиты			Средства защиты	Прочность
		I	II	III		
1	Устройства ввода (вывода) информации	+	+	+	Система контроля и разграничения доступа в помещения.	P1
		+	+	-	Программно-аппаратный комплекс контроля входа в систему.	P2
		+	+	+	Программа контроля и разграничения доступа к ПО и информации КСА.	P3
		+	+	+	Антивирусные средства	P4
2	Аппаратура отображения и документирования информации	+	+	+	Система разграничения и контроля доступа в помещения	P1
3	Ремонтируемая и профилактируемая аппаратура	+	+	-	Система разграничения и контроля доступа в помещения.	P1
		+	+	-	Система контроля ввода (вывода) аппаратуры в (из) рабочий контур обмена информацией.	P5
		+	+	+	Средства стирания остатков информации.	P14
		+	-	-	Средства наложения на остатки информации случайной последовательности символов и чисел.	P15
		+	-	-	Средства уничтожения носителей секретной информации	P16
		+	-	-		
4	Машинные носители информации	+	+	+	Учет и разграничение доступа к носителям.	P6
		+	-	-	Электронная идентификация носителей.	P7
		+	-	-	Шифрование информации.	P8
		+	+	-	Резервирование информации с охраной ее копии	P9
5	Документы	+	+	+	Учет, регистрация и разграничение доступа к документам	P10
		+	+	+		
6	Носители программного обеспечения	+	+	+	Учет, регистрация и разграничение доступа к носителям ПО.	P11
		+	+	+	Верификация и контроль целостности ПО.	P12
		+	+	+	Резервирование ПО с контролем доступа к его копии	P13

Продолжение

№ п/п	Наименование ВК НСД	Класс защиты			Средства защиты	Прочность
		I	II	III		
7	Машинные носители с остатками информации (диски, ленты)	+	+	+	Учет, регистрация и разграничение доступа.	P6
		+	+	+	Средства стирания информации.	P14
		+	-	-	Наложение случайной последовательности символов и чисел.	P15
		+	-	-	Средства уничтожения носителей	P16
8	Бумажные носители с остатками информации	+	+	-	Средства уничтожения носителей	P17
9	Средства загрузки ПО	+	+	+	Средства контроля и разграничения доступа в помещения.	P1
		+	+	-	Средства контроля и блокировки доступа к загрузке ПО.	P18
		+	+	+	Антивирусные средства	
		+	+	-		
10	Технологические пульты и органы управления, внутренний монтаж аппаратуры	+	+	-	Средства контроля и разграничения доступа в помещения.	P1
		+	+	-	Система контроля вскрытия аппаратуры	P19
11	Внутренние линии связи между аппаратными средствами КСА	+	+	-	Средства контроля доступа на территорию КСА.	
		+	+	-	Средства контроля вскрытия аппаратуры.	P19
		-	+	-	Скрытая прокладка линий связи.	P20
		+	-	-	Шифрование передаваемой информации	P21
12	Внешние каналы связи КСА	+	+	+	Программа контроля и разграничения доступа к информации КСА (на входе КСА).	P24
		+	-	-	Шифрование передаваемой информации	P22
		+	+	+	Антивирусные средства	
13	Побочное электромагнитное излучение и наводки информации	+	-	-	Средства снижения или зашумления уровня излучения и наводок информации на границе контролируемой зоны объекта автоматизации	P23
14	Мусорная корзина	+	+	-	Средства уничтожения носителей закрытой информации	P17

Примечание: Знак "+" — наличие средства защиты;
знак "-" — отсутствие средства защиты.

Перечисленные в таблице средства могут быть применены, если они удовлетворяют требованиям к системе защиты информации и заданной прочности защитной оболочки того или иного класса. Однако этот расчет необходимо уточнить после объединения этих средств в единую систему, т.е. после создания средств централизованного контроля и управления.

3.5.4. Построение системы безопасности информации КСА

Приведенные выше средства защиты информации, обладающие высокой эффективностью каждое в отдельности, могут оказаться недостаточными, если они не будут объединены в единый постоянно действующий механизм – систему безопасности информации (СБИ). Задачу объединения выполняют специально выделенные централизованные средства управления и контроля, которые назовем *средствами управления безопасностью информации (СУБИ)*.

Средства управления безопасностью информации в КСА должны обеспечивать возможность выполнения для I класса защиты примерного перечня следующих функций:

- ввод в систему списка имен пользователей и терминалов, допущенных к информации КСА;
- подготовку и ввод в систему, запись паролей пользователей на носители;
- ввод в систему назначенных полномочий пользователей и терминалов;
- раздачу пользователям носителей с паролями и значений паролей, запоминаемых и вводимых пользователями вручную с клавиатуры;
- сбор сигналов несовпадения паролей и нарушения полномочий пользователей;
- установление времени, места и причины НСД;
- анализ ситуации, принятие адекватных мер и восстановление нормального функционирования КСА;
- контроль конфигурации системы;
- сбор сигналов вскрытия аппаратуры и контроль ввода (вывода) аппаратуры в (из) ремонт (а) и на (из) профилактику(и);
- контроль журнала регистрации доступа к информации КСА и периодический вызов справок из него;
- взаимодействие со службой функционального контроля КСА;
- контроль функционирования системы защиты;
- подготовку ключей, контроль и обеспечение функционирования средств шифрования информации;
- контроль стирания и уничтожения остатков секретной информации на машинных и бумажных носителях;
- регистрацию, учет и разграничение доступа к носителям информации и ПО;
- ведение статистики и прогнозирование НСД.

Выполнение перечисленных функций должно осуществляться с помощью специальных программных и аппаратных средств, входящих в состав технических средств КСА, и организационных мероприятий, включаемых в отдельную инструкцию по эксплуатации средств защиты информации в КСА. Управление и контроль безопасностью информации осуществляет специальная служба объекта-потребителя КСА.

В результате мы можем построить систему безопасности информации (СБИ) КСА, пример структуры которой в КСА с сосредоточенной обработкой информации представлен на рис. 3.10. В состав СБИ КСА с сосредото-

ченной обработкой данных (см. рис. 3.10) предложены три группы средств: средства защиты информации (СЗИ) от преднамеренного НСД, средства защиты от случайных НСД и средства управления безопасностью информации (СУБИ), объединяющие упомянутые средства в единый механизм – систему безопасности информации КСА.



Рис. 3.10. Структурная схема системы безопасности информации КСА

3.5.5. Анализ средств и метод расчета прочности защиты

В таблице 3.3 не приведены средства контроля целостности программного обеспечения (ПО) и информации в КСА, а также средства регистрации, обычно рекомендуемые современными специалистами и нормативными документами. С позиций предлагаемой концепции эти средства не имеют достаточно быстрой реакции на НСД и являются необходимыми лишь для проведения следствия после того, как событие уже свершилось, и нарушитель может быть уже далеко. Их функции защиты эффективны лишь в сдерживании потенциального неквалифицированного нарушителя. Процедура контроля целостности в принципе выдает оператору информацию о нарушении, как только в момент проведения этой процедуры. Ее частота проведения, как правило, устанавливается организационно и проводится относительно редко по причине большого времени процедуры и отвлечения значительных ресурсов ЭВМ. Однако необходимость в применении этих средств не отрицается. Они необходимы для дублирования основных средств, но прежде всего для проведения анализа события и обнаружения случайных воздействий.

В последнее время с развитием возможностей вычислительной техники появились разработки, позволяющие в фоновом режиме постоянно контролировать целостность ПО и данных (Щеглов А., Тарасюк М. Круговая оборона. // Сети. – 1999. – №3. – С. 50). В этом случае данная программа выступает в роли средства контроля, которое должно отвечать требованиям его периодичности, ожидаемых затрат времени нарушителя на НСД, времени передачи сообщения о НСД на средства централизованного контроля и возможных путей обхода преграды, т.е. полноты охвата контролем ПО и данных. Тогда прочность данного средства защиты должна рассчитываться по формуле (3.8). Однако процесс функционирования КСА может предусматривать законные изменения данных пользователем. Самое главное при этом заключается в том, чтобы данные и программы, к которым пользователь не допущен, находились под контролем, ему неподвластны, и алгоритм контрольного суммирования должен быть достаточно сложным, а в ответственных системах – криптографическим, т.е. возможный путь обхода данного средства контроля целостности (подгонка контрольной суммы при изменении ПО и информации КСА) должен быть перекрыт достаточно прочным средством защиты. Расчет прочности в этом случае должен производиться по формуле (3.1), где в роли защищаемой информации выступает контрольная сумма.

Антивирусные средства в настоящее время также могут работать в фоновом режиме. К ним может быть применен тот же подход к оценке процессов контроля и обнаружения вирусов во времени и их количестве.

Особенность средств контроля целостности ПО и данных, включая антивирусные средства, заключается в попытке создания защиты всей вычислительной среды, ограниченной составом ПО конкретного КСА. В случае контроля целостности создается защитная оболочка, контролирующая независимо от вида и характера воздействий изменения ПО и данных. В случае же антивирусных средств предпринимается попытка обнаружения определенных видов угроз в количестве, известном на момент создания КСА. С течением времени это количество увеличивается, и поэтому приходится постоянно поддерживать эти средства на соответствующем уровне.

Формальный расчет прочности антивирусной программы – это результат будущих исследований. На предварительном этапе достаточно его оценить как отношение количества видов вирусов, обнаруживаемых данной программой, к количеству видов вирусов, известных на момент расчета, т.е. по формуле

$$P_{ав} = \frac{K_{пр}}{K_{ив}}$$

Таким образом, работающие в фоновом режиме упомянутые средства контроля целостности и антивирусные средства образуют отдельную защитную оболочку на ПО и информации КСА. Учитывая самостоятельность выполняемых функций этими оболочками, целесообразно их прочность выделить отдельными показателями.

Особо следует остановиться на программах разграничения и контроля доступа к ПО и данным КСА, в том числе на программе-диспетчере, специально разрабатываемой для конкретной программной платформы. Эта программа, как правило, обеспечивает доступ в два этапа: контроль доступа к операционной системе путем аутентификации пользователя по предъявленному паролю и разграничение доступа к ресурсам согласно полномочиям, данным ему и введенным предварительно в систему службой безопасности. В соответствии с этим должны быть два средства защиты: контроля доступа и контроля полномочий пользователя.

С позиции оценки их прочности необходимо определить величину отношения ожидаемого времени затрат нарушителя к времени реакции системы на НСД и вероятность обхода преграды. Последний параметр должен рассматриваться с учетом перечисленных выше средств защиты. Оценка прочности каждого из упомянутых средств должна производиться по формуле (3.8). Учитывая зависимость прочности указанных средств от перечисленных в табл. 3.3, целесообразно их оставить в составе общей оболочки защиты, а уровень стойкости пароля, предназначенного для защиты санкционированного входа в систему, представить отдельным показателем.

Для расчета прочности защиты информации в КСА проводится анализ ВК НСД на предмет соответствия их состава и количества заданному классу защиты, разделения их на контролируемые и неконтролируемые, наличие соответствующих средств защиты и возможное их дублирование. К контролируемым в нашем примере по I классу защиты предлагается отнести средства со значениями прочности: $P_1, P_2, P_3, P_5, P_6, P_{10}, P_{11}, P_{18}, P_{19}, P_{24}$.

Перечисленные значения вычисляются по формуле (3.8).

Для каждого ВК НСД с учетом дублирования средств защиты вычисляется значение прочности защиты. В нашем случае такой расчет для каналов $NN_1, 3, 9, 10, 11$ производится по формуле (3.18).

После сравнения полученных значений выбираем меньшее из них, которое и будет значением прочности защитной оболочки, образованной данными средствами, т.е. используем формулу (3.16).

К неконтролируемым можно отнести средства со следующими значениями прочности: $P_8, P_{14}, P_{15}, P_{16}, P_{17}, P_{21}, P_{23}$.

Расчет прочности защиты для каждого канала ведем аналогичным образом, используя соответствующие формулы (3.1), (3.2), (3.8), (3.12), оболочки в целом – по формулам (3.14), (3.15) (3.16) и (3.17).

Следует отметить особенности средств верификации и резервирования. Первые, с одной стороны, по определению относятся к средствам контроля; с другой – к средствам предупреждения в смысле стойкости средств верификации к подделке на случай, если носитель может быть заменен, и информация или программное обеспечение, записанное на нем, подвергается специальному криптографическому преобразованию. Результат его служит критерием оценки предъявляемого продукта. Принятое решение, очевидно, будет зависеть от конкретной реализации средства верификации.

Резервирование обычно относят к средствам защиты от случайных воздействий. Но оно может служить также и для защиты от преднамеренного разрушения и хищения информации, если объект резервирования находится под охраной. В этом смысле резервирование следует отнести к категории контролируемых средств защиты.

Учитывая широкое распространение систем обработки не очень важной информации, а также применение организационных мероприятий по защите и на более важных системах, необходимо отразить в формализованном виде и их возможную эффективность. Предлагаемые расчетные соотношения это предусматривают (см. подразд. 3.1). При коэффициенте автоматизации средств защиты, меньшем 1, рекомендуется прочность организационных мероприятий выделить в отдельный показатель.

В итоге для расчета прочности системы защиты информации от преднамеренного НСД в КСА с сосредоточенной обработкой данных можно предложить следующие показатели [42]:

- показатель прочности *контролируемой* оболочки защиты;
- показатель прочности *превентивной* оболочки защиты;
- показатель *стойкости пароля* законного пользователя к несанкционированному подбору;
- показатель прочности *средств контроля целостности ПО и данных* (используется только при применении данных средств с возможностью работы в фоновом режиме);
- показатель прочности *антивирусных средств*;
- показатель прочности *организационных мероприятий* (для систем 3 и 4 классов);
- коэффициент *автоматизации средств защиты* (для систем 1 и 2 классов должен быть равен 1).

По случайным событиям воспользуемся показателями функционального контроля (ФК) автоматизированной системы, приведенными в [39]. Способность средств ФК обеспечить своевременно (до начала последующей обработки) обнаружение и блокировку ошибок заданной кратности определяет уровень достоверности контроля обработки информации. Существенную роль для качества ФК играет плотность распределения его средств обнаружения ошибок по всей «площади» контролируемой вычислительной системы, т.е. полнота ее охвата функциональным контролем. В связи с этим при создании вычислительных систем используются показатели качества ФК, приведенные в подразд. 2.6, с. 141:

- время обнаружения и локализации отказов аппаратуры с точностью до съемного элемента:

$$T_{\text{обн}} = \frac{\sum_{i=1}^m t_{\text{обн}i}}{m},$$

где m – число экспериментов;

i – номер эксперимента;

$t_{\text{обн}i}$ – время обнаружения отказа в i -м эксперименте.

- полнота контроля функционирования вычислительной системы

$$K_{\text{п}} = \frac{\lambda_{\text{к}}}{\lambda_{\text{о}}},$$

где $\lambda_{\text{к}}$ – суммарная интенсивность появления отказов составных частей, охваченных контролем;

$\lambda_{\text{о}}$ – суммарная интенсивность отказов всех составных частей вычислительной системы.

- достоверность контроля

$$K_{\text{д}} = \frac{n_{\text{обн}}}{n_{\text{пр}}},$$

где $n_{\text{обн}}$ – общее число отказов, обнаруженных данной системой функционального контроля;

$n_{\text{пр}}$ – общее число отказов при проведении ФК при условии появления или искусственного введения отказов в каждом опыте.

3.5.6. Технология проектирования защиты информации в КСА

В итоге в основу технологии проектирования системы защиты информации в КСА можно предложить следующий порядок действий разработчика [42]:

- 1) определение перечня, мест сосредоточения, важности и динамики цены данных, подлежащих защите в данном КСА;
- 2) выбор ожидаемой модели поведения нарушителя и его квалификации;
- 3) анализ КСА на предмет определения в соответствии с заданной моделью поведения нарушителя возможного количества каналов НСД к информации, подлежащей защите;
- 4) выбор или разработка новых средств защиты с показателями прочности, отвечающими заданным требованиям с учетом распределения средств защиты по возможным каналам НСД;

5) перекрытие средствами защиты всех выявленных каналов НСД и возможных путей их обхода нарушителем;

6) создание централизованных средств контроля и управления защитой в данном КСА, обеспечивающих возможность объединения средств защиты в одну самостоятельную структуру – систему безопасности информации;

7) количественная оценка уровня прочности каждого средства защиты;

8) количественная оценка уровня прочности системы безопасности информации в КСА в целом на соответствие заданному;

9) замена на более прочные или дублирование средств защиты при несоответствии результата оценки заданному уровню безопасности;

10) встраивание в КСА средств защиты и управления;

11) испытания и повторная оценка прочности защиты.

Приведенный метод построения защиты является инструментом, с помощью которого можно осуществить разработку, анализ, распределение и расчет прочности отдельных средств защиты, а затем и всей системы защиты информации в комплексе средств автоматизации с сосредоточенной обработкой данных как автономной системы и как элемента более сложной системы – вычислительной сети или АСУ.

3.6. Метод построения защиты информации в системах с распределенной обработкой данных

3.6.1. Объект исследования

Анализ АСУ позволяет представить их в обобщенном виде как совокупность КСА, соединенных между собой каналами связи (см. рис. 3.4). На первый взгляд достаточно защитить данные элементы, и задача защиты информации в АСУ в целом будет решена. Первое время такая концепция имела место.

Последующие исследования показали, что при большом количестве пользователей необходима также защита и от нарушителя-пользователя, являющегося штатным работником или законным абонентом вычислительной сети. Кроме того, территориальное распределение КСА предполагает реализацию связи на далекие расстояния по кабелю, радиоканалам и другим, физически доступные для нарушителя, так как реализовать их охрану и контроль доступа к ним не представляется возможным. Поэтому вполне реальна возможность подключения нарушителя к каналам или линиям связи в виде шлюза, через который информация может подвергаться не только утечке, но и модификации, разрушению, в результате чего могут подвергаться опасности системные отношения и связи между элементами сети и АСУ. Носителем этих отношений и связей, а также передаваемых сообщений является кадр кодограммы, которым обмениваются КСА между собой.

В системах с распределенной обработкой данных (сетях и АСУ) к возможным каналам НСД следует отнести уже упомянутые выше КСА, являющиеся согласно рис. 3.4 ее структурными элементами, и каналы связи. Метод построения защиты информации в КСА приведен в разд. 3.5. Рассмотрим каналы связи. Как условились выше, принимаем наиболее опасный случай, когда потенциальный нарушитель имеет свободный доступ к каналам связи и, следовательно, к кодограмме. Идея концептуальной модели построения защиты, приведенной на рис. 3.2, заключается в защите информации, обрабатываемой в КСА, и защите не каналов связи, а передаваемых по ним кадров кодограммы. Образованная таким образом совокупность средств защиты информации КСА и кадра кодограммы составит оболочку защиты в распределенной АС.

3.6.2. Предмет защиты и потенциальные угрозы

Кадр кодограммы включает в себя служебные признаки, адресную и содержательную части. Тогда кажется, что при отсутствии защиты нарушитель может делать с ней все, что угодно. На самом же деле перечень его возможных несанкционированных действий (ВНСД) по максимуму хотя и обширен, но ограничен и хорошо известен. В этот перечень входят:

- изменение, удаление, задержка, переупорядочение, дублирование регулярных и посылка ложных сообщений;
- воспрепятствование передаче сообщений;
- осуществление ложных соединений;
- чтение содержания сообщений;
- анализ трафика и идентификаторов абонентов сети;
- чтение и использование пароля законного пользователя;
- нарушение своих полномочий законным пользователем путем обращений к запрещенной для него информации.

К ним в последнее время добавляются возможные особого рода несанкционированные действия законных пользователей-нарушителей: отказ отправителя от собственного сообщения и получателя – от принятого, а также маскированные повторы сообщений и передача различного рода информационного «мусора».

3.6.3. Классификация возможных несанкционированных действий

В зависимости от ожидаемой модели нарушителя этот перечень может быть сокращен до определенной степени. Отметим еще раз, что для определенной модели потенциального нарушителя этот перечень конечен, т.е. задача может быть достаточно строго определена.

Учитывая множество различного рода создаваемых вычислительных сетей и АСУ, различные требования к уровню безопасности обрабатываемой информации в них, целесообразно ввести соответствующую классификацию. В ее основу предлагается положить модель ожидаемого поведения и класси-

фикацию потенциального нарушителя, приведенные в подраз. 3.1, а также перечень его возможных несанкционированных действий, приведенный выше. Предлагаемая классификация уровней безопасности:

I класс – все приведенные выше несанкционированные действия;

II класс – все НСД, кроме анализа трафика и идентификаторов абонентов;

III класс – все НСД, кроме анализа трафика и идентификаторов, дублирования, переупорядочения и задержки сообщений.

IV класс предлагается не вводить на основании того, что создаваемые вычислительные сети и АСУ слишком дороги, чтобы в них были созданы условия безопасной обработки информации ниже III класса, так как динамика современной жизни часто меняет отношение к той или иной информации по различным причинам.

Далее эти ожидаемые действия также должны быть поделены на технически контролируемые и неконтролируемые. Здесь существенную роль играет время. При попытках несанкционированного чтения кодограммы время противостояния защиты или ожидаемое время преодоления ее нарушителем должно превышать время жизни защищаемой информации. В случае активных действий из числа указанных необходимы средства своевременного их обнаружения и блокировки. Отсутствие последних в современных системах и является основной причиной успешных действий нарушителей. Здесь следует признать положительную роль появления межсетевых экранов.

3.6.4. Метод применения средств защиты

В настоящее время в системах с распределенной обработкой данных в целях защиты информации от *преднамеренного* НСД широко применяются средства криптографического преобразования данных (линейное и абонентское шифрование, цифровая подпись) и упомянутые экраны. При этом в тракте передачи данных от пользователя к пользователю криптосредствами не всегда защищаются содержательная и служебная части кодограммы. Выполняемые этими средствами функции не объединены общей целью – созданием единой равнопрочной оболочки защиты, в которой применяемые в данной системе средства защиты дополняют друг друга. А отсутствие идеи *конечного* перечня возможных угроз не позволяло обосновать полноту их охвата средствами предупреждения и довести поставленную задачу до логического конца.

При проектировании защиты служебной части кодограммы выбранный метод должен быть таким, чтобы в ней с целью выполнения нормальной ее обработки сохранились некоторые адреса и служебные признаки в открытом виде. Таким методом может быть использование механизма цифровой подписи на базе несимметричных алгоритмов шифрования. Отдельные части кодограммы формируются и читаются на разных этапах ее обработки разными устройствами, узлами сети и аппаратурой ее абонентов. Для каждого из формируемых признаков и частей кодограммы должен быть свой ключ шифрования и ответственный за их распределение и последующую замену.

Обратим внимание на существенную разницу во времени жизни содержательной и служебной частей кодограммы. Содержательная часть может со-

хранять цену десятки лет, а служебная – не более десяти минут (время доведения сообщения до адресата). Это позволяет снизить требования к стойкости шифрования служебных частей, упростить его и уменьшить время обработки кодограммы.

Не останавливаясь подробно на уже известных средствах защиты и их возможностях, максимально возможные несанкционированные действия нарушителя (по I классу) и соответствующие им средства защиты на примере АСУ, приведенной на рис. 3.4, можно представить в виде табл. 3.4.

Таблица 3.4

№ п/п	Возможные несанкционированные действия	Средства защиты информации АСУ	Прочность	Средства защиты информации СПД	Прочность
1	Чтение содержания сообщения	Абонентское шифрование	P_1	Линейное шифрование	P_{10}
2	Дублирование сообщения в целях навязывания ложной информации	Средства шифрования даты и времени отправления сообщения вместе с его содержательной частью	P_2	–	
3	Переупорядочение сообщения	Средства шифрования даты и времени отправления сообщения вместе с содержательной частью	P_2	Шифрование и цифровая подпись служебных частей кодограммы	P_{11}
4	Задержка или удаление сообщения	Квитанция о получении сообщения Введение контрольного интервала времени ответа	P_3 P_4	Дублирование соединения или маршрута	P_{12}
5	Переадресация сообщения	Цифровая подпись адреса получателя одновременно с содержательной частью сообщения	P_5	Шифрование и цифровая подпись служебных частей кодограммы	P_{11}
6	Посылка ложного сообщения	Цифровая подпись содержательной части сообщения	P_5	–	
7	Анализ трафика	Специальные средства заполнения потока	P_6	Линейное шифрование	P_{10}
8	Анализ идентификаторов получателей сообщений	–		Линейное шифрование	P_{10}
9	Чтение и подбор паролей отправителей сообщений	Межсетевой экран КСА АСУ Средства идентификации и аутентификации	P_7 P_8	Средства идентификации и аутентификации	P_{14}
10	Нарушение законным пользователем своих полномочий	Межсетевой экран КСА АСУ Средства разграничения и контроля доступа КСА АСУ	P_7 P_9	Средства разграничения и контроля доступа УК СПД	P_{15}
11	Отказ отправителя от переданного, получателя – от принятого сообщения	Центр контроля и управления безопасностью информации в АСУ	P_{13}	Центр контроля и управления безопасностью информации в СПД	P_{13}

Полнота перекрытия перечисленных несанкционированных действий соответствующими средствами будет определять степень замыкания защитных оболочек. Их также будет две: контролирующая и превентивная, прочность которых рассчитывается аналогично расчету защиты для КСА. При этом средства защиты от отказов законных пользователей от принадлежащих им документов в оболочку входить не должны по причине выполнения ими другой задачи – регистрации сообщения в центре управления и контроля, результаты решения которой должны проходить отдельным показателем. Вполне возможно, что показатели средств защиты ресурсов сети от повторов сообщений и информационного «мусора» также будут отдельными.

Для полноты средств защиты информации в АСУ в их состав должны войти средства защиты информации на уровне КСА, УК и СПД.

3.6.5. Построение системы безопасности информации АСУ и СПД

Объединение функций контроля НСД и централизация функций подготовки ключей шифрования и цифровой подписи на управляющих КСА АСУ (УК СПД) (см. рис. 3.4) позволит создать в каждой системе встроенную единую структуру защиты – автоматизированную систему безопасности информации (СБИ АСУ и СБИ СПД). Для этого в КСА АСУ и УК СПД помимо собственной системы безопасности информации, построенной по принципам, приведенным в разд. 3, должны предусматриваться средства защиты, указанные в табл. 3.4, и специальные средства приема, обработки и передачи на управляющий КСА (УК) информации о НСД.

На управляющих КСА (УК) должны быть соответствующие средства централизованного сбора и управления безопасностью информации АСУ и СПД. Предполагается, что данные средства войдут в состав функциональной подсистемы, которую назовем центром управления безопасностью информации в АСУ (ЦУБИ АСУ) и соответственно в СПД (ЦУБИ СПД).

Управление доступом к информации в СПД и АСУ осуществляется при их подготовке, в процессе эксплуатации и завершения работ.

При подготовке СПД и АСУ к эксплуатации управление доступом заключается в выполнении следующих функций:

- уточнении задач и распределении функций пользователей и элементов сети и АСУ;
- контроле ввода адресных таблиц в элементы сети;
- вводе таблиц полномочий элементов сети и АСУ, пользователей;
- выборе значений, распределении и рассылке паролей и ключей шифрования по назначению;

В процессе эксплуатации управление доступом предполагает:

- контроль за конфигурацией АСУ и СПД;
- контроль за аутентификацией пользователей и элементов сети и АСУ;
- контроль за соблюдением полномочий элементами сети, пользователями и своевременное обнаружение и блокировку НСД;

- контроль за соблюдением правил шифрования данных и применением ключей шифрования;
- регистрацию всех фактов обращений пользователей одного КСА к информации другого КСА с указанием соответствующих атрибутов;
- сбор, регистрацию и документирование информации о НСД с указанием места, даты и времени события;
- выбор, распределение, рассылку и синхронизацию применения новых значений ключей шифрования;
- изменение и ввод при необходимости новых полномочий элементов сети, процессов, терминалов и пользователей;
- контроль за функционированием перечисленных функций;
- проведение организационных мероприятий по защите информации в СПД и АСУ.

Предполагая вопрос о большом времени реакции системы контроля на сигнал НСД в региональных и глобальных системах, предлагается в целях уменьшения этого времени передавать сигнал в первую очередь на средства управления защитой КСА АСУ (СПД), ближайшего канала связи, подвергнувшегося нападению, а затем на указанные выше централизованные средства управления. Это говорит о необходимости иметь подобные средства на каждом КСА АСУ и УК СПД. В настоящее время в роли датчиков обнаружения нападений могут также выступать межсетевые экраны.

Например, для рассматриваемой АСУ в целях обеспечения управления защитой информации по I классу может быть предложен следующий состав средств управления.

В состав ЦУБИ АСУ должны входить:

- автоматизированное рабочее место централизованного управления безопасностью информации (АРМ ЦУБИ);
- специально выделенный ПК;
- сервер базы данных по обеспечению безопасности;
- сервер регистрации и документирования;
- принтер;
- межсетевой экран.

На АРМ ЦУБИ должна обеспечиваться возможность выполнения следующих функций:

- отображения единого времени АСУ;
- отображения действующей конфигурации АСУ и СПД;
- ведения списка должностных лиц – пользователей АСУ;
- отображения организационной структуры должностных лиц – пользователей АСУ;
- ведения таблиц паролей пользователей, допущенных к информационному обмену между КСА;
- ведения таблиц полномочий пользователей, АРМ, КСА;
- генерации паролей, ключей преобразования, шифрования и кодов цифровой подписи в виде случайных чисел;
- централизованного распределения и автоматизированной рассылки паролей, ключей шифрования и кодов цифровой подписи по назначению;

- автоматизированной подготовки носителей таблиц паролей и полномочий пользователей, АРМ к их загрузке в АРМ, серверы и вычислительные комплексы (ВК) КСА;
- автоматизированной подготовки носителей ключей абонентского шифрования информации, передаваемой по каналам связи сети передачи данных;
- контроля результатов аутентификации пользователей, АРМ на входах КСА;
- централизованного сбора и отображения в сопровождении звуковой сигнализации сообщений о НСД и его атрибутов;
- получения по запросу за любой промежуток времени справки по выдаче (приему) с (на) КСА сообщений с возможностью ее получения по имени пользователя, АРМ по заданному объекту обращения (документу, техническому средству, КСА);
- получения с КСА по вызову оператора отдельных справок по НСД за заданный промежуток времени;
- получения с СПД и отображения справки о состоянии связи перечисленных КСА между собой;
- сбора и учета «открытых» кодов цифровой подписи пользователей, их регистрации и отображения с атрибутами переданного сообщения: времени и даты отправления, имени пользователя, адреса отправителя и получателя, заголовка, номера квитанции о приеме, времени и даты получения;
- маркировки, электронной идентификации и регистрации машинных носителей.

Специальный ПК должен обеспечивать возможность централизованного сбора, обработки и рассылки информации по управлению безопасностью информации в АСУ и выполнение следующих функций:

- сбор и обработку информации с КСА, а также с межсетевых экранов ЦУБИ;
- прием, обработку и выдачу информации по командам АРМ ЦУБИ;
- рассылку по командам оператора АРМ ЦУБИ паролей, ключей шифрования;
- автоматическую выдачу контрольных сообщений о наступлении сроков замены значений паролей, ключей шифрования информации.

Сервер базы данных ЦУБИ должен обеспечивать возможность записи, хранения и выдачи следующих данных:

- списков должностных лиц – пользователей, их условных номеров, таблиц паролей, таблиц полномочий, таблиц ключей шифрования, «открытых» ключей цифровой подписи;
- действующей оргштатной структуры АСУ;
- справок, запрашиваемых оператором АРМ ЦУБИ;
- входящих и исходящих документов службы безопасности;
- адресных таблиц СПД.

Сервер регистрации должен обеспечивать возможность регистрации всех обращений пользователей, включая и несанкционированные, к информации и ресурсам ЦУБИ, запрашиваемых справок и распечатки документов на «твердый» носитель, а также ведение архива и журналов регистрации сообщений и результатов их обработки в АСУ.

При функционировании ЦУБИ должна обеспечиваться безопасность собственной информации на уровне входящих в нее технических средств: АРМ ЦУБИ, серверах, ПК по методу, приведенному в разд. 3.5, а информации на уровне ЦУБИ как подсистемы в целом – по методу данного раздела.

Централизованный контроль и управление безопасностью собственной информации центра должны обеспечиваться **также с АРМ ЦУБИ**. Пример структуры системы безопасности информации в АСУ и СПД приведен на рис. 3.11.

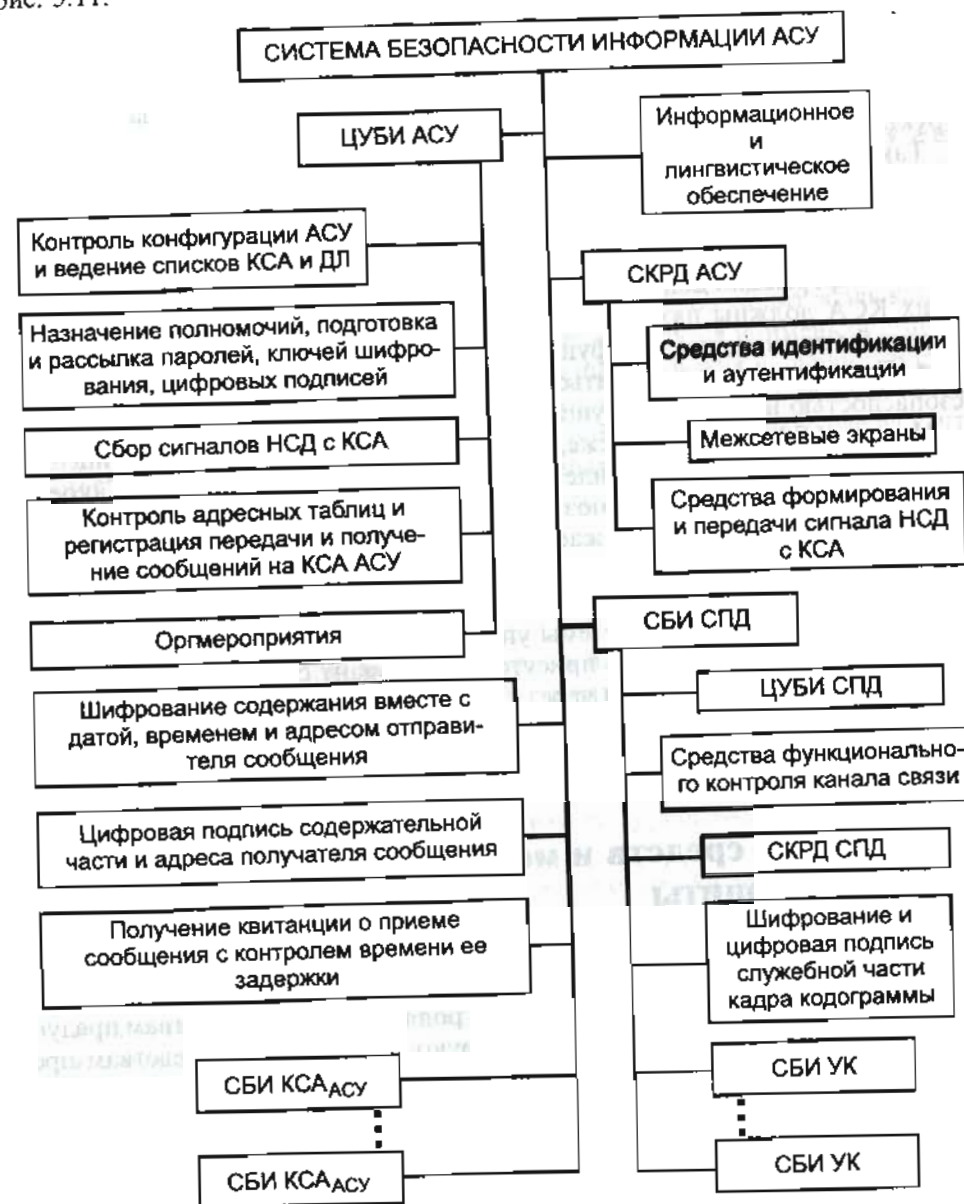


Рис. 3.11. Структурная схема системы безопасности информации АСУ

В состав СБИ АСУ (см. рис. 3.11) предложены следующие средства:

- группа средств контроля и разграничения доступа (СКРД);
- средства шифрования содержательной части сообщения;
- средства цифровой подписи содержательной части и адреса получателя сообщения;
- средства получения квитанции о приеме сообщения с контролем времени ее задержки;
- системы безопасности информации КСА, входящих в АСУ;
- системы безопасности информации (СБИ) сети передачи данных;
- центр управления безопасностью информации АСУ;
- информационное и лингвистическое обеспечение безопасности.

Однако глобальная АСУ может иметь многоступенчатую иерархическую структуру, например такую, как на рис. 1.32 (СПД на рисунке не показана).

Такая структура, как правило, отражает структуру организации, процесс функционирования которой АСУ автоматизирует. КСА на каждом уровне (кроме последнего) такой структуры является управляющим по отношению к КСА нижнего уровня. Логично предположить, что и управление безопасностью информации должно производиться по такой же схеме, и на управляющих КСА должны находиться средства, выполняющие функции ЦУБИ. Масштабы применения этих функций с понижением уровня управления убывают. Поэтому может измениться и состав технических средств управления безопасностью на соответствующих уровнях.

На рис. 1.32 показано также, почему в основу предлагаемой концепции защиты положена модель в виде триады, приведенной на рис. 3.2. Такое решение принято потому, что с позиций размещения, распределения и безопасности информации она отражает элементы практически всех возможных структур сетей и АСУ: с сосредоточенной обработкой данных (технические средства, КСА) и с распределенной обработкой (локальные, региональные и глобальные системы и подсистемы управления, сети передачи данных и вычислительные сети). В модели присутствует вариант связи объектов автоматизации по прямым каналам и через третий объект, который может быть управляющим, т.е. модель может быть также базовым элементом иерархической структуры, приведенной на рис. 1.32.

3.6.6. Анализ средств и метод расчета прочности защиты

Анализ средств защиты, приведенных в табл. 3.4, позволяет определить, какие средства относятся к средствам контроля, а какие – к средствам предупреждения, а также какие средства дублируют друг друга. К средствам предупреждения относятся преграды со значениями прочности: $P_1, P_2, P_3, P_4, P_5, P_6, P_{10}, P_{11}, P_{12}, P_{13}$. Их значения вычисляются по формулам (3.1), (3.2).

К средствам контроля относятся преграды, имеющие следующие значения прочности:

$$P_7, P_8, P_9, P_{14}, P_{15}.$$

Их значения вычисляются по формуле (3.8).

Дублируют друг друга преграды со значениями P_1, P_{10} . Их суммарное значение определяется по формуле (3.18). Но оно при сравнении с другими средствами защиты этой же защитной оболочки будет наверняка избыточным. Поэтому линейное шифрование для защиты от этой угрозы можно не применять.

Итоговое значение прочности неконтролируемой оболочки защиты согласно формуле (3.14) будет составлять наименьшую величину после вычисления и сравнения значений $P_1, P_2, P_3, P_4, P_5, P_{10}, P_{11}, P_{12}$ и результата вычисления значений прочности после дублирования преград. Аналогично получаем значение прочности контролируемой оболочки, применяя формулу (3.16).

Для ответственных систем целесообразно значение прочности неконтролируемой оболочки рассчитывать по формуле (3.15).

Для получения показателей прочности защиты информации в АСУ в целом дополнительно привлекаем значения прочности защиты информации в КСА и СПД, входящих в ее состав. Расчеты ведем аналогичным образом.

Если важность обрабатываемой на разных уровнях АСУ информации отличается между собой (на верхних объектах автоматизации согласно иерархии она более ценная), то расчет прочности защиты производится для каждого уровня КСА отдельно и за результат оценки берутся наименьшие значения прочности защиты информации КСА данного уровня иерархии. В СПД оценку прочности защиты производим, исходя из того, что в ее КСА (УКС) возможно появление информации любого уровня АСУ, из чего следует, что в этом случае при оценке необходимо учитывать КСА с наименьшими значениями прочности. Для СПД можно получить отдельную оценку, используя показатели ее средств и системы защиты.

Отдельным показателем, как и в КСА, целесообразно представить защиту обращений законных пользователей одного КСА АСУ к информации другого КСА по паролю, так как здесь предполагается применить специальный алгоритм аутентификации по одноразовому паролю.

В конечном итоге оценка прочности защиты в системе с распределенной обработкой данных, например, для структуры, приведенной на рис. 3.4, будет состоять из группы показателей. Количество показателей в группе будет зависеть от степени важности информации, циркулирующей в каждом КСА АСУ и каналах связи. Если она одинаковая, то группа будет включать следующие показатели:

- показатель прочности *контролируемой оболочки* защиты информации (КСА АСУ с наименьшими значениями);
- показатель прочности *превентивной оболочки* защиты информации КСА (АСУ с наименьшими значениями);

- показатель *стойкости пароля* пользователя КСА АСУ;
- группа показателей прочности защиты *кодограммы*;
- группа показателей СПД.

В группу показателей прочности защиты *кодограммы* войдут:

- показатель прочности *контролируемой оболочки* защиты кодограммы (из состава средств контроля, перечисленных в таблице);

- показатель прочности *превентивной оболочки* защиты кодограммы (из состава средств предупреждения, перечисленных в таблице);

- показатель стойкости пароля сетевой аутентификации.
- В группу показателей СПД войдут:
- показатель прочности контролируемой оболочки защиты информации УК с наименьшими значениями;
 - показатель прочности превентивной оболочки защиты информации УК с наименьшими значениями;
 - показатель стойкости пароля пользователя УК.

Если степень важности информации, циркулирующей в отдельных КСА и каналах связи, выше или ниже общего показателя, то их показатели защиты целесообразно задать дополнительно отдельным перечнем.

3.6.7. Технология проектирования защиты информации АСУ

На основании изложенного можно предложить следующий порядок проектирования системы безопасности информации в АСУ:

- 1) определение перечня, динамики, важности и цены данных, обрабатываемых в КСА и передаваемых по каналам связи СПД;
- 2) выбор модели ожидаемого поведения потенциального нарушителя и соответствующих ей каналов несанкционированного доступа к информации КСА и угроз информации, передаваемой по каналам связи;
- 3) разработка системы безопасности информации в КСА и оценка ее прочности;
- 4) выбор для защиты кодограммы обмена информацией готовых или разработка новых средств защиты, обладающих приемлемыми расчетными характеристиками;
- 5) адаптация или встраивание в систему средств защиты, анализ и оценка их на предмет прочности и полноты перекрытия возможных каналов НСД к информации КСА и потенциальных угроз на каналах связи;
- 6) создание в разрабатываемой системе централизованных средств контроля и управления защитой на всех уровнях иерархии системы;
- 7) качественная и количественная оценка прочности защиты информации по каждому объекту: КСА, УК, СПД и АСУ в целом.

На основе вышеизложенного можно сделать выводы.

1. Приведенный метод построения защиты является руководством, с помощью которого можно осуществить разработку, анализ, распределение и расчет прочности отдельных средств защиты кода кодограммы, а затем (с учетом метода построения защиты информации в КСА) и всей системы защиты информации в АСУ.

2. В разделе 3 предложены достаточно строгая постановка задачи, опирающаяся на конкретные виды АСУ, и методология ее решения с возможностью получения количественных показателей прочности защиты.

3. Изложенное в разд. 3 позволяет сформулировать важное определение. Автоматизированная система считается безопасной в смысле обработки информации, если в ней предусмотрена система централизованно управляемых и взаимосвязанных преград, перекрывающих с гарантированной прочностью

заданное в соответствии с моделью потенциального нарушителя количество возможных каналов НСД к информации, подлежащей защите от угроз, направленных на утечку, модификацию и утрату ее владельцем или его доверенным лицом.

3.7. Основные принципы и порядок проектирования защиты

3.7.1. Основные принципы проектирования защиты

Система безопасности информации встраивается в АС и является ее неотъемлемой составной частью, придающей ей важное качество. Поэтому ее созданию свойственны все этапы создания АС: разработка технических предложений, эскизный и технический проекты, выпуск рабочей документации, изготовление, испытания и сдача системы заказчику.

Отсюда следует основное требование к порядку проведения работ, заключающееся в необходимости *параллельного проектирования* системы защиты информации с проектированием системы управления и обработки данных, начиная с момента выработки общего замысла построения АС.

Невыполнение этого принципа, «наложение» или «встраивание» средств защиты в уже готовую систему, может привести к низкой эффективности защиты, невозможности создания цельной системы защиты, снижению производительности и быстродействия вычислительных средств, а также к большим затратам.

При параллельном проектировании разработчиками системы защиты информации (СЗИ) производится анализ циркуляции и мест сосредоточения информации. В проекте АС, определяются наиболее уязвимые для НСД точки и своевременно предлагаются взаимоприемлемые технические решения по сокращению их количества путем изменения принципиальной схемы АС, что позволит обеспечить простоту, надежность и экономичную реализацию защиты с достаточной эффективностью. Функционирование механизма защиты должно планироваться и обеспечиваться наряду с планированием и обеспечением процессов автоматизированной обработки информации, что важно для определения степени влияния СЗИ на основные вероятностно-временные характеристики АС, которые, как правило, изменяются в сторону ухудшения. Но это является платой за приобретение нового и необходимого качества, которая иногда является причиной пренебрежительного отношения некоторых разработчиков и заказчиков АС к защите. За такую недальновидность им придется расплачиваться потом несоизмеримо более дорогой ценой.

При разработке технического задания и дальнейшем проектировании АС следует помнить, что создание системы защиты информации – *задача не второстепенная*, ибо невыполнение ее может быть причиной недостижения цели, поставленной АС, потери доверия к ней, а в некоторых случаях утечки и модификации информации – причиной более тяжелых последствий.

Техническое задание на проектируемую АС должно содержать перечень сведений и характеристик, подлежащих защите, возможные пути циркуляции и места их сосредоточения, а также специальные требования к системе защиты информации. Если это АСУ или вычислительная сеть, то должна соблюдаться *иерархия требований* с СЗИ. Они должны входить:

- в общее техническое задание на АСУ или сеть в целом;
- в частные технические задания на функциональные подсистемы управления, на отдельные автоматизированные звенья, объекты, комплексы, технические средства;
- в технические задания на сопряжение с внешними системами;
- в технические задания на общее программное обеспечение отдельных ЭВМ и вычислительных комплексов, на специальное программное обеспечение элементов вычислительной сети и АСУ.

Требования общего технического задания к вычислительной сети и АСУ являются руководящими для частных технических заданий подсистем, звеньев, объектов и т.д.

При этом в АСУ *требования* на подсистемы одного уровня иерархии, информационно связанные с одним вышестоящим объектом автоматизации, должны быть *унифицированы* между собой и не вступать в противоречие.

При проектировании защиты следует внимательно провести *исследование* разрабатываемой АС на предмет *выявления* всех возможных каналов несанкционированного доступа к информации, подлежащих защите, средствам ее ввода-вывода, хранения, обработки и только после этого строить защиту. Первое знакомство с разрабатываемой АС должно закончиться рекомендациями по сокращению обнаруженных каналов доступа путем ее принципиальных изменений без ущерба выполнению основных задач.

Анализ важнейших задач организации и формирования функций, удовлетворяющих целям управления, носит обычно итеративный характер, обеспечивающий *последовательное уточнение задач* и функций, согласование их на всех уровнях и ступенях АС и сведение в единую функциональную схему. Это означает, что проведенные на некотором этапе проектирования технические решения, накладываемые системой защиты на основные задачи АС, должны проверяться по степени их влияния на решения основных процессов управления и наоборот: после принятия решения по изменению основных процессов управления и составу технических средств должно проверяться их соответствие решениям по защите информации, которые при необходимости должны корректироваться или сохраняться, если корректировка снижает прочность защиты, и т.д.

Важную роль играет *простота* системы защиты. Она должна быть простой настолько, насколько позволяют требования по ее эффективности. Простота защиты повышает ее надежность функционирования, экономичность, уменьшает ее влияние на вероятностно-временные характеристики АСУ, создает удобства в обращении с ней. При неудобных средствах защиты пользователь будет стараться найти пути ее обхода, отключить ее механизм, что делает защиту бессмысленной и ненужной.

При проектировании защиты, как и в обычных разработках, вполне разумно применение унифицированных или стандартных средств защиты. Од-

нако желательно, чтобы указанное средство при применении в проектируемой АС приобрело *индивидуальные свойства защиты*, которые бы потенциальному нарушителю не были известны.

Данные по защите информации в проектируемой АС должны содержаться в отдельных документах и *засекречиваться*. Нельзя согласиться с рекомендуемым зарубежными специалистами [78] принципом несекретности проектирования защиты. Ознакомление опытных и квалифицированных специалистов с уязвимыми точками проекта на предмет его доработки можно осуществить путем организации контролируемого допуска их к секретному проекту. В этом случае, по крайней мере, будут известны лица, ознакомленные с проектом. Таким образом сокращается число лиц – потенциальных нарушителей, а лица, ознакомленные с проектом, несут ответственность перед законом, что, как известно, является сдерживающим фактором для потенциального нарушителя.

В процессе проектирования и испытаний рекомендуется по возможности использовать исходные *данные, отличающиеся от действительных*, но позволяющие при последующей загрузке системы действительными данными не проводить доработки. Загрузка действительных данных должна производиться только после проверки функционирования системы защиты информации в данной АС.

Учитывая то, что защита информации в АС предусматривает, кроме аппаратно-программных средств, применение в качестве преграды и организационных мероприятий, выполняемых человеком – наиболее слабым звеном защиты, необходимо стремиться к максимальной *автоматизации* его функций и сокращению доли его участия в защите.

Для того чтобы спроектированная система защиты обрела жизнь, необходимо также, чтобы технические средства защиты по возможности не ухудшали вероятностно-временные характеристики АС: быстрдействие, производительность и др. При проектировании необходимо найти разумное соотношение в удовлетворении тех и других требований.

3.7.2. Порядок проектирования защиты

Решение вопросов создания СБИ должно поручаться лицам *одного уровня* с лицами, занимающимися вопросами функционирования АС. У главного конструктора АС должен быть соответствующий *заместитель*, профессионально отвечающий за качество СБИ. На всех документах, касающихся изменений АС, должна быть его виза. Под его руководством должно работать подразделение специалистов, профессионально занимающихся разработкой СБИ АС. Разработка СБИ требует привлечения *специалистов широкого профиля*, знающих, кроме системных вопросов, вопросов программного обеспечения, разработки систем, комплексов и отдельных аппаратных средств, специальные вопросы защиты информации. В этом подразделении независимо от масштабов работ должно быть как минимум три направления: анализа АС на предмет постановки задач СБИ, проектирования СБИ и применения готовых криптографических средств.

