# Требования к системам защиты информации


### *В этой главе*

- *Общие требования*
- *Организационные требования*
- *Требования к подсистемам защиты информации*
- *Требования к техническому обеспечению*
- *Требования к программному обеспечению*
- *Требования по применению способов, методов и средств защиты*
- *Требования к документированию*
- *Технические требования по защите информации от утечки по каналам ПЭМИН*

| <<< Этапы | Направления >>> | 010 | | | | 020 | | | | 030 | | | | 040 | | | | 050 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Защита объектов ИС | | | | Защита процессов и программ | | | | Защита каналов связи | | | | ПЭМИН | | | | Управление системой защиты | | | |
| | Основы >>> | База | Структура | Меры | Средства | База | Структура | Меры | Средства | База | Структура | Меры | Средства | База | Структура | Меры | Средства | База | Структура | Меры | Средства |
| | | 011 | 012 | 013 | 014 | 021 | 022 | 023 | 024 | 031 | 032 | 033 | 034 | 041 | 042 | 043 | 044 | 051 | 052 | 053 | 054 |
| 100 | Определение информации, подлежащей защите | 111 | 112 | 113 | 114 | 121 | 122 | 123 | 124 | 131 | 132 | 133 | 134 | 141 | 142 | 143 | 144 | 151 | 152 | 153 | 154 |
| 200 | Выявление угроз и каналов утечки информации | 211 | 212 | 213 | 214 | 221 | 222 | 223 | 224 | 231 | 232 | 233 | 234 | 241 | 242 | 243 | 244 | 251 | 252 | 253 | 254 |
| 300 | Проведение оценки уязвимости и рисков | 311 | 312 | 313 | 314 | 321 | 322 | 323 | 324 | 331 | 332 | 333 | 334 | 341 | 342 | 343 | 344 | 351 | 352 | 353 | 354 |
| 400 | Определение требований к СЗИ | 411 | 412 | 413 | 414 | 421 | 422 | 423 | 424 | 431 | 432 | 433 | 434 | 441 | 442 | 443 | 444 | 451 | 452 | 453 | 454 |
| 500 | Осуществление выбора средств защиты | 511 | 512 | 513 | 514 | 521 | 522 | 523 | 524 | 531 | 532 | 533 | 534 | 541 | 542 | 543 | 544 | 551 | 552 | 553 | 554 |
| 600 | Внедрение и использование выбранных мер и средств | 611 | 612 | 613 | 614 | 621 | 622 | 623 | 624 | 631 | 632 | 633 | 634 | 641 | 642 | 643 | 644 | 651 | 652 | 653 | 654 |
| 700 | Контроль целостности и управление защитой | 711 | 712 | 713 | 714 | 721 | 722 | 723 | 724 | 731 | 732 | 733 | 734 | 741 | 742 | 743 | 744 | 751 | 752 | 753 | 754 |

Требования по защите информации определяются владельцем ИС и согласовываются с исполнителем работ по созданию системы защиты информации (исполнитель должен иметь соответствующую лицензию на право проведения таких работ).

***В процессе формирования требований к СЗИ целесообразно найти ответы на следующие вопросы.***

1. Какие меры безопасности предполагается использовать?
2. Какова стоимость доступных программных и технических мер защиты?
3. Насколько эффективны доступные меры защиты?
4. Насколько уязвимы подсистемы СЗИ?
5. Имеется ли возможность провести анализ риска (прогнозирование возможных последствий, которые могут вызвать выявленные угрозы и каналы утечки информации)?

Совокупность требований к системам защиты информации представлена на рисунке 20.1.

***В общем случае целесообразно выделить следующие группы требований к системам защиты информации***

- общие требования
- организационные требования
- конкретные требования к подсистемам защиты, техническому и программному обеспечению, документированию, способам, методам и средствам защиты.

Рассмотрим указанные группы требований более подробно.

## Общие требования (400)

Прежде всего необходима полная идентификация пользователей, терминалов, программ, а также основных процессов и процедур, желательно до уровня записи или элемента. Кроме того ***следует ограничить доступ к информации, используя совокупность следующих способов:***

- иерархическая классификация доступа,
- классификация информации по важности и месту ее возникновения,
- указание ограничений к информационным объектам, например пользователь может осуществлять только чтение файла без права записи в него,
- определение программ и процедур, предоставленных только конкретным пользователям.

