В.П. Пушкарев, В.В. Пушкарев

ЗАЩИТА ИНФОРМАЦИОННЫХ ПРОЦЕССОВ
в компьютерных системах
(Безопасность жизнедеятельности 2)

Учебное пособие

ТОМСК – 2012

Министерство образования и науки Российской Федерации

Федеральное бюджетное государственное образовательное учреждение высшего профессионального образования

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

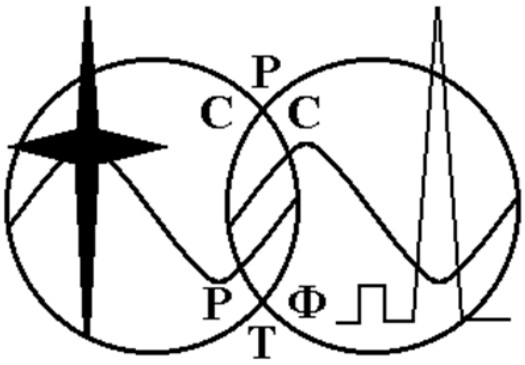
Кафедра средств радиосвязи (СРС)

В.П. ПУШКАРЕВ, В.В. ПУШКАРЕВ

ЗАЩИТА ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

(Безопасность жизнедеятельности 2)

Учебное пособие



2012

Рецензент: кандидат технических наук Бацула А.П.

Пушкарев В.П., Пушкарев В.В.
Защита информационных процессов в компьютерных системах: Учебное пособие. Томск: Томский межвузовский центр дистанционного образования, 2005. - 131 с.

Учебное пособие предназначено для студентов очного, вечернего форм обучения направления специальностей «Радиотехника», «Телекоммуникации», «Информационная безопасность», а также для студентов, обучающихся с использованием дистанционных образовательных технологий.

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ 6
2. ПРАВОВЫЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ 9
2.1. Правовые и нормативные акты, квалифицирующие информационные компьютерные преступления 9
2.2. Понятие информационной безопасности 12
2.3. Понятия, свойства информации 15
2.4. Законодательство об информационных правоотношениях 19
2.5. Классификация компьютерных систем 22
2.6. Объекты защиты в персональных компьютерах и компьютерных системах 26
3. АНАЛИЗ ПОТЕНЦИАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ 29
3.1. Постановка задачи анализа потенциальных угроз 29
3.1.1. Случайные угрозы 29
3.1.2. Преднамеренные угрозы 31
3.2. Анализ электромагнитных излучений и наводок в компьютерных системах 37
3.2.1. Характеристики излучения протоколов обмена 37
3.2.2. Анализ спектра излучения протокола обмена 38
3.2.3. Анализ спектра излучения наводок оборудованием компьютерной системы 40
4. МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ 42
4.1. Обзор методов защиты информационных процессов в компьютерных системах 42
4.2. Организационные методы защиты информационных процессов в компьютерных системах 43
4.2.1. Ограничение доступа 43
4.2.2. Контроль доступа к аппаратуре 44
4.2.3. Разграничение и контроль доступа 45
4.2.4. Разделение привилегий на доступ 47
4.2.5. Идентификация и установление подлинности 48

4.3. Инженерно-технические методы защиты информационных процессов 52
4.3.1. Пассивные методы инженерно-технической защиты 55
4.3.2. Активные методы инженерно-технической защиты. 55
4.4. Программно-аппаратные методы защиты информационных процессов 56
5. АНАЛИЗ И ОЦЕНКА ПРОЧНОСТИ ЗАЩИТЫ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ 66
5.1. Основы теории защиты информационных процессов от несанкционированного доступа 66
5.1.1. Модель поведения потенциального нарушителя 66
5.1.2. Модель защиты информационного процесса 67
5.2. Концептуальные основы построения защиты информационных процессов от несанкционированного доступа в компьютерных системах 78
5.3. Оценка эффективности автоматических средств управления защитой информационных процессов в компьютерных системах 83
6. СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ 85
6.1. Распределение средств защиты информации и информационных процессов компьютерных систем 85
6.1.1. Распределение средств защиты информации и информационных процессов в компьютерных сетях 85
6.1.2. Распределение средств защиты в модели взаимосвязи открытых систем 88
6.2. Инженерно-технические средства защиты 94
6.3. Программно-аппаратные средства защиты информации и информационных процессов 122
6.3.1. Основы построения программно-аппаратных средств защиты 122
6.3.2. Технические средства программно-аппаратной защиты информационных процессов 124
ЛИТЕРАТУРА 131

1. ВВЕДЕНИЕ

Развитие компьютерных средств передачи, приема, обработки информации и распространения требуют разработки методов технических и программных средств обеспечения сохранности информации. Следует также отметить и необходимость принятия мер по обеспечению информационной безопасности общества. Масштабы и сферы применения компьютерной техники и технологии стали таковы, что наряду с надежностью ее функционирования встает вопрос не только защиты информации, но и информационной безопасности ее владельца и потребителя, кому она предназначается. Решение этой проблемы, несмотря на большой объем проведенных исследований, классификации объектов обработки информации, методов определения возможных каналов несанкционированного доступа (НСД), методов расчета прочности защиты информации, усложняется отсутствием единой теории и концепции обеспечения защиты информационных процессов компьютерных системах.

С появлением сложных информационных систем управления, связанных с автоматизированным хранением, обработкой и выводом информации, проблема ее защиты обусловлена [1]:

- увеличением объемов информации, накапливаемой, хранимой и обрабатываемой с помощью ЭВМ и других средств компьютерной техники;
- сосредоточением в единых базах данных информации различного назначения и принадлежности;
- расширением круга пользователей, имеющих доступ к ресурсам информационных систем и находящимся в ней массивам данных;
- усложнением режимов функционирования технических средств компьютерной техники и широкое внедрение многопрограммного режима, режима разделения времени и реального времени;
- автоматизацией межмашинного обмена информацией, в том числе и на больших расстояниях;

- увеличением количества технических средств связей в автоматизированных системах управления и обработки данных;
- появлением персональных компьютеров, расширяющих возможности не только пользователям, но и нарушителям.

Развитие информационных технологий привело к появлению нового вида преступления – специальные компьютерные злоумышленники: ХАКЕРЫ, КРЭКЕРЫ. Хакеры (Hacker, анг.) – компьютерный хулиган, получающий удовольствие от проникновения в чужой компьютер. Крэкер (Cracker, анг.) – вор–взломщик.

Последствия несанкционированных воздействий и несанкционированного использования информации наносят огромный ущерб политического, экономического характера, ставящий на грань жизни земной цивилизации. Имеется большой перечень примеров несанкционированного запуска боевых машин.

Для предотвращения возможных инцидентов проводится работа по совершенствованию правовых и юридических норм в области компьютерной технологии. При разработке мероприятий по обеспечению защиты информационных процессов следует придерживаться следующих требований:

- выбор информации в качестве предмета защиты (ресурсы тоже защищаются, но только в необходимых случаях);
- использование в расчетах прочности защиты время жизни информации;
- использование в построении защиты классификацию компьютерных систем по видам, принципам построения и обработки данных;
- применение различных подходов к непреднамеренным и преднамеренным угрозам информации;
- приложение известной стратегии и тактики защиты любого объекта к защите информации и информационных процессов в компьютерных системах;
- сведение всех потенциальных угроз к трем событиям: *утечке, модификации и утрате;*
- разработка и использование в постановке задачи простой модели ожидаемого поведения нарушителя и его классификации;

- определение в компьютерных системах возможных каналов несанкционированного доступа к информации со стороны нарушителя того или иного класса;
- разработке расчетных соотношений для построения средств и систем защиты, перекрывающие возможные каналы несанкционированного доступа.

При разработке средств защиты информационных процессов разработчик должен руководствоваться следующим:

- созданием основ единой, для всех видов компьютерных систем, теории безопасности информации;
- созданием, в заданной компьютерной системе, встроенной автоматизированной подсистему безопасности информации в виде единого механизма с гарантированными количественными и качественными характеристиками;
- достижением возможности получения с позиций безопасности информации оптимальных требований к аппаратным и программным средствам компьютерных систем;
- достижением возможности включения типовых требований по безопасности информации техническое задание на разработку компьютерной системы;
- необходимостью разработки четких и ясных руководящих нормативных документов по безопасности информации при создании компьютерных систем.

Таким образом, защита информации, информационных процессов, а также информационные отношения требует тщательной проработке уголовно-правовой защиты, т.к. информация и информационные отношения в этом случае являются объектом преступления.

2. ПРАВОВЫЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

2.1. Правовые и нормативные акты, квалифицирующие информационные компьютерные преступления

Проработка правовой основы, законодательства и положения по их применению необходима для успешной работы по обеспечению достаточного уровня защиты информации. Это продиктовано особенностями, присущими для информационных преступлений с использованием высоких компьютерных технологий, а также проблемами информационных нападения и преступлений.

Проблема информационных нападений. Как показывает анализ рост преступности в области информационных технологий является практически не контролируемым процессом. Практически все государственные и коммерческие структуры подвергаются информационному нападению, последствия которых не афишируются. Это затрудняет проводить целенаправленную профилактическую работу по предотвращению подобного вида преступления. Факты говорят об убытках только американских компаний, исчисляются сотнями миллиардов долларов. На российском рынке программного обеспечения ежемесячно фиксируется появление более 10 новых вирусов. За период 1991-1995 годы зарегистрированы факты хищений из российских банков сотни тысяч долларов и разовые попытки хищений превышающих 50 млрд. рублей. Все чаще фиксируются попытки проникновения в компьютерные сети банковских организаций Российской Федерации. Свыше 50% из тех, кто испытал вторжения или проводил исследования, установил факт несанкционированных действий со стороны собственных служащих. Опрос владельцев и законных пользователей информационных сетей показал, что свыше 50% не имеют плана мероприятий на случай несанкционированного вторжения. Свыше 60% не имеют стратегии сохранения доказательства нарушений для дальнейшего судебного и уголовного разбирательства. Свыше 70% рассматривают возможность обращения к правоохранительным органам как «АНТИРЕКЛАМУ».

Все эти предпосылки заставляют необходимость уяснения основных понятий - «ИНФОРМАЦИЯ», «ИНФОРМАЦИОННЫЙ ПРОЦЕСС», «КОМПЬЮТЕР» для правового регулирования и совокупности понятия нормативного регулирования в России информационных отношений и определить состояние правового обеспечения ситуации, складывающей в данной области.

Проблема информационных преступлений. Развитие терминологического аппарата позволило сформулировать новые терминологические определения видам информационных преступлений. Следует отметить такие наименования как «компьютерные преступления», «коммуникационные преступления», «кибербандитизм». При проведении расследований информационных несанкционированных действий терминологическая неточность толкования закона или методологические рекомендации по его исполнению может повлечь неправильное его применение. Поэтому необходимо знать правовые законодательные определения и терминологию, регулирующие правила расследований ситуаций, повлекшие за собой уголовную ответственность.

В соответствии с действующим законодательством: *информационные правоотношения – это отношения, возникающие при: формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации; создании и использовании информационных технологий и средств их обеспечения; защите информации, прав субъектов, участвующих в информационных процессах и информатизации.*

На основе действующего законодательства (Федеральный закон от 20 февраля 1995 г. №24-ФЗ) приняты следующие основные понятия [1].

1. *Информация* – сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления.

2. *Информатизация* – организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной вла-

сти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов.

3. *Документированная информация (документ)* – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

4. *Информационные процессы* – процессы сбора, обработки, накопления, хранения, поиска и распространения информации.

5. *Информационная система* – организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

6. *Информационные ресурсы* – отдельные документы и отдельные массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

7. *Информация о гражданах (персональные данные)* – сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.

8. *Конфиденциальная информация* – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

9. *Средства обеспечения автоматизированных информационных систем и их технологий* – программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию.

10. *Собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения* – субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами.

11. *Владелец информационных ресурсов, информационных технологий и средств их обеспечения* – субъект, осуществляю-

щий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных Законом.

12. *Пользователь (потребитель) информации* – субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

Под понятием «*информационные преступления*» понимаются – *общественно опасные деяния, запрещенные уголовным законом под угрозой наказания, совершенные в области информационных технологий.*

Основными задачами специалиста по защите информации в области информационных, компьютерных технологий являются:

♦ освоение студентами квалификации и навыков определения основных угроз информации в компьютерных системах и сетях;

♦ освоение принципов параллельного анализа целей и возможностей злоумышленника в компьютерных системах и методов проведения организационных мероприятий по обеспечению защиты информационных процессов;

♦ освоение методов защиты информационных процессов в автоматизированных системах приема, обработки, хранения и распространения информации в компьютерных системах.

2.2. Понятие информационной безопасности

Под термином «информационная безопасность», согласно определению Гостехкомиссии при Президенте РФ, понимают состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз: от нежелательного ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также ее незаконного тиражирования [2, 3], которые приводят к материальному или моральному ущербу владельца или пользователя информации [4]. Соответственно, под защитой информации подразумевается комплекс мероприятий, проводимых с целью предотвращения от действий угроз безопасности

информации, где угроза является потенциальной возможностью нарушения безопасности информации [4].

Когда говорят об информационной безопасности, то имеют в виду широкий спектр проблем: от стихийных бедствий и проблем с электропитанием до искушенных злоумышленников, которые используют вычислительные системы к своей выгоде, или шпионов, которые охотятся за государственными и коммерческими секретами.

Возникновение проблемы обеспечения информационной безопасности при подключении организаций к мировым открытым сетям напрямую связано с их основными достоинствами - оперативностью, открытостью, глобальностью. Без реализации основных мер безопасности любой пользователь имеет возможность добраться до любого компьютера, чтобы получить доступ к информации, к сетевым ресурсам или запустить программный модуль на удаленном компьютере.

Подключение к *Internet*, использование ее служб и сервисов само по себе не создает каких-либо принципиально новых проблем в области обеспечения информационной безопасности, отличных от тех, которые существуют при связи компьютерных систем по открытым каналам межмашинного обмена.

В общем виде основными угрозами информационной безопасности при подключении к *Internet* являются:

- несанкционированный (неавторизированный) доступ внешних пользователей сети *Internet* к какому-либо виду сервисного обслуживания, предоставляемого легальным пользователям (подобная угроза возникнет, если пользователи некоторых банковских сетей России, которым в *Internet* открыты только три сервиса - *WWW*, *FTP*, e-mail - попытаются воспользоваться сервисом telnet, позволяющим выполнять на удаленном компьютере команды, как если бы эти пользователи сидели за терминалом, непосредственно подключенном к данному компьютеру);
- доступ к информации и базам данных организаций без идентификации и аутентификации внешнего пользователя в сети, включая проникновение к ресурсам абонентов в абонентских пунктах или на хосты с целью НСД к информации, ее разрушения или искажения (по определению Гостехкомиссии России НСД - это доступ к информации, осуществляемый штатными техниче-

скими средствами с нарушением установленных правил разграничения доступа);

- перенос (импорт) в системы и сети организаций разрушающего программного обеспечения (ПО), которое может иметь вид вирусов, "троянских коней", "закладок" в теле электронных сообщений и т.д.;
- искажение (нарушение целостности) ПО систем и сетей организаций с целью изменения выполняемых ими функций, вплоть до полной дезорганизации их работы;
- нарушение конфиденциальности информационного обмена по каналам связи абонентов систем и сетей организаций, для чего эти каналы могут "прослушиваться" с помощью специальных программно-аппаратных средств;
- доступ к информации о топологии сетей и используемых в них механизмах защиты, что облегчает злоумышленникам проникновение в сети.

Результаты воздействия угроз могут выражаться в появлении сбоев в работе информационных систем организаций, искажении либо разрушении циркулирующей или хранящейся в них информации, нарушении защитных механизмов систем, что позволяет осуществить НСД к информации и контролировать работу информационных систем.

Internet в кредитно-финансовой сфере используется для взаимного информационного обмена между различными субъектами, а также для постоянной связи между территориально удаленными подразделениями и филиалами. Компьютерных преступлений в этой сфере, совершаемых через Internet, также существует очень много. Преступникам наиболее интересна информация о банковской, коммерческой тайне, тайне вкладов, сведения о финансовом положении самого банка и его клиентов, служебная информация, а также информация, позволяющая сделать выводы об инвестиционной и кредитной политике конкретного банка и направлениях его дальнейшего развития.

Другую группу преступлений в Internet - экономических - можно подразделить на два основных класса:

1) нарушение авторских и других смежных прав - незаконное копирование и продажа компьютерных программ, получен-

ных с хакерских узлов; изготовление пиратских копий компакт-дисков; незаконное изготовление печатной продукции с использованием компьютерных мини-типографий;

2) неоплачиваемое получение товаров и услуг (например, телефонных компаний – инструкции как это делать есть в журнале Phrack (http://www.phrack.com); модификация информации об услугах и их потребителях в базах данных соответствующих компаний путем взлома защиты компьютерных систем; другие виды мошенничества - незаконная организация азартных игр, организация фиктивных контор и т.д.).

Из вышеизложенного следует, что в Internet выделяется три уровня обеспечения информационной безопасности, начиная от простых и переходя к все более сложным механизмам защиты:

1) безопасность вычислительных платформ (аппаратного и программного обеспечения) сети или компьютера, что равнозначно обеспечению защиты каждого хоста в отдельности;

2) безопасность отдельно взятых сети или компьютера, что определяет политику защиты сети с контролем сетевого доступа к различным хостам и сервисам;

3) безопасность межсетевого взаимодействия сетей и отдельных компьютеров, имеющих подключение к Internet, что конкретизирует меры и средства защиты каналов связи между сетями и ПК.

2.3. Понятия, свойства информации

Информация – это результат отражения и обработки в человеческом сознании многообразия окружающего мира, это сведения об окружающих человека предметах, явления природы, деятельности других людей и т.д. Однако защите подлежит та информация, которая представляет ценность. Ценность определяется исключительно способностью получения выигрыша: морального, материального и т.д. Так как всегда находятся заинтересованные в получении такой информации, то и необходимо принимать меры по ее защите.

Необходимо отметить, что важность информации может быть представлена по категориям важности в следующем виде:

1) *жизненно* важная информация - незаменимая информация, наличие которой необходимо для функционирования организации;

2) *важная* информация – информация, которая может быть заменена или восстановлена, но процесс восстановления затруднен и связан с большими затратами;

3) *полезная* информация – информация, которую трудно восстановить, но организация может эффективно функционировать и без нее;

4) *несущественная* информация – информация, которая больше не нужна организации.

Данный принцип согласуется с принципом секретности. Под этим принципом понимается – административная или законодательная мера, соответствующая мере ответственного лица за утечку информации и потерю конкретной, с учетом государственных, военно-стратегических, коммерческих, служебных или частных интересов.

Виды и формы представления информации. Информация в компьютерных системах, как правило, представляется в виде: букв, символов, цифр; слов; текста; рисунков; формул; графиков; таблиц; планов; чертежей; карт географических, топологических и т.д.; технологических карт; алгоритмов и т.д. которых могут быть представлены в виде: постоянных переменных данных; команд; сообщений; справок; решений; приказов; распоряжений; заданий; отчетов; ведомостей; инструкций; комментариев; писем и записок; телеграмм; чеков; массивов; файлов и т.д.

Машинное представление информации. Информация, зафиксированная в материальной форме, называется сообщением. Сообщения могут быть *непрерывными* и *дискретными* (цифровыми).

Непрерывное сообщение – представление информации некоторой физической величины (электрический ток, напряжение и т.д.).

Дискретное сообщение – представление информации в виде фиксированного набора отдельных элементов в дискретные моменты времени. В компьютерных системах, использующие цифровое представление информации называют цифровыми системами.

Элементы, из которых состоит дискретное сообщение, называют буквами или символами. Набор этих букв – алфавит. Число символов в алфавите – объем алфавита. Объем алфавита определяет количество информации, доставляемый одним символом сообщения.

Физическое представление информации и процессы ее обработки. Непременным требованиям к физическим аналогам двоичного представления алфавита – надежность распознавания двух различных значений сигнала “0” или “1”.

В цифровых системах применяют три способа физического представления информации: потенциальный, импульсный и динамический в виде последовательного или параллельным кода. При использовании последовательного кода компьютерные системы (КС) работают медленно, при параллельном представлении быстрее, но при этом требуются значительные затраты на аппаратное оснащение.

Информация в КС подвергается вводу, хранению, обработке и выводу. Ввод информации в КС осуществляется с физических носителей информации: бумажных, магнитных, клавиатуры, специальных пультов и т.д.

Хранение информации производится на запоминающих устройствах: кратковременное – в ОЗУ и различных регистрах памяти; долговременное хранение – во внешних запоминающих устройствах, выполненных на магнитных лентах, барабанах, дисках и т.д.

Вывод информации производится на внешние устройства связи и регистрации информации без ее визуального отображения (на указанные выше носители информации), печатающие устройства, индикаторные табло и т.д. Выбор методов вывода информации определяется возможностями КС.

Информационные процессы в системах обработки данных может быть условно определены на три группы:

- информационно-справочное обеспечение должностных лиц органов управления;
- информационное обеспечение расчетных задач;
- обслуживание информационной базы КС.

Эти процессы реализуют должностные лица органов управ-

ления и обслуживающий персонал с помощью аппаратных средств автоматизации и связи.

Информация как объект права собственности. Большая проблема данного вопроса заключается в том, что защите подлежит не сама информация, а права собственности на информации. Это следует из того, что исторически сложилось - объектом собственности всегда являлось - материальные вещи. Информация - это идеальная категория, но всегда связана с материальными предметами - носителями информации: мозг человека, книга, диски, дискеты и т.п. Эти объекты обладают всеми свойствами товаров, с той лишь разницей, что подобный товар может копироваться, распространяться. Таким образом, не смотря на ряд особенностей, информация должна быть объектом собственности. Юридически это закреплено в Гражданском кодексом РФ (ст.128) от 21.10.94 г. Федеральным законом “Об информации, информатизации и защите информации” от 20.02.95 г. определено, что информационные ресурсы, отдельные документы или массивы документов, являясь объектами отношений физических и юридических лиц, подлежать обязательному учету и защите как материальное имущество собственника (ст. 4.1, ст. 6.1).

Информация - коммерческая тайна. Понятие коммерческой тайны, впервые, введено с 1 января 1991 г. статьей 33 закона “О предприятиях в СССР”. Правительство России 5 декабря 1991 года приняло постановление №35 «О перечне сведений, которые не могут составлять коммерческую тайну». Защита информации и прав субъектов в области информационных процессов регулируется главой 5 Федерального закона РФ «Об информации, информатизации и защите информации» и «Об коммерческой тайне». Перечень сведений сгруппированы по тематическим группам:

1. Сведения о финансовой деятельности.
2. Информация о рынке.
3. Сведения о производстве и продукции.
4. Сведения о научных разработках.
5. Сведения о системе материально-техническом обеспечении.
6. Сведения о персонале предприятии.
7. Сведения о принципах управления предприятием.
8. Прочие сведения (элементы систем безопасности, прин-

ципы защиты коммерческой тайны).

Законом РФ от 2 декабря 1990 года введено понятие «Банковская тайна».

2.4. Законодательство об информационных правоотношениях

Вся совокупность преступлений в сфере компьютерной информации может быть представлена в виде таблицы 2.1 (в скобках указаны соответствующие статьи УК РФ).

Виды субъектов	Виды действий	Виды объектов воздействия	Виды местонахождения объектов	Виды последствий
Лицо, имеющее доступ к ЭВМ (ст. 272, 274)	Неправомерный доступ (ст. 272)	Охраняемая законом компьютерная информация (ст. 272)	ЭВМ (ст. 272, 273, 274)	Уничтожение информации (ст. 272, 273, 274)
	Создание вредоносных программ (ст. 273)	Информация (ст. 273)	Система ЭВМ (ст. 272, 273, 274)	Блокирование информации (ст. 272, 273, 274)
	Использование вредоносных программ (ст. 273)	Программы (ст. 273)	Сеть ЭВМ (ст. 272, 273, 274)	Модификация информации (ст. 272, 273, 274)
	Распространение вредоносных программ (ст. 273)	Охраняемая законом информация (ЭВМ) (ст. 274)	Машинный носитель (ст. 272, 273)	Копирование информации (ст. 272, 273, 274)
	Внесение изменений в существующие программы (ст. 273)	Вредоносные программы (ст. 272)		Нарушение работы ЭВМ (ст. 272, 273, 274)
	Нарушение правил эксплуатации ЭВМ (ст. 274)			

Основные законодательные акты, регулирующие информационные отношения в области компьютерных преступлений представлены следующими законами [1].

Закон Российской Федерации «*О правовой охране программ для электронных вычислительных машин и баз данных*» (1992 г.). Целью данного закона является активизация и стимулирование отечественных разработчиков программных средств в области информационных технологий.

Закон Российской Федерации «*О правовой охране топологий интегральных микросхем*» (1992 г.). Данный закон регулирует в сфере защиты прав авторов и разработчиков программно-технического обеспечения. В законе зафиксированы понятия и правовые конструкции, отражающие представления законодателя об элементах охраняемой сфере. Даны юридические определения *программа для ЭВМ* и *базы данных*. Программа для ЭВМ рассматривается как форма представления совокупности данных и команд. База данных рассматривается как объективная форма представления и организации совокупности данных (например, статей, расчет), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны на ЭВМ.

Закон Российской Федерации «*Об авторском праве и смежных правах*» (1993 г.) регулирует отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства, фонограмм, исполнений, постановок, передач организаций эфирного и кабельного вещания (смежные права).

Закон Российской Федерации «О государственной тайне» (1993 г.) регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации. Законом определено понятие *государственной тайны* как защищаемые государством сведения в области военной, внешнеполитической, экономической, разведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. В закон введено определение носителей сведений, составляющих государственную тайну и средства защиты информации. К носителям сведений отнесены материальные объекты, в том числе физические поля в которых сведения, составляющие государственную тайну, находят

свое отражение в виде символов, образов, сигналов, технических решений и процессов. К средствам защиты относятся технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющие государственную тайну, а также средства контроля эффективности защиты информации. Важным является и определение доступа к сведениям, составляющим государственную тайну.

Закон Российской Федерации «*Об обязательном экземпляре документов*» (1993 г.) определяет понятие *документа*. Под документом понимается материальный объект с зафиксированной на нем информацией в виде текста, звукозаписи или изображения, предназначенный для передачи во времени и пространстве в целях хранения и общественного использования. В 5 статье этого закона отражена классификация документов.

Закон Российской Федерации «*О связи*» (1995 г.) установил правовую основу деятельности в области связи, определил полномочия органов государственной власти по регулированию указанной деятельности, а также права и обязанности физических лиц, участвующих в указанной деятельности или пользующихся услугами связи.

Закон Российской Федерации «*Об информации, информатизации и защите информации*» (1995 г.) регулирует отношения, возникающие при: формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации; создании и использовании информационных технологий и средств их обеспечения; защите информации, прав субъектов, участвующих в информационных процессах и информатизации.

Закон Российской Федерации «*Об участии в международном информационном обмене*» (1995 г.) создает условия для эффективного участия России в международном обмене в рамках мирового информационного пространства, защита интересов Российской Федерации, субъектов Российской Федерации, и муниципальных образований при международном обмене, защита интересов, прав и свобод физических и юридических лиц при международном информационном обмене.

2.5. Классификация компьютерных систем

Классификация компьютерных систем проводится по следующим признакам [2]:

- по способу построения;
- по функциональному назначению;
- по размещению информации в сети;
- по числу главных вычислительных машин (ГВМ)
- по типу используемых ЭВМ
- по методу передачи данных
- по реализации топологии соединения компьютерных систем в сети.

По способу построения, различают на сосредоточенные и распределенные (Рис. 2. 1).

По функциональному назначению различают компьютерные системы: автоматизированной обработки данных и автоматизированные системы контроля управления производством, технологическими процессами и объектами. Автоматизированные системы обработки данных различают: *информационные,* предоставляющие пользователю в основном информационное обслуживание; *вычислительные,* выполняющие главным образом решение задач с обменом данными и программами между ЭВМ сети, и *смешанные информационно-вычислительные.*

По размещению информации в системе разделяют с централизованным банком данных, формируемым в одном из узлов системы, и с распределенным банком данных, состоящим из отдельных локальных банков, расположенных в узлах системы.