Для построения системы защиты информации в комплексе средств автоматизации к началу рабочего проектирования должны быть известны следующие исходные данные:

- назначение и выполняемые функции;
- состав и назначение аппаратных и программных средств;
- структурная или функциональная схема;
- структура и состав информационной базы;
- перечень, время жизни, важность, места размещения и циркуляции сведений, подлежащих защите;
- модель ожидаемого поведения потенциального нарушителя;
- состав, количество и виды внутренних и выходных документов;
- описание функциональных задач прикладного программного обеспечения;
- состав и выполняемые функции должностных лиц – пользователей и обслуживающего персонала;
- режим работы (закрытый или открытый, круглосуточный или с перерывами, оперативный или пакетный);
- способы и средства загрузки программного обеспечения;
- базовые вычислительные средства и их характеристики;
- интенсивность отказов входящих технических средств;
- показатели качества функционального контроля;
- план и условия размещения технических средств на объекте эксплуатации.

Перечисленные данные являются параметрами конкретного объекта автоматизации. Его назначение и выполняемые функции дают первое представление о необходимом уровне защиты информации (например, для военных целей – один уровень, для гражданских – другой и т.д.). Уточняет эту задачу режим работы КСА, а также перечень сведений, подлежащих защите. Состав и назначение аппаратных средств, структурная и функциональная схема, способ загрузки программного обеспечения, план размещения технических средств и другие параметры дают представление о возможных каналах несанкционированного доступа к информации, подлежащей защите. Перечень ВКНСД представлен выше (подразд. 3.5). Однако он не является исчерпывающим, или наоборот, некоторые ВКНСД на конкретном КСА могут отсутствовать. Это зависит также от заданных модели поведения нарушителя и класса безопасности информации КСА.

Перечень сведений, подлежащих защите, состав, количество и виды документов, содержащих эти сведения, дают представление о предмете защиты. Состав и выполняемые функции должностных лиц – пользователей и обслуживающего персонала, структура и состав информационной базы, операционная система программного обеспечения базовых вычислительных средств позволяют построить систему контроля и разграничения доступа к информации, подлежащей защите от преднамеренного НСД. Интенсивность отказов входящих в комплекс технических средств и показатели качества функционального контроля необходимы для оценки эффективности защиты от случайных НСД. План размещения и состав технических средств, а также данные о наличии соответствующих датчиков дают представление о возмож-

ности и выборе принципов построения системы контроля вскрытия аппаратуры и системы контроля доступа в помещения объекта эксплуатации КСА.

При построении системы защиты информации в распределенных АС должны быть известны следующие исходные данные:

- структура, состав, назначение и задачи АС и ее элементов;
- территориальное размещение ее элементов;
- информационные процессы, подлежащие автоматизации;
- задачи и функции управления, их распределение между исполнителями;
- схема информационных потоков и места сосредоточения информации, подлежащей защите;
- структура, состав и размещение информационной базы;
- перечень, размещение, циркуляция, важность и сроки сохранения сведений, подлежащих защите;
- перечень, форма и количество входных, внутренних и выходных документов (при взаимодействии с другими АС);
- режим использования (открытый, закрытый и т.д.);
- вероятностно-временные характеристики обработки сообщений;
- органы управления и их размещение в АС.

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ С СОСРЕДОТОЧЕННОЙ ОБРАБОТКОЙ ДАННЫХ

4

4.1. Системы охранной сигнализации на территории и в помещениях объекта обработки информации

4.1.1. Требования к системам охранной сигнализации

Создание на территории некоторой замкнутой зоны с установкой преграды по периметру является очень старой проблемой, и по этому вопросу имеется много отечественной и зарубежной литературы. Анализ принципов построения и параметров данных систем, а также принятая выше концепция построения системы защиты позволяют сформулировать следующие требования к таким системам:

- максимальная полнота охвата контролируемой зоны;
- минимальная вероятность необнаруживаемого обхода преграды нарушителем;
- достаточные избирательность и чувствительность к присутствию, перемещению и другим действиям нарушителя;
- возможность исключения «мертвых» зон и простота размещения датчиков обнаружения;
- устойчивость к естественным случайным помехам;
- удовлетворительное время обнаружения нарушителя;
- достаточно быстрая и точная диагностика места нарушения;
- простота и надежность конструкции;
- возможность централизованного контроля событий;
- приемлемая стоимость.

Выполнение одной системой всех указанных требований является непростой задачей. Важным моментом в построении охранных систем являются датчики обнаружения нарушителя, область охвата контролируемой зоны

которыми ограничена их физическими свойствами. По этой причине в зависимости от конкретных условий часто применяют не одну, а несколько охранных систем, объединяя их в один охранный комплекс.

Рассмотрим кратко некоторые системы.

4.1.2. Наружные системы охраны

Существует ряд устройств охраны, которые устанавливаются снаружи охраняемого помещения на ограждениях или под землей и образуют предварительную линию защиты. Такие системы целесообразно использовать для больших земельных участков, территорий промышленных предприятий и т.д.

Наружные устройства охранной сигнализации должны иметь стабильные характеристики, не подверженные влиянию условий окружающей среды. В наружных системах охраны используются специализированные устройства: подземные датчики и датчики «прикосновения». Последние устанавливаются на опорных столбах или на проволоочной решетке заграждений и срабатывают при попытке перелезть через ограду, перерезать ее или сломать. Американская фирма Sylvania, например, выпустила систему FPS (*Fence Protection System*), которая состоит из датчика, процессора с предварительным программированием и сигнального устройства. Датчик — это тонкий коаксиальный кабель специальной конструкции, который фактически представляет собой микрофон, чувствительный к колебаниям звуковой частоты. При малейших вибрациях ограды между центральным проводником и экраном возникает переменное электрическое поле. Частота колебаний и временные характеристики сравниваются с предварительно запрограммированными данными, и в случае рассогласования включается сигнал тревоги. Длина коаксиального кабеля может достигать 300 м. В системе имеется специальное устройство, предотвращающее ложные срабатывания, а также схема, срабатывающая при попытке перерезать кабель.

К кабельным периметральным охранным системам также относятся английская GUARDWIR и российская «Ворон».

В системе охраны Intertiaquard Fence System американской фирмы Morse Products в качестве чувствительных элементов используются отдельные датчики, расположенные на ограде между опорным столбом и сеткой на расстоянии 6 м один от другого. Каждый датчик представляет собой герметичный водонепроницаемый пластмассовый корпус, в котором находится металлизированный шарик, лежащий на трех выступах. Масса шарика и расположение выступов обеспечивают такой режим работы датчика, при котором система реагирует только на колебания, возникающие при попытке перелезть через ограду, и не воспринимает ложные сигналы. Выходные сигналы датчиков поступают на твердотельный электронный анализатор, который распознает определенную частотно-временную комбинацию и начинает счет. Когда число отсчетов достигает 4–8, система включает сигнал тревоги. На панели управления зажигается лампочка, указывающая, в какой зоне произошло нарушение. Каждый анализатор контролирует до 25 датчи-

ков (это соответствует одной зоне), а всего система может следить за 20 зонами.

Подземные датчики разделяются на сейсмические, магнитные и датчики давления. Необходимо, чтобы все подземные датчики обладали стабильными характеристиками, не зависящими от состава почвы и атмосферных условий. Зону чувствительности следует делать как можно более узкой с целью уменьшения вероятности ложных срабатываний, но защитный «барьер» должен иметь достаточную протяженность над землей и вглубь, чтобы через него нельзя было перепрыгнуть или сделать под ним подкоп.

Сейсмические датчики – геофоны – аналогичны используемым при геофизических исследованиях. Они соединяются последовательно, а перекрывающиеся диаграммы направленности создают непрерывную линию защиты.

Недостатком магнитных датчиков является то, что они срабатывают от множества сигналов, часто оказывающихся ложными. В значительной степени этот недостаток уменьшается средствами электроники.

Датчики давления в отличие от магнитных обладают высокой избирательной способностью по отношению к внешним сигналам, следовательно, их помехозащищенность выше. Многие датчики давления являются электретными устройствами, т.е. любое незначительное перемещение проводника по отношению к диэлектрику с накопленным зарядом вызывает на выходе датчика появление электрического сигнала, пропорционального этому перемещению. В подземных магнитных датчиках используется эффект Виллари, который заключается в изменении магнитной индукции, когда вдоль продольной оси металлического намагниченного стержня действует сила давления. Стержень располагают вдоль оси обмотки, и давление, приложенное к стержню, преобразуется в выходное напряжение.

В настоящее время разрабатываются наружные системы охраны с использованием микропроцессоров, которые должны распознавать и идентифицировать причину, вызвавшую срабатывание датчика, с тем чтобы предотвратить появление ложного сигнала тревоги.

К системам прерывания луча, телевизионным и радиолокационным системам, используемым в качестве наружных средств охраны, также предъявляется дополнительное требование – независимость характеристик от условий окружающей среды. В инфракрасных и лазерных системах это достигается с помощью модуляции луча. В большинстве инфракрасных систем протяженность луча не превышает 90 м, в некоторых системах – достигает 300 м.

В отдельных случаях целесообразно применять многолучевые системы, эффективность которых значительно выше, так как вместо защитной линии формируется защитная стена. Многолучевую систему можно сформировать посредством зеркал или расходящегося пучка излучения.

Следует заметить, что полностью исключить влияние метеоусловий на лучевые системы не удастся, поэтому возникает ряд ограничений, например расстояние между излучателем и приемником (размеры контролируемой зоны) не должно превышать определенной величины, чтобы система нормально функционировала во время снегопадов, тумана и т.д.

4.1.3. Традиционные системы

Эти системы реализуются либо на токопроводящих линиях, подводимых к контактам, встроенным в оконные стекла и дверные проемы (коммутационные системы), либо на датчиках звукового давления, сигнализирующих о проломах витрин, потолков, стен и взломе сейфов, либо на емкостных датчиках, реагирующих на приближение человека к охраняемым объектам (сейфам, кассам и т.п.).

Коммутационные системы являются простейшим и дешевым типом устройств охранной сигнализации. Большинство из них сконструировано таким образом, что срабатывание происходит при размыкании сигнальной цепи.

Простейшая коммутационная система состоит из микропереключателя или магнитного переключателя с нормально-замкнутыми контактами (в рабочем состоянии контакты разомкнуты), устанавливаемого на двери или на окне, звонка или зуммера и батареи питания. Достоинством таких устройств являются низкая стоимость, простота конструкции и установки. Но устройства такого типа малоэффективны, так как датчик контролирует одну конкретную точку, а для отключения сигнализации достаточно перерезать провода. Недостатком системы является и то, что отсутствует активный контроль цепи и простое отключение питания.

Несколько более сложная для нарушителя коммутационная система создана на базе переключателя-детектора с нормально-разомкнутыми контактами. Детектор, устанавливаемый на двери или окне, состоит из магнита и язычкового переключателя и срабатывает при размыкании цепи. При этом сигнал тревоги выключается только при отключении питания. Кроме того, в систему может входить автоматическое устройство, которое через определенное время отключает сигнализацию. Сигнальные провода можно замаскировать снаружи помещения так, чтобы сигнальная цепь размыкалась до того, как взломщик войдет в дом. Величина рабочего тока обычно мала. Для различных типов устройств она колеблется в пределах от 30 мкА до 10 мА. Задача нарушителя здесь заключается в поиске сигнальных цепей и последующем их замыкании, после которого такое устройство не работает.

Защитой от обрыва и замыкания сигнальных цепей обладают **контактные датчики с резисторами**. В настоящее время датчик и подключенные к нему сигнальные цепи называют шлейфом. Несколько шлейфов с подключенной к ним контрольной панелью (приемно-контрольным прибором) образуют простейшую систему охранной сигнализации. Для увеличения количества шлейфов применяются специальные расширители: к одному расширителю подключается одна группа шлейфов, к другому расширителю – другая и т.д. Расширители подключаются к специально образованной из нескольких проводов информационной шине, с которой поступает информация на более сложную контрольную панель. Такая контрольная панель может также подключаться к телефонной линии, а через сетевую карту – и к компьютеру. Образуется древовидная структура, позволяющая построить централизованную многофункциональную систему охранной сигнализации.

В контактной схеме с резисторами применяется схема шлейфа, приведенная на рис. 4.1¹.

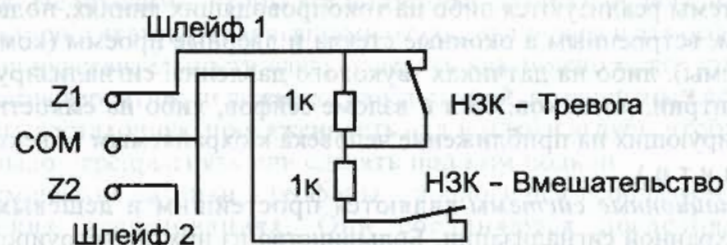


Рис. 4.1. Схема шлейфа с резисторно-контактными датчиками:
НЗК – нормально-замкнутый контакт

Такая схема позволяет различать следующие четыре состояния:

Сопротивление шлейфа	Состояние шлейфа	Реакция системы
0 Ом	Закорочен	ВМЕШАТЕЛЬСТВО
1 кОм	Не нарушен	НОРМА
2 кОм	Нарушен	ТРЕВОГА
Бесконечно	Обрыв	ВМЕШАТЕЛЬСТВО

Устройства охраны, выполненные на емкостных датчиках, реагируют на изменение величины электрической емкости при приближении к объекту посторонних лиц. Прибор CPS-1 американской фирмы GTE Sylvania предназначен для охраны различного рода металлических предметов (сейфов, картотек, пультов и т.д.). Устройство может контролировать одновременно до 20 объектов и срабатывает при приближении человека на расстояние в несколько дюймов, а также при обрыве соединительных проводов и перебоях в подаче питания. Изменения емкости, вызванные изменением условий окружающей среды (например, влажности), не влияют на работу устройства.

Вибрационный датчик фирмы Sai Rodar обладает чрезвычайно высокой чувствительностью и способен улавливать колебания, возникающие при попытках вырезать стекло в окне или в витрине стеклорезом. При этом он абсолютно не подвержен воздействию уличных шумов или громкой музыки и не требует специальной настройки. При желании к одному блоку управления можно подключать несколько таких датчиков (число их не ограничивается) или применять их совместно с магнитными переключателями. Тревожная сигнализация включается также при коротком замыкании, обрыве проводов и при попытке их перерезать. В случае повреждения сети питания система переключается на питание от встроенной батареи, срок службы которой составляет 2–3 года. Диапазон рабочих температур от –15 до +60°C.

¹ См.: Контрольные панели Securit 724/764: Справочное пособие. – СПб.: C&K Systems (Europe) BV, 1997.

4.1.4. Ультразвуковые системы

В комплекс аппаратуры входят излучатель ультразвуковых волн и приемник (микрофон). Излучаемые волны (диапазон частот, как правило, от 35 до 60 кГц) отражаются от стен и предметов обстановки и воспринимаются микрофоном. В помещении образуются стоячие волны; значение напряженности поля в месте установки микрофона является опорной величиной, от которой ведется отсчет системой. При перемещении какого-либо объекта внутри звукового поля изменяется распределение напряженности поля. Эти изменения «улавливаются» микрофоном, и примерно через 20–30 с подается сигнал тревоги. Система не реагирует на кратковременное возмущение, вызываемое, например, летящим насекомым.

Существуют три варианта применения этих систем.

1. Охрана конкретных предметов (письменный стол, шкаф, картина) путем их непосредственного облучения ультразвуком. Сигнал тревоги подается немедленно при приближении к охраняемому объекту посторонних лиц.
2. Охрана целого помещения или какой-то его части (зоны); для этих целей ультразвуковой «луч» направляется на вход или на определенную зону помещения таким образом, что нарушитель обязательно его пересечет.
3. В случае нескольких смежных помещений организуется охрана того места, через которое вероятнее всего будет проникать взломщик (вход, вестибюль, лестничная клетка).

Излучатель и приемник могут размещаться в одном корпусе или выполняться в виде двух отдельных блоков. Датчик, выполненный как единое устройство, устанавливается на стене или потолке помещения и контролирует пространство радиусом приблизительно 6 м.

Если излучатель и приемник представляют собой отдельные блоки, то обычно они устанавливаются на потолке на расстоянии не более 6 м друг от друга.

Как правило, ультразвуковые системы предназначены для охраны лишь небольших закрытых помещений. Использование ультразвука – самый простой метод обеспечения защиты помещений площадью около 20 м².

Следует отметить, что ультразвуковые системы подвержены воздействию помех. Ложное срабатывание системы может быть вызвано порывом ветра, колыбанием оконных занавесок, движением воздуха, вызванным нагревательными приборами или кондиционером, сквозняком, а также некоторыми звуковыми сигналами, например шипением клапана батареи, свистом ветра в щелях оконных рам, телефонным звонком (поэтому в помещениях с ультразвуковыми системами охраны рекомендуется звонок заменять зуммером). Данный тип устройств охранной сигнализации пользуется большой популярностью, так как частота появления сигналов ложной тревоги мала, и, кроме того, системы имеют сравнительно низкую стоимость.

Изготовители ультразвуковых систем разрабатывают различные способы защиты от помех. Примером такого устройства является автономный ультразвуковой датчик Cyclops американской фирмы Macard Security Systems, изготовленный по новейшей технологии. Датчик способен отличить движение взломщика внутри охраняемого помещения от всякого рода случайных

помех и характеризуется высокой стабильностью. Устанавливать его можно на несущей поверхности (стенка или потолок) или в специальном углублении. Питание осуществляется от низковольтного трансформатора, а в случае выхода из строя цепи питания происходит автоматическое переключение на встроенную перезаряжаемую батарею.

4.1.5. Системы прерывания луча

В системах этого типа сигнал тревоги подается при прерывании инфракрасного (ИК), лазерного или светового луча (так называемого светового барьера) и при нарушении зоны действия электромагнитного или электростатического поля. Наиболее широко применяются ИК-устройства. Как правило, излучатель формирует ИК-луч, модулированный по закону импульсной модуляции. Приемник излучения настроен на частоту модуляции. В этом случае система не подвержена действию интерференционных помех от какого-либо постороннего источника световых колебаний. В качестве источника инфракрасного излучения широко применяются светоизлучающие диоды. Радиус действия инфракрасных систем составляет 3–300 м. Излучатель и приемник могут располагаться на расстоянии друг от друга или конструктивно объединяться в один блок. В первом случае сигнал тревоги включается, как только между ними оказывается посторонний объект, во втором – используется отраженный луч. Кроме того, имеются инфракрасные системы, работающие по принципу поглощения инфракрасного излучения, испускаемого телом человека.

Малогабаритная ИК-система Pulsar 30В фирмы *Takenaka Engineering* (Япония) состоит из источника и приемника инфракрасного излучения, которые устанавливаются перед входом или внутри охраняемого помещения. Обе части системы расположены так, что входящий в помещение человек обязательно пересекает луч, и в этот момент срабатывает сигнализация. В систему входит специальный зеркальный отражатель, что позволяет обеспечить достаточно большую дальность действия (30 м), несмотря на малые размеры самой системы. Внешнее освещение не влияет на работу системы, так как она работает по принципу импульсной модуляции.

4.1.6. Телевизионные системы

Телевизионные системы состоят из одной или нескольких телевизионных камер и видеоконтрольных устройств (мониторов). Необходимость постоянного наблюдения за экранами мониторов телевизионных систем охраны банков, универмагов, стоянок автомашин и других довольно утомительна для дежурных (особенно в ночные часы, когда «картинка» обычно не меняется). Для облегчения несения службы фирмой *Retan* разработан «телевизионный извещатель перемещения» типа VM 216, способный непрерывно следить за изображением, передаваемым 6–8 телевизионными камерами. Экран монитора остается затемненным до тех пор, пока в кадре не наблюдается

изменений. Если же, например, открывается дверь, то кадры немедленно воспроизводятся на экране и подается звуковой сигнал. Одновременно автоматически включается видеомagneтофон, записывающий изображение.

Телевизионный извещатель перемещения можно уподобить мини-процессору, «опрашивающему» до 20 раз в секунду изображения, поступающие с телевизионных камер, и сравнивающему их с предшествующим накопленным кадром. Цифровые схемы, использованные в устройстве, дают возможность варьировать режимы его работы. В частности, устройство можно запрограммировать таким образом, что оно будет следить лишь за совершенно определенными частями изображения; при этом на экране высвечиваются метки в тех местах кадра, где происходит перемещение предметов или лиц. Извещатель перемещения легко встраивается в уже имеющуюся телевизионную систему охраны; для этого достаточно подсоединить его к видеосигналу между телевизионными камерами и монитором.

4.1.7. Радиолокационные системы

Действие радиолокационных систем основано на изменении частоты отраженного сигнала (эффект Доплера). В зависимости от типа системы и высоты ее установки дальность обнаружения может составлять от нескольких десятков сантиметров до десятков метров. Большинство радиолокационных систем работает на частотах 900 МГц, некоторые системы работают в микроволновом диапазоне (10 ГГц). Изготавливаемые в настоящее время радиолокационные системы отличаются большой сложностью, поэтому выпуск таких систем может быть налажен только при высоком уровне технологии производства. Но в последнее время в Японии были разработаны УВЧ полупроводниковые элементы и ВЧ сигнал-генераторы, применение которых позволило значительно упростить конструкцию радиолокационных систем. Это вызвало рост числа фирм-изготовителей и увеличение выпуска таких систем.

В качестве примера системы на СВЧ-энергии можно назвать отечественную систему «ВИТИМ», специально разработанную для срочной организации временного рубежа охраны в условиях острого дефицита времени.

Недостатком радиолокационных систем является трудность обнаружения очень медленно движущихся объектов, а также недостаточная эффективность систем, установленных в помещениях, загроможденных мебелью (радиоволны отражаются от препятствий, поэтому отдельные участки комнаты могут превратиться в «мертвую» зону). Кроме того, радиолокационные системы нельзя использовать, когда в помещении находятся люди. Существенной проблемой является также сравнительно высокая стоимость систем.

4.1.8. Микроволновые системы

В состав микроволновых систем входят передатчик и приемник микроволнового диапазона, которые могут быть разнесены на расстояние до 300 м. Принцип обнаружения постороннего лица, пытающегося проникнуть

на объект, основан на прерывании направленного микроволнового «луча», вследствие чего сигнал на входе приемника ослабляется и срабатывает устройство тревожной сигнализации. Микроволновые датчики удобно использовать для установки в коридорах, проходах и других вытянутых в длину помещениях, так как передающая и приемная антенны могут быть выбраны таким образом, чтобы формировалась узкая, вытянутая диаграмма направленности. Способность микроволнового излучения проходить сквозь перекрытия из неметаллических материалов одновременно является и достоинством системы, и ее недостатком. Положительная сторона этого явления заключается в том, что охраняемая зона несколько расширяется, охватывая участки, прилегающие к охраняемому помещению. Но при этом создаются условия для воздействия помех, например, от движущихся транспортных средств, если датчики установлены таким образом, что излучение проникает за наружные стены объекта. Однако по сравнению с радиолокационными системами микроволновые устройства обладают значительно более высокой помехозащищенностью, так как проникающая способность излучения уменьшается с увеличением частоты. Срабатывание микроволновой системы может вызывать также близко расположенная люминесцентная лампа, поэтому датчики должны располагаться на расстоянии не менее 6 м от нее.

4.1.9. Беспроводные системы

Среди многочисленных устройств и систем охранно-пожарной сигнализации особое место занимают системы, использующие для передачи сообщений радиоканал. Это обусловлено, с одной стороны, дополнительными важными преимуществами, такими, как отсутствие соединительных проводов и быстрота установки, с другой – возникновением ряда специфических особенностей, связанных с надежностью канала связи, помехоустойчивостью, ресурсом источников питания и др. В качестве примера рассмотрим систему *SpreadNet* разработки «C&K Systems, Inc.».

Особенность этой системы заключается прежде всего в сигнале, используемом для передачи информации. Это шумоподобный сигнал, состоящий из 126 элементов, разных частот со спектром, распределенным в широкой полосе частот. Со спектральной точки зрения такой сигнал выглядит как шум. Поэтому крайне сложно не только зафиксировать его параметры, используя соответствующую аппаратуру, но даже обнаружить факт работы системы. При ширине рабочей полосы частот 2,4 МГц и выходной мощности передатчиков 100 мВт средняя мощность на полосу частот 10 кГц (как в обычной узкополосной системе) составляет 0,417 мВт. Длительность сигнала равна 7,6 мс.

Важнейшим требованием к любой системе охранной сигнализации является контроль за каналом связи. Требование контроля за каналом во много раз важнее и сложнее реализуется в системах, использующих радиоканал. Это обусловлено тем, что реально в радиосистемах постоянный контроль за каналом связи не осуществить, так как для этого требуется отдельный частотный канал для каждого передатчика. При разумных требованиях к таким системам контроль канала обычно осуществляется с той или иной периодич-

ностью. Система *SpreadNet* позволяет осуществить передачу тестовых сигналов контроля передатчиков с интервалом от 30 с до 5 мин.

Структура используемого сигнала обеспечивает также высокую помехоустойчивость системы. Для подавления сигнала необходимо создать помеху в широкой полосе частот (более половины ширины спектра), что достаточно сложно технически. Но даже при постановке такой помехи система зафиксирует тревогу. Это объясняется тем, что для этого необходимо решить противоречивую задачу. С одной стороны, подавить сигнал тревоги, а с другой – сохранить сигнал контроля передатчиков в той же полосе частот с теми же параметрами, что практически нереально.

Информативность сообщений от элементов системы (передатчиков) также весьма важный показатель. Система *SpreadNet* дает возможность регистрировать тревогу, вскрытие извещателей, разряд батарей, отсутствие сигнала контроля и нарушение линии связи приемник – интерфейс (контрольная панель).

Если при установке проводных систем охранно-пожарной сигнализации не возникает проблем с взаимным влиянием одной системы на другую, то в беспроводных системах взаимные помехи могут стать причиной неработоспособности системы. *SpreadNet* позволяет осуществить автоматический контроль эфира на наличие других радиоканальных систем, создающих взаимные помехи, и соответствующим образом изменить параметры устанавливаемой системы. Также производится автоматический выбор параметров сигнала, обеспечивающих максимальное отношение сигнал/шум в месте конкретной установки.

Перед принятием окончательного решения об установке беспроводной системы охранной сигнализации необходимо проверить ее работоспособность в конкретном месте предполагаемой установки. Это вызвано существенной зависимостью условий прохождения сигнала на различных объектах от их конфигурации, материала, толщины и количества стен, наличия металлической арматуры, металлических предметов и т.п. Существующие системы других типов позволяют сделать это, используя бинарную оценку (да/нет), принят или нет сигнал конкретного передатчика с определенной точки объекта. Одна из чрезвычайно полезных особенностей системы *SpreadNet* – способность измерить реальное отношение сигнал/шум для каждого передатчика объективно, в цифрах, в децибелах. Это позволяет, во-первых, снять точную карту распределения качества приема сигнала из различных частей объекта и, во-вторых, выбрать оптимальное место расположения каждого извещателя с точки зрения максимума отношения сигнал/шум, перемещая его на некоторое расстояние и измеряя при этом соотношение уровней сигнала и шума.

Ресурс источников питания беспроводных систем, определяющих продолжительность функционирования передатчиков до замены источников питания, зависит от многих условий. В системе *SpreadNet* продолжительность использования источников питания достаточно велика благодаря ряду параметров и конструктивных особенностей устройств. Например, используемый диапазон частот 900 МГц позволяет реализовать оптимальные четвертьволновые антенны внутри корпуса извещателей без увеличения размера. Это, а также малая длительность передаваемого сигнала позволяют уменьшить по-

требление энергии и увеличить срок службы источников питания в зависимости от режима работы до 5 лет.

В состав *SpreadNet* входит полный функциональный набор извещателей: универсальный передатчик для подключения проводных устройств (он же магнитоконтактный датчик, пассивный инфракрасный акустический для разбивания стекла, комбинированный), пожарные датчики – тепловой и дымовой, три вида кнопок тревоги, педаль тревоги, датчик банкнот для кассовых аппаратов. Этот набор устройств, а также возможность подключать приемник *SpreadNet* почти к любой контрольной панели с помощью интерфейса обеспечивают достаточную универсальность системы.

Система позволяет организовать эффективную охрану помещений, групп объектов (например, нескольких зданий) и многих других [11].

В настоящее время на рынке систем безопасности предлагается широкий выбор зарубежных и отечественных систем. Технические параметры и рекомендации по их применению регулярно публикуются, например, в журнале «Системы безопасности» и ежегодном тематическом каталоге с тем же названием, выпускаемым компанией «Гротек».

4.2. Система контроля вскрытия аппаратуры

4.2.1. Требования, предъявляемые к системе контроля вскрытия аппаратуры

Система контроля вскрытия аппаратуры (СКВА) [42] предназначена для контроля доступа к внутреннему монтажу аппаратуры, технологическим пультам управления, кабельным соединителям, т.е. к таким элементам вычислительной системы, которые в процессе эксплуатации при нормальном функционировании должны находиться в неизменном состоянии. Иначе это состояние называют механической целостностью системы. Предпочтительным для обеспечения высокой защиты информации, циркулирующей в данной системе, является такой режим, при котором работы ведутся пользователями только со штатных терминалов в соответствии с основным назначением системы, все остальные работы производятся автоматически. Для обеспечения определенных гарантий того, что в данный момент в обработку информации не вмешиваются посторонние процессы, за исключением случайных, и служит контроль механической целостности аппаратуры.

Однако на практике для обеспечения нормального функционирования системы необходимо круглосуточно поддерживать ее аппаратуру и программное обеспечение в работоспособном состоянии. Для этого производятся ремонт и профилактика аппаратуры, тестовый контроль функционирования трактов и отдельных устройств, восстановление технологической информации, перезагрузка программного обеспечения, восстановление работоспо-

способности отказавшего технического средства, замена неисправных устройств исправными и т.д. Перечисленные работы часто проводят параллельно с выполнением основных задач по обработке информации, подлежащей защите. Поэтому важно эти работы держать под контролем. Кроме того, перед отправкой устройства в ремонт или на профилактику должно обеспечиваться логическое отключение его от рабочего контура обмена информацией и уничтожение остатков секретной информации, если таковые в нем оказались. Для решения этой задачи вся аппаратура, входящая в состав КСА, должна иметь на дверцах, крышках и кожухах датчики вскрытия, а на внешних кабельных соединителях – переключки, выполняющие роль датчиков, или другие датчики.

Рассматривая сложный комплекс средств автоматизации обработки информации как объект ее защиты, отметим следующие его характерные особенности:

- наличие большого количества технических средств и кабельных соединений;
- территориальную в пределах контролируемой зоны рассредоточенность и удаленность технических средств;
- размещение части технических средств в отдельных помещениях;
- наличие на некоторых технических средствах нескольких дверц, крышек, соединителей;
- наличие технологических пультов управления, позволяющих вмешиваться в процесс обработки информации;
- наличие средств функционального контроля, регистрации и документирования информации;
- необходимость в процессе эксплуатации загрузок и перезагрузки программных средств;
- ограниченные площади размещения аппаратуры и оборудования;
- круглосуточный режим работы;
- возможность возникновения аварийных ситуаций, влекущих за собой кратковременное отключение электропитания КСА и освещения помещений;
- необходимость проведения на технических средствах профилактических и восстановительных работ.

С учетом стратегии и тактики защиты информации в КСА в этом случае необходимо обеспечить:

- централизованный автоматизированный контроль доступа;
- своевременное обнаружение и блокировку несанкционированного доступа;
- установление причины и принятие мер по устранению несанкционированного доступа;
- регистрацию и учет места и времени доступа.

Централизованный автоматизированный контроль доступа заключается в создании и внедрении в КСА средств контроля, сбора и обработки электрических сигналов с датчиков вскрытия, установленных на технических средствах.

Своевременное обнаружение несанкционированного доступа заключается в выработке на устройстве централизованного контроля сигнала тревожной

сигнализации за время, не позволяющее нарушителю успеть совершить несанкционированный доступ к внутреннему монтажу и технологическим органам управления путем быстрой блокировки датчика вскрытия. Своевременная блокировка несанкционированного доступа заключается в реализации по сигналу тревожной сигнализации возможности вывода данного технического средства из рабочего контура обмена информацией в комплексе средств автоматизации и вывода соответствующего сигнала на средства отображения и управления должностного лица, отвечающего за безопасность информации. Существенную роль при этом играет точность указания места и времени совершения несанкционированного доступа и блокировки.

После выработки тревожной сигнализации и блокировки доступа к информации необходимо установить причину появления сигнала. Причиной его появления может быть и неисправность датчика или цепей контроля, включая устройство контроля вскрытия.

При постановке нашей задачи исходим из того, что возможная попытка вскрытия для каждого технического средства равновероятна, и должна не исключаться попытка несанкционированного доступа к одному ТС под прикрытием ложного сигнала тревожной сигнализации с другого технического средства.

В большинстве КСА средства функционального контроля предусматривают в программном обеспечении этой задачи наличие таблицы состояний технических средств комплекса. Таблица состояний содержит следующую информацию о каждом техническом средстве КСА:

- включено – выключено;
- исправно – неисправно;
- в работе – в профилактике.

Механизм контроля состояний технических средств, как правило, предполагает при наличии сигналов «неисправно», «выключено» и «неопределенного состояния» перевод данного технического средства в состояние «профилактика», что автоматически выводит его из рабочей конфигурации КСА. После выяснения и устранения причины отказа, окончания ремонта или профилактики оператор рабочего места функционального контроля путем изменения таблицы состояний вводит данное техническое средство в рабочую конфигурацию под контролем службы безопасности.

Казалось бы, очевидно, что установленные в технических средствах датчики вскрытия можно использовать для формирования дополнительных сигналов «вскрыто» и «закрыто», которые можно включить в вышеуказанную таблицу и передавать ее по информационному тракту КСА на рабочее место службы безопасности. Однако не следует торопиться с таким решением по причине, в основе которой лежит тезис: «Безопасность информации важнее функционирования системы», что означает: при отказе функционирования КСА, включая отключение электропитания и освещения, информация должна быть защищена от утечки, модификации и утраты. Отказы вычислительных средств и электропитания КСА отразятся также и на функционировании системы контроля вскрытия, что не отвечает требованиям более высокой надежности средств контроля по отношению к надежности объекта контроля и простоте защиты.

Таким образом, анализируя особенности рассматриваемого КСА как объекта защиты информации, применяя указанные стратегию и тактику за-

щиты, а также учитывая технические возможности ее реализации, можно сформулировать следующие основные требования, предъявляемые к системе контроля вскрытия аппаратуры:

- централизованный автономный независимый контроль датчиков вскрытия удаленных технических средств и кабельных соединений;
- выработка и запоминание сигнала несанкционированного вскрытия в интервал времени, не позволяющий нарушителю заблокировать датчик вскрытия (условие прочности защиты $t_n > T_{обл}$ см. подразд. 3.4);
- обеспечение возможности определения места возникновения сигнала с точностью до каждого технического средства (для уменьшения $T_{обл}$);
- обеспечение возможности индивидуального отключения (включения) механизма тревожной сигнализации по каждому техническому средству;
- обеспечение возможности проведения индивидуального контроля вскрытия (закрытия) технического средства, выведенного в ремонт или на профилактику;
- обнаружение и запоминание нескольких одновременно возникающих сигналов несанкционированного вскрытия;
- обеспечение возможности круглосуточной непрерывной работы при кратковременных отключениях электропитания КСА и освещения;
- обеспечение возможности работы системы в присутствии человека – законных пользователей и технического персонала КСА;
- обеспечение минимальной вероятности возможности скрытного отключения нарушителем цепей контроля;
- обеспечение надежности функционирования системы контроля вскрытия, превышающей надежность объекта контроля – вычислительной системы.

4.2.2. Принципы построения СКВА

Анализ материалов зарубежных и отечественных источников информации показывает, что решению проблемы контроля вскрытия аппаратуры уделяется недостаточно внимания. В этих материалах в основном рассматриваются устройства охранной и пожарной сигнализации, в которых применяются датчики обнаружения присутствия человека или пожара. В отличие от указанных систем, в СКВА задача несколько иная. Здесь в основном допускается присутствие рядом с аппаратурой человека, выполняющего свои обязанности с другими задачами. Кроме того, необходимость контроля за стыковкой кабельных соединителей и применение для этой цели перемычек предопределяет выбор датчика, который должен быть однотипным, т.е. контактным, так как это упрощает задачу построения централизованного устройства контроля.

Системы контроля вскрытия аппаратуры включают датчики вскрытия аппаратуры, цепи сбора сигналов и специальное рабочее место (устройство) централизованного контроля [53]. Контактные датчики обладают в данных условиях определенными достоинствами:

- простотой схемы и совместимостью с цифровыми схемами;
- возможностью объединения датчиков в группу параллельно или последовательно;

- отсутствием гальванической связи со схемой контролируемого технического средства;
- малым электрическим активным сопротивлением в замкнутом состоянии и большим – в разомкнутом;
- отсутствием емкости и индуктивности;
- возможностью контроля одним и тем же устройством сигналов с датчиков и кабельных соединителей технических средств;
- отсутствием влияния присутствия человека вблизи контролируемого технического средства;
- низкой стоимостью.

Облегченный режим работы контактного датчика, не требующий большого количества срабатываний, увеличивает срок его службы.

При создании систем контроля вскрытия аппаратуры применяются различные принципы построения сетей сбора сигналов с контактных датчиков вскрытия. Известны следующие варианты построения сети сбора сигналов НСД: радиальные, с резисторной, радиально-резисторной сборкой сигналов и матричные [42] электрические схемы таких сетей приведены на рис. 4.2–4.5.

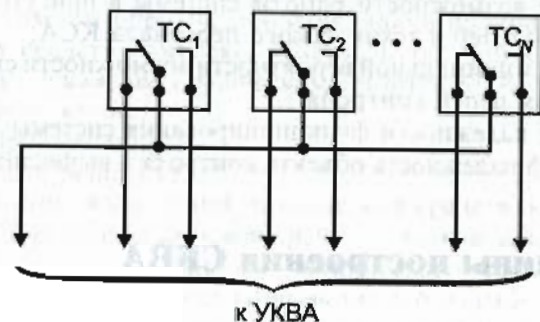


Рис. 4.2. Схема радиальной сети сбора сигналов

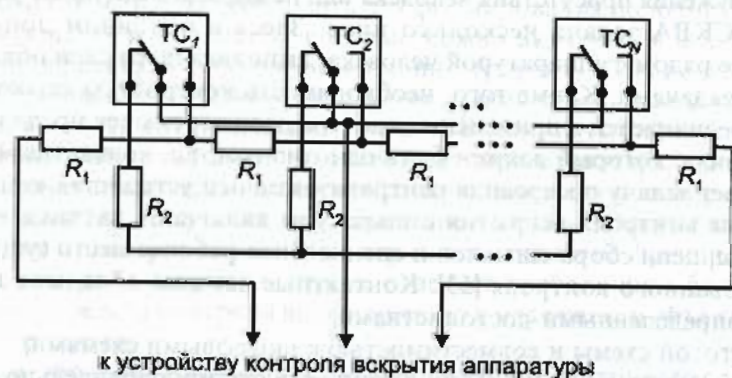


Рис. 4.3. Схема сети с резисторной сборкой сигналов

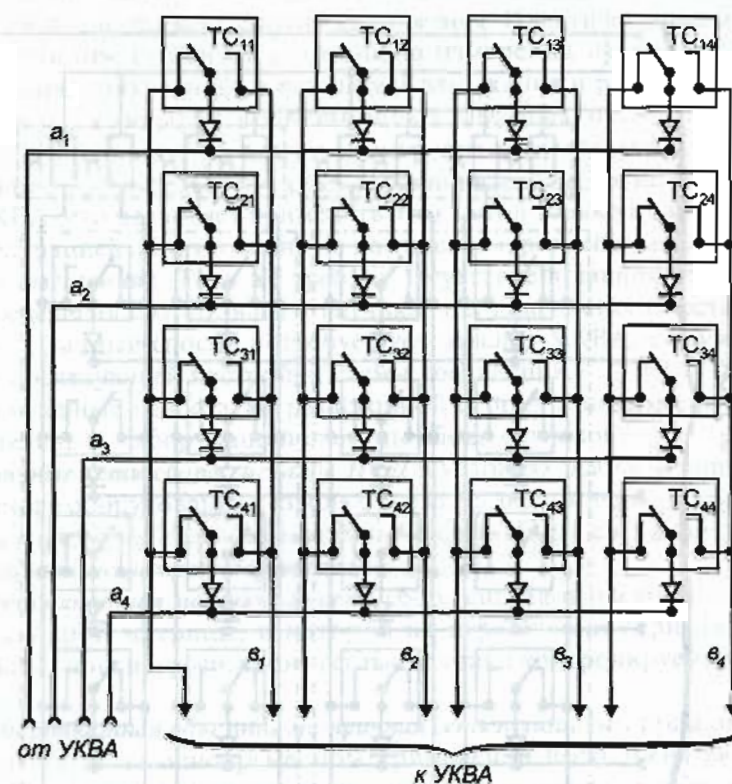


Рис. 4.4. Схема двухкоординатной матричной сети сбора сигналов

В наиболее известной и распространенной сети сбора сигналов НСД (радиальной) один из контактов (переключающийся) каждой из имеющихся в контролируемом техническом средстве контактных групп заземляется, при этом через «сухие» контакты на выход выдаются прямой и (или) инверсный сигналы (например, «земля» и «обрыв») по разным проводам на устройство контроля вскрытия аппаратуры (УКВА). Прием в устройство контроля парафазных сигналов НСД позволяет получить информацию не только о факте и месте возникновения сигнала, но и нарушения монтажа в сети (обрывов и закорачиваний проводов на «землю»). В вычислительной системе, насчитывающей сотни устройств вычислительного и периферийного оборудования, «радиальная» организация сети с увеличением количества контролируемых технических средств приводит к усложнению и удлинению монтируемых цепей. В этом случае необходимо применить промежуточное звено – локальные устройства сбора сигналов (ЛУСС), представляющие собой обычные мультимплексоры, размещаемые вблизи группы контролируемых технических средств. Сигналы с нескольких ЛУССов будут поступать на УКВА. При этом количество проводов, поступающих на него, уменьшится.

Монтажное объединение сигналов НСД и выдача только суммарного сигнала от нескольких устройств вычислительной системы снижает степень детализации места НСД и ухудшает оперативные характеристики системы защиты

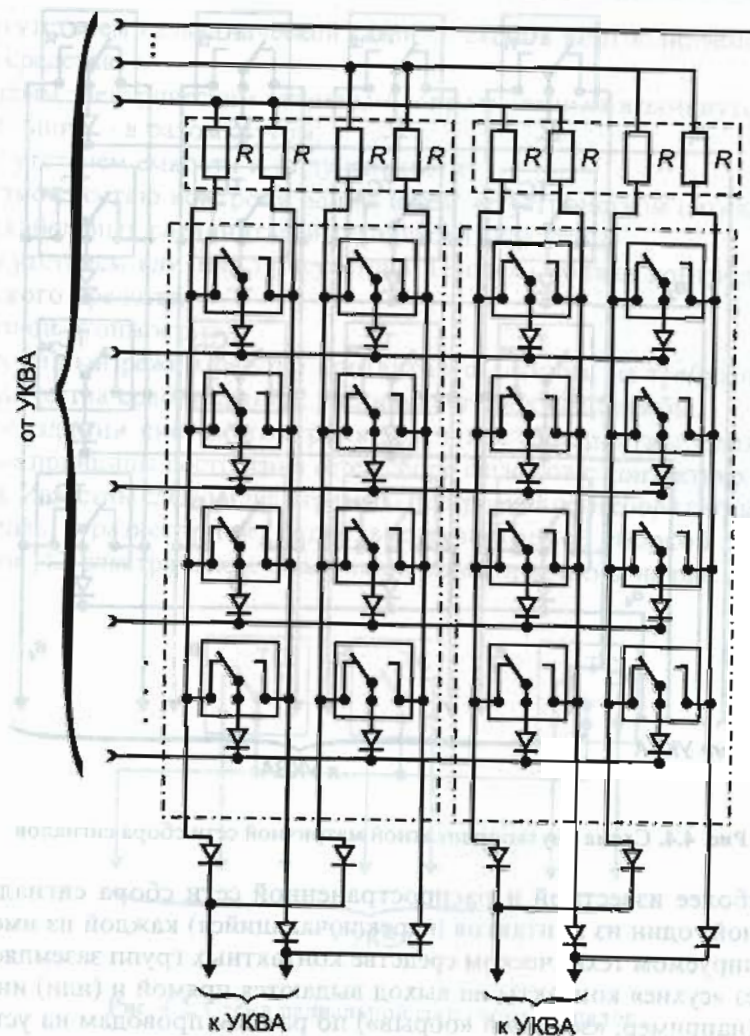


Рис. 4.5. Схема трехкоординатной матричной сети сбора сигналов

[1]. Однако такое соединение в определенных условиях имеет смысл, например, на одном техническом средстве обработки информации, имеющем несколько дверц или съемных крышек. Но даже на одном и тем более на разных технических средствах монтажное объединение недопустимо, если в одном техническом средстве размещены резервные блоки или модули, а разные технические средства дублируют друг друга в целях повышения надежности функционирования КСА. Такие условия необходимы для одновременного выполнения требований к безопасности информации и непрерывности работы КСА в случае проведения ремонта или профилактики технического средства.

Сеть с резисторной сборкой сокращает количество контрольных цепей, поступающих на УКВА, за счет применения в виде отдельного устройства, установленного между группой датчиков и УКВА, резисторной «сборки»,

образующей специальный делитель напряжения. Идентификация места НСД в этом случае производится с помощью измерения итогового значения сопротивления, полученного в результате замыкания и размыкания контактов датчиков. Учитывая погрешность известных методов измерения сопротивлений, количество датчиков в группе рекомендуется не более 10–20. Указанное обстоятельство также ограничивает расстояние между датчиками и УКВА, что позволяет применять этот метод только в системах с высокой концентрацией оборудования по комплексам, размещаемым в одном или смежных помещениях. Того же требует отсутствие в данной схеме возможности определения сработавшего датчика, т.е. диагностики места события. Кроме того, данный способ потребует усложнения УКВА, а также точного расчета и последующей настройки схемы соединений.

Перечисленные недостатки резисторной сборки в нашем случае делают затруднительным выбор данной системы сбора сигналов.

Матричные сети сбора сигналов НСД в условиях высокой концентрации размещаемого оборудования позволяют создать экономичные и относительно простые структуры. Условно матричные сети сбора сигналов делятся на *двухкоординатные* и *трехкоординатные*.

Двухкоординатная матричная сеть сбора сигналов построена на использовании диодной матрицы, в которой на пересечении горизонтальных и вертикальных шин встроены контактные датчики контролируемых технических средств.

Трехкоординатная объемная матричная сеть использует принцип построения, основанный на одновременном применении нескольких двухкоординатных («плоскостных») диодных матриц, объединенных в общую схему. В трехкоординатной матричной сети на первую группу горизонтальных шин (к резисторам) подается последовательность выборки в виде сигналов высокого уровня (на невыбираемых шинах – сигналы низкого уровня), а на вторую группу горизонтальных шин (к диодам) – последовательность выборки в виде сигналов низкого уровня (на невыбираемых шинах присутствуют сигналы высокого уровня), на вертикальных парах шин сигналы в зависимости от состояния датчиков дешифруются так же, как в двухкоординатной матричной сети.

Сравнительный анализ вариантов сетей сбора с целью оптимизации структуры сети сбора сигналов НСД по наименьшим количеству и длине соединительных кабелей показывает, что более экономичные матричные структуры рекомендуются при значительной концентрации контролируемых технических средств вокруг места положения рабочего места контроля НСД. Кроме того, отмечается неудобство монтажа кабельных соединений из-за неприспособленности штепсельных разъемов к использованию в матричной сети.

Концентрация контролируемых технических средств в матричном варианте сети необходима для уменьшения длины проводов, соединяющих датчики с матрицей. В противном случае матричная сеть вырождается в «радиальную», так как сама матрица, которую придется реализовывать в виде отдельного конструктива, становится местом сбора сигналов по радиальной схеме. Очевидно, что применение матричной сети целесообразно только при

длине проводов от матрицы до УКВА, значительно превышающей длину проводов от датчиков до матрицы. При этом необходимо также учесть затраты на разработку конструктива матрицы.

Однако на практике при создании вычислительных систем часто возникает необходимость в рассредоточенном размещении групп технических средств одного КСА на различных расстояниях друг от друга до 1–2 км. При создании вычислительных сетей и больших АСУ, состоящих из нескольких принципиально одинаковых по составу и назначению КСА, приходится использовать уже имеющиеся площади, которые различны по планировке, составу и размерам, а также расстояниям между отдельными ее частями. В данных условиях применение вариантов сетей с резисторной и матричной сборкой нецелесообразно. Применение в одном КСА совмещенного варианта (радиального и матричного) значительно усложняет схему комплекса и УКВА, в котором придется совместить два различных принципа сбора и обработки информации.

Анализ существующей в настоящее время тенденции построения КСА на базе локальных вычислительных сетей, использующих в основном принципы последовательного соединения технических средств, указывает на возможность применения тех же принципов в системе контроля вскрытия аппаратуры (рис. 4.6).

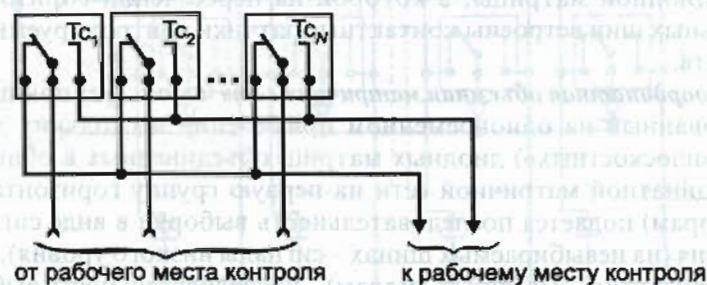


Рис. 4.6. Схема сети с последовательным сбором сигналов

В сети с последовательным сбором сигналов на подвижный контакт датчика с УКВА подается сигнал последовательной выборки, а неподвижные контакты, соединенные параллельно, объединены по нормально-замкнутым и нормально-разомкнутым контактам в две шины, которые подключаются ко входам рабочего места контроля сигналов НСД. Данная схема соединений по сравнению со схемой радиального сбора сигналов позволяет почти в два раза сократить количество связей контролируемых технических средств с УКВА.

