Подавление побочных электромагнитных излучений

15

В этой главе

- *Источники утечки информации по каналам ПЭМИН*
- *Организация защиты информации в ИС от утечки по каналам ПЭМИН*
- *Рекомендации по защите информации от перехвата излучений технических средств объектов ИС*
- *Оценка защищенности 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

Наибольшую опасность с точки зрения утечки информации представляют побочные (паразитные, непреднамеренные) излучения технических средств, участвующих в процессе передачи, обработки и хранения секретной информации. Роль и место вопросов подавления ПЭМИН в общей структуре СЗИ показаны на рис. 15.1.

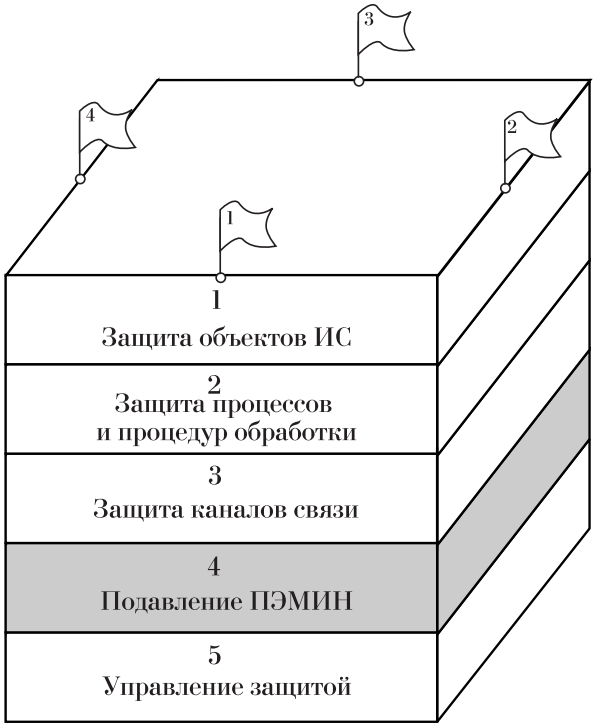


РИСУНОК 15.1. *Вопросы подавления ПЭМИН в общей структуре СЗИ.*

Определение

Под утечкой информации по каналам ПЭМИН понимается возможность доступа к информации в ИС, осуществляемого путем перехвата и соответствующей обработки побочных (паразитных, непреднамеренных) излучений технических средств передачи информации, используемых в указанной системе для сбора, обработки, хранения и обмена информацией.

Канал утечки информации включает в себя технические средства передачи, обработки или хранения секретной информации, среду распространения паразитных электромагнитных или других излучений и средство перехвата и первичной обработки побочных (паразитных) излучений.

Контролируемая территория (КТ) включает в себя пространство вокруг *технических средств (ТС)*, в пределах которого исключается неконтролируемое пребывание посторонних лиц, транспортных средств и других посторонних объектов, не имеющих постоянного или разового допуска.

Среда распространения опасных сигналов...

Среда распространения опасных сигналов может быть представлена в виде свободного пространства с параметрами, учитывающими реальное ослабление электромагнитных полей экранами, стенами зданий и помещений и другими местными предметами, находящимися между ТС и антенной системы перехвата, а также в виде проводов, линий кабелей связи и металлических конструкций систем водо-, газо-, электроснабжения и центрального отопления, выходящих за пределы контролируемых зон. Кроме того, в качестве среды распространения может часто выступать грунт в районе контуров заземления.

Система перехвата может быть представлена в виде комплекса, содержащего приемное устройство, согласующий фильтр и анализатор, обеспечивающие соответственно обнаружение и самые лучшие условия для выделения интересующего противника излучения, оптимальную обработку данного вида сигнала с помехой в целях улучшения “понятности” сигнала и принятие решения, обеспечивающего предельную “разборчивость” сигнала. При этом анализ зарегистрированного сигнала может проводиться многократно с использованием методов обработки сигналов на ПК.

Определение

Разработка средств ВТ с уровнем излучения, безопасным для информации, обходится в 3—4 раза дороже, чем средств ВТ для обработки открытой информации. Считалось очень трудоемким процессом расшифровать информацию, содержащуюся в излучении, и что такое восстановление информации под силу только профессионалам, располагающим сложной аппаратурой обнаружения и декодирования. Так, у ВТ для обработки частной или деловой информации даже не проверяют уровень безопасности излучения. Однако исследования показали, что восстановить информацию от некоторых средств ВТ можно с помощью общедоступных радиоэлектронных средств.

В частности, при восстановлении информации с дисплеев можно использовать обычный черно-белый телевизор с незначительными усовершенствованиями. Если дисплей является элементом вычислительной системы, то он может оказаться самым слабым ее звеном, которое сведет на нет все меры по увеличению безопасности излучений, принятые во всех остальных частях системы. Применение в средствах ВТ импульсных сигналов прямоугольной формы и высокочастотной коммутации приводит к тому, что в спектре излучений будут компоненты с частотами вплоть до СВЧ. Энергетический спектр сигналов убывает с ростом частоты, но эффективность излучения при этом увеличивается и уровень излучений может оставаться постоянным до частот нескольких гигагерц. Резонансы от паразитных связей могут вызвать усиление излучения на некоторых частотах спектра. Цепи, не предназначенные для передачи цифровых сигналов, могут излучать их вследствие наводок. Примером таких излучателей могут служить провода источников питания.

Источники утечки информации по каналам ПЭМИН (240)

Поговорим о защите важной (критической) информации, которая обрабатывается, циркулирует, отображается в ИС и средствах вычислительной техники (СВТ).

Носителями такой информации являются электрические и электромагнитные поля и сигналы, образующиеся в результате работы средств обработки информации или воздействия опасного сигнала на средства обработки открытой информации и на системы жизнеобеспечения.

К техническим средствам, которые могут быть источником утечки информации по каналам ПЭМИН относятся:

- средства и системы телефонной, телеграфной (телетайпной), директорской, громкоговорящей, диспетчерской, внутренней, служебной и технологической связи;
- средства и системы звукоусиления, звукозаписи и звуковоспроизведения;
- устройства, образующие дискретные каналы связи: абонентская аппаратура со средствами отображения и сигнализации, аппаратура повышения достоверности передачи, каналообразующая и т.п.;
- аппаратура преобразования, обработки, передачи и приема видеоканалов, содержащих факсимильную информацию;
- средства и системы специальной охранной сигнализации (на вскрытие дверей, окон и проникновение в помещение посторонних лиц), пожарной сигнализации (с датчиками, реагирующими на дым, свет, тепло, звук);
- система звонковой сигнализации (вызов секретаря, входная сигнализация);
- контрольно-измерительная аппаратура;
- средства и системы кондиционирования (датчики температуры, влажности, кондиционеры);
- средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения (абонентские громкоговорители системы радиовещания и оповещения, радиоприемники и телевизоры);
- средства и системы часофикации (электронные часы, вторичные электрочасы);
- средства и системы электроосвещения и бытового электрооборудования (светильники, люстры, настольные и стационарные вентиляторы, электронагревательные приборы, холодильники, бумагорезательные машины, проводная сеть электроосвещения);
- электронная и электрическая оргтехника.

Перечисленные технические средства (ТС) могут представлять собой сосредоточенные случайные антенны (аппаратура и ее блоки) и распределенные случайные антенны (кабельные линии и провода).

Указанными элементами могут быть:

- технические средства и приборы;
- кабельные сети и разводки, соединяющие устройства и оборудование;
- коммутационные устройства (коммутаторы, кроссы, боксы и т.п.);
- элементы заземления и электропитания.