По степени территориальной рассредоточенности можно выделить крупномасштабные, или *глобальные, вычислительные системы,* охватывающие территорию страны, нескольких стран с расстояниями между узлами сети, измеряемыми тысячами километров; *региональные системы,* охватывающие определенные регионы — город, район, область и т. п.; *локальные вычислительные системы* с максимальным расстоянием между узлами системы не более нескольких километров.

Рис. 2. 1. Классификация компьютерных систем по способу построения

По числу ГВМ следует различать сети с несколькими и с одной ГВМ. Последние относятся к вычислительным системам с телеобработкой, которые представляют собой комплексы, состоящие из вычислительной машины и удаленных абонентских пунктов (АП), связанных с помощью каналов и аппаратуры передачи данных.

По типу используемых ЭВМ выделяют *однородные сети,* содержащие программно-совместимые машины, и *неоднородные,* если машины сети программно несовместимы. На практике сети часто являются неоднородными.

По методу передачи данных различают вычислительные сети с коммутацией *каналов*, с коммутацией *сообщений*, с коммутацией *пакетов* и со *смешанной* коммутацией. Для современных

компьютерных систем и сетей характерно использование коммутации пакетов.

Коммутация пакетов является развитием метода коммутации сообщений. Она позволяет добиться дальнейшего увеличения пропускной способности сети, скорости и надежности передачи данных.

Поступающее от абонента сообщение разбивается на пакеты, имеющие фиксированную длину, например 1 Кбайт. Пакеты метятся служебной информацией-заголовком, указывающим адрес пункта отправления, адрес пункта назначения и номер пакета в сообщении.

В системе передачи данных между абонентами с коммутацией пакетов используются два способа передачи: *дейтаграммный* и *виртуальный.*

Дейтаграммный способ — передача данных отдельных, не связанных между собой пакетов. Важным достоинством дейтаграммного способа коммутации пакетов является возможность одновременной передачи пакетов одного и того же сообщения разными маршрутами, что уменьшает время и увеличивает надежность передачи сообщения. При передаче короткими пакетами уменьшаются вероятность появления ошибок и время занятости каналов повторными передачами. Однако при этом наблюдаются случаи обгона сообщений. Привязка сообщений ко времени их выдачи и нумерация позволяют это обнаружить. При дейтаграммном способе не гарантируется очередность и надежность доставки пакетов.

Виртуальный способ – передача данных в виде последовательностей связанных в цепочки пакетов. Организация виртуального канала между двумя процессами равносильна выделению им дуплексного канала связи, по которому данные передаются в их естественной последовательности. Виртуальный канал сохраняет все вышеописанные преимущества коммутации пакетов в отношении скорости передачи и мультиплексирования, но требует предварительной процедуры установления соединений. По окончании сеанса связи канал распадается и возвращает ресурсы для установления новых виртуальных соединений.

Важным признаком классификации компьютерных систем является *реализация топологии их соединения в сети.* Топологи-

ческая структура сети оказывает значительное влияние на ее пропускную способность, устойчивость сети к отказам ее оборудования, на логические возможности и стоимость сети. В настоящее время наблюдается большое разнообразие в топологических структурах вычислительных сетей: (Рис. 2. 1).

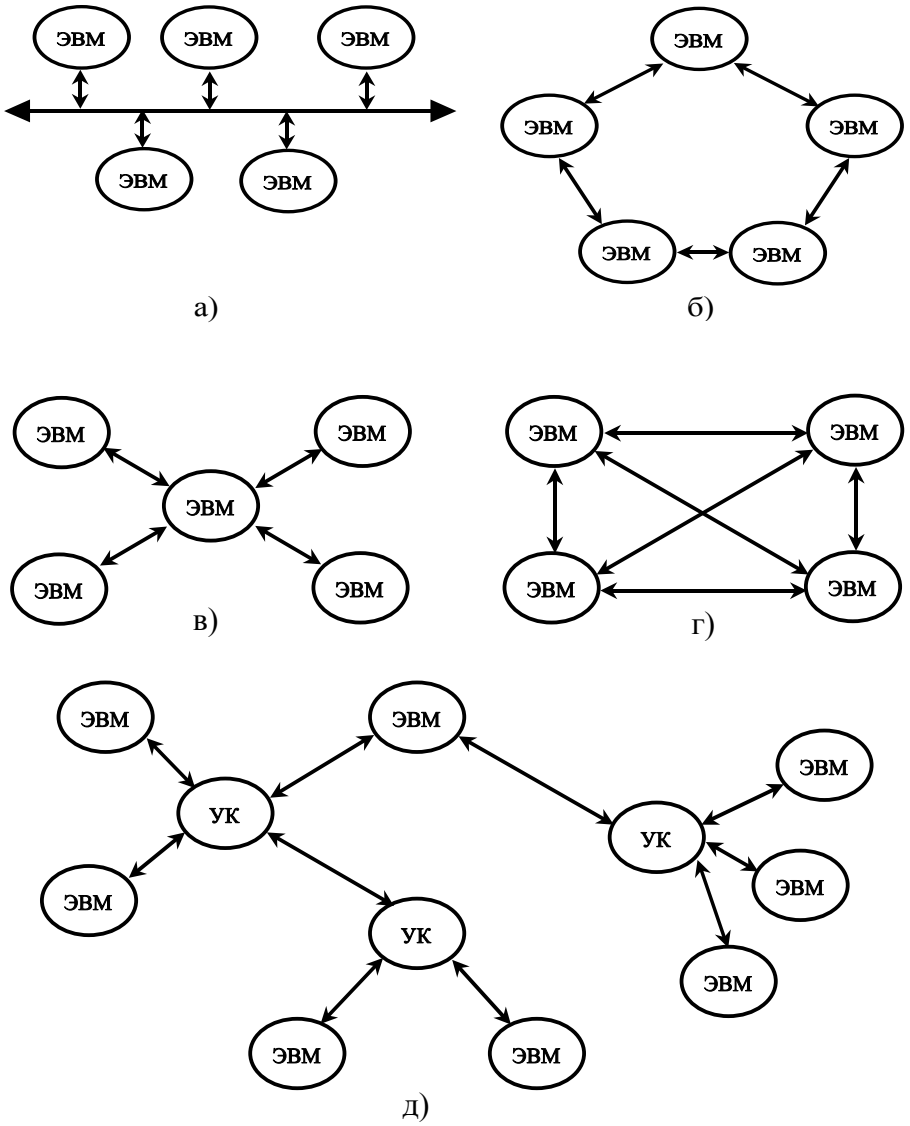


Рис. 2. 2. Топологические структуры компьютерных вычислительных сетей (*а* — одинарная многоточечная линия типа «шина»; *б* — петлевая сеть типа «кольцо»; *в* — звездообразная сеть типа «звезда»; *г* — полносвязная сеть; *д* — древовидная сеть

Топология крупных компьютерных систем может представлять собой комбинацию нескольких топологических решений.

В вычислительных сетях (системах) ее абоненты оснащаются специальными программными средствами для сетевой обработки данных. К программным средствам предъявляются требования по сохранению работоспособности сети при изменении ее структуры, при отказах отдельных ЭВМ, каналов и узлов связи, а также обеспечению возможности работы ЭВМ с терминалами различных типов и взаимодействия разнотипного оборудования.

2.6. Объекты защиты в персональных компьютерах и компьютерных системах

При анализе и оценки прочности защиты информации необходимо знание объекта защиты, основ построения компьютерных систем, их перечень основных компонент. Основой компьютерных систем является персональный компьютер [2].

Классическая структурная схема компьютера представлена на рисунке (Рис. 2. 3), включающая: арифметическо-логическое устройство, память, управляющее устройство, устройство ввода-вывода, клавиатура, операционная система, комплект программ технического обслуживания, пакета прикладных программ.

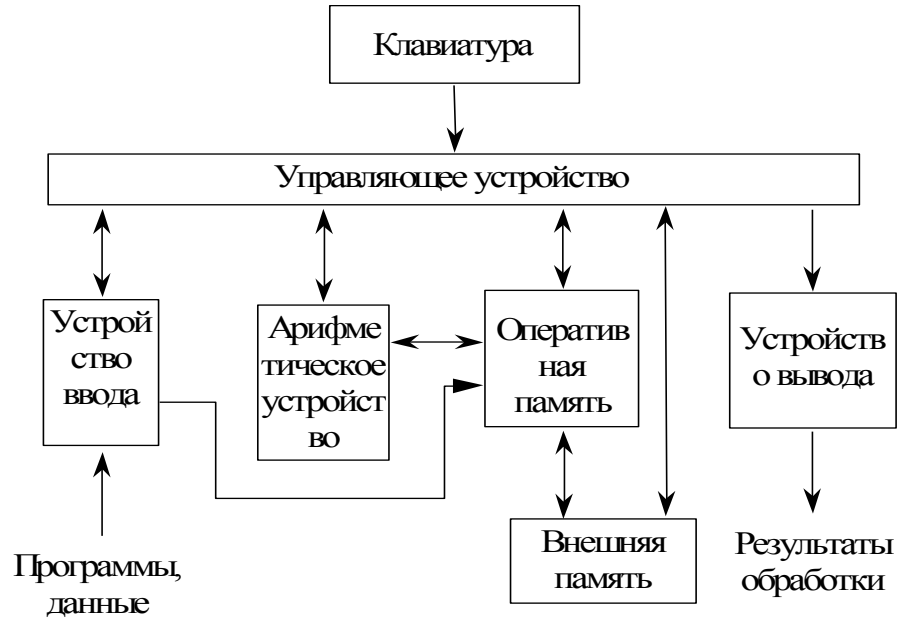


Рис. 2. 3. Структурная схема персонального компьютера

Арифметическо - логическое устройство (АЛУ) производит арифметические и логические преобразования над поступающи-

ми в него машинными словами, т.е. кодами определенной длины, представляющими собой числа или другой вид информации.

Память - хранит информации, передаваемую из других устройств в том числе извне через устройство ввода и вывода информации, необходимую для протекания вычислительного процесса.

Управляющее устройство - необходимо для обеспечения автоматического управления вычислительного процесса. Выполняет отдельные операции по заданному *алгоритму решения задачи численным методом.* Все операции проводятся в соответствии с программой, состоящей из отдельных команд.

Устройство вывода служит для выдачи из машины информации.

Клавиатура необходима для обеспечения ручного ввода, запуска, остановки и изменения алгоритма или программы работы компьютера.

Система программного обеспечения поддерживается с помощью *операционной системы.* Структура программного обеспечения представлена на рисунке (Рис. 2. 4).

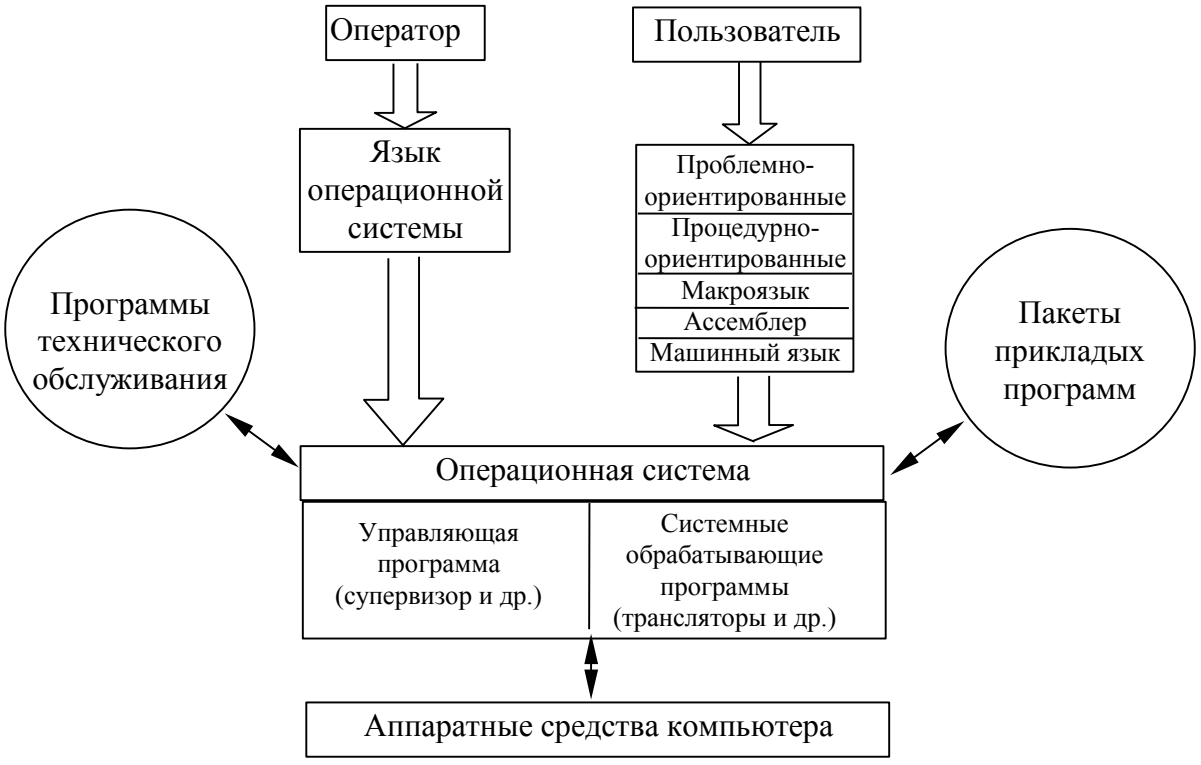


Рис. 2. 4.Структурная схема программного обеспечения персонального компьютера

Операционные системы предназначены для эффективного управления вычислительным процессом, планирования и автоматизации процесса. Операторы, работающие за компьютером, не имеют прямого доступа к устройствам ЭВМ. Связь операторов с компьютером проводится при помощи операционной системы, поддерживающей определенный уровень общения человека с машиной. Уровень общения определяется уровнем языка, на котором оно происходит (Си++, Паскаль, и др.).

Комплект программ технического обслуживания предназначены для уменьшения трудоемкости эксплуатации компьютера и содержит программы проверки работоспособности машины и отдельных ее устройств и их диагностики.

Пакеты прикладных программ предназначены для решения конкретных задач (инженерно-технических, планово- экономических и др.), а также для расширения функций операционных систем (управления базами данных, управления режимами телеобработки и др.).

3. АНАЛИЗ ПОТЕНЦИАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

3.1. Постановка задачи анализа потенциальных угроз

Исследование и анализ случаев воздействий на информацию и НСД к ней показывают, что их можно разделить на непренамеренные и преднамеренные. При этом преднамеренные угрозы, как правило, в результате систематического применения могут быть приведены через случайные путем долговременной массивной атаки несанкционированными запросами или вирусами.

Последствия, к которым приводит реализация угроз: разрушение (утрата) информации, модификация (изменение на ложную, которая корректна по форме и содержанию, но имеет другой смысл) и утечки информации (несанкционированное копирование с целью хищения). Для создания средств защиты информационных процессов и информации необходимо определить природу угроз и путей их возможного проявления в КС. Для решения поставленной задачи все многообразие угроз и путей их воздействия приведем к простейшим видам и формам, которые были бы адекватны их множеству в КС.

Исследование и оценка уровня защиты информации и информационных процессов сводится к классификации потенциальных угроз, которые могут быть определены как случайные угрозы и преднамеренные угрозы.

3.1.1. Случайные угрозы

При исследовании опыта проектирования отмечается, что информация подвергается угрозе в процессе ввода, хранения, обработки, вывода и передачи. В результате таких воздействий на аппаратном уровне происходят физические изменения уровней сигналов в цифровых кодах, несущих информацию. При этом наблюдается изменение «1» на «0» или «0» на «1». Если применяемые средства функционального воздействия способны это обнаружить (например, обнаружение однократной ошибки), то произ-

водится браковка данного кода, а устройство или изделие признается неисправным. В противном случае происходит дальнейшее изменение передаваемой информации.

Если изменения происходят на *программном* уровне, в результате случайных воздействий возможно изменение алгоритма обработки информации, что ведет к непредсказуемым последствиям. При программных ошибках могут подключаться устройства ввода-вывода и передача их на запрещенные устройства.

Причинами случайного воздействия могут быть:

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

Частота отказов и сбоев аппаратуры увеличивается, если на *этапе проектирования* не учитывают перечисленные выше факторы возникновения случайных угроз. Помехи, возникающие в линиях связи, зависят от выбора технических средств и их размещения относительно друг друга и по отношению к другим компьютерным системам. В процессе проектирования компьютерных систем на надежность оказывает квалификация разработчиков, условия их работы, наличие опыта и др.

На *этапе изготовления* и испытаний на качество входящей в компьютерную систему аппаратуры влияют полнота и качество технической документации, по которой она изготавливается и технологическая дисциплина на этапе изготовления.

К ошибкам человека как звена системы следует отнести ошибки как источника информации, человека – неправильные действия работы обслуживающего персонала и ошибки человека, как звена принимающего решения. Ошибки человека делятся на *логические* (неправильные решения), *сенсорные* (неправильное восприятия оператором информации) и *оперативные*, или моторные (неправильная реализация решения). Интенсивность ошибок человека может колебаться в переделах от 1-2% до 15-40% и выше общего числа операция, выполняемых при решении задач.

Интенсивность ошибок влияет от состояния человека и характеризуется его утомляемостью, его психологического параметра, возраста, чувствительность к изменению окружающей среды, зависимость качества работы от физического состояния, эмоциональность.

Для расчета достоверности выходной информации важны статистические данные по уровню ошибок человека как звена системы. Как показывает анализ работы систем, интенсивность ошибок человека составляет $2 \cdot 10^{-2} – 4 \cdot 10^{-3}$. Ошибки человека как звена системы, принимающего решения, определяются неполной адекватностью представления человеком реальной ситуации и создание упрощенной модели рассматриваемой ситуации.

К угрозам случайного характера следует отнести также аварийные ситуации, которые могут возникнуть на объекте, где размещена компьютерная система. К таким аварийным ситуациям следует отнести:

- ♦ отказ функционирования компьютерной системы в целом в результате отключения электропитания и освещения;
- ♦ стихийные бедствия: пожар, наводнение и т.п.;
- ♦ отказ системы жизнеобеспечения на объекте эксплуатации компьютерной системы.

Вероятность этих событий связана с правильным размещением, включая его географическое размещение, организаций противопожарных мероприятий.

3.1.2. Преднамеренные угрозы

Преднамеренные угрозы связаны с действиями человека, причинами которых могут быть определенные недовольства своей жизненной ситуацией, материальным интересом или простым развлечением. Потенциальные угрозы с этой стороны следует рассматривать только в техническом аспекте. Для постановки задачи защиты информационных процессов необходим анализ объекта защиты на предмет ввода-вывода, хранения и передачи информации и возможностей нарушителя по доступу при отсутствии средств защиты. Для компьютерных систем характерны следующие штатные каналы доступа к информации:

♦ терминалы пользователей;

♦ терминал администратора системы;

♦ терминал оператора функционального контроля (оператора системы);

♦ средства отображения информации;

♦ средства документирования информации;

♦ средства загрузки программного обеспечения в компьютерной системы;

♦ носители информации (ОЗУ, ДЗУ, бумажные носители);

♦ внешние каналы связи.

Для реализации НСД нарушитель может получить доступ к аппаратуре, программному обеспечению и осуществить хищение, модификацию, разрушение информации:

♦ при их использовании законными пользователями не по назначению и за пределами своих полномочий всех перечисленных штатных средств;

♦ использование посторонними лицами все перечисленные штатные средства;

а также по следующим техническим каналам через:

♦ технологические пульты;

♦ внутренний монтаж аппаратуры;

♦ линии связи между аппаратными средствами данной компьютерной системы;

♦ побочное электромагнитное излучение информации средствами данной компьютерной 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, брошенных в мусорную корзину.

В состав аппаратуры компьютерной системы (Рис. 3. 1) входят персональный компьютер, принтер, цифровые табло, телефонные аппараты, ксерокс, сканер и т.п.

При наличии *свободного доступа*, при отсутствии служебного персонала нарушитель может наблюдать информацию на устройствах отображения, похитить информацию, как на бумажных, так и на магнитных носителях. Наиболее опасным является незаконная загрузка нештатного программного продукта типа «троянского коня», вируса и т.д. Если нарушитель является законным пользователем, то данная опасность возрастает многократно, так как возможен съём информации, ценность который выходит за пределы его полномочий и доступа. При неоднозначной идентификации информационных ресурсов нарушитель способен подавить системную библиотеку своей, позволяющую обеспечить свободный доступ ко всей информации имеющейся в данной компьютерной системе.

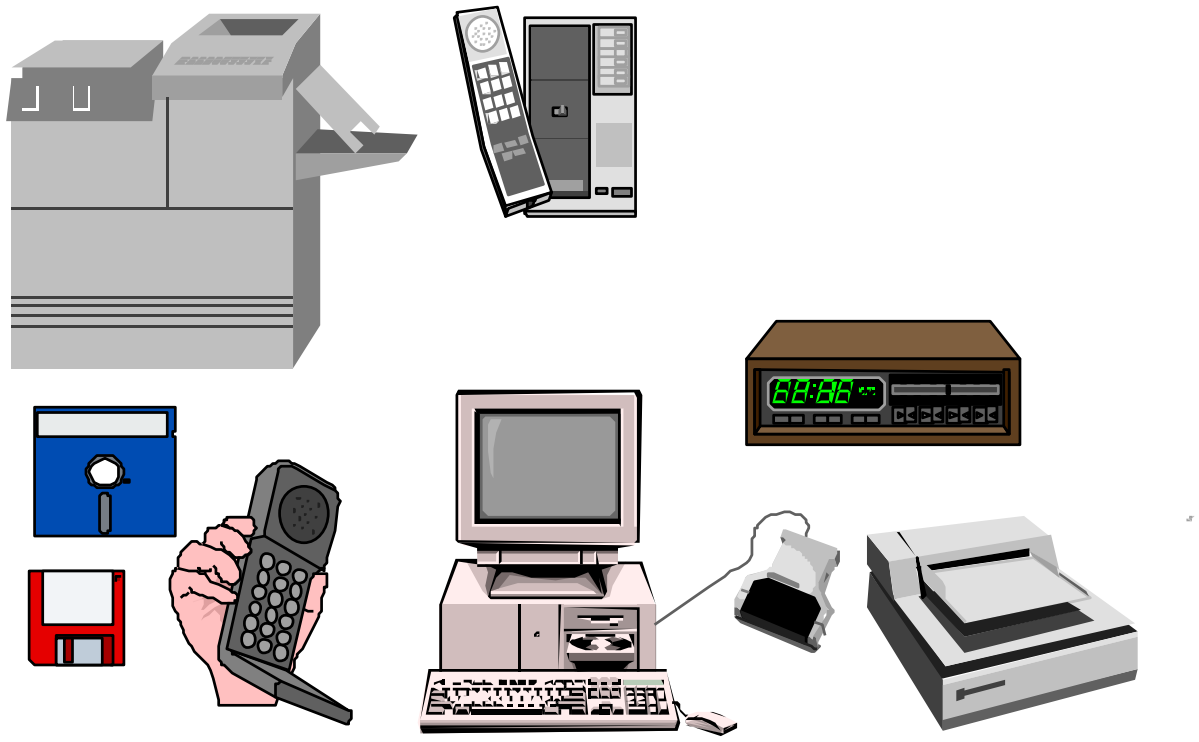


Рис. 3. 1. Состав аппаратуры компьютерной системы

При техническом обслуживании (профилактике и ремонте) аппаратуры могут быть обнаружены остатки стертой информации. При обычной процедуре удаления файлов на диске остаются

фрагменты удаленной информации. При транспортировании магнитных носителей может быть осуществлен ее перехват и прочтение посторонними лицами с целью извлечения секретной информации.

При анализе возможных путей доступа к информационным процессам следует отметить угрозы, которым могут подвергаться каналы и компьютерные сети (Рис. 3. 2). На схеме показана, что нарушитель может подключит на участке *B* и работать под мнимом шлюзом, контролируя тем самым весь информационный поток и осуществлять как пассивный, так и активный его перехват.

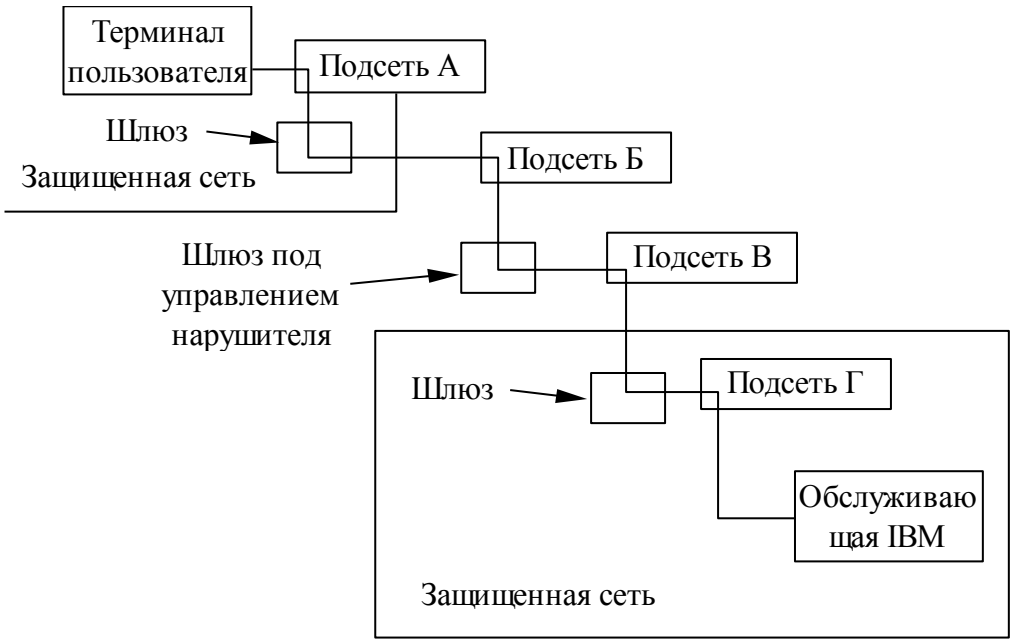


Рис. 3. 2. Схема возможного подключения нарушителя к сети компьютерной системы

При *пассивном* перехвате нарушитель следит только за потоком информации, раскрывая содержание сообщений. Нарушитель определяет длину передаваемого сообщения, частоту их передачи с целью анализа потока данных.

При *активном* перехвате нарушитель имеет возможность модифицировать или вводит дезинформацию (ложное сообщение), задержку сообщений. Подобные нарушения квалифицируется как изменение потока и содержания сообщений.

Как показывает анализ угроз информационным процессам, следует отметить пять видов угроз:

1) раскрытие содержания передаваемых сообщений;

2) анализ трафика, позволяющий определить принадлежность отправителя и получателя;

3)изменение потока сообщений, что может привести к нарушению режима работы какого-либо объекта, управляемого удаленным компьютером;

4)неправомерный отказ в представлении услуг;

5)несанкционированное установление соединений.

Все перечисленные определения классификации не противоречат принципу деления на угрозы: модификации и утраты информации.

В компьютерных системах нарушитель может применить следующие стратегии:

- получить несанкционированный доступ;
- выдать себя за другого пользователя и воспользоваться его полномочиями;
- отказаться от факта формирования переданной информации;
- утверждать, что информация получена от некоторого пользователя, хотя она сформирована им самим;
- утверждать, что информации передана пользователю, на самом деле она им не была отправлена;
- отказаться от факта получения информации;
- незаконно расширить свои полномочия;
- незаконно сменить полномочия других пользователей;
- скрыть факт наличия некоторой информации в другой информации (скрытая передача одной информации в содержании другой);
- подключиться к линии связи между другими пользователями в качестве активного ретранслятора;
- изучить, кто и когда и к какой информации получает доступ;

- заявить о сомнительности протокола обеспечения информацией из-за раскрытия некоторой информации, которая должна быть секретной;
- модифицировать программное обеспечение путем добавления новых функций;
- преднамеренно изменить протокол обмена информацией с целью его нарушения или подрыва доверия к нему;
- помешать обмену сообщения между другими пользователями.

Таким образом, очень важно считать, кого считать нарушителем. Поэтому необходимо рассматривать в качестве нарушителя не только постороннее лицо, но законного пользователя.

Большая вероятность угрозы исходит для нарушителя в сети *Internet*. В таблице 3 представлены вероятности проявления угроз информационной безопасности в *Internet*.