Система защиты должна гарантировать, что любое движение данных идентифицируется, авторизуется, обнаруживается и документируется.

Обычно ***формулируются общие требования к следующим характеристикам:***

- способам построения СЗИ либо ее отдельных компонент (к программному, программно-аппаратному, аппаратному);
- архитектуре СВТ и ИС (к классу и минимальной конфигурации ЭВМ, операционной среде, ориентации на ту или иную программную и аппаратную платформы, архитектуре интерфейса);
- применению стратегии защиты;
- затратам ресурсов на обеспечение СЗИ (к объемам дисковой памяти для программной версии и оперативной памяти для ее резидентной части, затратам производительности вычислительной системы на решение задач защиты);
- надежности функционирования СЗИ (к количественным значениям показателей надежности во всех режимах функционирования ИС и при воздействии внешних разрушающих факторов, к критериям отказов);
- количеству степеней секретности информации, поддерживаемых СЗИ;
- обеспечению скорости обмена информацией в ИС, в том числе с учетом используемых криптографических преобразований;
- количеству поддерживаемых СЗИ уровней полномочий;
- возможности СЗИ обслуживать определенное количество пользователей;
- продолжительности процедуры генерации программной версии СЗИ;
- продолжительности процедуры подготовки СЗИ к работе после подачи питания на компоненты ИС;
- возможности СЗИ реагировать на попытки несанкционированного доступа, либо на “опасные ситуации”;
- наличию и обеспечению автоматизированного рабочего места администратора защиты информации в ИС;
- составу используемого программного и лингвистического обеспечения, к его совместимости с другими программными платформами, к возможности модификации и т.п.;
- используемым закупаемым компонентам СЗИ (наличие лицензии, сертификата и т.п.).

## Организационные требования (400)

Организационные требования к системе защиты предусматривают реализацию совокупности административных и процедурных мероприятий.

Требования по обеспечению сохранности должны выполняться прежде всего на административном уровне. ***Организационные мероприятия, проводимые с целью повышения эффективности защиты информации, должны предусматривать следующие процедуры:***