Краткое описание возможной утечки информации по каналам ПЭМИН (240)

В процессе функционирования средств вычислительной техники в конструктивных элементах и кабельных соединениях циркулируют электрические токи информативных сигналов, в результате чего формируются электромагнитные поля, уровни которых могут быть достаточными для приема сигналов и извлечения информации с помощью специальной аппаратуры.

Каналы утечки информации могут возникать вследствие излучения информативных сигналов при работе ТС и наведения этих сигналов в линиях связи, цепях электропитания и заземления, других коммуникациях, имеющих выход за пределы ***контролируемой территории (КТ)***. Информативные сигналы могут распространяться на большие расстояния и регистрироваться средствами технических разведок за пределами КТ.

Частоты, на которых могут излучаться (наводиться) информативные сигналы, зависят от типов и видов

аппаратурных средств и могут распространяться в диапазоне от сотен герц до нескольких десятков гигагерц.

Уровень наводок определяется расстоянием между источниками излучения и аппаратурой, подверженной влиянию этих излучений, длиной параллельного пробега и величиной переходного затухания линий, напряжением информативного сигнала в линии и уровнем шумов (помех).

Утечка информации по цепям заземления может возникнуть при наличии разнесенных точек заземления информативных цепей в случае образования в разных точках системы заземления разности потенциалов и возникновения в результате этого токов в цепях заземления, при большом значении сопротивления цепи заземления, а также вследствие несовершенства экранов, приводящего к асимметрии линий относительно экрана и к возникновению в цепи между корпусом экрана и землей информативных токов.

Кроме того, ***возможные каналы утечки информации образуются:***

- низкочастотными электромагнитными полями, возникающими при работе ТС;
- при воздействии на ТС электрических, магнитных и акустических полей;
- при возникновении паразитной высокочастотной (ВЧ) генерации;
- при прохождении информативных (опасных) сигналов в цепи электропитания;
- при взаимном влиянии цепей;
- при прохождении информативных (опасных) сигналов в цепи заземления;
- при паразитной модуляции высокочастотного сигнала;
- вследствие ложных коммутаций и несанкционированных действий.

При передаче информации в элементах схем, конструкций, в подводящих и соединяющих проводах технических средств протекают токи информативных (опасных) сигналов. Возникающие при этом электромагнитные поля могут воздействовать на случайные антенны. Сигналы, принятые случайными антеннами, могут привести к образованию каналов утечки информации.

Источниками возникновения электромагнитных полей в ТС могут быть неэкранированные провода, разомкнутые контуры, элементы контрольно-измерительных приборов, контрольные гнезда на усилительных блоках и пультах, неэкранированные оконечные устройства, усилители мощности и линейные усилители, трансформаторы, дроссели, соединительные провода, разъемы, громкоговорители, кабельные линии.

Информативные (опасные) сигналы могут возникать на элементах технических средств, чувствительных к воздействию:

- электрического поля (неэкранированные провода и элементы технических средств);
- магнитного поля (микрофоны, громкоговорители, головные телефоны, трансформаторы, катушки индуктивности, дроссели, электромагнитные реле);
- акустического поля (микрофоны, громкоговорители, головные телефоны, трансформаторы, катушки индуктивности, дроссели, электромагнитные реле).

При наличии в технических средствах элементов, способных преобразовывать эти поля в электрические сигналы, возможна утечка информации по незащищенным цепям абонентских линий связи, электропитания, заземления, управления и сигнализации.

Паразитная высокочастотная генерация (ПВЧГ) в ТС возникает вследствие самовозбуждения усилительных устройств (активная ПВЧГ) либо вследствие отражения сигналов от концов линий связи между усилителями при переходных процессах (пассивная ПВЧГ).

Высокочастотные паразитные колебания, промодулированные информативным (опасным) сигналом по амплитуде, частоте и фазе (активная ПВЧГ) или по амплитуде и частоте (пассивная ПВЧГ), создают канал утечки информации.

ПВЧГ образуется в элементах аппаратуры, охваченных отрицательной обратной связью и не имеющих достаточного запаса устойчивости, в концах линий связи между усилительными устройствами в моменты переключений из-за возникновения переходных процессов.

Кстати

Во время работы ТС возможна утечка информации через источники электропитания:

- в результате прохождения информативного (опасного) сигнала через технические средства на входном сопротивлении его источника питания может возникнуть напряжение, несущее сигнал, содержащий информативную составляющую. Через выпрямительное устройство и силовой трансформатор этот сигнал распространяется по сетевым линиям за пределы контролируемой территории;
- при прохождении речевого сигнала через оконечное усилительное устройство может наблюдаться неравномерное потребление тока от источника питания. Ток, потребляемый усилителем от сети, может быть промодулирован информативным (опасным) сигналом, проходящим через усилитель.

Трассы кабельных цепей, несущих информацию, могут прокладываться в одной кабельной канализации

с незащищенными цепями ТС и проходить через общие протяжные коробки и шкафы.

При передаче информативного (опасного) сигнала по одной цепи в соседних цепях — при их параллельном пробеге — возникают токи, наведенные вследствие электромагнитного влияния. Переход электромагнитной энергии из одной цепи в другую является возможным каналом утечки информации.

Надо знать

Источниками образования информативных (опасных) сигналов являются участки, охваченные случайными емкостными и магнитными связями. Такими участками могут быть отрезки параллельного пробега линий, несущих информацию, с незащищенными линиями, уходящими за пределы контролируемой территории; монтажные колодки, разъемы блоков, контакты переключателей и реле, используемые для коммутации выходных линий и блоки, подверженные влиянию электромагнитного поля.

Источником образования информативных (опасных) сигналов являются элементы цепей и схем, если эти элементы находятся под потенциалом таких сигналов и выходят из экранов.

При поступлении высокочастотных сигналов в нелинейные (или параметрические) цепи, несущие информативные (опасные) сигналы, происходит модуляция высокочастотного сигнала. Таким образом, высокочастотные колебания становятся носителями информативных (опасных) сигналов и создают канал утечки информации.

Линиями, на которые подается или с которых снимается высокочастотный сигнал, могут быть незащищенные линии связи, цепи электропитания, заземления, управления и сигнализации; цепи, образованные паразитными связями, конструктивными элементами зданий, сооружений, оборудования и т.п.

Источниками информативных (опасных) сигналов являются нелинейные радиоэлементы, на которых происходит модуляция таких сигналов.

При возникновении неисправностей в аппаратуре или несанкционированных действиях обслуживающего персонала в схемах управления может возникнуть нежелательная коммутация информативного (опасного) сигнала, приводящая к выходу информации в незащищенный канал связи.

Источниками информативного (опасного) сигнала этого канала являются пульты управления, щиты распределения и коммутации, блоки контроля, реле, трансформаторы, разъемы, переключатели или запоминающие устройства, в которых может возникнуть ложная коммутация в результате неисправностей или несанкционированных действий.

Основными параметрами возможной утечки информации по каналам ПЭМИН являются:

- напряженность электрического поля информативного (опасного) сигнала;
- напряженность магнитного поля информативного (опасного) сигнала;
- величина звукового давления;
- величина напряжения информативного (опасного) сигнала;
- величина напряжения наведенного информативного (опасного) сигнала;
- величина напряжения шумов (помех);
- величина тока информативного (опасного) сигнала;
- величина чувствительности к воздействию магнитных полей для точечного источника;
- величина чувствительности аппаратуры к воздействию электрических полей (собственная емкость аппаратуры);
- величина чувствительности к воздействию акустических полей;
- отношение “информативный сигнал/шум”;
- отношение напряжения опасного сигнала к напряжению шумов (помех) в диапазоне частот информативного сигнала.