Таблица 3. 1 - Угрозы информационной *безопасности в Internet*

Угрозы	Вероятность проявления
Небрежность	0,188
Пиратство	0,166
Неточная или устаревшая информация	0,159
Утечка данных	0,159
"Шутки" над коллегами	0,150
Наблюдение за излучением	0,133
Умышленные повреждения данных и программ	0,129
Нарушение аутентификации	0,129
Перегрузка	0,119
Неправильная маршрутизация	0,106
Аппаратные сбои	0,090
Искажение	0,080
Сетевые анализаторы	0,074
Мошенничество	0,058
Пожары и другие стихийные бедствия	0,043
Подлог	0,033
"Логические бомбы"	0,032
Кража	0,032
Блокирование информации	0,016
"Потайные ходы и лазейки"	0,010

Возможные пути реализации угроз потенциальными нарушителями приведены в таблице 3.2.

Таблица 3. 2 - Матрица угроз информации и информационным процессам

Объекты воздействия	Нарушение конфиденциальности информации	Нарушение целостности информации	Нарушение работоспособности системы
Аппаратные средства	НСД - подключение; использование ресурсов; хищение носителей	НСД - подключение; использование ресурсов; модификация, изменение режимов	НСД - изменение режимов; вывод из строя; разрушение
Программное обеспечение	НСД - копирование; хищение; перехват	НСД, внедрение "троянского коня", "вирусов", "червей"	НСД - искажение; удаление; подмена
Данные	НСД - копирование; хищение; перехват	НСД - искажение; модификация	НСД - искажение; удаление; подмена
Персонал	Разглашение; передача сведений о защите; халатность	"Маскарад"; вербовка; подкуп персонала	Уход с рабочего места; физическое устранение

Следует также, что задачу защиты от нарушителей условно можно разделить на два уровня:

- пользовательский уровень;
- уровень элементов и компонентов компьютерной системы.

При анализе прочности защиты информации и информационной процессов необходимо учитывать также уровень доверия между пользователями

3.2. Анализ электромагнитных излучений и наводок в компьютерных системах

3.2.1. Характеристики излучения протоколов обмена

Известно, что спектр периодического сигнала имеет дискретный характер, т.е. определен набором амплитуд отдельных гармонических составляющих, частота которых кратна частоте сигнала. Поэтому использование в протоколах обмена импульсных сигналов прямоугольной формы и высококачественной коммутации в аппаратной части средств защиты информации (СЗИ) приводит к тому, что в спектр излучений входят различные компоненты, вплоть до СВЧ. Измерения показали, что напряженность электрического поля излучения протоколов обмена дости-

гает 25 дБ и выше - до частот в сотни МГц. В качестве примера в таблице 3.3 приведены данные измерений нормированной величины излучения сигналов протокола обмена контроллера СЗИ, встроенного в ПЭВМ, с электронным идентификатором DS.

Таблица 3. 3 - Нормированные величины излучения

Частота излучения, МГц	Относительная напряженность электрического поля E, дБ	Частота излучения F, МГц	Относительная напряженность электрического поля E, дБ
1,08	13	6,2	17
1,35	13	10,15	25
2,05	13	18,2	25
2,8	23	27,1	20
3,6	20	54,6	23
5,13	25	135,2	24

Съем параметров проводится на расстоянии одного метра от объекта. Вид принимаемых сигналов контролировался с помощью осциллографа, подключенного к выходу селективных приемников. Для других систем защиты информации или контроля доступа (например, использующих в качестве устройств аутентификации пользователей *Proximiti*-карты) значения относительной напряженности поля могут значительно превышать величины, указанные в таблице 4.1. Расчеты показывают, что с учетом минимальной длительности импульсных сигналов обмена приемник, предназначенный для съема информации и ее полного восстановления, при соотношении сигнал - шум 10 дБ, должен обладать полосой пропускания не менее 40 кГц и чувствительностью приемника 0,15 - 0,2 мкВ. Указанными параметрами обладает ряд устройств, предлагаемых на российском рынке.

3.2.2. Анализ спектра излучения протокола обмена

Не выделяя акцентов на конкретных средствах защиты, системах контроля доступа, электронных идентификаторах и их конструктивных особенностях, рассмотрим возможные способы, обеспечивающие надежную защиту протоколов обмена СЗИ от «взлома» путем перехвата и последующего анализа побочных электромагнитных излучений. Это, прежде всего, использование в протоколах обмена сигналов в виде псевдослучайных импульс-

ных последовательностей (ИП), представляющих собой дискретные стационарные процессы с распределением отдельных параметров (независимых между собой) по тому или иному заранее заданному принципу. Такой анализ параметров импульсной последовательности в любом интервале времени позволяет идентифицировать пользователя. После каждого обмена между средством идентификации и аппаратной частью СЗИ необходимо изменение и запись характеристик последовательности распределения случайных параметров импульсной последовательности. Это позволит максимально снизить возможность «взлома» системы путем перехвата и анализа ПЭМИН. В качестве случайных параметров импульсной последовательности в цифровых схемах обработки сигналов используются: длительность отдельных импульсов, временные расстояния между импульсами или комбинации длительности и расстояния.

При цифровой обработке предыскаженных импульсных последовательностей для восстановления исходной формы цифровых сигналов в аппаратной часты средств защиты используются программируемые цифровые фильтры с максимальной разрядностью, соизмеримой с шумами канала связи. С помощью программируемых предыскажений задается определенная скорость изменения огибающей импульсов цифровых сигналов, соответственно, фиксирование уровней внеполосных излучений. Максимальная вероятность идентификации при минимальных временных интервалах анализа сигнала и затраты памяти ПЭВМ достигается путем применения интерполяционного метода обращения к табличному ПЗУ, содержащему информацию о форме генерируемого импульса.

Идентификация пользователя в этом случае основана на фильтрации сигнала на входе системы и анализе информационного импульса. При построении данного способа защиты учитывается необходимость генерации шумового сигнала в достаточно широком диапазоне частот и восстановления исходной формы видеосигналов после фильтрации шумовой помехи.

3.2.3. Анализ спектра излучения наводок оборудованием компьютерной системы

Наряду с общеизвестными каналами утечки информации (несанкционированный доступ, подключения к линиям связи или устройствам вычислительной техники и т.д.), возможен и радиотехнический канал утечки, когда информация может быть перехвачена приёмом сигналов побочного электромагнитного излучения и наводок (ПЭМИН), возникающего при функционировании устройств вычислительной техники. Одним из направлений обеспечения информационной безопасности является защита информационных процессов и информации снимаемой за счет ПЭМИН. Для создания простейшей системы восстановления информации за счет приема ПЭМИН необходимо знать, частоты излучения, мощность и полосу принимаемых полезных сигналов, необходимое усиление приемника и антенны.

Измерения в помещении при расстоянии от приемной антенны до ПЭВМ 15 м наблюдается относительное отсутствие помех, вносимых различными устройствами. Результаты, характеризующие окружающую электромагнитную обстановку, представлены на рисунках (Рис. 3. 3) … (Рис. 3. 5) [4].

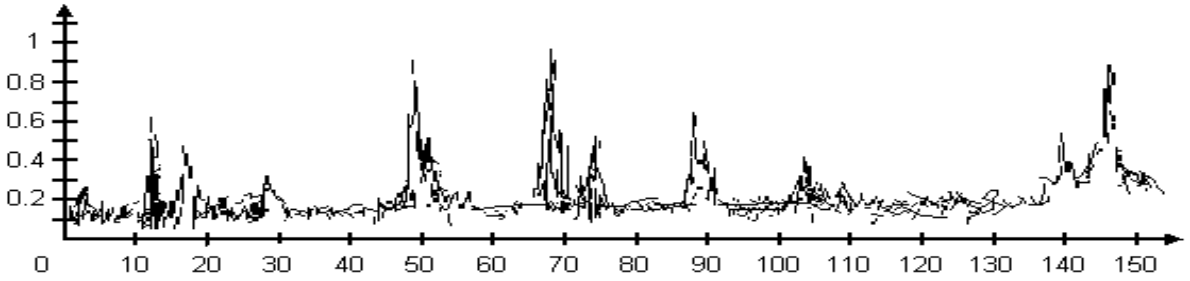


Рис. 3. 3. Электромагнитная обстановка при отключенном компьютерном оборудовании

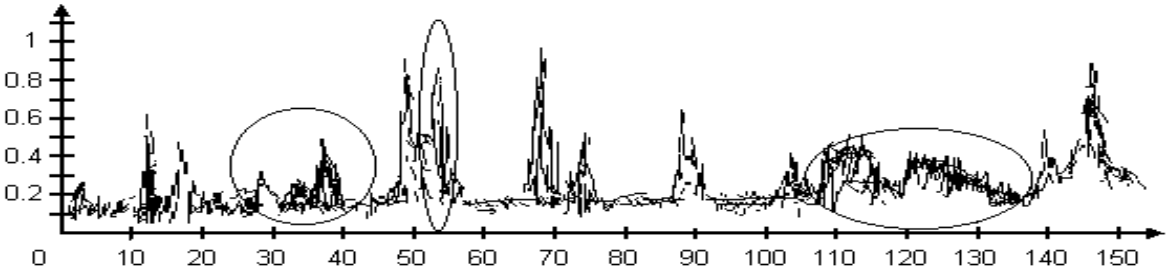


Рис. 3. 4. Электромагнитная обстановка при включенных мониторе и системном блоке

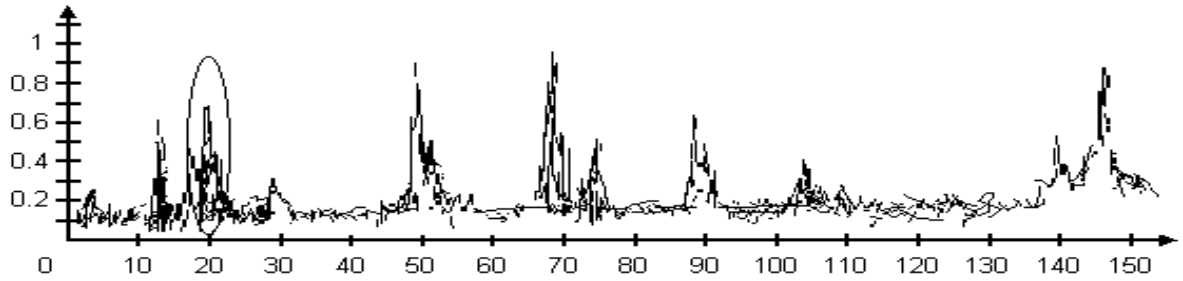


Рис. 3. 5. Электромагнитная обстановка при включенном принтере

Как видно из результатов исследования побочного электромагнитного излучения и наводок дисплея занимают несколько частотных диапазонов: 30…40 МГц; 50…55 МГц; 110…150 МГц. Побочное излучение принтера зафиксировано на частоте 20 МГц. Уровень принимаемых сигналов имеет значения от 3 … 25 дБ при чувствительности радиоприёмной системы –115 дБ/Вт. Максимальный уровень сигнала излучает дисплей практически со всех сторон кроме экрана.

Экран с расчетными характеристиками установленный по периметру внутри корпуса дисплея показал, что в этом случае ПЭМИН можно зафиксировать непосредственно у экрана дисплея на расстоянии 0,2 м.

4. МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

4.1. Обзор методов защиты информационных процессов в компьютерных системах

Как бы сложна не была техника приема, передачи, хранения и обработки информации в компьютерных системах, до настоящего времени не потеряли своей актуальности такие традиционные методы как:

- ограничение доступа;
- разграничение доступа;
- разделение доступа;
- криптографическое преобразование;
- контроль и учет доступа;
- законодательные меры.

Указанные методы производятся с помощью организационных мероприятий и технических средств. Расширенный перечень носителей информации, требует и сложный механизм организации информационных процессов. В связи с этим увеличилось число случайных воздействий, число каналов утечки информации от несанкционированного доступа. Поэтому одновременно с развитием информационных процессов возникают новые дополнительные методы по их защите в компьютерных системах, такие как инженерно-технические и программно-аппаратные.

К *организационным методам* следует отнести такие методы как:

- методы функционального контроля, обеспечивающие обнаружение и диагностику отказов и сбоев аппаратуры и ошибок человека;
- методы повышения достоверности принимаемой и обрабатываемой информации;
- методы защиты информационных процессов от аварийных ситуаций;
- методы контроля доступа к внутреннему монтажу аппаратуры, линиям связи и технологическим органам контроля;

• методы разграничения и контроля доступа к информационным процессам;

• методы идентификации и аутентификации пользователей, технических средств, носителей информации и документов.

К *инженерно-техническим методам* защиты информации и информационных процессов относятся методы:

• пассивной защиты;

• активной защиты.

К *программно-аппаратные методам* защиты основаны на использовании *Программно-аппаратные методы* реализуются с использованием всех организационных и инженерно-технических средств как на территории, где размещена компьютерная система, так и за ее пределами.

Все перечисленные методы используются и применяются в компьютерных системах только с использованием организационной защиты информации и информационных процессов.

4.2. Организационные методы защиты информационных процессов в компьютерных системах

4.2.1. Ограничение доступа

Ограничение доступа заключается в создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лица, связанного с объектом защиты.

Ограничение доступа к комплексам средств автоматизации заключается:

♦ в выделении специальной территории для размещения системы;

♦ в сооружении по периметру зоны специальных заграждений с охраняемой сигнализацией;

♦ в сооружении специальных зданий или других сооружений;

♦ в выделении специальных помещений в здании;

♦ в создании контрольно-пропускной системы на территориях, зданиях, помещениях.

Задача средств ограничения доступа - исключить случайный и преднамеренный доступ посторонних лиц на территорию размещения компьютерной системы. В этом случае достаточно хорошо используются традиционные способы (удостоверения личности, контрольно-пропускная система, охранная сигнализация т.п.) и внедряются новые достижения идентификации сотрудника (отпечатки пальцев, голосовые и т.п.).

В настоящее время государственные предприятия выпускают электронные системы для защиты государственных и частных объектов от проникновения посторонних лиц. К таким системам относятся сигнализация использующие специализированные автоматизированные подключаемые к охраняемому объекту через телефонные каналы связи.

По принципу действия системы тревожной сигнализации можно классифицировать как:

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

В настоящее время на рынке средств защиты информации и информационных процессов появляются все новые и новые устройства, системы и комплексы. Разрабатываются и принимаются законодательные акты, регулирующие взаимоотношения владельцев, пользователей информационных ресурсов и служб безопасности.

4.2.2. Контроль доступа к аппаратуре

В целях контроля доступа к внутреннему монтажу, линиям связи и технологическим пультам управления используется аппаратура контроля вскрытия аппаратуры. Это обеспечивается установкой датчиков, которые срабатывают при вскрытии охраняемо-

го оборудования. Сигналы с датчиков поступают к автоматизированным системам контроля.

Контроль доступа к внутреннему монтажу необходим также для обеспечения технологической дисциплины обслуживающего персонала.

С позиции защиты от несанкционированного доступа от следующих действий:

♦ изменения и разрушения принципиальной схемы компьютерной системы;

♦ подключения постороннего устройства;

♦ изменения алгоритма работы КС путем использования технологических пультов и органов управления;

♦ загрузки посторонних программных продуктов (вирусов, и т.д.);

♦ использование терминалов посторонними лицами.

Основная задача контроля вскрытия аппаратуры - перекрытие на период эксплуатации всех нештатных и технологических подходов. Если такая ситуация требуется, то выводимая аппаратура за пределы контура для ремонта, профилактики т.д., в последствии вводится в контур под наблюдением специалистов ответственных за безопасность информационных процессов и защиты информации.

Доступ к штатным входам в систему - терминалам контролируется с помощью контроля выдачи ключей, а доступ к информации - с помощью системы опознания и разграничения доступа, включающей применение кодов паролей, соответствующие функциональные задачи программного обеспечения и специального терминала службы безопасности информации. Указанный терминал и устройство контроля входит в состав рабочего места службы безопасности информации.

4.2.3. Разграничение и контроль доступа

Разграничение доступа в компьютерной 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 разграничения доступа - сокращение количества должностных лиц, не имеющих к компьютерной системе отношение при выполнении служебных обязанностей.

Для обеспечения разграничения и контроля доступа к информационным процессам организация их обслуживания строится следующим образом:

♦ техническое обслуживание КС в процессе эксплуатации должно выполняться отдельным персоналом без доступа к информационным процессам;

♦ перезагрузка программного обеспечения и всякие его изменения должны производиться специально выделенными для этого специалистами;

♦ функции обеспечения безопасности должны выполнятся специальным подразделением в организации - владельце КС, вычислительной сети или АСУ;

♦ организация доступа пользователей к памяти КС обеспечивала возможность разграничения доступа к информации, хранящей в ней, с достаточной степенью детализации и в соответствии и в соответствии с заданным уровнем полномочий пользователей;

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

Разграничение доступа пользователей - потребителей КС может быть:

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

На этапе проектирования базового комплекса КС производят:

♦ разработку операционной системы с возможностью реализации разграничения доступа к информации и информационному процессу;

♦ изоляция общего доступа;

♦ разделение базы данных на группы;
♦ процедуры контроля перечисленных функций

При проектировании автоматизированных вычислительных комплексов и баз обработки банных производится:

♦ разработка и реализация функциональных задач по разграничению и контролю доступа к аппаратуре и информации как в рамках данной КС, так и в целом всей системы и контроля;

♦ 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 КС. В помощь пользователя в системах с повышенными требованиями большие значения кодов паролей записываются на специальные носители - электронные ключи или карточки.

4.2.4. Разделение привилегий на доступ

Разделение привилегий на доступ к информационным процессам 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 данного метода - существенно затруднить преднамеренный перехват информации нарушителем. Примером может служить сейф с замком, который открывается несколькими ключами одновременно. Такой же принцип механизм разделения привилегий доступа используется при использовании в КС.

Данный метод значительно усложняет процедуру работы, но является высокоэффективным средством защиты. На его принци-

пах 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 защиту информации и информационных процессов от преднамеренного несанкционированного доступа.

При наличии дефицита в средствах, а также в целях постоянного контроля доступа к ценной информации со стороны администрации и пользователя КС 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 только на дисплей руководителя, а на дисплей подчиненного - только информация о факте ее вызова.

4.2.5. Идентификация и установление подлинности

Объект идентификации и установление 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.

Объектами идентификации могут быть:

- ♦ человек (оператор, пользователь, оператор);
- ♦ техническое средство (терминал, дисплей, компьютер и т.д.);
- ♦ документы (распечатки, листинги и т.п.);
- ♦ носители информации (магнитные диски, ленты и т.п.);
- ♦ информация (табло, информация на дисплее).

Идентификация может быть произведена как специальным персоналом, так и техническими средствами.

Идентификация и установление подлинности личности. В качестве признака подлинности личности внешние признаки (рост, вес, формы отдельных частей тела и т.п.) правда со временем параметры человека меняются, но с развитием техники рас-

тет и точность прогнозирования этих изменений (отпечатки пальцев, голос и т.д.). Кроме антропологических параметров более внимательно необходимо относится к конфиденциальности, так как записанная информация на носителях является ключом к информации, подлежащей защите. Для этого существует система аутентификации “ключ-замок”. Система “ключ-замок” имеет локальный применение. Одним из распространенным методом аутентификации является присвоение лицу или объекту уникального имени или числа - пароля и хранение его в компьютерной системе. При входе в компьютерную систему пользователь открывает доступ к разрешенной только ему информации.

Алгоритм идентификации компьютерной системы представлен (Рис. 4. 1). Наиболее высокий уровень входа в систему разделение кода на две части: одну запоминаемую пользователем и вводимую вручную, вторую с помощью магнитной или иной карточкой.

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 экстренной ситуации.

Однако, учитывая опасность для жизни пользователя необходимо в компьютерной системе одновременно со скрытой сигнализацией предусмотреть механизм обязательного выполнения требований преступника, воспользовавшись средствами аутентификации законного пользователя.

Идентификация и установление подлинности технических средств. При организации системы защиты информационных процессов является идентификация подлинности технических средств. Данный уровень защиты осуществляется с помощью паролей. Пароль используется не только для пользователя и терминала по отношению к системе, но и для обратного установления подлинности компьютера по отношению к пользователю. Это используется для работы с удаленным объектом. В этом случае используются одноразовые пароли или более сложные системы шифрования информации.

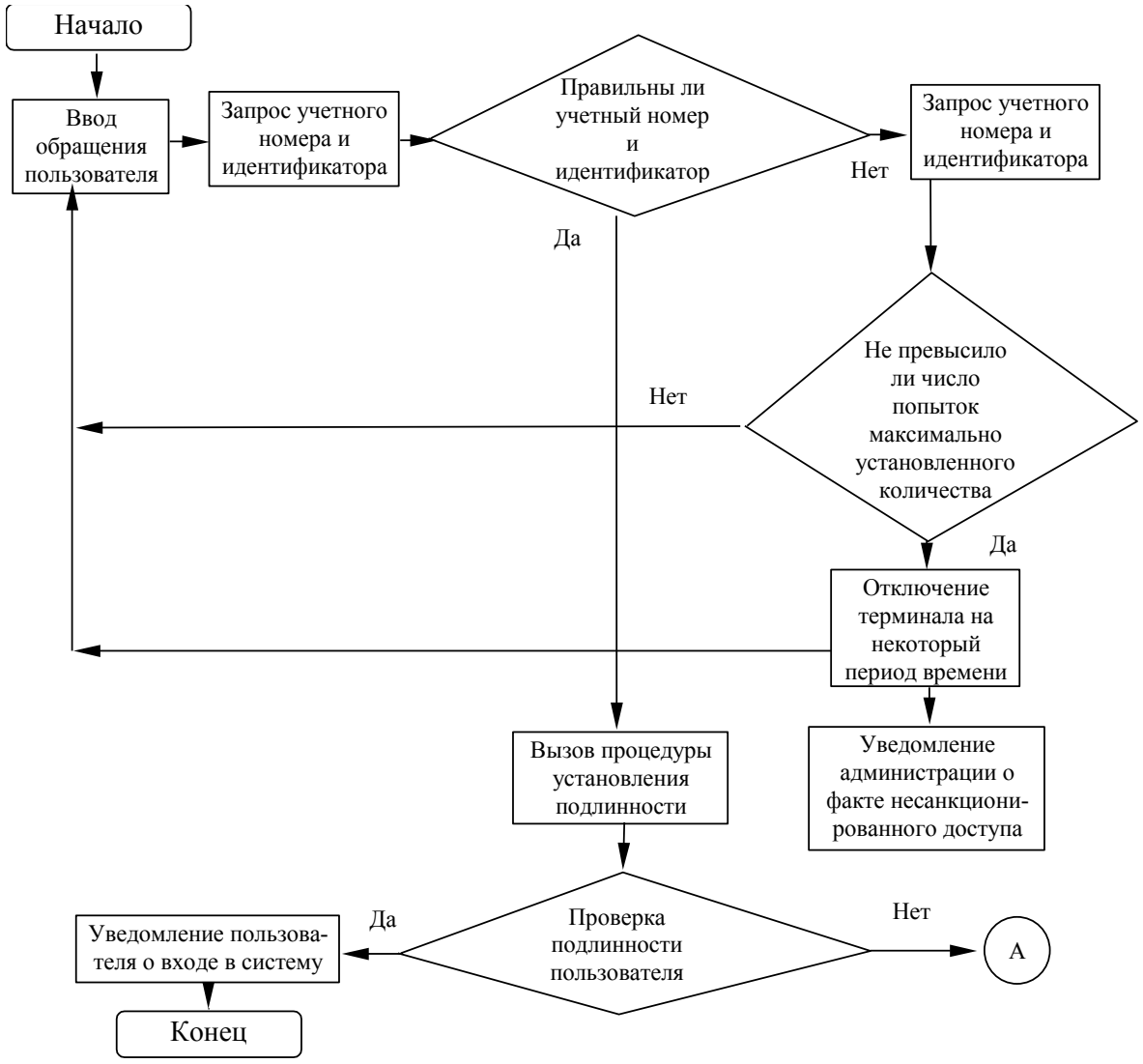


Рис. 4. 1. Процедура идентификации и установления подлинности пользователя

Идентификация и установление подлинности документов. В компьютерных системах документами являются распечатки, листинги, перфоленты, перфокарты, магнитные носители и т.д. Для этого случая используется два подхода:

* получение документа, сформированного непосредственно в КС и на ее документирования;
* получение ее с удаленных объектов КС.

В первом случае подлинность гарантируется системой, имеющие средства защиты от НСД, а также физическими характеристиками печатающего устройства, присущие только этой системы. При недостаточности необходимо использовать крипто-

графическое преобразование. Это особенно актуально для второго случая, когда документ доставляется через неохраняемую территорию с территории удаленного объекта. При этом к носителю прилагаются документы с подписями ответственных лиц, заверенными печатями.

При неавтоматизированном обмене информацией подлинность документов удостоверяется личной подписью человека, автора документа. Проверка осуществляется визуально по личным документам.

При автоматизированной передаче документов по каналам связи, расположенным на неконтролируемой территории, меняются условия обмена. Так как в этом случае подделка подписи документов является относительно простой, то используется так называемая электронная подпись. Этим пользуются организации занимающими банковскими и другими жизненно важной деятельностью. При этом участники нуждаются в защите от преднамеренных НСД в виде:

* отказа отправителя от переданного сообщения;
* изменения получателем полученного сообщения;
* маскировки отправителя под другого сообщения;

Обеспечение защиты каждой стороны, участвующей в обмене информации, осуществляется с помощью ведения специальных протоколов. Для верификации используют следующие положения:

* отправитель вносит в передаваемую информацию свою электронную подпись, представляющую собой дополнительную информацию, зависящую от передаваемых данных, имени получателя и некоторой закрытой информации, который обладает только отправитель;
* получатель должен иметь возможность удостовериться в том, что в составе сообщения подпись есть подлинная подпись отправителя;
* получение правильной подписи отправителя возможно только при использовании закрытой информации, которой обладает только отправитель;
* для исключения возможности повторного использования устаревшего сообщения верификация должна зависеть от времени.

Подпись сообщения представляет собой способ шифрования сообщения с помощью криптографического преобразования. Закрываемым элементом в преобразовании является код ключа.

Идентификация и установление подлинности информации на средствах ее отображения и печати. В компьютерных системах с централизованной обработкой данных и относительно низкими требованиями к защите установлении ее подлинности на технических средствах отображения информации гарантируется данной КС. Однако с усложнением системы увеличивается и вероятность возникновения НСД к информации, ее модификации и хищению. Поэтому в более ответственных случаях отдельные сообщения или блоки информации подвергаются специальной защите, которая заключается в создании средств повышения достоверности информации, ее криптографического преобразования. Установление подлинности полученной информации, включая отображение на табло и терминалах, заключается в контроле обеспечения достоверности информации, результатов дешифрования полученной информации до отображения ее на дисплее. Подлинность информации на средствах ее отображения тесно связана с подлинностью документов. Поэтому все положения приведены ранее справедливы и для этого случая. Чем ближе к полю отображения (бумажному носителю) эта процедура приближается, тем достовернее отображаемая информация.

4.3. Инженерно-технические методы защиты информационных процессов

Организации, эксплуатирующие персональные компьютеры или автоматизированные комплексы, базирующиеся на микропроцессорной технике, сталкиваются с проблемами защиты обрабатываемой и хранящейся информации. При создании и эксплуатации систем безопасности необходимо учитывать выполнение ряда условий:

- запрет на доступ к информационным ресурсам без создания необходимых для этого условий;
- простота механизма защиты;
- закрытие всех возможных каналов утечки.

Практически все программно-аппаратные средства защиты

информации (СЗИ) от несанкционированного доступа в той или иной степени предполагают выполнение первых двух условий. Однако при проектировании не всегда учитывается возможность "взлома" системы путем анализа электромагнитных наводок и излучений, проходящих между средством идентификации пользователя и аппаратной частью СЗИ, устанавливаемой в ПЭВМ илы микропроцессорном блоке обработки сигналов. Это создает предпосылки восстановления протоколов обмена между идентификаторами и аппаратной частью СЗИ по радиоканалу. Причем величина зоны излучения, на которой возможен перехват радиосигналов, содержащих информацию о протоколе обмена, может достигать десятка метров. В частности, данный недостаток имеется у средств защиты и систем контроля доступа в помещения, реализованных на основе электронных идентификаторов семейства DS 199x. Естественно, что обнаружить в этом случае устройства съема информации достаточно проблематично. Тем более что, несмотря на указы Президента и федеральные законы в области защиты информации, на российском рынке чаще всего предлагаются различные системы перехвата и анализа побочных электромагнитных излучений и наводок (ПЭМИН).