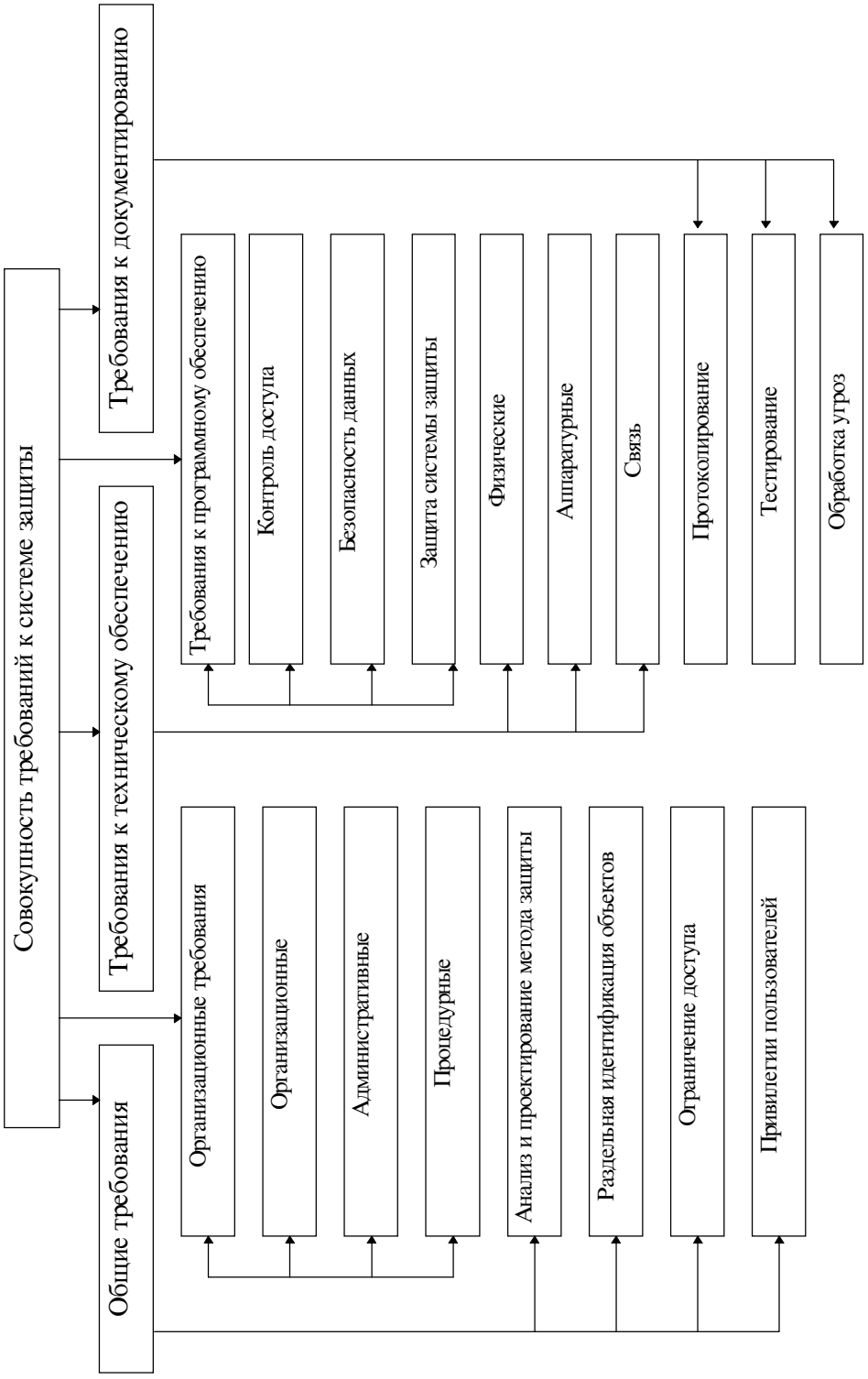



**РИСУНОК 20.1.** *Совокупность требований к СЗИ.*

- ограничение несопровождаемого доступа к вычислительной системе (регистрация и сопровождение посетителей);
- осуществление контроля за изменением в системе программного обеспечения;
- выполнение тестирования и верификации изменений в системе программного обеспечения и программах защиты;
- организацию и поддержку взаимного контроля за выполнением правил защиты данных;
- ограничение привилегии персонала, обслуживающего ИС;
- осуществление записи протокола о доступе к системе;
- гарантию компетентности обслуживающего персонала;
- разработку последовательного подхода к обеспечению сохранности информации для всей организации;
- организацию четкой работы службы ленточной и дисковой библиотек;
- комплектование основного персонала на базе интегральных оценок и твердых знаний;
- организацию системы обучения и повышения квалификации обслуживающего персонала.

С точки зрения обеспечения доступа к ИС необходимо выполнить следующие процедурные мероприятия:

- разработать и утвердить письменные инструкции на загрузку и остановку работы операционной системы;
- контролировать использование магнитных лент, дисков, карт, листингов, порядок изменения программного обеспечения и доведение этих изменений до пользователя;
- разработать процедуру восстановления системы при отказах;
- установить политику ограничений при разрешенных визитах в вычислительный центр и определить объем выдаваемой информации;
- разработать систему протоколирования использования ЭВМ, ввода данных и вывода результатов;
- обеспечить проведение периодической чистки архивов и хранилищ носителей информации для исключения и ликвидации неиспользуемых;
- ◆ поддерживать документацию вычислительного центра в соответствии с установленными стандартами.

## Требования к подсистемам защиты информации (400)

В общем случае СЗИ целесообразно условно разделить на подсистемы:

- управления доступом к ресурсам ИС (включает также функции управления системой защиты в целом);
- регистрации и учета действий пользователей (процессов);
- криптографическую;
- обеспечения целостности информационных ресурсов и конфигурации ИС.

***Для каждой из них определяются требования в виде:***

- перечня обеспечиваемых подсистемой функций защиты;
- основных характеристик этих функций;
- перечня средств, реализующих эти функции.

**Подсистема управления доступом** должна обеспечивать:

- идентификацию, аутентификацию и контроль за доступом пользователей (процессов) к системе, терминалам, узлам сети, каналам связи, внешним устройствам, программам, каталогам, файлам, записям и т.д.;
- управление потоками информации;
- очистку освобождаемых областей оперативной памяти и внешних накопителей.