Указанные параметры определяются и рассчитываются по результатам измерений в заданных точках. Предельно допустимые значения основных параметров являются нормируемыми величинами и определяются по соответствующим методикам. Отношения расчетных

(измеренных) значений основных параметров к предельно допустимым (нормированным) значениям определяют необходимые условия защиты информации.

Организация защиты информации в ИС от утечки по каналам ПЭМИН (640)

Работы по защите информации (ЗИ) в ИС предусматривают:

- категорирование объектов электронно-вычислительной техники (ЭВТ);
- включение в технические задания на монтаж ИС и СВТ раздела по ЗИ;
- монтаж ИС и СВТ в соответствии с рекомендациями настоящего документа;
- обследование (в том числе технический контроль) объектов ЭВТ;
- установку (при необходимости) аттестованных средств защиты;
- технический контроль за эффективностью принятых мер.

Рекомендуемый алгоритм обследования содержит следующие процедуры:

Совет

- анализ в технических средствах (ТС) ЭВТ потоков информации, требующей защиты;
- определение состава ТС на объекте ЭВТ;
- определение состава кабельных линий, выходящих за пределы КТ и имеющих параллельный пробег с кабелями ИС и СВТ;
- выявление коммуникаций, проходящих через территорию объекта ЭВТ и имеющих выход за пределы КТ;
- инструментальное измерение информативных побочных электромагнитных излучений и наводок;
- оценку соответствия уровней сигналов и параметров полей – носителей информации нормам эффективности защиты.

По результатам обследования составляется акт, в котором отражаются:

- категория объекта ЭВТ;
- перечень ТС (наименование, тип, заводской номер);
- перечень ТС и коммуникаций, находящихся на объекте ЭВТ;
- оценка соответствия монтажа настоящим рекомендациям;
- предложения по применению дополнительных мер защиты (при необходимости).

К акту прилагаются:

- схема размещения ТС объекта ЭВТ и прохождения коммуникаций на нем;
- протоколы измерений.

Организационные мероприятия (043)

На этапе проведения организационных мероприятий необходимо:

- определить перечень сведений, подлежащих технической защите (определяет собственник информации в соответствии с действующим законодательством Украины);
- обосновать необходимость разработки и реализации защитных мероприятий с учетом материального или иного ущерба, который может быть нанесен вследствие возможного нарушения целостности информации либо ее утечки по техническим каналам;
- установить перечень выделенных помещений, в которых не допускается реализация угроз и утечка информации с ограниченным доступом;
- определить перечень технических средств, которые должны использоваться как ТС;
- определить технические средства, применение которых не обосновано служебной и производственной необходимостью и которые подлежат демонтажу;
- определить наличие используемых и неиспользуемых воздушных, наземных, настенных и скрытых кабелей; цепей и проводов, уходящих за пределы выделенных помещений;
- определить системы, подлежащие демонтажу, требующие переоборудования кабельных сетей, цепей питания, заземления или установки в них защитных устройств.

Подготовительные технические мероприятия (043)

Состоят из первичных мер блокирования электроакустических преобразователей и линий связи, выходящих за пределы выделенных помещений.

Блокирование линий связи может выполняться следующими способами:

- отключением линий связи ТС или установкой простейших схем защиты;
- демонтажем отдельных технических средств, кабелей, цепей, проводов, уходящих за пределы выделенных помещений;

- удалением за пределы выделенных помещений элементов технических средств, которые могут служить источником возникновения канала утечки информации.

Блокирование каналов возможной утечки информации в системах городской и ведомственной телефонной связи может осуществляться:

- отключением звонковых (вызывных) линий телефонного аппарата;
- установкой в цепи телефонного аппарата безразрывной розетки для временного отключения;
- установкой простейших устройств защиты.

Предотвращение утечки информации через действующие системы громкоговорящей диспетчерской и директорской связи осуществляется применением следующих защитных мер:

- установкой в вызывных цепях выключателей для разрыва цепей;
- установкой на входе громкоговорителей выключателей (реле), позволяющих разрывать цепи по двум проводам;
- обеспечением возможности отключения питания микрофонных усилителей;
- установкой простейших устройств защиты.

Защита информации от утечки через радиотрансляционную сеть, выходящую за пределы выделенного помещения, может быть обеспечена:

- отключением громкоговорителей по двум проводам;
- включением простейших устройств защиты.

Для службы оповещения следует выделить дежурные абонентские устройства вне выделенных помещений; цепи к этим устройствам должны быть проложены отдельным кабелем.

Блокирование каналов ***утечки информации через цепи электрочасов*** системы часофикации осуществляется отключением их на период проведения закрытых мероприятий.

Предотвращение ***утечки информации через системы пожарной и охранной сигнализации*** осуществляется отключением датчиков пожарной и охранной сигнализации на период проведения важных мероприятий, содержащих информацию, или применением датчиков, не требующих специальных мер защиты.

В целях исключения возможности утечки информации при работе незащищенных техническими средствами телевизоров, радиоприемников, звукоусилительной и звуковоспроизводящей аппаратуры необходимо на период проведения важных мероприятий указанные устройства отключать от сети электропитания по двум проводам.

Блокирование утечки информации через системы электронной оргтехники и кондиционирования может быть обеспечено следующими мерами:

- расположением указанных систем внутри контролируемой территории без выноса отдельных компонентов за ее пределы;
- электропитанием систем от трансформаторной подстанции, находящейся внутри контролируемой территории.

При невыполнении перечисленных условий системы должны отключаться от сети электропитания по двум проводам.

Защита информации от утечки через цепи электроосвещения и электропитания бытовой техники должна осуществляться подключением указанных цепей к отдельному фидеру трансформаторной подстанции, к которому не допускается подключение сторонних пользователей.

В случае невыполнения указанного требования электробытовые приборы на период проведения закрытых мероприятий должны отключаться от цепей электропитания.

Технические мероприятия (044)

Это основной этап работ по защите информации, состоящий в обеспечении ТС устройствами ЗИ.

При выборе, установке, замене технических средств следует руководствоваться прилагаемыми к этим средствам паспортами, техническими описаниями, инструкциями по эксплуатации, рекомендациями по установке, монтажу и эксплуатации.

ТС должны размещаться, по возможности, ближе к центру здания или в сторону наибольшей части контролируемой территории. Составные элементы ТС должны размещаться в одном помещении либо в смежных.

Если указанные требования невыполнимы, следует принять ***дополнительные меры защиты***:

- установить высокочастотные ТС в экранированное помещение (камеру);
- установить в незащищенные каналы связи, линии, провода и кабели специальные фильтры и устройства;
- проложить провода и кабели в экранирующих конструкциях;
- уменьшить длину параллельного пробега кабелей и проводов разных систем с проводами и кабелями, несущими информацию;
- выполнить технические мероприятия по защите информации от утечки по цепям заземления и электропитания.

К средствам технической защиты относятся:

Надо знать

- фильтры-ограничители и специальные абонентские устройства защиты для блокирования утечки речевой информации через двухпроводные линии телефонной связи, системы директорской и диспетчерской связи;
- устройства защиты абонентских однопрограммных громкоговорителей для блокирования утечки речевой информации через радиотрансляционные линии;
- фильтры сетевые для блокирования утечки речевой информации по цепям электропитания переменного (постоянного) тока;
- фильтры защиты линейные (высокочастотные) для установки в линиях аппаратов телеграфной (телекодовой) связи;
- генераторы линейного зашумления;
- генераторы пространственного зашумления;
- экранированные камеры специальной разработки.