Инженерно-техническая защита информации - одна из основных составляющих комплекса мер по защите информации и информационных процессов, составляющей государственную и коммерческую тайну. Проблемы защиты информации усугубляются ещё и несовершенством законодательной базы по сохранению государственной и коммерческой тайн.

Инженерно-техническая защита информации включает комплекс организационных и технических мер по обеспечению информационной безопасности, на основе организационных мероприятий, техническими средствами и решает следующие задачи:

1. Предотвращение проникновения злоумышленника к источникам информации с целью её уничтожения, хищения или изменения.

2. Защита носителей информации от уничтожения в результате воздействия стихийных сил и, прежде всего, пожара и воды (пены) при его тушении.

3. Предотвращение утечки информации по различным тех-

ническим каналам.

Способы и средства решения первых двух задач не отличаются от способов и средств защиты любых материальных ценностей, третья задача решается исключительно способами и средствами инженерно-технической защиты информации.

Инженерно-техническая защита информации представляет собой достаточно быстро развивающуюся область науки и техники на стыке теории систем, физики, оптики, акустики, радиоэлектроники, радиотехники, электро- и радиоизмерений и других дисциплин. Круг вопросов, которыми вынуждена заниматься инженерно-техническая защита, широк и обусловлен многообразием источников и носителей информации, способов и средств её добывания, а, следовательно, и защиты. Для обеспечения эффективной инженерно-технической защиты информации необходимо определить:

- что защищать техническими средствами в данной организации, здании, помещении
- каким угрозам подвергается защищаемая информация со стороны злоумышленников и их технических средств какие способы и средства целесообразно применять для обеспечения информационной безопасности с учётом как величины угрозы, так и затрат на её предотвращение
- как организовать и реализовать техническую защиту информации в организации

Без этих знаний защита информации и информационных процессов может проводиться в форме круговой обороны (при неограниченных ресурсах) или "латания дыр" в более реальном варианте ограниченности средств.

При организации защиты информации, как и других видов защиты, необходимо также знать и учитывать психологические факторы, влияющие на принятие решения руководителем или любым другим ответственным лицом. Это обусловлено тем, что меры по защите имеют превентивную направленность без достаточно достоверных данных о потенциальных угрозах не вообще, а применительно к конкретной организации. Кроме того, последствия скрытого хищения информации проявляются спустя неко-

торое время, когда порой бывает достаточно трудно выявить истинную причину ухудшения финансового положения фирмы или появления у конкурента идентичной продукции. Эти факторы не способствуют психологической готовности руководителя на достаточно большие затраты на защиту информации. Тем не менее, мировой опыт организации защиты информации подтверждает, что на информационную безопасность фирмы вынуждены выделять порядка 10-20% от общей прибыли. Поскольку значительную часть расходов на защиту информации составляют затраты на покупку и эксплуатацию средств защиты, то методология инженерно-технической защиты информации должна обеспечивать возможность рационального выбора средств защиты информации. Поэтому основы инженерно-технической защиты информации должны содержать как теоретические знания, так и методические рекомендации, обеспечивающие решение этих задач. Среди методов инженерно-технической защиты следует выделить: пассивные, активные и комбинированные методы.

4.3.1. Пассивные методы инженерно-технической защиты

Пассивные методы защиты информации направлены на:

- ослабление побочных электромагнитных излучений (информационных сигналов) технических средств передачи информации на границе контролируемой зоны;
- ослабление наводок побочных электромагнитных излучений и наводок техническими средствами передачи информации;
- исключение (ослабление) просачивания информационных сигналов в цепи электропитания, выходящие за пределы компьютерных систем.

4.3.2. Активные методы инженерно-технической защиты

Активные методы защиты информации направлены на:

- создание маскирующих пространственных электромагнитных помех с целью уменьшения отношения сигнал/шум на границе контролируемой компьютерной системы;
- создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях телекоммуни-

кационных и силовых цепях с целью уменьшения отношения сигнал/шум на границе контролируемой компьютерной системы.

4.4. Программно-аппаратные методы защиты информационных процессов

Программно-аппаратные методы защиты информации основаны на основе использовании средств, содержащих в своем составе элементы, реализующие функции защиты информации, в которых программные (микропрограммные) и аппаратные части полностью взаимозависимы и неразделимы.

На первоначальном этапе развития методов и средств защиты информации защита осуществлялась на программном уровне, например проверка целостности программной среды другой, специально разработанной программой. Однако специальная программа находилась на одном носителе с проверяемыми объектами, то такие методы не могут дать гарантии правильности проведения процедур. При этом необходимо проводить проверку самой проверяющей программы. Таким образом, необходимо использование аппаратным средств со встроенными процедурами контроля целостности программ и данных, идентификации и аутентификации, регистрации и учета.

Объектом программно-аппаратной защиты являются:

- персональный компьютер;
- информационные ресурсы;
- сетевые (телекоммуникационные) средства:
- информационные технологии.

Для обеспечения заданного уровня защиты информационных процессов и информации необходимо использовать такие методы программно-аппаратной защиты как [7, 8]:

- аутентификации участников информационного взаимодействия;
- защиты технических средств от несанкционированного доступа;
- разграничения доступа к документам, ресурсам персонального компьютера и сети;
- защиты электронных документов;

- защиты данных в каналах связи;
- защиты информационных технологий;
- разграничения доступа к потокам данных.

Участниками информационными взаимодействия являются операторы и удаленные пользователи. Аутентификация/ идентификация операторов выполняется аппаратно до этапа загрузки операционной системы. Базы данных идентификации/ аутентификации должны хранится в энергонезависимой памяти системы защиты информации, организованной так, чтобы доступ к ней средствами персонального компьютера был невозможен, т.е. энергонезависимая память должна быть размещена вне адресного пространства компьютера. Программное обеспечение контроллера должно хранится в памяти специального контроллера, защищенной от несанкционированных модификаций. Целостность программного обеспечения обеспечивается технологией изготовления контроллера системы защиты. Идентификация осуществляется с применением отчуждаемого носителя информации.

Аутентификация/идентификация удаленных пользователей выполняется с использованием аппаратной реализации. Процедура аутентификации может быть выполнена различными способами, включая электронную цифровую подпись. Обязательным является требование «усиленной аутентификации», т.е. периодического повторения процедуры в процессе работы через интервалы времени, достаточно малые для того, чтобы при преодолении защиты нарушитель не мог нанести ощутимого ущерба.

Защита технических средств от несанкционированного доступа обеспечиваются электронными замками и аппаратными модулями доверенной загрузки. Различие способов защиты заключается в реализации контроля целостности. Электронные замки аппаратно выполняют процедуры идентификации/ аутентификации с использованием внешнего программного обеспечения для выполнения процедура проверки контроля целостности. Аппаратные модули доверенной загрузки реализуют как функции электронных замков, так и функции контроля целостности и функции администрирования. В результате обеспечивается не только идентификации/аутентификации пользователя, но и осуществляется доверенная загрузка операционной системы - важ-

нейшая функция для построения изолированной программной среды. Функционально аппаратные модули доверенной загрузки значительно полнее, чем электронными замками. Модули требуют аппаратной (без использования ресурсов операционной системы) реализации сложных функций, таких, как разбор файловых систем (ФС), обеспечение чтения реальных данных и др. При этом, за счет интеграции контрольных функций в аппаратуре, модули доверенной загрузки обеспечивает также более высокую надежность и доверенность результатов.

Контроль целостности технического состава ПЭВМ должен выполняться контроллером СЗИ до загрузки ОС. При этом должны контролироваться все ресурсы, которые (потенциально) могут использоваться совместно, в том числе:

- центральный процессор;
- системный BIOS;
- дополнительный BIOS;
- вектора прерываний;
- CMOS, в том числе гибких дисков, жестких дисков и CD-ROM.

Целостность технического состава ЛВС обеспечивается процедурой усиленной аутентификации сети. Процедура должна выполняться на этапе подключения проверенной ПЭВМ к сети и далее через заранее определенные администратором безопасности интервалы времени.

Усиленная аутентификация должна выполняться с применением рекомендованного варианта аппаратного датчика случайных чисел. Качество работы датчика должно контролироваться системой рекомендованных тестов.

Контроль целостности системных областей и файлов ОС должен выполняться контроллером до загрузки ОС, чем обеспечивается механизм чтения реальных данных. Так как в электронном документообороте могут использоваться различные операционные системы, то встроенное в контроллер программное обеспечение должно обеспечивать разбор наиболее популярных файловых систем.

Целостность данного программного обеспечения должно гарантироваться технологией изготовления контроллеров системой защиты информации.

Защита программного обеспечения от несанкционированных модификаций должна обеспечиваться аппаратными средствами контроллера.

Для контроля целостности должна применяться известная (опубликованная) хэш-функция, эталонное значение которой должно храниться в энергонезависимой памяти контроллера, защищенной аппаратно от доступа из ПЭВМ.

Контроль целостности программного обеспечения и данных может выполняться как аппаратной компонентой, так и программной компонентой системой защиты в том случае, если ее целостность была зафиксирована аппаратно на предыдущем этапе. Для контроля целостности должна применяться известная (опубликованная) хэш-функция, эталонное значение которой должно аутентифицироваться с помощью отчуждаемого технического носителя информации (идентификатора).

Разграничение доступа к документам, ресурсам ПЭВМ и сети. Современные операционные системы (ОС) содержат встроенные средства разграничения доступа. Эти средства используют особенности конкретной файловой системы и основаны на атрибутах, связанных с одним из уровней интерфейса API операционной системы.

Привязка к особенностям файловой системы. В современных операционных системах, как правило, используются не одна, а несколько ФС - как новые, так и устаревшие. При этом обычно на новой ФС встроенное в ОС разграничение доступа работает, а на старой - может и не работать, так как использует существенные отличия новой ФС. Это обстоятельство обычно прямо не оговаривается в сертификате, что может ввести пользователя в заблуждение. Представим, что на компьютере с новой ОС эксплуатируется программное обеспечение, разработанное для предыдущей версии, ориентированное на особенности прежней ФС. Пользователь вправе полагать, что установленные защитные механизмы, сертифицированные и предназначенные именно для используемой ОС, будут выполнять свои функции, тогда как в действительности они будут отключены. В реальной жизни с це-

лью обеспечения совместимости старые ФС и включаются в состав новых ОС.

Привязка к API операционной системы. Как правило, операционные системы меняются сейчас очень быстро - раз в год - полтора. Не исключено, что будут меняться еще чаще. Некоторые такие смены связаны с изменениями, в том числе и API - например, смена Win9x на WinNT. Если при этом атрибуты разграничения доступа отражают состав API - с переходом на современную версию ОС будет необходимо переделывать настройки системы безопасности, проводить переобучение персонала и т.д.

Таким образом, можно сформулировать общее требование - подсистема разграничения доступа должна быть наложенной на операционную систему, и тем самым, быть независимой от файловой системы. Разумеется, состав атрибутов должен быть достаточен для целей описания политики безопасности, причем описание должно осуществляться не в терминах API ОС, а в терминах, в которых привычно работать администраторам безопасности.

Защита электронных документов. Жизненный цикл электронного документа протекает в трех средах существования, вложенных одна в другую:

- электронная - среда цифровых процессов;
- аналоговая - среда объектов, предметов;
- социальная - среда мыслящих субъектов.

Внешняя оболочка - подмножество мыслящих субъектов социальной среды, образует сектор действенности документа, диктующий правила обмена информацией свои членам-субъектам, в том числе, требования к технологии взаимодействия. Если эти правила и требования выполнены, то сообщение признается документом, а содержащаяся в нем информация признается сектором как (юридический) факт - формальным основанием для возникновения, изменения, прекращения конкретных отношений между субъектами общества.

Требования сектора действенности можно разделить на семантические, предъявляемые к отображению смысла информации, и технологические, диктующие оформление документа. Семантические аспекты являются прерогативой социальной среды, и потому здесь не рассматриваются, полагаются выполненными.

При таком условии для признания сообщения документом необходимо, чтобы параметры технологий, использованных при его формировании, преобразовании, передаче и хранении, лежали бы в рамках допустимых отклонений от некоторого эталона, предписываемого сектором для документального электронного взаимодействия. Только в этом случае возникают юридические основания считать, что выполняются требования, например, по обеспечению целостности, конфиденциальности, аутентичности документа.

Традиционный, аналоговый документ (АнД) формируется однократно в виде предмета - лист бумаги с поверхностью, раскрашенной узорами-буквами. Физические параметры предмета устойчивы к внешнему воздействию, их изменение сравнительно просто индицируется, в течение всего жизненного цикла предмет-документ не преобразуется в другой предмет, в любой момент времени АнД сосредоточен в единственной точке пространства, так что возможности несанкционированного доступа ограничены. Выбор возможных традиционных информационных технологий узок, так что требования эталонной технологии очевидны по умолчанию. Иное дело - электронный документ (ЭлД). Легкость и простота модификации ЭлД заложена самой средой его существования: операции копирования и замены являются фундаментальными в машине Тьюринга. ЭлД многократно преобразуется в течение жизненного цикла, физическая индикация искажения ЭлД трудна. Требования соответствия применяемых информационных технологий эталонным технологиям крайне значимы. Поэтому защита электронного обмена информацией включает два класса задач: обеспечение эквивалентности документа в течение его жизненного цикла исходному ЭлД - эталону; обеспечение эквивалентности примененных электронных технологий эталонным, предписываемым сектором действенности.

В электронной среде не имеет смысла интерпретация информации как сведения, смысла, знания, факта. Для компьютера стихи и случайное число - это множество двоичных бит, на котором задан порядок - последовательность нулевых и единичных бит. Любые два множества отображают одну и ту же информацию, если сохраняется заданное отношение упорядоченности - если множества изоморфны [9]. Так как двоичную ограниченную

последовательность всегда можно преобразовать в число, то в электронной среде информация есть число. Число не меняется во времени и пространстве, оно всегда фиксировано, статично. При хранении на диске памяти число отображается "раскраской" поверхности диска магнитными доменами с разной ориентацией. Говорят, что в памяти ЭВМ хранятся данные, которые понимаются как фиксированная форма существования электронной информации: данные - это число.

Назначение любой защиты - обеспечение стабильности (фиксированности!) заданных свойств защищаемого объекта во всех точках жизненного цикла. Защищенность объекта индицируется сопоставлением эталона (объекта в исходной точке пространства и времени) и результата (объекта в момент наблюдения). В нашем случае в точке наблюдения (получения ЭлД) имеется только весьма ограниченная контекстная информация об эталоне (содержании исходного ЭлД), но зато имеется полная информация о результате (наблюдаемом документе). Это означает, что ЭлД должен включать в свой состав атрибуты, удостоверяющие соблюдение технических и технологических требований, а именно - неизменность сообщения на всех этапах изготовления и транспортировки документа. Одним из вариантов атрибутов могут быть защитные коды аутентификации (ЗКА), описанные в [8].

Защита документа при его создании. При создании документа должен аппаратно вырабатываться защитный код аутентификации (ЗКА). При этом до начала выработки ЗКА должна быть обеспечена изолированность программной среды (ИПС). Запись копии электронного документа на внешние носители до выработки ЗКА должна быть исключена. Если ЭлД порождается оператором, то ЗКА должен вырабатываться с привязкой к оператору. Если ЭлД порождается программной компонентой АС, то ЗКА должен вырабатываться с привязкой к данной программной компоненте.

Защита документа при его передаче по внешним (открытым) каналам связи должна выполняться на основе применения сертифицированных криптографических средств, в том числе с использованием электронно-цифровой подписи (ЭЦП) для каждого передаваемого документа. Возможен и другой вариант - с помо-

щью ЭЦП подписывается пачка документов, а каждый отдельный документ заверяется другим аналогом собственноручной подписи (АСП) - например, ЗКА.

Защита документа при его обработке, хранении и исполнении. На этих этапах защита документа осуществляется применением двух ЗКА - входного и выходного для каждого этапа. При этом ЗКА должны вырабатываться аппаратно с привязкой ЗКА к процедуре обработки (этапу информационной технологии). Для поступившего документа (с ЗКА и ЭЦП) вырабатывается $ЗКА_2$ и только затем снимается ЭЦП. Затем на следующем этапе (n) вырабатывается $ЗКА_{n+1}$ и снимается $ЗКА_{n-1}$. Таким образом, в любой момент времени документ защищен двумя ЗКА - $ЗКА_n$ и $ЗКА_{n+1}$. ЗКА должны вырабатываться и проверяться для документа, размещенного в оперативной памяти ЭВМ, в которой создана и поддерживается ИПС. Снятие $ЗКА_{n-1}$ выполняется после установки $ЗКА_{n+1}$.

Защита документа при доступе к нему из внешней среды включает два уже описанных механизма - идентификация/аутентификация удаленных пользователей и разграничение доступа к документам, ресурсам ПЭВМ и сети.

Защита данных в каналах связи. Традиционно для защиты данных в канале связи применяют канальные шифраторы, и альтернативы этому нет. Нужно помнить о двух вещах - о сертификации и о том, что по каналам передаются не только данные, но и управляющие сигналы.

Защита информационных технологий.. Электронные документы в АС не только хранятся, но и обрабатываются. Компьютер - это не только память, но и вычисления. При обработке документа одни данные исчезают, другие возникают, хотя информация остается той же самой. Числа меняются, а информация - нет, так как сохраняется изоморфизм между множествами двоичных сигналов при "старом" и "новом" форматах. В электронной среде принципиально должна существовать некая новая форма существования информации, соответствующая процессу преобразования данных - информация не может исчезнуть между "входом" и "выходом" процесса. Но процесс динамичен, являющейся изменением чего-либо во времени, тогда как информация должна быть постоянной. Чтобы избежать противоречия, необходимо,

чтобы динамичный процесс имел бы некую фиксированную во времени, статичную, характеристику - фиксированность описания процесса во времени, в какой бы точке пространства (компьютере) и момент времени этот процесс ни наблюдался. Действительно, конкретный процесс обработки информации в ЭВМ определяется фиксированным алгоритмом, процедурой, протоколом. Допустив, что в электронной среде существуют две формы отображения информации: статическая - в форме объекта, динамическая - в форме процесса, мы тем самым допустили два кардинально отличных класса элементов электронной среды. Коль скоро первый класс определен как числа, то второй класс логично назвать функциями (преобразованиями, отображениями). На "вход" функции поступают числа-данные, на "выходе" появляются новые числа-данные. В любой момент времени и в любой точке пространства функция остается функцией. Функция (или родственные понятия - отображение, алгоритм, преобразование), - неизменны.

В пассивной форме (хранение) ЭлД есть фиксированный объект в аналоговой среде (устройство памяти), в активизированной форме ЭлД существует как фиксированный процесс в электронной среде. Соответственно, выделим две составляющих защиты: защита данных (чисел) - собственно ЭлД как физического объекта; защита процессов (функций), реализующих активизированную форму существования ЭлД. Информация-данные определяется как множество с заданным на нем отношением порядка. Защита функций, т.е. алгоритмов, означает защиту вычислительной среды, инвариантной к той информации, тем данным, которые в ней обрабатываются. Электронная технология также есть упорядоченное множество (операций, процессов), и потому формально может быть признана как информация - технология. Выявляется внутреннее единство составляющих защиты - это защита информации - данных и защита информации - технологии.

Таким образом, статус документа предполагает не только идентичность (соответствие эталону) собственно документа, но и соответствие эталонным требованиям примененных информационных технологий.

Несмотря на известное сходство, механизмы защиты собственно ЭлД как объекта (число, данные) и защита ЭлД как процес-

са (функция, вычислительная среда) радикально отличаются. При защите информации - технологии, в отличие от защиты ЭлД, достоверно известны характеристики требуемой технологии - эталона, но имеются ограниченные сведения о выполнении этих требований фактически использованной технологией - о результате. Единственным объектом, который может нести информацию о фактической технологии (как последовательности операций), является собственно ЭлД, а точнее - входящие в него атрибуты. Как и ранее, одним из видов этих атрибутов могут быть ЗКА. Эквивалентность технологий может быть установлена тем точнее, чем большее количество функциональных операций привязывается к сообщению через ЗКА. Механизмы при этом не отличаются от применяемых при защите ЭлД. Более того - можно считать, что наличие конкретного ЗКА характеризует наличие в технологическом процессе соответствующей операции, а значение ЗКА - характеризует целостность сообщения на данном этапе технологического процесса.

Разграничение доступа к потокам данных. Для целей разграничения доступа к потокам данных используются, как правило, маршрутизаторы с функцией "*VPN* - построителя". Надежно эта функция может быть реализована только с помощью криптографических средств. Как всегда в таких случаях - особое внимание должно уделяться ключевой системе и надежности хранения ключей. Естественно, что требования к политике доступа при разграничении потоков совершенно отличаются от таковых при разграничении доступа к файлам и каталогам. Здесь возможен только простейший механизм - доступ разрешен или запрещен.

Выполнение перечисленных требований обеспечивает достаточный уровень защищенности электронных документов как важнейшего вида сообщений, обрабатываемых в информационных системах.

5. АНАЛИЗ И ОЦЕНКА ПРОЧНОСТИ ЗАЩИТЫ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

5.1. Основы теории защиты информационных процессов от несанкционированного доступа

5.1.1. Модель поведения потенциального нарушителя

Нарушением считается попытка несанкционированного доступа к подлежащей защите информационных процессов. Поскольку невозможно предсказать время и место НСД, то, безусловно, целесообразно создать модель поведения потенциального нарушителя, предполагая наиболее опасную ситуацию:

1) нарушитель может появиться в любое время в месте периметра охраняемой зоне;

2) квалификация и осведомленность нарушителя может быть на уровне разработчика данной КС;

3) постоянно хранимая информация и принципах работы системы (включая секретную информацию) нарушителю известна;

4) для достижения своей цели нарушитель выберет наиболее слабое звено в защите;

5) нарушителем может быть не только постороннее лицо, но и законный пользователь;

6) нарушитель действует один.

На основе анализа перечня опасных ситуаций для выбора модели поведения потенциального нарушителя целесообразно дифференцированного подхода. Поскольку квалификация нарушителя понятие относительное за основу принимается четыре класса безопасности:

1- й класс рекомендуется для защиты жизненно важной информации, утечки, разрушение или модификация которой может привести к большим последствиям. Прочность защиты должна быть рассчитана на нарушителя-профессионала;

2-й класс рекомендуется использовать для защиты важной информации при работе нескольких пользователей, имеющих

доступ к разным массивам данных или формирующих свои файлы, недоступные другим пользователям. Прочность защиты должна быть рассчитана на нарушителя высокой квалификации, но не взломщика-профессионала;

3-й класс рекомендуется использовать для защиты относительно важной информации, постоянный несанкционированный доступ к которой путем ее накопления может привести к утечки более важной информации. Прочность защиты при этом должна рассчитана на относительно квалифицированного нарушителя-профессионала;

4-й класс рекомендуется для защиты прочей информации, не представляющей интереса для серьезных нарушителей. Однако его необходимость диктуется соблюдением технологической дисциплины учета и обработки информации служебного пользования в целях защиты от случайных нарушений в результате безответственных пользователей и некоторой подстраховки от случаев преднамеренного НСД.

Реализация перечисленных уровней безопасности должна обеспечиваться необходимым набором средств защиты в соответствии с ожидаемым классом потенциального нарушителя. Уровень безопасности защиты внутри класса обеспечивается количественной оценкой прочности отдельных средств защиты и оценкой прочности контура защиты от преднамеренного НСД по расчетным формулам.

5.1.2. Модель защиты информационного процесса

Модель элементарной защиты. Модель элементарной защиты информационных процессов представлена на (Рис. 5. 1). Предмет защиты помещен в замкнутую защитную оболочку, называемой преградой. Прочность защиты зависит от свойств преграды. Способность противостоять вторжению со стороны нарушителя характеризуется прочностью преграды. Таким образом производится оценка защищенности информации и их процессов КС. При этом считается, прочность созданной преграды достаточна, если стоимость ожидаемых затрат на ее преодоление потенциальным нарушителем превышает стоимость защищаемой

информации. Однако возможен и другой подход в оценки прочности защиты.

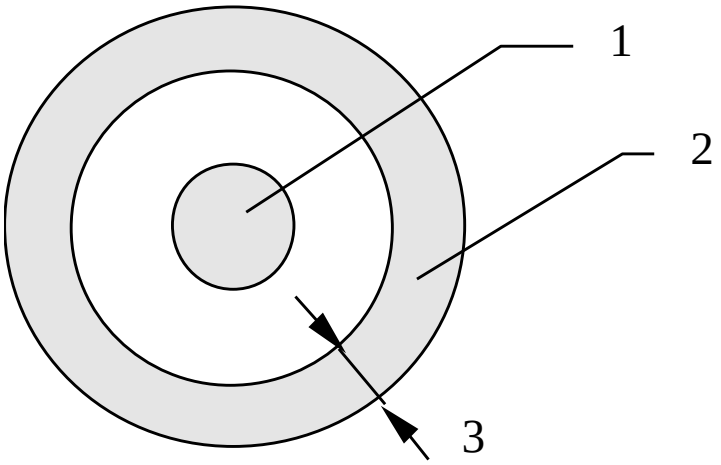


Рис. 5. 1. Модель элементарной защиты
(1 – предмет защиты; 2 - преграда; 3 – прочность преграды)

Известно, что информация со временем теряет свою привлекательность, стареет, 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. Если вероятность непреодоления преграды нарушителем через $P_{\text{сзи}}$, время жизни информации через $t_{\text{ж}}$, ожидаемое время преодоления преграды нарушителем через $t_{\text{н}}$, вероятность обхода преграды нарушителем через $P_{\text{обх}}$, то для случая старения информации условие достаточности получается в виде:

$P_{\text{сзи}} = 1$, если $t_{\text{ж}} < t_{\text{н}}$ и $P_{\text{обх}} = 0$.

$P_{\text{обх}}$ равное нулю, отражает необходимость замыкания преграды вокруг предмета защиты. Если $t_{\text{ж}} > t_{\text{н}}$, а $P_{\text{обх}} = 0$, то

$$P_{\text{сзи}} = (1- P_{\text{нр}}), \qquad (5.1)$$

где $P_{\text{нр}}$ – вероятность преодоления преграды нарушителем за время меньшее $t_{\text{ж}}$.

Для реального случая, когда $t_{\text{ж}} > t_{\text{н}}$ и $P_{\text{обх}} > 0$, прочность защиты представляется в виде:

$P_{\text{сзи}} = (1- P_{\text{нр}})\ (1- P_{\text{обх}})$,

$P_{\text{нр}} = 0$, если $t_{\text{ж}} < t_{\text{н}}$; $P_{\text{нр}} > 0$, если $t_{\text{ж}} \geq t_{\text{н}}$.

Последнее выражение справедливо при наличии двух нарушителей, т.е. когда один преодолевает преграду, другой в это время ее обходит. При условии если в наличии имеется один нарушитель, то нарушитель выберет наиболее простой т.е.:

$$P_{\text{сзи}} = (1- P_{\text{нр}}) \cup (1- P_{\text{обх}}), \qquad (5.2)$$

где знак $\cup$ означает логическое действие "*ИЛИ*"

Следовательно, прочность преграды после определения и сравнения будет равна меньшему значению из них (5.2).

В качестве примера элементарной защиты, рассчитываемой по формуле (5.2), может названа криптографическая защиты информации, где величина $P_{\text{нр}}$ может быть определена путем оценки вероятности подбора кода ключа, с помощью которого можно дешифровать закрытую информацию и определится по формуле:

$$P_{\text{íð}} = \frac{n}{A^S}, \qquad (5.3)$$

где n - количество попыток подбора кода;

A - число символов в выбранном алфавите кода ключа;

S - длина кода ключа в количестве символов.

Величина $P_{\text{обх}}$ – зависит от выбранного метода шифрования, способа применения, полноты перекрытия текста информации, существующих методов криптоанализа, а также способа хранения действительного значения кода ключа и периодичности его замены на новое значение, если информация, закрытая данным способом, постоянно хранится у владельца. Возможны также и другие обстоятельства, влияющие на вероятность обхода криптографической защиты.