Если в радиальной сети при количестве контролируемых технических средств, равном n , количество проводов до УКВА $K_p = 2n + 1$, то для «последовательной» $K_n = n + 2$. Вариант сети с «последовательным» сбором сигналов согласуется с принципами построения КСА на базе локальных вычислительных сетей, что позволяет производить прокладку цепей с датчиков технических средств по тем же трассам. Данный вариант позволяет применить его в вычислительных системах с рассредоточенными техническими средствами на различных расстояниях от УКВА и друг от друга.

Вариант сети с последовательным сбором сигналов вскрытия технических средств обладает следующими достоинствами:

а) по сравнению с радиальным вариантом сети:

- меньшим количеством связей ТС с УКВА;
- возможностью снижения затрат при прокладке кабелей;

б) по сравнению с вариантом сети с резисторной сборкой:

- возможностью контроля рассредоточенных технических средств на различных расстояниях;

- простотой схемы;
- возможностью высокой степени детализации сигнала НСД;
- возможностью контроля большого количества ТС;
- возможностью определения количества одновременных НСД;

в) по сравнению с матричными вариантами сети:

- возможностью контроля рассредоточенных ТС на различных расстояниях;

- простотой схемы.

Применение в схеме сбора парафазных сигналов с каждого контролируемого технического средства позволяет организовать на УКВА непрерывный контроль целостности цепей сбора, т.е. защиту от случайных воздействий. Но от преднамеренных обрывов и замыканий, совершенных одновременно по отношению к одному контролируемому датчику, это слабая защита, так как единственным препятствием для нарушителя в этом случае могут быть только поиск и определение нужных проводов в кабеле. Далее одновременное замыкание параллельно нормально-замкнутому контакту и обрыв в цепи нормально-разомкнутого контакта датчиков скрытно выводят из-под контроля техническое средство. Поэтому несанкционированные поиск проводов и изменение всех упомянутых вариантов сбора усложняют. Данное требование касается всех упомянутых вариантов сбора сигналов, кроме варианта с резисторной сборкой, в котором трудности с точной настройкой сети дают в смысле защиты положительные результаты, так как значительно усложняют задачу нарушителя. Но с увеличением количества датчиков сложность настройки становится неприемлемой.

Возможны и другие варианты схем с защитой сигнальных цепей. Например, вариант *радиально-резисторный*, приведенный в подразд. 4.1.3 на рис. 4.1.

В качестве устройства контроля вскрытия аппаратуры рекомендуется использовать устройства, приведенные в [42, 53]. По сравнению со своими аналогами данные устройства обладают следующими преимуществами:

- возможностью централизованного контроля большого числа удаленных объектов с помощью малогабаритного устройства, размещаемого на столе;

- возможностью быстрого и точного определения места вскрытия;
- возможностью применения малогабаритных автономных источников постоянного тока, обеспечивающих непрерывное функционирование системы охраны при долговременном отключении сети электропитания и освещения на объекте применения;
- непрерывностью контроля остальных датчиков при возникновении сигнала НСД на одном, двух, трех и т.д.;

- высокой надежностью в работе за счет применения простой схемы и полупроводниковых приборов.

Достоинством этих устройств является также возможность работы и с бесконтактными датчиками, на выходе которых вырабатываются сигналы высокого и низкого уровней. Если после аналогового датчика установить пороговый преобразователь, то все датчики охранной сигнализации могут быть задействованы на эти устройства, что позволит построить единую систему охранной и пожарной сигнализации на любом объекте.

Серийный выпуск подобных устройств позволит получить еще одно преимущество – низкую стоимость. Применение для этих целей персональных компьютеров в любом случае потребует разработки устройства сбора сигналов. Кроме того, по сравнению с компьютером применение таких схем позволяет получить систему контроля с малым токопотреблением, которое позволяет применить автономный источник питания и выполнить важное требование к независимости работы СКВА. Это качество необходимо на случай прекращения работы АС по причинам перезагрузки АС и аварийных ситуаций. Перечисленные достоинства рассмотренных устройств делают их довольно перспективными.

Предъявляемые требования и подробный анализ ожидаемой эффективности системы контроля вскрытия аппаратуры технических средств автоматизированной системы с позиций прочности создаваемой защиты приведен в подразд. 3.4.4.

4.3. Программы контроля и разграничения доступа к информации

4.3.1. Задачи и общие принципы построения программ контроля и разграничения доступа к информации

Основная задача программы контроля и разграничения доступа (ПКРД) – это блокировка несанкционированного, контроль и разграничение санкционированного доступа к информации, подлежащей защите. При этом разграничение доступа к информации и программным средствам ее обработки должно осуществляться в соответствии с функциональными обязанностями и полномочиями должностных лиц-пользователей, обслуживающего персонала и руководителей работ.

Основной принцип построения ПКРД состоит в том, что допускаются и выполняются только такие обращения к информации, в которых содержатся соответствующие признаки разрешенных полномочий. В указанных целях осуществляются идентификация и аутентификация пользователей, устройств и т.д., деление информации и функций ее обработки согласно установленным требованиям разграничения доступа, установка и ввод полномочий пользователей.

Деление информации и функций ее обработки обычно производится по следующим признакам:

- по степени важности;
- по степени секретности;
- по выполняемым функциям пользователей, устройств;
- по наименованию документов;
- по видам документов;
- по видам данных;
- по наименованию томов, файлов, массивов, записей;
- по имени пользователя;
- по функциям обработки информации: чтению, записи, исполнению;
- по времени дня.

Выбор конкретных признаков деления и их сочетаний производится в соответствии с техническим заданием при проектировании программного обеспечения автоматизированной системы.

Информация, подлежащая защите, должна быть размещена в непересекающихся областях памяти. В любой из этих областей хранится совокупность информационных объектов, каждый из которых подлежит защите. Защита в этом случае сводится к тому, что доступ к информационному объекту осуществляется через единственный охраняемый вход. В функцию «охраны» входят опознание пользователя по имени (или условному номеру) и коду предъявленного пароля. При положительном результате проверки разрешается допуск его к информации в соответствии с выделенными пользователю полномочиями. Эти процедуры выполняются при каждом обращении пользователя: запросе, выдаче команд и т.д. Чтобы не набирать каждый раз пароль, удобно предъявляемый пароль хранить на специальном физическом носителе (ключе, карте), который перед входом в вычислительную систему должен вставляться пользователем в специальное гнездо АРМ. Кроме того, после изъятия носителя с паролем из гнезда вход в систему сразу блокируется.

Если же требования к защите информации для конкретной системы позволяют применение набора пароля вручную, необходимо сделать так, чтобы предъявляемый пароль при повторных обращениях в процессе работы с информацией находился в памяти данного АРМ. Хранение в центральном вычислителе допускается только при обеспечении его связки с условным номером данного АРМ, т.е. все последующие обращения в центральный вычислитель должны приниматься на обработку только с условным номером АРМ, с которого предъявлялся хранимый код пароля. По окончании работы для исключения возможности несанкционированного доступа со стороны посторонних пользователей необходимо с АРМ ввести соответствующую команду, по которой предъявленный ранее и хранимый пароль стирается. О факте стирания на АРМ пользователя должно быть выдано сообщение. Для проверки последней операции полезно повторить одно из предыдущих обращений без пароля и убедиться в этом по отрицательной реакции вычислительной системы.

Пример типового алгоритма контроля и управления разграничением доступа приведен на рис. 4.7.

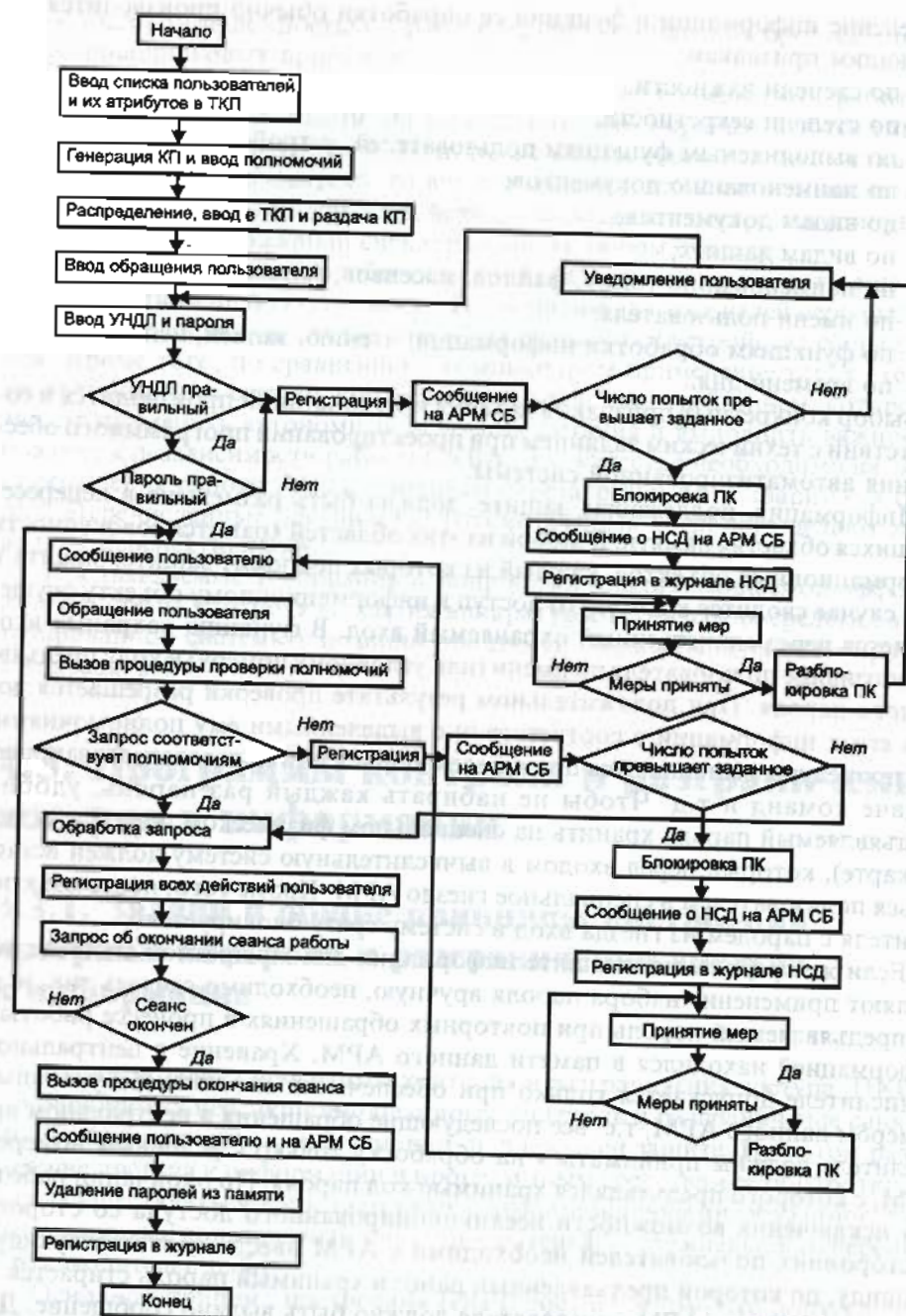


Рис. 4.7. Типовой алгоритм контроля и управления разграничением доступа к информации:

УНДЛ – условный номер должностного лица; КП – ключ-пароль;
ТКП – таблица КП; АРМ СБ – АРМ службы безопасности

4.3.2. Выбор значений паролей (кодов паролей)

Чем больше длина пароля, тем большую безопасность будет обеспечивать система, так как потребуются большие усилия для его отгадывания. Вероятность наступления этого события определяется формулой (3.9). Учитывая увеличение вероятности с увеличением количества попыток подбора, необходимо количество попыток ограничить до трех, после чего должен выработываться сигнал тревожной сигнализации и блокировки обращения с указанием времени и места события.

Если количество попыток не ограничивать, то ожидаемое время раскрытия пароля или ожидаемое безопасное время (T_c) будет равно полупроизведению числа возможных паролей и времени, требуемого нарушителю, чтобы попробовать каждый пароль из последовательности запросов. Оно представлено формулой (3.10), приведенной в подразд. 3.2.4. В этом случае придется пожертвовать быстродействием, чтобы ввести временную задержку выдачи результата контроля совпадения введенного и хранимого паролей для того, чтобы увеличить ожидаемое время раскрытия пароля. Если после каждой неудачной попытки подбора предусматривается задержка 0,01с, безопасное время увеличивается на $(0,01 \cdot A^s)$ с, где A – число символов в алфавите, s – длина пароля. Например, при $A = 10$ и $s = 10$ безопасное время увеличится более чем на 3 года.

Из формул следует, что стойкость пароля в основном определяется его длиной в количестве символов и количеством символов в применяемом алфавите. В настоящее время широко применяются многосимвольные пароли, где $s > 8$. В связи с увеличением длины пароля возникают вопросы его запоминания, хранения и связи его с личностью пользователя. На эти вопросы ответы помещены выше в подразд. 2.7.

При расчете длины кода пароля не следует забывать о том, что при увеличении длины пароля нельзя увеличивать периодичность его смены на новые значения более 1 года. Коды паролей необходимо менять обязательно, так как за большой период времени увеличивается вероятность их перехвата путем прямого хищения носителя, снятия его копии, принуждения человека. Выбор периодичности необходимо определять из конкретных условий работы системы, но не реже одного раза в год. Выбор численного значения пароля, дата замены и ее периодичность должны носить случайный характер.

Некоторые изменения в схеме применения простого пароля создают большую степень безопасности. Например, в схеме однократного использования пароля пользователю выдается список из N паролей. Такие же пароли хранятся в ЭВМ (конечно, в зашифрованном виде). После использования 1-го по списку пароля в следующий раз должен быть применен 2-й пароль, так как 1-й пароль в памяти ЭВМ стирается, и т.д. Этот способ весьма эффективен, но не всегда удобен. Он используется при относительно редких обращениях или при передаче специальной информации.

Пароли однократного использования могут применяться также для проверки подлинности сообщения об окончании обслуживания пользователя или завершении его работы на ЭВМ. В этом случае уменьшается вероятность использования системы опытным нарушителем, который может послать пользователю ложное сообщение об отключении ЭВМ и продолжать с ней работу от его имени.

Схема применения паролей однократного использования имеет следующие недостатки [78]:

- пользователь должен помнить или иметь при себе весь список паролей и следить за текущим паролем;
- в случае, если встречается ошибка в процессе передачи, пользователь оказывается в затруднительном положении: он не знает, следует ли ему передать тот же самый пароль или послать следующий;
- если пароли однократного использования передаются с терминалов, а сами пароли были получены из линейной последовательности псевдослучайных чисел $X_1, X_2, \dots, X_k$, они могут быть перехвачены определенными ловушками.

Если существует реальная опасность перехвата значений паролей в линиях связи, например, при работе с удаленного терминала, необходим более надежный и более дорогой способ защиты паролей – применение одноразовых сеансовых паролей по специальному алгоритму аутентификации. Алгоритм предполагает по запросу пользователя передачу ему со стороны ЭВМ случайного числа, который на его терминале преобразуется с помощью необратимой функции с применением пароля пользователя. Результат преобразования во время сеанса связи посылается на ЭВМ, которая сравнивает полученный результат с собственным результатом такого же преобразования (алгоритм и пароль введены ранее). При их совпадении она принимает запрос в обработку. Новый запрос ЭВМ обслуживает по этому же алгоритму, но с другим случайным числом. Это число называется *сеансовым паролем*.

Однако в этом случае (кроме защиты паролей) возникает вопрос защиты передаваемой информации. Она закрывается с помощью шифрования. Алгоритм передачи и аутентификации усложняется и приближается к задачам, решаемым в системах с распределенной обработкой данных, которые рассмотрены ниже.

4.3.3. Разграничение полномочий пользователей

В автоматизированных системах нашли применение два метода организации разграничения доступа [27]: дискреционный и мандатный.

Дискреционный метод предполагает использование матриц доступа. Матрица доступа представляет собой таблицу, в которой объекту доступа соответствует столбец Q_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. 4.8).

	Q_1	Q_2	...	Q	...	Q_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. 4.8. Матрица доступа

При определении полномочий доступа администратор безопасности по указанию руководителя работ на АС устанавливает операции, которые разрешено выполнять пользователю (субъекту доступа). Разработчиком для этой цели в АС предусматривается соответствующий механизм.

Применяют следующие операции с файлами:

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

В тип доступа «чтение» могут входить следующие запросы:

- чтение с логического диска;
- поиск файла (каталога);
- открытие файла на чтение;
- чтение атрибута файла;

В тип доступа «запись» – включаются:

- запись на логический диск;
- создание файла (каталога);
- удаление файла (каталога);
- переименование файла (каталога);
- открытие файла на запись;
- установка атрибута файла.

Доступ Запись в файл может иметь две модификации: указанную выше (W) и другую организацию доступа – разрешение только дописывания в файл, без изменения старого содержимого (A).

Матричный метод разграничения доступа позволяет с максимальной детализацией установить права субъекта доступа по выполнению разрешенных операций над объектами доступа. Такой подход нагляден и легко реализуем. Однако при большом количестве субъектов и объектов доступа реализация этого метода усложняется. Чтобы не допустить этого, необходимо объединять объекты доступа, пользователей в группы и сокращать количество субъектов доступа за счет так называемых «процессов – субъектов доступа» до полного исключения их из таблицы (не из обработки). Тем более это необходимо, если существует техническая возможность установления имени первоначального инициатора процесса обработки информации – пользователя. Если необходимо разграничение доступа процессов к процессам и объектам доступа, целесообразно создать отдельную матрицу. Однако при этом следует руководствоваться правилом: не создавать механизмов, функционирование которых нельзя или сложно проверить. Кроме того, на практике не требуется тотальное разграничение доступа, которое усложняет защиту и не отвечает требованиям ее простоты.

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 доступ. 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 равен уровню конфиденциальности документа или выше его, а в наборе категорий, присвоенных данному субъекту доступа, содержатся все категории, определенные для данного документа.

В АС 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 [27].

Мандатный метод в таком виде, по мнению автора книги, существенно усложняет разграничение доступа, а эффективность защиты информации практически не повышает и при управлении приходится завышать конфиденциальность информации из-за невозможности детального разграничения доступа.

Приведенная выше матрица является таблицей рабочих полномочий пользователей. Эту таблицу заполняет не он, а потому ответственности за несоответствие его мандата вызванной им информации не несет. По этой же причине вызывает сомнение необходимость автоматизации процесса присвоения уровня конфиденциальности документу, который создает пользователь. Решение об уровне конфиденциальности должен принимать только он и его руководитель работ. Совсем недопустимо считать процесс субъектом доступа и присвоение им уровня конфиденциальности документу. Контроль уровня секретности имеет смысл только при записи его на машинный носитель, печати документа и передаче другому пользователю, в архив и в каналы связи на другую АС.

4.3.4. Концепция построения систем контроля и разграничения доступа

В основе построения систем контроля и разграничения доступа (СКРД) ЭВМ лежит концепция разработки защищенной универсальной ОС на базе ядра безопасности [13]. Под ядром безопасности понимают локализованную, минимизированную, четко ограниченную и надежно изолированную совокупность программно-аппаратных механизмов, доказательно правильно реализующих функции диспетчера доступа, через который должны проходить все обращения к программному обеспечению и информации АС [55]. 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 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.

4.3.5. Средства перекрытия путей обхода программ контроля и разграничения доступа

На эффективность работы ПКРД влияют:

- неконтролируемый вход в ОС ЭВМ;
- неконтролируемый доступ к таблицам действительных значений паролей и полномочий;
- метод защиты кодов паролей, хранимых в вычислительной системе;
- выбор параметров паролей;

- метод запоминания и хранения кодов паролей для пользователя вне вычислительной системы;
- организация контроля и управления доступом к информации и средствам ее обработки в вычислительной системе.

Неконтролируемый вход в ОС ЭВМ нарушитель может использовать для доступа к информации, таблицам паролей, полномочий и другой цели. Предупредить подобные действия должны меры, изложенные в 4.3.3, а также средства контроля целостности ПО и антивирусные средства защиты, которые рассмотрены ниже.

Действительные значения кодов паролей в вычислительной системе рекомендуется хранить в преобразованном криптографическом методе виде. Подобный метод обеспечивает высокий уровень защиты кодов паролей и, следовательно, малую вероятность обхода защиты.

Для закрытия кодов паролей можно использовать методы шифрования, необратимого преобразования с помощью хэш-функции, например по ГОСТ Р 34.11-94 или более сложный метод «необратимой беспорядочной сборки» [78], когда пароли с помощью специального полинома преобразуются в зашифрованный пароль. В этом случае не существует никакой схемы для возвращения к оригиналу пароля. При вводе пароля система преобразует его по данному закону во время процесса регистрации и сверяет результат с преобразованным ранее паролем, хранящимся в системе.

Возможен и другой способ защиты паролей, использующих метод гаммирования (наложения) при наличии в ЭВМ (КСА) по меньшей мере двух (не считая резервных) конструктивно разделенных областей памяти.

Если обозначить через $X_1, X_2, \dots, X_n$ коды паролей, подлежащие защите, а через $K_1, K_2, \dots, K_n$ – соответствующие коды их закрытия, то, используя метод гаммирования, можно получить закрытые значения кодов паролей $Y_1, Y_2, \dots, Y_n$ путем сложения чисел X и K по mod 2

$$X_1 + K_1 = Y_1$$

$$X_2 + K_2 = Y_2$$

$$\dots$$

$$\dots$$

$$X_n + K_n = Y_n$$

Значения K и Y хранятся в ЭВМ в разных областях памяти, а значения X не хранятся. При поступлении в ЭВМ кода пароля от пользователя производится сложение по mod 2 его значений с соответствующим кодом закрытия « K ». Результат сложения проверяется на совпадение с хранимым значением Y . Идея защиты заключается в раздельном хранении значений « K » и « Y » (так как $K + Y = X$), доступ к которым должен быть открыт только программе аутентификации пользователей и программе ввода их значений. Последняя должна работать только на оператора службы безопасности, у которого должен быть свой пароль из числа тех же паролей, но со своим идентификатором. Значение его идентификатора можно также сделать переменным. При вводе новых паролей оператор службы безопасности выбирает случайные значения паролей и кодов их закрытия. Достоинство

этого метода – более простая возможность вызова на терминал службы безопасности и контроля с его помощью состояния таблицы паролей.

Для повышения степени защиты кодов паролей в ЭВМ можно применить на программном уровне метод генератора псевдослучайных чисел, позволяющий из одного числа получить группу чисел, которые можно использовать в качестве кодов закрытия (метод см. в подразд. 2.8).

При этом первое число, называемое главным паролем, может на время работы храниться в памяти терминала службы безопасности, а выбранные из него коды закрытия – в памяти вычислительного комплекса КСА. В случае ремонта ЗУ значения паролей и кодов закрытия заменяются новыми. Данная мера необходима для исключения несанкционированного доступа к паролям на случай содержания значений « K » и « Y » в остатках информации ЗУ. Поэтому его съем должен производиться под контролем службы безопасности информации.

В целях защиты от компрометации действительные значения паролей (кроме терминалов службы безопасности, размещаемых в отдельных помещениях) не отображаются и не распечатываются. В системах, где технические характеристики терминалов не позволяют это сделать, пароль печатается на маску, закрывающую его значение.

Важную роль при применении носителей кодов паролей (НКП) на практике играет вопрос синхронизации записи паролей на носители и ввод их значений в вычислительную машину. При значительном количестве пользователей возникает необходимость в увеличении объемов этих работ. Однако не следует торопиться автоматизировать этот процесс путем совмещения ввода паролей в вычислитель и записи их значений на НКП, так как это потребует разработки специальной аппаратуры, что может усложнить техническую задачу, и увеличит расходы.

При сохранении раздельной записи большой объем работ действительно будет, но только при первоначальной загрузке вычислительной системы. Необходимая в процессе эксплуатации системы замена паролей может производиться в течение долгого времени по группам паролей без ущерба уровню безопасности. Для этого в таблице кодов паролей на переходный период (например, в течение суток) могут храниться одновременно старое и новое значения пароля. После выдачи пользователю НКП с новым значением пароля старое значение стирается. При этом надо еще принять во внимание психологический аспект в работе службы безопасности, выполняющей эту работу. Напомним, что ее функции в основном контрольные и сводятся к наблюдению, т.е. пассивной роли, которая на практике притупляет бдительность и внимание. Живая и активная деятельность повышает эффективность работы.

4.3.6. Выбор носителей кодов паролей

При выборе и создании НКП для проектируемой системы необходимо учитывать следующие требования:

- характер и стоимость защищаемой информации;
- количество пользователей;

- стойкость к компрометации паролей и необходимость в защите пароля от пользователя;
- возможность многократной записи информации;
- объем записываемой в носитель информации;
- стойкость к подделке и фальсификации носителя с паролем;
- устойчивость к внешним воздействиям, механическим, климатическим, магнитным полям, свету и др.;
- время хранения записанной информации;
- скорость считывания информации;
- периодичность повторной записи информации в носитель;
- условия и способ хранения носителя у пользователя;
- взаимозаменяемость конструкции носителя;
- габариты и вес носителя;
- конструкцию и принцип работы ответной части устройства считывания пароля с носителя;
- согласование содержания и объема информации на носителе с идеологией применения кодов паролей в системе опознавания и разграничения доступа;
- надежность хранения информации и функционирования;
- срок службы;
- стоимость работ, связанных с изготовлением и эксплуатацией носителей.

Влияние перечисленных требований на выбор конструкции носителя кодов паролей и системы их применения выражается следующим образом.

При большом количестве пользователей увеличивается вероятность потери, хищения, фальсификации носителя и компрометации кода пароля. Характер и высокая стоимость защищаемой информации могут быть привлекательными для квалифицированного нарушителя. Защита кода пароля от пользователя вряд ли целесообразна при невысоких стоимости и важности информации, так как пароль является его идентификатором, и носитель выполняет вспомогательную роль в запоминании пароля. В этом смысле содержание записанной в нем информации от владельца скрывать не стоит. Однако слишком очевидная и легко читаемая информация может быть доступна и для посторонних лиц. В ответственных системах может потребоваться защита кода пароля от компрометации. Большой стойкостью к компрометации обладают носители, требующие специальной аппаратуры для считывания информации.

Возможность многократной записи в НКП позволяет использовать одни и те же носители при замене кодов паролей, выполняемой в интересах сохранения уровня эффективности защиты информации в системе, что может потребовать наличия у владельца КСА соответствующей аппаратуры записи. Использование носителей с готовой записью кодов, произведенной на заводе-изготовителе, требует соблюдения некоторых условий:

- записи кодов паролей в виде случайных чисел;
- изготовления НКП с разными значениями паролей в количестве, превышающем количество пользователей, и с учетом периодичности замены и выполнения требуемой стойкости к подбору паролей;
- соблюдение при записи и поставке НКП режима секретности.

Однако, принимая во внимание один из принципов построения защиты – (исходить из наихудших условий), следует считать: что записанные на заводе значения паролей независимо от грифа секретности будут храниться постоянно и, следовательно, могут быть известны нарушителю. Случайный характер значений паролей в данном случае теряет свой смысл, а стойкость к подбору пароля с первой попытки будет равна $P = 1/N$, где N – количество записанных паролей. По этой причине запись паролей на заводе менее предпочтительна.

Объем записываемой в носитель информации определяется исходя из длины записываемого пароля и технических возможностей носителя по выбранной технологии записи информации. Ранее уже отмечалось, что чем длиннее пароль, тем выше его стойкость к подбору. Стойкость к компрометации пароля и фальсификации носителя нужна только для особых систем, связанных с большим риском потери или искажения ценной информации, и должна быть такой, чтобы стоимость работ нарушителя по вскрытию пароля или фальсификации НКП превышала его материальную выгоду от НСД.

Другим критерием оценки стойкости к компрометации пароля и фальсификации носителя может быть сравнение ожидаемого времени, затрачиваемого потенциальным нарушителем на НСД, и времени действия данного пароля в вычислительной системе, т.е. периода его замены. Если первое превышает второе, стойкость обеспечена.

Время надежного хранения паролей в НКП должно быть не меньше периода замены паролей в вычислительной системе на новые, а скорость считывания информации с него должна удовлетворять требованиям быстродействия вычислительной системы, в которой применяется данный НКП. Периодичность повторной замены информации в носителе связана с его техническими возможностями по времени хранения информации. Условия и способ хранения носителя у пользователя связаны с назначением вычислительной системы, с габаритом и весом носителя, его конструкцией, которые должны быть минимальными, желательно в виде плоской карточки, помещающейся в кармане одежды пользователя. Взаимозаменяемость конструкции носителя необходима для обеспечения его работы на ответных частях всех терминалов данной вычислительной системы. Содержание и объем паролей и служебной части информации НКП должны строго соответствовать идеологии применения паролей в системе опознавания и разграничения доступа, так как НКП, если таковые применены, являются неотъемлемой ее частью, разработанной по единому техническому заданию.

Применяемые носители кодов паролей (НКП) можно разделить на контактные, бесконтактные и смешанного типа. Каждый вид носителя обладает своими достоинствами и недостатками. При частом применении контактных НКП (стыковке и расстыковке с ответной частью) предъявляются высокие требования к качеству контактной поверхности и механической прочности контактов. С увеличением числа контактов эти характеристики ухудшаются.

Бесконтактные носители могут быть простыми, а аппаратура записи или применяемое для этой цели оборудование – относительно сложным и дорогим, объем записываемой информации небольшой. Простые носители часто не отвечают требованиям защиты от компрометации, которые в последнее время существенно возросли.

Логично утверждать, что стойкость НКП к компрометации тем выше, чем сложнее аппаратура считывания информации. Этим требованиям наиболее полно отвечает ППЗУ. Процесс усложнения несанкционированного считывания информации далее идет по пути применения криптографических методов, когда на НКП, кроме памяти, помещаются защитные схемы и преобразователи, не позволяющие считать информацию с НКП без дополнительных специальных, периодически заменяемых парольных процедур. При этом следует иметь в виду, что непосредственное шифрование только кода пароля, его стойкость к компрометации не увеличит, так как по сути паролем становится результат преобразования, а он остается легкодоступным. Поэтому подделка и фальсификация НКП должны быть существенно затруднены.

С переходом на «электронные деньги» потребовалось создание НКП массового применения (кредитных карточек), надежных и удобных в обращении с высокой достоверностью хранения и стойкости к компрометации информации.

Еще недавно существенную роль в выборе конструкции НКП играли объем записываемой информации и физический процесс записи информации в носитель. Развитие технологии изготовления элементов памяти позволило получить перепрограммируемые полупроводниковые энергонезависимые запоминающие устройства с достаточно большим объемом памяти, что почти решило проблему создания НКП широкого применения с высокими показателями.

Выбор того или иного носителя определяется требованиями к автоматизированной системе, ее назначению; выполняемым функциям, режиму использования, степени защиты информации, количеству пользователей, стоимости и т.д., на основе которых определяются требования к НКП.

В зависимости от физических принципов записи, хранения и считывания идентификационной информации носители кодов делятся на следующие виды:

- 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 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 1 Кбит до 4 Кбит. 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 вычислительной системе. 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. Однако и они подвержены вскрытию [33]. Вопрос заключается только в квалификации, времени и средствах. Карты «проксимити» очень удобны в эксплуатации.

Все атрибутивные идентификаторы обладают одним существенным недостатком. Идентификационный признак слабо связан или совсем не связан с личностью предъявителя. Как было показано выше (п. 2.7), необходимо запоминание дополнительного несложного кода.

4.3.7. Оценка программ контроля и разграничения доступа как средства защиты

Такую оценку необходимо провести по двум ее составляющим: аутентификации и разграничению доступа с учетом возможных путей их обхода в конкретной автоматизированной системе.

При этом целесообразно разделить оценки ПКРД и стойкости пароля. Оценку ПКРД целесообразно производить по формуле (3.14) для многозвенной защиты контролируемых каналов НСД, где роль звеньев будут выполнять средства защиты, перекрывающие контролируемые пути обхода, перечисленные выше. Прочность отдельного средства защиты оцениваем по формуле (3.8). Прочность защиты на неконтролируемых путях обхода необходимо оценить по формуле (3.14), а отдельного средства защиты – по формуле (3.1).

Стойкость пароля к подбору его значения определяется по формулам (3.9) и (3.10). Разграничение доступа оценивается по формуле (3.8).

При этом время реакции системы контроля (от момента передачи запроса до отображения на терминале службы безопасности сообщения о НСД) измеряется экспериментально с применением искусственного нарушения (неправильного пароля, обращения к информации за пределами полномочий) по каждому виду НСД не менее 10 раз в разное время в режиме наибольшей нагрузки АС. Ожидаемое время нарушителя на успешный доступ к информации определяется методом экспертных оценок с учетом принятой модели его поведения, приведенной в подразд. 1.3.3.

4.4. Контроль целостности программного обеспечения и информации

Контроль целостности программ и данных выполняется одними и теми же методами. 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 байтов. Все двоичные слова поразрядно суммируются с накоплением по mod2, образуя в результате контрольную сумму. Разрядность контрольной суммы равняется разрядности двоичного слова. Алгоритм получения контрольной суммы может отличаться от приведенного, но, как правило, не является сложным и может быть получен по имеющейся контрольной сумме и соответствующему файлу.

Другой подход к получению характеристик целостности связан с использованием **циклических кодов** [83]. Суть метода состоит в следующем. Исходная двоичная последовательность представляется в виде полинома $F(x)$ степени $n-1$, где n – число битов 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;
 $R(x)$ – 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 нарушитель может провести изменения таким образом, чтобы контрольная характеристика не изменилась (например, добавив коды).

Задача нарушителя усложнится, если использовать переменную длину двоичной последовательности при подсчете контрольной характеристики, а характеристику хранить в зашифрованном виде в отдельном каталоге службы безопасности информации или вне АС (например, в ЗУ Touch Memory). Доступ к программе подсчета контрольной суммы для пользователя должен быть закрыт.

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:

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

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

Двоичная последовательность с синдромом имеет вид:

$A' = 1010010011$ (синдром подчеркнут).

Последовательность A' хранится и(или) передается в КС.

Б. Контроль целостности информации.

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

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

Результат произведенных вычислений свидетельствует о целостности информации.

Если синдром отличен от нуля, то это значит, 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 АС. 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.

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

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. Системы обработки информации. Защита криптографического преобразования);
- перемешивание результатов;
- поразрядное суммирование по mod2 слов длиной 256 бит исходной последовательности;
- вычисление функции H .

В результате получается хэш-функция длиной 256 бит. Значение хэш-функции можно хранить вместе с контролируемой информацией, так как, 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 [27].

Прочность защиты целостности ПО определяется в первую очередь соотношением ожидаемого времени затрат нарушителя на подгонку контрольной суммы с суммой периода контроля целостности, времени контрольной процедуры и времени передачи сигнала НСД на терминал службы безопасности. Если временные затраты нарушителя больше периода контроля, прочность защиты обеспечена. В случае с хэшированием его затраты значительно больше периода времени контроля.

Если гипотетически допустить попытку нарушителя определить стартовый вектор путем перебора его значений, то согласно расчетам, приведенным в подразд. 3.2, на эту работу уйдут годы. Поэтому, принимая во внимание такую ситуацию, целесообразно значение стартового вектора менять не реже одного раза в год.

Особенность такой защиты заключается в том, что криптографические средства здесь работают не с временем жизни информации, а с периодом контроля состояния предмета защиты. По-прежнему остается актуальным вопрос блокировки несанкционированных действий нарушителя, который, зная о периоде времени контроля и сознавая неизбежность обнаружения его действий, не будет заниматься подгонкой контрольной суммы, а будет искать другие пути НСД (например, использовать свободные точки входа, модифицировать ПО или внедрить собственную программу с целью получения ценной информации или отключения процедуры проверки). Поэтому период контроля целостности очень важен.

Для решения этой проблемы нужно найти разумный компромисс между качеством и периодичностью контроля. Возможно построение некоторой системы, состоящей из отдельных процедур, автоматически проверяющих по случайному графику отдельные части программного обеспечения информации. Данные процедуры, меньшие по объему, будут меньше влиять на производительность системы, и нарушитель не будет знать времени наступления той или иной проверки.

4.5. Дублирование информации

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

В зависимости от ценности информации, особенностей построения и режимов функционирования АС могут использоваться различные методы дублирования, которые классифицируются по различным признакам [27].

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 АС. Все методы, не обеспечивающие выполнения этого условия, относят к *неоперативным методам* дублирования.

По используемым средствам для целей дублирования 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 и многоуровневые. Как правило, число уровней не превышает трех.

По степени пространственной удаленности носителей основной и резервной информации методы дублирования могут быть разделены на методы сосредоточенного дублирования и 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.

Методы дублирования разделяются на методы со сжатием информации и 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 АС 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 цилиндрах и поверхностях жесткого диска (пакета дисков), отличных от тех, на которых находятся рабочие таблицы. Такое дублирование защищает от полной потери информации при повреждении отдельных участков поверхности дисков.

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

В автоматизированных системах, к которым предъявляются высокие требования по сохранности информации (военные системы, АСУ технологическими процессами, серверы сетей, коммуникационные модули сетей и др.), 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 технологии RAID (*Redundant Array of Independent Disks*) [42]. Эта технология реализует концепцию создания блочно-го 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 выделяются 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 разное 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 блоков данных и контрольной информации. На этом уровне можно 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 мин.

Блочная конструкция подсистем RAID позволяет наращивать число дисков. Реальные подсистемы поддерживают несколько уровней, которые выбираются пользователем с учетом требований, предъявляемых к внешним запоминающим устройствам (ВЗУ) конкретной АС. 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 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 ленты 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 применяться 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 применения 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, получения важных сообщений по сети или результатов выполнения программ) [27].

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

4.6. Средства защиты программного обеспечения и информации от несанкционированной загрузки

Практика показывает, что наиболее слабым местом с позиций НСД являются каналы доступа к информации и программному обеспечению КСА со стороны средств загрузки как при начале работы, так и в процессе эксплуатации АС.

К средствам, с помощью которых проводятся процессы загрузки и перезагрузки ПО и информации, относятся машинные носители в виде магнитных лент, гибких и жестких дисков, магнитооптических дисков. На одних носителях могут находиться операционная система вычислительного комп-

лекса, отдельные сервисные программы, на других – прикладные программы, базы данных и т.д.

В этом случае необходимо рассматривать потенциальные угрозы, которые возможны на этапе создания ПО, транспортировке носителя на объект эксплуатации, копировании ПО и информации на другой носитель, хранении и возможной его транспортировке на другой объект эксплуатации.

На этапе создания ПО для исключения преднамеренных несанкционированных изменений и ознакомления с информацией к работам привлекаются проверенные и квалифицированные специалисты, которым создаются необходимые условия для работы, исключающие доступ посторонних лиц к документам, по которым изготавливается программное изделие; предоставляется стендовое оборудование, проверенное на отсутствие программных «вирусов»; обеспечивается хранение носителя в специальных шкафах, закрываемых на ключ, и помещениях с ограниченным и контролируемым доступом.

При разработке программного обеспечения разработчик применяет следующие меры:

- точное и однозначное определение для каждой разрабатываемой программы перечня автоматизируемых функций;
- использование средств и технологии программирования, минимизирующих число точек входа и вероятность наличия дополнительных функциональных возможностей, которые могут быть использованы для несанкционированных действий;
- исключение из состава ПО отладочных программ и средств программирования за исключением тестовых;
- исключение возможности внесения посторонними лицами несанкционированных изменений в программу в процессе ее разработки и отладки.

После того как программное изделие будет готово, обеспечиваются определенные гарантии того, что после продажи и передачи его новому владельцу последний будет иметь средства проверки (верификации) неизменности и подлинности программного изделия.

Самыми простыми и необходимыми средствами для этой цели являются маркировка носителя и паспорт на него, подписанный главным конструктором, разработчиком и приемщиком изделия. В паспорте на изделие проставляется контрольная сумма всех машинных слов данного изделия. Кроме того, с данного изделия снимается несколько копий, количество которых определяется исходя из потребностей заказчика, но не менее двух, одна из которых будет считаться эталонной, а вторая – рабочей. Эталон изделия должен храниться в удаленном и надежном месте в условиях ограниченного доступа, исключающих влияние внешних случайных и преднамеренных воздействий. Он используется для периодических проверок рабочей копии во время эксплуатации АС и на случай аварийной ситуации на объекте эксплуатации. Средства обеспечения контроля подлинности ПО и информации рассмотрены в подразд. 4.4.

Защита процесса загрузки ПО предполагает исключение постороннего вмешательства. Для этого на аппаратном или программном уровне блокируется работа всех внешних устройств за исключением того, на котором установлен носитель с загружаемым ПО. Пока не будет завершена загрузка, уста-

новлены и проверены на функционирование механизмы защиты информации, должны быть заблокированы устройства ввода информации и каналы связи.

В ответственных АС рекомендуется применять ПК без дисководов, а загрузку и перезагрузку ПО производить сетевыми средствами.

В процессе эксплуатации на случай непонятных сбоев работы АС предусматривается перезагрузка ПО. Она может проводиться со съемного и не съемного носителя. В первом случае носитель должен находиться на учете у службы безопасности и храниться в сейфе. При нормальном функционировании системы доступ к средствам управления загрузкой и местам установки носителя должен быть закрыт крышкой или дверцей, находящейся под централизованным контролем вскрытия аппаратуры технических средств АС. При начале процесса перезагрузки операторы терминалов должны прекратить свои работы до особого указания руководителя работ, внешние каналы связи должны быть отключены. Выполнение указанных действий должно контролироваться службой безопасности информации организационными мерами.

В процессе эксплуатации согласно инструкции на АС, по желанию системного администратора или администратора безопасности информации (ответственность за контроль функционирования и безопасности данных должна быть разделена) проводится периодическая проверка контрольной суммы на соответствие ее значению, указанному в паспорте на программное изделие.

4.7. Защита информации на машинных носителях

Современные машинные носители информации имеют малые габариты и вес, а также большую емкость, стандартные размеры и интерфейс с вычислительными средствами. Эти достоинства делают их весьма привлекательными для нарушителя. Он может их легко похитить, скопировать, модифицировать или подменить. Для защиты от подобных угроз рекомендуется:

- сократить до минимума количество применяемых носителей в создаваемой АС;
- провести маркировку и электронную идентификацию носителей. Маркировка должна отражать уровень конфиденциальности носителя;
- применяемые носители поставить на строгий учет с ежедневной выдачей его пользователям под расписку;
- при транспортировке и долговременном хранении использовать шифрование информации.

При шифровании информации на дисковых носителях для транспортирования по неохраняемой территории можно использовать упрощенный алгоритм – гаммирование. При этом доставку информации следует производить на двух носителях в разное время и разным маршрутом. На одном носителе доставляется информация, закрытая методом ее сложения по mod2 со случайной последовательностью символов длиной, равной длине информации, подлежащей защите; на другом – упомянутая последовательность сим-

волов. Второй носитель доставляется после подтверждения доставки первого. На месте доставки на ПЭВМ операция сложения повторяется, и в результате получатель имеет информацию в открытом виде.

Достоинства этого метода: простота реализации (простая программа шифрования-дешифрования) и высокая прочность защиты (длина ключа шифрования равна длине информации). При повторении транспортировки новой информации датчиком случайных чисел вырабатывается новый ключ. При этом длина закрываемого текста не должна быть больше длины вырабатываемого ключа.

Ограничением на применение данного метода являются частота его применения, быстрота передачи и объемы информации. При увеличении этих параметров имеет смысл воспользоваться сетью передачи данных и другими средствами защиты, которые рассмотрены ниже.

4.8. Защита остатков информации

Определенную проблему представляет собой защита от НСД остатков информации на магнитных носителях, которые могут сохраниться даже при наложении на старую запись новой информации на одном и том же носителе. Это может произойти в том случае, когда новый файл оказывается короче предыдущего, а также при отказах аппаратуры. Применение обычного стирания и наложения новой записи на старую также не гарантируют пропадание старой информации, так как физически за счет некоторого смещения записываемой головки возможно смещение новой записи относительно старой, которое обнаруживается специальной аппаратурой.

Обычно защита остатков файла осуществляется с помощью программы, на что затрачивается значительное время. Сложность возрастает в связи с тем, что основной источник остатков – рабочие файлы освобождаются после окончания работы пользователя. Все файлы управляются операционной системой, распределяющей память в соответствии с запросами различных пользователей. Поэтому вводится указатель областей основной памяти, отводимых всем файлам. По мере освобождения области памяти необходимо затирать ее путем записи нулей. Но это сложная работа, требующая значительного машинного времени.

С другой стороны, защита остатков от НСД может предполагать и другое решение – запрет доступа к ним. При последовательном размещении файлов пользователю не разрешается считывать участки за пределами сделанной им ранее записи. Но этот способ предполагает защиту остатков файлов только при доступе через операционную систему. Если же магнитная лента или пакет дисков вынесены с объекта эксплуатации, то содержимое может быть прочитано на другой ЭВМ. В этом случае даже запись нулей на место остатка может оказаться недостаточной. Зарубежные специалисты рекомендуют в этом случае на место остатка записывать шумовую (случайную) информацию с повторением записи не менее семи раз.

При отсутствии возможности стереть остаточную информацию носитель, ЗУ или устройство уничтожается физически на специальном оборудовании под контролем службы безопасности.

В настоящее время разработано несколько модификаций устройств стирания информации:

- для экстренного уничтожения информации на накопителе, установленном в компьютере, тип 2с-994е и 2е-994i;
- для защиты информации на серверах – «Цунами»;
- утилизаторы информации – «Горгона»;
- защита информации при транспортировке носителей – «Тень»;
- информационный сейф – «Миг»¹.

4.9. Защита информации в линиях связи

Решение вопроса защиты информации от преднамеренного НСД в линиях связи автоматизированной системы с сосредоточенной обработкой данных связано с конкретным размещением ее технических средств на объекте эксплуатации, количеством этих средств, пользователей и обслуживающего персонала, а также режимом работы, объемом и важностью данных.

Предполагается, что данная АС находится на контролируемой владельцем АС территории. Считается, что в данных условиях линии связи находятся под определенной защитой и вероятность появления нарушителя незначительна. Однако с увеличением количества работающих на объекте эта вероятность повышается, и возникает необходимость в дополнительных мерах защиты. Распределение большого количества технических средств по территории увеличивает длину и количество кабелей и, следовательно, вероятность несанкционированного подключения к ним. Современное развитие техники съема информации с кабеля связи и подключения к нему позволяет относительно легко это сделать.

В качестве средств защиты от подобных угроз рекомендуются:

- концентрация технических средств АС на объекте эксплуатации;
- прокладка кабелей в металлических трубах, труднодоступных местах;
- периодический визуальный контроль состояния кабелей;
- применение оптоволоконного кабеля;
- шифрование информации;
- аутентификация пользователей по специальному алгоритму с применением одноразовых паролей.

Шифрование информации и аутентификация используются, если в АС применяются удаленные терминалы и технические средства.

Указанные средства применяются в зависимости от требуемого уровня безопасности информации. По предлагаемой в данной книге классификации рекомендуются:

- по I классу – все перечисленные средства защиты;
- по II классу – все, кроме последнего;
- по III классу – все, кроме двух последних.

¹ См.: Прокофьев Н. Тяжелая артиллерия информационной безопасности // КомпьютерПресс. – 2002. – № 3.

4.10. Средства регистрации доступа к информации АС

Регистрация является одним из эффективных и важных методов увеличения безопасности систем. Без ведения точного регистрационного машинного журнала невозможно проследить за тем, что произошло в прошлом, и перекрыть каналы доступа к информации. Регистрационный журнал может анализироваться как периодически, так и непрерывно. Записи журнала можно выводить на экран или распечатывать на принтере. Их также можно использовать и для статистического анализа.

В журнале регистрации должны отмечаться [12]:

- регистрация входа/выхода пользователей в систему/из системы либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратного отключения АС. При этом в параметрах регистрации указываются:
 - время и дата входа/выхода в систему/из системы или загрузки/останова системы;
 - результат попытки входа: успешный или неуспешный – несанкционированный;
 - идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
 - код или пароль, предъявленный при неуспешной попытке;
- регистрация запуска/завершения всех программ и процессов (заданий, задач) в АС. В параметрах регистрации указываются:
 - дата и время запуска;
 - имя (идентификатор) программы (процесса, задания);
 - идентификатор субъекта доступа, запросившего программу (процесс, задание);
 - результат запуска (успешный, неуспешный – несанкционированный);
 - полная спецификация соответствующего файла «образа» программы (процесса, задания) – устройство (том, каталог), имя файла (расширение);
- регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:
 - дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная – несанкционированная;
 - идентификатор субъекта доступа;
 - спецификация защищаемого файла;
 - имя программы (процесса, задания, задачи), осуществляющей доступ к файлу;
 - вид запрашиваемой операции (чтение, запись, удаление, выполнение, расширение и т.п.);
- регистрация попыток доступа программных средств к терминалам, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная – несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого объекта (логическое имя/номер);
- имя программы (процесса, задания, задачи), осуществляющей доступ к защищаемому объекту;
- вид запрашиваемой операции (чтение, запись, монтирование, захват и т.п.);
- регистрация выдачи печатных (графических) документов на «твердую» копию.

Администратор безопасности информации должен иметь возможность периодически выводить на печать информацию, отсортированную по пользователям, терминалам, датам, элементам данных и т.д. Если объем информации в регистрационном журнале достаточно велик, не следует отказываться от тех возможностей, которые он позволит получить, а именно определить для любого заранее заданного периода времени (в прошлом) следующие события:

- учет изменений полномочий пользователей;
- содержание изменений полномочий;
- все доступы к любому защищаемому ресурсу, выделенные по каждому пользователю, программе, терминалу, заданию, элементу данных и т.д.;
- все отказы в доступе;
- случаи неиспользованного разрешенного доступа;
- изменения показаний системных часов;
- другие изменения, производимые оператором в содержании памяти системы.

Журналы регистрации могут помочь выявить пользователей, которые случайно допускали ошибки, и оказать им помощь в приобретении навыков, необходимых для работы. Журналы могут также показывать, что некоторые пользователи или терминалы никогда не обращаются к элементу данных, и их профили полномочий могут быть сокращены. Журналы могут служить инструментом психологического воздействия на потенциальных нарушителей. Кроме того, они часто используются для возврата системы в исходное состояние и восстановления наборов данных, которые были искажены во время неполадок в системе.