Выбор методов и способов защиты элементов ТС, обладающих микрофонным эффектом, зависит от величины их входного сопротивления на частоте 1 кГц.

Элементы с входным сопротивлением менее 600 Ом (головки громкоговорителей, электродвигатели вентиляторов, трансформаторы и т.п.) рекомендуется отключать по двум проводам или устанавливать в разрыв цепей устройства защиты с высоким выходным сопротивлением для снижения до минимальной величины информативной составляющей тока.

Элементы с высоким входным сопротивлением (электрические звонки, телефонные капсюли, электромагнитные реле) рекомендуется не только отключать от цепей, но и замыкать на низкое сопротивление или закорачивать, чтобы уменьшить электрическое поле от данных элементов, обусловленное напряжением, наведенным при воздействии акустического поля. При этом следует учитывать, что выбранный способ защиты не должен нарушать работоспособность технического средства и ухудшать его технические параметры.

Высокочастотные автогенераторы, усилители (микрофонные, приема, передачи, громкоговорящей связи) и другие устройства, содержащие активные элементы, рекомендуется отключать от линий электропитания в “дежурном режиме” или “режиме ожидания вызова”.

Подключение устройств защиты следует проводить без нарушения или изменения электрической схемы и ТС.

Защиту информации от утечки по кабелям и проводам рекомендуется осуществлять путем:

- применения экранирующих конструкций;
- раздельной прокладки кабелей.

Электропитание следует осуществлять либо экранированными кабелями, либо с использованием разделительных систем, либо через сетевые фильтры.

Не допускается образование петель и контуров кабельными линиями. Пересечение кабельных трасс разного назначения рекомендуется осуществлять под прямым углом друг к другу.

Электропитание ТС должно быть стабилизировано по напряжению и току для нормальных условий функционирования ТС и обеспечения норм защищенности.

В цепях выпрямительного устройства источника питания необходимо устанавливать фильтры нижних частот. Фильтры должны иметь фильтрацию по симметричным и несимметричным путям распространения.

Необходимо предусмотреть отключение электросети от источника питания ТС при исчезновении напряжения в сети, при отклонении параметров электропитания от норм, заданных в ТУ, и при появлении неисправностей в цепях электропитания.

Все металлические конструкции ТС (шкафы, пульты, корпуса распределительных устройств и металлические оболочки кабелей) должны быть заземлены.

Заземление ТС следует осуществлять от общего контура заземления, размещенного в пределах контролируемой территории, с сопротивлением заземления по постоянному току в соответствии с требованиями стандартов.

Система заземления должна быть единой для всех элементов ТС и строиться по радиальной схеме.

Образование петель и контуров в системе заземления не допускается.

Экраны кабельных линий ТС, выходящих за пределы контролируемой территории, должны заземляться в кроссах от общего контура заземления в одной точке для исключения возможности образования петель по экрану и корпусам.

В каждом устройстве должно выполняться условие непрерывности экрана от входа до выхода. Экраны следует заземлять только с одной стороны. Экраны

Система заземления должна быть единой для всех...

кабелей не следует использовать в качестве второго провода сигнальной цепи или цепи питания.

Экраны кабелей не должны иметь электрического контакта с металлоконструкциями. Для монтажа следует применять экранированные кабели с изоляцией или надевать на экраны изоляционную трубку.

В длинных экранированных линиях (микрофонных, линейных, звукоусилительных) рекомендуется делить экран на участки для получения малых сопротивлений для высокочастотных токов и каждый участок заземлять только с одной стороны.

Рекомендации по защите информации от перехвата излучений технических средств объектов ИС (740)

Территория вокруг ТС должна контролироваться; за ее пределами отношение "информативный сигнал/шум" не превышает нормы. С этой целью ТС рекомендуется располагать во внутренних помещениях объекта, желательно, на нижних этажах.

В случае невозможности обеспечения данного условия необходимо:

- заменить ТС на защищенные;
- провести частичное или полное экранирование помещений или ТС;
- установить системы пространственного зашумления;
- заменить незащищенные ТС на защищенные;
- применить помехоподавляющие фильтры.

В экранированных помещениях (капсулах) рекомендуется размещать высокочастотные (ВЧ) ТС. Как правило, к ним относятся процессоры, запоминающие устройства, дисплеи и т.п.

Защита информации от перехвата наводок на незащищенных ТС, имеющие выход за пределы контролируемой территории

В незащищенных каналах связи, линиях, проводах и кабелях ТС, имеющих выход за пределы КТ, устанавливаются помехоподавляющие фильтры.

Провода и кабели прокладываются в экранированных конструкциях.

Монтаж цепей ТС, имеющих выход за пределы КТ, рекомендуется производить экранированным или проложенным в экранирующих конструкциях симметричным кабелем.

Кабели ТС прокладываются отдельным пакетом и не должны образовывать петли. Пересечение кабелей ТС, имеющих выход за пределы КТ, рекомендуется производить под прямым углом, обеспечивая отсутствие электрического контакта экранирующих оболочек кабелей в месте их пересечения.

Незадействованные провода и кабели демонтируются или закорачиваются и заземляются.

Защита информации от утечки по цепям заземления

Система заземления ЭВТ не должна иметь выход за пределы КТ и должна размещаться на расстоянии не менее 10–15 м от них.

Заземляющие провода должны быть выполнены из медного провода (кабеля). Сопротивление заземления не должно превышать 4 0м.

Не рекомендуется использовать для системы заземления ЭВТ естественные заземлители (металлические трубопроводы, железобетонные конструкции зданий и т.п.), имеющие выход за пределы КТ.

Для устранения опасности утечки информации по металлическим трубопроводам, выходящим за пределы КТ, рекомендуется использовать токонепроводящие вставки (муфты) длиной не менее 1 м.

Выход за пределы контролируемой территории недопустим...

При наличии в ЭВТ “схемной земли” отдельное заземление для них создавать не требуется. Шина “схемная земля” должна быть изолирована от защитного заземления и металлоконструкций и не должна образовывать замкнутую петлю.

При невозможности провести заземление ЭВТ допускается их “зануление”.

Защита информации от утечки по цепям электропитания

Наиболее эффективно гальваническую и электромагнитную развязку кабелей электропитания ТС ЭВТ от промышленной сети обеспечивает их разделительная система типа “электродвигатель-генератор”. Электропитание допускается также осуществлять через помехоподавляющие фильтры.

Электропитание должно осуществляться экранированным (бронированным) кабелем.

Цепи электропитания ЭВТ на участке от ТС до разделительных систем или помехоподавляющих фильтров рекомендуется прокладывать в жестких экранирующих конструкциях.

Не допускается прокладка в одной экранирующей конструкции кабелей электропитания, развязанных от промышленной сети, с любыми кабелями, имеющими выход за пределы КТ.

Запрещается осуществлять электропитание технических средств, имеющих выход за пределы КТ, от защищенных источников электроснабжения без установки помехоподавляющих фильтров.

Системы пространственного зашумления объектов ЭВТ

Устройства пространственного зашумления применяются в случаях, когда пассивные меры не обеспечивают необходимой эффективности защиты объекта ЭВТ.

Установке подлежат только сертифицированные средства пространственного зашумления, в состав которых входят:

- сверхширокополосные генераторы электромагнитного поля шума (генератор шума);
- система рамочных антенн;
- пульт сигнализации исправности работы системы.