**Подсистема регистрации и учета** выполняет:

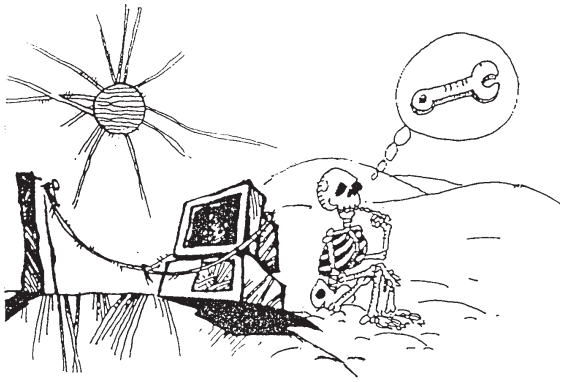
- регистрацию и учет: доступа в ИС, выдачи выходных документов, запуска программ и процессов, доступа к защищаемым файлам; передачу данных по линиям и каналам связи;
- регистрацию изменения полномочий доступа, создание объектов доступа, подлежащих защите;
- учет носителей информации;
- оповещение о попытках нарушения защиты.

**Криптографическая подсистема** предусматривает:

- шифрование конфиденциальной информации.
- шифрование информации, принадлежащей разным субъектам доступа (группам субъектов), с использованием разных ключей.
- использование аттестованных (сертифицированных) криптографических средств.

**Подсистема обеспечения целостности** осуществляет:

- обеспечение целостности программных средств и обрабатываемой информации,
- физическую охрану средств вычислительной техники и носителей информации,
- наличие администратора (службы) защиты информации в ИС,
- периодическое тестирование СЗИ,
- наличие средств восстановления СЗИ,



*Криптографическая подсистема предусматривает использование ключей...*

- использование сертифицированных средств защиты,
- контроль за целостностью:
  - программных средств защиты информации при загрузке операционной среды,
  - операционной среды перед выполнением процессов,
  - функционального ПО и данных,
  - конфигурации ИС,
- оперативное восстановление функций СЗИ после сбоев,
- тестирование средств защиты информации,
- обнаружение и блокирование распространения вирусов,
- резервное копирование программного обеспечения и данных,
- контроль доступа к СВТ, дающий уверенность в том, что только авторизованный пользователь использует имеющиеся рабочие программы и информацию,
- контроль действий с персональной авторизацией, запрещающий операции, которые делают операционную среду уязвимой,
- защиту программного обеспечения, исключающую повреждение инсталлированных программ,
- использование только лицензионного программного продукта с целью обеспечения защиты от встроенных модулей разрушения информационной среды и дискредитации систем защиты;
- защиту коммуникаций для обеспечения недоступности передаваемой информации.

## Требования к техническому обеспечению (410)

В этой группе формулируются требования к таким параметрам:

- месту применения средств защиты;
- способам их использования (например, реализация требований по защищенности должна достигаться без применения экранирования помещений, активные средства могут применяться только для защиты информации главного сервера и т.п.);
- размерам контролируемой зоны безопасности информации;
- требуемой величине показателей защищенности, учитывающей реальную обстановку на объектах ИС;
- применению способов, методов и средств достижения необходимых показателей защищенности.
- проведению специсследования оборудования и технических средств, целью которого является измерение показателей ЭМИ;
- проведению спецпроверки технических объектов ИС, целью которой является выявление специальных электронных (закладных) устройств.

## Требования к программному обеспечению (420)

Программные средства защиты информации должны обеспечивать контроль доступа, безопасность и целостность данных и защиту самой системы защиты. Для этого ***необходимо выполнить следующие условия:***

- объекты защиты должны идентифицироваться в явном виде при использовании паролей, пропусков и идентификации по голосу;
- система контроля доступа должна быть достаточно гибкой для обеспечения многообразных ограничений и различных наборов объектов;
- каждый доступ к файлу данных или устройству должен прослеживаться через систему контроля доступа для того, чтобы фиксировать и документировать любое обращение.

***Безопасность данных может обеспечиваться следующей системой мероприятий:***

- объекты данных идентифицируются и снабжаются информацией службы безопасности. Целесообразно эту информацию размещать не в отдельном каталоге, а вместе с информацией, имеющей метки;
- кодовые слова защиты размещаются внутри файлов, что в значительной мере повышает эффективность защиты;

- доступ к данным целесообразен с помощью косвенных ссылок, например списка пользователей, допущенных владельцем файла к размещенным в нем данным;
- данные и программы могут преобразовываться (кодироваться) внутренним способом для хранения.