Для дальнейшего повышения безопасности записи регистрационного журнала могут быть зашифрованы. Доступ к журналу должен быть открыт только для системного администратора и администратора безопасности информации. Стирание информации в журнале следует заблокировать. Регистрационный журнал должен быть независим от системы, которую он контролирует. В противном случае имеется риск вмешательства системы в ведение журнала и превращение его в неэффективное средство защиты.

Перечисленные меры приведены для АС первого класса безопасности. Для АС более низкого класса эти меры могут быть сокращены количественно и качественно на усмотрение разработчика и заказчика. Регистрация как средство защиты носит профилактический характер, поэтому в расчет прочности защитной оболочки не включается. Однако применение ее обязательно в целях проведения анализа различных ситуаций и документирования событий.

4.11. Защита информации при документировании

Документирование информации должно сопровождаться автоматической маркировкой каждого листа (страницы) документа, его последовательным номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). Вместе с выдачей документа должна автоматически оформляться учетная карточка документа с указанием даты выдачи документа, учетных реквизитов документа, краткого содержания (наименования, вида, шифра, кода) и уровня конфиденциальности документа, фамилии лица, выдавшего документ, количества страниц и копий документа (при неполной выдаче документа – фактически выданного количества листов в графе брака). В параметрах регистрации печати документов указываются:

- время и дата выдачи (обращения к подсистеме вывода);
- спецификация устройства выдачи (логическое имя/номер внешнего устройства);
- краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
- идентификатор пользователя, запросившего документ;
- объем фактически выданного документа (количество страниц, листов, копий) и результат (успешный, неуспешный).

4.12. Организационные мероприятия по защите информации в АС

В процессе подготовки системы к эксплуатации в целях защиты информации необходимо:

- при выделении территории, зданий и помещений обозначить контролируемую зону вокруг места размещения АС;
- установить и оборудовать охранную сигнализацию по границам контролируемой зоны;
- создать контрольно-пропускную систему;
- проверить схему размещения и места установки аппаратуры АС;
- проверить состояние системы жизнеобеспечения людей, условия функционирования аппаратуры и хранения документации.

Параллельно с указанными мероприятиями организацией-потребителем АС провести:

- перестройку структуры организации-потребителя в соответствии с потребностями внедряемой системы;
- подобрать кадры для технического обслуживания и управления АС;
- при необходимости подобрать специальные кадры для работы по защите информации в АС и создать централизованную службу безопасности информации при руководстве организацией-потребителем АС;

- провести обучение кадров у разработчиков АС;
- организовать распределение функциональных обязанностей и ответственности должностных лиц;
- установить полномочия должностных лиц по доступу к техническим средствам и информации АС;
- разработать должностные инструкции по выполнению функциональных обязанностей технического, оперативного состава должностных лиц, включая службу безопасности информации.

После выполнения указанных мероприятий и приема аппаратуры необходимо выполнить:

- постановку на учет аппаратуры, носителей информации и документации;
- проверку отсутствия посторонней аппаратуры;
- контроль размещения аппаратуры в соответствии с требованиями по разграничению доступа, побочного электромагнитного излучения и наводок информации;
- проверку функционирования системы контроля вскрытия технических средств АС;
- проверку функционирования АС с помощью средств функционального контроля;
- проверку на отсутствие штатных и посторонних коммуникаций, выходящих за пределы контролируемой зоны;
- верификацию и загрузку штатного программного обеспечения;
- ввод в систему оргштатной структуры организации, списка должностных лиц и их условных номеров;
- запись значений паролей в носители и таблицы их ответных значений;
- запись на носители ключей шифрования информации;
- ввод соответствующих признаков в таблицы полномочий пользователей;
- загрузку информации, имитирующей штатную работу системы;
- проверку функционирования АС, включая систему защиты информации, по специально разработанным организацией-потребителем программам испытаний с участием оперативного состава должностных лиц;
- тренировку оперативного состава должностных лиц и опытную эксплуатацию АС;
- проверку побочного излучения и наводок информации аппаратурой АС на границах контролируемой зоны во время наибольшей активности работы системы.

По положительным результатам указанных проверок и тренировок загрузить штатную информацию, сменить значения паролей в носителях и таблицах их ответных значений, при необходимости уточнить и скорректировать полномочия пользователей в соответствующей таблице АС.

В процессе эксплуатации системы служба безопасности информации осуществляет:

- контроль и регистрацию доступа к техническим средствам АС с помощью системы контроля вскрытия аппаратуры;
- контроль полномочий и доступа к информации с помощью системы контроля разграничения доступа, включающей систему паролей;

- контроль функционирования системы защиты информации;
- контроль целостности программного обеспечения;
- контроль целостности данных;
- контроль ввода технических средств в рабочую конфигурацию обработки информации и вывода из нее;
- контроль стирания остатков информации при проведении профилактических и восстановительных работ на технических средствах АС;
- контроль документирования информации и учета документов.

При получении сигналов тревожной сигнализации необходимо быстро установить место ее возникновения, время и причину несанкционированных действий. По результатам расследования принимаются меры в соответствии с действующими инструкциями.

В процессе эксплуатации может возникнуть необходимость в доработках АС, которые должны проводиться под контролем службы безопасности. При доработках программного обеспечения старое ПО заменяется новым при выводе АС в режим прекращения функционирования и удаления штатной информации. Кроме того, в процессе эксплуатации системы рекомендуется проводить:

- периодические проверки полномочий лиц, работающих на АС;
- инспектирование правильности и полноты выполнения персоналом мер по обеспечению сохранности необходимых дубликатов файлов, библиотеки программ, оборудования АС;
- практическую проверку функционирования отдельных средств защиты;
- контроль недозволённых изменений программ и оборудования;
- контроль всех процедур с библиотеками файлов на носителях и т.д.;
- стимулирование персонала в вопросах обеспечения защиты;
- разработку и обеспечение всех противопожарных мероприятий и обучение персонала действиям по тревоге;
- консультирование всех сотрудников, работающих с АС, по вопросам обеспечения защиты информации.

Одна из обязанностей службы безопасности – организация и проведение обучения персонала методам обеспечения защиты информации. Обучение необходимо для всех сотрудников, начиная с момента их поступления на работу, включая руководящий состав организации – потребителя вычислительной системы.

Все служащие должны знать, что данные и файлы, с которыми они работают, могут быть в высшей степени конфиденциальны. Программы и документы с информацией, подлежащей защите, не следует брать для работы на дом. В детальной степени должны быть определены и идентифицированы все функции и ограничения при выполнении каждой работы. Это связано с необходимостью минимизировать сведения, которыми обладает каждый сотрудник, сохранив при этом их эффективное взаимодействие.

В системах с высокой степенью безопасности специалисты, обслуживающие АС в процессе эксплуатации, делятся на три категории:

- пользователи, т.е. представители организации – владельца АС, выполняющие оперативные задачи при работе с информацией (старший – руководитель всех работ на объекте автоматизации);

- технический персонал, поддерживающий нормальное функционирование АС (старший – системный администратор);
- должностные лица службы обеспечения безопасности информации, подчиненные руководству организации – владельца АС.

Если АС, АСУ или вычислительная сеть используется для обслуживания населения, то появляется другой тип пользователей и значительно повышается риск несанкционированного доступа к информации (например, в банковских АС).

Для обеспечения безопасности информации разграничение доступа к ней осуществляется как по вертикали, так и по горизонтали структуры организации – владельца АС, АСУ или сети, включая категории специалистов и пользователей.

Особая категория – специалисты и должностные лица службы безопасности информации, которая, владея средствами управления защитой, может иметь доступ к охраняемой информации. Однако и здесь существуют возможности разграничения и ограничения доступа, которые необходимо по возможности реализовать.

Принятая система распределения обязанностей между отдельными служащими может в значительной мере способствовать повышению уровня безопасности информации со стороны персонала.

В интересах безопасности информации специалисты рекомендуют следующие принципы организации работ.

Минимизация сведений, доступных персоналу. Каждый служащий должен знать только ту информацию, которая необходима ему для успешного выполнения своих обязанностей.

Минимизация связей персонала. Организация технологического процесса сбора и обработки информации и планирование помещений должны по мере возможности исключать или сводить к минимуму контакты персонала в процессе выполнения работ.

Разделение полномочий (привилегий). В системах с высокими требованиями безопасности некоторая ответственная процедура выполняется после подтверждения ее необходимости двумя сотрудниками. Например, изменение полномочий пользователя осуществлялось только в том случае, когда руководитель и сотрудник СБИ одновременно послали в систему свои пароли со своих терминалов.

Минимизация данных, доступных персоналу. Данные, которые могут быть обозримы персоналом, ограничиваются. Отходы должны систематически уничтожаться. Выходные данные, полученные на печатающих устройствах, должны быть взяты на учет и могут предоставляться только тем, кому они предназначены. Количество копий документов должно строго контролироваться. Обозначения и наименования документов и носителей информации не должны раскрывать их содержание.

Дублирование контроля. Контроль важных операций никогда нельзя поручать одному сотруднику. Присутствие еще одного человека оказывает психологическое влияние на другого и делает его более добросовестным в работе.

Факт передачи рабочей смены должен быть зафиксирован в специальных журналах с собственноручными подписями ответственных и сдающих сме-

ну, причем должно быть документально зафиксировано не только то, что передается, но и в каком состоянии.

В специальных хранилищах носителей информации должен вестись учет, фиксироваться каждая выдача и возвращение носителей. Носители с данными ограниченного пользования должны выдаваться только допущенным к ним лицам под расписку. Факты выдачи этих данных на печатающие устройства и записи на другие носители должны немедленно фиксироваться в журнале с указанием времени, объема и назначения проведенных работ.

В конце рабочей смены должны быть уничтожены установленным порядком накопившиеся за смену рабочие отходы, о чем должна быть произведена соответствующая запись с подписями должностных лиц в рабочем журнале.

Независимо от того, в круглосуточном режиме или с перерывами в работе организации – владельца АС, в ответственных системах обработки данных осуществляется непрерывный контроль доступа к информации, подлежащей защите. Это означает, что по окончании рабочей смены, прекращении функционирования АС и необходимости его выключения контроль доступа в помещения с аппаратурой АС и носителями информации должен передаваться под расписку другим ответственным за их охрану лицам до последующей передачи контроля следующей смене с регистрацией и подписями должностных лиц в специальном журнале.

Специалисты СБИ должны быть разносторонне подготовленными и разбираться не только в вопросах защиты, но и в технических вопросах, включая принципы работы и эксплуатации вычислительной техники, особенно средства хранения, ввода и вывода информации.

По окончании эксплуатации АС (связанной с ее заменой на более современную) необходимо провести ревизию остатков хранимой информации в АС; ценную информацию с обеспечением режима ограничения доступа переписать на более современные носители, а остальную – уничтожить.

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ С РАСПРЕДЕЛЕННОЙ ОБРАБОТКОЙ

5

5.1. Линейное шифрование

Линейному шифрованию сообщение подвергается на входе в коммуникационную систему. При линейном шифровании сообщение перед передачей в каналы связи зашифровывается полностью, включая все служебные данные. После получения на узле коммутации это сообщение дешифруется. После обработки служебной части согласно заданному маршруту определяется следующий канал связи для дальнейшей передачи, перед которой сообщение снова шифруется. Далее сообщение по каналу связи поступает на объект-получатель по назначению или, если данный узел не имеет прямой связи с объектом-получателем, – на следующий узел коммутации. При этом каждый раз на узле коммутации сообщение при получении дешифруется, при передаче снова шифруется, т.е. информация на нем какое-то время циркулирует в открытом виде.

В итоге передаваемая информация в региональных и глобальных системах проходит довольно сложный путь. При этом передается множество других сообщений. Пользователи, передающие и принимающие информацию, могут относиться к разным организациям с разными полномочиями. Последнее обстоятельство с позиций безопасности является особенно неприемлемым для собственника информации.

Функционирование такой системы в глобальной сети требует значительное множество кодов ключей шифрования, что затрудняет их централизованную рассылку и последующую замену. Уменьшение количества ключей увеличивает количество пользователей, работающих на одном ключе, что снижает безопасность информации. Поэтому такой способ шифрования целесообразен при небольшом количестве пользователей и узлов коммутации, а также в условиях принадлежности сети передачи данных и ее абонентов одной организации. С появлением других методов шифрования информации в сетях линейное шифрование теряет свои позиции. Сочетание его с абонентским шифрованием существенно увеличивает безопасность передаваемой информации, но увеличивает стоимость работ.

5.2. Абонентское шифрование

При абонентском шифровании [37] схема подготовки, передачи и приема информации в классическом варианте (применение одного общего секретного ключа шифрования-дешифрования) выглядит согласно рис. 5.1.

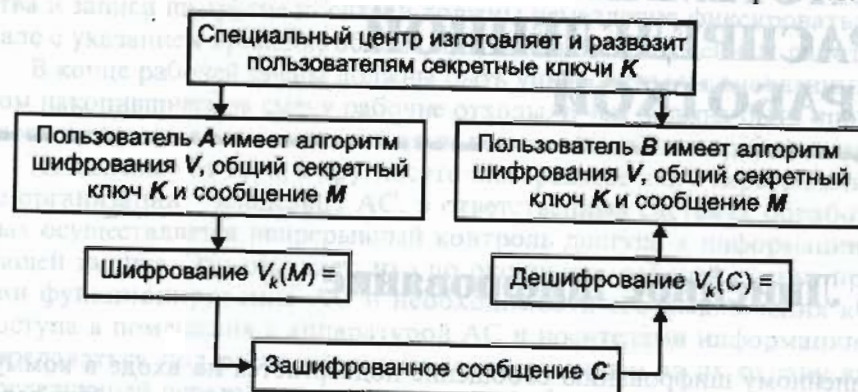


Рис. 5.1. Схема рассылки и использования ключей при симметричном шифровании

В такой системе центр изготовления и рассылки ключей не только снабжает пользователей ключами, но и несет ответственность за их сохранение в секрете при изготовлении и доставке. А поскольку в случае утечки информации в результате компрометации ключей в такой системе практически невозможно доказать, где произошла компрометация (у одного из пользователей или в центре), то обычно принимается, что центр в этом смысле надежнее, и потому на него возлагается контроль за всеми ключами на протяжении всего цикла от изготовления до их уничтожения у пользователя. Таким образом, вопрос о том, кто является истинным хозяином информации, получает однозначный ответ. По этой причине функции центра должны принадлежать АСУ, а не сети передачи данных.

Центр выступает и как гарант подлинности передаваемых сообщений, так как, если пользователю В (см. рис. 5.1) удастся с помощью секретного ключа K , доставленного из центра, расшифровать сообщение M , полученное им от пользователя А, то он уверен, что зашифровать и отправить его мог только обладатель того же ключа K , а это мог быть только пользователь А (или другой пользователь, получивший такой же ключ из центра).

Здесь мы подходим к следующей проблеме. Если в сети обмениваются информацией по принципу «каждый с каждым», например 100 пользователей, то потенциально возможных связей между ними $(99 \cdot 98)/2 = 4851$, т.е. для обеспечения независимого обмена информацией между каждой парой пользователей центр С должен изготовить и разослать 100 комплектов по 99 ключей в каждом, сформированных надлежащим образом из исходного набора 4851 ключа. Если ключи сменяются хотя бы один раз в месяц, то в течение года необходимо изготовить 58212 исходных ключей, сформировать из них 1200 комплектов по 99 ключей в каждом и развести всем пользовате-

лям системы. И это для сети только из 100 пользователей. А если в сети работают несколько тысяч пользователей, то получится почти как у гоголевского героя «тридцать пять тысяч одних курьеров».

Этот «генетический дефект» традиционных систем обмена шифрованной информацией сразу же был остро прочувствован разработчиками коммерческих телекоммуникационных сетей при первых попытках использовать шифрование как средство подтверждения подлинности и авторства электронных документов при передаче их по каналам электросвязи 70-х годов. Даже такие мощные организации в области межбанковских расчетов, как S.W.I.F.T. (Международная межбанковская организация по финансовым расчетам), вынуждены идти на риск и прибегать при рассылке части секретных ключей к услугам обычной почты. Это дает возможность несколько снизить расходы, но применение дополнительных мер защиты секретных ключей, пересылаемых в конвертах, делает удешевление не столь ощутимым.

Размышления о том, как избавиться от недостатков традиционных систем криптографической защиты, связанных с необходимостью содержать мощную и дорогую службу изготовления секретных ключей и снабжения ими пользователей, привели двух американских исследователей У. Диффи и М. Хеллмана в 1976 г. к следующим принципиально новым идеям.

Предполагая, что пользователи имеют некоторую общеизвестную надежную процедуру (программу) шифрования и общеизвестные процедуры преобразования исходных ключей, можно изобразить схему формирования парой пользователей А и В общего секретного ключа K для шифрования/расшифрования (рис. 5.2).



Рис. 5.2. Схема формирования общего секретного ключа

Главным пунктом, принципиально отличающим данную схему получения пользователями общего секретного ключа от традиционной, является то, что обмен открытыми ключами $f(x)$ и $g(y)$ производится по любому доступному каналу связи в открытом виде. При этом должна быть гарантия, что по перехваченным в канале открытым ключам $f(x)$ и $g(y)$ практически невозможно получить общий ключ K , не зная хотя бы один из исходных секретных ключей x, y . В качестве такой гарантии в данном случае выступает сложность известной математической проблемы, которую приходится решать в ходе вычисления K по $f(x)$ и $g(y)$.

Если в качестве ключей x и y выбираются случайные целые числа из 512 бит каждое, то для вычисления K по $f(x) = a^x \bmod p$ и $g(y) = a^y \bmod p$ с целыми a и p (также по 512 бит каждое) необходимо проделать работу не менее чем из 10^{24} операций, что потребовало бы более 1000 лет работы любой современной суперЭВМ.

Таким образом, вычисление общего секретного ключа K только по открытым ключам $f(x)$ и $g(y)$ является практически невыполнимой задачей, что позволяет применять ключ K для надежного зашифрования информации.

Другой принцип, предложенный У. Диффи и М. Хеллманом для решения проблемы снабжения пользователей сети ключами шифрования/расшифрования, получил название *открытое шифрование*.

Для зашифрования и расшифрования информации используются различные ключи, которые хотя и связаны между собой, но устроены так, что вычислить по одному из них (открытому) второй (секретный) практически невозможно (в том же смысле, что и выше).

Теперь обмен зашифрованной информацией между пользователями можно изобразить так, как показано на рис. 5.3.



Рис. 5.3. Схема открытого шифрования

Первое практическое воплощение принцип открытого шифрования получил в системе RSA, разработанной в 1977 г. в Массачусетском Технологическом институте (США).

Идея авторов состояла в том, что, взяв целое число n в виде произведения двух больших простых чисел $n = p \cdot q$, легко подобрать пару чисел e и d , таких, что $1 < e, d < n$, чтобы для любого целого числа m , меньшего n , было справедливо соотношение $(m^e)^d = m \bmod n$.

В качестве открытого ключа шифрования в системе RSA выступает пара $Y = (n, e)$, а секретным ключом для расшифрования сообщений является число d .

Процедура шифрования сообщения M , рассматриваемого как целое число, меньшее n (при необходимости длинное сообщение разбивается на отрезки, шифруемые независимо), состоит в вычислении значения

$$C = M^e \bmod n.$$

Расшифрование осуществляется аналогично с помощью секретного ключа d :

$$M = C^d \bmod n.$$

Математически строго можно доказать, что определение по паре чисел n , e секретного ключа d не проще разложения на множители числа n , т.е. нахождения p и q . Задача же разложения на множители целого числа изучается в математике с древнейших времен и известна как очень сложная вычислительная задача. На современных ЭВМ разложение числа, состоящего из нескольких сотен десятичных знаков, потребует тысячи лет непрерывной работы.

Кроме системы RSA известен ряд систем открытого шифрования, основанных на других сложных математических задачах (укладка ранца, декодирование линейных кодов и т.д.), однако все они не получили достаточно широкого распространения, являясь теоретическими разработками.

С идейной точки зрения разница между системами открытого распределения ключей и открытого шифрования не настолько принципиальна: каждая из них при небольшой модификации может использоваться не только для шифрования, но и для распространения секретных ключей по открытым каналам связи.

Переход от открытого шифрования к открытому распределению ключей достаточно прозрачен: отправитель шифрует и передает с помощью системы открытого шифрования секретный ключ, на котором потом будет традиционным способом шифроваться информация. Общий секретный ключ, получаемый при открытом распределении ключей, можно использовать непосредственно для шифрования, побитно складывая его с передаваемым сообщением, в результате чего получается система открытого шифрования. Поэтому для именования обеих систем часто употребляют единый термин «системы с открытым ключом», не уточняя, какой тип обмена сообщений или ключей имеется в виду.

Дополнительным соображением в пользу единого именования систем является то, что с практической точки зрения их эффективнее использовать лишь для распределения секретных ключей, осуществляя шифрование информации традиционным способом. Дело в том, что основной операцией в этих системах является возведение в степень по модулю 500–1000-битовых чисел, что при программной реализации в несколько десятков раз медленнее, чем шифрование того же размера данных стандартным алгоритмом (например, DES). В связи с этим для быстрой обработки большого потока сообщений применяют специализированные процессоры, выполняющие данную операцию, или же используют системы с открытым ключом только для получения секретного ключа шифрования [37].

5.3. Цифровая подпись

Принципы открытого распределения ключей и открытого шифрования [37], решая наиболее трудоемкую проблему изготовления и рассылки секретных ключей для шифрования и предоставляя абонентам открытых систем возможность передать конфиденциальную информацию без непосредственного контакта и предварительного обмена ключами, поставили во главу угла

проблему подлинности партнера и авторства принимаемых сообщений. Развитие деловой переписки в электронном виде требовало не только возможности самому получателю удостовериться в подлинности документа, но и возможности доказать авторство документа третьей стороне, например суду.

Классическое распределение ключей посредством центра решало данную проблему частично: автором правильно расшифрованного сообщения мог быть только тот, кто знал ключ, т.е. отправитель, получатель и, возможно, центр.

Кроме того, предъявление третьему лицу документа вместе с ключом шифрования означает, что становятся известными и все остальные сообщения, переданные с помощью данного ключа, что не всегда приемлемо, а обеспечить всем по разовому ключу на каждое сообщение не представляется возможным. Следовательно, потребовался электронный аналог физической подписи, обладающий двумя свойствами:

- подпись воспроизводится только одним лицом, а подлинность ее может быть удостоверена многими;
- подпись неразрывно (посредством листа бумаги) связывается с данным документом и только с ним.

Путь создания электронной подписи также был предложен У. Диффи и М. Хеллманом и основывался, как и при открытом шифровании, на использовании пары связанных между собой ключей (секретного и открытого). Их идея состояла в том, чтобы в системе открытого шифрования поменять роли секретного и открытого ключей: ключ подписывания сделать секретным, а ключ проверки – открытым. Если при этом сохраняется свойство, что по открытому ключу с вычислительной точки зрения нельзя в обозримое время найти секретный ключ подписывания, то в качестве электронной подписи может выступать само сообщение, подписанное на секретном ключе. Тем самым подписать сообщение может только владелец секретного ключа, но каждый, кто имеет его открытый ключ, может проверить подпись, обработав ее на известном ключе.

В системе открытого шифрования RSA секретный и открытый ключи – числа e и d – равноправны, что позволяет непосредственно применить данную конструкцию и получить цифровую подпись RSA.

Использование в качестве цифровой подписи результата шифрования не является общим методом, а скорее служит иллюстрацией перехода от прежнего способа подтверждения подлинности, основанного на наличии у сторон одинакового секретного ключа, к системам с двумя разными ключами.

В общем случае под цифровой подписью понимается числовое значение, вычисляемое по сообщению с помощью секретного ключа подписывающего. Цифровая подпись проверяется общеизвестной процедурой на основании открытого ключа.

Открытый и секретный ключи жестко связаны между собой, но с вычислительной точки зрения невозможно как найти по открытому ключу секретный, так и подобрать саму подпись исходя только из известной процедуры проверки (рис. 5.4).

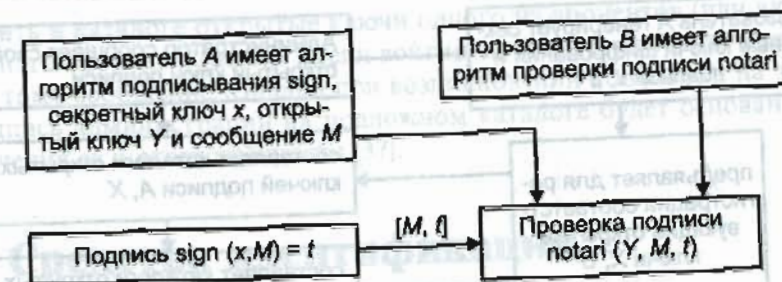


Рис. 5.4. Схема подписывания сообщения

Как видно из рис. 5.4, в эту схему естественным образом вписывается цифровая подпись на основе открытого шифрования.

Недостатки алгоритма цифровой подписи RSA [65]:

- 1) возможность фальсификации подписи при обнаружении невыполнения хотя бы одного из дополнительного множества условий проверки вычислений;
- 2) относительно большие вычислительные затраты по сравнению с другими алгоритмами при сохранении того же уровня криптостойкости;
- 3) уязвимость к так называемой мультипликативной атаке.

Поэтому в 1991 г. в США в качестве основы для национального стандарта был принят алгоритм американского ученого Эль-Гамала (Т. ElGamal). В его алгоритме открытый ключ Y , как и в открытом распределении ключей У. Диффи и М. Хеллмана, определяется по формуле:

$$Y = a^k \bmod p.$$

Подпись t состоит из пары чисел R и S , где $R = a \bmod p$ вычисляется для случайно взятого значения k , а $S = M + x \bmod p$.

Проверка подписи состоит в проверке соотношения $a^S = Y^R \cdot R^M \bmod p$.

Цифровая подпись в сочетании с открытым распределением ключей и (или) открытым шифрованием позволяет организовать защищенный обмен электронными документами с подтверждением подлинности как абонента, так и самих сообщений, прибегать к услугам дорогостоящей службы изготовления и развоза секретных ключей не требуется. При этом электронным документам может быть придана юридическая значимость.

Единственная проблема, которая не может быть решена при заочном общении пользователей, – обеспечение их достоверным каталогом открытых ключей пользователей (достаточно ограничиться открытыми ключами подписи). Однако в большинстве открытых систем имеется администратор системы, осуществляющий прием и регистрацию пользователей. Естественно, на него можно возложить сбор и предоставление открытых ключей.

Регистрация пользователей проводится так, как показано на рис. 5.5.

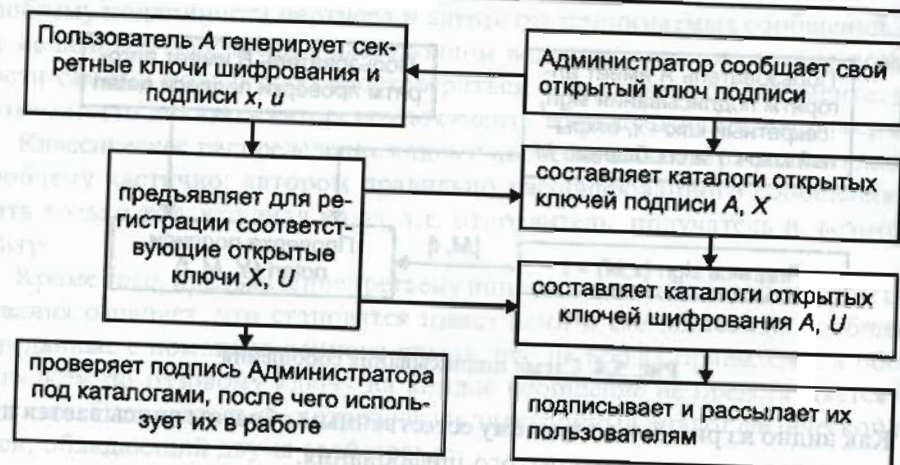


Рис. 5.5. Схема подготовки и рассылки ключей

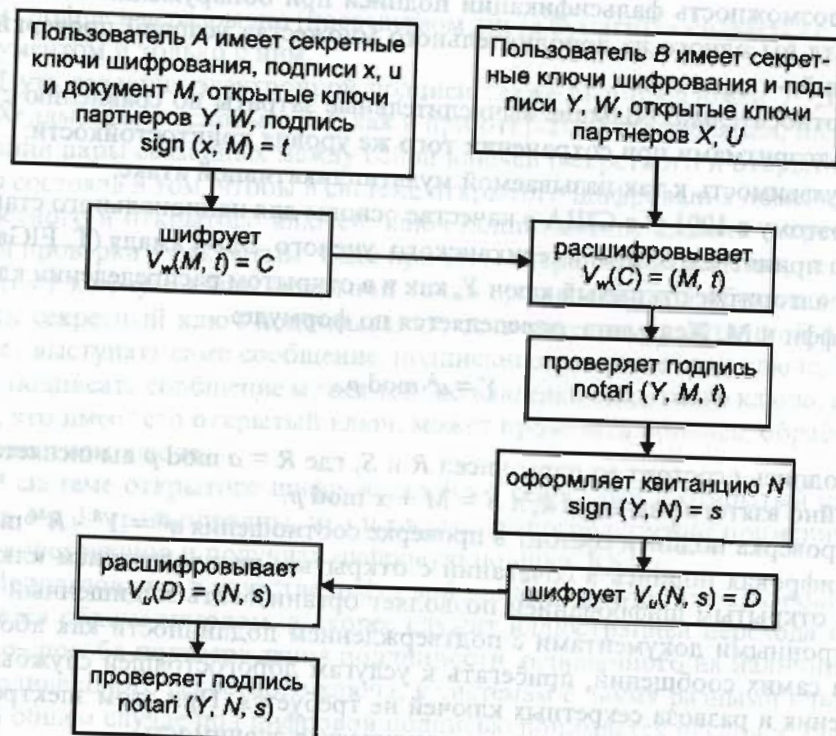


Рис. 5.6. Схема подписывания закрытых электронных документов

На рис. 5.6 схематично представлена работа с электронными документами. При такой организации в отличие от первоначальной схемы административной системы не имеет доступа к секретным ключам пользователей, а значит, — и к защищаемой с их помощью информации. Администрация может лишь

подменить в каталоге открытые ключи одного из абонентов (или включить фиктивного абонента), от его имени войти в контакт и получить предназначенное тому сообщение. Однако при возникновении конфликта на этой почве подпись администрации на подложном каталоге будет основанием для привлечения ее к ответственности [37].

5.4. Средства идентификации и аутентификации

Обычно стороны, вступающие в информационный обмен, нуждаются во взаимной проверке подлинности (аутентификации) друг друга. Этот процесс взаимной аутентификации выполняют в начале сеанса связи.

После того как соединение установлено, необходимо обеспечить выполнение следующих требований при обмене данными [40]:

- получатель должен быть уверен в подлинности источника данных;
- получатель должен быть уверен в подлинности получаемых данных;
- отправитель должен быть уверен в доставке данных получателю;
- отправитель должен быть уверен в подлинности доставленных данных;
- отправитель и получатель должны быть уверены в том, что в процессе передачи действительные значения секретных данных были недоступны посторонним лицам.

В число открытых данных могут входить идентификатор пользователя-отправителя, сообщение и уведомление отправителя о доставке сообщения, а секретных — пароль и сообщение. При этом уведомление посылается отправителю после проведения получателем процедуры приема сообщения.

Выполнение первых двух требований обеспечивается процедурой аутентификации и цифровой подписью данных; третьего и четвертого требований — уведомлением, подписанным цифровой подписью получателя; пятого требования — специальным алгоритмом аутентификации пароля и шифрованием данных.

Электронная цифровая подпись при удаленном обмене поставленные задачи решает только совместно с другими механизмами защиты. Считается, что процедура аутентификации достаточно легко реализуется путем обмена случайными числами, шифрованными или хэшированными на общем ключе участников обмена данными. Надежность данной процедуры требует выполнения непрерывности сеанса связи по причине возможности в другом случае подключения нарушителя после окончания процедуры аутентификации до начала передачи содержательной части сообщения.

Рассмотрим в качестве примера процедуру аутентификации для двух пользователей А и В. (Такая же процедура используется, когда вступающие в связь стороны не являются пользователями). Пусть применяется симметричная криптосистема. Пользователи А и В в исходном состоянии имеют одинаковые алгоритмы шифрования E_K и дешифрования D_K , секретный ключ K_{AB} и одностороннюю функцию $\alpha(\cdot)$. Вся процедура показана на рис. 5.7 [65].

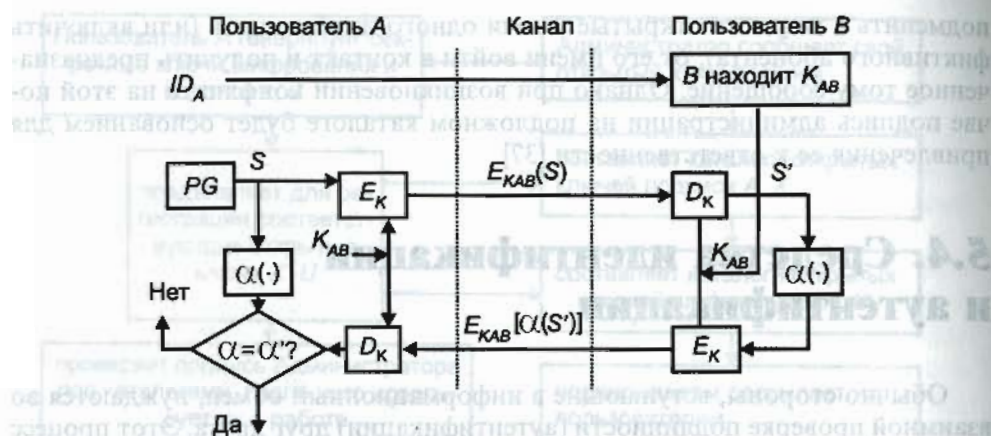


Рис. 5.7. Схема процедуры аутентификации

- Пусть пользователь А инициирует процедуру аутентификации пользователя В, отправляя ему свой идентификатор ID_A в открытой форме.
- Пользователь В, получив идентификатор ID_A , находит в своей базе данных секретный ключ K_{AB} и вводит его в свою криптосистему.
- Тем временем пользователь А с помощью псевдослучайного генератора PG генерирует случайную последовательность S , шифрует ее на ключе K_{AB} и отправляет ее пользователю В в виде криптограммы $E_{K_{AB}}(S)$.
- Пользователь В расшифровывает эту криптограмму и раскрывает исходный вид последовательности S' .
- Затем оба пользователя А и В преобразуют соответственно последовательности S и S' , используя открытую одностороннюю функцию $\alpha(\cdot)$.
- Пользователь В шифрует сообщение $\alpha(S')$ и отправляет пользователю А криптограмму $E_{K_{AB}}[\alpha(S')]$.
- Наконец, пользователь А расшифровывает эту криптограмму и сравнивает полученное сообщение $\alpha'(S')$ с исходным $\alpha(S)$. Если эти сообщения равны, пользователь А признает подлинность пользователя В.

Очевидно, пользователь В проверяет подлинность пользователя А таким же способом. Обе эти процедуры образуют процедуру взаимной аутентификации – «рукопожатия», которая обычно выполняется в самом начале любого сеанса связи между любыми двумя сторонами в компьютерных сетях.

Достоинством такой процедуры является то, что ни один из участников сеанса связи не передает и не получает никакой секретной информации.

В целях защиты от вмешательства нарушителя в процесс обмена полезно объединить процессы аутентификации и передачи сообщения и тем самым получить непрерывную проверку подлинности отправителей в течение всего сеанса связи. Один из простейших способов непрерывной проверки подлинности показан на рис. 5.8 [65]. Передаваемая криптограмма имеет вид $E_K(ID_A, M)$, где ID_A – идентификатор отправителя А; M – сообщение.

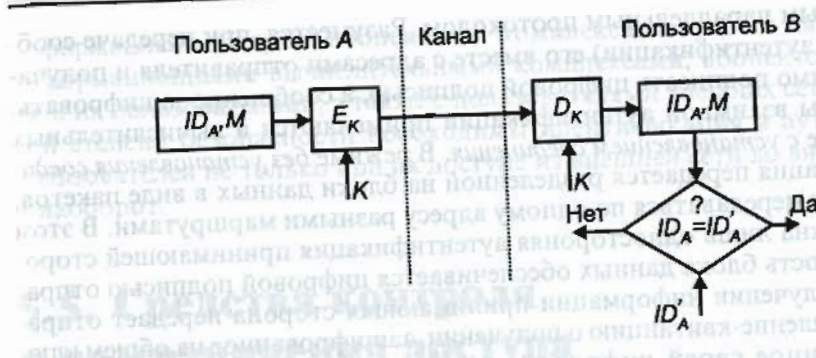


Рис. 5.8. Схема непрерывной проверки подлинности отправителя

Получатель В, принявший эту криптограмму, расшифровывает ее и раскрывает пару (ID_A', M) . Если принятый идентификатор ID_A' совпадает с хранящимся значением ID_A , получатель В признает эту криптограмму.

Другой вариант непрерывной проверки подлинности использует вместо идентификатора отправителя его секретный пароль, а идентификатор передается в открытом виде. С позиций стойкости к компрометации и простоты исполнения представляется приемлемым вариант аутентификации, приведенный на рис. 5.9 [2].

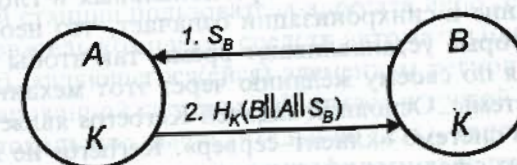


Рис. 5.9. Схем протокола аутентификации:

А и В – объекты взаимной аутентификации; К – секретный ключ хэширования;
 $||$ – знак конкатенации (приписывания)

Если инициатором обмена является объект В, то он генерирует случайное число S_B и посылает его объекту А в открытой форме. А посылает хэшированное на ключе К значение приписанных аргументов: адреса объекта В, своего адреса (А) и полученного числа S_B , т.е. $H_K(B || A || S_B)$. Объект В при получении H_K сравнивает его со значением, вычисленным у себя на том же ключе К от аргументов. Совпадение означает, что объект А аутентифицирован. Аналогично аутентифицируется объект В. Для усиления защиты в число аргументов можно включить время события. Но при проверке его необходимо учитывать поправку на ожидаемое время обработки и передачи сигналов.

Операция хэширования выполняется проще, чем операция шифрования. От нее не требуется свойство обратимости при известном ключе К. Свойство необратимости играет положительную роль в том, что пары соответствий $S - H_K(S)$ практически бесполезны для нарушителя при разрядности чисел S , $H_K(S)$ более 95 двоичных знаков. Учитывая время жизни передаваемой информации в конкретной автоматизированной системе, количество этих знаков можно сократить. Кроме того, данная схема защищена от атак с несанк-

ционированным параллельным протоколом. Разумеется, при передаче сообщения (после аутентификации) его вместе с адресами отправителя и получателя необходимо подписать цифровой подписью, а сообщение зашифровать.

Протоколы взаимной аутентификации применяются в вычислительных сетях в режиме *с установлением соединения*. В режиме *без установления соединения* информация передается разделенной на блоки данных в виде пакетов, которые могут передаваться по одному адресу разными маршрутами. В этом случае возможна лишь односторонняя аутентификация принимающей стороной. Подлинность блока данных обеспечивается цифровой подписью отправителя. По получении информации принимающая сторона передает отправителю уведомление-квитанцию о получении, зашифрованное на общем ключе и подписанное своей цифровой подписью. Для усложнения задачи нарушителя в уведомление целесообразно включить свой адрес, время приема последнего блока данных и случайное число, размер которого доводит бы объем уведомления до величины, приемлемой для обеспечения стойкости цифровой подписи к компрометации.

Возможны и другие алгоритмы идентификации и аутентификации, например Kerberos и стандарт X.509. За рубежом широкое распространение получил первый алгоритм. Однако специалисты отмечают его недостатки.

Для успешной работы Kerberos критически важны временные штампы. Время на машине-источнике и целевой машине должно быть точно согласованным, иначе возможен отказ в услуге законному пользователю. Это обстоятельство затрудняет его применение в региональных и глобальных сетях. Кроме того, требование к синхронизации означает, что необходимо защищать протоколы, которые устанавливают время, так чтобы нарушитель не мог установить время по своему желанию через этот механизм или просто нарушить работу системы. Основной задачей Kerberos является аутентификация пользователя в системе «клиент-сервер». Kerberos не является системой обращения равных с равным, предназначенной для использования связи одного компьютера с другим. В этой системе билеты разрешения допуска базируются на системном адресе идентификации личности. В системах со многими адресами и сетевыми интерфейсами это может вызвать проблему, поскольку билет действителен для одного из этих интерфейсов.

Kerberos применяет при передаче любой управляющей информации в сети сложную систему многократного шифрования с использованием комплекса секретных ключей, что не отвечает требованиям простоты защиты, усложняет работу администратора безопасности и поиск причины конфликтных ситуаций и отказов системы.

Выбор того или иного алгоритма аутентификации зависит от требований к безопасности информации в конкретной автоматизированной системе. Для надежной аутентификации обычно используется несколько признаков доказывающего в целях защиты от нескольких несанкционированных действий нарушителя, возможных при конкретной реализации системы из числа приведенных в табл. 3.4. Любой метод аутентификации предполагает некоторый уровень доверия между участниками протокола: проверяющим, доказывающим и центром управления и контроля за процессом.

Аутентификация осуществляется в локальной сети между пользователями, пользователями и сервером, в сложной локальной сети – между серверами и рабочими станциями, в региональной и глобальной сетях – при обмене

информацией между их абонентами: комплексами средств автоматизации, информационными вычислительными комплексами, абонентскими пунктами и их пользователями, а также с пользователями внешних сетей. Для высокой степени безопасности необходимы идентификация и аутентификация пользователей не только при их доступе из внешней сети во внутреннюю, но и наоборот.

5.5. Средства контроля и разграничения доступа

После того как объект аутентифицирован и подтверждена его подлинность, необходимо определить судьбу его сообщения и сферу его действия, доступные ему ресурсы и данные, т.е. его полномочия. Решение этих вопросов зависит от вида автоматизированной системы, элементом которой является аутентифицированный объект, полномочий объекта-получателя и содержания сообщения.

Если объект является пользователем локальной вычислительной сети, обротившимся к пользователю этой же сети, то в зависимости от ее принципов построения его полномочия реализует программа контроля и разграничения доступа рабочей станции пользователя-адресата либо сервера (см. разд. 4).

Если пользователь комплекса средств автоматизации (локальной вычислительной сети), являющегося(ейся) элементом региональной или глобальной автоматизированной системы, обратился в другой комплекс средств автоматизации (локальную вычислительную сеть), являющийся(юся) элементом этой же системы, то его аутентификацию и проверку полномочий осуществляет межсетевой экран, установленный на выходе первого комплекса. Если результат положительный, обращение через маршрутизатор согласно сетевому адресу направляется на второй комплекс (локальную вычислительную сеть). На его (ее) входе установлен другой экран, который осуществляет регистрацию, аутентификацию и проверку полномочий и других параметров обращения. При положительном результате оно пропускается согласно содержанию обращения на вычислительный комплекс, рабочую станцию или сервер, где также проверяется на подлинность и объем полномочий на доступ, после чего принимается в обработку.

5.6. Межсетевые экраны

5.6.1. Постановка задачи

При подключении любой закрытой компьютерной сети к открытым сетям, например к сети Интернет, высокую актуальность приобретают угрозы несанкционированного вторжения в закрытую сеть из открытой, а также угрозы

утечки информации из закрытой сети. Подобный вид угроз характерен также для случая, когда объединяются отдельные сети, ориентированные на обработку конфиденциальной информации совершенно разного уровня секретности или разных категорий важности. При ограничении доступа этих сетей друг к другу возникают угрозы нарушения установленных ограничений, а именно: угрозы неправомерного вторжения во внутреннюю сеть из внешней и угрозы несанкционированного доступа во внешнюю сеть из внутренней.

Неправомерное вторжение во внутреннюю сеть из внешней может выполняться как с целью несанкционированного использования информации внутренней сети, так и с целью нарушения работоспособности последней. Без соответствующих средств защиты вероятность успешной реализации данных угроз является достаточно высокой. Это связано с «врожденными» недостатками наиболее широко используемого для межсетевого взаимодействия набора протоколов TCP/IP. Ведь данный стек протоколов изначально был разработан для глобальной сети Интернет, которая создавалась как открытая система для свободного обмена информацией. В более ранних версиях, а также в текущей версии протокола IP (версии IPv4) не предусматривались какие-либо функции защиты от несанкционированных действий.

Угрозы несанкционированного доступа во внешнюю сеть из внутренней сети актуальны в случае ограничения разрешенного доступа во внешнюю сеть правилами, установленными в организации. Такое ограничение, что особенно характерно для взаимодействия с открытыми сетями, может потребоваться в следующих случаях:

- для предотвращения утечки конфиденциальных данных;
- при запрете доступа, например в учебных заведениях, к информации нецензурной и нежелательной направленности;
- в случае запрета служебного доступа к развлекательным компьютерным ресурсам в рабочее время.

Бороться с рассмотренными угрозами безопасности межсетевого взаимодействия средствами универсальных операционных систем (ОС) не представляется возможным. Универсальная операционная система – это слишком большой и сложный комплекс программ, который, с одной стороны, может содержать внутренние ошибки и недоработки, а с другой – не всегда обеспечивает защиту от ошибок администраторов и пользователей.

Современная технология программирования не позволяет сделать столь большие программы безопасными. Для операционных систем характерны как явные ошибки разработки, так и существенные недостатки, связанные с недоработкой концептуальных и ряда детальных требований к системе безопасности. Кроме того, администратор, имеющий дело со сложной системой, далеко не всегда в состоянии эффективно ее настроить и сконфигурировать. Наконец, в универсальной многопользовательской системе брешы в безопасности постоянно создаются самими пользователями (например, тривиальные и редко изменяемые пароли).

Следует учитывать также неоднородность современных компьютерных сетей. Сеть любой организации в общем случае представляет собой неоднородный набор из различных компьютеров, управляемых различными операционными системами и связанных между собой с помощью сетевого оборудо-

ования. Компьютеры одного типа и с одной ОС могут в соответствии с их назначением иметь совершенно разные конфигурации. В таких условиях проблематично осуществить надежную защиту каждого компьютера в отдельности от несанкционированного доступа к информации и ресурсам со стороны внешней сети.

Поэтому проблема защиты от несанкционированных действий при взаимодействии с внешними сетями успешно может быть решена только с помощью специализированных программно-аппаратных комплексов. Такие комплексы называют межсетевыми экранами, брандмауэрами или системами FireWall. Межсетевой экран устанавливается на стыке между внутренней и внешней сетями и функции противодействия несанкционированному межсетевому доступу берет на себя. Автоматизированная система обработки информации может включать в себя комплексы средств автоматизации с сосредоточенной обработкой данных и несколько вычислительных сетей, использующих незащищенные линии и каналы связи. Поэтому экраны устанавливаются также и на стыках внутренних сетей, а в некоторых случаях на входах указанных комплексов. Для краткого описания межсетевого экранирования воспользуемся материалами [28].

5.6.2. Функции межсетевого экранирования

Межсетевой экран должен учитывать протоколы информационного обмена, положенные в основу функционирования внутренней и внешней сетей. Если эти протоколы отличаются, то брандмауэр должен поддерживать многопротокольный режим работы, обеспечивая протокольное преобразование отличающихся по реализации уровней модели OSI для объединяемых сетей. Чаще всего возникает необходимость в совместной поддержке стеков протоколов SPX/IPX и TCP/IP. Схема подключения экрана приведена на рис. 5.10.

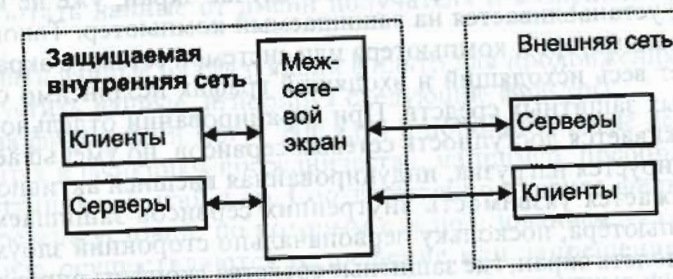


Рис. 5.10. Схема подключения межсетевого экрана

Брандмауэр не является симметричным. Для него отдельно задаются правила, ограничивающие доступ из внутренней сети во внешнюю сеть и наоборот. В общем случае работа межсетевого экрана основана на динамическом выполнении двух групп функций: фильтрации проходящих через него информационных потоков и посредничества при реализации межсетевых взаимодействий.

В зависимости от типа экрана эти функции могут выполняться с различной полнотой. Простые межсетевые экраны ориентированы на выполнение только одной из данных функций. Комплексные экраны обеспечивают совместное выполнение указанных функций защиты.

Чтобы эффективно обеспечивать безопасность сети, комплексный брандмауэр обязан управлять всем потоком, проходящим через него, и отслеживать свое состояние. Для принятия управляющих решений по используемым сервисам межсетевой экран должен получать, запоминать, выбирать и обрабатывать информацию, полученную от всех коммуникационных уровней и от других приложений. Недостаточно просто проверять пакеты по отдельности. Информация о состоянии соединения, полученная из инспекции соединений в прошлом и других приложений, — главный фактор в принятии управляющего решения при попытке установления нового соединения. Для принятия решения могут учитываться как состояние соединения (полученное из прошлого потока данных), так и состояние приложения (полученное из других приложений). Полнота и правильность управления требуют, чтобы комплексный брандмауэр имел возможность анализа и использования следующих элементов:

- **информации о соединениях** — информации от всех семи уровней в пакете;
- **истории соединений** — информации, полученной от предыдущих соединений. Например, исходящая команда PORT сессии FTP должна быть сохранена для того, чтобы в дальнейшем можно было проверить входящее соединение FTP data;
- **состояния уровня приложения** — информации о состоянии, полученной из других приложений. Например, аутентифицированному до настоящего момента пользователю можно предоставить доступ через брандмауэр только для авторизованных видов сервиса;
- **агрегирующих элементов** — вычислений разнообразных выражений, основанных на всех вышеперечисленных факторах.

Устройство, подобное межсетевому экрану, может использоваться и для защиты отдельного компьютера. В этом случае экран, уже не являющийся межсетевым, устанавливается на защищаемый компьютер. Такой экран, называемый брандмауэром компьютера или системой сетевого экранирования, контролирует весь исходящий и входящий трафик независимо от всех прочих системных защитных средств. При экранировании отдельного компьютера поддерживается доступность сетевых сервисов, но уменьшается или вообще ликвидируется нагрузка, индуцированная внешней активностью. В результате снижается уязвимость внутренних сервисов защищаемого таким образом компьютера, поскольку первоначально сторонний злоумышленник должен преодолеть экран, где защитные средства сконфигурированы особенно тщательно и жестко [28].