Установку генераторов шума, монтаж антенн, а также их обслуживание в процессе эксплуатации осуществляют предприятия, учреждения и организации, имеющие соответствующую лицензию.

Питание генераторов шума должно осуществляться от того же источника, что и питание ТС ЭВТ. Антенны рекомендуется располагать вне экранированного помещения.

Применение экранирующих конструкций

Экранирующие кабельные конструкции совместно с экранирующими конструкциями ТС ЭВТ должны создавать экранирующий замкнутый объем.

Выведение кабелей из экранирующих конструкций и введение в них необходимо осуществлять через помехоподавляющие фильтры.

Экранирующие кабельные конструкции могут быть жесткими и гибкими. Основу жестких конструкций составляют трубы, короба и коробки; основу гибких конструкций — металлорукава, заключенные в оплетку, и сетчатые рукава.

Для экранирования проводов и кабелей применяются водогазопроводные трубы. Рекомендуется применять стальные тонкостенные оцинкованные трубы или стальные электросварные.

Соединение неразъемных труб осуществляется сваркой, разъемных — с помощью муфты и контргайки.

Для экранирования проводов и кабелей применяются короба прямоугольного сечения. Их преимущества по сравнению с трубами — возможность прокладки кабеля с раздельными разъемами.

Короба изготавливаются из листовой стали. На концах секций короба должны быть фланцы для соединения коробов между собой и с другими экранирующими конструкциями. Для получения надежного электрического контакта поверхность фланцев должна иметь антикоррозийное токопроводящее покрытие.

Гибкие конструкции служат для соединения жестких экранирующих кабельных конструкций с экранирующими конструкциями ТС ЭВТ и одновременно являются компенсаторами температурных и монтажных деформаций.

В качестве экрана может быть использован металлорукав типа Р3 по ТУ 22-3688-77, заключенный в стальную оцинкованную оплетку.

Для повышения эффективности экранирования рекомендуется применять комбинированные экраны, состоящие из медной и стальной оплеток.

Окончательное заключение об эффективности мероприятий по технической защите информации дается по результатам инструментального контроля.

Структура электромагнитного излучения дисплея (044)

Изображение на экране дисплея формируется в основном так же, как и ТВ-приемнике — оно состоит из светящихся точек на строках. Видеосигнал является цифровым: сигнал логическая единица создает световую точку, а логический нуль препятствует ее появлению. Однако в цепях дисплея присутствует не только видеосигнал, но и тактовые синхроимпульсы. Посколь-

ку последние повторяются, то энергетический спектр видеосигнала содержит гармоники, интенсивность которых убывает с ростом частоты. Источником излучения видеосигнала дисплея могут быть элементы обработки сигнала изображения электронным лучом кинескопа. В отличие от других сигналов, существующих в дисплее, видеосигнал усиливается до нескольких десятков вольт для подачи на электронно-лучевую трубку (ЭЛТ). Следовательно, именно его излучение наиболее опасно для дисплея.

Результаты экспериментов показали, что уровень широкополосного излучения дисплея зависит от числа букв на экране; уровень узкополосных составляющих не зависит от заполнения экрана; он определяется системой синхронизации и частотой повторения светящихся точек. Следовательно, видеоусилитель — наиболее мощный источник широкополосного излучения, а система синхронизации — узкополосного. Таким образом, излучение дисплеев, содержащих гармоники видеосигналов, охватывает диапазон дециметровых волн.

Восстановление информации по электромагнитному излучению дисплея

Информация, отображенная на экране дисплея, может быть восстановлена с помощью ТВ-приемника. Он обрабатывает лишь небольшую часть спектра шириной около 8 МГц на частотах в диапазонах метровых и дециметровых волн.

В отличие от дисплея максимум видеосигнала в ТВ-приемнике определяет уровень черного, а минимум определяет уровень белого фона. Таким образом, изображение на экране ТВ-приемника будет представлять собой копию изображения на экране дисплея и состоять из черных букв на белом (или сером) фоне. Если видеосигнал представляет собой длинный импульс, то лучше всего будут излучаться в пространство его фронты.

Повышение безопасности электромагнитного излучения дисплея

В конструкции дисплея не следует использовать элементы, быстродействие которых меньшее необходимого, это ограничит верхнюю частоту спектра его излучения. Площадь их участков схемы должна быть как можно меньше. Это можно сделать, располагая выходной проводник на печатной плате как можно ближе к тем, где сигнал. Длина соединительных проводов должна быть минимальной.

Эти меры снижают уровень излучения от печатных плат, но не уменьшают излучение, вызванное электронным лучом кинескопа. Для снижения последнего используется экранирование, причем эффективность экранирования почти пропорциональна толщине экрана в диапазоне частот от сотен килогерц до нескольких гигагерц.

Для уменьшения уровня излучений от дисплея имеется широкий ассортимент экранирующих материалов и средств: экраны с золотым покрытием, проволочные сетки для установки перед экраном дисплея, вентиляционные решетки с ячейками малых размеров, электрические фильтры для уменьшения излучений от кабелей и проводов питания, специальные материалы для соединения различных частей экранирующих конструкций.

Вследствие жестких норм на электромагнитные сигналы практически невозможно снабдить техническое средство генератором шума. Поэтому единственным решением является создание взаимных помех, т.е. размещение в одном месте как можно большего числа однотипных технических средств, в частности — дисплеев. Однако эксперимент показал, что это решение не приводит к увеличению безопасности излучений. Как уже упоминалось, в спектре излучения дисплеев имеются резонансные частоты, которые не совпадают даже с образцами одного и того же типа аппаратуры. Это означает, что информация может быть восстановлена при обработке этих преобладающих участков спектра.

Третьим способом повышения безопасности излучения является создание криптографического дисплея. Основной причиной восстановления информации, отображаемой дисплеем с помощью обычного приемника ТВ-сигнала, является сходство в построении изображения двумя этими устройствами. Если изменить последовательность строк изображения на экране дисплея, то с помощью обычного ТВ нельзя будет восстановить информацию с экрана.

Последовательность строк изображения дисплея может меняться с помощью кодового ключа, вводимого в дисплей. Чтобы по принятому сигналу восстановить информацию, нужно знать последовательность строк. Для еще большего затруднения восстановления информации кодовый ключ может меняться по случайному закону. Таким образом, из всех рассмотренных способов повышения безопасности дисплея с точки зрения их излучения самым дешевым оказывается изменение последовательности строк на экране. Наиболее же универсальным способом является экранирование.

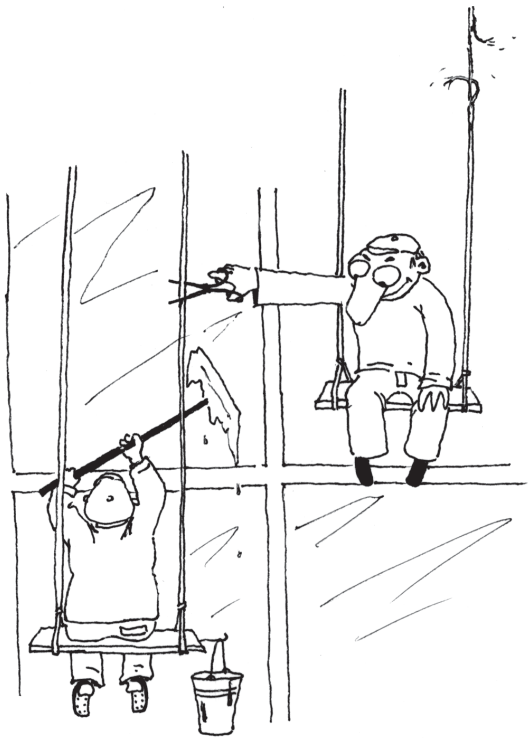
Безопасность электромагнитного излучения кабелей передачи данных

Как правило, причиной излучения кабелей является плохое состояние соединителей, направленных ответвителей и т.п. Теоретически, если нет дефектов в экране (оплетка кабеля, соединителях и других компо-

нентах кабельной сети, эффективность экранированного кабеля составляет более 100 дБ. Этого более чем достаточно для предотвращения излучения от кабеля, которое можно зарегистрировать.