Система защиты информации должна быть защищена от воздействия окружающей среды. С этой целью выполняется следующая совокупность мероприятий:

- информация по отрицательным запросам не выдается;
- повторные попытки доступа после неудачных обращений должны иметь предел;
- при уменьшении конфигурации системы или при ее тестировании функции защиты сохраняются;
- никакие изменения таблиц безопасности, кроме изменения со специального устройства или пульта управления, не разрешаются.

## Требования по применению способов, методов и средств защиты (400)

Рекомендуется применение следующих способов, методов и средств, которые предполагают использование:

- интерфейсов с передачей сигналов в виде последовательного кода и в режиме многократных повторений;
- мультиплексных режимов обработки информации, а также СВТ и системного обеспечения, базирующихся на многоразрядных платформах, интерфейсов с передачей сигналов в виде многоразрядного параллельного кода;
- рациональных способов монтажа, при которых обеспечивается минимальная протяженность электрических связей и коммуникаций;
- технических средств, в состав которых входят устойчивые к самовозбуждению схемы, развязывающие и фильтрующие элементы, комплектующие с низкими уровнями ЭМИ;
- сетевых фильтров для блокирования утечки информации по цепям электропитания, а также линейных (высокочастотных) фильтров для блокирования утечки информации по линиям связи;
- технических средств в защищенном исполнении;
- средств пространственного и линейного “зашумления”;
- средств локального либо общего экранирования;
- способов оптимального размещения технических средств с целью минимизации контролируемой зоны безопасности информации.

## Требования к документированию (400)

Можно выделить три группы требований к документированию системы защиты информации. Это протоколирование, тестирование программ и обработка угроз.

При разработке системы **протоколирования** следует учитывать следующие специфические требования:

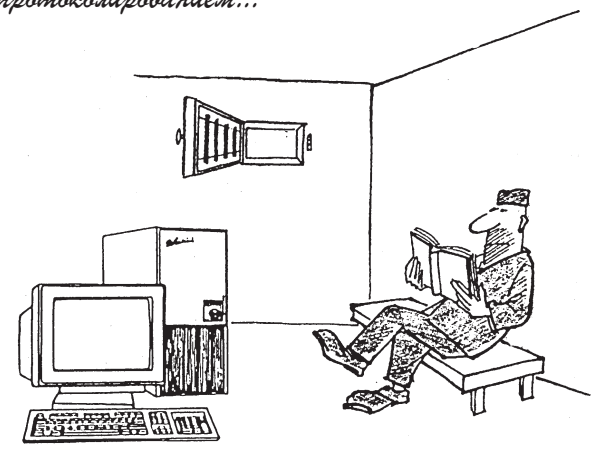
- необходимость записей всех движений защищаемых данных;
- возможность воссоздания при необходимости ретроспективы использования защищаемого объекта, для реализации которой обеспечивается запоминание состояний программы и окружающей среды;
- накопление статистики по протоколам использования информации в системе.

Существенной особенностью **тестирования программ** системы защиты информации должно быть наличие специальной программы генерации ложных адресов, несанкционированных попыток доступа к данным, моделирования сбойных ситуаций и других специфических свойств. При тестировании системы защиты информации необходимо также обратить внимание на тщательную проверку таблиц безопасности, системы паролей и программ доступа.

***Система защиты информации должна иметь специальное программное обеспечение обработки угроз, включающее:***

- регистрацию событий в системном журнале, защищенном от попыток изменения со стороны программ пользователей;

*Администратору следует знать разницу между документированием и протоколированием...*



- использование собранных сведений для анализа качественного решения проблемы защиты информации и разработки мероприятий по ее совершенствованию.

Перечисленные требования и мероприятия по обеспечению сохранности информации показывают, что она связана с решением серьезных математических и технических проблем.

Задача защиты информации в ИС обычно сводится к выбору средств контроля за выполнением программ, имеющих доступ к информации, хранящейся в системе.

## Требования к составу проектной и эксплуатационной документации (400)

В состав разрабатываемой документации входят:

- проектная документация разработчика системы (подсистемы, компонента) защиты информации;
- руководство пользователя;
- руководство администратора защиты информации;
- руководство по тестированию системы защиты информации.

### Проектная документация

Проектная документация разработчика системы (подсистемы, компонента) защиты информации состоит из описания:

- системы защиты информации;
- концепции защиты;
- модели защиты (формальной или неформальной);
- интерфейса СЗИ и пользователя, а также интерфейсов между отдельными модулями СЗИ;
- применяемых средств защиты;
- результатов анализа и идентификации скрытых каналов передачи информации;
- таблицы соответствия формальных спецификаций и объектных кодов версий программных компонент СЗИ.