5.6.3. Фильтрация трафика

Фильтрация информационных потоков состоит в их выборочном пропуске через экран, возможно, с выполнением некоторых преобразований и извещением отправителя о том, что его данным в пропуске отказано. Филт-

рация осуществляется на основе набора правил, предварительно загруженных в экран и являющихся выражением сетевых аспектов принятой политики безопасности. Поэтому межсетевой экран удобно представлять как последовательность фильтров (рис. 5.11), обрабатывающих информационный поток.

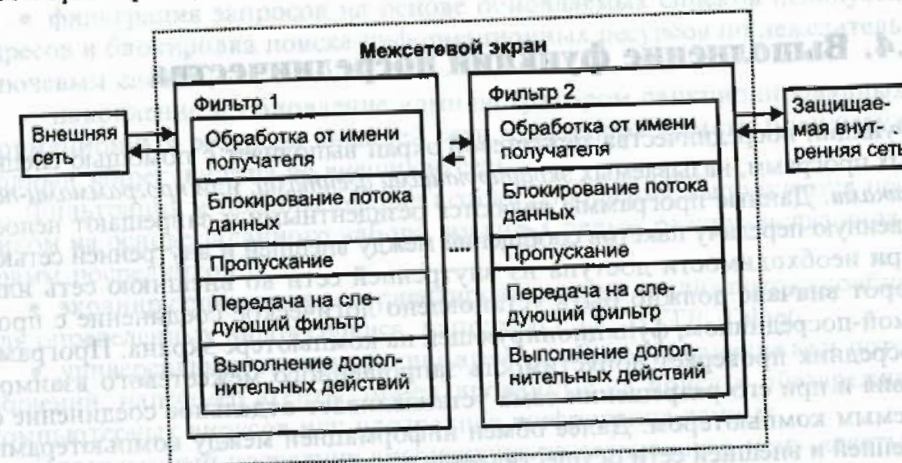


Рис. 5.11. Структура межсетевого экрана

Каждый из фильтров предназначен для интерпретации отдельных правил фильтрации путем выполнения следующих стадий:

- 1) анализа информации по заданным в интерпретируемых правилах критериям, например по адресам получателя и отправителя или по типу приложения, для которого эта информация предназначена;
- 2) принятия на основе интерпретируемых правил одного из следующих решений:
 - не пропустить данные;
 - обработать данные от имени получателя и вернуть результат отправителю;
 - передать данные на следующий фильтр для продолжения анализа;
 - пропустить данные, игнорируя следующие фильтры.

Правила фильтрации могут задавать и дополнительные действия, которые относятся к функциям посредничества, например преобразование данных, регистрация событий и др. Соответственно правила фильтрации определяют перечень условий, по которым с использованием указанных критериев анализа осуществляются разрешение или запрещение дальнейшей передачи данных и выполнение дополнительных защитных функций.

В качестве критериев анализа информационного потока могут использоваться следующие параметры:

- служебные поля пакетов сообщений, содержащие сетевые адреса, идентификаторы, адреса интерфейсов, номера портов и другие значимые данные;
- непосредственное содержимое пакетов сообщений, проверяемое, например, на наличие компьютерных вирусов;
- внешние характеристики потока информации, например временные, частотные характеристики, объем данных и т.д.

Используемые критерии анализа зависят от уровней модели OSI, на которых осуществляется фильтрация. В общем случае, чем выше уровень модели OSI, на котором брандмауэр фильтрует пакеты, тем выше и обеспечиваемый им уровень защиты [28].

5.6.4. Выполнение функций посредничества

Функции посредничества межсетевой экран выполняет с помощью специальных программ, называемых *экранирующими агентами*, или *программами-посредниками*. Данные программы являются резидентными и запрещают непосредственную передачу пакетов сообщений между внешней и внутренней сетью.

При необходимости доступа из внутренней сети во внешнюю сеть или наоборот вначале должно быть установлено логическое соединение с программой-посредником, функционирующей на компьютере экрана. Программа-посредник проверяет допустимость запрошенного межсетевого взаимодействия и при его разрешении сама устанавливает отдельное соединение с требуемым компьютером. Далее обмен информацией между компьютерами внутренней и внешней сети осуществляется через программного посредника, который может выполнять фильтрацию потока сообщений, а также осуществлять другие защитные функции.

Следует уяснить, что функции фильтрации межсетевой экран может выполнять без применения программ-посредников, обеспечивая прозрачное взаимодействие между внутренней и внешней сетью. Вместе с тем программные посредники могут и не осуществлять фильтрацию потока сообщений.

В общем случае экранирующие агенты, блокируя прозрачную передачу потока сообщений, могут выполнять следующие функции:

- идентификацию и аутентификацию пользователей;
- проверку подлинности передаваемых данных;
- разграничение доступа к ресурсам внутренней сети;
- разграничение доступа к ресурсам внешней сети;
- фильтрацию и преобразование потока сообщений, например динамический поиск вирусов и прозрачное шифрование информации;
- трансляцию внутренних сетевых адресов для исходящих пакетов сообщений;
- регистрацию событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и генерацию отчетов;
- кэширование данных, запрашиваемых из внешней сети.

Программы-посредники могут осуществлять *проверку подлинности получаемых и передаваемых данных*. Это актуально не только для аутентификации электронных сообщений, но и мигрирующих программ (Java, ActiveX Controls), по отношению к которым может быть выполнен подлог. Проверка подлинности сообщений и программ заключается в контроле их цифровых подписей.

Идентификация и аутентификация пользователей при обращении к межсетевому экрану позволяют *разграничить их доступ к ресурсам внутренней или внешней сети*. Способы разграничения к ресурсам внутренней сети ни-

чем не отличаются от способов разграничения, поддерживаемых на уровне операционной системы. При разграничении доступа к ресурсам внешней сети чаще всего используется один из следующих критериев отбора:

- разрешение доступа только по заданным адресам во внешней сети;
- фильтрация запросов на основе обновляемых списков недопустимых адресов и блокировка поиска информационных ресурсов по нежелательным ключевым словам;
- накопление и обновление администратором санкционированных информационных ресурсов внешней сети в дисковой памяти брандмауэра и полный запрет доступа во внешнюю сеть.

Фильтрация и преобразование потока сообщений выполняются посредником на основе заданного набора правил. Следует различать два вида программ посредников:

- экранирующие агенты, ориентированные на анализ потока сообщений для определенных видов сервиса, например FTP, HTTP, Telnet;
- универсальные экранирующие агенты, обрабатывающие весь поток сообщений, например агенты, ориентированные на поиск и обезвреживание компьютерных вирусов или прозрачное шифрование данных.

Программный посредник анализирует поступающие к нему пакеты данных, и если какой-либо объект не соответствует заданным критериям, то посредник либо блокирует его дальнейшее продвижение, либо выполняет соответствующие преобразования, например обезвреживание обнаруженных компьютерных вирусов. При анализе содержимого пакетов важно, чтобы экранирующий агент мог автоматически распаковывать проходящие файловые архивы.

Брандмауэры с посредниками позволяют также организовывать защищенные виртуальные сети (*Virtual Private Network – VPN*), например, безопасно объединить несколько локальных сетей, подключенных к Интернету, в одну виртуальную сеть. VPN обеспечивают прозрачное для пользователей соединение локальных сетей, сохраняя секретность и целостность передаваемой информации путем ее динамического шифрования. При передаче по Интернету возможно шифрование не только данных пользователей, но и служебной информации – конечных сетевых адресов, номеров портов и т.д.

Программы-посредники могут выполнять и такую важную функцию, как трансляция внутренних сетевых адресов. Данная функция реализуется по отношению ко всем пакетам, следующим из внутренней сети во внешнюю. Для этих пакетов посредник выполняет автоматическое преобразование IP-адресов компьютеров-отправителей в один надежный IP-адрес, ассоциируемый с брандмауэром, из которого передаются пакеты оказываются отправленными межсетевым экраном, что исключает прямой контакт между авторизованной внутренней сетью и являющейся потенциально опасной внешней сетью. IP-адрес брандмауэра становится единственным активным IP-адресом, который попадает во внешнюю сеть.

При таком подходе топология внутренней сети скрыта от внешних пользователей, что усложняет задачу несанкционированного доступа. Кроме повышения безопасности, трансляция адресов позволяет иметь внутри сети соб-

ственную систему адресации, не согласованную с адресацией во внешней сети, например в сети Интернет. Это эффективно решает проблему расширения адресного пространства внутренней сети и дефицита адресов внешней сети.

Важными функциями программ-посредников являются регистрация событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и составление отчетов. В качестве обязательной реакции на обнаружение попыток выполнения несанкционированных действий должно быть определено уведомление администратора, т.е. выдача предупредительных сигналов. Любой брандмауэр, который не способен посылать предупредительные сигналы при обнаружении нападения, не является эффективным средством межсетевой защиты.

Многие межсетевые экраны содержат мощную систему регистрации, сбора и анализа статистики. Учет может вестись по адресам клиента и сервера, идентификаторам пользователей, времени сеансов, времени соединений, количеству переданных/принятых данных, действиям администратора и пользователей. Системы учета позволяют произвести анализ статистики и предоставляют администраторам подробные отчеты. За счет использования специальных протоколов посредники могут выполнить удаленное оповещение об определенных событиях в режиме реального времени.

С помощью специальных посредников поддерживается также кэширование данных, запрашиваемых из внешней сети. При доступе пользователей внутренней сети к информационным ресурсам внешней сети вся информация накапливается на пространстве жесткого диска брандмауэра, называемого в этом случае **прокси-сервером**. Поэтому, если при очередном запросе нужна информация окажется на прокси-сервере, то посредник предоставляет ее без обращения к внешней сети, что существенно ускоряет доступ. Администратору следует позаботиться только о периодическом обновлении содержимого прокси-сервера.

Функция кэширования успешно может использоваться для ограничения доступа к информационным ресурсам внешней сети. В этом случае все санкционированные информационные ресурсы внешней сети накапливаются и обновляются администратором на прокси-сервере. Пользователям внутренней сети разрешается доступ только к информационным ресурсам прокси-сервера, а непосредственный доступ к ресурсам внешней сети запрещается.

Экранирующие агенты намного надежнее обычных фильтров и обеспечивают большую степень защиты. Однако они снижают производительность обмена данными между внутренней и внешней сетями и не обладают той степенью прозрачности для приложений и конечных пользователей, которая характерна для простых фильтров [28].

5.7. Средства защиты трафика

В глобальных автоматизированных системах защита сетевого трафика (потока сообщений) от наблюдения осуществляется специальными средствами, имитирующими по сети передачи данных передачу информации при от-

сутствии штатных сообщений. Если применяется линейное шифрование, то между узлами сети устанавливается непрерывный поток битов зашифрованного текста. Если каналы связи используются несколькими соединениями, линейное шифрование скрывает адреса источника и получателя информации. В случае применения абонентского шифрования строится искусственный трафик с использованием «пустых» сообщений различной длины. При этом в сообщение вводятся скрытые признаки, известные только получателю. В локальной сети для этой цели также применяется шифрование пакетов канального уровня.

5.8. Особенности защиты информации в базах данных

Базы данных рассматриваются как надежное хранилище структурированных данных, снабженное специальным механизмом для их эффективного использования в интересах пользователей (процессов). Таким механизмом является система управления базой данных (СУБД). Под **системой управления базой данных** понимаются программные или аппаратно-программные средства, реализующие функции управления данными, такие как просмотр, сортировка, выборка, модификация, выполнение операций определения статистических характеристик и т.п. Базы данных размещаются:

- на автоматизированном рабочем месте или рабочей станции пользователя;
- на информационном вычислительном комплексе;
- на специально выделенной ЭВМ (сервере).

Как правило, на компьютерной системе пользователя размещаются личные или персональные базы данных, которые обслуживают процессы одного пользователя.

В вычислительных сетях базы данных размещаются на серверах. В локальных и корпоративных сетях, как правило, используются централизованные базы данных. Общедоступные глобальные сети имеют распределенные базы данных. В таких сетях серверы размещаются на различных объектах сети. В качестве серверов часто используются специализированные ЭВМ, приспособленные к хранению больших объемов данных, обеспечивающие сохранность и доступность информации, а также оперативность обработки поступающих запросов. В централизованных базах данных проще решаются проблемы защиты информации от преднамеренных угроз, поддержания актуальности и непротиворечивости данных. Достоинством распределенных баз данных при условии дублирования данных является их высокая защищенность от стихийных бедствий, аварий, сбоев технических средств, а также диверсий.

Защита информации в базах данных в отличие от защиты данных в файлах имеет и свои особенности:

- выбор механизмов защиты с учетом принципов построения базы данных и системы управления базой данных;

• разграничение доступа к информации, как правило, реализуется не на уровне файлов, а на уровне частей баз данных.

При создании средств защиты информации в базах данных необходимо учитывать их взаимодействие не только с ОС, но и с СУБД. При этом возможно встраивание механизмов защиты в СУБД или использование их в виде отдельных компонентов. Для большинства СУБД придание им дополнительных функций возможно только на этапе разработки СУБД.

В современных базах данных довольно успешно решаются задачи разграничения доступа, поддержания физической целостности и логической сохранности данных. Алгоритмы разграничения доступа к записям и даже к полям записей в соответствии с полномочиями пользователя хорошо отработаны. Разграничение доступа к файлам баз данных и к частям баз данных осуществляется СУБД путем установления полномочий пользователей и контроля этих полномочий при допуске к объектам доступа.

Полномочия пользователей устанавливаются администратором СУБД. Обычно стандартным идентификатором пользователя является пароль, передаваемый в зашифрованном виде. 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 базах данных, работающих с конфиденциальной информацией, необходимо дополнительно использовать криптографические средства закрытия информации. Для этой цели используется шифрование как с помощью единого ключа, так и с помощью индивидуальных ключей пользователей. Применение шифрования с индивидуальными ключами повышает надежность механизма разграничения доступа, но существенно усложняет управление.

Возможны два режима работы с зашифрованными базами данных. Наиболее простым является такой порядок работы с закрытыми данными, при котором для выполнения запроса необходимый файл или часть файла расшифровывается на внешнем носителе, с открытой информацией производятся необходимые действия, после чего информация на ВЗУ снова зашифровывается. Достоинством такого режима является независимость функционирования средств шифрования и СУБД, которые работают последовательно друг за другом. В то же время сбой или отказ в системе может привести к тому, что на ВЗУ часть базы данных останется записанной в открытом виде.

Второй режим предполагает возможность выполнения СУБД запросов пользователей без расшифровывания информации на ВЗУ. Поиск необходимых файлов, записей, полей, групп полей не требует расшифровывания. Оно производится в оперативной памяти непосредственно перед выполнением конкретных действий с данными. Такой режим возможен, если процедуры шифрования встроены в СУБД. При этом достигается высокий уровень за-

щиты 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 разграничении доступа и распределении полномочий пользователей необходимо учитывать ряд специфических угроз безопасности информации, связанных с концентрацией в базах данных большого количества разнообразной информации, а также с возможностью использования сложных запросов обработки данных. К таким угрозам относятся:

- инференция;
- агрегирование;
- комбинирование 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, как, 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 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 базами данных. Использование сложных, а также последовательности простых логически связанных запросов позволяет получать данные, к которым доступ пользователю закрыт. Такая возможность имеется прежде всего в базах данных, позволяющих получать статистические данные. При этом отдельные записи, поля (индивидуальные данные) являются закрытыми. В результате запроса, в котором могут использоваться логические операции AND, OR, NOT, пользователь может получить такие величины, как количество записей, сумма, максимальное или минимальное значение. Используя сложные перекрестные запросы и имеющуюся в его распоряжении дополнительную информацию об особенностях интересующей записи (поля), нарушитель путем последовательной фильтрации записей может получить доступ к нужной записи (полю).

Противодействие подобным угрозам осуществляется следующими методами:

- блокировкой ответа при неправильном числе запросов;
- искажением ответа путем округления и другой преднамеренной коррекции данных;
- разделением баз данных;
- случайным выбором записи для обработки;
- контекстно-ориентированной защитой;
- контролем 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 нарушитель сможет выявить некоторые данные, то он не сможет определить, к какой конкретно записи они относятся.

Применяется также метод *разделения баз данных* на группы. В каждую группу может быть включено не более определенного числа записей. Запросы разрешены к любому множеству групп, но запрещаются к подмножеству записей из одной группы. Применение этого метода ограничивает возможности выделения данных нарушителем на уровне не ниже группы записей. Метод разделения баз данных не нашел широкого применения из-за сложности получения статистических данных, обновления и реструктуризации данных.

Эффективным методом противодействия исследованию баз данных является метод *случайного выбора записей* для статистической обработки. Такая организация выбора записей не позволяет нарушителю проследить множество запросов.

Сущность *контекстно-ориентированной защиты* заключается в назначении атрибутов доступа (чтение, вставка, удаление, обновление, управление и т.д.) элементам базы данных (записям, полям, группам полей) в зависимости от предыдущих запросов пользователя. Например, пусть пользователю доступны в отдельных запросах поля: «идентификационные номера» и «фамилии сотрудников», а также «идентификационные номера» и «размер заработной платы». Сопоставив ответы по этим запросам, нарушитель может получить закрытую информацию о заработной плате конкретных работников. Для исключения такой возможности пользователю следует запретить доступ к полю «идентификатор сотрудника» во втором запросе, если он уже выполнил первый запрос.

Одним из наиболее эффективных методов защиты информации в базах данных является *контроль поступающих запросов* на наличие «подозритель-

ных» запросов или комбинации запросов. Анализ подобных попыток позволяет выявить возможные каналы получения несанкционированного доступа к закрытым данным [27].

В настоящее время СУБД со встроенной системой контроля и разграничения доступа выпускаются в виде отдельных программных продуктов. При этом она называется «защищенной». Этому заявлению не следует доверять. Об этом можно говорить лишь после того, как данная СУБД будет установлена в автоматизированную систему, согласована с ее базой данных и системой защиты информации, исследована, проверена на предмет наличия возможных путей обхода защиты и произведен анализ прочности защиты на соответствие заданному уровню.

МЕТОД ПОСТРОЕНИЯ СИСТЕМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ РАБОЧЕЙ СТАНЦИИ, ЛВС, ГЛОБАЛЬНОЙ СЕТИ И АСУ

6

6.1. Построение системы безопасности информации рабочей станции

6.1.1. Рабочая станция как объект обработки и защиты информации

Рабочей станцией согласно определению, приведенному во введении, называется автоматизированная система, состоящая из персональной ЭВМ, сетевого программно-аппаратного и прикладного программного обеспечения, которая является элементом вычислительной сети.

Типовой состав устройств персонального компьютера (ПК): системный блок обработки и управления, средства взаимодействия пользователей с системным блоком, средства долговременного хранения и накопления данных, средства подключения к линиям связи.

Системный блок, включающий центральный процессор, основную память (ОЗУ и КЭШ), контроллеры и адаптер канала связи, строится на основе микропроцессорных комплектов БИС, БИС ОЗУ и ПЗУ. ОЗУ ПК являются энергозависимыми ЗУ, у которых информация разрушается при отключении питания. Информация, размещаемая в ПЗУ, записывается при изготовлении ПК и не изменяется в течение всего периода ее эксплуатации. В ПЗУ обычно размещаются системные программы, обеспечивающие подготовку ПЭВМ к работе после включения питания, т.е. инициализацию (приведение в исходное состояние функциональных модулей), тестирование (проверка работоспособности функциональных модулей) и загрузку операционной системы.

Средства взаимодействия пользователей с системным блоком обработки и управления включают клавишное устройство, печатающее устройство (принтер), устройство отображения информации на ЭЛТ (монитор). Кроме того, в качестве устройств ввода-вывода информации, подключаемых к системному блоку, используются:

- манипулятор «мышь» для ввода информации;
- плоттер – устройство для вывода рисунков и другой графической информации на бумагу;

- графопостроитель – устройство для вывода чертежей на бумагу;
- сканер – устройство для считывания графической и текстовой информации в компьютер;
- стриммер – устройство для быстрого сохранения всей информации, находящейся на жестком диске. Стриммер записывает информацию на кассеты с магнитной лентой.

Средства долговременного хранения и накопления данных (внешние запоминающие устройства) обеспечивают запись и чтение больших массивов информации (тексты программ на языках высокого уровня, программы в машинных кодах, файлы с данными и т.д.). В качестве внешних запоминающих устройств в ПК в основном используются накопители на гибких магнитных дисках (НГМД) и накопители на жестких магнитных дисках (НМД) типа «винчестер». Сейчас для энергонезависимого хранения программ и данных применяются накопители на магнитооптических дисках. При этом используются оптические дисководы и диски двух типов: только для чтения и средства, позволяющие как чтение, так и запись информации.

Гибкие диски (дискеты) позволяют переносить документы и программы с одного компьютера на другой, хранить информацию, не используемую постоянно, делать архивные копии информации, содержащейся на жестком диске. Чаще всего используются дискеты 3,5 дюйма емкостью 1,44 Мбайта.

Накопители на жестком диске (винчестеры) предназначены для постоянного хранения информации, используемой при работе с компьютером: программ операционной системы, части используемых пакетов программ, редакторов документов, трансляторов с языков программирования и т.д. Программное обеспечение ПК включает систему программирования, операционную систему и пакеты прикладных программ. Основой программного обеспечения является операционная система, с помощью которой достигается взаимодействие пользователя с аппаратными средствами ПК.

Системы программирования служат инструментальным средством, с их помощью пользователи создают программы решения задач на ПК. Система программирования включает в свой состав средства написания программ, преобразования их к виду, пригодному для выполнения на ПК, контроля и отладки программ. Данные средства в готовой АС применяться не должны.

Наиболее распространены в ПК операционная система Windows и UNIX – подобные операционные системы.

Операционная система выполняет следующие функции:

- обеспечивает связь между пользователем и компьютером, создавая специальную среду общения человека с компьютером (интерфейс);
- является базовым программным обеспечением, на основе которого могут работать многочисленные прикладные программы, такие, как текстовые редакторы, электронные таблицы, базы данных и др.;
- предоставляет ряд служебных программ, обслуживающих систему, управляющих аппаратными компонентами и устройствами: памятью компьютера, периферией, устройствами ввода и вывода данных и т.п.;
- организует взаимодействие с файлами, папками и дисками.

Первой операционной системой, разработанной для IBM-совместимых персональных компьютеров, была DOS (Disk Operating System – дисковая операционная система). Наиболее распространенной системой такого типа является MS DOS фирмы Microsoft. На своих ПК фирма IBM устанавливала аналогичную операционную систему собственного производства – PC DOS. Для любителей альтернативных решений фирма Digital Research предлагала ОС DR DOS. Различия между этими операционными системами не были существенными. Затем наступила «эра Windows».

Вплоть до версии Windows 3.1/3.11 это была не операционная система в том смысле, который придают данному понятию, а всего лишь графическая оболочка, надстройка над ОС MS DOS. Полноценной операционной системой Windows стала, начиная с четвертой версии, с Windows 95. Все последующие версии Windows (и Windows 98, и Windows Me, и Windows NT, и Windows 2000) – это операционные системы.

Корпорация Microsoft развивает также линию операционных систем Windows NT (NT – от New Technology), предназначенных в основном для использования в сфере бизнеса. Это – и серверные варианты операционной системы, и те, которые устанавливаются на пользовательских компьютерах (на рабочих станциях). Несколько уступая Windows 95/98 в удобстве (не поддерживается технология Plug&Play) и имея худшую совместимость со старыми программами, Windows NT обладает высокой устойчивостью, может эффективно управлять локальными сетями.

Программисты корпорации Microsoft планировали разработать такую операционную систему (на эту роль определяли Windows 2000), которая одновременно заменила бы и Windows 95/98, и Windows NT. Однако этого не случилось. Различие подходов к использованию компьютеров в сфере бизнеса и в быту ощутимо, и пока эволюция операционных систем идет двумя потоками. На рубеже веков на арену практически одновременно вышли две операционные системы:

Microsoft Windows 2000 Professional (далее Windows 2000) и Microsoft Windows Millennium Edition (называемая также Windows Me). Обе системы – и Windows 2000, и Windows Me – внешне подобны, им свойственны однотипные приемы работы. Однако имеются и специфические отличия, которые делают Windows 2000 оптимальной для бизнеса, а Windows Me – для домашнего использования. Корпорация Microsoft так и рекомендует: бизнес-пользователям приобретать Windows 2000, а в домашних условиях устанавливать Windows Me.

Windows NT в соответствии с требованиями безопасности C2 предусматривает наличие следующих функций:

- защищенный вход в систему. Обязательная регистрация пользователя с указанием имени и пароля;
- дискреционный контроль за доступом. Владелец ресурса (например, каталога) должен сам определять круг пользователей, которые могут обращаться к нему, и назначать уровень их доступа;
- ревизия системы. Это способность операционной системы обнаруживать и регистрировать события безопасности, чтобы выявить возможные попытки взлома защиты и противодействовать им;

- защита памяти. Защита памяти предотвращает несанкционированный доступ процесса к данным другого и обеспечивает полную очистку памяти перед ее повторным использованием.

По данным Р. Франклина Смита (www.kiev-security.org.ru), многие функции Windows 2000 имеют прямое отношение к системе безопасности, учитывая наличие в составе этой ОС таких компонентов, как Kerberos, Aktiv Directory (AD) и встроенной поддержки шифрования по открытому ключу (PKI). Ядро системы безопасности Windows 2000 по-прежнему базируется на инфраструктуре Windows NT 4.0.

Хотя в Windows NT 4.0 система безопасности считалась достаточно надежной, администраторы, которые устанавливали NT как систему уровня предприятия, обнаружили в ней ряд недостатков. Например, без подключения программных надстроек нельзя было реализовать распределенную систему поддержки однократного входа в сеть (SSO), уязвимым местом в системе защиты стала обратная совместимость с LAN Manager, функции NT PKI интегрированы в операционную систему не полностью и т.д.

В Windows 2000 заметно усовершенствована система безопасности. Для замены уязвимой сетевой аутентификации NT LAN Manager добавлен протокол Kerberos; для снижения уровня риска, связанного с парольной защитой, можно применять PKI и смарт-карты при использовании закрытого ключа. Для защиты от физического доступа к жесткому диску реализована технология шифрования данных на диске Encrypting File System. Усовершенствованы также и другие функции.

Сегодня весомой альтернативой системе Windows является семейство операционных систем UNIX и в первую очередь яркие представители этого небольшого сообщества: ОС Linux и ОС FreeBSD¹.

Надо заметить, что для персональных компьютеров UNIX-подобные системы появились сравнительно недавно, хотя возраст ОС UNIX – более 20 лет. Дело в том, что долгие годы платформой для их работы в основном служили «большие» вычислительные системы. И только в последние годы началось бурное развитие версий ОС UNIX для ПК. В настоящее время ситуация такова, что версии UNIX для персональных компьютеров характеризуются многофункциональностью, защищенностью от чуждого вмешательства, естественной сочетаемостью с Интернет-сетями, масштабируемостью (масштабным переносом основных характеристик системы на аппаратные комплексы иных размеров). К тому же нынче UNIX-системы дополняются мощными интегрированными графическими оболочками, офисными пакетами, приложениями для работы с графикой и Интернетом, файловым проводником, архиваторами и другими программами, приспособленными для использования в офисах. Почему же применение UNIX там пока весьма ограниченное? – Потому что есть Windows, и все привыкли работать под Windows. Пока операционные системы корпорации Microsoft лидируют по популярности.

Сегодня большинство серверов в Интернете работают под управлением ОС UNIX, а архитектура Интернета и идеология UNIX неплохо сочетаются.

¹ См.: Новиков А., Черепанов А. Персональные компьютеры, аппаратура, системы, Интернет: Учеб. курс. – СПб.: Питер, 2001.

UNIX-системы традиционно сильны в качестве серверов служб Интернета, в качестве систем защиты локальных сетей от вмешательства извне (брандмауэров). И если преимущества UNIX-систем перед Windows при оборудовании офисных рабочих станций в настоящее время пока мало ощутимы, то достоинства UNIX при построении Интернет-серверов любого уровня неоспоримы.

Система UNIX разработана в подразделении Computing Science Research Group фирмы Bell Labs в штате Нью-Джерси в США. Широкое распространение ОС UNIX получила с 1974 г. после описания этой системы Томпсоном и Ритчи. Ею заинтересовались и начали во многих местах устанавливать. Особенно быстро UNIX распространилась по ведущим университетам, поскольку им она доставалась бесплатно. Но, что особенно важно, к системе прилагался исходный программный код. Это позволяло устанавливать UNIX на разных аппаратных платформах, а также постоянно модифицировать и улучшать компоненты системы, разрабатывать новые версии. Именно поэтому расплодилось великое множество версий UNIX-систем, приспособленных под самые изощренные аппаратные решения. А вот широкое наступление UNIX на персональные компьютеры началось сравнительно недавно – в начале 90-х гг. XX в., одновременно с появлением компьютеров на базе процессора Intel 386. Данный процессор обеспечивал функционирование многозадачных защищенных операционных систем, и это обстоятельство стимулировало разработку версий ОС UNIX, ориентированных на ПК. Персональные компьютеры дешевели, быстро и широко распространялись. Нашлось немало способных энтузиастов программирования, которые, воспользовавшись открытостью спецификаций на UNIX-системы, начали разрабатывать на базе программных кодов UNIX свои собственные оболочки и системы. Так, в частности, появилась знаменитая ОС Linux.

Примечание. Версии UNIX по-прежнему успешно работают на самых больших ЭВМ. Например, ОС AIX корпорации IBM поддерживает работу мощных современных мейнфреймов – гигантских многопроцессорных компьютеров.

Итак, различных модификаций UNIX-систем (их еще называют «клонами») много. Сегодня понятие «UNIX» стало собирательным для множества родственно близких операционных систем, отвечающих основным принципам идеологии UNIX. Под ОС UNIX нередко подразумевают не столько конкретную ОС, сколько все семейство идеологически родственных операционных систем.

Любой представитель семейства UNIX, предназначенный для использования на персональном компьютере, – это многозадачная защищенная многопользовательская сетевая операционная система. Перечисленные свойства были заложены в нее еще на раннем этапе становления и благополучно перенесли на те современные варианты UNIX, которые сегодня применяют на персональных компьютерах.

Основополагающие принципы ОС UNIX:

1. Система предназначена для одновременной коллективной работы пользователей. При этом каждый вошедший в систему чувствует себя «комфортно», не ощущая присутствия других в системе (если только речь не идет о коллективной работе). Пользователь сам назначает права доступа к своим каталогам и файлам.

2. При каждом входе в систему необходимо проходить обязательную процедуру авторизации – называть себя заранее обусловленным именем и вводить пароль.

3. Файловая система ОС UNIX имеет строгие разграничения прав на доступ к файлам и каталогам. Ей присущ жестко задаваемый порядок расположения файлов в файловой системе, который согласован с уровнями привилегий.

4. Система решает пользовательские и системные задачи одновременно. При этом пользователю предоставляется возможность запускать параллельно несколько задач и взаимодействовать с теми устройствами, доступ к которым разрешен администратором.

5. В ОС UNIX системные процессы строго отделены от пользовательских. Это важная предпосылка надежной и безотказной работы. Как бы ни вел себя пользователь в системе, он не получит эксклюзивный доступ к аппаратным ресурсам, не сможет инициировать сбой системы.

6. ОС UNIX допускает работу через Интернет и телефонные каналы в терминальном режиме на далеких UNIX-компьютерах, в том числе можно их администрировать: перезапускать систему, настраивать конфигурацию, устранять сбои. Системный администратор может с одного компьютера администрировать сразу несколько далеких машин.

Все перечисленные позиции реализуются и на персональном компьютере, управляемом ОС UNIX. Действительно, можно представить, что ОС UNIX формирует на ПК сложный комплекс. Он представляет собой одновременно и вычислительную машину (сам ПК), и терминалы, которые расположены и тут же, на этом же персональном компьютере. Получается, будто разработчики просто «собрали» весь описанный выше вычислительный комплекс на одной машине – персональном компьютере.

Многие черты ОС UNIX из тех, которые проявляются на «больших» машинах, здесь сохранились. Сохранилась также возможность захода в персональный UNIX-компьютер и с удаленных терминалов, и с других компьютеров издалека: через Интернет, последовательный порт, модем.

Персональный компьютер (ПК) по составу аппаратных и программных средств, а также по принятой классификации можно отнести к разряду малогабаритных комплексов средств автоматизации, поэтому на нее можно распространить тот же подход. С позиций защиты информации ПК как автономная система имеет такой же состав типовых средств ввода-вывода, обработки и хранения информации, как и КСА, описанный в подразд. 3.5.

Особенностью ПК с позиций защиты является его конструкция, программные средства и стоимость.

Конструкция ПК рассчитана на работу в одно время только одного пользователя. Масса и габаритные размеры этой вычислительной системы таковы, что ее можно разместить в небольшом металлическом шкафу. Благодаря своему назначению, стоимости и конструкции ПК может использоваться только одним пользователем. А сокращение количества пользователей уменьшает и количество потенциальных нарушителей.

Программное обеспечение персонального компьютера дает возможность изменять и разрабатывать любые программы, что является одновременно и большим достоинством системы, и недостатком с позиций защиты обрабатываемой на ней информации. Здесь два требования вступают в противоречие.

Во-первых, ПК отличается полной доступностью всех ресурсов машины. Например, адресуется вся оперативная память, включая области, используемые системой. Пользователь может свободно обращаться к любой ячейке памяти и изменять ее содержимое. Конечно, многие программные продукты, используемые на ПК, включают в себя отдельные средства защиты, однако отсутствие базового набора средств гарантированного обеспечения безопасности информации, как и отсутствие сколь-нибудь системной политики значительно снижает эффективность использования отдельных, не связанных друг с другом средств защиты.

Во-вторых, один ПК может работать в многопользовательском режиме и широко использоваться в вычислительных сетях различного масштаба и в круглосуточном режиме, что повышает уязвимость обрабатываемой информации и делает проблему ее безопасности в ПК весьма актуальной. В силу данных обстоятельств защита информации в РС имеет свои особенности.

6.1.2. Потенциальные угрозы информации, обрабатываемой в рабочих станциях

Потенциальные угрозы информации в рабочей станции так же, как и в большом КСА, выражаются в виде случайных и преднамеренных воздействий, а также их сочетаний. Общий концептуальный подход, методы и средства борьбы с ними, приведенные в подразд. 3.2–3.5, в основном применимы и для рабочей станции. Отличие заключается в возможных каналах НСД к информации.

Возможные каналы преднамеренного несанкционированного доступа к информации в РС зависят от условий ее эксплуатации: используется ли она одним пользователем или группой. Поскольку многосменный режим работы на одной рабочей станции считается многопользовательским, его и рассмотрим как наиболее опасный режим. Кроме того, будем считать, что на рабочей станции обрабатывается важная информация, к которой может проявить интерес нарушитель I класса. Тогда при отсутствии средств защиты возможны следующие каналы несанкционированного доступа к информации РС (рис. 6.1):

- клавиатура, манипулятор «мышь»;
- монитор;
- принтер;
- средства загрузки ПО;
- носители информации (машинные и бумажные);
- внутренний монтаж системного блока ПК;
- побочное электромагнитное излучение;
- побочные наводки информации по сети электропитания и заземления аппаратуры;
- побочные наводки на цепях посторонней аппаратуры;
- ремонтируемые электронные блоки с остатками информации;
- отходы, брошенные в мусорную корзину.

Наблюдая за информацией на экране дисплея и распечаткой на принтере, нарушитель может ознакомиться с обрабатываемой информацией. Вла-

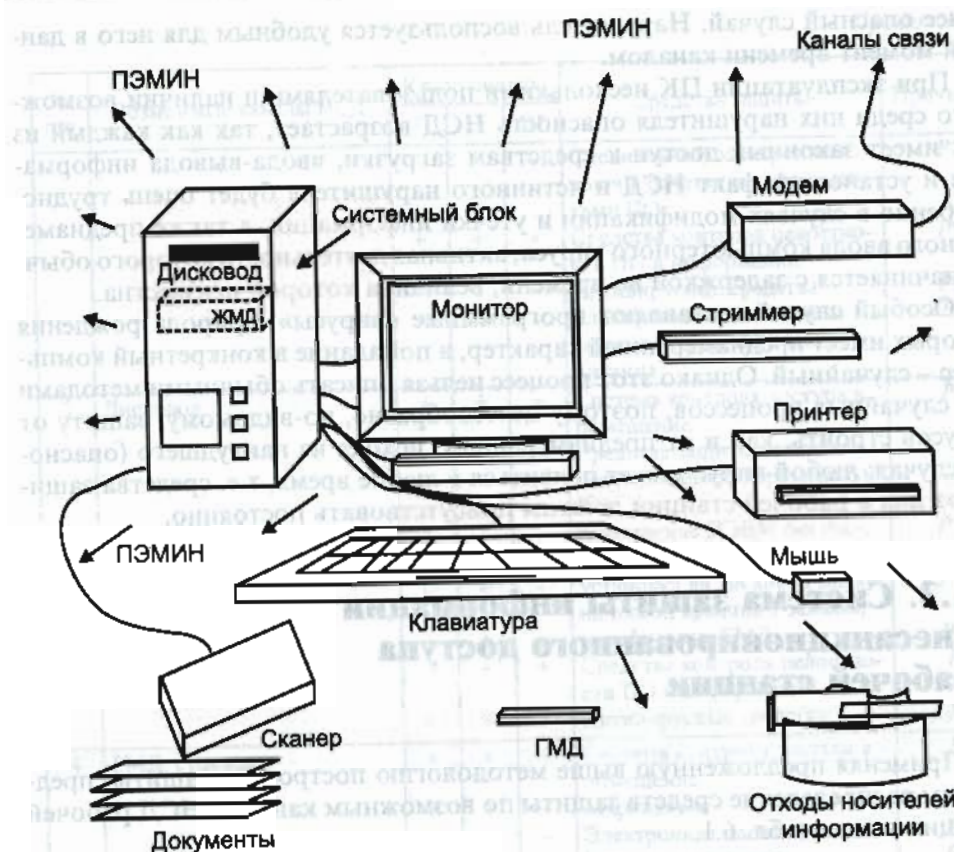


Рис. 6.1. Рабочая станция и возможные каналы НСД к ее информации

дея средствами загрузки (клавиатурой и собственным ГМД), нарушитель может модифицировать программное обеспечение и ввести компьютерный вирус. Несанкционированный доступ к носителям информации может выразиться в подмене, хищении, снятии копии программ и информации, что может привести к их модификации, утечке и разрушению. На сданных в ремонт или переданных для других целей машинных носителях может быть прочитана остаточная информация, даже если она была стерта. НСД к внутреннему монтажу может привести к подмене узлов, вводу сложной неисправности или установке постороннего устройства – передатчика информации по радиоканалу. Побочные электромагнитные излучения и наводки, несущие информацию, могут приниматься и декодироваться на специальных высокочувствительных приемниках, находящихся на значительном расстоянии от работающего ПК.

Перечисленные ВКНСД имеют место независимо от присутствия или отсутствия штатного пользователя, так как мы вначале условились, что средства защиты, включая организационные, отсутствуют, и несанкционированным действиям нарушителя ничто и никто не препятствует, т.е. исходя из принятой в концепции защиты модели нарушителя мы рассматриваем наи-

более опасный случай. Нарушитель воспользуется удобным для него в данный момент времени каналом.

При эксплуатации ПК несколькими пользователями и наличии возможного среди них нарушителя опасность НСД возрастает, так как каждый из них имеет законный доступ к средствам загрузки, ввода-вывода информации и установить факт НСД и истинного нарушителя будет очень трудно, особенно в случаях модификации и утечки информации, а также преднамеренного ввода компьютерного вируса, активная деятельность которого обычно начинается с задержкой во времени, величина которой неизвестна.

Особый случай составляют программные «вирусы», природа рождения которых имеет преднамеренный характер, а попадание в конкретный компьютер – случайный. Однако этот процесс нельзя описать обычными методами для случайных процессов, поэтому целесообразно, по-видимому, защиту от вирусов строить, как и от преднамеренных, исходя из наихудшего (опасного) случая: любой вирус может появиться в любое время, т.е. средства защиты от них в рабочей станции должны присутствовать постоянно.

6.1.3. Система защиты информации от несанкционированного доступа в рабочей станции

Применяя предложенную выше методологию построения защиты, представим распределение средств защиты по возможным каналам НСД рабочей станции в виде табл. 6.1.

Таблица 6.1

№ п/п	Возможные каналы НСД	Класс защиты			Средства защиты	Прочность
		I	II	III		
1	Монитор, принтер, плоттер, графопостроитель	+	+	+	Система контроля доступа в помещение	P2
2	Клавиатура, сканер, манипулятор «мышь»	+	+	+	Система контроля доступа в помещение	P2
		+	+	+	Программные средства идентификации и аутентификации пользователя (ввод паролей с клавиатуры)	P3
		+	+	+	Программно-аппаратные средства идентификации и аутентификации пользователя (ввод паролей с носителя)	P4
		+	+	+	Программные средства разграничения и контроля доступа к ПО	P5
		+	+	+	Программные средства разграничения и контроля доступа к информации	P6

Продолжение

№ п/п	Возможные каналы НСД	Класс защиты			Средства защиты	Прочность
		I	II	III		
		-	+	-	Специальный электронный ключ в сочетании с фрагментами ПО	P7
		+	+	+	Средства контроля целостности ПО и информации	P8
		+	+	+	Антивирусные средства	P9
		+	-	-	Блокировка механическим замком включения электропитания	P10
3	Дисковод	+	+	+	Система контроля доступа в помещение	P2
		+	+	+	Средства защиты от несанкционированной перезагрузки ПО:	
		+	-	-	применение ПЭВМ без дисковода;	P11
		-	+	-	установка на дисковод механической крышки с замком;	P12
		+	+	+	верификация ГМД.	P13
		+	+	+	Средства контроля целостности ПО и информации	P8
4	ГМД, стриммер	+	+	+	Антивирусные средства	P9
		+	+	+	Система контроля доступа в помещение	P2
		+	+	+	Маркировка	P14
		+	-	-	Электронная идентификация	P15
		+	+	+	Регистрация и учет	P16
		-	+	-	Хранение в металлических шкафах с замком	P17
		+	-	-	Хранение в сейфах	P18
		-	+	+	Стирание остатков информации в режиме замены	P19
		+	-	-	Трехкратное наложение произвольной последовательности символов на остатки информации	P20
		+	-	-	Шифрование данных	P21
5	ЖМД	+	+	+	Система контроля доступа в помещение	P2
		+	-	-	Механический замок на системном блоке	P22
		+	+	+	Средства контроля функционирования ПЭВМ	P23
		-	+	-	Стирание остаточной информации в режиме замены	P19
		+	-	-	Трехкратное наложение произвольной последовательности символов на остатки информации	P20
		+	-	-	Шифрование данных	P21
		+	+	-	Съемный ЖМД и сейф	P27
		+	+	-		

Продолжение

№ п/п	Возможные каналы НСД	Класс защиты			Средства защиты	Прочность
		I	II	III		
6	Внутренний монтаж	+	+	+	Система контроля доступа в помещение	P2
		+	+	-	Механический замок на системном блоке	P22
7	Модем	+	+	-	Система контроля доступа в помещение	P2
8	Внешние линии связи	+	+	+	Программные средства разграничения и контроля доступа к ПО	P5
		+	+	+	Программные средства разграничения и контроля доступа к информации	P6
9	Отходы носителей с остатками информации	+	+	-	Система контроля доступа в помещение	P2
		+	+	-	Средства уничтожения носителей	P24
10	ПЭМИН	+	-	-	Средства уменьшения и зашумления полезных сигналов с установлением границы контролируемой зоны	P25
11	Документы	+	+	+	Система контроля доступа в помещения	P2
		+	+	+	Регистрация и учет документов	P26
		+	+	-	Разграничение и контроль доступа к документам	P28
		+	+	-	Сейф	P18

Примечания: 1. Знак «+» означает наличие средства защиты, знак «-» – отсутствие средства защиты.
2. На всех каналах действует также система контроля доступа на территорию объекта размещения рабочей станции, ее прочность обозначим через P1.

При этом средства защиты от нарушителя, не являющегося законным пользователем, образуют по I классу нижеследующие защитные оболочки.

Контролируемую оболочку составят средства со следующими значениями прочности: P1, P2, P4 – P6, P8, P9, P15, P16, P18, P23, P25, P26. Данные значения вычисляются по формуле (3.8). При этом считаем, что антивирусные средства и средства контроля целостности ПО работают автоматически через определенный период времени и образуют отдельную защитную оболочку.

Перечисленные средства защиты необходимо проанализировать на предмет того, что на одном канале НСД, вероятно, одна часть будет дублировать друг друга, другая – перекрывать возможный путь обхода средства защиты, т.е. защита данного канала может состоять из параллельно и последовательно соединенных преград. Например:

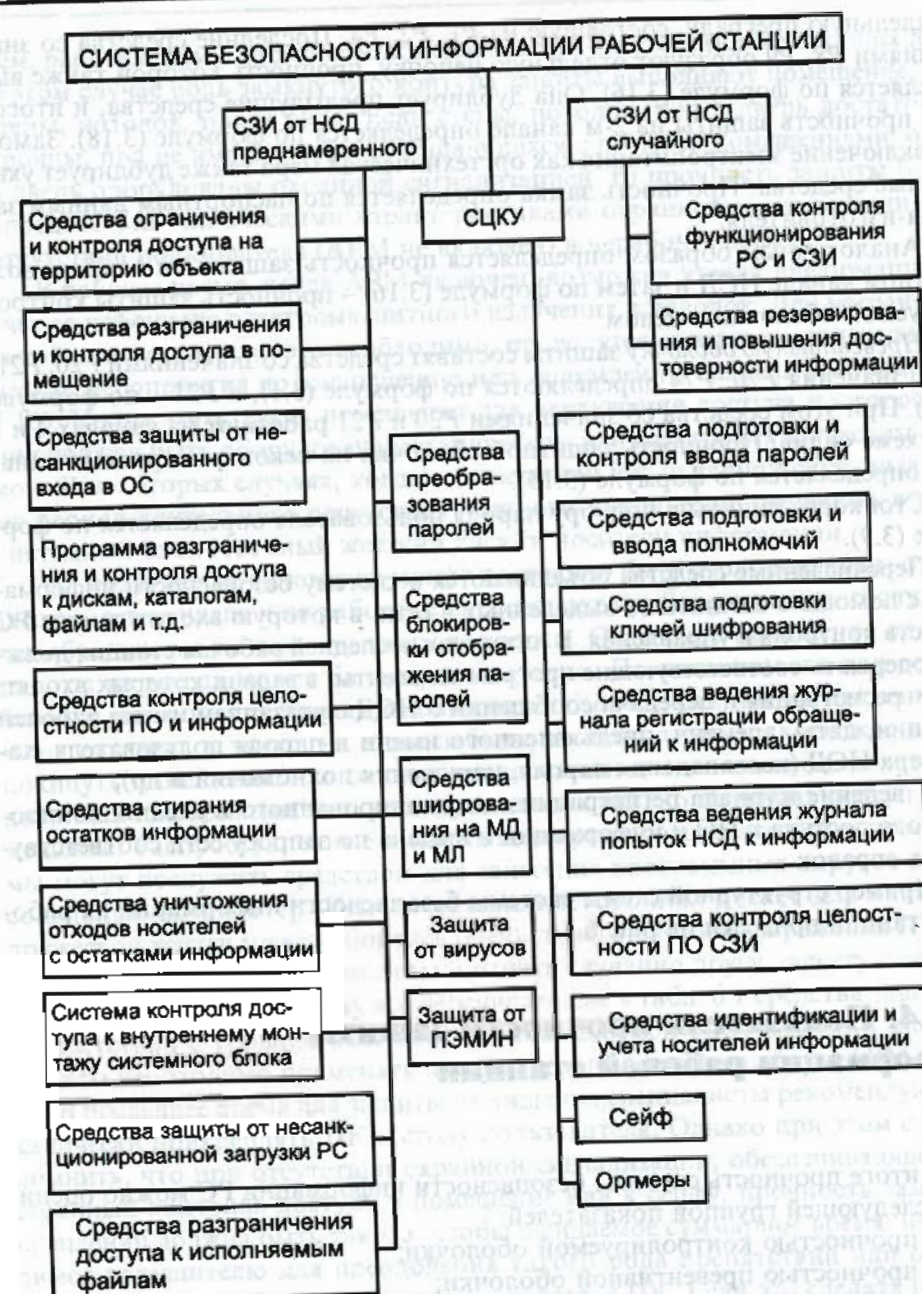


Рис. 6.2. Схема системы безопасности информации рабочей станции

на 1-м канале дублировать друг друга будут средства со значениями P1 и P2; в итоге прочность преграды на 1-м канале вычисляется по формуле (3.18);

на 2-м канале дублируют друг друга средства со значениями P1, P2, P4; средства со значениями P5 и P6 образуют отдельную последовательную цепочку, прочность которой вычисляется по формуле (3.16), она дублирует па-

параллельную преграду, состоящую из $P1, P2, P4$. Последние средства со значениями $P8, P9$ образуют отдельную цепочку, прочность которой также вычисляется по формуле (3.16). Она дублирует предыдущие средства, и итоговая прочность защиты на 2-м канале определяется по формуле (3.18). Замок на включение электропитания как оргтехническая мера также дублирует указанные средства. Прочность замка определяется по паспортным данным завода-изготовителя.

Аналогичным образом определяется прочность защиты на каждом возможном канале НСД и затем по формуле (3.16) – прочность защиты контролируемой оболочки в целом.

Превентивную оболочку защиты составят средства со значениями $P20, P21, P24$. Значения $P20, P24$ определяются по формуле (3.1), а $P21$ – по формуле (3.2). При этом средства со значениями $P20$ и $P21$ работают на каналах 4 и 5 по схеме «или». Прочность защитной оболочки на неконтролируемых каналах определяется по формуле (3.15).

Стойкость защиты к подбору пароля пользователя определяется по формуле (3.9).

Перечисленные средства объединяются в систему безопасности информации с помощью специально выделенных в сети, в которую входит данная РС средств контроля и управления. В интересах последней рабочая станция должна содержать соответствующие программы-агенты, в задачи которых входят:

- регистрация и передача сообщений о НСД с указанием имени рабочей станции, даты, времени, предъявленного имени и пароля пользователя, характера НСД (несовпадения пароля, нарушения полномочий и др);
- ведение журнала регистрации санкционированного и несанкционированного доступа к ПО и информации и выдача по запросу сети соответствующих справок.

