Методы и средства защиты от электромагнитных излучений и наводок

Пассивные методы защиты от побочных электромагнитных излучений и наводок

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

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

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

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

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


Пассивные методы защиты от ПЭМИН
Экранирование
Снижение мощности излучений и наводок
Снижение информативности сигналов

Экранирование является одним из самых эффективных методов защиты от электромагнитных излучений. Под *экранированием* понимается размещение элементов КС, создающих электрические, магнитные и электромагнитные поля, в пространственно замкнутых конструкциях.

Способы экранирования зависят от особенностей полей, создаваемых элементами КС при протекании в них электрического тока.

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

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

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

Экранирование осуществляется на пяти уровнях:

• уровень элементов схем;

• уровень блоков;

• уровень устройств;

• уровень кабельных линий;

• уровень помещений.

Выбор числа уровней и материалов экранирования осуществляется с учетом:

• характеристик излучения (тип, частота и мощность);

• требований к уровню излучения за пределами контролируемой зоны и размеров зоны;

• наличия или отсутствия других методов защиты от ПЭМИН;

• минимизации затрат на экранирование.

Снижение мощности излучений и наводок

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

К данной группе относятся следующие методы:

• изменение электрических схем;

• использование оптических каналов связи;

• изменение конструкции;

• использование фильтров;

• гальваническая развязка в системе питания.

Снижение информативности сигналов

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

• специальные схемные решения;

• кодирование информации.

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

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

Используется пространственное и линейное зашумление. ***Пространственное зашумление*** осуществляется за счет излучения с помощью антенн электромагнитных сигналов в пространство.

Применяется *локальное пространственное зашумление* для защиты конкретного элемента КС и *объектовое пространственное зашумление* для защиты от побочных электромагнитных излучений КС всего объекта.

При *локальном пространственном зашумлении* используются прицельные помехи. Антенна находится рядом с защищаемым элементом КС.

Объектовое пространственное зашумление осуществляется, как правило, несколькими генераторами со своими антеннами, что позволяет создавать помехи во всех диапазонах побочных электромагнитных излучений всех излучающих устройств объекта.

Методы защиты от несанкционированного изменения структур КС

Несанкционированному изменению могут быть подвергнуты алгоритмическая, программная и техническая структуры КС на этапах ее разработки и эксплуатации.

На этапе эксплуатации необходимо выделить работы по модернизации КС, представляющие повышенную опасность для безопасности информации.

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

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

• привлечение к разработке высококвалифицированных специалистов;

• использование иерархических структур;

• применение стандартных блоков;

• дублирование разработки;

• контроль адекватности;

• многослойная фильтрация;

• автоматизация разработки;

• контроль процесса разработки;

• сертификация готового продукта.

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

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

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

Защита от закладок при разработке программ *Современные технологии программирования*

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

• использование современных технологий программирования;

• наличие автоматизированной системы разработки;

• наличие автоматизированных контрольно-испытательных стендов;

• представление готовых программ на языках высокого уровня;

• наличие трансляторов для обнаружения закладок.

Одним из перспективных направлений создания программного обеспечения повышенной безопасности является использование объектно-ориентированного программирования, идущего на смену структурному программированию. Применение объектно-ориентированного программирования (ООП) позволяет разделить фазы описания и фазы реализации абстрактных типов данных. Два выделенных модуля допускают раздельную компиляцию. В модуле описания задаются имена и типы внутренних защищенных и внешних данных, а также перечень процедур (методов) с описанием типов и количества параметров для них. В модуле реализации находятся собственно процедуры, обрабатывающие данные. Такое разделение повышает надежность программирования, так как доступ к внутренним данным возможен только с помощью процедур, перечисленных в модуле описания.

Автоматизированная система разработки программных средств

Автоматизированная система создается на базе локальной вычислительной сети (ЛВС). В состав ЛВС входят рабочие станции программистов и сервер администратора.

Программисты имеют полный доступ только к информации своей ЭВМ и доступ к ЭВМ других программистов в режиме чтения. С рабочего места администратора возможен доступ в режиме чтения к любой ЭВМ разработчиков.

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

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

Контрольно-испытательный стенд должен отвечать следующим требованиям:

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

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

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

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

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

• модель системы, которая состоит из моделей программных модулей и программных модулей реальной системы;