### Руководство пользователя (400)

Руководство пользователя должно содержать краткое описание механизмов защиты и инструкции по работе с ними в процессе взаимодействия пользователя и ИС.

### Руководство администратора защиты информации (400)

Руководство администратора защиты информации применяется при выполнении функциональных обязанностей им или сотрудниками службы защиты информации в ИС и должно состоять из таких документов:

- описания контролируемых функций СЗИ;
- инструкции по управлению защитой, управлению и контролю за привилегированными процессами при функционировании ИС;
- описания процедур работы со средствами регистрации;
- инструкции по расшифровке диагностических сообщений и анализу аудиторских файлов;
- инструкции по сопровождению копий программного обеспечения (ПО) СЗИ, проверке их работоспособности и тестированию;
- инструкции по генерации новой версии после модификации;
- описания процедуры старта;
- описания процедур верификации защищенности после старта (сбоев);
- описания процедур оперативного восстановления работоспособности СЗИ.

### Руководство по тестированию системы защиты информации (400)

Руководство по тестированию системы защиты информации должно включать документацию разработчика для оценивания защищенности, содержащую полное описание порядка тестирования и тестовых процедур механизмов системы защиты, а также результатов функционального тестирования уровня защищенности информации.

## Перечень основных функциональных задач, которые должна решать СЗИ (400)

На основе анализа рассмотренных требований формулируются основные функциональные задачи, которые должна решать СЗИ, например:

- предоставление пользователям права доступа к ресурсам ИС, согласно принятой стратегии безопасности, а также отмена этого права по окончании срока действия;
- обеспечение входа в ИС при условии предъявления электронного идентификатора и ввода личного пароля;
- многоуровневое разграничение полномочий пользователей по отношению к ресурсам ИС;
- контроль за запуском процессов и их исполнением;
- контроль за логическим входом пользователей в ИС и доступом к ресурсам;
- управление информационными потоками, автоматическое маркирование ресурсов, создаваемых объектов, экспорта (импорта) информации;

- защита информации при ее передаче по каналам связи;
- регистрация действий пользователей по отношению к ресурсам системы;
- обеспечение целостности информационных ресурсов (в том числе обеспечение антивирусной защиты);
- криптографическая защита ресурсов (шифрование в каналах связи, “прозрачное” шифрование, электронная подпись, криптографическая поддержка других механизмов защиты и т.п.);
- поддержка целостности и работоспособности СЗИ;
- поддержка функций администратора защиты информации в ИС.

## Технические требования по защите информации от утечки по каналам ПЭМИН (440)

Объекты защищенных ИС категорируются по степени секретности обрабатываемой (циркулирующей в устройствах ИС) информации и по условиям расположения объекта.

По объему решаемых задач все объекты делятся на специализированные и универсальные.

Объекты ИС, предназначенные для решения одной или нескольких сходных задач обработки информации, относятся к специализированным объектам (СО), а объекты ИС, предназначенные для решения широкого круга задач обработки информации — к универсальным объектам.

*Определение*

Защита от перехвата секретной информации в непосредственной близости от объекта ИС обеспечивается соблюдением контролируемой зоны вокруг него.

***Оценка эффективности мер защиты на этапах проектирования, разработки и эксплуатации объектов ИС по каналам, обусловленным:***

- электромагнитными полями в диапазоне частот обрабатываемого сигнала;
- наводками опасных сигналов на цепи питания, линии связи и другие токопроводящие коммуникации, уходящие за границу контролируемой зоны;
- излучениями электромагнитных полей высокочастотных гармонических составляющих обрабатываемого сигнала;
- излучениями электромагнитных полей автогенераторов, входящих в состав технических средств (ТС) производится в соответствии со специальными требованиями и рекомендациями по обеспечению защиты от утечки речевой информации посредством побочных электромагнитных излучений и наводок”.

Комплексы и объекты ИС необходимо комплектовать ТС, прошедшими специальные исследования.

Размещение и монтаж оборудования ТС необходимо осуществлять с учетом специальных требований на конкретную систему (комплекс), в которых допускаются ссылки на конструкторские или другие технические документы, прилагаемые к данному техническому средству, а также на действующие стандарты, типовые инструкции и нормативно-методические документы.