Пример структурной схемы системы безопасности информации на рабочей станции приведен на рис. 6.2.

6.1.4. Показатели прочности защиты информации рабочей станции

В итоге прочность системы безопасности информации РС можно оценивать следующей группой показателей:

- прочностью контролируемой оболочки;
- прочностью превентивной оболочки;
- стойкостью пароля пользователя к подбору.

В случае применения персонального компьютера в качестве автоматизированного рабочего места (АРМ) в автономном режиме принципы управления защитой изменяются. При этом возможны два варианта применения автономного режима работы АРМ: одиночное и групповое.

Наиболее простой и надежный по прочности способ защиты информации от НСД – режим автономного использования АРМ одним пользовате-

лем, работающим в отдельном помещении при отсутствии посторонних лиц. В этом случае роль замкнутого контура защиты выполняют помещение, его стены, потолок, пол и окна. Если стены, потолок, пол и дверь достаточно прочны, пол не имеет люков, сообщающихся с другими помещениями, окна и дверь оборудованы охранной сигнализацией, то прочность защиты будет определяться техническими характеристиками охранной сигнализации при отсутствии пользователя (АРМ не включен) в нерабочее время.

В рабочее время, когда АРМ включен, возможна утечка информации за счет ее побочного электромагнитного излучения и наводок. Для устранения такой опасности, если это необходимо, проводятся соответствующие технические мероприятия по уменьшению или зашумлению сигнала (см. подразд. 2.10). Кроме того, дверь помещения для исключения доступа посторонних лиц должна быть оборудована механическим или электромеханическим замком. В некоторых случаях, когда в помещении нет охранной сигнализации, на период длительного отсутствия пользователя полезно помещать в сейф системный блок (съёмный жесткий диск) и носители информации.

На практике же человек не может постоянно быть изолированным от общества, в том числе и на работе. Его посещают друзья, знакомые, сослуживцы обращаются по тем или иным вопросам. Отдельное помещение для его работы не всегда может быть предоставлено. По рассеянности или озабоченный личными проблемами пользователь может компьютер включить, а ключ оставить в замке; на столе забыть дискету, а сам на короткое время покинуть помещение, что создает предпосылки для несанкционированного доступа к информации лиц, не допущенных к ней, но имеющих доступ в помещение. Распространенные в настоящее время развлекательные программы могут послужить средством для занесения программных вирусов в персональный компьютер. Использование посторонних дискет для оказания дружеской услуги может обойтись очень дорого. Помимо заражения ПК вирусом можно перепутать дискеты и отдать случайно другу дискету с секретной информацией. Поэтому все перечисленные в табл. 6.1 средства защиты в соответствии с уровнем важности обрабатываемой информации и классом защиты необходимо применять и в автономном режиме работы АРМ.

В последнее время для защиты от хищения специалисты рекомендуют механически прикреплять ПК к столу пользователя. Однако при этом следует помнить, что при отсутствии охранной сигнализации, обеспечивающей постоянный контроль доступа в помещение или к сейфу, прочность замков и креплений должна быть такова, чтобы ожидаемое суммарное время, необходимое нарушителю для преодоления такого рода препятствий или обхода их, превышало время отсутствия пользователя ПК. Если это сделать не удастся, то охранная сигнализация обязательна. Тем самым будет соблюдаться основной принцип срабатывания защиты и, следовательно, будут выполняться требования по ее эффективности.

Все перечисленные средства и им подобные должны с различной степенью безопасности обеспечивать только санкционированный доступ к информации и программам со стороны клавиатуры, средств загрузки и внутреннего монтажа компьютера.

В автономном режиме работы АРМ предполагается, что владельцем или ответственным за информацию является его пользователь, других пользователей нет. Поэтому подготовка и управление защитой данных также входит в его обязанности.

На отечественном рынке предлагается ряд готовых программных и программно-аппаратных комплексов средств защиты, которые в той или иной мере отвечают составу средств, указанному в табл. 6.1 (например, ряд комплексов серии «Аккорд» производства ОКБ САПР; «SekretNet» – ЗАО НПП «Информзащита»; «Страж» – ЗАО «НИИ проблем управления, информатизации и моделирования Академии военных наук»; «Системпром – ЦНКТ» – концерн «Системпром», «КРИПТОН» – ООО «АНКАД» и др.).

Однако следует предупредить разработчиков АС о том, что готовность перечисленных средств (даже сертифицированных) не исключает хлопот по их внедрению в АС. Это обстоятельство связано не только с тем, что в указанных средствах и данной АС есть ошибки или логические и программные расхождения, но и с тем, что параметры средств защиты (прочность и пути ее обхода) в АС приобретают конкретное выражение, которое может не отвечать заданным требованиям.

6.2. Построение системы безопасности информации локальной вычислительной сети

6.2.1. Локальная вычислительная сеть как объект обработки и защиты информации

Принципы построения различных ЛВС приведены в разд. 1.

Рассматривая объект обработки с позиций защиты циркулирующей в ней информации, в общем случае автономную ЛВС можно представить как сеть, элементами которой являются малые комплексы средств автоматизации – рабочие станции с различным набором внешних устройств, автоматические технические средства: серверы, коммутаторы, концентраторы, мосты, маршрутизаторы, а каналами связи – кабельные магистрали (линии связи). Потенциальные угрозы в виде попыток несанкционированного доступа с целью модификации, разрушения, хищения информации или ознакомления с нею аналогичны приведенным в разд. 1. Возможные каналы несанкционированного доступа к информации в ЛВС такие же, как и в глобальных вычислительных сетях. Единственным отличием ЛВС, учитывая ее относительно малую территорию размещения, является возможность расположения линий связи ЛВС на охраняемой территории, что значительно сокращает количество потенциальных нарушителей и в некоторых менее ответственных системах позволяет с целью экономии уменьшить прочность защиты кадра кодограммы. Малые габариты компьютера позволяют разместить его на столе

в отдельном защищенном помещении и облегчают, с одной стороны, проблему контроля доступа к его внутренним линиям связи и монтажу устройств.

С другой стороны, возникает вопрос контроля целостности ЛВС, т.е. схемы соединений сети, так как ЛВС – система по своей идее децентрализованная. Вполне естествен вопрос: «А всегда ли необходим такой контроль?» Специалисты считают, что в очень маленьких ЛВС с парой компьютеров, которые разделяют жесткий диск и принтер, диагностика является ненужным излишеством. Но по мере роста сети возникает необходимость в мониторинге сети и ее диагностике. Большинство ЛВС имеют процедуры самотестирования низкого уровня, которые должны запускаться при включенной сети. Эти тесты обычно охватывают кабель, конфигурацию аппаратных средств, в частности плату интерфейса сети. В составе больших ЛВС предусмотрены сложные системы с двойным назначением – мониторингом и диагностикой. Центр управления сетью (ЦУС) – это пассивное мониторинговое устройство, которое собирает данные о потоках сообщений в сети, ее характеристиках, сбоях, ошибках и т.д. Данные о потоках сообщений показывают, кто пользуется сетью, а также когда и как она применяется.

Однако упомянутые выше средства диагностики ЛВС не обнаруживают несанкционированное подключение к сети постороннего ПК. Отключение компьютера от сети контролируется, иногда с перерывами по желанию оператора или по запросу пользователя.

В больших ЛВС (до 10 км) кабельные линии могут иногда выходить за пределы охраняемой территории или в качестве линий связи могут использоваться телефонные линии связи обычных АТС, на которых информация может подвергнуться несанкционированному доступу. Кроме того, сообщения в локальной сети могут быть прочитаны на всех ее узлах, несмотря на специфические сетевые адреса. Посредством пользовательских модификаций последних все узлы сети могут считывать данные, циркулирующие в данной ЛВС.

6.2.2. Возможные каналы несанкционированного доступа

Применяя приведенный в данной работе концептуальный подход, определяем максимальное количество возможных каналов преднамеренного несанкционированного доступа к информации ЛВС. В качестве типового примера рассмотрим схему большой ЛВС, приведенной на рис. 6.3. Со стороны «периметра» системы возможными каналами НСД могут быть:

- рабочие станции;
- серверы;
- автоматические технические средства (мосты, коммутаторы, концентраторы, маршрутизаторы);
- профилируемая и ремонтируемая аппаратура;
- кабельные линии связи;
- внешние каналы связи.

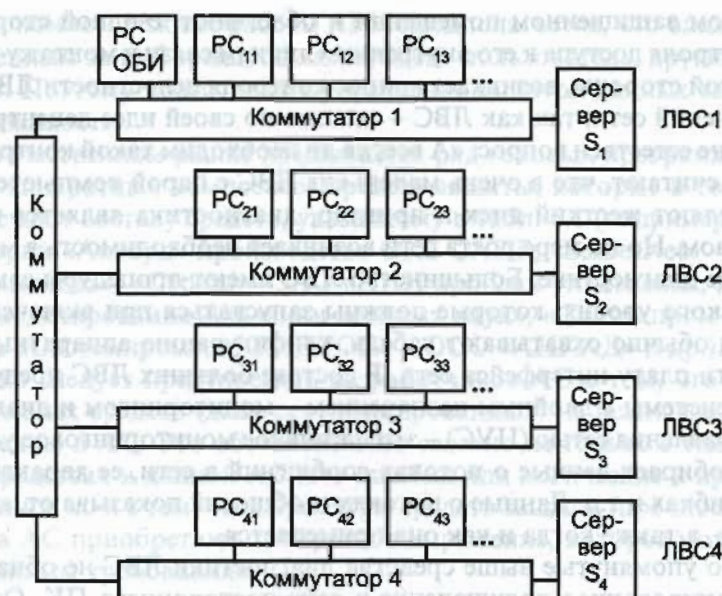


Рис. 6.3. Схема большой локальной вычислительной сети

Несанкционированный доступ к информации ЛВС со стороны рабочей станции возможен по каналам, перечисленным в подразд. 6.1. В ЛВС необходимо защищаться также и от законного пользователя-нарушителя, допущенного только к определенной информации сервера и (или) ограниченного круга других пользователей данной ЛВС.

Несанкционированный доступ в ЛВС со стороны кабельных линий может произойти по следующим каналам:

- со стороны штатного пользователя-нарушителя одной РС при обращении к информации другой, в том числе серверу;
- при подключении постороннего компьютера и другой посторонней аппаратуры;
- побочным электромагнитным излучениям и наводкам информации.

Так как наиболее опасную ситуацию представляет подключение к линиям связи посторонней ЭВМ и данная ситуация фактически включает и первую, целесообразно их объединить и рассматривать как одну, а решение по ее защите распространить на обе ситуации.

Так как ЛВС согласно принятому выше решению относится к системам с распределенной обработкой данных, необходимо в ней реализовать подход, заключающийся в анализе возможных несанкционированных действий над кадром кодограммы, передаваемой по линиям связи между ее техническими средствами. Анализ такого рода действий нарушителя, приведенных в подразд. 3.4.3, с учетом масштабов и предполагаемого размещения ЛВС на охраняемой территории позволяет их сократить до следующих видов:

- чтение содержания сообщения;
- дублирование или переупорядочивание сообщения;

- переадресация сообщения;
- задержка или удаление сообщения;
- посылка ложного сообщения;
- чтение и подбор сетевых паролей;
- нарушение пользователем своих полномочий в сети;
- отказ от переданного и принятого сообщения.

6.2.3. Построение системы безопасности информации в ЛВС

Анализ перечисленных выше возможных каналов НСД к информации ЛВС, рассмотренных с позиций максимально возможных угроз, ожидаемых от нарушителя-профессионала, а также выбор соответствующих средств защиты позволяют представить их распределение в виде табл. 6.2.

Таблица 6.2

№ п/п	Наименование ВК НСД	Класс защиты			Средства защиты	Прочность
		I	II	III		
1	ВК НСД рабочей станции (см. табл. 6.1)	+	+	+	Система безопасности информации рабочей станции с учетом параметров ПК, ПО, прикладных программ и функциональных задач пользователей данной рабочей станции	G_{pc}
2	ВК НСД файлсервера (см. ВК НСД РС в табл. 6.1)	+	+	+	Система безопасности, построенная аналогично системе на рабочей станции с учетом параметров выбранного для сервера ПК, ПО и функциональных задач ЛВС	G_{fc}
3	ВК НСД сервера регистрации и документирования (см. ВК НСД РС в табл. 6.1)	+	+	+	Система безопасности информации, аналогичная рабочей станции с учетом параметров, выбранных для сервера ПК, ПО и их функциональных задач	G_{ra}
4	ВК НСД рабочей станции службы безопасности (см. ВК НСД РС в табл. 6.1)	+	+	+	Система безопасности, аналогичная рабочей станции с учетом параметров выбранного ПК, ПО и функциональных задач службы безопасности	G_{cb}
5	Автоматические технические средства	+	+	-	Система разграничения и контроля доступа в помещения Система контроля вскрытия аппаратуры	P_2 P_{28}
6	Ремонтируемая и профилактисруемая аппаратура	+	+	-	Система разграничения и контроля доступа в помещения Система контроля конфигурации ЛВС	P_2 P_{27}

Продолжение

№ п/п	Наименование ВК НСД	Класс защиты			Средства защиты	Прочность
		I	II	III		
7	Блоки электропитания	+	+	-	Средства контроля и разграничения доступа в помещения	P2
		+	+	-	Система контроля вскрытия аппаратуры	P28
8	Внутренние линии связи между аппаратными средствами ЛВС	+	+	-	Система контроля вскрытия аппаратуры	P28
		+	-	-	Скрытая прокладка линий связи (см. табл. 6.3)	P29
		+	+	+		
9	Побочное электромагнитное излучение от линий связи и наводки информации	+	-	-	Шифрование содержательной части кадра кодограммы обмена	P30
		-	+	-	Средства зашумления информационного сигнала	P25
10	Внешние каналы связи (при их наличии)	+	+	+	Межсетевой экран	P31

Примечания:

1. Знак «+» обозначает наличие средства защиты, «-» – отсутствие.
2. G_{pc} – группа показателей прочности защиты информации рабочей станции.
3. G_{fc} – группа показателей прочности защиты информации файлсервера, количество показателей в группе должно соответствовать количеству показателей для рабочей станции.
4. G_{rd} – группа показателей прочности защиты информации сервера регистрации и документирования, количество показателей в группе должно соответствовать количеству показателей для рабочей станции.
5. G_{cb} – группа показателей прочности защиты информации рабочей станции службы безопасности, количество показателей в группе должно соответствовать количеству показателей для рабочей станции.
6. Технические средства ЛВС размещены на территории, охваченной системой контроля доступа, прочность защиты которой обозначается через P1.
7. Нумерация показателей прочности средств защиты проведена с учетом табл. 6.1.

НСД со стороны пользователя-нарушителя, очевидно, потребует создания на уровне ЛВС специальной системы контроля и разграничения доступа к информации со всеми ее атрибутами: средствами идентификации и аутентификации пользователей, а также разграничения их полномочий по доступу к информации серверов и (или) другим ПК данной ЛВС. Она же будет полезна для защиты от несанкционированного подключения к линиям связи.

С учетом количества видов несанкционированных действий, приведенных в 6.2.2, и классификации уровней защиты (подразд. 3.4.3) распределение средств защиты по возможным действиям нарушителя на линиях связи ЛВС по отношению к кадру кодограммы можно представить в виде табл. 6.3.

Перечисленные в табл. 6.2 и 6.3 средства защиты объединяются в систему безопасности информации ЛВС с помощью средств управления безопасностью информации (СУБИ): специально разработанного ПО и выделенной рабочей станции службы безопасности, на основе которой строится автоматизированное рабочее место ее представителя. В состав этого АРМ должен войти

пульт централизованного контроля доступа в помещения и контроля вскрытия аппаратуры с автономным резервированным электропитанием. Программные средства рабочих станций пользователей, серверов и его рабочей станции, кроме стандартных, в интересах функционирования средств защиты информации и управления ими должны обеспечить выполнение следующих функций:

- отображения единого времени ЛВС;
- отображения действующей конфигурации ЛВС;
- ведения списка должностных лиц – пользователей ЛВС;
- ведения оргштатной структуры должностных лиц – пользователей ЛВС;
- ведения таблиц паролей пользователей, допущенных к информационному обмену в ЛВС;
- ведения таблиц полномочий пользователей, рабочих станций;

Таблица 6.3

№ п/п	Возможные несанкционированные действия	Класс защиты			Средства защиты информации ЛВС	Прочность
		I	II	III		
1	Чтение содержания сообщения	+	+	-	Шифрование содержательной части сообщения	P30
2	Дублирование сообщения	+	-	-	Шифрование даты и времени отправления сообщения вместе с его содержательной частью	P32
3	Переупорядочение сообщения	+	-	-	Шифрование и цифровая подпись служебных частей кадра	P33
4	Задержка или удаление сообщения	+	-	-	Средства подтверждения о получении сообщения с цифровой подписью	P34
5	Переадресация сообщения	+	-	-	Цифровая подпись адреса получателя одновременно с содержательной частью сообщения	P35
6	Посылка ложного сообщения	+	-	-	Цифровая подпись адреса получателя одновременно с содержательной частью сообщения	P35
7	Чтение и подбор сетевых паролей	+	+	+	Программный комплекс идентификации и аутентификации пользователей и рабочих станций в сети	P36
		+	+	-	Средства контроля конфигурации сети	P27
8	Нарушение законным пользователем своих полномочий в сети	+	+	+	Программа контроля и разграничения доступа к ПО и информации сервера и рабочей станции	P4
9	Отказ от переданного и принятого сообщения	+	+	-	Регистрация на РС ОБИ фактов передачи и приема сообщений	P37

- Примечания: 1. Знак «+» означает наличие средства защиты, «-» – отсутствие.
2. Нумерация прочности средств защиты проведена с учетом табл. 6.1 и 6.2.

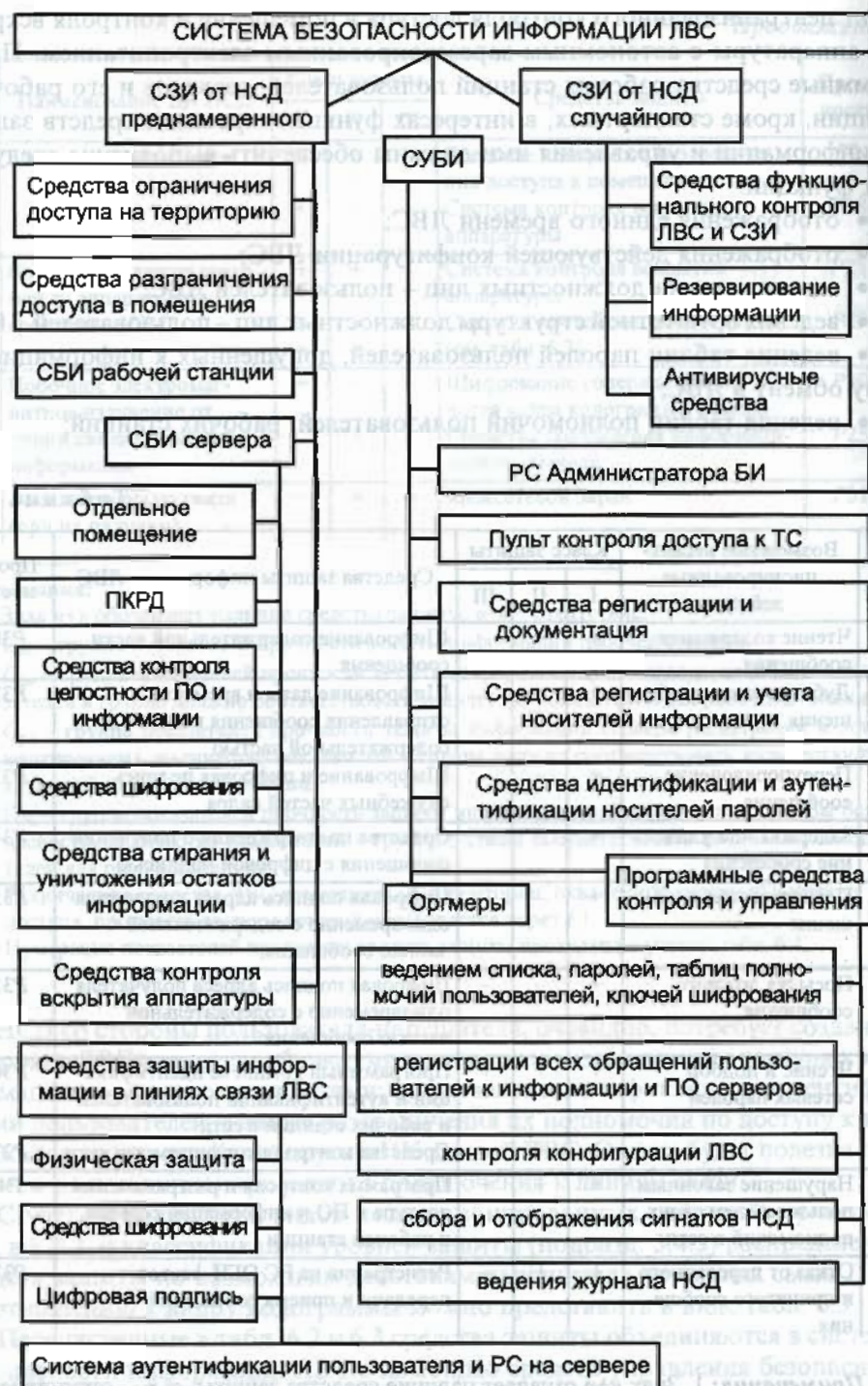


Рис. 6.4. Схема системы безопасности информации ЛВС

- генерации паролей, ключей шифрования и кодов цифровой подписи в виде случайных чисел;
- централизованного распределения и автоматизированной рассылки паролей, ключей шифрования по назначению;
- автоматизированной подготовки носителей таблиц паролей и полномочий пользователей к их загрузке в РС и серверы;
- контроля результатов аутентификации пользователей, РС;
- централизованного сбора и отображения в сопровождении звуковой сигнализации сообщений о НСД и его атрибутов;
- получения по запросу за любой промежуток времени справки о выдаче(приеме) с(на) сервера сообщений с возможностью ее получения по имени пользователя, РС, по заданному объекту обращения (документу, техническому средству);
- получения с РС и серверам по вызову оператора отдельных справок по НСД за заданный промежуток времени;

сбора и учета «открытых» кодов цифровой подписи пользователей, их регистрации и отображения с атрибутами переданного сообщения: времени и даты отправления, имени пользователя, адреса отправителя и получателя, заголовка, номера квитанции о приеме, времени и даты получения;

электронной идентификации и регистрации машинных носителей. Кроме того, в результате аварийных ситуаций, отказов аппаратуры, ошибок операторов и разработчиков ПО ЛВС возможны переадресация информации, отображение и выдача ее на рабочих местах, для нее не предназначенных, потеря информации в результате ее случайного стирания или пожара. Практика показывает, что большинство людей не уделяют серьезного внимания защите данных, особенно резервированию, до тех пор, пока у них не произойдет серьезная их потеря.

Проникновение сетевого вируса в рабочую станцию и сервер может также неприятно отразиться на всей работе и информации ЛВС, а также остальных рабочих станций, входящих в состав ЛВС.

Пример возможной структуры системы безопасности информации ЛВС приведен на структурной схеме рис. 6.4.

6.2.4. Показатели оценки прочности защиты информации ЛВС

Анализ приведенных в табл. 6.2 и 6.3 средств защиты показывает, что контролируемую сетевую оболочку защиты составят средства со значениями прочности $P_2, P_4, P_{27}, P_{28}, P_{31}, P_{34}, P_{36}, P_{37}$; превентивную – со значениями $P_{25}, P_{30}, P_{32}, P_{33}, P_{35}$.

Расчет прочности средств контроля ведем по формуле (3.8). Прочность контролируемой оболочки определяем по наименьшему значению, т.е. по формуле (3.16); с учетом дублирования средств защиты – по формуле (3.18).

Учитывая размещение линий связи ЛВС на контролируемой территории, целесообразно вести расчет прочности превентивных средств даже для I клас-

са по формуле (3.12), исходя из модели нарушителя, действующего в единственном числе. По такому же принципу определяем прочность превентивной сетевой оболочки защиты по формуле (3.14).

Прочность защиты санкционированного входа в серверы ЛВС определяется стойкостью пароля сетевой аутентификации к подбору, т.е. вычисляется по формуле (3.9). Полученные результаты составят группу сетевых показателей прочности защиты рассматриваемой ЛВС:

- прочности контролируемой сетевой оболочки защиты;
- прочности неконтролируемой сетевой оболочки защиты;
- стойкости пароля сетевой аутентификации.

Согласно методу, предложенному в подразд. 3.4.6, если на рабочих станциях пользователей обрабатывается информация одинаковой важности, общая оценка прочности защиты информации от преднамеренного НСД в рассматриваемой ЛВС может быть представлена следующими показателями:

- группой показателей прочности защиты информации на рабочей станции;
- группой показателей прочности защиты информации на файловом сервере;
- группой показателей прочности защиты информации на сервере регистрации и документирования;
- группой показателей прочности защиты информации рабочей станции службы безопасности;
- группой сетевых показателей прочности оболочек защиты.

6.3. Построение системы безопасности информации в глобальных АСУ и телекоммуникационных вычислительных сетях

6.3.1. Особенности построения защиты информации в АСУ

Предложенный выше метод построения защиты информации позволяет применить его в АСУ любой сложности и масштаба. При построении системы защиты информации в АСУ необходимо определить следующие исходные данные:

- структуру, состав и назначение АСУ и ее элементов;
- структуру, состав и принципы построения сети передачи данных (СПД);
- информационные процессы, подлежащие автоматизации;
- задачи и функции управления, их распределение между исполнителями;
- схему информационных потоков и места сосредоточения информации, подлежащей защите;
- структуру, состав и размещение информационной базы АСУ;

- перечень и сроки сохранения сведений, подлежащих защите;
 - состав и выполняемые функции должностных лиц – пользователей;
 - перечень, формы и количество входных, внутренних и выходных документов;
 - режим использования АСУ (открытый, закрытый и т.д.);
 - вероятностно-временные характеристики обработки сообщений;
 - органы управления функционированием и их размещение в АСУ;
 - органы управления сетью передачи данных и их размещение в АСУ.
- Предметом защиты в этом случае может быть следующая информация:
- структура, состав, назначение и принципы построения АСУ;
 - структура, состав, назначение и принципы обмена данными в АСУ;
 - состояние направлений связи в сети передачи данных;
 - адресные таблицы АСУ и сети;
 - таблицы полномочий элементов АСУ и сети;
 - информация, обрабатываемая в КСА и узлах коммутации СПД, а также циркулирующая в каналах связи.

Согласно принципам построения АСУ данная информация может размещаться на каждом КСА АСУ. Системные отношения между КСА АСУ имеют практический характер по схеме рис. 1.32, а описание АСУ приведено в подразд. 1.2.12. Степень важности информации КСА может быть одинаковой или значительно отличаться.

Соответственно на разных КСА потребуется разный уровень защиты. По этой причине показатель уровня безопасности информации АСУ в целом общим быть не может и представляет собой группу показателей. Однако группа показателей защиты кадра кодограммы в коммутируемых каналах связи (за исключением прямых) является общей.

Анализ принципов построения АСУ показывает, что обработка и обмен информацией в ней производятся на уровнях:

- КСА АСУ;
- УК СПД (сети передачи данных);
- СПД в целом;
- АСУ в целом.

На каждом из уровней образуется своя автоматизированная система, выполняющая свои задачи, связанные с вводом-выводом, хранением, обработкой и передачей определенной информации, соответствующей функциональным задачам и обязанностям должностных лиц и пользователей в структуре АСУ и СПД.

Если КСА представляет собой локальную вычислительную сеть, то в ней ведется обработка информации на уровне технических средств и ЛВС в целом.

Аналогичным образом целесообразно распределить в АСУ функции обеспечения защиты информации и создать на соответствующих уровнях встроенные системы защиты информации. Средства защиты информации так же, как и основные средства ее обработки в системе, реализуются на программном, аппаратном и организационном уровнях. При этом они выполняют свои функции в тесном взаимодействии с основными компонентами комп-

лексов средств автоматизации АСУ и сети. Совокупность определенных средств защиты на уровнях КСА, СПД и АСУ образует на каждом уровне свою систему защиты информации. Причем, с одной стороны, средства защиты являются общесистемными ресурсами, а с другой – в силу специфики решаемых задач система защиты для каждого уровня может быть представлена в виде встроенной самостоятельной структуры, которая нуждается в собственном управлении в целях координации и контроля своих процессов по обеспечению безопасности данных.

В каждой из перечисленных систем должна быть система опознавания, разграничения доступа и средства контроля и управления, с помощью которых в рамках данной системы можно выполнять следующие функции:

- составление перечня, ранжирование по важности и степени секретности, назначение сроков действия документов и других данных, подлежащих защите от НСД;
- разграничение, распределение и контроль полномочий должностных лиц-пользователей по отношению к информации и функциям управления;
- организацию и поддержку функционирования системы безопасности информации в системе;
- подготовку, выбор, распределение и периодическую замену ключей шифрования информации и кодов цифровой подписи;
- своевременное обнаружение, блокировку, сбор, регистрацию и документирование всех обращений к защищаемой информации и фактов НСД;
- своевременное установление места, времени и причины НСД;
- взаимодействие со службой функционального контроля и администраторами системы;
- взаимодействие со службами безопасности других систем;
- взаимодействие со службой безопасности нижестоящих объектов управления (КСА).

6.3.2. Особенности построения защиты информации в телекоммуникационных вычислительных сетях

Анализируя современную ситуацию с разработкой и созданием защиты информации в телекоммуникационных вычислительных сетях (по классификации, см. подразд. 1.2.13), можно выделить четыре направления работ:

- построение защиты на новых самостоятельных (выделенных) сетях, создаваемых с использованием элементов технологии Интернета;
- модернизация средств и системы защиты параллельно с доработкой существующих сетей;
- разработка методов и средств защиты информации в Интернете;
- создание защищенных корпоративных сетей на базе существующих телекоммуникационных сетей общего пользования, в которых применяются открытые протоколы Интернета.

Как отмечалось выше, действующий сегодня общий концептуальный подход во всех направлениях работ заключается в попытке создания в указанных сетях для обработки и передачи информации защищенной среды. Данный подход является продолжением общего подхода к реализации информационных технологий в виде вычислительной среды в той или иной предметной области. Современные информационные технологии основаны на применении программных продуктов, обладающих широкими функциональными возможностями и развитым пользовательским интерфейсом. В результате такого подхода создавалась иллюзия возможности решения вопросов защиты информации таким же путем. Далее, несмотря на привлечение к этому вопросу и аппаратной реализации этой технологии, упомянутый подход, к сожалению, сохранился. Подход не учитывает специфику конкретных видов автоматизированных систем. Вместо термина «АСУ» применяется термин «корпоративная вычислительная сеть» термины «виртуальная сеть», «облако» и т.д.

Не подвергая сомнению правильность выбора пути развития средств автоматизации процессов приема, хранения, обработки и передачи информации, включая терминологию, в данной работе в интересах обеспечения более высокого уровня безопасности информации предлагается при проектировании ее защиты в вычислительных сетях «спуститься с облаков на землю» и для начала посмотреть, где находятся эти процессы. При разработке вычислительной сети известны состав и размещение технических средств, узлов коммутации пакетов, абонентских комплексов и связей между ними. Далее предлагается выделить в сети объекты автоматизации с территориально-сосредоточенной обработкой данных и каналы связи между ними и затем реализовать предложенную в разд. 3 методологию построения системы безопасности информации.

Предмет защиты в телекоммуникационной сети вычислительной сети определяется ее техническими и экономическими задачами. К техническим задачам относятся: защита управляющих функций на пункте управления сетью, коммутационных – на узлах коммутации пакетов, кадров кодограммы обмена – в каналах связи. Потенциальные угрозы информации в такой сети, очевидно, будут связаны только с модификацией и утратой. Руководствуясь этим, можно сократить количество возможных каналов НСД на пункте управления и узлах коммутации (см. табл. 3.3), а на кадре кодограммы – количество возможных несанкционированных действий (см. табл. 3.4).

В экономические задачи сети в числе прочих входят предоставляемые услуги, в которые могут войти предоставление информации из базы данных сети и услуги по обмену информацией между ее абонентами. Все услуги оказываются за плату. Это обстоятельство требует регистрации и аутентификации пользователя по паролю и защиты последнего от НСД. Разные услуги имеют разные цены и, следовательно, требуют разграничения доступа. В услугу по обмену может добавиться услуга по обеспечению безопасности информации. Тогда придется строить защиту от НСД, приведенных в табл. 3.3 и 3.4, с учетом возможной утечки информации.

Если к создаваемой сети подключаются одна или несколько других сетей, то не следует спешить с созданием единой системы безопасности инфор-

мации. Такое решение прежде всего зависит от того, кто является собственником сетей и каковы ее задачи. Если собственники разные, то решение отрицательное, потому что возникает вопрос ответственности за безопасность. Один собственник будет против того, чтобы его контролировал другой. Даже если удастся договориться, первый фактически не отвечает за свою сеть и будет халатно относиться к своим обязательствам. В случае, когда у всех сетей один собственник, решение будет зависеть от технических возможностей входящих сетей, масштабов применения и нагрузки, которую возьмет на себя единая служба безопасности. Чаще всего встречается попытка объединения гетерогенных сетей, созданных в разное время на разных аппаратных и программных платформах и с различным уровнем безопасности данных. В этом случае необходимо учитывать, что уровень безопасности информации в тракте «абонент 1 – сеть 1 – сеть 2 – абонент 2» определяется сетью с наименьшим значением этого уровня. Существует еще пара аргументов, влияющих на принятие решения. Средства управления каждой сетью наверняка сохранятся, а управление сетью и управление безопасностью ее информации – вещи неразделимые. Следовательно, целесообразно то и другое сохранить. Кроме того, даже в случае наличия одного собственника у сетей сохраняется коллизия, упомянутая выше для разных собственников, так как в том и другом случае решающую роль играет фактор ответственности должностных лиц.

С другой стороны, необходимы координация действий, разрешение конфликтных ситуаций, централизованный контроль функционирования сетей и распределение паролей аутентификации и ключей шифрования. В решении этих вопросов принципиальную роль играет назначение сетей. Если они служат для выполнения задач передачи данных в АСУ или корпоративной сети, их абоненты являются членами одной организации, в которой существует определенная иерархия их отношений. Тогда единая служба необходима (этот вопрос рассмотрен в подразд. 3.6). В случае выполнения сетями задач обслуживания независимых абонентов ситуация меняется. Скорее всего абоненты для обмена информацией между собой пожелают пользоваться собственной системой абонентского шифрования или, по крайней мере, собственными ключами шифрования и цифровой подписи (это подтверждается появлением сетей VPN). Для получения открытой информации из баз данных сетей абоненту достаточно будет предъявить пароль сетевой аутентификации (в неявном виде – многозначный и в явном виде – однозначный), который (ые) должен(ы) быть выдан ему лично при регистрации в сети. Защиту собственной информации по обеспечению функционирования сети целесообразно оставить за ее собственной службой безопасности. В итоге нетрудно заметить, что в объединенных некорпоративных сетях организация единой службы безопасности информации не актуальна. При этом для реализации взаимодействия достаточно составить и подписать соответствующее соглашение при разработке моста или шлюза.

Развивая далее последнюю тему, заметим, что глобальная сеть Интернет с технической точки зрения – это объединение транснациональных компьютерных сетей, работающих по самым разнообразным протоколам, связывающим всевозможные типы компьютеров, физически передающих данные по

телефонным проводам и оптоволокну, через местные, региональные, глобальные сети, радиомодемы и спутники. С административной точки зрения – это не более чем удобная терминологическая условность. Координацию сети осуществляет Центр информационных сетей при Стэнфордском исследовательском институте в Менло-парке (Калифорния, США). Принимая во внимание изложенное выше, уровень безопасности информации в Интернете определяется уровнем безопасности информации сетей, входящих в нее, а слабость последних заключается прежде всего в противоречии задач обслуживания абонентов и безопасности информации. Известно, что основной задачей Интернета является автоматизировать обмен информацией как можно большего количества людей, предоставить как можно больше информационных услуг. С позиций безопасности чем больше абонентов, тем больше вероятность появления нарушителя; чем больше услуг, тем сложнее система, больше каналов несанкционированного доступа к информации и сложнее построить защиту. Налицо действие известного закона о переходе количества в качество. По указанным выше причинам централизованную систему безопасности информации создавать сложно, не эффективно и не нужно, а с экономической и политической точек зрения даже опасно. На информационном рынке появится монополист, который будет навязывать свои продукты и политическую волю. Каков же выход из этого положения? – В разумном сочетании децентрализации и централизации управления и контроля, применении последней на уровне входящих в Интернет самостоятельных сетей, совершенствовании в них защиты информации и взаимодействия в этом плане между собой. Совершенствование предлагается проводить на основе модели и методологии построения защиты, приведенной в разд. 3.

Пока реализуются эти предложения, существующие телекоммуникационные вычислительные сети продолжают работать, и было бы неразумно их не использовать. При этом для защиты обмена информацией в открытых сетях целесообразно применить специальные средства защиты трактов передачи данных. Такой метод используется при построении защищенных *виртуальных частных сетей* (Virtual Private Network – VPN). Виртуальная сеть формируется на основе каналов связи открытой сети. Сам термин «виртуальная» основан на том, что каналы связи виртуальной сети моделируются с помощью каналов связи реальной. Открытая сеть может служить основой для одновременного сосуществования множества независимых виртуальных сетей, количество которых определяется пропускной способностью открытых каналов связи.

Виртуальную сеть, использующую в качестве внешней среды передачи информации глобальную сеть Интернет, часто называют еще сетью *Extranet*.

Эффективность использования виртуальных сетей во многом определяется степенью защищенности информации, циркулирующей по открытым каналам связи. Безопасность информационного обмена необходимо обеспечить как в случае объединения локальных сетей, так и в случае доступа к локальным сетям удаленных пользователей [28].

Защита информации в процессе ее передачи по открытым каналам основана на построении защищенных виртуальных каналов связи, называемых крипто-защищенными туннелями, или туннелями VPN. Каждый такой тун-

нель представляет собой соединение, проведенное через открытую сеть, по которому передаются криптографически защищенные пакеты сообщений виртуальной сети [28].

Для защиты от повтора, удаления и задержек пакетов сообщений, передаваемых по туннелю VPN, используются встроенные возможности стека протоколов TCP/IP. Для защиты от повтора, удаления и задержек на уровне отдельных сообщений в состав каждого сообщения подсистемой защиты прикладного уровня должна добавляться дополнительная информация. В качестве такой дополнительной информации могут использоваться номера, случайные числа, а также отметки времени.

С целью защиты от отказа получения сообщений подсистема защиты прикладного уровня должна предусматривать при приеме каждого сообщения передачу отправителю уведомления о получении сообщения. Такое уведомление должно криптографически подписываться получателем сообщения. Защита от отказа отправления сообщения, т.е. защита от непризнания цифровой подписи, может быть обеспечена только правовыми и организационными мерами по приданию цифровой подписи юридической силы. Чтобы предотвратить отказы от открытых ключей, а соответственно и отказы от цифровой подписи, обмен открытыми ключами должен подкрепляться юридической процедурой [28].

МЕТОДЫ ОЦЕНКИ УРОВНЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

7.1. Анализ современных методов оценки

Вопрос оценки безопасности информации в автоматизированных системах обработки данных, несмотря на существующие в настоящее время решения [14, 29, 31, 34, 64, 67, 73], является по-прежнему актуальным. Безопасность информации – важнейшая характеристика автоматизированной системы, как любая характеристика, должна иметь единицы измерения. Оценка безопасности информации необходима для определения его достаточности или недостаточности для той или иной системы.

Вопросам оценки безопасности информации посвящено много литературы. Первыми, завершившимися выпуском нормативных документов в этой области являются работы, проводимые в США.

Так, в начале 1980 г. в США были разработаны Критерии оценки доверенных компьютерных систем (TCSEK). В следующем десятилетии уже сразу несколько стран принялись разрабатывать критерии оценки. Данные критерии базировались на концепции TCSEK, но были более гибкими и адаптируемыми по отношению к развитию информационных технологий [59].

В 1991 г. Европейской комиссией были выпущены европейские Критерии оценки безопасности информационных технологий (ITSEK), явившиеся результатом совместных усилий специалистов Франции, Германии, Нидерландов и Великобритании. В начале 1993 г. как комбинация подходов ITCSEK и ITSEK в Канаде были выпущены Канадские критерии оценки доверенных компьютерных продуктов (CTCPEC), а в США – рабочая версия Федеральных критериев безопасности информационных технологий (FC).

Учитывая потребность во взаимном признании результатов оценки безопасности на глобальном рынке информационных технологий международной рабочей группой ИСО (ISO/IEC JTC 1/SC 27/WG 3) в 1996, 1998 и 1999 гг. соответственно были разработаны три версии (1.0, 2.0 и 2.1) «Общих критериев». Последняя версия приняла вид стандарта ИСО.МЭК 15408-99 «Критерии оценки безопасности информационных технологий» [Criteria for Information Technology Security Evaluation], разработанного в рамках проекта «Общие критерии».

Общие критерии (ОК) представляют собой структурированную универсальную библиотеку требований безопасности, сформулированных в довольно общем виде. Их специализация и конкретизация осуществляются в двух основных конструкциях, определенных в ОК: профилях защиты (ПЗ) и заданиях по безопасности (ЗБ).

Профили защиты являются дальнейшим развитием классов безопасности Оранжевой книги и хорошо известных Руководящих документов (РД) Гостехкомиссии России. Но в отличие от их жесткой классификационной схемы число профилей защиты не ограничено. Они содержат более полный, целенаправленный и обоснованный набор требований безопасности, учитывающий назначение, угрозы безопасности и условия применения объекта оценки (ОО).

Профиль защиты предназначен для сертификации средств защиты информации продуктов и систем информационных технологий (ИТ) и получения сопоставимых оценок их безопасности. Профили защиты служат также основой для разработки разделов требований безопасности информации (заданий по безопасности) в ТЗ (ТТЗ) на конкретные изделия ИТ.

В известном смысле можно утверждать, что профили защиты важнее самого стандарта ISO/IEC 15408. Данный стандарт по сути является метасредством, инструментом, предназначенным для разработки нормативных документов, позволяющих оценивать средства безопасности определенных классов или информационных системы определенного назначения. Предполагается, что именно эти нормативные документы, а не сам стандарт способны найти практическое применение, обеспечить соответствие законодательного и технического аспектов информационной безопасности [59].

Базовый подход к разработке ПЗ предусматривает выполнение следующей последовательности действий:

1. Описание предполагаемой среды, связанной с безопасностью функционирования продукта или системы ИТ:

- существующие угрозы, которым должен противостоять продукт или система ИТ;
- предположения о среде функционирования;
- подлежащие учету правила безопасности, устанавливаемые средой (например, законы, политика безопасности организации).

2. Определение стратегии противостояния каждой угрозе и формулировка соответствующих целей безопасности. Цели должны не только обеспечивать противостояние угрозам, но и быть реалистичными и достижимыми. На этой стадии фактически определяется область действия ПЗ. Цели безопасности следует разделить на цели, достижение которых возлагается на объект оценки; цели, достижение которых возлагается на среду (ИТ или не ИТ), и цели, достижение которых возлагается на объект оценки и среду как единое целое.

3. Использование каталога функциональных требований безопасности из части 2 ОК для спецификации функциональных возможностей, направленных на достижение целей безопасности для продукта/системы ИТ, а также для ИТ-среды. При необходимости в детализации обобщенных требований, определенных в части 2 ОК, следует выполнить разрешенные операции над соответствующими компонентами требований. Если для выражения требо-

ваний безопасности отсутствуют надлежащие компоненты из части 2 ОК, допускается разработка новых компонентов требований, оформленных в подобном компонентам из части 2 ОК стиле.

4. Использование каталога требований доверия к безопасности из части 3 ОК для спецификации компонентов доверия, направленных на обеспечение уровня доверия к безопасности, соответствующего целям безопасности. При этом можно либо использовать один из predetermined пакетов требований доверия, либо разработать новый пакет, либо применить комбинацию этих подходов.

5. Разработка логического обоснования того, что выбранные функциональные компоненты и компоненты доверия к безопасности подходят для противодействия угрозам в предполагаемой среде.

В модели Общих критериев роли оценщиков и органов сертификации разделены. Сертификаты выдаются национальными системами сертификации по результатам оценки, проводимой независимыми оценщиками [59].

Анализ применяемых в указанных стандартах терминов и определений (гарантированности, корректности, адекватности, функциональности, мощности) говорит о весьма приближенном характере их влияния на конечный результат оценки. Их основной недостаток заключается в том, что при проектировании автоматизированной системы разработчик не имеет четких исходных данных и методов расчета, руководствуясь которыми он должен строить систему. Другими словами, процессы проектирования и оценки слабо связаны между собой. При проведении такой оценки в сложных системах может оказаться, что она будет иметь отрицательный результат и потребуются большая доработка автоматизированной системы, затраты на которую разработчиком не учтены. В первой книге [42] и разделе 3 данной книги автором дается подробный анализ этих недостатков.

Из-за отсутствия соответствующей теории и расчетных соотношений в «Оценочных критериях...» не приведены единицы измерения и количественная оценка безопасности информации в автоматизированных системах.

С позиций предлагаемой автором концепции защиты информации критерии оценки безопасности информации, используемые в указанных стандартах, не всегда учитывают или не учитывают совсем следующие данные:

- классификацию объектов обработки и передачи данных;
- классификацию потенциальных угроз, адекватную классификации объектов обработки и передачи данных;
- возможные каналы НСД к информации на объектах обработки и передачи данных;
- деление средств защиты на средства защиты от случайных и преднамеренных НСД, имеющих различные физическую природу, характер воздействия и точки приложения в объекте обработки и передачи данных;
- образование системы взаимосвязанных преград, замыкающихся вокруг предмета защиты и препятствующих обходу преград нарушителем;
- время жизни информации, обнаружения и блокировки НСД;
- ожидаемое время преодоления преграды нарушителем.

Учитывая изложенное, в данном исследовании предложен другой концептуальный подход к построению и оценке защиты в АС, позволяющий ус-

транить указанные выше недостатки. Как было показано выше, вопрос разработки средств защиты от случайных воздействий в достаточной степени решается средствами повышения надежности технических средств и достоверности информации, созданию и оценке которых посвящено много исследований [39, 54, 79, 80]. Поэтому в этой книге считается целесообразным рассмотреть прежде всего вопрос оценки средств защиты от преднамеренного НСД.

7.2. Совершенствование методов оценки уровня безопасности информации в автоматизированных системах

Решение поставленной задачи связано с первоначальными условиями, которые должны быть заданы в техническом задании на АС. Эти условия должны содержать модель ожидаемого поведения нарушителя. Для квалифицированного нарушителя, владеющего информацией о принципах работы и построения АС, возможности более широкие, чем у неквалифицированного, следовательно, при оценке защиты потребуются рассмотреть большее количество ВКНСД, большее количество средств защиты, другого качества с лучшими показателями. Выбор модели поведения нарушителя оказывает существенное влияние на конечный результат оценки безопасности информации в АС. Поэтому в подразд. 3.1 была предложена классификация нарушителей и соответствующая ей классификация уровней безопасности информации:

- I класс – высококвалифицированный нарушитель-профессионал;
- II класс – квалифицированный нарушитель-непрофессионал;
- III класс – неквалифицированный нарушитель-непрофессионал;
- IV класс – недисциплинированный пользователь.

При этом каждому классу нарушителей согласно 3.3, 3.5.2 и 3.6.3 в АС будет соответствовать определенное число возможных каналов несанкционированного доступа.

Для распределенных АС: региональных и глобальных сетей и АСУ из-за их высокой стоимости целесообразна классификация нарушителя только по двум классам: I и II, а для локальных – по I, II, III классам. Входящие в них КСА должны обеспечивать защиту того же класса, а информация, передаваемая по каналам связи, должна быть защищена по тому же классу. При этом согласно 3.6.3 классификация потенциального нарушителя ориентируется на выполнение определенного набора требований к безопасности информации, передаваемой по каналам связи. Распределение этих требований по классам следующее:

I класс – все требования; II класс – все требования, кроме сокрытия факта передачи сообщения; III класс – все требования, кроме сокрытия факта передачи сообщения, гарантированной защиты от ознакомления с ним постороннего лица, гарантированной подлинности принятых и доставленных данных.

Кроме того, для оценки безопасности информации имеет значение исходная позиция нарушителя по отношению к объекту защиты: вне контролируемой территории – является ли нарушитель посторонним лицом или на контролируемой территории; является ли он законным пользователем, относится ли к техническому персоналу, обслуживающему КСА. Если нарушителем становится законный пользователь, то для него не является преградой контрольно-пропускной пункт на территорию объекта защиты, но система контроля доступа в помещения может разрешать доступ ему только в определенное помещение, т.е. оценку уровня безопасности информации необходимо проводить без учета средств контроля доступа на территорию объекта автоматизации. А если в помещении работает много пользователей, – то и без учета системы контроля доступа в это помещение.

Очевидно, что оценка безопасности должна проводиться отдельно для каждого случая. При этом следует учитывать соответствующее количество ВКНСД и средств защиты. В отдельных случаях в будущем возможно придется проводить такую оценку для каждого пользователя.

В качестве исходной предпосылки согласно описанной выше модели потенциального нарушителя принято считать, что нарушителем может быть только один человек, так как защита от организованной группы нарушителей – задача более сложная. Однако на неконтролируемых каналах НСД это не исключается, и расчетные соотношения для оценки прочности соответствующих средств защиты предусмотрены в подразд. 3.4.

Оценка заключается в проверке правильности расчетов прочности защиты на основе соотношений, приведенных в подразд. 3.4, т.е. оценщик и разработчик работают с одними и теми же формулами, позволяющими всесторонне и глубоко исследовать предъявляемую защиту и получить количественные показатели ее прочности. Перед проведением оценки разработчик представляет соответствующий расчет, сделанный в зависимости от вида АС (см. подразд. 3.5.5 или 3.6.6).

Приведенные расчетные соотношения позволяют оценить:

- полноту и правильность определения возможных каналов НСД к информации в предъявленной автоматизированной системе;
- полноту перекрытия возможных каналов НСД и прочность применяемых средств защиты;
- прочность защитной оболочки отдельных комплексов средств автоматизации обработки и передачи информации;
- прочность защиты информации АС в целом.