Таким образом, при исправном кабеле восстановить информацию по излучению очень трудно. Однако на практике кабели не всегда полностью экранированы. Неисправные или поврежденные коррозией соединители могут быть причиной значительных излучений. Обнаружители утечки сигналов, часто используемые персоналом, обслуживающим кабельные системы ТВ, могут быть использованы для поиска мест излучений в любых кабелях.

Описанные недостатки электрических кабелей полностью устраняются их заменой волоконно-оптическими. Однако это требует использования оптических и оптико-электрических преобразователей с обеих сторон волоконного кабеля, используемого для передачи данных в двух направлениях. Переходить на волоконно-оптические кабели уместно только при безопасных электромагнитных излучениях от этих преобразователей.



Следует исключить паразитные воздействия в параллельных линиях...

Оценка защищенности информации от утечки по каналам ПЭМИН (741)

Анализ физических процессов, сопровождающих работу различных технических средств связи и оргтехники, показывает, что в окружающем их пространстве и отходящих цепях возникают паразитные информационные сигналы, которые могут обнаруживаться на значительных расстояниях (до сотен метров) от создающих их технических средств (ТС). Последнее обстоятельство может использоваться технической разведкой злоумышленника для перехвата этой информации. Эта разведка получила наименование “разведки побочных электромагнитных излучений”.

Задача защиты информации от утечки по техническим каналам требует решения ряда вопросов, в том числе изучения физических явлений, приводящих к появлению паразитных информационных сигналов в окружающем техническое средство пространстве и отходящих от него цепях, и разработки конкретных методов и средств предотвращения возможности утечки информации.

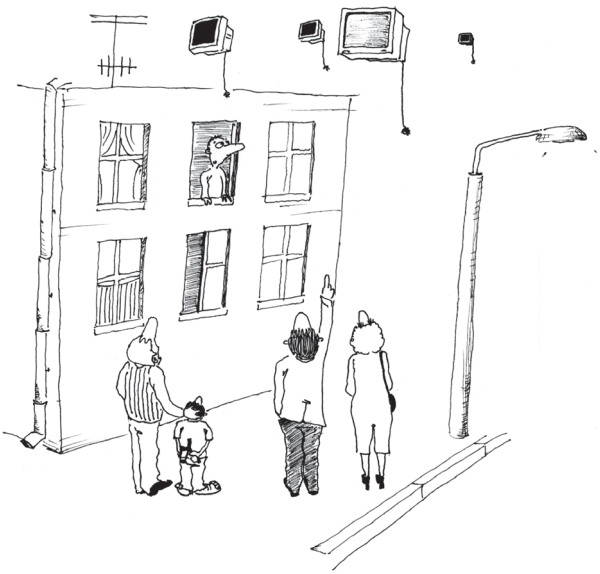
Одним из основных моментов процесса защиты информации от утечки является разработка критериев оценки защищенности информации и норм на параметры информационных сигналов, т.е. сигналов, несущих информацию, выполнение которых не позволит осуществить перехват информации.

Однако разработка норм на допустимые с точки зрения невозможности утечки информации параметры информационных сигналов еще не являются решением задачи оценки защищенности информации: необходимы методики проверки соответствия этим нормам параметров информационных сигналов, т.е. методики оценки эффективности защиты информации от утечки.

Модель утечки информации по каналам ПЭМИН (741)

В процессе функционирования ТС создают в окружающем пространстве электромагнитное поле информационного сигнала. Это электромагнитное поле может быть обнаружено на каком-то расстоянии от технического средства и, следовательно, та информация, переносчиком которой она является, может быть перехвачена.

Кроме того, электромагнитное поле, воздействуя на различные технические средства и системы, не обрабатывающие секретную информацию, наводит в их элементах и отходящих от них цепях напряжения и токи информационного сигнала. Рассматривая частный случай влияния электромагнитного поля — гальваническую связь (в общем случае “паразитную”) вспомогательных цепей ТС с элементами его тракта передачи



Информация может "улетучиться" за счет паразитных излучений дисплея...

(обработки, хранения) информации, приходим к выводу, что в этих цепях будут также появляться напряжения и токи информационного сигнала.

Причем указанная гальваническая связь может быть линейной и нелинейной. В случае линейной связи, как и при воздействии электромагнитного поля, могут происходить какие-то частотные искажения исходного информационного сигнала, в случае нелинейной связи — более сложные его преобразования, например появление огибающей информационного сигнала в цепях электропитания ТС.

Анализ условий эксплуатации ТС на различных объектах показывает, что может иметь доступ к указанным выше цепям и, следовательно, могут быть обнаружены токи и напряжения, а в общем случае — электромагнитные поля информационного сигнала.

Несмотря на различия физических явлений, приводящих к возникновению информационных сигналов в пространстве вокруг ТС и в различных цепях, разработка критериев оценки эффективности защиты осуществляется на единой основе. В связи с этим вводится обобщенная модель канала утечки информации.

В настоящее время известны семь видов каналов утечки информации. Они отличаются физическими явлениями, которые обуславливают наличие в них информационного сигнала. Поэтому для каждого канала утечки можно выделить один или несколько источников информационного сигнала, например источник электромагнитного поля, источник огибающей речевого сигнала и т.д.

На уровень информационного сигнала влияют факторы, определяемые условием прохождения информационного сигнала внутри ТС и вне его, т.е. параметры среды распространения (СР) информационного сигнала.

Как и в обычном канале связи, в канале утечки информации действуют помехи, маскирующие информационный сигнал. Это мультипликативные (МП) и аддитивные (АП) помехи.

Для получения информации из канала злоумышленник должен использовать аппаратуру перехвата, которая в общем случае должна состоять из приемника, реализующего по тому или иному правилу выделения информационного сигнала, и регистрирующего устройства (РУ) — буквопечатающий аппарат, видеоконтрольное устройство, ухо человека и т.п.

Таким образом, обобщенная модель канала утечки информации состоит из источника информационного сигнала, среды распространения информационного сигнала, источников мультипликативных и аддитивных помех и аппаратуры перехвата

Критерии защиты информации от утечки по каналам ПЭМИН (741)

Одним из критериев защиты информации от утечки является обеспечение невозможности ее утечки более какого-то предела (процента от всего объема информации). Это могут быть допустимые величины разборчивости речевого сигнала, распознавания изображения сюжета телевизионного сигнала и т.д. С точки зрения злоумышленника информация — это то, что дает возможность ему получить какие-то новые сведения об объекте разведки.

Если рассматривать информацию по отношению к ТС, то она содержится во всем потоке сообщений, циркулирующих в нем (весь объем информации). Поэтому одной из задач при нормировании является определение именного допустимого процента от всего объема информации, утечка которого не приведет к потере сведений, т.е. определение смыслового критерия защиты.

Определение смыслового критерия защиты — сложная аналитическая задача для высококвалифицированных специалистов, знающих в целом проблему, информация о которой подлежит защите.