Конструкция и алгоритм работы элементов управления системой (комплексом) в различных режимах работы аппаратуры должны затруднять (исключать) возможность ошибочных действий обслуживающего персонала, приводящих к утечке секретной информации.

Требования защиты должны выполняться во всех режимах работы системы, комплекса, объекта, которые могут быть установлены в соответствии с эксплуатационной документацией, при различных положениях переключателей, органов настройки и регулировки аппаратуры, а также при неисправностях технических средств.

### Требования по защите от перехвата ПЭМИН (440)

При выборе мест для размещения объектов ИС необходимо строго соблюдать требования по обеспечению размеров контролируемой зоны R. Конкретный состав ТС определяется заказчиком совместно с главным конструктором объекта ИС.

Если на объекте невозможно обеспечить размер контролируемой зоны либо если для размещения отдельных ТС требуется контролируемая зона, большая чем R, заказчику совместно с главным конструктором необходимо проанализировать состав ТС и разделить его на 2 группы устройств, прошедших специальные исследования и удовлетворяющие реальным размерам контролируемой зоны объекта и не удовлетворяющие этим требованиям.

Для устройств второй группы в данном случае и следующем необходимо применять дополнительные меры защиты, которые определяются заказчиком совместно с главным конструктором и головной организацией по ТЗИ на основании категории и вида объекта, реального размера контролируемой зоны и состава ТС.

Если на объекте невозможно обеспечить требуемые минимальные расстояния или если для размещения отдельных ТС необходимо проанализировать состав ТС и разделить его на две группы устройств:

1) устройства, прошедшие специсследования и удовлетворяющие реальным, т.е. максимально возможным для данного объекта, расстоянием до технических средств, имеющих выход за пределы контролируемой зоны;

2) устройства, прошедшие специсследования, но не удовлетворяющие реальным расстояниям.

Рекомендуются такие ***дополнительные меры защиты ТС:***

- установка в незащищенных каналах связи, линиях, проводах и кабелях, выходящих за пределы контролируемой зоны, соответствующих фильтров для защиты высокочастотных ТС;
- прокладка проводов и кабелей в экранирующих конструкциях;

## Требования по защите системы заземления объекта ИС (410)

Сопротивление заземлителя объекта ИС не должно превышать 4 Ома. Заземляющее устройство должно размещаться в пределах контролируемой зоны. Защитное заземление объекта ИС не должно иметь выход за пределы контролируемой зоны по экранным оболочкам канальных кабелей, по токопроводящим конструктивным элементам кабелей, металлическим трубопроводам, металлоконструкциям здания, и другими коммуникациями, связанным с системой заземления.

Запрещается использовать для системы заземления объекта естественные заземлители (металлические трубопроводы, железобетонные конструкции здания и т.п.), имеющие выход за пределы контролируемой зоны.

*Это важно*

Для устранения опасности утечки секретной информации по экранным оболочкам кабелей и по металлическим трубопроводам, имеющим выход за пределы контролируемой зоны, рекомендуется использовать токонепроводящие вставки (муфты) длиной не менее 0,1 м – в экранные оболочки кабелей и длиной не менее 1 м – в трубопроводы или применять неметаллические трубопроводы и т.п.

Заземлитель объекта ИС следует располагать не ближе 10–15 м от других подземных коммуникаций (водопровода, кабелей и т.п.), имеющих выход за пределы контролируемой зоны.

В том случае, когда нет возможности удалить заземлитель от подземных коммуникаций либо обеспечить требуемое расстояние от него до границы контролируемой зоны, рекомендуется использовать глубинные заземлители.

При наличии в ТС “схемной земли”, отдельного заземлителя для нее создавать не требуется. Шина “схемной земли” должна быть проложена изолированно от защитного заземления и металлоконструкций сооружений и не должна образовывать замкнутых петель. Заземляющие проводники должны быть выполнены из медного провода (кабеля) сечением не менее 10 мм.

## Требования по защите систем электроснабжения объекта ИС (410)

Все устройства и кабели электроснабжения объекта ИС, включая трансформаторную подстанцию (ТП) низкого напряжения с заземляющим устройством и средствами защиты системы электроснабжения, необходимо размещать в пределах контролируемой зоны и не ближе 10–15 м от ее границ.

Запрещается подключение потребителей электроэнергии, расположенных за пределами контролируемой зоны.