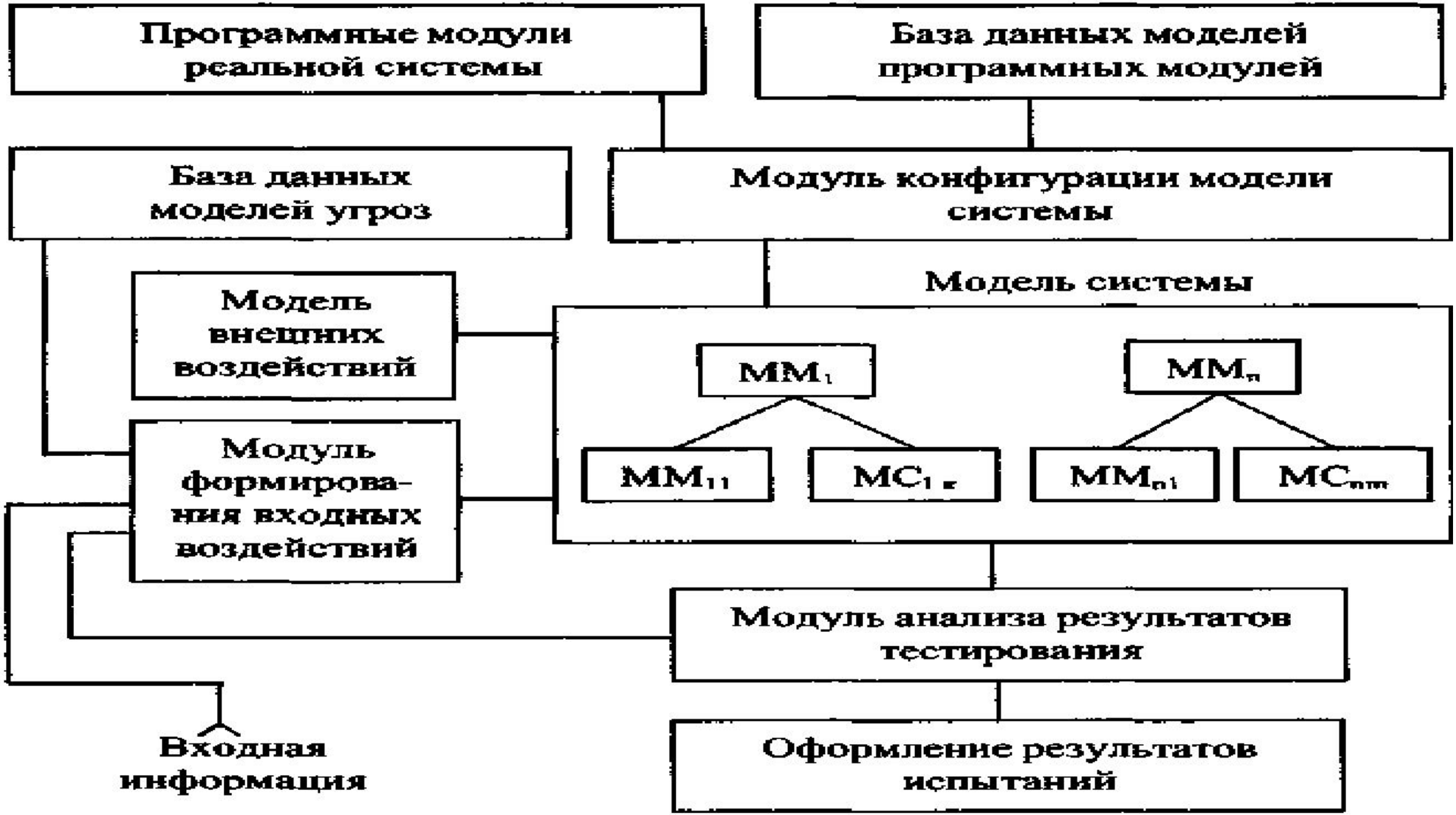
• модуль конфигурации модели системы, осуществляющий регистрацию и динамическое включение программных модулей реальной системы и моделей программных модулей из соответствующих баз данных;

• база данных моделей угроз - для накопления и модификации моделей угроз, представленных в формализованном виде;

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

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

• модуль анализа результатов тестирования.


Программные модули реальной системы
База данных моделей программных модулей
База данных моделей угроз
Модуль конфигурации модели системы
Модель системы
Модель внешних воздействий
Модуль формирования входных воздействий
MM_1
MM_n
MM_{11}
$MC_{1\,k}$
MM_{n1}
MC_{nm}
Модуль анализа результатов тестирования
Входная информация
Оформление результатов испытаний

Защита от внедрения аппаратных закладок на этапе разработки и производства

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

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

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

Разграничение доступа к оборудованию

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

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

• охрана помещений, в которых находятся аппаратные средства КС;

• разграничение доступа к оборудованию;

• противодействие несанкционированному подключению оборудования;

• защита внутреннего монтажа, средств управления и коммутации от несанкционированного вмешательства;

• противодействие внедрению вредительских программ.

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

• идентификация и аутентификация субъекта доступа;

• разблокирование устройства;

• ведение журнала учета действий субъекта доступа.

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

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

• пароли;

• съемные носители информации;

• электронные жетоны;

• пластиковые карты;

• механические ключи.

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

Пароли должны храниться в КС таким образом, чтобы они были недоступны посторонним лицам.

Этого можно достичь двумя способами:

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

• криптографическое преобразование пароля.

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

Пароль должен легко запоминаться и в тоже время быть защищенным.