В общем случае смысловой критерий должен зависеть от грифа секретности информации, статуса (категории) объекта, где она циркулирует, заинтересованности предполагаемого злоумышленника в ее получении и т.п.

Для обобщенной модели канала утечки информации выполнение смыслового критерия защиты определяется по анализу результатов обработки сигналов, получае-

мых с регистрирующего устройства. Поэтому предельно допустимое отношение сигнал/помеха, являющееся энергетическим критерием защиты, должно быть определено на входе регистрирующего устройства, т.е. на выходе приемника.

Производить оценку защищенности информации от утечки по нормам на предельно допустимое отношение сигнал/помеха будет уже значительно легче, чем по смысловому критерию, так как эта оценка хотя и связана в некоторых случаях с необходимостью решения сложной радиотехнической задачи, может быть выполнена инженерно-техническими работниками.

Сложность решаемой задачи в этом случае заключается в моделировании технических возможностей предполагаемого а, т.е. в моделировании приемника аппаратуры перехвата, реализующего по тому или иному правилу оптимальное выделение информационного сигнала из смеси с помехой.

Дальнейшим упрощением задачи оценки защищенности информации от утечки является пересчет предельно допустимого отношения сигнал/помеха на вход приемника по разработанному алгоритму его работы. В общем случае алгоритм работы приемника должен определяться видом информации, видом (формой) информационного сигнала и параметрами помех на его входе. Тогда оценка защищенности информации от утечки по допустимому отношению сигнал/помеха на входе приемника аппаратуры перехвата сведется к объективным измерениям электрических величин параметров информационного сигнала и помехи.

Защита от утечки по каналам ПЭМИН (744)

К настоящему времени сложилась система защиты информационных объектов от утечки информации, включающая проведение организационных, организационно-технических, технических мероприятий и мероприятий по контролю за выполнением защиты.

В процессе организационных мероприятий определяют контролируемую территорию, в которой исключается неконтролируемое пребывание лиц, не имеющих допуска, выделяют из эксплуатируемых технических средств, выявляют наличие в контролируемой зоне ВТС, уточняют существующую кабельную разводку, обращая особое внимание на кабели, выходящие за пределы контролируемой зоны, составляют перечни выделенных помещений, предназначенных для проведения закрытых мероприятий (переговоров, обсуждений, бесед, совещаний и т.д.)

По результатам работ составляют протоколы обследований; обобщенные данные протоколов оформляют соответствующим актом. После завершения предусмотренных в акте работ проводят аттестацию выделенных помещений и составляют график периодических аттестационных проверок.

Организационно-технические мероприятия осуществляют путем блокирования возможных каналов утечки информации через действующие на объекте ТС с помощью отключения цепей и установки простейших схем и устройств защиты, демонтажа отдельных кабелей, выходящих за пределы контролируемой зоны, изъятий из выделенных помещений устройств ТС, применение которых может привести к утечке секретной информации; перемонтажа отдельных коммутационных устройств и оборудования систем, в том числе систем заземления и электропитания технических средств для внесения их в пределы контролируемой зоны. Этап завершается составлением инструкции по контролю защищенности технических средств и систем, смонтированных на объекте.

Требования к уровню защищенности объекта зависят от грифа секретности обрабатываемой информации и его дислокации, что учитывается при определении категории объекта и при проведении защитных мероприятий.

За отсутствием защищенных ТС проводят доработку технических средств, эксплуатируемых на объекте. Доработка не должна существенно ухудшать их эксп-

Организационно-технические мероприятия осуществляют путем блокирования...

луатационные параметры. Если сигналы в выходящих за пределы контролируемой территории кабелях превышают допустимые величины, применяют буферные и отключающие устройства; ограничителями малых амплитуд осуществляют фильтрацию цепей.

Иногда для блокирования сигналов в цепях электропитания ТС применяют мотор-генераторы, которые в данном случае выполняют роль механического фильтра.

Мероприятия по контролю заключаются в проверке специальных параметров защитных ТС, исправности эксплуатируемых средств и устройств защиты.

Как известно, при проведении защитных мероприятий используют пассивные и активные методы защиты. Методы защиты, направленные на снижение уровня информационного сигнала до величины, при которой они маскируются естественными шумами, относятся к пассивным; методы, направленные на преднамеренное увеличение уровня помехи в техническом канале, — к активным.

Рассмотрим требования, предъявляемые к зашумляющим сигналам. При определении оптимальных параметров шума рассматривают две группы критериев — информационные и энергетические.

Сначала по информационным критериям обеспечивают самое высокое качество помехового сигнала, затем выбирают его параметры, при которых обеспечивается зашумление информации при наименьшей мощности шума.

Идеальные маскирующие помеховые сигналы должны создавать такие условия, при которых апостериорная вероятность опознавания была бы равна нулю при максимальной априорной вероятности наличия сигнала с известными параметрами. Это исключает возможность применения для цепей маскировки детерминированных помеховых сигналов, так как они легко распознаются, а поэтому не могут увеличить неопределенность в системе.

Поскольку детерминированные помеховые сигналы обладают низкими потенциальными возможностями маскировки, их можно устранить сравнительно простыми техническими приемами. Маскирующие помеховые сигналы должны содержать элемент неопределенности.

Мерой неопределенности случайных величин или случайного процесса является энтропия. При прочих равных условиях среды маскирующих помеховых сигналов (шумов) лучшим является тот, энтропия которого больше. Шум, создаваемый реальными источниками, имеет ограничения как по максимально достижимым значениям, так и по средней мощности (дисперсии). Следовательно, из всех ограниченных сверху и снизу шумов, представленных одномерным распределением, максимальную энтропию имеет тот, у которого плотность распределения вероятности является равномерной.

В реальных условиях шумовое напряжение ограничено как по средней мощности, так и по максимальным вопросам, в результате чего оптимальное распределение будет отличаться от равномерного и от гауссова. Чтобы обеспечить маскирование при наименьшей мощности шума, параметры маскирующего шума выбирают с учетом параметра защищаемых сигналов. Сигналы, циркулирующие в технических средствах, имеют ограниченный спектр, поэтому для их зашумления энергетически целесообразно выбирать зашумляющие сигналы, лежащие в той же области частот.

Следует также учитывать, что статистические параметры информационного сигнала известны злоумышленнику и он может применять приемные устройства с оптимальным фильтром. Исходя из этого необходимо, чтобы шум также прошел оптимальную обработку. Самым сильным маскирующим эффектом при наименьшей мощности шумового генератора будет обладать шум со спектром, повторяющим спектр зашумляемого сигнала.

Еще больший выигрыш обеспечивается при зашумлении телевизионных сигналов шумом, прошедшим оптимальную обработку. Основная доля энергии видеосигнала заключена в строчной структуре, поэтому оптимальным устройством для обнаружения видеосигнала в шумах будет устройство, имеющее передаточную характеристику, определяемую спектром последовательности строчных гасящих импульсов. Применение для активной защиты помехового сигнала, имеющего нормальный закон распределения в видимой части строки и распределение спектральной плотности, подобное строчной структуре защищаемого видеосигнала обеспечивает выигрыш в энергии более чем в 20 раз по сравнению с применением для этой цели квазибелого шума.

С учетом рассмотренных требований к шуму структурная схема устройства зашумления должна состоять из последовательно соединенных генераторов шума, узла формирования шума с требуемой спектральной характеристикой, усилителя и узла сопряжения с нагрузкой.