Выбор и определение конкретной величины $P_{\text{обх}}$ сначала проводится экспертным путем на основе опыта специалиста. Величина $P_{\text{обх}} = 1$ защиты теряет всякий смысл

Возможна также и другая ситуация при которой у одной преграды есть несколько путей обхода. Тогда выражение (5.2) примет вид:

$$P_{\text{сзи}} = (1- P_{\text{нр}}) \cup (1- P_{\text{обх1}}) \cup (1- P_{\text{обх2}}) \cup \ldots \cup (1- P_{\text{обхk}}), \qquad (5.4)$$

где k - число путей обхода преграды, т.е. прочность преграды равна наименьшему значению, полученному после определения и сравнения величин

$$(1 - P_{\text{нр}}),\ (1- P_{\text{обх1}}),\ (1- P_{\text{обх2}}), \ldots , (1- P_{\text{обхk}}).$$

В случае если информация, подлежащая защите, не устаревает или периодически обновляется, т.е. $t_{\text{ж}} > t_{\text{н}}$ постоянно или когда $t_{\text{н}} > t_{\text{ж}}$ невозможно обеспечить, то применяется постоянно действующая преграда, обладающая свойствами обнаружения и блокировки доступа нарушителя к предмету или объекту защиты. В качестве защиты используется человек или автоматизированная система под контролем человека. Безусловно, параметры этой преграды будут влиять на ее прочность.

Способность преграды обнаруживать и блокировать НСД должна учитываться при оценке ее прочности путем введения в расчетную формулу (5.4) вместо $(1- P_{\text{нр}})$, где $P_{\text{обл}}$ - вероятность обнаружения и блокировки несанкционированного доступа.

Принцип работы автоматизированной преграды основан на том, что производится периодический контроль датчиков обнаружения нарушителя. Периодичность контроля может достигать сотые доли секунды и менее. В этом случае ожидаемое время преодоления преграды нарушителем превышает время опроса датчиков обнаружения. Поэтому такой контроль считается постоянным. Но для обнаружения нарушителя человеком (оператором) этого недостаточно. Необходимо время для срабатывания тревожной сигнализации, так это время значительно превышает время опроса датчиков и тем самым увеличивается время обнаружения нарушителя. Практика показывает, что сигнал тревоги, как правило, приостанавливает действия нарушителя, если этот сигнал дошел до него. Но поскольку физический доступ к объек-

ту еще открыт, то охрана должна локализовать нарушителя и организовать его блокировку.

Таким образом, условие прочности преграды с обнаружением и блокировкой НСД можно представить в виде соотношения:

$$\frac{T_{Д} + t_{СР} + t_{ом} + t_{бл}}{t_{Н}} < 1, \qquad (5.5)$$

где $T_д$ - период опроса датчиков;

$t_{ср}$ - время срабатывания тревожной сигнализации;

$t_{ом}$ - время определения места доступа;

$t_{бл}$ - время блокировки доступа.

Если ($T_д$ + $t_{ср}$ + $t_{ом}$ + $t_{бл}$) через $T_{обл}$, получим соотношение

$$\frac{T_{обл}}{t_{Н}} < 1, \qquad (5.6)$$

где $T_{обл}$ - время обнаружения и блокировки несанкционированного доступа.

Процесс контроля НСД и несанкционированных действий нарушителя представлен на рисунке (Рис. 5. 2).

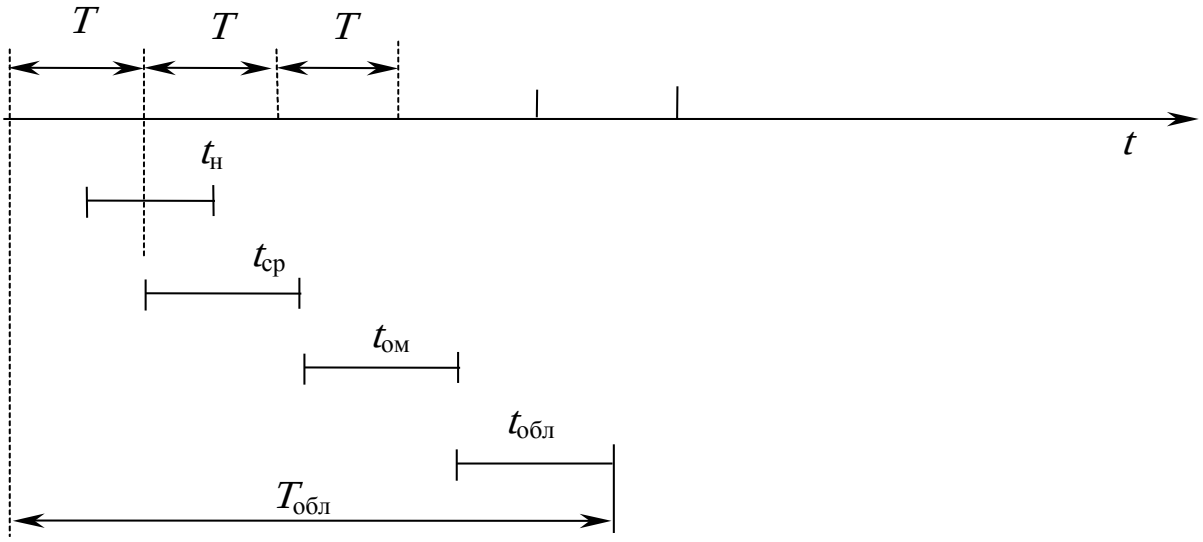


Рис. 5. 2. Временная диаграмма контроля НСД

Из диаграммы видно, что нарушитель может быть не обнаружен в двух случаях:

а) когда $t_н < T$;

б) когда $T < t_н < T_{обл}$;

В первом случае требуется дополнительное условие - попадание интервала времени $t_н$ в интервал T, т.е. необходима система синхронизация действий нарушителя с частотой опроса датчиков обнаружения. Для решения этой проблемы нарушителю придется скрытно подключить измерительную аппаратуру в момент выполнения НСД, что является достаточно сложной задачей для постороннего человека. Поэтому считаем, что свои действия с частотой опроса датчиков он синхронизовать он не может и приходится надеяться на некоторую вероятность попадания отрезка времени $t_н$ в промежуток между импульсами опроса датчиков, равны T.

Согласно определению геометрической вероятности (курс теории вероятности) получим выражение для определения вероятности успеха нарушителя в следующем виде.

$$P_{îá} = \frac{T - t_í}{T} = 1 - \frac{t_í}{T}. \qquad (5.7)$$

Вероятность обнаружения НСД нарушителя определяется выражением:

$$P_{íá} = 1 - P_{îá} \qquad (5.8)$$

или $$P_{íá} = \frac{t_í}{T}, \qquad (5.9)$$

если $t_н > T$ нарушитель будет обнаружен наверняка, т.е. $T_{об} = 1$. Во втором случае, когда $T < t_н < T_{обл}$, вероятность успеха нарушителя будет определяться по аналогии с предыдущим соотношением:

$$P_{îá} = 1 - \frac{t_í}{T_{íá.ë}}. \qquad (5.10)$$

Вероятность обнаружения и блокировки НСД:

$$P_{\text{об.л}} = 1 - P_{\text{пр}} \qquad (5.11)$$

$$P_{\text{об.л}} = \frac{t_{\text{н}}}{T_{\text{об.л}}}. \qquad (5.12)$$

При $t_{\text{н.}} > T_{\text{обл}}$ попытка НСД не имеет смысла, так как она будет обнаружена.

Таким образом, прочность преграды со свойствами обнаружения и блокировки можно производить по формуле:

$$P_{\text{сзи}} = P_{\text{обл}} \cup (1- P_{\text{обх1}}) \cup (1- P_{\text{обх2}}) \cup ... \cup (1- P_{\text{обхj}}), \qquad (5.13)$$

где j - число путей обхода этой преграды;

$\cup$ - знак “ИЛИ”.

Следует отметить, что эта формула справедлива также и для организационной меры защиты.

Для более полного 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 ее по формуле:

$$P_{\text{отк}}(t) = 1 - e^{-\lambda t}, \qquad (5.14)$$

где λ - интенсивность отказов группы технических средств, составляющих систему обнаружения и блокировки НСД;

t - рассматриваемый интервал времени функционирования системы обнаружения и блокировки НСД.

С учетом возможного отказа системы контроля прочность преграды будет:

$$P_{\text{сзиК}} = P_{\text{обл}} (1- P_{\text{отк1}}) \cup (1- P_{\text{обх1}}) \cup (1- P_{\text{обх2}}) \cup ... \cup (1- P_{\text{обхj}}), \qquad (5.15)$$

где $P_{\text{об.л}}$ и $P_{\text{отк}}$ определяется по формулам (5.12) и (5.14);

$P_{обх}$ – количество путей обхода *j* определяется экспертным путем на основе анализа принципов построения системы контроля и блокировки НСД.

Одним из возможных способов обхода системы обнаружения и блокировки – возможное ее отключение или замыкание (обрыва) контрольных цепей. Таким образом следует, что защитные преграды могут быть двух типов контролируемые и неконтролируемые человеком. Неконтролируемые определяется по формуле (5.4), а контролируемые (5.15).

Значения $P_{обх1}$, $P_{обх2}$,…, $P_{обхj}$ определяются в пределах от 0 до 1 экспертным путем на основе опыта специалистов. При экспертной оценке вероятности наступления того или иного события ($P_{нр}$, $P_{обх}$ и т. д.) в целях унификации метода за основу приняты следующие градации значений [3]:

$P = 0$ — 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;

$P = 1$ — событие произойдет наверняка.

Модель многозвенной защиты. На практике в большинстве случаев защитный контур состоит несколько “соединенных” между собой преград с различной прочностью. Модель такой защиты представлена на рис 5.3.

Примером такого вида защиты может служить помещение, в котором хранится оборудование. В качестве преград с различной прочностью здесь могут служить стены, пол, окна и замок на двери.

Для вычислительной системы соединение преград имеет несколько иную реализацию. Здесь следует отнести систему контроля доступа к аппаратуре, систему защиты от вскрытия, систему опознавания, систему, контролирующую доступ к периметру компьютерной системы. Однако такая система не является замкнутой. Система не защищена от доступа к средствам отображения информации, документирования, от побочного излучения и другим каналам. Таким образом, в состав защиты информацион-

ных процессов войдут еще система контроля доступа в помещение, система шифрования и т.п. Таким образом, система защиты не будет замкнутой и будет оставаться не защищенной пока есть возможность каналов утечки.

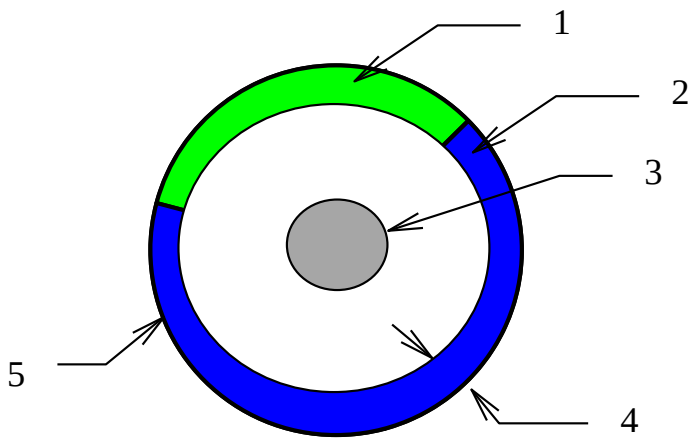


Рис. 5. 3. Модель многозвенной защиты (1-преграда 1; 2- преграда 2; 3 предмет защиты; 4-прочность преграды; 5-преграда 3)

Формальное описание для прочности многозвенной защиты практически совпадает с выражениями (5.2) и (5.15), так как наличие нескольких обходных путей одной преграды, не удовлетворяющей для неконтролируемой преграды.

$$P_{\text{сзи}} = P_{\text{сзи1}} \cup P_{\text{сзи2}}\ P_{\text{сзи3}} \cup ... \cup P_{\text{сзи}i} \cup (1- P_{\text{обх1}}) \cup (1- P_{\text{обх2}}) \cup ... \cup (1- P_{\text{обх}k}), \quad (5.16)$$

где $P_{\text{сзи}i}$ - прочность i-той преграды.

Выражение для прочности многозвенной защиты с контролируемыми преградами будет иметь вид:

$$P_{\text{сзик}} = P_{\text{сзик1}} \cup P_{\text{сзик2}}\ P_{\text{сзик3}} \cup ... \cup P_{\text{сзикn}} \cup (1- P_{\text{обх1}}) \cup (1- P_{\text{обх2}}) \cup ... \cup (1- P_{\text{обхj}}), \quad (5.17)$$

где $P_{\text{сзикn}}$ - прочность n-ой преграды.

Здесь следует, что оценка прочности защиты информации для неконтролируемой и контролируемой преграды могут быть раздельными, так как исходные данные для них различны.

Если прочность слабейшего звена удовлетворяет предъявленным требованиям контура защиты в целом, возникает вопрос об избыточности прочности на всех остальных звеньях данного контура. Поэтому при проектировании экономически целесообразно использовать равнопрочные звенья.

При расчете прочности контура защиты возникает ситуация, когда звено с наименьшей прочностью не удовлетворяет предъявленным требованиям. В этом случае звено заменяют на более прочное или его дублируют. Иногда дублируется слабое звено двумя и более преград. Дополнительные преграды должны перекрывать то же количество или более возможных каналов НСД, что и первая. Тогда суммарная прочность дублированных преград будет:

$$P_{\Sigma} = 1 - \prod_{i=1}^{m} (1 - P_i), \qquad (5.18)$$

где $i = \overline{1, m}$ - порядковый номер преграды;

m - количество дублирующих преград;

P_i - прочность i-й преграды.

Участок защитного контура с параллельными (дублированными) преградами иногда называют *многоуровневой* защитой. В компьютерной системе защитные преграды часто перекрывают друг друга (например, системы контроля доступа в помещение, охранной сигнализации и контрольно-пропускного пункта на территорию объекта защиты).

Многоуровневая защита. В ответственных случаях при повышенных требованиях к защите применяется многоуровневая защита, модель которой представлена на рис 5.4. Данная модель позволяет систематизировать работу по созданию комплексной системы защиты информации и информационных процессов [6].

В качестве объекта защиты в такой модели являются: информационные ресурсы, информационные процессы и информация.

Число уровней защиты компьютерной системы или сети должно быть не менее четырех.

- Внешний уровень, охватывающий территорию, где расположено оборудование системы или сети.
- Уровень сооружений, помещений или устройств.
- Уровень компонентов системы (технических средств, программного обеспечения, элементов баз данных).
- Уровень технологических процессов обработки данных (ввод-вывод, внутренняя обработка т.д.).

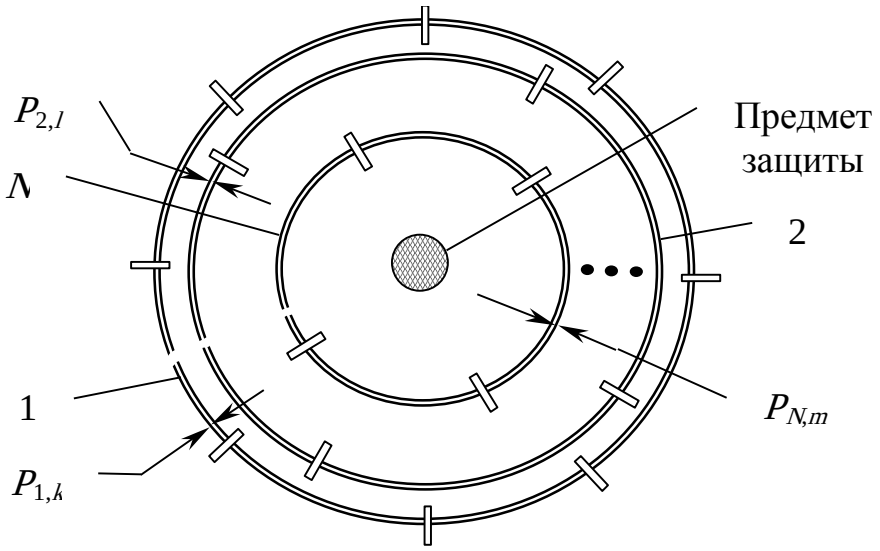


Рис. 5. 4. Модель многоуровневой защиты информации

1, 2,…, N – уровни защиты; $P_{1,k}$ – прочность 1-го уровня k-го звена; $P_{2,l}$ – прочность 2-го уровня l-го звена; $P_{N,\mathrm{m}}$ – прочность N-го уровня m-го звена.

При практической реализации системного подхода принимают три положения: 1) система защиты и внедрение системы защиты проводится одновременно с разработкой компьютерной системы; 2) реализация функции защиты - преимущественно аппаратная; 3) строгое доказательство обеспечения задаваемого уровня защиты.

Прочность многоуровневой системы защиты определяется выражением

$$P_{\Sigma} = 1 - \prod_{n=1}^{N} (1 - P_n), \qquad (5.19)$$

где P_{Σ} - суммарная прочность системы защиты;

P_n - прочность *n*-го уровня;

N – число уровней системы защиты.

При $P_N = 0$ данный уровень в расчет не принимается. При $P_N = 1$ остальные уровни являются избыточными. Данная модель справедлива для контуров защиты, перекрывающие одни и те же каналы ВКНСД к одному и тому же предмету.

Прочность защиты преграды является достаточной, если затраты на создание систем защиты адекватны ценности объекта защиты и ожидаемое время преодоление ее нарушителем больше времени жизни предмета защиты или больше времени обнаружения и блокировки его доступа при отсутствии путей скрытого обхода этой преграды.

При расчете суммарной прочности нескольких контуров защиты в формулу (5.18) вместо P_{i} включают $P_{\text{кi}}$ - прочность каждого контура, значение которой определяется по одной из формул (5.16) и (5.17), т.е. для контролируемых и неконтролируемых преград опять расчеты должны быть раздельными и производиться для разных контуров, образующих каждый отдельную многоуровневую защиту. При $P_{\text{кi}} = 0$ данный контур в расчет не принимается. При $P_{\text{кi}} = 1$ остальные контуры являются избыточными. Данная модель справедлива лишь для контуров защиты, перекрывающие одни и те же каналы НСД к одному и тому же предмету защиты.

5.2. Концептуальные основы построения защиты информационных процессов от несанкционированного доступа в компьютерных системах

С позиций входа в систему и выхода из нее, отметим штатные средства готовых к работе:

* терминалы пользователей;
* средства отображения и документирования;
* средства загрузки программного обеспечения в систему;
* носители информации, ОЗУ, ДЗУ, распечатки и т.д.;
* внешние каналы связи.

Все перечисленные каналы называются штатными каналами, по которым ведет санкционированный доступ законным пользователям. В данном случае точки приложения *случайных* воздействий распределены по всей «площади» компьютерной системы. Опасность возникновения *случайных* воздействий заключается в случайном искажении информации, приводящий к утере, модификации и утечки информации. Для обнаружения и блокирования случайных воздействий применяются встроенные в систему средства функционального контроля, качественными показателями которого являются:

* время обнаружения и локализации отказа;
* достоверность контроля функционирования;
* полнота контроля (охват компьютерной системы);
* время задержки и обнаружения отказа.

Точки приложения *преднамеренных* воздействий связаны прежде всего со входами в систему и выходами информации из нее, т.е. “периметром” системы. Эти входы и выходы могут быть законными и незаконными т.е.:

* все перечисленные штатные средства при незаконном использовании;
* технологические пульты и органы управления;
* внутренний монтаж аппаратуры;
* линии связи между аппаратными средствами КС;
* побочные электромагнитное излучение;
* побочные наводки на сетях электропитания и заземления аппаратуры, вспомогательных и посторонних коммуникациях, размещенных вблизи КС;
* внешние каналы связи.

Опасность преднамеренных НСД заключается во вводе нарушителем незаконных команд, запросов, сообщений, программ и т.д., приводящих к утрате, модификации и НС ознакомлению, а также перехвате нарушителем секретной информации путем приема и наблюдения сигналов побочного электромагнитного излучения и наводок.

Анализ КС позволяет рассматривать ее как объект, в котором имеется некоторое множество возможных каналов несанкционированного доступа (ВКНСД) к предмету защиты.

Для построения системы защиты в данной системе на каждом ВКНСД, а если возможно сразу на нескольких необходимо установить соответствующую преграду. Чем большее количество возможных каналов доступа перекрыто средствами защиты и выше их вероятность непреодолимость потенциальным нарушителем, тем выше безопасности информационных процессов в КС. Количество перекрываемых ВКНСД при этом будет зависеть от заданной квалификации нарушителя. На практике используются следующее распределение по классам.

1-й класс - все ВКНСД, возможные в данной КС на текущий момент времени.

2-й класс - все ВКНСД, кроме машинных носителей с остатками информации, подлежащие специальной криптографическими методами.

3-й класс - только следующие ВКНСД:

- ♦ терминалы пользователей;
- ♦ аппаратура регистрации и бумажные носители информации;
- ♦ средства загрузки программного обеспечения;
- ♦ технологические пульты и органы управления;
- ♦ внутренний монтаж аппаратуры;
- ♦ линии связи между аппаратными средствами.

4-й класс - только следующие ВКНСД:

- ♦ терминалы пользователей;
- ♦ машинные и бумажные документы;
- ♦ средства загрузки программного обеспечения.

Анализ возможных каналов НСД показывает, что данные каналы делятся на: контролируемые и неконтролируемые перечень которых упоминался ранее.

Для обеспечения замыкания контура защиты из нескольких различных по исполнению преград, недостаточно только перекрытия всех возможных каналов НСД. Необходимо еще обеспечить их взаимодействие между собой, т.е. объединить их в еди-

ный постоянно действующий механизм. Эту задачу должны выполнять централизованные средства управления.

На контролируемом ВКНСД все цепи и тракты контроля аппаратно, программно и организационно должны сходиться на одном рабочем месте службы безопасности. Для успешного проектирования и разработки системы безопасности необходимо придерживаться следующего порядка:

1) анализ заданных требований к КС на предмет определения перечня, структуры и динамики стоимости обрабатываемых данных, подлежащих защите;

2) выбор модели потенциального нарушителя;

3) выявление в данной КС максимально возможного количества каналов НСД согласно выбранной модели потенциального нарушителя;

4) анализ выявленных ВКНСД и выбор готовых или разработка новых средств защиты, способных их перекрытие с заданной прочностью;

5) качественная и количественная оценка прочности каждого из применяемых средств защиты;

6) проверка возможности адаптации средств защиты в разрабатываемой КС;

7) создание в разрабатываемой КС средств централизованного контроля и управления;

8) количественная и качественная оценка прочности системы защиты информации в НСД с отдельными показателями по контролируемым и неконтролируемым ВКНСД.

При создании защиты необходимо учитывать следующие свойства предмета защиты:

♦ информация - объект права собственности, подлежащей защите от НСД;

♦ время жизни информации;

♦ разные источники, место и время приложения случайных и преднамеренных НСД;

♦ наличие достаточно простой модели потенциального нарушителя;

♦ степень охвата КС фундаментальным контролем и средствами повышения достоверности информации, определяющая вероятность появления случайных НСД;

♦ возможные каналы НСД к информации;

♦ степень замыкания преграды вокруг предмета защиты, определяющая вероятность ее обхода нарушителем;

♦ деление возможных каналов НСД на контролируемые и неконтролируемые;

♦ зависимость прочности преграды, не обладающей способностью контроля НСД, от способности преграды в своевременному обнаружению и блокировке попыток НСД;

♦ зависимость уровня прочности защиты информации в КС в целом от уровня прочности слабейшего звена;

♦ возможность создания системы защиты информации в виде единого целого и реально действующего механизма.

Основная тактика и стратегия защиты информации от НСД заключается в выполнении следующих задач:

♦ предупреждении и контроле попыток НСД;

♦ своевременном обнаружении, определении места и блокировки несанкционированных действий;

♦ регистрации документирования события;

♦ установлении и устранении причин НСД;

♦ ведении статистики и прогнозировании НСД.

Предупреждение и контроль заключается в:

♦ применение средств функциональной контроля технических средств КС и средств повышения достоверности информации;

♦ для защиты от преднамеренных НСД создание в КС замкнутого контура защиты, состоящего из системы преград, перекрывающих максимально возможное количество каналов НСД и обладающих такой прочность, затраты времени на преодолении которой больше времени жизни защищаемой информации или больше времени обнаружения и блокировки НСД в ней.

Компьютерная система обеспечивает безопасность информационных процессов, если в ней предусмотрена централизован-

ная система управляемых и взаимосвязанных преград, перекрывающих с гарантированной прочностью в соответствии с моделью потенциального нарушителя количество возможных каналов НСД и воздействий, направленных на утрату или модификацию информации, а также несанкционированное ознакомление с нею посторонних лиц.

5.3. Оценка эффективности автоматических средств управления защитой информационных процессов в компьютерных системах

Средства управления защитой информации выполняют эту функцию, являясь важной составной частью средств защиты. Управление обеспечивает функции контроля, обнаружения и блокировки НСД, а также бесперебойное функционирование аппаратных, программных и организационных средств защиты, ведение статистики и прогнозирование событий. Все эти параметры учитываются при оценке прочности отдельных средств защиты. В результате оценка эффективности средств управления защитой может проводиться лишь с качественной стороны на предмет реализации защиты как единого механизма. Механизм реализации защиты включает в себя: системы защиты информации в техническом смысле, технологию управления, состав аппаратных и программных средств управления, организационных мероприятий, наличие централизации контроля и управления защитой.

Оценка степени централизации контроля и управления защитой предполагает оценку степени охвата отдельных средств защиты средствами контроля и управления. Этот параметр определяет вероятность обхода защитных преград нарушителем, устанавливаемую экспертным путем. В ответственных системах все преграды должны находиться под централизованным контролем. Оценка эффективности средств управления защитой информации должна даваться отдельным показателем. При этом важную роль играет степень автоматизации контроля функционирования той или иной защитной преграды. Данный показатель можно определить по отношению количества преград с автоматической подачей сигнала НСД на централизованное средство контроля к общему количеству преград, используемых в системе защиты ин-

формации в КС. Это отношение можно выразить формулой определяющейся коэффициентом автоматизации

$$K_A = \frac{N_A}{N}, \qquad (5.20)$$

где K_A – коэффициент автоматизации;

N_A – количество средств защиты с автоматической подачей сигнала и блокировкой НСД;

N – общее количество средств защиты информации в КС.

Такая оценка необходима для определения степени приближения полученных значений прочности защиты к действительным. Чем больше автоматизированных средств защиты, тем меньше экспертных оценок и достоверней результаты оценок и выше гарантии эффективности защиты.

6. СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

6.1. Распределение средств защиты информации и информационных процессов компьютерных систем

6.1.1. Распределение средств защиты информации и информационных процессов в компьютерных сетях

Точки приложения преднамеренных воздействий связаны прежде всего со входами в систему и выходами информации из нее, т.е. «периметром» системы. Эти входы и выходы могут быть законными и незаконными т.е.:

* все перечисленные штатные средства при незаконном использовании;
* технологические пульты и органы управления;
* внутренний монтаж аппаратуры;
* линии связи между аппаратными средствами КС;
* побочные электромагнитное излучение;
* побочные наводки на сетях электропитания и заземления аппаратуры, вспомогательных и посторонних коммуникациях, размещенных вблизи КС;
* внешние каналы связи.

Анализ компьютерных систем как объекта защиты, возможных каналов несанкционированного доступа (ВКНСД) к информации ограниченного пользования и потенциальных угроз позволяет выбрать и построить соответствующую систему защиты.

Возможные каналы несанкционированного доступа со стороны пользователя-нарушителя требуют создания на программном уровне *системы опознания и разграничения доступа к информации* со всеми ее атрибутами: средствами идентификации и аутентификации пользователей, а также разграничения их полномочий по доступу к информации файл-сервера и (или) другим субъектом данной сети.

Средства защиты сети позволяют устанавливать, кто имеет право доступа к конкретным каталогам и файлам. При этом за-

щита данных файл-сервера осуществляется одним способом или в различных сочетаниях четырьмя уровнями.

Первым уровнем сетевой защиты является защита данных входным паролем. Защита при входе в сеть применяется по отношению ко всем пользователям.