Оценку уровня безопасности информации предлагается проводить по единому руководящему документу, проект которого представлен в приложении 1. С учетом предложенной концепции и методологии построения защиты оценка уровня безопасности информации в конкретной АС должна проводиться в следующей последовательности:

- 1) анализ вида и состава АС. Если это система с распределенной обработкой данных, проводится сначала оценка АС с сосредоточенной обработкой;
- 2) оценка информации, обрабатываемой АС, на предмет ее ценности, секретности, мест размещения, циркуляции ее потоков и сроков действия;

3) оценка правильности выбора ожидаемой модели потенциального нарушителя на ее соответствие уровню важности информации, подлежащей защите;

4) анализ АС как объекта защиты на предмет наличия в нем максимально возможного числа каналов НСД к информации на объектах ее обработки и несанкционированных действий на линиях и каналах связи, соответствующих ожидаемой модели потенциального нарушителя;

5) проверка наличия реализованных в АС средств защиты по каждому возможному каналу несанкционированного доступа к защищаемой информации и возможных путей их обхода;

6) количественная оценка прочности каждого средства защиты;

7) оценка ожидаемой прочности системы защиты информации в АС в целом.

На начальном этапе освоения РД предлагается оценивать количественные показатели прочности, представляемые в расчете Главного конструктора АС. После накопления определенного опыта предельные значения для уровней безопасности должны быть приведены в РД. Однако уже сейчас, учитывая приблизительный характер оценки и необходимость в гарантированном запасе прочности защиты, можно утверждать, что на неконтролируемых каналах ожидаемое время затрат на преодоление защиты должно превышать время жизни защищаемой информации в десятки раз. Возможно придется установить в этом случае допустимые значения запаса прочности для уровней безопасности I класса не менее 10, для II – не менее 5, для III – не менее 2 раз, т.е. значения показателей прочности некоторых средств защиты будут больше 1. Но при этом необходимо учитывать возможные пути обхода средства защиты, которые могут быть перекрыты другими средствами с меньшими значениями прочности. В этом направлении необходимо провести дополнительные исследования.

ЗАКЛЮЧЕНИЕ

В книге предложено решение актуальной задачи повышения уровня безопасности информации в АС путем изменения действующей концепции и разработки методологии построения защиты на основе защитной оболочки.

Основные результаты:

1. Проведен анализ действующей концепции построения защиты, определены ее недостатки и пути их устранения.

Дан анализ современного состояния решения проблемы безопасности данных в АС. Проведенные исследования в этой области дают возможность сформулировать следующие недостатки действующей концепции создания их защиты, приводящие к снижению уровня безопасности данных в АС:

1) отсутствие четких и ясных определений предмета защиты, а также возможных потенциальных угроз предмету и объекту его обработки;

2) выбор концепции построения защиты, основанной на построении защитной среды, границы и плотность которой носят неопределенный характер;

3) классификации средств защиты по технологии исполнения (аппаратной, программной, физической и т.д.), а не по способности выполнять функции защиты, в результате чего отсутствует их взаимодействие и образуются «дыры» в защите;

4) отсутствие расчетных соотношений и механизма образования замкнутой оболочки защиты и ее прочности;

5) уменьшение роли или полное пренебрежение временными факторами, являющимися ключевыми параметрами защиты: быстродействием обнаружения и блокировки НСД, временем преодоления преграды нарушителем и временем жизни информации;

6) отсутствие расчетных формул для количественной оценки прочности отдельных средств (за исключением криптографических) и защиты информации в АС в целом, что не позволяет разработчику заранее рассчитать уровень безопасности информации в создаваемой системе.

Эти обстоятельства являются также причиной того, что имеющиеся на сегодняшний день стандарты по безопасности информации, несмотря на их большие объемы и количество, неполны, противоречивы и не отражают действительную картину возможных событий.

2. Для устранения перечисленных недостатков разработана новая постановка задачи, заключающаяся в применении следующих исходных положений:

- определении информации как предмета собственности, подлежащего защите;
- анализе видов АС, их классификации и определении с позиций безопасности информации типовых структур в целях разработки совокупности общих решений по созданию механизма защитной оболочки в АС;

- разделении задач защиты информации от случайных воздействий и от преднамеренного доступа;
- разработке модели ожидаемого поведения потенциального нарушителя;
- разработке классификации потенциальных нарушителей.

3. Разработаны *методический подход, принципы построения защиты и расчетные соотношения*, позволяющие спроектировать на научной основе средства защиты данных и получить в АС виртуальную замкнутую *оболочку защиты* с гарантированными значениями ее прочности в *количественном* выражении.

Предлагаемые в книге подход, модель и теория защиты отвечают привычному и понятному всем физическому смыслу, заключающемуся в создании вокруг предмета защиты замкнутой оболочки. Расчетные соотношения даны для прочности отдельных средств и их соединения в последовательную, параллельную и параллельно-последовательную цепь, а также для образования из них защитной оболочки. Благодаря расчетным соотношениям этот принцип удалось сохранить в физическом и виртуальном представлении в системах обработки данных, что позволило подойти с единой мерой к расчету ожидаемой эффективности защиты информации от преднамеренного НСД на любом уровне ее обработки: от персонального компьютера до глобальных АС в целом.

Использование в расчете прочности защиты временного фактора представляется более удачным, чем фактор стоимости. Известно, что оценка стоимости информации может быть весьма приблизительной, и в настоящее время практических методик для этого не существует. Для больших систем подобная оценка, учитывая динамику цены обрабатываемой информации, вообще вряд ли целесообразна. Известно, что временной фактор уже используется при оценке стойкости криптографических средств защиты, что говорит в пользу принятого решения. В результате получаем возможность применения общей для всех средств защиты одной широко известной единицы измерения – вероятности наступления события.

4. Разработаны *методы построения защиты информации* для различных видов АС.

На примерах типовых объектов исследования предложены определение в автоматизированных системах возможных каналов НСД к информации, выбор средств, их перекрывающих, и средств управления, объединяющих их в единый механизм – систему безопасности информации, а также методика оценки ожидаемой прочности защиты, что позволяет определить уровень безопасности в конкретной АС и задать соответствующие показатели в техническом задании на системы подобного рода в будущем.

Объединение средств защиты с помощью специальных средств централизованного контроля и управления позволяет создать на пути нарушителя и случайных воздействий строгую и управляемую систему равнопрочных и взаимосвязанных преград, отвечающих заданным требованиям по уровню безопасности обрабатываемой информации.

Предложенная автором концепция безопасности информации позволяет:

- обозначить предмет защиты, сосредоточить усилия на его защите и устранить избыточность применяемых средств защиты;

• провести всесторонний анализ разрабатываемой автоматизированной системы на предмет выявления возможных каналов НСД к информации в соответствии с заданной моделью поведения потенциального нарушителя;

• выбрать готовые и разработать на основе предлагаемых расчетных соотношений новые средства защиты с получением гарантированных показателей их прочности;

• создать научно обоснованную замкнутую оболочку защиты с гарантированными показателями ее прочности;

• применить единые для всех АС методы и расчетные соотношения для построения и расчета прочности защиты информации от НСД;

• сократить количество экспертных оценок эффективности средств и систем защиты, а также упростить их методику;

• на основе более точных расчетов прочности средств защиты и создания защитной оболочки получить значительное повышение уровня безопасности информации в разрабатываемых АС независимо от выбранных аппаратных и программных платформ.

Кроме того, предложенная в книге классификация автоматизированных систем может быть использована не только в целях обеспечения безопасности данных, но и для решения других задач при их проектировании.

Ожидаемая экономическая эффективность применения методов выражается в следующем:

• значительном сокращении возможных потерь за счет повышения уровня прочности защиты;

• сокращении сроков разработки систем безопасности информации за счет определенности постановки задачи и применения простых положений и расчетных соотношений для ее решения;

• сокращении времени сертификации изделий за счет уменьшения количества критериев оценки и экспертных оценок, а также упрощения методик оценки.

В случае если предложенные в данной работе концепция, теория, методы и принципы построения защиты информации в АС станут общепринятыми, открываются возможности для решения следующих задач разработки:

• единого информационного и лингвистического обеспечения системы безопасности информации в АС;

• направлений унификации и стандартизации методов и средств защиты информации;

• методов сертификации АС в интересах определения в них гарантированного уровня безопасности данных;

• типовых требований к аппаратуре, программному обеспечению и организационным мероприятиям для обеспечения в АС необходимой безопасности информации.

Изложенное выше, по мнению автора, позволяет надеяться на то, что в условиях бурно развивающейся информатизации нашего общества данные исследования внесут весомый вклад в решение проблемы повышения уровня безопасности информации в автоматизированных системах ее хранения, обработки и передачи.

ПРИЛОЖЕНИЕ 1

РУКОВОДЯЩИЙ ДОКУМЕНТ «АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ ОБРАБОТКИ И ПЕРЕДАЧИ ДАННЫХ»

СИСТЕМА БЕЗОПАСНОСТИ ИНФОРМАЦИИ

(Проект)

СОДЕРЖАНИЕ

Введение

1. Концепция построения системы безопасности информации в АС.
2. Требования к тактико-техническому заданию на АС по обеспечению безопасности информации.
3. Требования к обеспечению безопасности информации при проведении ОКР, изготовлении и испытаниях АС.
4. Общие требования к построению системы безопасности информации АС.
5. Специальные требования к средствам защиты информации для АС I класса.
6. Требования к средствам централизованного контроля и управления защитой.
7. Состав эксплуатационной документации на систему безопасности информации АС.
8. Выходные показатели оценки ожидаемой эффективности защиты информации в АС.
9. Порядок сертификации систем безопасности информации автоматизированных систем.
10. Требования к поставке и сдаче АС на объекты заказчика.

ВВЕДЕНИЕ

Настоящий документ предназначен для руководства при создании и сертификации систем и средств обеспечения безопасности информации в автоматизированных системах (АС) ввода/вывода, хранения, обработки и передачи данных.

Документ определяет единые нормативные требования и рекомендации по обеспечению гарантированной защиты данных от несанкционированного доступа на всех этапах жизненного цикла АС, включая единую классификацию уровней обеспечения безопасности в соответствии с важностью обрабатываемой информации.

Данный документ является руководством для разработчиков АС, заказчиков, испытательных лабораторий и центров, уполномоченных проводить сертификацию АС.

Данный документ заменяет:

Руководящий документ. Концепция защиты СВТ и АС от НСД к информации. – М.: Гостехкомиссия России, 1992.

Руководящий документ. Защита от НСД к информации. Термины и определения. – М.: Гостехкомиссия России, 1992.

Руководящий документ. Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации. – М.: Гостехкомиссия России, 1992.

ГОСТ Р 50739–95. СВТ. Защита от НСД. Общие технические требования.

ГОСТ Р 50922–96. Защита информации. Основные требования и определения. Категорирование важности информации.

ГОСТ Р 51275–99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

Потребуется доработки ГОСТ Р 51583–2000. Защита информации. Порядок создания АС в защищенном исполнении. Общие положения.

Термины и определения в документе даны в редакции книги: Мельников В.В. Безопасность информации в автоматизированных системах. – М.: Финансы и статистика, 2003.

1. КОНЦЕПЦИЯ ПОСТРОЕНИЯ СИСТЕМЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В АС

1.1. Концепция построения системы безопасности в АС включает постановку задачи, концептуальный подход, основные направления и принципы ее решения.

Предметом защиты в АС является информация. Ресурсы АС защищаются только тогда, когда информацию непосредственно защитить сложно, и только те, через которые возможен доступ к информации, а также те, несанкционированный доступ к которым отрицательно влияет на право собственника или его доверенного лица беспрепятственно работать со своей информацией (юридическую ответственность за информацию и за ресурсы, как правило, несут разные должностные лица).

Примечание. Право собственности государства на обрабатываемую в АС информацию передается должностным лицам-пользователям в рамках полномочий, данных им государственной организацией – владельцем АС в соответствии с функциональными обязанностями и иерархией их отношений.

Критериями при принятии решения о защите являются право владения и важность информации.

1.2. Рекомендуются следующая классификация информации по ее важности:

1) **жизненно важная** незаменимая информация, наличие которой необходимо для функционирования организации, утечка, модификация или утрата которой связана с существованием организации;

2) **важная** информация – информация, которая может быть заменена или восстановлена, но процесс восстановления очень труден и связан с большими затратами, утечка, модификация или утрата которой могут привести к большим потерям в организации;

3) **полезная** информация – информация, которая используется в работе, которую при утрате трудно восстановить, а также утечка, модификация или утрата которой существенно не влияет на функционирование организации;

4) **несущественная** информация – информация, не представляющая серьезного интереса для нарушителей, но ее утрата не желательна для ее владельца.

1.3. Перед проектированием системы должны быть известны перечень, важность (цена), время жизни, владельцы (или ответственные должностные лица), места сосредоточения и циркуляции в ней сведений, подлежащих защите.

1.4. В качестве объектов обработки и передачи информации рассматриваются типовые виды АС по нижеследующей классификации.

Автоматизированное рабочее место (АРМ) – работающая автономно или в составе вычислительной сети или вычислительного комплекса автоматизированная система, представляющая собой персональную ЭВМ с прикладными программами или специально разработанный аппаратно-программный комплекс, построенный на базе стандартных вычислительных блоков и нестандартного прикладного программного обеспечения.

Рабочая станция (РС) – работающая в составе вычислительной сети или вычислительного комплекса стандартная персональная ЭВМ с сетевым аппаратным и программным обеспечением, а также пакетом прикладных программ.

Информационно-вычислительный комплекс (ИВК) – автоматизированная система, состоящая из мощного универсального вычислителя с централизованной обработкой данных и внешних устройств, в числе которых могут быть РС, АРМ, принтеры, табло отображения и т.д.

Локальная вычислительная сеть (ЛВС) – автоматизированная система, состоящая из группы РС (АРМ) и вспомогательных технических средств (серверов, общего принтера, коммутатора и др.), соединенных между собой линиями связи и объединенных сетевым аппаратным и программным обеспечением в целях выполнения общей задачи.

Комплекс средств автоматизации (КСА) – территориально сосредоточенная или распределенная автономная или являющаяся элементом региональной или глобальной вычислительной сети (АСУ) автоматизированная система, состоящая из одного или нескольких объединенных линиями связи и общими задачами вышеуказанных видов АС: АРМ, РС, ИВК, ЛВС.

Телекоммуникационная вычислительная сеть (ТВС) – территориально-распределенная региональная или глобальная вычислительная сеть, состоящая из нескольких узлов коммутации, выполняющих задачи маршрутизации сообщений, каналов связи между ними и аппаратуры передачи данных комплексов средств автоматизации, являющихся ее абонентами. Данная сеть выполняет услуги по обмену данными и предоставлению своих данных.

Сеть передачи данных (СПД) – территориально распределенная региональная или глобальная вычислительная сеть, состоящая из одного или нескольких узлов коммутации, выполняющих задачи маршрутизации сообщений, каналов связи между ними и аппаратуры передачи данных КСА, являющиеся одновременно ее абонентами и элементами АСУ.

Автоматизированная система управления (АСУ), или корпоративная вычислительная сеть, – территориально распределенная региональная или глобальная вычислительная структура, состоящая из сети передачи данных и ее абонентов – КСА с иерархической системой отношений. В глобальную АСУ может входить несколько региональных.

Данные виды АС могут быть не только законченными самостоятельными структурами, способными выполнять свои задачи, но и быть элементами более сложной АС. Кроме того, в состав АС с распределенной обработкой данных в зависимости от выполняемых задач может входить группа не имеющих самостоятельного применения вспомогательных технических средств с автоматической обработкой данных:

- вычислительные комплексы (комплекс ЭВМ без внешних устройств);
- серверы;
- табло коллективного пользования;
- аппаратура передачи данных, модемы;
- коммутаторы;
- концентраторы;
- маршрутизаторы;
- мосты;
- шлюзы и другие подобные технические средства.

Перечисленные технические средства во время нормального функционирования АС не требуют вмешательства человека. Поэтому с позиций безопасности

информации достаточно того, что доступ к ним (кроме табло) будет закрыт механически корпусом и крышками с датчиками вскрытия, находящимися под централизованным контролем службы безопасности. В технических средствах, имеющих дистанционное управление, в ответственных АС рекомендуется его отключить. Среди них с позиций безопасности информации необходимо выделить вычислительные комплексы, серверы и табло.

Вычислительные комплексы могут решать некоторое множество специальных функциональных задач. Серверы являются накопителями больших объемов данных различного назначения и важности. С вычислительными комплексами и серверами может работать некоторое множество пользователей, обращаясь к ним по линиям связи, что потребует создания на программном уровне соответствующей системы контроля и разграничения доступа. Табло по определению является средством коллективного отображения информации, доступ к которой может быть ограничен только отдельным помещением.

1.5. Потенциальные угрозы информации определяются условиями сохранения права собственности на нее. Если защита отсутствует, то могут произойти утечка, модификация и (или) утрата информации. При этом под *утечкой* информации понимается несанкционированное ознакомление с ней постороннего лица; под *модификацией* – несанкционированное изменение информации на корректную по форме и содержанию, но другую по смыслу; под *утратой* – хищение, искажение с потерей смысла, уничтожение, недоведение информации до адресата или блокировка доступа к ней ее владельца или его доверенного лица.

Все остальные угрозы – способы достижения целей, которые в конечном итоге сводятся к этим трем событиям. Эти события могут произойти *случайно* по причине ошибок пользователя, сбоев или отказов аппаратуры, алгоритмических или программных ошибок, аварийных ситуаций, стихийных бедствий и т.д. или созданы нарушителем преднамеренно. Техника исполнения вторжений последним имеет множество вариантов.

1.6. Случайные воздействия (см. выше) возможны в любой точке системы, т.е. на всей ее «площади». Время их наступления определяется законами случайных чисел. Средства защиты от них связаны с обеспечением надежности функционирования АС по ГОСТам:

ГОСТ 24.701–86. Надежность автоматизированных систем управления. Основные положения;

ГОСТ 27.002–89. Надежность в технике. Основные показания. Термины и определения;

ГОСТ 27301–95. Надежность в технике. Расчет надежности. Основные положения;

ГОСТ 27.310–95. Надежность в технике. Анализ видов, последствий и критичности отказов. Основные положения.

Методы оценки эффективности средств контроля отказов аппаратуры регулируются отраслевым стандартом.

1.7. Преднамеренные действия человека-нарушителя начинаются на «периметре» системы. Под «периметром» АС понимается ее внешняя физическая оболочка, элементами которой являются корпуса, крышки, дверцы, свободные внешние соединители технических средств, средства управления, отображения, печати, ввода и вывода, носители информации, кабельные соединения, каналы и линии связи.

1.8. Нарушением считается попытка доступа к любой части информации, подлежащей защите. Предсказать время и характер возможных действий нарушителя невозможно. Поэтому целесообразно предположить наиболее опасную для системы *модель его возможного поведения*:

- а) нарушитель может появиться в любое время и в любой точке «периметра» системы;
- б) для достижения своей цели он выберет наиболее слабое звено в защите;
- в) квалификация и осведомленность нарушителя будет соответствовать важности защищаемой информации;
- г) постоянно хранимая информация о принципах работы системы, включая секретную, нарушителю известна;
- д) нарушителем может быть не только постороннее лицо, но и законный пользователь системы;
- е) нарушитель действует в единственном числе; однако нарушителей может быть несколько, но их действия не согласованы между собой.

Примечание. На неконтролируемых средствах хранения и передачи данных возможны действия организованной группы нарушителей.

Из данных условий вытекают следующие *исходные положения*. Согласно п. «а» вокруг предмета защиты необходимо строить замкнутую оболочку (контур) защиты.

Согласно п. «б» прочность защиты должна определяться ее слабым звеном.

Согласно п. «в» прочность защиты должна соответствовать квалификации потенциального нарушителя.

Согласно п. «г» информация для входа в систему должна быть не только закрытой, но и изменяемой.

Согласно п. «д» при наличии некоторого множества пользователей необходимо обеспечить разграничение доступа.

Согласно п. «е» в расчете прочности защиты должны быть учтены количество и возможное взаимодействие нарушителей.

1.9. Однако для различной по назначению, виду и ценности обрабатываемой информации в АС «опасная» квалификация потенциального нарушителя будет также отличаться.

В выборе исходной модели потенциального нарушителя целесообразен дифференцированный подход в соответствии с назначением АС и ценностью информации, обрабатываемой в ней. Поскольку модель нарушителя – понятие относительное и приближенное, рекомендуется за основу принять четыре класса потенциальных нарушителей:

- 1) высококвалифицированный нарушитель-профессионал (специалист по вычислительной технике, специально подготовленный к НСД к информации);
- 2) квалифицированный нарушитель-непрофессионал (специалист по вычислительной технике, не подготовленный к НСД к информации);
- 3) неквалифицированный нарушитель-непрофессионал;
- 4) прочие нарушители.

В соответствии с данной классификацией и классификацией информации по степени важности рекомендуется ввести классификацию уровней безопасности информации в создаваемых АС.

I класс – рекомендуется для защиты жизненно важной информации. Прочность ее защиты должна быть рассчитана на нарушителя-профессионала.

II класс – рекомендуется использовать для защиты важной информации, Прочность ее защиты должна быть рассчитана на нарушителя высокой квалификации, но не на взломщика-профессионала.

III класс – рекомендуется для защиты относительно ценной информации, утечка, модификация или утрата которой может привести к незначительным потерям для ее владельца или постоянный несанкционированный доступ к которой путем ее накопления может привести к утечке и более ценной информации. Прочность защиты при этом должна быть рассчитана на относительно квалифицированно-го нарушителя-непрофессионала.

IV класс – рекомендуется для защиты прочей информации, не представляющей интереса для серьезных нарушителей. Однако необходимость его диктуется соблюдением технологической дисциплины учета и обработки информации служебного пользования в целях защиты от случайных нарушений и подстраховки от случаев преднамеренных НСД.

1.10. Безопасность информации в АС заключается в создании условий ее ввода(вывода), хранения, обработки и передачи, при которых обеспечивается защита от ее утечки, модификации и утраты, а также гарантируется свободный доступ к ней ее владельца или его доверенного лица.

1.11. Стратегия и тактика при построении защиты заключается в применении на возможных каналах НСД к информации средств контроля и предупреждения событий. При этом средства **контроля** устанавливаются на каналах, технически или организационно позволяющих это реализовать, а **средства предупреждения** устанавливаются на каналах, выходящих за пределы возможностей контроля событий.

1.12. Средства контроля должны обеспечивать **периодичность контроля и время передачи** сигнала НСД на АРМ СБ в сумме, меньшей ожидаемого времени, затрачиваемого нарушителем на НСД. В случаях обратного соотношения стойкость данного средства защиты определяется вероятностной величиной.

1.13. Средства предупреждения должны обеспечивать такую стойкость, при которой ожидаемые затраты времени на преодоление ее нарушителем больше времени **жизни** защищаемой информации. В случаях обратного соотношения стойкость определяется вероятностной величиной.

1.14. Величина вероятности непреодоления нарушителем средства защиты в течение времени его эксплуатации называется **прочностью защиты**.

1.15. Реализация заданных уровней безопасности должна обеспечиваться совокупностью средств защиты, перекрывающих возможные каналы НСД в АС со стороны ее «периметра» в количестве, соответствующем ожидаемой модели поведения потенциального нарушителя. Данная совокупность средств, связанных расчетными соотношениями прочности, должна образовать виртуальную оболочку защиты. Уровень безопасности защиты внутри класса должен обеспечиваться количественной оценкой прочности защитного контура (оболочки).

1.16. Модель защиты информации АС должна соответствовать рис. 3.2. В модели представлены КСА, соединенные каналами связи, и технические средства, соединенные линиями связи. Первый вариант представляет собой фрагмент структуры глобальной (региональной) АС, второй – локальной вычислительной сети.

Средства защиты информации в автоматизированной системе без каналов (линий связи) образуют одну защитную оболочку, в каналах связи (линиях связи) – другую.

2. ТРЕБОВАНИЯ К ТАКТИКО-ТЕХНИЧЕСКОМУ ЗАДАНИЮ НА АС ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

2.1. ТТЗ должно содержать перечень, возможные места сосредоточения, гриф секретности и время действия сведений и характеристик АС, подлежащих защите на каждой стадии ее жизненного цикла: проектирования, изготовления, испытаниях, эксплуатации и завершения последней.

2.2. При проектировании региональных и глобальных АС должны быть указаны каналы связи, используемые для передачи охраняемой информации с приведением данных по п. 2.1.

2.3. Требования к средствам защиты и к уровню безопасности информации должны содержать соответствующие требования настоящего РД и не противоречить им. Общий уровень безопасности информации (I, II, III класс) АС с распределенной обработкой данных задается только для АС с одинаковой степенью важности информации, обрабатываемой на ее элементах.

При задании уровней безопасности информации в сложных АС: КСА, ТВС, АСУ – может оказаться, что ценная информация распределена неравномерно (например, в КСА ее содержит только ВК или одна из ЛВС, в АСУ – КСА только верхнего уровня). Тогда в техническом задании на АС, кроме общих, допускается с соответствующим обоснованием приводить отдельные показатели уровня безопасности на ее составные части. На СПД в силу равнозначности ее КСА (узлов коммутации) данное допущение не распространяется (на разные СПД, соединенные между собой мостом, требования к безопасности могут отличаться между собой, взаимодействие между ними в этом случае выполняется по согласованному протоколу и закрепляется соответствующим соглашением с использованием межсетевого экрана).

3. ТРЕБОВАНИЯ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ ОКР, ИЗГОТОВЛЕНИИ И ИСПЫТАНИЯХ АС

3.1. Перечень сведений и характеристик АС, подлежащих защите на предприятии – разработчике и изготовителе, должен быть задан в ТТЗ в соответствии с важностью выполняемых ею задач.

3.2. Возможные каналы НСД к информации АС на предприятии – разработчике и изготовителе определяются в плане мероприятий по обеспечению режима секретности в соответствии с важностью циркулирующей при проведении работ информацией п 3.1. Например, к ним можно отнести:

- людей;
- документы: машинные и бумажные;
- средства связи: мобильную связь, АТС местную и городскую;
- линии и каналы связи при проведении испытаний АС;
- акустические и визуальные каналы;
- радиоканалы;
- ПЭМИН и т.д.

3.3. Мероприятия по ОБИ АС на предприятии – разработчике и изготовителе.

3.3.1. Создание на предприятии режима секретности с обеспечением ограничения и разграничения доступа и проведение организационно-технических мероприятий по защите от утечки информации по акустическим и визуальным каналам, радиоканалам и каналам ПЭМИН.

3.3.2. Мероприятия должны также обеспечивать защиту от программных и аппаратных закладок в аппаратуру и ПО создаваемых АС. В законченной и годной к эксплуатации автоматизированной системе обработки информации *должны отсутствовать средства программирования и отладочные средства* за исключением тестовых программ, предусмотренных конструкторской документацией на эту систему.

3.3.3. Приемно-сдаточные испытания системы безопасности информации должны проводиться по отдельной программе и методике одновременно с приемно-сдаточными испытаниями АС в целом.

4. ОБЩИЕ ТРЕБОВАНИЯ К ПОСТРОЕНИЮ СИСТЕМЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ АС

4.1. Вид АС определяется по результатам анализа ее состава и структуры на соответствие определениям п. 1.4. В случае создания АС с распределенной обработкой данных распределение информации по степени важности определяется в результате анализа ее структурной схемы и ее элементов: КСА (ТС), каналов (линий) связи.

4.2. В соответствии с важностью обрабатываемой информации определяется класс модели ожидаемого поведения нарушителя и требуемый уровень безопасности данных в создаваемой АС (если он не задан в ТТЗ).

4.3. Возможные каналы НСД к информации АС и ее элементов, а также соответствующие средства защиты определяются по табл. 1П.

Таблица 1П

Возможные каналы НСД в АС					Рекомендуемые средства защиты и класс защиты	
Вид АС и возможные каналы НСД к ее информации	Привлекаемые каналы согласно классу БИ				Наименование средства защиты	Класс защиты
	I	II	III	IV		
1. РС (АРМ):						
1) клавиатура;	+	+	+	+	Пароль начальной загрузки BIOS.	III, IV
2) «мышь»;					Программа контроля и разграничения доступа операционной системы.	I-III
3) сканер;					Программно-аппаратные средства контроля доступа в систему на уровне BIOS.	I, II
					Съемный ЖМД, убираемый в сейф.	I
					Шифрование информации на логических дисках.	
4) монитор;	+	+	-	-	Средства ограничения доступа на территорию объекта автоматизации.	I-III
5) принтер;					Система контроля и разграничения доступа в помещения объекта автоматизации.	I, II
6) плоттер;						
7) графопостроитель;					Отдельное помещение с контролируемым доступом.	I

Продолжение

Возможные каналы НСД в АС					Рекомендуемые средства защиты и класс защиты	
Вид АС и возможные каналы НСД к ее информации	Привлекаемые каналы согласно классу БИ				Наименование средства защиты	Класс защиты
	I	II	III	IV		
8) дисковод;	+	+	+	-	Маркировка ГМД. Электронная идентификация ГМД. Крышка с замком. Применение ПЭВМ без дисковода. Антивирусные средства. Контроль целостности ПО. Пароль начальной загрузки BIOS.	I-IV I-III I-II I I-IV I-IV II, III
9) ГМД, стриммер;	+	+	+	-	Учет и регистрация. Маркировка. Электронная идентификация. Хранение в металлическом шкафу с замком. Хранение в сейфе.	I-IV I-IV I-II II-III I
10) ЖМД с остатками информации;	+	+	-	-	Стирание остатков информации. Наложение на остатки информации случайных чисел. Уничтожение ЖМД с остатками информации. Шифрование данных.	II I I I
11) внутренний монтаж;	+	+	+	-	Контроль вскрытия аппаратуры: • опечатывание кожуха системного блока; • установка механического замка на его кожух; • установка датчика вскрытия	III II I
12) ПЭМИН;	+	-	-	-	Средства уменьшения и зашумления сигналов, экранирование.	I
13) отходы носителей с остаточной информацией;	+	+	-	-	Учет и регистрация носителей. Стирание остатков информации. Уничтожение остатков информации. Шифрование данных. Уничтожение носителей.	I-IV I-II I I I
14) бумажные документы;	+	+	-	-	Учет и регистрация. Хранение в металлическом шкафу с замком. Хранение в сейфе.	I-IV II I
15) машинные носители с рабочей информацией или ПО;	+	+	+	+	Учет и регистрация носителей. Контроль целостности данных. Шифрование данных.	I-IV I-IV I
16) операционная система (нарушение полномочий штатным пользователем);	+	+	+	-	Контроль целостности ПО. Программа контроля разграничения доступа.	I-IV I-III
17) штатный вход законного пользователя в систему.	+	+	+	+	Имя, условный номер и пароль должностного лица, набираемые на клавиатуре. Сочетание ручного набора и размещения части пароля на физическом носителе.	II-IV I

Продолжение

Возможные каналы НСД в АС				Рекомендуемые средства защиты и класс защиты		
Вид АС и возможные каналы НСД к ее информации	Привлекаемые каналы согласно классу БИ				Наименование средства защиты	Класс защиты
	I	II	III	IV		
2. Информационно-вычислительный комплекс			Примечания: а) III и IV классы не рекомендуются б) Размещается в 1-3 помещениях			
1) ВК НСД РС (АРМ);			См. п.1			
2) ВК НСД ВК: • средства управления системного оператора; • технологические пульты и органы управления; • средства загрузки ПО;	+	+	Контроль вскрытия аппаратуры: • опечатывание крышек и дверей аппаратуры; • установка датчиков вскрытия.			I-III I, II
3) средства коллективного отображения информации;	+	+	Средства ограничения доступа на территорию объекта автоматизации. Система контроля и разграничения доступа в помещения объекта автоматизации.			I, II I, II
4) блоки электропитания;	+	+	Контроль вскрытия аппаратуры.			I, II
5) ремонтируемые ТС;	+	+	Система контроля вскрытия аппаратуры ТС. Система контроля рабочей конфигурации АС. Средства контроля отсутствия остатков информации.			I, II I, II I
6) машинные носители информации;	+	+	Учет и регистрация носителей. Контроль целостности данных. Шифрование данных. Электронная идентификация носителей.			I, II I, II I, II I
7) внутренний монтаж аппаратуры технических средств;	+	+	Система контроля вскрытия аппаратуры ТС. Система контроля рабочей конфигурации АС.			I, II I
8) линии связи между техническими средствами;	+	+	Размещение в отдельном помещении. Система контроля вскрытия аппаратуры ТС. Система контроля рабочей конфигурации АС.			I, II I, II I
9) ПЭМИН;	+	-	Средства уменьшения и зашумления сигналов. Экранирование помещений. Сокращение коммуникаций, выходящих за пределы контролируемого помещения.			I I I
10) отходы носителей с остаточной информацией;	+	+	Учет и регистрация носителей. Стирание остатков информации. Уничтожение остатков информации путем наложения последовательности случайных чисел. Шифрование данных. Уничтожение носителей.			I, II I, II I, II I, II I

Продолжение

Возможные каналы НСД в АС				Рекомендуемые средства защиты и класс защиты		
Вид АС и возможные каналы НСД к ее информации	Привлекаемые каналы согласно классу БИ				Наименование средства защиты	Класс защиты
	I	II	III	IV		
1) бумажные документы.	+	+	Учет и регистрация. Хранение в металлическом шкафу с замком. Хранение в сейфе.			I, II II I
3. Локальная вычислительная сеть:	I	II	III			
1) ВК НСД РС (АРМ);				См. п.1		
2) ВК НСД сервера: • средства управления системного оператора; • средства загрузки ПО; • доступ со стороны линий связи; • законный вход пользователя в систему по линиям связи;	+	+	+	Отдельное помещение с охранной сигнализацией. Система контроля вскрытия аппаратуры ТС. Программа контроля и разграничения доступа к ПО и информации. Идентификация пользователя и РС. Система аутентификации пользователя и РС.		
3) табло коллективного отображения информации;	+	+	-	Средства ограничения доступа на территорию объекта автоматизации. Система контроля и разграничения доступа в помещения объекта автоматизации. Отдельное помещение с контролируемым доступом.		
4) ремонтируемые технические средства;	+	+	-	Система контроля вскрытия аппаратуры ТС. Система контроля рабочей конфигурации АС. Средства контроля отсутствия остатков информации.		
5) ПЭМИН;	+	-	-	Средства уменьшения и зашумления сигналов. Экранирование помещений. Сокращение коммуникаций, выходящих за пределы контролируемой территории.		
6) внутренний монтаж технических средств автоматической обработки информации: табло коллективного пользования, аппаратуры передачи данных, модемов, коммутаторов, концентраторов;	+	+	-	Система контроля вскрытия аппаратуры ТС.		

Продолжение

Возможные каналы НСД в АС		Рекомендуемые средства защиты и класс защиты			
Вид АС и возможные каналы НСД к ее информации	Привлекаемые каналы согласно классу БИ				Класс защиты
	I	II	III	IV	
7) линии связи. Возможные не-санкционированные действия:					
а) чтение содержания сообщения;	+	+	-		Шифрование содержания сообщения. I, II
б) переадресация сообщения и посылка ложного сообщения;	+	-	-		Цифровая подпись отправителем адреса получателя одновременно с содержательной частью. I
в) удаление сообщения;	+	-	-		Контроль через заданный интервал времени факта доставки по квитанции о получении сообщения адресатом, подписанной его цифровой подписью. I
г) обращения законных пользователей к ТС, ему не разрешенных;	+	-	-		Аутентификация пользователей по одноразовому сетевому паролю. I, II
д) чтение и подбор сетевого пароля пользователя;	+	+	-		Применение одноразового пароля заданной стойкости с ограничением количества попыток входа в систему. I, II
е) нарушение законным пользователем своих полномочий в сети;	+	+	-		Программа контроля и разграничения доступа к ПО и информации ТС. I, II
8) несанкционированный доступ со стороны каналов связи;	+	+	-		Межсетевой экран. I, II
9) система электропитания.	+	-	-		Контроль вскрытия ТС. I
4. КСА:					
1) ВК НСД РС;					см. п. 1
2) ВК НСД АРМ;					см. п. 1
3) ВК НСД ИВК;					см. п. 2
4) ВК НСД ЛВС;					см. п. 3
5) линии связи;					см. п. 3.7
6) система электропитания	+	-	-		Система контроля вскрытия ТС. Контроль доступа в помещение. I, II, III
7) несанкционированный доступ со стороны каналов связи.	+	+	-		Межсетевой экран. I, II
5. АСУ (СПД, ТВС):	I кл.		II кл.		
1) ВК НСД КСА;					см. п. 4
2) ВК НСД УК;					см. п. 4

Продолжение

Возможные каналы НСД в АС		Рекомендуемые средства защиты и класс защиты			
Вид АС и возможные каналы НСД к ее информации	Привлекаемые каналы согласно классу БИ				Класс защиты
	I	II	III	IV	
3) каналы связи. Возможные не-санкционированные действия:					
чтение содержания сообщения;	+	+			Шифрование содержания сообщения. I, II
переадресация сообщения посылка ложного сообщения;	+	+			Цифровая подпись отправителем адреса получателя одновременно с содержательной частью. I, II
удаление сообщения;	+	+			Контроль через заданный интервал времени факта доставки по квитанции о получении сообщения адресатом, подписанной его цифровой подписью. I, II
обращения законных пользователей к КСА, ему не разрешенных;	+	+			Аутентификация пользователей по одноразовому сетевому паролю. Межсетевой экран. I, II
подбор сетевого пароля пользователя;	+	+			Применение одноразового пароля заданной стойкости с ограничением количества попыток входа в систему. I, II
нарушение законным пользователем своих полномочий в сети;	+	-			Программа контроля и разграничения доступа к ПО и информации КСА. I
дублирование и переупорядочивание сообщений;	+	-			Шифрование даты и времени отправления сообщения вместе с его содержательной частью. II
задержка сообщения;	+	+			Контроль через заданный интервал времени факта доставки по квитанции о получении сообщения адресатом, подписанной его цифровой подписью. I, II
анализ трафика;	+	-			Специальные средства заполнения потока. I
отказ отправителя от собственного сообщения и получателя от принятого;	+	+			Регистрация третьей стороной сообщений, подписанных цифровой подписью. I, II
загрузка сети информационным мусором;	+	-			Межсетевой экран. I
несанкционированный доступ через мост со стороны посторонней сети.	+	-			Межсетевой экран. I

Примечания: 1. Знак «+» обозначает наличие, знак «-» — отсутствие канала.

2. Защитные оболочки линий и каналов связи строятся отдельно.

3. При отсутствии в составе АС некоторых входящих элементов, перечисленных в таблице, соответствующие им каналы НСД не учитываются.

4.4. Конкретные средства защиты выбираются разработчиком АС. При выборе средств защиты определяются технические возможности контроля каналов НСД к информации и несанкционированных действий по отношению к кадру, передаваемому по линиям и каналам связи АС. В соответствии с данным признаком средства защиты делятся на контролирурующие и превентивные. Группа средств защиты по каждому признаку образует свою защитную оболочку. Для каждой из них определяется показатель ее прочности.

Кроме того, необходимо учитывать возможность перекрытия одного канала несколькими преградами в трех случаях:

- когда одной преграды недостаточно для перекрытия одного канала (существуют пути ее обхода);
- прочность одной преграды не отвечает заданным требованиям;
- прочность преграды увеличивается за счет расширенного действия средств защиты другого канала (например, системы контроля доступа в помещения объекта автоматизации).

4.5. Прочность средства защиты (преграды) с возможностью контроля преднамеренного НСД определяется выражением

$$P_k = \min \{P_{обл} (1-P_{отк}), (1-P_{обх1}), (1-P_{обх2}), \dots, (1-P_{обхn})\}, \quad (1)$$

где $P_{обл} = \frac{t_{нр}}{T_{обл}}$ – вероятность обнаружения НСД при $t_{нр} < T_{обл}$;

- $t_{нр}$ – время, необходимое нарушителю на преодоление преграды;
- $T_{обл}$ – время обнаружения и блокировки НСД, равное сумме времени доведения сообщения о НСД от момента фиксации события датчиком обнаружения до момента отображения сообщения на терминале оператора службы безопасности и времени блокировки действий нарушителя;
- $P_{отк}$ – вероятность отказа технических средств, составляющих преграду;
- $P_{обх}$ – вероятность обхода преграды по одному, второму, третьему и т.д. пути, характерным для данной технической реализации преграды, определяется методом экспертных оценок;
- n – число возможных путей обхода данной преграды.

4.6. Прочность преграды с отсутствием технической возможности контроля преднамеренного НСД одним нарушителем определяется выражением

$$P_{нк} = \min \{(1-P_{нр}), (1-P_{обх1}), (1-P_{обх2}), \dots, (1-P_{обхn})\}, \quad (2)$$

- где $P_{нр}$ – вероятность преодоления неконтролируемой преграды нарушителем за время, меньшее времени жизни информации;
- $P_{обх}$ – вероятность обхода преграды по одному, второму, третьему и т.д. пути, характерному для данной технической реализации преграды.

4.7. На неконтролируемых каналах вероятнее всего будет действовать организованная группа нарушителей. Тогда формула (2) приобретает вид

$$P_{нк} = (1-P_{нр}) (1-P_{обх1}) (1-P_{обх2}) \dots (1-P_{обхn}), \quad (3)$$

- где $P_{нр} = 1 - \frac{t_{нр}}{t_{ж}}$ – вероятность преодоления преграды нарушителем при $t_{нр} < t_{ж}$;
- $t_{ж}$ – время жизни защищаемой информации.

Поскольку точные значения данных параметров получить трудно на практике, чтобы гарантировать этот результат, в данном случае используются криптографические преобразования информации, значительно увеличивающие время, необходимое нарушителю для преодоления преграды, по отношению к времени жизни информации.

4.8. Создаваемые преграды вокруг предмета защиты должны составлять замкнутую оболочку (контур), прочность которой при защите от нарушителя в единственном числе определяется значением прочности наиболее слабого звена. Если несколько последовательно соединенных и образующих замкнутую оболочку (контур) контролируемых преград имеют прочность $P_{к1}, P_{к2}, P_{к3}, \dots, P_{кn}$, то прочность защитной оболочки (контура) будет определяться выражением

$$P_{ок} = \min \{P_{к1}, P_{к2}, P_{к3}, \dots, P_{кn}, (1-P_{обх1}) \cdot (1-P_{обх2}) \dots (1-P_{обхj})\}. \quad (4)$$

4.9. Для неконтролируемых преград с учетом наиболее опасной ситуации: нападения организованной группы нарушителей, т.е. совместности событий, прочность защитной оболочки определяется выражением

$$P_{онк} = P_{нк1} \cdot P_{нк2} \cdot P_{нк3} \cdot \dots \cdot P_{нкn} \cdot (1-P_{обх1}) \cdot (1-P_{обх2}) \dots (1-P_{обхj}), \quad (5)$$

где n – количество преград, составляющих замкнутую оболочку (контур) защиты, а j – количество путей обхода защиты.

4.10. Формулы (4) и (5) позволяют также в процессе проектирования рассчитать фрагмент защиты, перекрывающий один канал НСД и состоящий из нескольких преград, соединенных последовательно.

4.11. Если прочность преграды не удовлетворяет заданным требованиям, она может дублироваться второй, третьей и т.д. преградами, т.е. преграды соединяются параллельно. Тогда итоговая прочность преграды определяется по формуле

$$P_W = 1 - (1-P_1)(1-P_2) \dots (1-P_N), \quad (6)$$

где P – значение прочности преграды;
 N – порядковый номер преграды.

Если несколько оболочек (контуров) защиты дублируют друг друга, итоговая прочность будет определяться по аналогичной формуле, где вместо значений прочности преград проставляются значения прочности оболочек (контуров), составляющих защиту.

4.12. Защита законного входа в автоматизированную систему обеспечивается с помощью пароля, действительное значение которого может быть известно только законному пользователю или службе безопасности системы. Стойкость его к несанкционированному подбору при ограниченном числе попыток определяется по формуле

$$P_{нр} = \frac{n}{A^s}, \quad (7)$$

- где $P_{нр}$ – вероятность подбора пароля нарушителем;
- n – количество попыток подбора пароля;
- A – число символов в выбранном алфавите кода пароля;
- s – длина пароля в количестве символов.

4.13. В случае отсутствия средств ограничения количества попыток подбора стойкость пароля измеряется безопасным временем, которое определяется по формуле

$$T_6 = \frac{A^s \cdot E}{2R}, \quad (8)$$

где R – скорость передачи сообщения в линии связи, симв./мин;

E – число символов в передаваемом сообщении при попытке получить доступ (включая пароль и служебные символы).

4.14. Требования к защите информации от случайных воздействий АС должны отвечать требованиям обеспечения надежности функционирования согласно ГОСТ 24.701–86. Надежность автоматизированных систем управления. Основные положения. В интересах поддержания надежности в АС должны быть предусмотрены:

- средства функционального контроля;
- средства восстановления функционирования;
- резервирование технических средств обработки и передачи информации;
- средства повышения достоверности и резервирования информации.

5. СПЕЦИАЛЬНЫЕ ТРЕБОВАНИЯ К СРЕДСТВАМ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ АС I КЛАССА

5.1. Общие положения.

5.1.1. Для дифференцирования защиты I класса вводятся подклассы А, Б и В, где подкласс IA – высокий, IB – средний, IV – низкий.

5.2. Требования к АС класса IV.

5.2.1. Идентификация пользователей, РС, АРМ, ВК, внешних устройств ЭВМ, ЛВС, КСА и каналов связи должна осуществляться по логическим именам и/или адресам, а программ, томов, каталогов, файлов, записей, полей записей – по именам.

5.2.2. Аутентификация пользователей должна проводиться по идентификатору (коду) и паролю временного действия, длиной не менее 8 буквенно-цифровых символов в виде случайной комбинации, полученной генератором случайных чисел по аттестованному алгоритму.

5.2.3. Доступ к информации и ресурсам должен осуществляться только по предъявлении указанных параметров. При неудачных попытках в количестве более трех должно формироваться и передаваться сообщение о НСД с первым приоритетом на соответствующие средства контроля.

5.2.4. Должна обеспечиваться возможность смены паролей и ограничения времени их действия.

5.2.5. Программа разграничения доступа должна предусматривать возможность разграничения доступа законных пользователей к информации и ресурсам АС в соответствии с данными им полномочиями. Механизм разграничения доступа должен позволять изменять и вводить вновь эти параметры.

5.2.6. Разграничение доступа должно предусматривать возможность раздельного и/или совместного создания или использования томов, дисков, каталогов,

файлов, записей, полей записей, а также возможность разграничения доступа по выполняемым над ними функциям:

- чтению;
- записи;
- копированию;
- переименованию;
- передаче;
- уничтожению.

5.2.7. Разграничение доступа к программам должно быть только на РС, АРМ и сервере печати, если таковые предусмотрены в составе АС. Во всех остальных случаях доступ пользователей к программам при штатном функционировании должен быть заблокирован. К программам в штатной ситуации может иметь доступ только системный администратор АС с разрешения руководителя работ и службы безопасности информации.

5.2.8. При доступе к общим ресурсам должна обеспечиваться возможность управления приоритетами обслуживания.

5.2.9. Должна обеспечиваться возможность распределения (квотирования) администратором БИ совместно используемых ресурсов между пользователями (группами пользователей) в течение сеанса работы.

5.2.10. Уровень конфиденциальности записываемой на носитель информации должен быть не выше аналогичного уровня ее носителя.

5.2.11. Должно обеспечиваться разграничение доступа пользователей к носителям конфиденциальной информации.

5.2.12. Уровень конфиденциальности создаваемой информации определяется ее владельцем.

5.2.13. Полномочия пользователя по доступу к той или иной конфиденциальной информации определяются руководителем работ на АС и по его санкции вводятся администратором безопасности в таблицу полномочий пользователей.

5.2.14. Таблица полномочий должна содержать список должностных лиц с указанием в одной строке условного номера, фамилии и инициалов, перечень информации и функциональные задачи, к которым допущен пользователь.

5.2.15. Программа формирования таблицы полномочий должна обеспечивать возможность отображения по вызову службой безопасности справки о всех полномочиях одного пользователя и справки о том, какие пользователи и какой имеют доступ к запрошенной информации или функциональной задаче.

5.2.16. После определенного администратором безопасности интервала времени отсутствия активности пользователя и по его инициативе должна включаться блокировка сеанса его работы, а ее включение – после его аутентификации.

5.2.17. Очистка (обнуление, обезличивание) освобождаемых областей памяти ЭВМ и внешних накопителей должна осуществляться двукратной записью в эти области произвольной комбинации символов. При необходимости ремонта носителей и отсутствии технической возможности проведения процедуры очистки носители остатков важной информации должны механически уничтожаться.

5.2.18. Электронная идентификация машинного носителя и соответствующая программа в ЭВМ должны обеспечивать возможность определения разрешенного к применению учетного носителя и уровня его конфиденциальности.

5.2.19. Контроль целостности общего программного обеспечения, специального ПО осуществляется по именам и контрольным суммам постоянных файлов установленной версии. Контроль должен осуществляться по запросу оператора и автоматически с заданным интервалом времени.

Контроль целостности обрабатываемой информации осуществляется по контрольным суммам:

- при запросе оператора;
- при вводе информации с машинных носителей;
- при хранении и выборке нормативно-справочной и другой постоянной информации в базе данных;
- при обмене информацией между программными компонентами;
- при выводе информации на отчуждаемый машинный носитель.

Перечисленные процедуры должны быть подконтрольны только системному администратору. Пользователю сообщается только факт проверки и его положительный или отрицательный результат.

5.2.20. В состав средств защиты должны входить средства, обеспечивающие обнаружение и удаление известных на момент функционирования АС типов вирусов с восстановлением зараженных файлов. Антивирусный контроль производится при включении АС и возникновении ситуации, похожей на действие вируса.

Для непрерывной антивирусной профилактики должен быть выделен резидентный монитор, обнаруживающий опасную ситуацию. Для поддержания уровня защиты от вирусов в документации АС должен быть приведен механизм ее обновления.