Оценка защищенности информации от утечки по каналам ПЭМИН (740)

Завершающим этапом в процессе оценки защищенности информации от утечки является проверка на соответствие параметров информационных сигналов, создаваемых различными техническими средствами, разработанным нормам и, следовательно, проверка эффективности защиты информации от утечки.

В настоящее время при проведении указанной проверки выполняются:

- специальные исследования, охватывающие широкий круг теоретических и экспериментальных работ, конечной целью которых является обеспечение защищенности информации от утечки для конкретных технических средств и систем;
- контроль эффективности защиты информации от утечки, т.е. проверка на соответствие нормам параметров информационных сигналов, создаваемых определенными защищенными техническими средствами и совокупностью таких средств, размещенных на объекте.

Цели и задачи специальных исследований и контроля эффективности мер противодействия (740)

Одним из важных путей повышения эффективности противодействия перехвату информации является проведение специальных исследований и контроля защищенности информации, циркулирующей на объекте, от утечки и правильного и своевременного выполнения мероприятий по ее защите. Такие работы включают в себя процесс получения и обработки информации о состоянии объекта наблюдения, в сравнении ее с предъявленными к нему требованиями и обеспечивают принятие решений или выдачу управляющих воздействий.

Следует отметить, что технический контроль принятых мер противодействия перехвату информации отличается некоторыми особенностями. Это объясняется тем, что перехват ПЭМИН занимает особое место среди других видов информационных технических разведок, так как для получения сведений ею используется перехват информации за счет побочных процессов, которые лишь сопутствуют нормальной работе технических средств и представляют собой паразитные явления по отношению к его основным функциям.

Процессы эти часто не оказывают заметного негативного влияния на работу технического средства в целом и, как правило, не являются предметом пристального внимания разработчиков аппаратуры широкого назначения.

Поэтому без результатов контроля соответствия технических средств специальным требованиям и нормам невозможно принять правильное решение о достаточности принимаемых мер для защиты информации от утечки или найти оптимальное решение с целью исключения имеющих место недостатков.

Это важно

Происходящие в техническом средстве побочные процессы и их влияние на возможности предполагаемого а бывают столь сложными и неявными, что иногда для выявления необходимых для контроля параметров и функциональных зависимостей между ними приходится выполнять значительные теоретические и экспериментальные исследования.

Такие исследования защищенности информации, называемые часто специальными исследованиями, заключаются в получении и использовании более полной как в количественном, так и в качественном отношении информации об объекте наблюдения и разработке при необходимости рекомендаций по защите информации от утечки.

Комплекс исследований, направленный на определение эффективности проведенных работ по защите информации от утечки за счет побочных электромагнитных излучений и технических средств, размещенных на объекте, называется *контролем*.

Под эффективностью защиты понимается способность технического средства к выполнению определенных функций, которая характеризуется некоторыми параметрами, заданными нормативно-технической документацией. Если величины этих параметров соответствуют установленным для них нормам, то изделие считается защищенным; если хотя бы один параметр не соответствует нормам, то изделие считается незащищенным.

Мероприятия по контролю могут выполнятся на всех этапах изготовления и эксплуатации аппаратуры.

Основными задачами контроля являются:

- определение состояния защищенности от утечки и, в частности, работоспособности средств защиты;
- поиск неисправностей;
- выработка рекомендаций по устранению выявленных нарушений и недостатков, анализ причин их появления и проверка их устранения.

Специальные исследования создаваемой техники могут быть составной частью предварительных и государственных испытаний и заключаются в выявлении специальных параметров технических средств, необходимых для проверки защищенности информации от утечки на всех этапах жизненного цикла изделия, в разработке и выдаче рекомендаций по блокированию каналов утечки информации, выдаче заключения о соответствии технического средства и эксплуатационно-технической документации на него, требованиям технического задания по защите информации от утечки.

Резюме

Наибольшую опасность с точки зрения утечки информации представляют побочные (паразитные, непреднамеренные) излучения технических средств, участвующих в процессе передачи, обработки и хранения секретной информации.

Под утечкой информации понимается возможность доступа к информации в замкнутой, охраняемой системе управления, осуществляемого путем перехвата и соответствующей обработки побочных (паразитных, непреднамеренных) излучений технических средств передачи информации, используемых в указанной системе для сбора, обработки, хранения и обмена информацией.

Канал утечки информации включает в себя технические средства передачи, обработки или хранения секретной информации, среду распространения паразитных электромагнитных или других излучений и средство перехвата и первичной обработки побочных (паразитных) излучений.

Контролируемая зона включает в себя пространство вокруг технических средств (ТС), в пределах которого исключается неконтролируемое пребывание посторонних лиц, транспортных средств и других посторонних объектов, не имеющих постоянного или разового допуска.

В процессе функционирования средств вычислительной техники в конструктивных элементах и кабельных соединениях циркулируют электрические токи информативных сигналов, в результате чего формируются электромагнитные поля, уровни которых могут быть достаточными для приема сигналов и извлечения информации с помощью специальной аппаратуры.

Каналы утечки информации могут возникать вследствие излучения информативных сигналов при работе ТС и вследствие наведения этих сигналов в линиях связи, цепях электропитания и заземления, других коммуникациях, имеющих выход за пределы контролируемой территории. Информативные сигналы могут распространяться на большие расстояния и регистрироваться средствами технических разведок за пределами КТ.

На этапе проведения организационных мероприятий необходимо:

- определить перечень сведений, подлежащих технической защите (определяет собственник информации в соответствии с действующим законодательством Украины);
- обосновать необходимость разработки и реализации защитных мероприятий с учетом материального или иного ущерба, который может быть нанесен вследствие возможного нарушения целостности информации либо ее утечки по техническим каналам;
- установить перечень выделенных помещений, в которых не допускается реализация угроз и утечка информации с ограниченным доступом;
- определить перечень технических средств, которые должны использоваться как ТС;
- определить технические средства, применение которых не обосновано служебной и производственной необходимостью и которые подлежат демонтажу;
- определить наличие используемых и неиспользуемых воздушных, наземных, настенных и скрытых кабелей, цепей и проводов, уходящих за пределы выделенных помещений;
- определить системы, подлежащие демонтажу, требующие переоборудования кабельных сетей, цепей питания, заземления или установки в них защитных устройств.

К средствам технической защиты относятся:

- фильтры-ограничители и специальные абонентские устройства защиты для блокирования утечки речевой информации через двухпроводные линии телефонной связи, системы директорской и диспетчерской связи;
- устройства защиты абонентских однопрограммных громкоговорителей для блокирования утечки речевой информации через радиотрансляционные линии;
- фильтры сетевые для блокирования утечки речевой информации по цепям электропитания переменного (постоянного) тока;
- фильтры защиты линейные (высокочастотные) для установки в линиях аппаратов телеграфной (телекодовой) связи;
- генераторы линейного зашумления;
- генераторы пространственного зашумления;
- экранированные камеры специальной разработки.

Наиболее эффективно гальваническую и электромагнитную развязку кабелей электропитания ТС ЭВТ от промышленной сети обеспечивает их разделительная система типа “электродвигатель-генератор”. Электропитание допускается также осуществлять через помехоподавляющие фильтры.

Информация, отображенная на экране дисплея, может быть восстановлена с помощью ТВ-приемника. Он обрабатывает лишь небольшую часть спектра шириной около 8 МГц на частотах в диапазонах метровых и дециметровых волн.

К настоящему времени сложилась система защиты информационных объектов от утечки информации, включающая проведение организационных, организационно-технических, технических мероприятий и мероприятий по контролю за выполнением защиты.