Администратор безопасности уполномочен установку дополнительных ограничений по входу в сеть:

• период времени, в течение которого пользователь может входить в сеть;

• назначение рабочим станциям специального адреса, с которыми разрешено входить в сеть;

• ограничение количества рабочих станций, с которых можно выйти в сеть;

• установка режима «запрета постороннего вторжения», когда при нескольких несанкционированных попытках с неверным паролем устанавливается запрет на вход в сеть.

Второй уровень защиты данных в сети — попечительская защита данных при работе с файлами в заданном каталоге.

Третий уровень защиты данных в каталоге. Каждый каталог имеет «маску максимальных прав». Ограничения каталога применяются только в одном заданном каталоге. Защита в каталоге не распространяется на его подкаталоги.

Четвертый уровень - защита атрибутами файлов. Защита атрибутами файлов используется в основном для предотвращения случайных изменений или удаления отдельных файлов. В защите данных используются четыре файловых атрибута: «Запись-Чтение/Только чтение» и «Разделяемый/Неразделяемый».

Чтобы исключить возможность обхода систем опознания и разграничения доступа в КС и сетях путем применения отладочных программ, а также проникновения компьютерных вирусов, рекомендуется их работа без дисководов.

Перечисленные уровни защиты, предназначенные для перекрытия ВКНСД к информации, будут выполнять свою задачу, если они составляют замкнутый уровень защиты.

Для расчета и оценки уровня безопасности информации в компьютерной системы предлагается в зависимости от заданной модели нарушителя, ценности и важности обрабатываемой ин-

формации использовать три класса защиты. Распределение средств защиты по ВКНСД приведена в таблице 6.1.

Таблица 6. 1 - Распределение средств защиты по ВКНСД

Наименование ВКНСД	Средства защиты	Прочность	Класс защиты		
			I	II	III
ВКНСД элемента сети (ПЭВМ)	Система безопасности информации элемента сети (ПЭВМ)	$G_{РС}$	+	+	+
ВКНСД сервера	Средства контроля доступа на территорию объекта	$Р_1$	+	+	+
	Средства контроля доступа в помещение сервера	$Р_2$	+	+	—
	Программа контроля и разграничения доступа к информации ЛВС	$Р_3$	+	+	+
	Средства шифрования	$Р_4$	+	—	—
	Организационные мероприятия	$Р_5$	+	+	+
ВКНСД со стороны средств контроля и управления конфигурацией, адресными таблицами и функциональным контролем ЛВС	Средства контроля доступа на территорию объекта	$Р_1$	+	+	+
	Средства контроля доступа в помещение администратора	$Р_2$	+	+	—
	Программа опознания и контроля доступа к информации ПЭВМ	$Р_6$	+	+	+
	Программа контроля и разграничения доступа к информации ЛВС	$Р_3$	+	+	+
	Средства контроля целостности ЛВС	$Р_7$	+	+	—
ВКНСД со стороны линий связи ЛВС	Средства контроля доступа на территорию объекта	$Р_1$	+	+	+
	Организационные мероприятия	$Р_5$	+	+	—
	Система шифрования	$Р_4$	+	—	—
ВКНСД со стороны аппаратуры передачи данных в каналы связи, концентраторов, мостов, комму-	Средства контроля доступа на территорию объекта	$Р_I$	+	+	+
	Средства контроля доступа в помещение	$Р_2$	+	-	-
	Средства контроля вскрытия аппаратуры	$Р_8$	+	—	—
	Оргмероприятия	$Р_5$	+	+	+
ВКНСД к информации за счет ПЭМИН	Средства контроля доступа на территорию объекта	$Р_1$	+	—	—
	Средства уменьшения и зашумления сигналов, несущих секретную информацию	$Р_9$	+	—	—
ВКНСД со стороны каналов связи и трактов передачи данных	Средства защиты в каналах связи	$Р_{КС}$	+	+	+
	Средства защиты информации в трактах передачи данных	$Р_{ПД}$	+	+	+

ВКНСД со стороны средств контроля и управления безопасностью информации в ЛВС	Средства контроля доступа на территорию объекта	P_1	+	+	+
	Средства контроля доступа в помещение	P_1	+	+	-
	Программа опознания и контроля доступа к информации ПЭВМ	P_6	+	+	+
	Программа контроля и разграничения доступа к информации ЛВС	P_3	+	+	+
	Средства контроля целостности ЛВС	P_7	+	+	—
	Средства шифрования информации в ПЭВМ	P_{10}	+	—	—
	Средства шифрования информации ЛВС	P_4	+	—	—
	Оргмероприятия	P_5	+	+	+

Примечания: 1. Знак "+" означает наличие средства защиты, знак «—» — отсутствие средства защиты.
2. Считается, что все помещения оборудованы системой контроля одного типа.

6.1.2. Распределение средств защиты в модели взаимосвязи открытых систем

Модель взаимосвязи открытых систем состоит из 7 уровней взаимодействия компонентов сети компьютерной системы. На Рис. 6. 1 модель процесса взаимодействия двух субъектов компьютерной системы в режиме передачи данных от субъекта системы *A* к субъекту *B*. Непосредственно данные передаются на передающем конце с 7-го до 1-го уровня. На приемном конце данные передаются с 1-го до 7-го уровня. На передающей стороне на каждом из уровне к передаваемым данным добавляется информация о соотвествующем уровне, а на приемной стороне извлекается информации соответствующего уровня. Таким образом уровни с 7-го по 2-й образуют логический канал связи, а 1-й образует физический канал связи. Физический канал связи представляет собой физическую среду передачи сигналов (кабель, радиоканал, световой и др.).

Модель взаимосвязи открытых систем определется следующей иерархией.

- *7 уровень – прикладной.* Этот, высший уровень в иерархии, обеспечивает поддержку прикладных процессов конечных пользователей. Он содержит все необходимые элементы сервиса для прикладных программ пользователя. На этом уровне пользователь имеет свои прикладные программы, где может делать всё,

что ему необходимо, но руководствуется некоторыми установленными правилами при обменах с другим пользователем сети, т.е. выполнять соответствующие протоколы.

- *6 уровень – представительный* обеспечивает преобразование данных пользователя к форматам, принятым в данной системе; преобразует символьные строки и коды и организует файлы с целью обеспечения независимости прикладных программ от форм передачи и получения.
- *5 уровень – сеансовый* обеспечивает установление и поддержку сеансов связи между абонентами при обмене данными, организует двунаправленный обмен данными с размещением во времени, начало и окончание заданий, восстановление связи после ошибок, связанных с отказом канала и отказом сети взаимодействия, восстанавливается или повторно устанавливается соединение.
- *4 уровень – транспортный* обеспечивает управление соединением между различными абонентами, т.е. адресацию конечных абонентов, а также разборку и сборку сообщений, сохранность блоков данных, доставку данных от узла к конкретному адресату, приписанному к узлу и наоборот, выбирает маршрут пересылки данных в сеть. Таким образом, транспортный уровень предоставляет услуги сеансовому уровню. Граница между этими уровнями – это граница между владельцем сети и пользователем.

Три верхних уровня является прикладным процессом. Четвертый уровень обеспечивает взаимодействие между прикладными процессами, устанавливая между ними логические каналы и обеспечивая передачу по этим каналам информационных пакетов (группу байтов, передаваемых абонентами сети друг другу), которыми обмениваются процессы. Отметим, что столь популярный сегодня *Internet* - это транспортный уровень. Логические каналы, устанавливаемые транспортным уровнем, называются транспортными каналами.

- *3 уровень – сетевой*, обеспечивает интерфейс оконечного оборудования данных с сетью коммутации пакетов, маршрутизацию пакетов в коммуникационной сети, межсетевое взаимодействие. Сетевой уровень обеспечивает функции ретрансляции, в соответствии с которыми данные направляются по маршруту в

нужном направлении через устройства пакетной коммутации, т.е. к нужным узлам в соответствии с маршрутными таблицами.

- *2 уровень – канальный* обеспечивает процесс передачи данных по информационному каналу. Информационный канал это канал логический, который устанавливается между устройствами соединенными физическим каналом. Канальный уровень обеспечивает управление потоком данных в виде кадров, обнаруживает ошибки передачи, реализует алгоритмы восстановления информации в случае обнаружения сбоев или потерь данных. Второй уровень разбивается на два подуровня: LLC (Logical Link Control), обеспечивающий управление логическим звеном данных, и MAC (Media Access Control), обеспечивающий управление доступом к среде. Второй подуровень поддерживает метод, обеспечивающий выполнение совокупности правил, по которым узлы сети получают доступ к информационному ресурсу.
- *1 уровень – физический*, обеспечивает механические, электрические, функциональные и процедурные средства для осуществления физических соединений, их поддержания и разъединения. Среда распространения сигналов является также физическим уровнем.

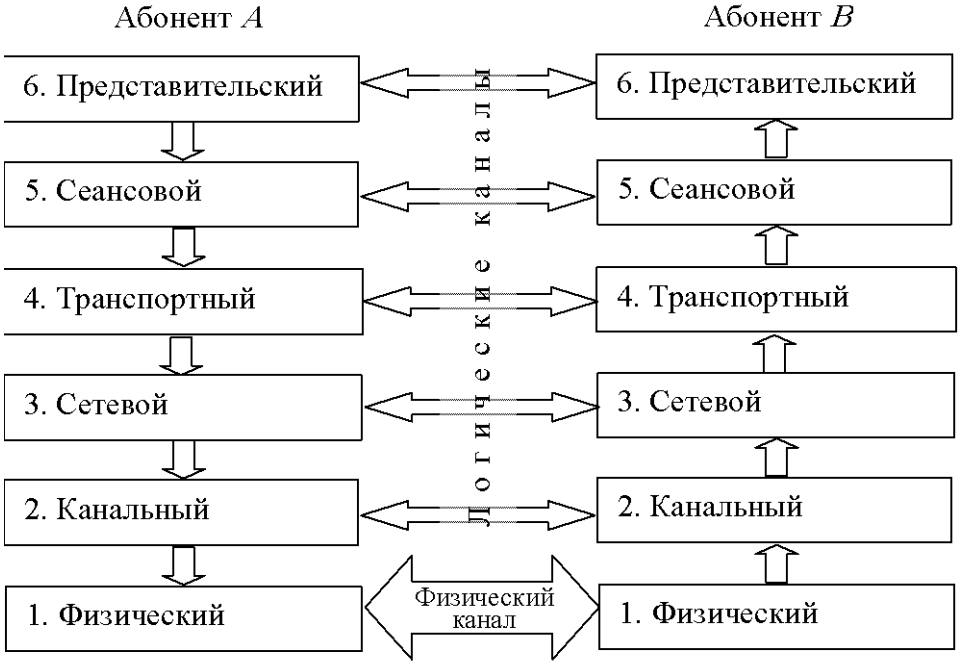


Рис. 6. 1. Модель взаимодействия уровней связи OSI открытых систем

Для создания сервисных служб защиты в открытых системах, функции которых реализуют процедуры организации этих служб (таблица 6.2) [2, 6]. К процедурам организации служб или средств защиты относятся следующие процедуры.

1. *Шифрование данных* предназначено для закрытия всех данных абонента или некоторых полей сообщения, может иметь два уровня: шифрование в канале связи (линейное) и межконцевое (абонентское) шифрование. В первом случае, чтобы предотвратить возможности анализа графика, шифруется вся информация, передаваемая в канал связи, включая все сетевые заголовки. Абонентское шифрование предназначено для предотвращения раскрытия только данных абонента.

2. *Цифровая подпись* передаваемых сообщений служит для подтверждения правильности содержания сообщения. Она удостоверяет факт его отправления именно тем абонентом, который указан в заголовке в качестве источника данных. Цифровая подпись является функцией от содержания секретного сообщения, известного только абоненту-источнику, и общей информации, известной всем абонентам сети.

3. *Управление доступом* к ресурсам сети выполняется на основании множества правил и формальных моделей, использующих в качестве аргумента доступа информацию о ресурсах (классификацию) и идентификаторы абонентов. Служебная информация для управления доступом (пароли абонентов, списки разрешенных операций, персональные идентификаторы, временные ограничители и т. д.) содержится в локальных базах данных службы обеспечения безопасности сети.

4. *Обеспечение целостности данных* предполагает введение в каждое сообщение некоторой дополнительной информации, которая является функцией от содержания сообщения. В рекомендациях МОС рассматриваются методы обеспечения целостности двух типов: первые обеспечивают целостность единственного блока данных, вторые — целостность потока блоков данных или отдельных полей этих блоков. Эти методы применяются в двух режимах — при передаче данных по виртуальному соединению и при использовании дейтаграммной передачи. В первом случае обнаруживаются неупорядоченность, потери, повторы, вставки данных при помощи специальной нумерации блоков или введе-

нием меток времени. В дейтаграммном режиме метки времени могут обеспечить только ограниченную защиту целостности последовательности блоков данных и предотвратить переадресацию отдельных блоков.

5. *Процедуры аутентификации* предназначены для защиты при передаче в сети паролей, аутентификаторов логических объектов и т. д. Для этого используются криптографические методы и протоколы, основанные, например, на процедуре "троекратного рукопожатия". Целью таких протоколов является защита от установления соединения с логическим объектом, образованным нарушителем или действующим под его управлением с целью имитации работы подлинного объекта.

6. *Процедура заполнения потока* служит для предотвращения возможности анализа графика. Эффективность применения этой процедуры повышается, если одновременно с ней предусмотрено линейное шифрование всего потока данных, т. е. потоки информации и заполнения делаются неразличимыми.

7. *Управление маршрутом* предназначено для организации передачи данных только по маршрутам, образованным с помощью надежных и безопасных технических устройств и систем. При этом может быть организован контроль со стороны получателя, который в случае возникновения подозрения о компрометации используемой системы защиты может потребовать изменения маршрута следования данных.

8. *Процедура подтверждения характеристик данных* предполагает наличие арбитра, который является доверенным лицом взаимодействующих абонентов и может подтвердить целостность, время передачи сообщения, а также предотвратить возможность отказа источника от выдачи какого-либо сообщения, а потребителя — от его приема.

Данные рекомендации по организации служб защиты информации в компьютерных системах требуют более детальной проработки на предмет их реализации в существующих протоколах. С позиций предлагаемой в данной работе концепции защиты можно заметить некоторую избыточность защитных функций, например аутентификации, которая является неотъемлемой частью функции контроля доступа и, следовательно, автоматически

в нее входит. Для сокращения количества средств защиты целесообразно взять за основу средства защиты на 7-м уровне и дополнить их средствами на остальных уровнях, но только теми, которые выполнят защитные функции, не охваченные средствами защиты на 7-м уровне.

Таблица 6. 2 - Организация служб защиты информации

Процедура защиты	Номер процедуры	Средство защиты	Логические уровни						
			1	2	3	4	5	6	7
Аутентификация: одноуровневых объектов источника данных	1	Шифрование, цифровая подпись	-	-	+	+	-	-	-
		Обеспечение аутентификации	-	-	+	+	-	-	+
	2	Шифрование	-	-	+	+	-	-	-
		Цифровая подпись	-	-	+	+	-	-	+
Контроль доступа	3	Управление доступом	-	-	+	+	-	-	+
Засекречивание: соединения	4	Шифрование	+	+	+	+	-	-	+
		Управление маршрутом	-	-	+	-	-	-	-
в режиме без соединения выборочных полей потока данных	5	Шифрование	-	+	+	+	-	+	+
		Управление маршрутом	-	-	+	-	-	-	-
	6	Шифрование	-	-	-	-	-	+	+
	7	Шифрование	+	-	-	-	-	+	-
		Заполнение потока	-	-	+	-	-	-	+
		Управление маршрутом	-	-	+	-	-	-	-
Обеспечение целостности: соединения с восстановлением	8	Шифрование, обеспечение целостности данных	-	-	-	+	-	-	+
соединения без восстановления	9	Шифрование, обеспечение целостности данных	-	-	+	+	-	-	+
выборочных полей данных без установления соединения данных	10	Шифрование, обеспечение целостности данных	-	-	-	-	-	-	+
	11	Шифрование, обеспечение целостности данных	-	-	+	+	-	-	+
		Цифровая подпись	-	-	-	+	-	-	-
выборочных полей без соединения	12	Цифровая подпись Обеспечение целостности данных	- -	- -	-	+ -	- -	- -	+ +
Информирование: об отправке	13	Цифровая подпись, обеспечение целостности данных, подтверждение характеристик данных	-	-	-	-	-	-	+
о доставке	14	Цифровая подпись, обеспечение целостности данных, подтверждение характеристик данных	-	-	-	-	-	-	+

Для распределенных автоматизированных систем обработки данных: региональных и глобальных сетей и автоматизированных систем управления из-за их высокой стоимости целесообразна классификация нарушителя только по двум классам: 1- и 2-му, а для локальных — по 1-, 2- и 3-му классам. Входящие в их состав компьютерных систем автоматики средства защиты могут обеспечивать защиту более низкого класса, а информация, передаваемая по каналам связи, должна быть защищена по тому же классу. 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 защищенности 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, техническим персоналом, обслуживающим компьютерную систему. Если нарушителем становится 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.

Оценка защищенности должна проводиться отдельно для каждого случая. При этом следует учитывать соответствующее количество ВКНСД и средств защиты. В отдельных случаях в необходимо проводить такую оценку для каждого пользователя.

6.2. Инженерно-технические средства защиты

Функционирование любого технического средства информации связано с протеканием по его токоведущим элементам

электрических токов различных частот и образованием разности потенциалов между различными точками его электрической схемы, которые порождают магнитные и электрические поля, называемые побочными электромагнитными излучениями.

Узлы и элементы электронной аппаратуры, в которых имеют место большие напряжения и протекают малые токи, создают в ближней зоне электромагнитные поля с преобладанием электрической составляющей. Преимущественное влияние электрических полей на элементы электронной аппаратуры наблюдается и в тех случаях, когда эти элементы малочувствительны к магнитной составляющей электромагнитного поля.

Узлы и элементы электронной аппаратуры, в которых протекают большие токи и имеют место малые перепады напряжения, создают в ближней зоне электромагнитные поля с преобладанием магнитной составляющей. Преимущественное влияние магнитных полей на аппаратуру наблюдается также в случае, если рассматриваемое устройство малочувствительно к электрической составляющей за счет свойств излучателя. Переменные электрическое и магнитное поля создаются в пространстве, окружающими соединительными линиями (проводами, кабелями) технических средств передачи информации (ТСПИ).

Побочные электромагнитные излучения ТСПИ являются причиной возникновения электромагнитных и параметрических каналов утечки информации, а также могут оказаться причиной возникновения наводки информационных сигналов в посторонних токоведущих линиях и конструкциях. Поэтому снижению уровня побочных электромагнитных излучений уделяется большое внимание.

Эффективным методом снижения уровня ПЭМИ является экранирование их источников.

Различают следующие способы экранирования:

- электростатическое;
- магнитостатическое;
- электромагнитное.

Электростатическое и магнитостатическое экранирование основано на замыкании экраном (обладающим в первом случае

высокой электропроводностью, а во втором - магнитопроводностью) соответственно электрического и магнитного полей.

Электростатическое экранирование по существу сводится к замыканию электростатического поля на поверхность металлического экрана и отводу электрических зарядов на землю (на корпус прибора). Заземление электростатического экрана является необходимым элементом при реализации электростатического экранирования. Применение металлических экранов позволяет полностью устранить влияние электростатического поля. При использовании диэлектрических экранов, плотно прилегающих к экранируемому элементу, можно ослабить поле источника наводки в ε раз, где ε - относительная диэлектрическая проницаемость материала экрана.

Основной задачей экранирования электрических полей является снижение емкости связи между экранируемыми элементами конструкции. Эффективность экранирования определяется в основном отношением емкостей связи между источником и рецептором наводки до и после установки заземленного экрана. Поэтому любые действия, приводящие к снижению емкости связи, увеличивают эффективность экранирования.

Экранирующее действие металлического листа существенно зависит от качества соединения экрана с корпусом прибора и частей экрана друг с другом. Особенно важно не иметь соединительных проводов между частями экрана и корпусом.

В диапазонах метровых и более коротких длин волн соединительные проводники длиной несколько сантиметров могут резко ухудшить эффективность экранирования. На еще более коротких волнах дециметрового и сантиметрового диапазонов соединительные проводники и шины между экранами недопустимы. Для получения высокой эффективности экранирования электрического поля здесь необходимо применять непосредственное сплошное соединение отдельных частей экрана друг с другом.

Узкие щели и отверстия в металлическом экране, размеры которых малы по сравнению с длиной волны, практически не ухудшают экранирование электрического поля.

С увеличением частоты излучения эффективность экранирования снижается.

Основные требования, которые предъявляются к электрическим экранам, можно сформулировать следующим образом:

- конструкция экрана должна выбираться такой, чтобы силовые линии электрического поля замыкались на стенки экрана, не выходя за его пределы;
- в области низких частот (при глубине проникновения (b) больше толщины (d), т.е. при $b > d$ эффективность электростатического экранирования практически определяется качеством электрического контакта металлического экрана с корпусом устройства и мало зависит от материала экрана и его толщины;
- в области высоких частот (при $d < b$) эффективность экрана, работающего в электромагнитном режиме, определяется его толщиной, проводимостью и магнитной проницаемостью.

Магнитостатическое экранирование используется при подавлении наводки на низких частотах от 0 до 3...10 кГц.

Основные требования, предъявляемые к магнитостатическим экранам, можно свести к следующим:

- магнитная проницаемость μ материала экрана должна быть возможно более высокой. Для изготовления экранов желательно применять магнитомягкие материалы с высокой магнитной проницаемостью (например, пермаллой);
- увеличение толщины стенок экрана приводит к повышению эффективности экранирования, однако при этом следует принимать во внимание возможные конструктивные ограничения по массе и габаритам экрана;
- стыки, разрезы и швы в экране должны размещаться параллельно линиям магнитной индукции магнитного поля. Их число должно быть минимальным;
- заземление экрана не влияет на эффективность магнитостатического экранирования.

Эффективность магнитостатического экранирования повышается при применении многослойных экранов.

Экранирование высокочастотного магнитного поля основано на использовании магнитной индукции, создающей в экране переменные индукционные вихревые токи (токи Фуко). Магнитное поле этих токов внутри экрана будет направлено навстречу

возбуждающему полю, а за его пределами – в ту же сторону, что и возбуждающее поле. Результирующее поле оказывается ослабленным внутри экрана и усиленным вне его. Вихревые токи в экране распределяются неравномерно по его сечению (толщине). Это вызывается явлением поверхностного эффекта, сущность которого заключается в том, что переменное магнитное поле ослабевает по мере проникновения в глубь металла, так как внутренние слои экранируются вихревыми токами, циркулирующими в поверхностных слоях.

Благодаря поверхностному эффекту плотность вихревых токов и напряженность переменного магнитного поля по мере углубления в металл падает по экспоненциальному закону.

Эффективность магнитного экранирования зависит от частоты и электрических свойств материала экрана. Чем ниже частота, тем слабее действует экран, тем большей толщины приходится его делать для достижения одного и того же экранирующего эффекта. Для высоких частот, начиная с диапазона средних волн, (500 кГц и выше) экран из любого металла толщиной 0,5 ... 1,5 мм действует весьма эффективно. При выборе толщины и материала экрана следует учитывать механическую прочность, жесткость, стойкость против коррозии, удобство стыковки отдельных деталей и осуществления между ними переходных контактов с малым сопротивлением, удобство пайки, сварки и пр.

Для частот выше 10 МГц медная или серебряная пленка толщиной более 0,1 мм дает значительный экранирующий эффект. Поэтому на частотах выше 10 МГц вполне допустимо применение экранов из фольгированного гетинакса или другого изоляционного материала с нанесенным на него медным или серебряным покрытием.

При экранировании магнитного поля заземление экрана не изменяет величины возбуждаемых в экране токов и, следовательно, на эффективность магнитного экранирования не влияет.

На высоких частотах применяется исключительно *электромагнитное экранирование.* Действие электромагнитного экрана основано на том, что высокочастотное электромагнитное поле ослабляется им же созданным (благодаря образующимся в толще экрана вихревым токам) полем обратного направления.

Теория и практика показывают, что с точки зрения стоимости материала и простоты изготовления преимущества на стороне экранированного помещения из листовой стали. Однако при применении сетчатого экрана могут значительно упроститься вопросы вентиляции и освещения помещения. В связи с этим сетчатые экраны также находят широкое применение.

Для изготовления экрана целесообразно использовать следующие материалы:

- сталь листовая декапированная ГОСТ 1386-47 толщиной (мм) 0,35; 0,50; 0,60; 0,70; 0,80; 1,00; 1,25; 1,50; 1,75; 2,00;
- сталь тонколистовая оцинкованная ГОСТ 7118-54 толщиной (мм) 0,35; 0,50; 0,60; 0,70; 0,80; 1,00; 1,25; 1,50; 1,75; 2,00;
- сталь тонколистовая оцинкованная ГОСТ 7118-54 толщиной (мм) 0,51; 0,63; 0,76; 0,82; 1,00; 1,25; 1,50;
- сетка стальная тканая ГОСТ 3826-47 номер 0,4; 0,5; 0,7; 1,0; 1,4; 1,6; 1,8; 2,0; 2,5;
- сетка стальная плетеная ГОСТ 5336-50 номер 3; 4; 5; 6;
- сетка из латунной проволоки марки Л-80 ГОСТ 6613-53 0,25; 0,5; 1,0; 1,6; 2,0; 2,5; 2,6.

Металлические листы или полотнища сетки должны быть между собой электрически соединены по всему периметру. Для сплошных экранов это может быть осуществлено электросваркой или пайкой. Шов электросварки или пайки должен быть непрерывным с тем, чтобы получить цельносварную конструкцию экрана,

Для сетчатых экранов пригодна любая конструкция шва, обеспечивающая хороший электрический контакт между соседними полотнищами сетки не реже чем через 10 ... 15 мм. Для этой цели может применяться пайка или точечная сварка.

Экран, изготовленный из луженой низкоуглеродистой стальной сетки с ячейкой 2,5 ... 3 мм, дает ослабление порядка 55 ... 60 дБ, а из такой же двойной (с расстоянием между наружной и внутренней сетками 100 мм) - около 90 дБ. Экран, изготовленный из одинарной медной сетки с ячейкой 2,5 мм, имеет ослабление порядка 65 ... 70 дБ.

Необходимая эффективность экрана в зависимости от его назначения и величины уровня излучения ПЭМИН обычно находится в пределах 60... 120 дБ.

Наряду блоками аппаратуры экранированию подлежат монтажные провода и соединительные линии.

Чтобы уменьшить уровень ПЭМИ, необходимо особенно тщательно выполнять соединение оболочки провода (экрана) с корпусом аппаратуры. Подключение оболочки должно осуществляться путем непосредственного контакта (лучше всего путем пайки или сварки) с корпусом.

Вместе с тем соединение оболочки провода с корпусом в одной точке не ослабляет в окружающем пространстве магнитное поле, создаваемое протекающим по проводу током. Для экранирования магнитного поля необходимо создать поле такой же величины и обратного направления. С этой целью необходимо весь обратный ток экранируемой цепи направить через экранирующую оплетку провода. Для полного осуществления этого принципа необходимо, чтобы экранирующая оболочка была единственным путем для протекания обратного тока.

Высокая эффективность экранирования обеспечивается при использовании витой пары, защищенной экранирующей оболочкой.

На низких частотах приходится использовать более сложные схемы экранирования - коаксиальные кабели с двойной оплеткой (триаксильные кабели).

На более высоких частотах, когда толщина экрана значительно превышает глубину проникновения поля, необходимость в двойном экранировании отпадает. В этом случае внешняя поверхность играет роль электрического экрана, а по внутренней поверхности протекают обратные токи.

Применение экранирующей оболочки существенно увеличивает емкость между проводом и корпусом, что в большинстве случаев нежелательно. Экранированные провода более громоздки и неудобны при монтаже, требуют предохранения от случайных соединений с посторонними элементами и конструкциями.

Длина экранированного монтажного провода должна быть меньше четверти длины самой короткой волны передаваемого по проводу спектра сигнала. При использовании более длинных уча-

стков экранированных проводов необходимо иметь в виду, что в этом случае экранированный провод следует рассматривать как длинную линию, которая во избежании искажений формы передаваемого сигнала должна быть нагружена на сопротивление, равное волновому.