5.2.21. В АС должны регистрироваться следующие события:

вход/выход субъектов доступа в систему/из системы, загрузка и инициализация операционной системы и ее программного обеспечения с указанием следующих параметров:

- времени и даты события;
- результата попытки входа: успешного, неуспешного – несанкционированного с указанием предъявленного субъектом идентификатора в случае успешного входа и пароля при НСД;

выдача печатных документов на «твердую» копию в сопровождении автоматической маркировки каждого листа (страницы) документа его учетным номером и реквизитами АС с указанием на последнем листе общего количества листов (страниц), а также с указанием в параметрах регистрации следующих параметров:

- времени и даты выдачи (обращение к подсистеме вывода);
- спецификации устройства выдачи (логическое имя/номер внешнего устройства);
- наименования и уровня конфиденциальности документа;
- идентификатора пользователя, запросившего документ;
- объема фактически выданного документа (количество листов, страниц, копий);

запуск/завершение программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов с указанием параметров:

- даты и времени;
- имени (идентификатора) программы (процесса, задания);

- идентификатора пользователя, запросившего программу (процесс, задание);
- результата запуска (успешного, неуспешного – несанкционированного), попытки доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам с указанием следующих параметров:

- даты и времени события;
- результата доступа: успешного, неуспешного – несанкционированного;
- идентификатора субъекта доступа;
- спецификации защищаемого файла;
- имени программы (процесса, задачи, задания), осуществляющей доступ;
- вида запрашиваемой операции (чтение, удаление, выполнение, расширение и т.п.);

попытки доступа программных средств (программ, процессов, задач, заданий) к защищаемым объектам доступа: терминалам ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей с указанием следующих параметров:

- даты и времени события;
- результата доступа: успешного, неуспешного – несанкционированного;
- идентификатора субъекта доступа;
- спецификации защищаемого объекта (логическое имя/номер);
- имени программы (процесса, задачи, задания), осуществляющей доступ к объекту;
- вида запрашиваемой операции (чтение, удаление, монтирование, захват и т.п.);
- изменение полномочий субъектов доступа и статуса объектов доступа с указанием:

- даты и времени события;
- идентификатора субъекта доступа (администратора), осуществившего изменение.

5.2.22. При сопряжении одной АС с другой должны использоваться сертифицированные межсетевые экраны не ниже третьего класса по РД Гостехкомиссии России.

5.2.23. Действительные значения паролей, ключей шифрования и секретных кодов цифровой подписи не должны храниться в долговременной памяти АС в открытом виде.

5.2.24. Доступ к параметрам аутентификации и разграничения доступа должен быть разрешен только должностным лицам службы безопасности информации и лицам, на то уполномоченным.

5.2.25. Тестирование функционирования АС должно обеспечивать:

- проверку выполнения поставленных задач по вводу/выводу, хранению, обработке и передаче информации;

• проверку функционирования программных средств защиты информации.

5.3. Требования к уровню безопасности информации АС класса 1Б (данного проекта РД):

1) совпадают с требованиями класса 1В в части п. 5.2.2 – 5.16, 5.18, 5.2.20, 5.2.23 – 5.2.25;

2) в части п. 5.2.1 требований класса 1В необходимо использовать физические адреса (номера) АРМ, РС, ЭВМ, КСА, каналов связи, узлов коммутации сети и т.д.;

3) в части п. 5.2.17 требований класса 1В необходимо дополнить требованием увеличения количества наложений записи произвольной информации на остатки важной информации до 4 раз;

4) в части п. 5.2.19 необходимо при контрольном суммировании использовать криптографический алгоритм;

5) в части п. 5.2.22 необходимо применить межсетевой экран 2 класса по РД Гостехкомиссии России.

5.4. Требования к уровню безопасности информации АС класса 1А:

1) аутентификация пользователей должна проводиться по идентификатору (коду) и паролю временного действия длиной не менее 8 буквенно-цифровых символов в виде случайной комбинации, полученной генератором случайных чисел по аттестованному алгоритму. Персональный идентификатор размером не менее 4 буквенно-цифровых символов должен набираться на клавиатуре, а пароль – размещаться на специальном носителе типа смарткарты;

2) при обмене информацией в АС должна обеспечиваться взаимная аутентификация РС, АРМ, ВК, внешних устройств ЭВМ, ЛВС, КСА, каналов и узлов связи;

3) совпадают с требованиями класса 1В в части п. 5.2.3 – 5.2.16, 5.2.18, 5.2.23 – 5.2.25;

4) в части п. 5.2.17 требования класса 1В необходимо дополнить требованием увеличения количества наложений записи произвольной информации на остатки важной информации до 4 раз. Налагаемая информация должна вырабатываться аттестованным генератором случайных символов;

5) в части п. 5.2.19 необходимо при контрольном суммировании использовать криптографический алгоритм. Период контроля должен быть меньше ожидаемого времени, необходимого нарушителю для модификации алгоритма и подгонку контрольной суммы с учетом перекрытия каналов НСД средствами защиты, приведенными выше в табл. 1П для данного вида АС;

6) в части п. 5.2.22 необходимо применить межсетевой экран I класса по РД Гостехкомиссии России.

6. ТРЕБОВАНИЯ К СРЕДСТВАМ ЦЕНТРАЛИЗОВАННОГО КОНТРОЛЯ И УПРАВЛЕНИЯ ЗАЩИТОЙ

6.1. Примененные в АС средства защиты с помощью средств централизованного контроля и управления должны быть объединены в единый механизм – систему безопасности информации. При этом для автономно работающих АРМ применяются организационно-технические средства управления, а для распределенных АС и ИВК должны быть выделены АРМ (РС) и программные средства.

6.2. В состав КСА с числом РС (АРМ) более 10 (число уточняется в ТЗ), в АСУ (вычислительную сеть) с числом КСА более двух должно быть включено специальное рабочее место службы безопасности информации (АРМ СБ). В КСА с меньшим числом РС (АРМ) функции централизованного управления безопасностью информации могут совмещаться с другими функциями.

6.3. С помощью АРМ СБ в зависимости от вида и уровня безопасности информации должна обеспечиваться возможность выполнения функций, приведенных в табл. 2.П. Необходимость их применения определяется после построения и получения положительной оценки прочности защитных оболочек, построенных из средств защиты, перечисленных в табл. 1.П.

Таблица 2П

№ п/п	Функции управления безопасностью информации в ИВК, ЛВС, КСА	Классы безопасности					
		IV	III	II	I IB	I IA	I IA
1	Отображение (по данным функционального контроля) состояния конфигурации АС	-	-	+	+	+	+
2	Контроль единого точного времени	+	+	+	+	+	+
3	Ведение списка имен и условных номеров должностных лиц – пользователей	+	+	+	+	+	+
4	Ведение таблиц паролей пользователей	-	-	+	+	+	+
5	Ведение таблиц полномочий пользователей	-	-	-	+	+	+
6	Генерация паролей, ключей шифрования в виде случайных чисел	-	-	-	+	+	+
7	Автоматизированная подготовка носителей к загрузке в АРМ, РС, серверы, вычислительные комплексы (ВК), межсетевые экраны таблиц паролей и полномочий пользователей	-	-	-	+	+	+
8	Автоматизированная подготовка носителей ключей шифрования информации	-	-	-	+	+	+
9	Централизованный сбор и отображение в сопровождении звуковой сигнализации сообщений о НСД	-	+	+	+	+	+
10	Централизованный сбор и отображение фактов санкционированного применения паролей	-	-	+	+	+	+
11	Получение по запросу за любой промежуток времени справки по обращениям пользователей к информации и ресурсам АС	-	-	+	+	+	+
12	Получение отдельных справок по имени пользователя, АРМ, РС, по заданному объекту обращения (документу, серверу, ВК, КСА)	-	-	+	+	+	+
13	Получение отдельных справок по НСД за заданный промежуток времени	-	-	-	+	+	+
14	Получение справки о времени начала и окончания работы пользователя за данным АРМ, РС	-	-	+	+	+	+
15	Получение справки о времени входа и выхода АРМ и РС (КСА) из конфигурации АС (сети, АСУ)	+	+	+	+	+	+
16	Сбор и учет «открытых» кодов цифровой подписи пользователей, их регистрации и отображения с атрибутами переданного сообщения: времени и даты отправления, имени пользователя, адреса отправителя и получателя, заголовка, номера квитанции о приеме, времени и даты получения	-	-	-	+	+	+
17	Контроль функционирования средств защиты информации	+	+	+	+	+	+
18	Отображение по запросу оператора АРМ СБ результатов контроля целостности ПО и информации на АРМ, РС, серверах и ВК с отдельным контролем целостности особо важной информации	-	-	-	+	+	+

Продолжение

№ п/п	Функции управления безопасностью информации в ИВК, ЛВС, КСА	Классы безопасности					
		IV	III	II	I		
					IB	IB	IA
19	Автоматический контроль выполнения сроков действия паролей	-	-	-	-	-	+
20	Контроль вывода технических средств в ремонт, профилактику и последующего их ввода в рабочую конфигурацию АС	-	-	+	+	+	+
21	Централизованный контроль вскрытия аппаратуры на отдельном устройстве с резервным автономным электропитанием	-	-	-	+	+	+
22	Централизованный контроль доступа в помещения объекта автоматизации на отдельном устройстве с резервным электропитанием	-	-	-	-	+	+
23	Маркировка и электронная идентификация с присвоением грифа секретности машинных носителей	-	-	-	+	+	+
24	Маркировка машинных носителей	+	+	+	-	-	-
24	Регистрация и учет машинных носителей и документов	+	+	+	+	+	+
25	Регистрация и документирование перечисленных работ	+	+	+	+	+	+

Примечания:

1. Знак «+» – наличие; «-» – отсутствие функции.
2. На уровнях СОД, АСУ и нижестоящих подсистем данной АСУ применяются собственные средства контроля и управления с выполнением функций п. 1–9, 11–13, 15–17, 19, 25.
3. СОД и АСУ должны отвечать требованиям не ниже II класса.
4. Генерацию и рассылку «открытых» кодов своей цифровой подписи осуществляет пользователь в соответствии с назначенными ему полномочиями. При формировании документов должна быть предусмотрена возможность визирования одного документа несколькими пользователями.
5. Необходимость управления цифровой подписью и ключами шифрования определяется выбором соответствующих средств защиты по табл. 1.П после проведения оценки прочности защитных оболочек данного вида АС.

7. СОСТАВ ЭКСПЛУАТАЦИОННОЙ ДОКУМЕНТАЦИИ НА СИСТЕМУ БЕЗОПАСНОСТИ ИНФОРМАЦИИ АС

7.1. Эксплуатационная документация на систему безопасности информации (СБИ) АС должна содержать следующие документы:

- техническое описание СБИ АС;
- инструкцию по обеспечению безопасности информации на объекте размещения АС;
- инструкцию оператору АРМ СБИ АС;
- инструкцию по безопасности информации при работе на АРМ (РС);
- инструкцию по безопасности информации при работе на рабочей станции.

7.2. Техническое описание СБИ АС должно содержать:

- краткую характеристику АС как объекта обработки информации, подлежащей защите;
- перечень и места сосредоточения информации, подлежащей защите;
- возможные каналы (ВК) НСД к информации;

- перечень, распределение по ВК НСД и описание применяемых средств защиты;
- описание средств централизованного контроля и управления защитой;
- описание механизмов санкционированного входа и выхода пользователя из системы;

- описание механизма разграничения доступа пользователей к информации;
- описание организационных мероприятий по защите;
- описание взаимодействия службы ОБИ с другими службами;
- необходимый состав должностных лиц службы ОБИ.

7.3. Инструкция по обеспечению БИ при работе пользователя на АРМ (РС) должна содержать:

- перечень сведений и документов, подлежащих защите на АРМ (РС);
- перечень ВК НСД к информации АРМ (РС);
- перечень и краткое описание средств защиты, с которыми работает пользователь;
- действия пользователя при подготовке СБИ и вводе АРМ (РС) в эксплуатацию;
- действия пользователя при входе и выходе из системы;
- порядок работы пользователя с информацией ограниченного доступа;
- указания пользователю при обнаружении НСД;
- указания пользователю в аварийных и экстремальных ситуациях;
- указания пользователю при перерывах в работе, окончании рабочей смены и завершении работ на АС.

7.4. Инструкция оператору АРМ СБ должна содержать:

- перечень выполняемых функций;
- указания при подготовке и вводе СБИ в эксплуатацию;
- указания при подготовке СБИ к началу работы пользователей;
- порядок работы за АРМ СБ при выполнении каждой функции;
- действия при перерывах в работе, окончании рабочей смены и завершении работ на АС;
- действия при обнаружении НСД, аварийных и экстремальных ситуациях;
- организационные меры.

7.5. Инструкция по ОБИ АС на объекте размещения должна содержать:

- перечень задач и выполняемых функций;
- состав должностных лиц и распределение их обязанностей по ОБИ;
- указания по ОБИ при вводе АС в эксплуатацию;
- указания при подготовке СБИ и АС к работе;
- порядок работы с СБИ и взаимодействие пользователей с оператором АРМ СБ;
- действия при обнаружении НСД, аварийной и экстремальной ситуации;
- действия при завершении работ на АС.

7.6. Оформление ЭД должно удовлетворять требованиям ГОСТ 2.601-95, ЕСКД. Эксплуатационные документы и ЕСКД.

8. ВЫХОДНЫЕ ПОКАЗАТЕЛИ ОЦЕНКИ ОЖИДАЕМОЙ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В АС

8.1. Общие требования содержат критерии оценки, проверку полноты перекрытия каналов НСД, количественную оценку прочности и качественную оценку полноты выполнения специальных требований.

8.1.1. Критерии оценки:

- полнота перекрытия возможных каналов НСД;
- количественная оценка уровня прочности системы безопасности информации АС;
- качественная оценка полноты выполнения специальных требований и требований по централизованному контролю и управлению системой защиты.

8.1.2. Проверка полноты перекрытия каналов производится на наличие средств защиты на каналах, перечисленных в табл. 1.П с последующим анализом установленных в АС средств защиты на предмет возможных путей их обхода. Результат проверки считается успешным, если:

- количество перекрытых средствами защиты каналов НСД соответствует заданному классу защиты;
- возможные пути обхода защиты отсутствуют.

8.1.3. Количественная оценка прочности защиты производится по методике, приведенной в п.п. 4.4–4.13. При предъявлении АС заказчику представляется соответствующий отчет, утвержденный Главным конструктором.

8.1.4. Качественная оценка полноты выполнения специальных требований производится на соответствие СБИ АС требованиям раздела 5, а требований контроля и управления – табл. 2.П.

8.2. Показатели оценки прочности защиты информации АРМ (РС):

- показатель прочности *контролируемой оболочки* защиты, включающей контроль доступа к средствам защиты и управления ими;
- показатель прочности *превентивной оболочки* защиты;
- показатель *стойкости пароля* пользователя;

8.3. Показатели оценки прочности защиты информации ИВК:

- показатель прочности *контролируемой оболочки* защиты;
- показатель прочности *превентивной оболочки* защиты;
- показатель *стойкости пароля* пользователя;
- наличие функций управления, приведенных в табл. 2.П, с учетом заданного уровня безопасности информации.

8.4. Показатели оценки прочности защиты информации ЛВС:

- показатели оценки прочности защиты информации АРМ (РС) с наименьшими значениями;
- показатель прочности *контролируемой оболочки* защиты информации в ЛВС;
- показатель прочности *превентивной оболочки* защиты информации в ЛВС;
- показатель прочности *контролируемой оболочки* защиты информации в линиях связи;

- показатель прочности *превентивной оболочки* защиты информации в линиях связи.

- показатель *стойкости сетевого пароля* пользователя;
- наличие функций управления, приведенных в табл. 2.П, с учетом заданного уровня безопасности информации.

8.5. Показатели оценки прочности защиты информации КСА:

- показатели оценки прочности защиты информации АРМ с наименьшими значениями;
- показатели оценки прочности защиты информации РС с наименьшими значениями;

- показатели оценки прочности защиты информации ИВК с наименьшими значениями;
- показатели оценки прочности защиты информации ЛВС с наименьшими значениями;
- показатель прочности *контролируемой оболочки* защиты информации в линиях связи;
- показатель прочности *превентивной оболочки* защиты информации в линиях связи;
- показатель *стойкости сетевого пароля* пользователя;
- показатель прочности системы контроля доступа на территорию объекта автоматизации;
- показатель прочности системы контроля доступа в помещения объекта автоматизации;
- класс межсетевого экрана;
- наличие функций управления, приведенных в табл. 2.П, с учетом заданного уровня безопасности информации.

8.6. Показатели оценки прочности защиты информации СОД:

- показатель прочности *контролируемой оболочки* защиты информации узлов коммутации (УК) с наименьшими значениями, определяемый по методологии КСА;
- показатель прочности *превентивной оболочки* защиты информации узлов коммутации (УК) с наименьшими значениями, определяемый по методологии КСА;
- показатель *стойкости сетевого пароля* СОД;
- показатель прочности *контролируемой оболочки* защиты кадра кодограммы (из состава средств контроля, перечисленных в табл. 1.П);
- показатель прочности *превентивной оболочки* защиты кадра кодограммы (из состава средств предупреждения, перечисленных в табл. 1.П);
- показатель прочности защиты *пароля* сетевой аутентификации;
- класс межсетевого экрана (при взаимодействии с другой СОД);
- наличие функций управления, приведенных в табл. 2.П, с учетом заданного уровня безопасности информации.

8.7. Показатели оценки прочности защиты информации АСУ:

- показатели оценки прочности защиты информации КСА с наименьшими значениями;

Примечания: 1. Данный показатель применяется в случае, когда в КСА обрабатывается информация одинаковой степени важности.

2. В случае отличия степени важности обрабатываемой информации в КСА от степени важности информации в других КСА его показатели должны приводиться отдельно.

- группа показателей прочности защиты кадра кодограммы в каналах связи;
- группа показателей оценки защиты информации СОД;
- наличие функций управления, приведенных в табл. 2.П, с учетом заданного уровня безопасности информации.

В группу показателей прочности защиты кадра кодограммы в каналах связи входят:

- показатель прочности *контролируемой оболочки* защиты кадра кодограммы (из состава средств контроля, перечисленных в табл. 1.П);

- показатель прочности *превентивной оболочки* защиты кадра кодограммы (из состава средств предупреждения, перечисленных в табл. 1.П);
- показатель прочности защиты *пароля* сетевой аутентификации.

9. ПОРЯДОК СЕРТИФИКАЦИИ СИСТЕМЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

9.1. Сертификация должна проводиться уполномоченными на то лабораториями и центрами сертификации.

9.2. Сертификация СБИ проводится после приемки опытного образца АС представителем заказчика, если иное не оговорено в ТТЗ.

Сдача в эксплуатацию АС производится после получения сертификата.

9.3. Порядок предъявления СБИ на сертификацию:

- подача заявки с указанием предмета сертификации и испытательной лаборатории;
- заключение с лабораторией или центром сертификации хозяйственного договора о сроках проведения и оплате работ;
- разработка, согласование и утверждение «Программы и методики сертификации»;
- предъявление АС и КД в составе, указанном в «Программе и методике сертификации»;
- предъявление сертификата и эксплуатационной документации на обеспечение безопасности информации АС, входящих АС, если таковые имеются в предъявляемой АС;
- предъявление актов, удостоверяющих отсутствие в АС программных и аппаратных закладок, средств программирования, а также отладочных программ;
- проведение испытаний с составлением протокола и акта;
- передача акта и протокола испытаний на экспертизу в сертификационный отдел Гостехкомиссии России;
- при положительных результатах экспертизы получение сертификата.

9.4. При серийном выпуске АС действие сертификата распространяется на всю серию, если в АС и СБИ не произошли принципиальные изменения.

9.5. В случае испытаний региональных и глобальных АС проводится сертификация только системы защиты информации в каналах связи. При подаче заявки на сертификацию предъявляются сертификаты на составные части АС. Допускается выдача единого сертификата на СБИ АС в целом и ее составные части.

9.6. Действие сертификата подтверждается через 5 лет.

10. ТРЕБОВАНИЯ К ПОСТАВКЕ И СДАЧЕ АС НА ОБЪЕКТЫ ЗАКАЗЧИКА

10.1. Требования к аппаратным средствам АС.

10.1.1. Покупная аппаратура должна также проверяться на отсутствие посторонних закладных устройств.

10.1.2. При транспортировке и поставке все технические средства должны быть опечатаны или опломбированы и охраняемы. При передаче на объект эксплуатации должен быть составлен соответствующий акт или сделана соответствующая отметка в паспортах ТС.

10.1.3. В АС 1 класса аппаратура на объекте эксплуатации должна быть проверена по уровню излучения радиопомех и информационному излучению по каналу ПЭМИН.

10.2. Требования к программному обеспечению автоматизированной системы.

10.2.1. Покупное ПО должно пройти проверку на отсутствие посторонних программных закладок.

10.2.2. Программное обеспечение АС должно пройти проверку на отсутствие технологических программ, применяемых для отладки и настройки АС.

10.2.3. Программное обеспечение АС не должно содержать средства программирования.

10.2.4. При отдельной транспортировке и поставке ПО контейнеры должны быть опечатаны или опломбированы и охраняемы. Носители ПО должны иметь фирменную идентификационную маркировку. При передаче на объект эксплуатации должен быть составлен соответствующий акт.

10.3. Требования к комплектности эксплуатационной документации.

10.3.1. Эксплуатационная документация на обеспечение безопасности информации АС должна пройти проверку на комплектность по техническим условиям.

Допускается в согласованном с заказчиком порядке поставка ЭД на машинном носителе.

10.4. Требования к сопроводительной документации. Сопроводительная документация должна содержать следующие документы:

- акты и аттестаты по проверке аппаратуры АС по 9.1.1, 9.1.2;
- акты и аттестаты по проверке покупного ПО по 9.2.1;
- акт о проверке отсутствия технологических программ по 9.2.2, 9.2.3;
- запись в формуляре АС о соответствии документации по обеспечению безопасности информации, комплектности эксплуатационной документации;
- приемо-сдаточные акты;
- сертификаты на соответствие АС и входящих в нее других АС заданному уровню безопасности информации;
- другие документы согласно действующим ГОСТам и ТУ на АС.

ПРИЛОЖЕНИЕ 2

ОСНОВНЫЕ НОРМАТИВНЫЕ АКТЫ РОССИЙСКОЙ ФЕДЕРАЦИИ ПО РАССМАТРИВАЕМОЙ ТЕМАТИКЕ

(по состоянию на 2000 г.)

Законы

1. Уголовный кодекс Российской Федерации (ст. 275, 276, 283, 284), Федеральный закон от 13.06.96 (№63-ФЗ с последующими изменениями и дополнениями) в редакции Федерального закона от 06.10.97 № 131-ФЗ.
2. Федеральный закон «О государственной тайне» от 21 июля 1993 г. № 5485-1.
3. Федеральный закон «Об информации, информатизации и защите информации» от 20 февраля 1995 г. № 24-ФЗ.
4. Федеральный закон «Об обороне» от 31 мая 1996 г. № 61-ФЗ (в редакции Федерального закона от 30.12.99 № 223-ФЗ).
5. Федеральный закон «Об участии в международном информационном обмене» от 4 июля 1996 г. № 85-ФЗ.

Указы Президента Российской Федерации

1. «О Межведомственной комиссии по защите государственной тайны» от 8 ноября 1995 г. № 1108.
2. «Вопросы Межведомственной комиссии по защите государственной тайны» от 20 января 1996 г. № 71 с последующими изменениями и дополнениями.
3. «О контроле за экспортом из Российской Федерации оборудования и материалов двойного назначения и соответствующих технологий, применяемых в ядерных целях, экспорт которых контролируется» от 21 февраля 1996 г. № 228.
4. «О государственной программе обеспечения защиты государственной тайны в Российской Федерации на 1996–1997 гг.» от 9 марта 1996 г. № 346.
5. «О контроле за экспортом из Российской Федерации товаров и технологий двойного назначения» от 26 августа 1996 г. № 1268 с последующими изменениями и дополнениями.
6. «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. № 188.
7. «О перечне сведений, отнесенных к государственной тайне» от 24 января 1998 г. № 61.
8. «О продлении срока реализации Государственной программы обеспечения защиты государственной тайны в Российской Федерации на 1996–1997 гг.» от 30 марта 1998 г. № 318.

9. «О внесении изменений и дополнений в перечень сведений, отнесенных к государственной тайне, утвержденный Указом Президента РФ от 30.11.95 №1203» от 06.06.01 №659.

10. Руководящий документ Президента РФ «Доктрина информационной безопасности Российской Федерации» от 09.09.2000 № Пр-1895.

Распоряжение Президента Российской Федерации

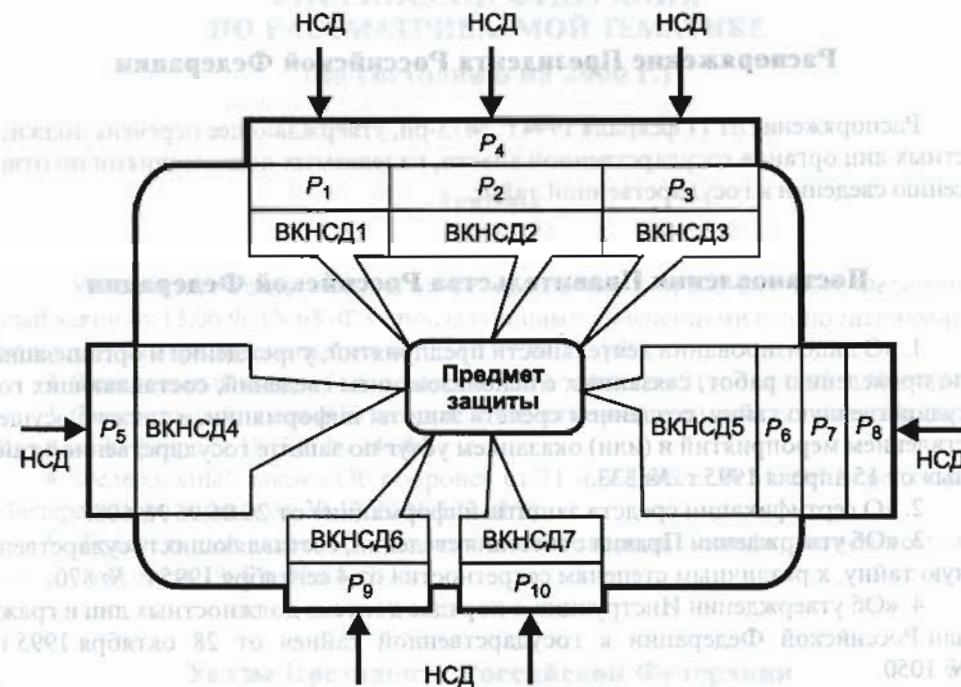
Распоряжение от 11 февраля 1994 г. №73-рп, утверждающее перечень должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне.

Постановления Правительства Российской Федерации

1. «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» от 15 апреля 1995 г. № 333.
2. «О сертификации средств защиты информации» от 26.06.95 № 608.
3. «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» от 4 сентября 1995 г. № 870.
4. «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне» от 28 октября 1995 г. № 1050.
5. «Об утверждении Положения о порядке контроля за экспортом из Российской Федерации оборудования и материалов двойного назначения и соответствующих технологий, применяемых в ядерных целях, экспорт которых контролируется» от 8 мая 1996 г. № 575.
6. «Об утверждении Положения о порядке контроля за вызовом из Российской Федерации товаров и технологий двойного назначения, экспорт которых контролируется» от 7 октября 1996 г. № 1172.
7. «Об утверждении Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам» от 2 августа 1997 г. № 973.
8. «Об усилении контроля за экспортом товаров и услуг двойного назначения, имеющих отношение к оружию массового уничтожения и ракетным средствам его доставки» от 22 января 1998 г. № 57.

ПРИЛОЖЕНИЕ 3

ПРИМЕР РАСЧЕТА ПРОЧНОСТИ ОБОЛОЧКИ ЗАЩИТЫ



Модель сложной оболочки защиты

В оболочке, приведенной на рисунке, P_1 – P_{10} – преграды, перекрывающие возможные каналы НСД: ВКНСД1–ВКНСД7. Если значения прочности данных преград: $P_1=0,7$; $P_2=0,8$; $P_3=0,5$; $P_4=0,6$; $P_5=0,9$; $P_6=P_7=P_8=0,4$; $P_9=0,78$; $P_{10}=0,75$, то расчет прочности защитной оболочки для защиты от нарушителя в единственном числе производится следующим образом.

Начинаем расчет с каналов НСД, перекрытых параллельными преградами. Но если и в ней присутствует последовательное соединение преград, логично определить в нем сначала преграду с наименьшим значением, т.е. рассчитать прочность данного участка по формуле (3.16). В нашем примере на участке ВКНСД1-3 это будет преграда $P_3=0,5$. Затем «суммарная» прочность защиты ВКНСД1-3 с учетом преграды P_4 определяется по формуле (3.18):

$$P\Sigma_1 = 1 - (1 - P_4)(1 - P_3) = 1 - (1 - 0,6)(1 - 0,5) = 1 - 0,4 \cdot 0,5 = 0,8.$$

Прочность «суммарной» защиты на ВКНСД5 определим по этой же формуле

$$P\Sigma_2 = 1 - (1 - P_6)(1 - P_7)(1 - P_8) = 1 - (1 - 0,4)(1 - 0,4)(1 - 0,4) = 1 - 0,216 = 0,784.$$

Прочность защитной оболочки согласно формуле (3.16) будет равна

$$P\Sigma = \min\{P\Sigma_1, P_5, P\Sigma_2, P_9, P_{10}\} = \min\{0,8, 0,9, 0,784, 0,78, 0,75\},$$

т.е. наименьшему из перечисленных в формуле значений P . В нашем примере оно будет определяться значением прочности преграды $P_{10}=0,75$. Если это значение прочности защитной оболочки не устраивает разработчика, то эта преграда заменяется новой или дублируется второй преградой. При этом может оказаться, что полученное суммарное значение прочности превышает значение прочности преграды, установленной на другом ВКНСД. Если и оно является недостаточным, процесс повышения прочности защиты повторяется до получения необходимых значений.

ЛИТЕРАТУРА

1. Аршинов М. Н., Садовский Л. Е. Коды и математика. – М.: Наука, 1983.
2. Андрианов В.В. и др. Аутентификация равноуровневых объектов // Защита информации. Конфидент. – 1997. – № 3.
3. Анин Б.Ю. Защита компьютерной информации. – СПб.: БХВ-Петербург, 2000.
4. Баранюк В.А. и др. Основы больших АСУ / В.А. Баранюк, Е.С. Бичугов, А.И. Черкашенко и др. – М.: Сов. радио, 1979.
5. Безруков Н.Н. Компьютерная вирусология: Справ. руководство. – М.: УРЕ, 1991. – 416 с.
6. Бияшев Р. Г., Диев С. И., Размахин М. К. Основные направления развития и совершенствования криптографического закрытия информации // Зарубежная радиоэлектроника. – 1989. – № 12.
7. Брассар Ж. Современная криптология: Пер. с англ. – М.: Издательско-полиграфическая фирма ПОЛИМЕД, 1999.
8. Брусницын С.В., Ловцов Д.А. Контроль и управление доступом к ресурсам АСУ // Вопросы защиты информации. – 1995. – № 4.
9. Вакка Д. Безопасность Intranet: Пер. с англ. – М.: Бук Медиа Паблишер. – 1998.
10. Варфоломеев А.А., Фомичев В.М. Информационная безопасность: Математические основы криптологии, 1995.
11. Волхонский В.В. Беспроводная система охранной сигнализации SpreadNet: Справ. пособие / C&K Systems (Europe) BV; Пер. с англ., 1996.
12. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. – М.: Гостехкомиссия РФ. – М.: Воениздат, 1992.
13. Гайкович В., Першин А. Безопасность электронных банковских систем. – М.: Единая Европа, 1994.
14. Гармонизированные критерии Европейских стран ITSEC [Information Technology Security Evaluation Criteria. Harmonised Criteria of France – Germany – the Netherlands – the United Kingdom. – Department of Trade and Industry, London, 1991].
15. Герасименко В. А. Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, 1994.
16. Герасименко В. А. Проблемы защиты данных в системах их обработки // Зарубежная радиоэлектроника. – 1989. – №12.
17. Герасименко В.А., Размахин М.К. Защита информации в вычислительных, информационных и управляющих системах // Зарубежная радиоэлектроника. – 1985. – №8.
18. Герасименко В.А., Размахин М.К., Родионов В.В. Технические средства защиты информации // Зарубежная радиоэлектроника. – 1989. – №12.
19. Герасименко В.А., Скворцов А.А., Харитонов И.Е. Новые направления применения криптографических методов защиты информации // Зарубежная радиоэлектроника. – 1989. – №12.
20. Генне О.В. Основные положения стеганографии // Защита информации Конфидент. – 2000. – №31.
21. Гнеденко Б.В., Хинчин А.Я. Элементарное введение в теорию вероятностей. – М.: ГИФЗМЛ, 1961.
22. Грушо А.А., Тимокина Е.Е. Теоретические основы защиты информации. – М.: Издательство Агентства «Яхтсмен», 1996. – С 126–151.
23. Давыдовский А.И., Дорошкевич П.В. Защита информации в вычислительных сетях // Зарубежная радиоэлектроника. – 1989. – №12.
24. Дворянкин С.В. Компьютерные технологии защиты речевых сообщений в каналах электросвязи / Под ред. А.В. Петракова. – М.: РИО МТУСИ, 1999.
25. Девянин П.Н. и др. Теоретические основы компьютерной безопасности / П.Н. Девянин, О.О. Михальский, Д.И. Правиков, А.Ю. Щербаков и др. – М.: Радио и связь, 2000.
26. Жельников В. Криптография от папируса до компьютера. – М.: АБВ, 1997.
27. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учеб. пособие. – М.: Логос; ПБОЮЛ Н.А.Егоров, 2001.
28. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. – СПб.: БХВ-Петербург, 2000.
29. Интерпретация TCSEC для сетевых конфигураций NCSC [National Computer Security Center. Trusted Network Interpretation. -NCSC-TG-005, 1987].
30. Калинин М. Имя им – легион, но с ними можно бороться // МИР ПК. – 2000. – №4.
31. Канадские критерии безопасности компьютерных систем CTCPEC [Canadian Trusted Computer Product Evaluation Criteria, Version 3.0. – Canadian System Security Centre, Communications Security Establishment, Government of Canada, 1993].
32. Касперский Е. Компьютерные вирусы: Что это такое и как с ними бороться. – М.: СКПресс, 1998. – 288 с.
33. Киви Б. Надежно ли защищены смарткарты? // Системы безопасности связи и телекоммуникаций. – 1999. – №25.
34. Критерии оценки безопасности компьютерных систем МО США («Оранжевая книга») TCSTC [Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, 1983].
35. Кузьмин И.В., Буназди Р.Г., Ковергин А.А. Аппаратный контроль электронных цифровых вычислительных машин. – М.: Энергия, 1974.
36. Кузьминов Т.В. Криптографические методы защиты информации. – Новосибирск: Наука, 1998.
37. Лебедев А.Н. Открытые системы для «закрытой» информации // Открытые системы. – 1993. – Вып. 3.
38. Маркин А.В. Безопасность излучений и наводок от средств электронно-вычислительной техники: домыслы и реальность // Зарубежная радиоэлектроника. – 1989. – №12.
39. Мамиконов А.Г. Проектирование АСУ. – М.: Высшая школа, 1987.

40. Мафтик С. Механизмы защиты в сетях ЭВМ. – М.: Мир, 1993.
41. Мельников В.В. Безопасность информации в компьютерных системах // Информ-Ревю. – 1999. – №2.
42. Мельников В.В. Защита информации в компьютерных системах. – М.: Финансы и статистика; Электронинформ, 1997.
43. Мельников В.В. Защита информации в трактах передачи данных. – М.: Инсвязьиздат. – (Тезисы докладов научно-технической конференции профессорско-преподавательского, научного и инженерно-технического состава. МТУСИ, 2002 январь).
44. Мельников В.В. Защита цепей охранной сигнализации. – М.: Инсвязьиздат. (Тезисы докладов научно-технической конференции профессорско-преподавательского, научного и инженерно-технического состава. МТУСИ, 2002 январь).
45. Мельников В.В. Исследование концептуальной модели защиты данных в автоматизированных системах: Тезисы докладов. – М.: Инсвязьиздат, 2001 (Международный форум информатизации «Коммуникационные технологии и сети»).
46. Мельников В.В. Концептуальные вопросы обеспечения гарантированной безопасности данных в автоматизированных системах их обработки // (Сб. тезисов докладов. – Ялта-Гурзуф, 1997. – (Международная конференция «Нейросетевые технологии обработки информации»).
47. Мельников В.В. Концептуальный подход к проектированию защиты информации в вычислительных сетях и АСУ: Тезисы докладов. – М.: МТУСИ, 1998. – (Международный форум информатизации «Коммуникационные технологии и сети»).
48. Мельников В.В. Основы теории защиты информации в автоматизированных системах // Вопросы защиты информации. – 2000. – №3.
49. Мельников В.В. Принципы построения гарантированной защиты цепей контроля охранной сигнализации: Тезисы докладов. – М.: МТУСИ, 1999. – (Международный форум информатизации «Коммуникационные технологии и сети»).
50. Мельников В.В. Принципы построения системы многоточечной сигнализации. – М.: Информсвязьиздат, 1999. – (Тезисы докладов XXXIII научно-методической конференции профессорско-преподавательского состава МТУСИ).
51. Мельников В.В. Прочность защиты – дело тонкое // Открытые системы. Сети. – 1999. – №3.
52. Мельников В.В. Элементы теории и основные принципы построения системы безопасности информации от преднамеренного несанкционированного доступа в автоматизированных системах с централизованной обработкой данных // XXV юбилейная международная конференция «Новые информационные технологии в науке, образовании, телекоммуникации и бизнесе». Труды конференции. – Ялта-Гурзуф, 1998.
53. Мельников В.В., Тырин И.В., Мухин С.Л. Устройство для многоточечной сигнализации. Патент № 1795496: G 08 B 23/00. 1993.
54. Мельников Ю.Н. Достоверность информации в сложных системах. – М.: Сов. радио, 1973.
55. Михайлов С.Ф., Петров В.А., Тимофеев Ю.А. Информационная безопасность. Защита информации в автоматизированных системах. Основные концепции: Учеб. пособие. – М.: МИФИ, 1995.
56. Молдован Н.А. Проблематика и методы криптографии. – СПб., 1998.

57. Мясников С. Пуленепробиваемая защита ПК // Открытые системы. – 2000. – №4.
58. Нестеров С.В. Использование модели иерархической машины состояний для защиты информации // Вопросы защиты информации. – 1996. – №2.
59. Общие критерии оценки безопасности информационных технологий: Учеб. пособие / Пер. с англ. Е.А. Сидак. – М.: ЦБИ, 2001.
60. Петраков А.В. Основы практической защиты информации. – М.: Радио и связь, 1999.
61. Петраков А.В., Лагутин В.С. Защита абонентского телеграфика. – М.: Радио и связь, 2001.
62. Пудовченко Ю.Е. Когда наступает время подбирать ключи // Защита информации. Конфидент. – 1998. – №3. – С. 65–71.
63. Пятибратов А.П., Гудыно Л.П., Кириченко А.А. Вычислительные системы, сети и телекоммуникации. – М.: Финансы и статистика, 1998.
64. Рекомендации X.800 для распределенных систем [Security Architecture for Open Systems Interconnection for CCITT Applications. Recommendation X.800. – CCINN, Geneva, 1991].
65. Романин Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – 2-е изд. – М.: Радио и связь, 2001.
66. Романцов А.П. Криптография и стеганография / Под ред. А.В. Петракова. – М.: РИО МТУСИ, 2002.
67. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от НСД. Показатели защищенности от НСД к информации. – М.: Гостехкомиссия РФ, 1996.
68. Сидак А.А. Формирование требований безопасности современных сетевых информационных технологий. – М.: МГУЛ, 2001.
69. Сяо Д., Керр Д., Мэдник С. Защита ЭВМ / Пер. с англ. – М.: Мир, 1982.
70. Тайли Э. Безопасность персонального компьютера. – Минск: ООО «Попурри», 1997.
71. Теория и практика обеспечения информационной безопасности / Под ред. П.Д. Зегжды. – М.: Издательство Агентства «Яхтсмен», 1996.
72. Ухлинов Л. М. Международные стандарты в области обеспечения безопасности данных в сетях ЭВМ. Состояние и направления развития // Электросвязь. – 1991. – № 6.
73. Федеральные критерии безопасности информационных технологий [Federal Criteria for Information Technology Security (FC), Draft Version 1.0, (Volumes I and II).- National Institute of Standards and Technology, National Security Agency, US Government, 1993].
74. Физурнов В. Э. IBM PC для пользователя. – 7-е изд. – М.: Инфра-М, 2000.
75. Фролов А.В., Фролов Г.В. Осторожно: компьютерные вирусы. – М.: ДИАЛОГ-МИФИ, 1996.
76. Харламов В.П. Некоторые концептуальные аспекты защиты информации / Вопросы защиты информации. – 1994. – № 1.

77. Хорев А.А. Способы и средства защиты информации. – М.: МО РФ, 1998.
78. Хоффман Л. Дж. Современные методы защиты информации / Пер. с англ. – М.: Сов. радио, 1980.
79. Шураков В.В. Надежность программного обеспечения систем обработки данных. – М.: Статистика, 1987.
80. Шураков В.В. Обеспечение сохранности информации в системах обработки данных. – М.: Финансы и статистика, 1985.
81. Щеглов А.Ю. Структура типовой системы защиты информации в корпоративной сети // Технологии и средства связи. – 1999. – №1.
82. Щербаков А.Ю. Введение в теорию и практику компьютерной безопасности. – М.: издатель Молгачева С.В., 2001.
83. Щербаков Н.С. Достоверность работы цифровых устройств. – М.: Машиностроение, 1989.
84. Электроника. – 1985. – Т. 58. – №18.
85. Dr. Dobb's Journal. – 1993. – V. 18. – № 13. – P. 50, 52, 54, 56.
86. Harrison M. A., Ruzzo W. L., Velmon I. D. On Protection Operation Systems // Communication of the ACM, 1975.
87. Wood C., Fernandes E. B., Sumes R. S. IBM System J. – 1980. – V. 19. – № 2.

Список сокращений

АПД	– аппаратура передачи данных.
АРМ	– автоматизированное рабочее место.
АРМ СБ	– автоматизированное рабочее место службы безопасности.
АСУ	– автоматизированная система управления.
ВКНСД	– возможный канал несанкционированного доступа.
ВНСД	– возможные несанкционированные действия.
ГМД	– гибкий магнитный диск.
ДЛ	– должностное лицо.
ЖМД	– жесткий магнитный диск.
ЖНСД	– журнал НСД.
ЗБ	– задание по безопасности.
ИВК	– информационно-вычислительный комплекс.
ИТ	– информационная технология.
КПП	– контрольно-пропускной пункт.
КСА	– комплекс средств автоматизации (обработки данных).
ЛВС	– локальная вычислительная сеть.
МД	– магнитный диск.
МЛ	– магнитная лента.
НЗК	– нормально-замкнутый контакт.
НКП	– носитель кода пароля.
НСД	– несанкционированный доступ.
НКП	– носители кодов паролей.
ОБИ	– обеспечение безопасности информации.
ОК	– общие критерии.
ОКР	– опытно-конструкторская разработка.
ОПО	– общее программное обеспечение.
ОС	– операционная система.
ПЗ	– профиль защиты.
ПКРД	– программа контроля и разграничения доступа.
ПО	– программное обеспечение.
ППО	– прикладное программное обеспечение.
ПЭМИН	– побочное электромагнитное излучение и наводки.
ПК	– персональный компьютер.
РД	– руководящий документ.
РС	– рабочая станция.
СБИ	– система безопасности (защиты) информации.
СБР	– система безопасности ресурса.
СВТ	– средство вычислительной техники.
СЗИ	– система защиты (безопасности) информации.
СКЗД	– система криптографической защиты данных.

СКРД	– система контроля и разграничения доступа.
СПД	– сеть передачи данных.
СКВА	– система контроля вскрытия аппаратуры.
СПДИ	– средства повышения достоверности информации.
СУБД	– система управления базой данных.
СУБИ	– система управления безопасностью информации.
СЦКУ	– средства централизованного контроля и управления.
ТЗ	– техническое задание.
ТКП	– таблица кодов паролей.
ТС	– технические средства.
ТТЗ	– тактико-техническое задание.
УК	– узел коммутации.
УУК	– управляющий узел коммутации.
УКВА	– устройство контроля вскрытия аппаратуры.
УНДЛ	– условный номер должностного лица.
ФЗ	– функциональные задачи.
ЦУБИ	– центр управления безопасностью информации.

Предметный указатель

А

Абонентское шифрование 18
 Аварийная ситуация 18, 147
 Автоматизированная система 156
 Автоматизированная система управления 18, 82
 Автоматизированное рабочее место 18
 Агрегирование 285
 Административные меры по защите информации 18, 149, 258
 Администрация АС 17, 148
 Алгоритм маршрутизации 76
 Антивирусные средства 128, 190
 Аутентификация 18, 106, 107

Б

База данных 36, 283
 Безопасность
 – информации 18, 165
 – АС 18
 Брандмауэр 275, 281

В

Вакцинация программ 132
 Верификация ПО 18, 192
 Виртуальная сеть 77
 Вычислительный комплекс 18
 Возможные каналы НСД в системах
 – с сосредоточенной обработкой данных 186
 – с распределенной обработкой данных 195
 Возможные несанкционированные действия над кадром кодограммы 195, 197

Г

Генератор псевдослучайных чисел 127
 Глобальная сеть 67, 75
 Графопостроитель 289

Д

Дискреционный доступ 234
 Документирование информации 258
 Дублирование информации 248

З

Законодательные меры 150
 Защита от вирусов 128, 190
 Защитная оболочка 165

И

Идентификация 18, 106, 107
 Инкапсуляция пакета 69
 Инференция 285
 Информационный вычислительный комплекс 18
 Информация 18

К

Классификация
 – автоматизированных систем 84
 – автоматизированных систем по уровню безопасности информации 162
 – возможных каналов НСД 185
 – возможных несанкционированных действий 196
 – информации 21
 – нарушителя 161
 Контроль
 – доступа к аппаратуре 103, 104
 – функциональный (см. Функциональный контроль) 20, 137
 – целостности ПО и данных 190, 244
 Комплекс средств автоматизации 19, 186
 Кодирование информации 18
 Корпоративная сеть 19, 51, 80
 Криптография 18, 113

Л

Линейное шифрование 19, 115, 263
 Линии связи 255

Локальная вычислительная сеть 19, 50, 302

- простая 57
- сложная 64

М

Мандатный доступ 235

MAC-адрес 55

Маршрутизатор 51, 52, 67

Межсетевое экранирование 275

Мейнфрейм 39

Многоуровневая защита 181

Модель

- защиты информации АС 157
- многозвенной защиты 179
- нарушителя 161
- элементарной защиты 166
- эталонная (см. *Эталонная модель OSI*) 48

Модификация информации 19, 160

Мост 51, 52, 67

Н

Надежность АС 137

Накопитель 289

Нарушитель в АС 19

Несанкционированный доступ к информации 19

Носитель кода пароля 239

О

Ограничение доступа 101

Оперативная информация 19

Операционная система 289

Опознавание пользователя 19

Опорная сеть 74

Организационные мероприятия по

защите информации 19, 149, 258

Открытое шифрование 266

Охранная сигнализация 210

П

Пакет 55, 61

Пароль 19

Плоттер 289

Побочное электромагнитное излучение и наводки (ПЭМИН) 19, 135

Повторитель 51

Пользователь АС 19

Предмет защиты в АС 19, 30

Преднамеренные угрозы 91

Программа-ревизор 131

Программный вирус 19, 130

Прокси-сервер 289

Простая ЛВС (см. *Локальная вычислительная сеть*) 57

Прочность

защиты информации в АС 19, 163

средства защиты (преграды) 166, 168

Р

Рабочая станция 20

Разграничение доступа 103, 105

Разделение привилегий 106

Региональная сеть 67, 75

Регистрация доступа 256

Резидентный сторож 131

Ресурсы АС 20, 30

С

Сегмент ЛВС 54, 64

Секретность информации 20

Сеть передачи данных 20, 159, 198

Сканер 289

Случайные угрозы 89

Случайный НСД 20, 143

Сложная ЛВС 64

Симметричное шифрование 264

Система

- безопасности информации АС 20, 188, 198
- контроля вскрытия аппаратуры 220, 223
- охранной сигнализации 210
- с распределенной обработкой данных 157
- с сосредоточенной обработкой данных 157

Спам 195

Стеганография 123

Стриммер 289

Стойкость пароля 174

Т

Телекоммуникационная вычислительная сеть 20, 312

Теория построения защиты 163

Технологическая информация АС 20

Топология ЛВС 57

Трафик 278, 282

У

Уровень безопасности информации в

АС 20, 320

Утечка информации 20, 160

Утрата информации 20, 160

Ф

Фильтрация трафика 278

Функциональный контроль

(см. *Контроль функциональный*) 20, 137

Х

Хэш-функция 238

Ц

Целостность данных 20, 244

Целостность программного обеспечения 190, 244

Цифровая подпись 267

Ш

Шифрование информации 20, 115

Шлюз 51, 53

Шлейф 214

Э

Эффективность защиты информации 20

Эталонная модель OSI (см. *Модель*) 48

Экран межсетевой 275

Информационная безопасность
53, 302

Информационная безопасность
Информационная безопасность
Информационная безопасность
Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Информационная безопасность
Информационная безопасность

Научно-практическое издание

Мельников Виталий Викторович

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Заведующая редакцией Л.А. Табакова
Редакторы Л.Д. Григорьева, Н.А. Кузнецова
Младший редактор Н.А. Федорова
Художественный редактор Ю.И. Артюхов
Технический редактор И.В. Завгородняя
Корректоры Г.В. Хлопцева, Н.П. Сперанская
Компьютерная верстка О.В. Фортунатовой
Обложка художника О.В. Толмачева

ИБ № 4457

Подписано в печать 25.04.2003

Формат 70х100^{1/16}. Печать офсетная.

Гарнитура «Таймс»

Усл.п.л. 22,54. Уч.-изд.л. 28,72

Тираж 4000 экз. Заказ 1523. «С» 106

Издательство «Финансы и статистика»

101000, Москва, ул. Покровка, 7

Телефон (095) 925-35-02, факс (095) 925-09-57

E-mail: mail@finstat.ru http://www.finstat.ru

ГУП «Великолукская городская типография»

Комитета по средствам массовой информации

Псковской области,

182100, Великие Луки, ул. Полиграфистов, 78/12

Тел./факс: (811-53) 3-62-95

E-mail: VTL@MART.RU