На универсальных объектах электропитание низкочастотных ТС необходимо осуществлять от разделительных систем типа электродвигатель-генератор, дизель-генератор и других в целях обеспечения гальванической и электромагнитной развязки кабелей электропитания ТС и их металлических оболочек от промышленной сети.

Электропитание высокочастотных ТС на универсальных объектах допускается осуществлять от разделительных систем электроснабжения, либо через помехоподавляющие фильтры.

Электропитание ТС должно осуществляться экранированными (бронированными) кабелями. При невозможности выполнения требований по указанному разносу, электропитание ТС должно осуществляться через помехоподавляющие фильтры или от разделительных систем электроснабжения.

Цепи электропитания ТС на участке от основных технических средств до разделительных систем или помехоподавляющих фильтров должны прокладываться в жестких экранирующих конструкциях. Цепи электропитания от помехоподавляющих фильтров или разделительных систем необходимо прокладывать от ТС на расстоянии не менее R.

При совместной прокладке экранированных кабелей электропитания, развязанных от промышленной сети, с кабелями, имеющими выход за пределы контролируемой зоны, необходимо указанные кабели размещать относительно друг друга на расстоянии, не менее 0,3 м при длине параллельного пробега не более 100 м.

При невозможности выполнения данного требования перечисленные кабели электропитания или кабели, имеющие выход за пределы контролируемой зоны,

необходимо прокладывать по всей длине параллельного пробега в жесткой экранирующей конструкции без разноса.

Недопустима прокладка в одной экранирующей конструкции кабелей электропитания, развязанных от промышленной сети, с любыми кабелями, имеющими выход за пределы контролируемой зоны.

Запрещается осуществлять электропитание ТС, имеющих выход за пределы контролируемой зоны, от защищенных источников электроснабжения ТС без установки в цепи электропитания ТС фильтров ФП.

За отсутствием разделительных систем допускается по согласованию с головной организацией по ТЗИ осуществлять питание ТС через машинные преобразователи

***При проектировании электроснабжения объектов защищенных ИС необходимо предусмотреть следующее:***

- исключить контакт заземлений ТП объекта ИС и питающего центра (ЦРП), расположенного за пределами контролируемой зоны. Для этой цели питающие высоковольтные кабельные линии между ними должны иметь вставки воздушной линии или кабеля без металлической оболочки на границе контролируемой зоны;
- при необходимости вывода питающих кабелей за пределы контролируемой зоны электропитание должно быть выполнено по схеме с изолированной нейтралью (через разделительный трансформатор) кабелем в пластмассовой оболочке.

При невозможности размещения ТП в пределах контролируемой зоны необходимо предусмотреть отдельную систему заземления объекта ИС, изолированную от заземления ТП.

В соответствии с этим от разделительного устройства к распределительному щиту должны прокладываться четырехжильные кабели с пластмассовой оболочкой. Через четвертую жилу кабеля нейтраль генератора заземляется на отдельный заземлитель объекта ИС. При этом должен быть выполнен контроль изоляции генератора относительно заземления ТП. Эти требования должны распространяться на всех потребителей, обеспечивающих работу ИС, машинные преобразователи, используемые для соблюдения специальных требований.

## Резюме

Система защиты информации должна гарантировать, что любое движение данных идентифицируется, авторизуется, обнаруживается и документируется.

Организационные требования к системе защиты предусматривают реализацию совокупности административных и процедурных мероприятий.

В общем случае СЗИ целесообразно условно разделить на следующие подсистемы:

- подсистему управления доступом к ресурсам ИС (включает также функции управления системой защиты в целом);
- подсистему регистрации и учета действий пользователей (процессов);
- криптографическую подсистему;
- подсистему обеспечения целостности информационных ресурсов и конфигурации ИС.

Для каждой из подсистем определяются требования в виде:

- перечня обеспечиваемых подсистемой функций защиты;
- основных характеристик этих функций;
- перечня средств, реализующих эти функции.

Программные средства защиты информации должны обеспечивать контроль доступа, безопасность и целостность данных и защиту самой системы защиты. Для этого необходимо выполнить следующие условия:

- объекты защиты должны идентифицироваться в явном виде при использовании паролей, пропусков и идентификации по голосу;
- система контроля доступа должна быть достаточно гибкой для обеспечения многообразных ограничений и различных наборов объектов;
- каждый доступ к файлу данных или устройству должен прослеживаться через систему контроля доступа для того, чтобы фиксировать и документировать любое обращение.