Для уменьшения взаимного влияния монтажных цепей следует выбирать длину монтажных высокочастотных проводов наименьшей, для чего элементы высокочастотных схем, связанные между собой, следует располагать в непосредственной близости, а неэкранированные провода высокочастотных цепей - при пересечении под прямым углом. При параллельном расположении такие провода должны быть максимально удалены друг от друга или разделены экранами, в качестве которых могут быть использованы несущие конструкции электронной аппаратуры (кожух, панель и т.д.).

Экранированные провода и кабели следует применять в основном для соединения отдельных блоков и узлов друг с другом.

Кабельные экраны выполняются в форме цилиндра из сплошных оболочек, в виде спирально намотанной на кабель плоской ленты или в виде оплетки из тонкой проволоки. Экраны при этом могут быть однослойными и многослойными комбинированными, изготовленными из свинца, меди, стали, алюминия и их сочетаний (алюминий-свинец, алюминий-сталь, медь-сталь-медь и т.д.).

В кабелях с наружными пластмассовыми оболочками применяют экраны ленточного типа в основном из алюминиевых, медных и стальных лент, накладываемых спирально или продольно вдоль кабеля.

В области низких частот корпуса применяемых многоштырьковых низкочастотных разъемов являются экранами и должны иметь надежный электрический контакт с общей шиной или землей прибора, а зазоры между разъемом и корпусом должны быть закрыты электромагнитными уплотняющими прокладками.

В области высоких частот коаксиальные кабели должны быть согласованы по волновому сопротивлению с используемыми высокочастотными разъемами. При заделке коаксиального кабеля в высокочастотные разъемы жила кабеля не должна иметь

натяжения в месте соединения с контактом разъема, а сам кабель должен быть жестко прикреплен к шасси аппаратуры вблизи разъема.

Для эффективного экранирования низкочастотных полей применяются экраны, изготовленные из ферромагнитных материалов с большой относительной магнитной проницаемостью. При наличии такого экрана линии магнитной индукции проходят в основном по его стенкам, которые обладают малым сопротивлением по сравнению с воздушным пространством внутри экрана. Качество экранирования таких полей зависит от магнитной проницаемости экрана и сопротивления магнитопровода, которое будет тем меньше, чем толще экран и меньше в нем стыков и швов, идущих поперек направления линий магнитной индукции.

Наиболее экономичным способом экранирования информационных линий связи между устройствами ТСПИ считается групповое размещение их информационных кабелей в экранирующий распределительный короб. Когда такого короба не имеется, то приходится экранировать отдельные линии связи.

Для защиты линий связи от наводок необходимо разместить линию в экранирующую оплетку или фольгу, заземленную в одном месте, чтобы избежать протекания по экрану токов, вызванных неэквипотенциальностью точек заземления.

Для защиты линии связи от наводок необходимо минимизировать площадь контура, образованного прямым и обратным проводами линии. Если линия представляет собой одиночный провод, а возвратный ток течет по некоторой заземляющей поверхности, то необходимо максимально приблизить провод к поверхности. Если линия образована двумя проводами, то их необходимо скрутить, образовав бифиляр (витую пару). Линии, выполненные из экранированного провода или коаксиального кабеля, в которых по оплетке протекает возвратный ток, также отвечают требованию минимизации площади контура линии.

Наилучшую защиту, как от электрического, так и от магнитного полей обеспечивают информационные линии связи типа экранированного бифиляра, трифиляра (трех скрученных вместе проводов, из которых один используется в качестве электрического экрана), триаксильного кабеля (изолированного коаксильального кабеля, помещенного в электрический экран), экраниро-

ванного плоского кабеля (плоского много-проводного кабеля, покрытого с одной или обеих сторон медной фольгой).

Приведем несколько схем, используемых на частотах порядка 100 кГц.

Схема на рис. 6.2.а, имеет большую площадь петли, образованной "прямым" проводом и "землей". Эта цепь подвержена, прежде всего, магнитному влиянию. Экран заземлен на одном конце и не защищает от магнитного влияния. Переходное затухание для этой схемы примем равным 0 дБ для сравнения с затуханием схем на рис. 6.2.б-и.

Схема на рис. 6.2.б практически не уменьшает магнитную связь, так как обратный провод заземлен с обоих концов, и в этом смысле она аналогична схеме на рис. 6.2.а. Степень улучшения соизмерима с погрешностью расчета (измерения).

Схема на рис. 6.2.в отличается от схемы на рис. 6.2.а наличием обратного провода- коаксиального экрана, однако экранирование магнитного поля ухудшено, так как цепь заземлена на обоих концах, в результате чего с "землей" образуется петля большой площади.

Схема на рис. 6.2.г позволяет существенно повысить защищенность цепи (- 49 дБ) благодаря скрутке проводов. В этом случае (по сравнению со схемой на рис. 6.2.б) петли нет, поскольку правый конец цепи не заземлен.

Дальнейшее повышение защищенности цепи достигается применением схемы на рис. 6.2.е, коаксиальная цепь которой обеспечивает лучшее магнитное экранирование, чем скрученная пара на рис. 6.2.г.

Площадь петли в схеме на рис. 6.2.д не больше, чем в схеме на рис. 6.2 .г, так как продольная ось экрана коаксиального кабеля совпадает с его центральным проводом.

Схема на рис. 6.2.е позволяет повысить защищенность цепи благодаря тому, что скрученная пара заземлена лишь на одном конце. Кроме того, в этой схеме используется независимый экран.

Схема на рис. 6.2.ж имеет ту же защищенность, что и схема на рис. 6.2.е: эффект тот же, что и при заземлении на обоих кон-

цах, поскольку длина цепи и экрана существенно меньше рабочей длины волны.

Причины улучшения защищенности схемы на рис. 6.2.з по сравнению с рис. 6.2.ж объяснить трудно. Возможной причиной может быть уменьшение площади эквивалентной петли.

Более плотная скрутка проводов (схема рис. 6.2.и) позволяет дополнительно уменьшить магнитную связь. Кроме того, при этом уменьшается и электрическая связь (в обоих проводах токи наводятся одинаково).

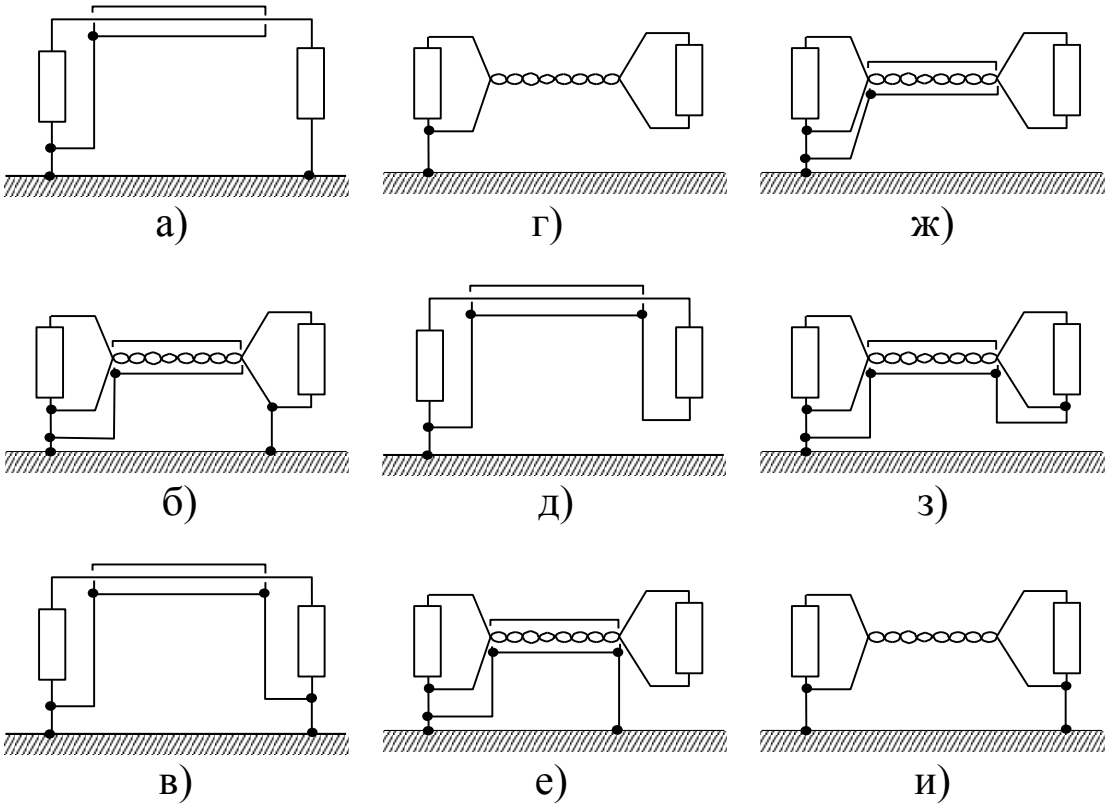


Рис. 6. 2. Сравнение защищенности различных цепей от влияния внешних магнитных и электрических цепей:

а) 0 дБ; б) -2 дБ; в) -5 дБ; г) - 49 дБ, скрученная пара, 18 витков на метр; д) - 57 дб; е) - 64 дБ, схема предпочтительна на высоких частотах; ж) - 64 дБ; з) - 71 дБ; и) - 79 дБ, скрученная пара (54 витка на метр)

Для уменьшения магнитной и электрической связи между проводами необходимо уменьшить площадь петли, максимально разнести цепи и максимально уменьшить длину параллельного пробега линий ТСПИ и посторонними проводниками.

При нулевых уровнях сигналов (0 dB) в соединительных линиях ТСПИ между ними и посторонними проводниками должно обеспечиваться переходное затухание не менее 114 dB. Данное переходное затухание обеспечивается, как правило, при прокладке кабелей ТСПИ на расстоянии не менее 0,1 м от посторонних проводников. При этом допускается прокладка кабелей ТСПИ вплотную с посторонними проводниками при суммарной длине их совместного пробега не более 70 м.

Экранироваться могут не только отдельные блоки аппаратуры и их соединительные линии, но и помещения в целом. В обычных (неэкранированных) помещениях основной экранирующий эффект обеспечивают железобетонные стены домов. Экранирующие свойства дверей и окон хуже. Для повышения экранирующих свойств стен применяются дополнительные средства, в том числе:

- токопроводящие лакокрасочные покрытия или токопроводящие обои;
- шторы из металлизированной ткани;
- металлизированные стекла (например, из двуокиси олова), устанавливаемые в металлические или металлизированные рамы.

В помещении экранируются стены, двери и окна.

При закрытии двери должен обеспечиваться надежный электрический контакт со стенками помещения (с дверной рамой) по всему периметру не реже чем через 10 ... 15 мм. Для этого может быть применена пружинная гребенка из фосфористой бронзы, которую укрепляют по всему внутреннему периметру дверной рамы.

Окна должны быть затянуты одним или двумя слоями медной сетки с ячейкой не более 2*2 мм, причем расстояние между слоями сетки должно быть не менее 50 мм. Оба слоя сетки должны иметь хороший электрический контакт со стенками помещения (с рамой) по всему периметру. Сетки удобнее делать съемными и металлическое обрамление съемной части также должно иметь пружинящие контакты в виде гребенки из фосфористой бронзы.

При проведении работ по тщательному экранированию подобных помещений необходимо одновременно обеспечить нор-

мальные условия для работающего в нем человека, прежде всего вентиляцию воздуха и освещение.

Конструкция экрана для вентиляционных отверстий зависит от диапазона частот. Для частот менее 1000 МГц применяются сотовые конструкции, закрывающие вентиляционное отверстие, с прямоугольными, круглыми, шестигранными ячейками. Для достижения эффективного экранирования размеры ячеек должны быть менее одной десятой от длины волны. При повышении частоты необходимые размеры ячеек могут быть столь малыми, что ухудшается вентиляция.

Экранировку электромагнитных волн более 100 дБ можно обеспечить только в специальных экранированных камерах, в которых электромагнитный экран выполнен в виде электрогерметичного стального корпуса, а для ввода электрических коммуникаций используются специальные фильтры.

Размеры экранированного помещения выбирают исходя из его назначения и стоимости. Обычно экранированные помещения строят площадью 6...8 м^2 при высоте 2,5...3 м.

Необходимо помнить, что экранирование ТСПИ и соединительных линий эффективно только при правильном их заземлении. Поэтому одним из важнейших условий по защите ТСПИ является правильное заземление этих устройств.

В настоящее время существуют различные типы заземлений. Наиболее часто используются одноточечные, многоточечные и комбинированные (гибридные) схемы.

На (Рис. 6. 3) представлена одноточечная последовательная схема заземления.

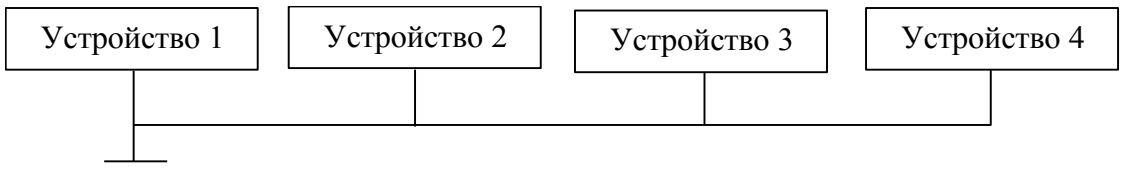


Рис. 6. 3. Одноточечная последовательная схема заземления

Эта схема наиболее проста. Однако ей присущ недостаток, связанный с протеканием обратных токов различных цепей по общему участку заземляющей цепи. Вследствие этого возможно появление опасного сигнала в посторонних цепях.

В одноточечной параллельной схеме заземления (Рис. 6. 4) этого недостатка нет. Однако такая схема требует большого числа протяженных заземляющих проводников, из-за чего может возникнуть проблема с обеспечением малого сопротивления заземления участков цепи. Кроме того, между заземляющими проводниками могут возникать нежелательные связи, которые создают несколько путей заземления для каждого устройства. В результате в системе заземления могут возникнуть уравнительные токи и появиться разность потенциалов между различными устройствами.

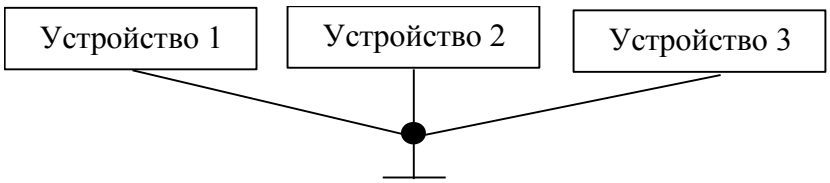


Рис. 6. 4. Одноточечная параллельная схема заземления

Многоточечная схема заземления (Рис. 6. 5) практически свободна от недостатков, присущих одноточечной схеме. В этом случае отдельные устройства и участки корпуса индивидуально заземлены. При проектировании и реализации многоточечной системы заземления необходимо принимать специальные меры для исключения замкнутых контуров.

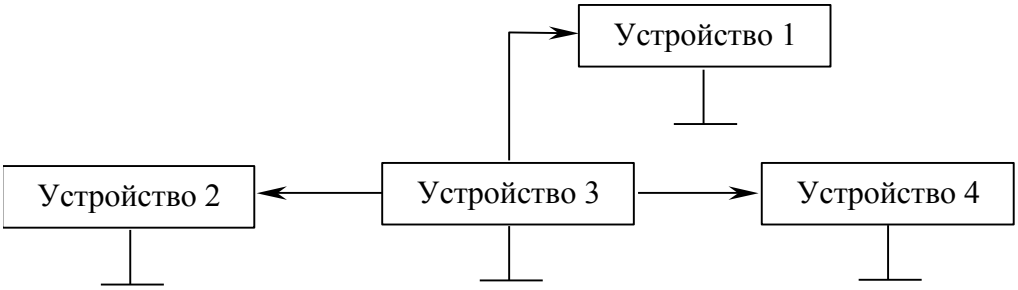


Рис. 6. 5. Многоточечная схема заземления

Как правило, одноточечное заземление применяется на низких частотах при небольших размерах заземляемых устройств и расстояниях между ними менее 0,5•λ. На высоких частотах при больших размерах заземляемых устройств и значительных расстояниях между ними используется многоточечная система заземления. В промежуточных случаях эффективна комбинирован-

ная (гибридная) система заземления, представляющая собой различные сочетания одноточечной, многоточечной и плавающей заземляющих систем.

Заземление технических средств систем информатизации и связи должно быть выполнено в соответствии с определенными правилами.

Основные требования, предъявляемые к системе заземления, заключаются в следующем:

- система заземления должна включать общий заземлитель, заземляющий кабель, шины и провода, соединяющие заземлитель с объектом;
- сопротивления заземляющих проводников, а также земляных шин должны быть минимальными;
- каждый заземляемый элемент должен быть присоединен к заземлителю или к заземляющей магистрали при помощи отдельного ответвления. Последовательное включение в заземляющий проводник нескольких заземляемых элементов запрещается;
- в системе заземления должны отсутствовать замкнутые контуры, образованные соединениями или нежелательными связями между сигнальными цепями и корпусами устройств, между корпусами устройств и землей;
- следует избегать использования общих проводников в системах экранирующих заземлений, защитных заземлений и сигнальных цепей;
- качество электрических соединений в системе заземления должно обеспечивать минимальное сопротивление контакта, надежность и механическую прочность контакта в условиях климатических воздействий и вибрации;
- контактные соединения должны исключать возможность образования оксидных пленок на контактирующих поверхностях и связанных с этими пленками нелинейных явлений;
- контактные соединения должны исключать возможность образования гальванических пар для предотвращения коррозии в цепях заземления;
- запрещается использовать в качестве заземляющего устройства нулевые фазы электросетей, металлоконструкции зданий, имеющие соединение с землей, металлические оболочки подзем-

ных кабелей, металлические трубы систем отопления, водоснабжения, канализации и т.д.

Сопротивление заземления определяется главным образом сопротивлением растекания тока в земле. Величину этого сопротивления можно значительно понизить за счет уменьшения переходного сопротивления между заземлителем и почвой путем тщательной очистки перед укладкой поверхности заземлителя и утрамбовкой вокруг него почвы, а также подсыпкой поваренной соли.

Таким образом, величина сопротивления заземления будет в основном определяться сопротивлением грунта.

Удельное сопротивление различных грунтов (т.е. электрическое сопротивление 1 $см^3$ грунта) зависит от влажности почвы, ее состава, плотности, температуры и т.п.. и колеблется в очень широких пределах (см. табл. 6.3).

Таблица 6. 3 - Значения удельного сопротивления различных грунтов

Тип грунта	Удельное сопротивление (р), $Ом/см^3$		
	среднее	минимальное	максимальное
Золы, шлаки, соляные отходы	2370	500	7000
Глина, суглинки, сланцы	4060	340	16300
То же с примесями песка	15800	1020	135 000
Гравий, песок, камни с небольшим количеством глины или суглинков	94000	59000	458 000

Хорошо проводящие грунты теряют свои свойства при отсутствии влаги. Для большинства грунтов 30 % содержания влаги достаточно для обеспечения малого сопротивления. Например, для суглинков удельное сопротивление при влажности 5 % составляет 165000 $Ом/см^3$, а при влажности 30 % - 6400 $Ом/см^3$.

При промерзании сопротивление грунтов резко возрастает. Например, для суглинков удельное сопротивление при влажности 15 % и температуре 20°С составляет 7200 $Ом/см^3$, при температуре -5°С - 79000 $Ом/см^3$, а при температуре -15°С - 330000 $Ом/см^3$.

Орошение почвы вокруг заземлителей 2...5 процентным соляным раствором значительно (в 5...10 раз) снижает сопротивление заземления.

Учесть все факторы, влияющие на проводимость почвы, аналитическим путем практически невозможно, поэтому при устройстве заземления величину удельного сопротивления грунта в тех местах, где предполагается размещение заземления, определяют опытным путем.

Как правило, измерение сопротивления заземления проводится два раза в год (зимой и летом).

Если заземлитель состоит из металлической пластины радиуса r, расположенной непосредственно у поверхности земли, то сопротивление заземления $R_З$ можно рассчитать по формуле

$$R_З = \frac{\rho}{4r_п}, \text{ Ом}, \qquad (6.\ 1)$$

где ρ - удельное сопротивление грунта, Ом/см^3;

$r_п$ - радиус пластины, см.

При увеличении глубины закапывания $l_З$ пластины сопротивление заземления уменьшается и при $l_З$ значительно больше r ($l_З » r$) величина $R_З$ уменьшается в два раза.

Довольно часто применяют заземляющее устройство в виде вертикально вбитой трубы. Сопротивление заземления в этом случае определяется формулой

$$R_З = \frac{\rho}{2\pi l}\left[\ln\left(\frac{4l}{r_Т}-1\right)\right], \text{ Ом}, \qquad (6.\ 2)$$

где l - длина трубы, см;

$r_Т$ - радиус трубы, см.

Из формулы видно, что сопротивление заземления зависит в большей степени не от радиуса трубы, а от ее длины. Поэтому при устройстве заземления целесообразнее применять тонкие и длинные трубы (стержни из арматуры).

В табл. 6.4. приведены экспериментально полученные значения сопротивления заземления стержневого заземлителя (0 15,9 мм, 1 = 1,5 м) для различных грунтов.

В качестве одиночных стержневых заземлителей целесообразно использовать медные заземляющие стержни.

Как видно из табл. 6.4., сопротивление простых одиночных заземлителей оказывается достаточно большим. Поэтому такие заземлители находят применение при невысоких требованиях к заземляющим устройствам или при почвах с очень большой проводимостью.

Таблица 6. 4 - Значения сопротивления заземления стержневого заземлителя (Ø 15,9 мм, *l* = 1,5 м) для различных грунтов

Тип грунта	Сопротивление заземления $R_З$, Ом		
	среднее	минимальное	максимальное
Золы, шлаки, соляные отходы	14	3,5	41
Глина, суглинки, сланцы	24	2	98
То же с примесями песка	93	6	800
Гравий, песок, камни с небольшим количеством глины или суглинков	554	35	2700

При повышенных требованиях к величине сопротивления заземления (сопротивление заземления ТСПИ не должно превышать 4 Ом) применяют многократное заземление, состоящее из ряда одиночных симметрично расположенных заземлителей, соединенных между собой.

На практике наиболее часто в качестве заземлителей применяют:

- стержни из металла, обладающие высокой электропроводностью, погруженные в землю и соединенные с наземными металлоконструкциями средств ТСПИ;
- сеточные заземлители, изготовленные из элементов с высокой электропроводностью и погруженные в землю (служат в качестве дополнения к заземляющим стержням).

При необходимости устройства высокочастотного заземления нужно учитывать не только геометрические размеры заземлителей, их конструкцию и свойства почвы, но и длину волны высокочастотного излучения. Суммарное высокочастотное сопротивление заземления Z_S складывается из высокочастотного сопротивления магистрали заземления Z_M (провода, идущего от заземляемого устройства до поверхности земли) и из высокочастотного сопротивления самого заземлителя $Z_З$ (провода, металлического стержня или листа, находящегося в земле).

Величина заземления в основном определяется не сопротивлением заземления, а сопротивлением заземляющей магистрали. Для уменьшения последнего следует стремиться прежде всего к уменьшению индуктивности заземляющей магистрали, что достигается за счет уменьшения ее длины и изготовления магистрали в виде ленты, обладающей по сравнению с проводом круглого сечения меньшей индуктивностью. В тех случаях, когда индуктивность заземляющей магистрали можно сделать весьма небольшой или использовать ее для получения последовательного резонанса при блокировании излучающих сетей защитными конденсаторами на землю (например, при комплексном подавлении излучения в помещениях), целесообразно значительно уменьшить величину сопротивления заземлителя $Z_З$. Уменьшить величину $Z_З$ можно также многократным заземлением из симметрично расположенных заземлителей.

При этом общее сопротивление заземления будет тем меньше, чем дальше друг от друга расположены отдельные заземлители.

При устройстве заземления в качестве заземлителей чаще всего применяются стальные трубы длиной 2 ... 3 м и диаметром 35 ... 50 мм и стальные полосы сечением 50 ... 100 мм.

Наиболее пригодными являются трубы, позволяющие достигнуть глубоких и наиболее влажных слоев земли, обладающих наибольшей проводимостью и не подвергающихся высыханию или промерзанию. Однако здесь необходимо учитывать, что с уменьшением сопротивления грунта возрастает коррозия металла. Кроме того, применение таких заземлителей не связано со значительными земляными работами, что неизбежно, например, при выполнении заземления из металлических листов или горизонтально закладываемых в землю металлических лент и проводов.

Заземлители следует соединять между собой шинами с помощью сварки. Сечение шин и магистралей заземления по условиям механической прочности и получения достаточной проводимости рекомендуется брать не менее (24 х 4) мм^2. Проводник, соединяющий заземлитель с контуром заземления, должен быть луженым для уменьшения гальванической коррозии, а соединения должны быть защищены от воздействия влаги.

Магистрали заземления вне здания необходимо прокладывать на глубине около 1,5 м, а внутри здания - по стене или специальным каналам таким образом, чтобы их можно было внешне осматривать. Соединяют магистрали с заземлителем только с помощью сварки. К заземляемому устройству ТСПИ магистраль подключают с помощью болтового соединения в одной точке.

Для уменьшения сопротивлений контактов наилучшим является постоянное непосредственное соединение металла с металлом, полученное сваркой или пайкой. При соединении под винт необходимо применять шайбы (звездочки или Гровера), обеспечивающие постоянство плотности соединения.

При соприкосновении двух металлов в присутствии влаги возникает гальваническая и (или) электрическая коррозия. Гальваническая коррозия является следствием образования гальванического элемента, в котором влага является электролитом. Степень коррозии определяется положением этих металлов в электрическом ряду. Электрическая коррозия может возникнуть при соприкосновении в электролите двух одинаковых металлов. Она определяется наличием локальных электротоков в металле, например, токов в заземлениях силовых цепей. Наиболее эффективным методом защиты от коррозии является применение металлов с малой электрохимической активностью, таких, как олово, свинец, медь. Значительно уменьшить коррозию и обеспечить хороший контакт можно, тщательно изолируя соединения от проникновения влаги.

Одним из методов локализации опасных сигналов, циркулирующих в технических средствах и системах обработки информации, является фильтрация. В источниках электромагнитных полей и наводок фильтрация осуществляется с целью предотвращения распространения нежелательных электромагнитных колебаний за пределы устройства - источника опасного сигнала. Фильтрация в устройствах - рецепторах электромагнитных полей и наводок должна исключить их воздействие на рецептор.

Для фильтрации сигналов в цепях питания ТСПИ используются *разделительные трансформаторы* и *помехоподавляющие фильтры.*

Разделительные трансформаторы должны обеспечивать развязку первичной и вторичной цепей по сигналам наводки. Это

означает, что во вторичную цепь трансформатора не должны проникать наводки, появляющиеся в цепи первичной обмотки. Проникновение наводок во вторичную обмотку объясняется наличием нежелательных резистивных и емкостных цепей связи между обмотками. Для уменьшения связи обмоток по сигналам наводок часто применяется внутренний экран, выполняемый в виде заземленной прокладки или фольги, укладываемой между первичной и вторичной обмотками. С помощью этого экрана наводка, действующая в первичной обмотке, замыкается на землю. Однако электростатическое поле вокруг экрана также может служить причиной проникновения наводок во вторичную цепь.

Разделительные трансформаторы используются с целью решения ряда задач, в том числе для:

- разделения по цепям питания источников и рецепторов наводки, если они подключаются к одним и тем же шинам переменного тока;
- устранения асимметричных наводок;
- ослабления симметричных наводок в цепи вторичной обмотки, обусловленных наличием асимметричных наводок в цепи первичной обмотки.

Средства развязки и экранирования, применяемые в разделительных трансформаторах, обеспечивают максимальное значение сопротивления между обмотками и создают для наводок путь с малым сопротивлением из первичной обмотки на землю. Это достигается обеспечением высокого сопротивления изоляции соответствующих элементов конструкции (~10^4 МОм) и незначительной емкости между обмотками. Указанные особенности трансформаторов для цепей питания обеспечивают более высокую степень подавления наводок, чем обычные трансформаторы.

Разделительный трансформатор со специальными средствами экранирования и развязки обеспечивает ослабление информационного сигнала наводки в нагрузке на 126 дБ при емкости между обмотками 0,005 пФ и на 140 дБ при емкости между обмотками 0,001 пФ.

Средства экранирования, применяемые в разделительных трансформаторах, должны не только устранять влияние асимметричных наводок на защищаемое устройство, но и не допустить на

выходе трансформатора симметричных наводок, обусловленных асимметричными наводками на его входе. Применяя в разделительных трансформаторах специальные средства экранирования, можно существенно (более чем на 40 дБ) уменьшить уровень таких наводок.

Помехоподавляющие фильтры. В настоящее время существует большое количество различных типов фильтров, обеспечивающих ослабление нежелательных сигналов в разных участках частотного диапазона. Это фильтры нижних и верхних частот, полосовые и заграждающие фильтры и т.д. Основное назначение фильтров - пропускать без значительного ослабления сигналы с частотами, лежащими в рабочей полосе частот, и подавлять (ослаблять) сигналы с частотами, лежащими за пределами этой полосы.

Для исключения просачивания информационных сигналов в цепи электропитания используются фильтры нижних частот.

Фильтр нижних частот (ФНЧ) пропускает сигналы с частотами ниже граничной частоты ($f \leq f_{гр}$) и подавляет- с частотами выше граничной частоты.

Последовательная ветвь ФНЧ должна иметь малое сопротивление для постоянного тока и нижних частот. Вместе с тем для того, чтобы высшие частоты задерживались фильтром, последовательное сопротивление должно расти с частотой. Этим требованиям удовлетворяет индуктивность L.

Параллельная ветвь ФНЧ, наоборот, должна иметь малую проводимость для низких частот с тем, чтобы токи этих частот не шунтировались параллельным плечом. Для высоких частот параллельная ветвь должна иметь большую проводимость, тогда колебания этих частот будут ею шунтироваться, и их ток на выходе фильтра будет ослабляться. Таким требованиям отвечает емкость *С.*

Более сложные многозвенные ФНЧ (Чебышева, Баттерворта, Бесселя и т.д.) конструируют на основе сочетаний различных единичных звеньев.

Количественно величина ослабления (фильтрации) нежелательных (в том числе и опасных) сигналов защитным фильтром оценивается в соответствии с выражением:

$$A = 20\lg\left(\frac{U_1}{U_2}\right) = 10\lg\left(\frac{P_1}{P_2}\right), \text{ дБ}, \qquad (6.\ 3)$$

где U_1 (P_1) - напряжение (мощность) опасного сигнала на входе фильтра;

U_2 (P_2) - напряжение (мощность) опасного сигнала на выходе фильтра при включенной нагрузке $Z_{\text{Н}}$.

Основные требования, предъявляемые к защитным фильтрам, заключаются в следующем:

- величины рабочего напряжения и тока фильтра должны соответствовать напряжению и току фильтруемой цепи;
- величина ослабления нежелательных сигналов в диапазоне рабочих частот должна быть не менее требуемой;
- ослабление полезного сигнала в полосе прозрачности фильтра должно быть незначительным;
- габариты и масса фильтров должны быть минимальными;
- фильтры должны обеспечивать функционирование при определенных условиях эксплуатации (температура, влажность, давление) и механических нагрузках (удары, вибрация и т.д.);
- конструкции фильтров должны соответствовать требованиям техники безопасности.

К фильтрам цепей питания наряду с общими предъявляются следующие дополнительные требования:

- затухание, вносимое такими фильтрами в цепи постоянного тока или переменного тока основной частоты, должно быть минимальным (например, 0,2 дБ и менее) и иметь большое значение (более 60 дБ) в полосе подавления, которая в зависимости от конкретных условий может быть достаточно широкой (до 10 ГГц);
- сетевые фильтры должны эффективно работать при сильных проходящих токах, высоких напряжениях и высоких уровнях мощности проходящих и задерживаемых электромагнитных колебаний;
- ограничения, накладываемые на допустимые уровни нелинейных искажений формы напряжения питания при максимальной нагрузке, должны быть достаточно жесткими (например, уровни гармонических составляющих напряжения питания с час-

тотами выше 10 кГц должны быть на 80 дБ ниже уровня основной гармоники).

Напряжение, приложенное к фильтру, должно быть таким, чтобы оно не вызывало пробоя конденсаторов фильтра при различных скачках питающего напряжения, включая скачки, обусловленные переходными процессами в цепях питания. Чтобы при заданных массе и объеме фильтр обеспечивал наилучшее подавление наводок в требуемом диапазоне частот, его конденсаторы должны обладать максимальной емкостью на единицу объема или массы. Кроме того, номинальное значение рабочего напряжения конденсаторов выбирают исходя из максимальных значений допускаемых скачков напряжения цепи питания.

Ток через фильтр должен быть таким, чтобы не возникало насыщения сердечников катушек фильтра. Кроме того, следует учитывать, что с увеличением тока через катушку увеличивается реактивное падение напряжения на ней. Это может привести к:

- ухудшению эквивалентного коэффициента стабилизации напряжения в цепи питания, содержащей фильтр;
- возникновению взаимозависимости переходных процессов в различных нагрузках цепи питания.

Наибольшие скачки напряжения при этом возникают во время отключения нагрузок, так как большинство из них имеет индуктивный характер.

Характеристики фильтров зависят от числа использованных реактивных элементов. Так, например, фильтр из одного параллельного конденсатора или одной последовательной индуктивной катушки может обеспечить затухание лишь 20 дБ/декада вне полосы пропускания, а LC – фильтр из десяти или более элементов – более 200 дБ/декада.

Из-за паразитной связи между входом и выходом фильтра на практике трудно получить затухание более 100 дБ. Если фильтр неэкранированный и сигнал подается на него и снимается с помощью неэкранированных соединений (проводов), то развязка между входом и выходом обычно не превышает 40 ... 60 дБ. Для обеспечения развязки более 60 дБ необходимо использовать

экранированные фильтры с разъемами и использовать для соединения экранированные провода.

Фильтры с гарантируемым затуханием 100 дБ выполняются в виде узла с электромагнитным экранированием, который помещается в корпус, изготовленный из материала с высокой магнитной проницаемостью магнитного экрана. Этим существенно уменьшается возможность возникновения внутри корпуса паразитной связи между входом и выходом фильтра из-за магнитных электрических или электромагнитных полей.

Из-за влияния паразитных емкостей и индуктивностей фильтр зачастую не обеспечивает требуемого затухания на частотах, превышающих граничную частоту (f_C) на две декады, и полностью может потерять работоспособность на частотах, превышающих граничную частоту на несколько декад.

Ориентировочные значения максимального затухания для сетевых фильтров, приведены в табл. 6.5.

Таблица 6. 5 - Значения максимального затухания для сетевых фильтров

Диапазон частот	Максимальное затухание фильтра вне полосы пропускания, дБ		
	экранированный		неэкранированный
	с разъемами	без разъемов	
Фильтры в цепях питания на токи не более 10 А			
$f_c \le f \le 10\ f_c$	80	—	—
$10\ f_c \le f \le 100\ f_c$	80	—	—
$f > 100\ f_c$	70	—	—
Фильтры в цепях питания на токи более 1 0 А			
$f_c \le f \le 10\ f_c$;	100	—	—
$10\ f_c \le f \le 100\ f_c$	100	—	—
$f > 100\ f_c$	90	—	—

Конструктивно фильтры подразделяются на:

- фильтры на элементах с сосредоточенными параметрами (*LC*-фильтры) - обычно предназначены для работы на частотах до 300 МГц;

- фильтры с распределенными параметрами (полосковые, коаксиальные или волноводные) - применяются на частотах свыше 1 ГГц;
- комбинированные - применяются на частотах 300 МГц ... 1 ГГц.

В настоящее время промышленностью выпускаются несколько серий защитных фильтров (ФП, ФБ, ФПС и др.).

Фильтры серии ФП обеспечивают затухание от 60 до 100 дБ. Они рассчитаны на номинальное напряжение переменного тока от 60 до 500 В и ток - от 2,5 до 70 А. Размеры фильтров составляют от 350•100•60 до 560•210•80 мм, а вес - от 2,5 до 25 кг.

Фильтры серии ФСПК-100 (200) предназначены для установки в четырехпроводных линиях электропитания частотой 50 Гц и напряжением 220/380 В. Максимальный рабочий ток составляет 100 (200) А. В диапазоне частот от 0,02 до 1000 МГц фильтры обеспечивают затухание сигнала не менее 60 дБ.

Конструктивно фильтры ФСПК выполнены в виде двух корпусов (полукомплектов), каждый из которых обеспечивает фильтрацию двухпроводной линии. Размеры одного корпуса составляют 800х320х92 мм, а вес - 18кг.

Реализация пассивных методов защиты, основанных на применении экранирования и фильтрации, приводит к ослаблению уровней побочных электромагнитных излучений и наводок (опасных сигналов) ТСПИ и тем самым к уменьшению отношения опасный сигнал/шум (с/ш). Однако в ряде случаев, несмотря на применение пассивных методов защиты, на границе контролируемой зоны отношение с/ш превышает допустимое значение. В этом случае применяются активные меры защиты, основанные на создании помех средствам разведки, что также приводит к уменьшению отношения с/ш.

Для исключения перехвата побочных электромагнитных излучений по электромагнитному каналу используется пространственное зашумление, а для исключения съема наводок информационных сигналов с посторонних проводников и соединительных линий ВТСС - линейное зашумление.

К системе пространственного зашумления, применяемой для создания маскирующих электромагнитных помех, предъявляются следующие требования:

- система должна создавать электромагнитные помехи в диапазоне частот возможных побочных электромагнитных излучений ТСПИ;
- создаваемые помехи не должны иметь регулярной структуры;
- уровень создаваемых помех (как по электрической, так и по магнитной составляющей поля) должен обеспечить отношение с/ш на границе контролируемой зоны меньше допустимого значения во всем диапазоне частот возможных побочных электромагнитных излучений ТСПИ;
- система должна создавать помехи как с горизонтальной, так и с вертикальной поляризацией (поэтому выбору антенн для генераторов помех уделяется особое внимание);
- на границе контролируемой зоны уровень помех, создаваемых системой пространственного зашумления, не должен превышать требуемых норм по электромагнитной совместимости (ЭМС).

Цель пространственного зашумления считается достигнутой, если отношение опасный сигнал/шум на границе контролируемой зоны не превышает некоторого допустимого значения, рассчитываемого по специальным методикам для каждой частоты информационного (опасного) побочного электромагнитного излучения ТСПИ.

В системах пространственного зашумления в основном используются помехи типа "белого шума" или "синфазные помехи".

Системы, реализующие метод "синфазной помехи", в основном применяются для защиты ПЭВМ. В них в качестве помехового сигнала используются импульсы случайной амплитуды, совпадающие (синхронизированные) по форме и времени существования с импульсами полезного сигнала. Вследствие этого по своему спектральному составу помеховый сигнал аналогичен спектру побочных электромагнитных излучений ПЭВМ. То есть, система зашумления генерирует "имитационную помеху", по спектральному составу соответствующую скрываемому сигналу.

В настоящее время в основном применяются системы пространственного зашумления, использующие помехи типа "белый шум", то есть излучающие широкополосный шумовой сигнал (как правило, с равномерно распределенным энергетическим спектром во всем рабочем диапазоне частот), существенно превышающий уровни побочных электромагнитных излучений. Такие системы применяются для защиты широкого класса технических средств: электронно-вычислительной техники, систем звукоусиления и звукового сопровождения, систем внутреннего телевидения и т.д.

Генераторы шума выполняются или в виде отдельного блока с питанием от сети 220В, или в виде отдельной платы, вставляемой (встраиваемой) в свободный слот системного блока ПЭВМ и питанием от общей шины компьютера.

Диапазон рабочих частот генераторов шума от 0,01 ... 0,1 до 1000 МГц. При мощности излучения около 20 Вт обеспечивается спектральная плотность помехи 40 ... 80 дБ.

В системах пространственного зашумления в основном используются слабонаправленные рамочные жесткие и гибкие антенны. Рамочные гибкие антенны выполняются из обычного провода и разворачиваются в двух-трех плоскостях, что обеспечивает формирование помехового сигнала как с вертикальной, так и с горизонтальной поляризацией во всех плоскостях.

При использовании систем пространственного зашумления необходимо помнить, что наряду с помехами средствам разведки создаются помехи и другим радиоэлектронным средствам (например, системам телевидения, радиосвязи и т.д.). Поэтому при вводе в эксплуатацию системы пространственного зашумления необходимо проводить специальные исследования по требованиям обеспечения электромагнитной совместимости (ЭМС). Кроме того, уровни помех, создаваемые системой зашумления, должны соответствовать санитарно-гигиеническим нормам. Однако нормы на уровни электромагнитных излучений по требованиям ЭМС существенно строже санитарно-гигиенических норм. Следовательно, основное внимание необходимо уделять выполнению норм ЭМС.

Пространственное зашумление эффективно не только для закрытия электромагнитного, но и электрического каналов утеч-

ки информации, так как помеховый сигнал при излучении наводится в соединительных линиях ВТСС и посторонних проводниках, выходящих за пределы контролируемой зоны.

Системы линейного зашумления применяются для маскировки наведенных опасных сигналов в посторонних проводниках и соединительных линиях ВТСС, выходящих за пределы контролируемой зоны. Они используются в том случае, если не обеспечивается требуемый разнос этих проводников и ТСПИ (то есть не выполняется требование по Зоне № 1), однако при этом обеспечивается требование по Зоне № 2 (то есть расстояние от ТСПИ до границы контролируемой зоны больше, чем Зона № 2).

В простейшем случае система линейного зашумления представляет собой генератор шумового сигнала, формирующий шумовое маскирующее напряжение с заданными спектральными, временными и энергетическими характеристиками, который гальванически подключается в зашумляемую линию (посторонний проводник).

На практике наиболее часто подобные системы используются для зашумления линий электропитания (например, линий электропитания осветительной и розеточной сетей).

6.3. Программно-аппаратные средства защиты информации и информационных процессов

6.3.1. Основы построения программно-аппаратных средств защиты

Пополнение парка ПЭВМ и развитие объектов связи и информатизации в течение последних лет позволяют отметить неуклонный рост их количества, зависимость экономики от внедренных систем и сетей, страны, изменения методологии их защиты.

В данной сфере наблюдаются следующие тенденции:

1. расширение функциональных возможностей и удешевление стоимости ПЭВМ;

2. специализация стационарных ПЭВМ в направлениях:

- домашнего и офисного применения;

- функционирования в качестве рабочих станций объектов связи и информатизации;
- функционирования в качестве серверов в производственных, транспортных, оборонных системах, в системах связи и т.п.;
- функционирования в качестве суперкомпьютеров;

3. повышение спроса на ПЭВМ со средствами защиты от несанкционированного доступа (НСД) к информации и средствами защиты от утечки информации по каналам побочных электромагнитных излучений и наводок;

4. интеграция ПЭВМ со средствами связи;

5. совершенствование показателей и характеристик как ПЭВМ, так и программных средств для них.

Основные требования к техническим и программным средствам (ТС и ПС) объектов связи и информатизации изложены в ряде нормативных документов, в том числе:

- ГОСТ 15.311-90 СРПП. Постановка на производство продукции по технической документации иностранных фирм;
- ГОСТ 21552-84. Средства вычислительной техники (СВТ). ОТТ, приемка, методы испытаний, маркировка, упаковка, транспортировка и хранение;
- ГОСТ 27201-87. Машины вычислительные электронные персональные. Типы, основные параметры, ОТТ;
- ИСО/МЭК 60050-191. Международный электротехнический словарь. Глава 191. Надежность и качество услуг;
- ГОСТ Р 51624-2000. Защита информации. Автоматизированная система в защищенном исполнении. Общие требования и др.

Разработке и производству современных средств защиты от несанкционированного доступа к информации предшествовало выполнение научно-исследовательских работ в этой области. Большинство разработчиков на первоначальном этапе были сосредоточены на создании только программного обеспечения, реализующего функции защиты в автоматизированных системах, что не может гарантировать надежной защищённости автоматизированных систем от НСД к информации.

Методология применения аппаратной защиты, признанная необходимой основой построения систем защиты от НСД к информации. Основные идеи этого подхода состоят в следующем:

- комплексный подход к решению вопросов защиты информации в автоматизированных системах (АС) от НСД;
- признание мультипликативной парадигмы защиты, и, как следствие, равное внимание надежности реализации контрольных процедур на всех этапах работы АС;
- "материалистическое" решение "основного вопроса" информационной безопасности: "что первично - *hard* или *soft*?";
- последовательный отказ от программных методов контроля как очевидно ненадежных и перенос наиболее критичных контрольных процедур на аппаратный уровень;
- максимально возможное разделение условно-постоянных и условно-переменных элементов контрольных операций;
- построение средств защиты информации от несанкционированного доступа (СЗИ НСД), максимально независимых от операционных и файловых систем, применяемых в АС. Это выполнение процедур идентификации/аутентификации, контроля целостности аппаратных и программных средств АС до загрузки операционной системы, администрирования и т.д.

Основным объектом программно-аппаратной защиты информационных процессов и информации является персональный компьютер, локальная и корпоративная вычислительная сеть предприятия, организации и фирмы. Угрозы могут исходить от законного пользователя (сотрудника организации фирмы) и нарушителя, находящего за пределами организации. На рабочем месте

6.3.2. Технические средства программно-аппаратной защиты информационных процессов

Одной из ведущих фирм на отечественном рынке является Особое конструкторское бюро систем автоматизированного проектирования (ОКБ САПР, г. Москва). Основой построения систем защиты от НСД ОКБ САПР является программно-аппаратный модуль доверенной загрузки (АМДЗ) - "Аккорд - АМДЗ". Этот модуль обеспечивает режим доверенной загрузки в

различных операционных средах: MS DOS; Windows 3.x; Windows 9.x; Windows NT; Windows 2000; Windows XP; OS/2; Unix; Linux. Основным принципом работы "Аккорд - АМДЗ" является выполнение процедур, реализующих основные функции системы защиты информации до загрузки операционной системы. Процедуры идентификации/аутентификации пользователя, контроля целостности аппаратных и программных средств, администрирование, блокировка загрузки операционной системы с внешних носителей информации размещены во внутренней памяти микроконтроллера платы "Аккорд". Таким образом, пользователь не имеет возможности изменения процедур, которые влияют на функциональность системы защиты информации. В энергонезависимой памяти контроллера "Аккорд" хранится информация о персональных данных пользователей, данные для контроля целостности программных и аппаратных средств, журнал регистрации и учета системных событий и действий пользователя. Эти данные могут быть изменены только авторизованным администратором безопасности информации, так как доступ к энергонезависимой памяти полностью определяется логикой работы программного обеспечения, размещенного в микроконтроллере платы.

Рис. 6. 6. Контроллер "Аккорд - 4.5"

Средства защиты информации от НСД семейства "Аккорд" реализованы на базе контроллера "Аккорд-4.5" (для ПЭВМ с шинным интерфейсом ISA) и его функционального аналога для шинного интерфейса PC1 -"Аккорд-5". PCI-устройства ОКБ САПР являются легальными и имеют свой идентификатор, пре-

доставленный ассоциацией разработчиков данных устройств (Vendor ID - 1795).

Рис. 6. 7. Контроллер "Аккорд - 5"

Для организаций, использующих промышленные PC компьютеры с шинным интерфейсом PC/104 рекомендуется программно-аппаратный комплекс "Аккорд-PC104". Он может применяться в специализированных компьютерах, используемых в бортовой аппаратуре (наземные, воздушные, морские и промышленные системы), в измерительной аппаратуре, в устройствах связи, в мобильных системах, в том числе и военного назначения.

Рис. 6. 8. Контроллер "Аккорд-PC104"

Наиболее наукоёмкой разработкой ОКБ САПР является сопроцессор безопасности "Аккорд-СБ", в котором интегрированы все необходимые средства для реализации комплексной защиты информации от НСД. Контроллер сопроцессора безопасности

"Аккорд-СБ/2" имеет высокопроизводительный микропроцессор и аппаратный ускоритель математических функций. Доступ к функциям этого процессора определяется встроенным программным обеспечением контроллера.

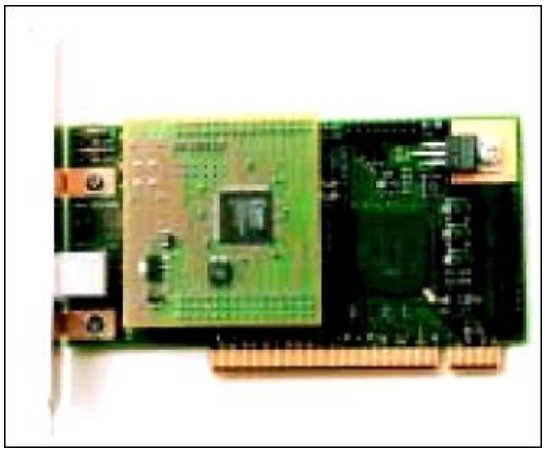


Рис. 6. 9. Сопроцессор безопасности "Аккорд - СБ/2"

Используя библиотеку программирования контроллера сопроцессора безопасности "Аккорд - СБ/2" (SDK), разработчик может применять данный комплекс как многофункциональное устройство. В частности, кроме задач по защите информации от несанкционированного доступа, он может быть использован для передачи конфиденциальной информации по открытым каналам связи в зашифрованном виде с высокой скоростью обработки и передачи данных, шифрования дисков, формирования и проверки ЭЦП, защиты электронных документов с использованием защитных кодов аутентификации (ЗКА), а также в качестве межсетевого экрана.

Требования к аппаратным СЗИ и принципы аппаратной защиты, реализованные в СЗИ НСД семейства "Аккорд", уже стали фактическим стандартом и применяются всеми крупными разработчиками средств защиты, действующими на российском рынке СЗИ. Применение сильной аппаратной поддержки в комплексах СЗИ НСД семейства "Аккорд" позволило выйти на новый уровень в развитии средств защиты информации. Как известно для построения автоматизированных систем по классам защищённости требуется установка правил разграничения доступа к ее информационным ресурсам. Для реализации функций разграниче-

ния доступа пользователей к информационным ресурсам и создания изолированной программной среды (ИПС) программистами разработано специальное программное обеспечение, поддерживающее все типы контроллеров "Аккорд", включая работу с датчиком случайных чисел. Это такие комплексы СЗИ НСД, как "Аккорд-1.95" (MS DOS, Windows 9x), "Аккорд-1.95-00" (Windows 9x), "Аккорд-NT/2000" (Windows NT/2000/XP).

Особенностью комплексов "Аккорд-1.95-00" и "Аккорд NT/2000" является то, что в данных версиях, кроме дискреционного, реализован мандатный принцип доступа субъектов к информационным ресурсам. Специальное программное обеспечение, реализующее функции разграничения доступа, позволяет администратору безопасности информации описать любую не противоречивую политику безопасности на основе наиболее полного набора атрибутов (более 15 атрибутов по доступу к файлам и каталогам) и меток конфиденциальности объектов (файлов) и процессов (программ), с помощью которых осуществляется их обработка.

Следующим этапом стала разработка основ защиты локальных вычислительных сетей с применением программно-аппаратных средств защиты от НСД к информации. Для полноценной защиты локальной вычислительной сети предлагается комплексная технология:

- установку на рабочих станциях СЗИ "Аккорд АМДЗ" с ПО "Аккорд-1.95", "Аккорд-1.95-00", "Аккорд-NT/2000";
- установку подсистемы контроля целостности на каждом файл-сервере;
- установку подсистемы распределенного аудита и управления;
- установку подсистемы усиленной аутентификации.

Управление вышеперечисленными подсистемами в локальных вычислительных сетях обеспечивается с помощью автоматизированного рабочего места администратора безопасности (АРМ АБИ). Данная технология позволяет администратору безопасности информации однозначно опознавать авторизованных пользователей и зарегистрированные рабочие станции в сети; в режиме

реального времени контролировать задачи, выполняемые пользователями; в случае несанкционированных действий блокировать рабочие станции, с которых такие действия осуществлялись; удаленно вести администрирование. Особый интерес представляет подсистема усиленной аутентификации, суть которой заключается в дополнительном механизме проверки подлинности рабочих станций. Процедура проверки подлинности выполняется не только в момент подключения станции, но и с установленной администратором периодичностью. Подсистема предотвращает как подмену локальной станции или сервера, так и подключение в ЛВС нелегальных станций/серверов. Усиленная аутентификация в ЛВС основана на применении математических методов, позволяющих однозначно опознать участников диалога.

Как известно, невозможно решить все вопросы обработки информации в АС только средствами защиты от НСД к защищаемой информации. Поэтому необходимо также обеспечить юридическую доказательность подлинности электронных документов. Специалистами ОКБ САПР предложен и реализован новый путь - разработка контролируемой технологии обработки вычислительных системах - технология защиты электронных документов с использованием защитных кодов аутентификации (ЗКА). Данная технология уже используется в банковских платежных системах с целью предотвращения попыток злоумышленников ввести фиктивные или модифицировать обрабатываемые электронные банковские документы, а также с целью организации сквозного контроля при прохождении электронных документов всех предписанных этапов их существования (создание, обработка, передача, хранение, окончательный зачет). Это обеспечивается установкой на документ ЗКА. В результате электронный документ на каждом этапе обработки имеет два ЗКА, первый из которых позволяет авторизовать и проконтролировать его целостность на предыдущем этапе обработки, а второй – является его индивидуальным признаком на текущем.

Технологическая защита электронного документооборота реализуется всеми типами контроллеров семейства "Аккорд". Кроме того, для реализации данной технологии при использовании других СЗИ НСД в ОКБ САПР разработаны эффективные устройства: блок установки кодов аутентификации (БУКА); из-

делие "ШИПКА" (Шифрование Аутентификация Подпись Коды Аутентификации). "ШИПКА" содержит микропроцессор с встроенным программным обеспечением, аппаратный датчик случайных чисел и подключается через имеющийся интерфейс - шину USB и может выполнять операции: шифрование по ГОСТ 28147-89; хеширование по ГОСТ Р 34.11-94; формирование и проверка электронной цифровой подписи по ГОСТ Р 34.10-94; выработка и проверка защитных кодов аутентификации. В последней модификации изделия имеется защищенный электронный диск объемом 16 Мб, 32 Мб, 64 Мб или 128 Мб для записи пользовательской информации.

Рис. 6. 10. Изделие "ШИПКА"

Любая система защиты информации - это комплекс организационно-технических мероприятий, который включает в себя совокупность правовых норм, организационных мер и программно-технических средств защиты, направленных на противодействие угрозам объекту информатизации с целью сведения до минимума возможного ущерба пользователям и владельцам системы. Без организационных мер, наличия четкой организационно-распорядительной системы на объекте информатизации эффективность любых технических СЗИ снижается. Поэтому большое внимание уделяет вопросам разработки нормативно-технической и методической документации, комплектов организационно-распорядительных документов по политике защиты объектов информатизации в соответствии с действующим законодательством РФ.

ЛИТЕРАТУРА

1. Крылов В.В. Информационные компьютерные преступления. – М.: Издательская группа ИНФРА • М – НОРМА, 1997. – 285 с.

2. Мельников В.В. Защита информации в компьютерных системах. – М.: Финансы и статистика; Электроинформ., 1997. – 368 с.

3. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. Под ред. В.Ф. Шаньгина. – М.: Радио и связь, 1999. – 328 с.

4. Бацула А.П. Подавление ПЭМИН дисплея ПЭВМ. Материалы. Первой межрегиональной научно-практической конференции «Проблемы информационной безопасности общества и личности», г. Томск, 24-26 мая 2000 г. – Томск 2001. – 140 с.

5. http://www.razvedka.ru/katalog/?kat=1

6. Пушкарев В.В., Пушкарев В.П. Защита информации в компьютерных системах и сетях. Материалы 4-й Всероссийской научно-практической конференции «Проблемы информационной безопасности общества и личности». – Томск, 2002, -С. 79 – 91.

7. Конявский В.А. Техническая защита электронных документов в компьютерных системах» http://www.accord.ru/index.shtml.

8. Конявский В.А. Управление защитой информации на базе СЗИ НСД "Аккорд". - М.: "Радио и связь", 1999. - 325 с.

9. Гадасин В.А., Конявский В.А. От документа - к электронному документу. Системные основы. - М.: "РФК-Имидж Лаб", 2001- 192с.