Л. А. Шивдяков (к. в. н.)
ФСТЭК России, г. Хабаровск

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КЛЮЧЕВЫХ СИСТЕМАХ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ОРГАНОВ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ. МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В КСИИ.

(Продолжение статьи, опубликованной в №3, 2008)

2. Модель угроз безопасности информации в КСИИ

Как правило, для качественного определения мер защиты необходимо знать, «от кого защищать», т. е. выявить все возможные угрозы. Типовая модель угроз безопасности в КСИИ представлена в документах ФСТЭК России, утвержденных 18 мая 2007 г. заместителем директора ФСТЭК России.

Модель угроз безопасности информации в КСИИ содержит систематизированные сведения о возможных угрозах безопасности информации на типовых объектах информатизации (автоматизированных системах, созданных на базе средств вычислительной техники (СВТ), автономных или подключаемых к другим вычислительным сетям, помещениях со средствами автоматизации и связи и т. п.).

Модель угроз безопасности информации в КСИИ разрабатывалась с учетом современных тенденций развития СВТ и компьютерных сетей, технологий промышленного шпионажа.

Документами вводится понятие **безопасности информации** (БИ) — это состояние информации, информационных ресурсов и информационных систем, при котором с **требуемой вероятностью** обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т. п.

Под **угрозой безопасности информации** понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее.

Последствием реализации угрозы может быть нарушение конфиденциальности, целостности или доступности информации.

К защищаемой относится информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. **Собственником информации** может быть государство, юридическое лицо, группа физических лиц, отдельное физическое лицо. К защищаемой информации, для которой определяются угрозы безопасности, могут относиться данные (сведения) собственника или пользователя информации, технологическая (служебная) информация, обеспечивающая функционирование аппаратных и программных средств на объекте информатизации (в том числе системное и/или прикладное программное обеспечение).

Несанкционированный доступ — это доступ с нарушением установленных прав или правил. Несанкционированный доступ к информации может осуществляться:

· в помещение, где производится обработка защищаемой информации;

· к аппаратуре, где обрабатывается защищаемая информация;

· к носителю защищаемой информации;

· к программной среде (к командам, драйверам, утилитам в составе системного или прикладного программного обеспечения);

· к собственно информации пользователя (владельца).

Каналы утечки информации в результате несанкционированного доступа к ней определяются как **каналы несанкционированного доступа**.

Каналы добывания защищаемой информации разведками иностранных государств или криминальными (террористическими) организациями с использованием технических (не программных) средств определяются как **технические каналы утечки информации** (ТКУИ).

КСИИ представляют собой совокупность объектов информатизации **(ОИ)**. Под **ОИ** понимается совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией; совокупность средств обеспечения ОИ, а также помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

К **техническим средствам обработки защищаемой информации**, входящим в состав ОИ, относятся:

— автоматизированные системы (АС) различного назначения;

— технические средства обработки и передачи информации (ТСОИ), не относящиеся к АС.

АС, размещенные на ОИ, могут быть представлены в виде автономных автоматизированных рабочих мест (АРМ) на базе ПЭВМ, локальных вычислительных сетей, распределенных («ведомственных», «корпоративных») вычислительных сетей.

К ТСОИ относятся также различные системы и средства защищенной или служебной связи, системы и средства звукозаписи и звуковоспроизведения, системы и средства телевизионного и видеооборудования, средства изготовления и размножения (печати) документов, проекционные средства и системы.

АС и ТСОИ, предназначенные для обработки защищаемой информации, относятся к **основным техническим средствам и системам** (ОТСС).

АС и ТСОИ, не предназначенные для обработки защищаемой информации, но размещаемые вместе с ОТСС, относятся к **вспомогательным техническим средствам и системам** (ВТСС).

К средствам обеспечения ОИ относятся средства и системы часофикации, охранной и пожарной сигнализации, а также технические средства, размещаемые на ОИ, но не предназначенные для обработки информации и входящие в состав систем заземления, электропитания, кондиционирования, тепло- и водоснабжения и т. п.

ОТСС размещаются в помещениях ОИ. Помещения (служебные кабинеты, актовые, конференц-залы и т. д.), специально предназначенные для обсуждения или обработки защищаемой информации, называются защищаемые помещения (ЗП). Каждое из помещений ОИ, в зависимости от его назначения и условий расположения, имеет определенный набор средств обеспечения.

Защищаемая информация, хранящаяся, обрабатываемая (циркулирующая) на ОИ, подразделяется на следующие виды:

— ***речевая*** (акустическая) информация, источниками которой являются должностные лица ОИ и звуковоспроизводящие устройства, а первичными носителями — акустические колебания в воздушной среде ОИ;

— ***графическая*** (видовая) информация, представленная в виде текста и изображений (рисунков, схем, фотографий и др.) на различных носителях (бумажных документах, плакатах, экранах и демонстрационных устройствах);

— ***информация***, обрабатываемая (циркулирующая) в ТСОИ и АС ***в виде электрических и оптических сигналов*** и распространяющаяся от них в виде побочных электромагнитных излучений (ПЭМИ);

— ***информация***, обрабатываемая (циркулирующая) непосредственно в АС, представленная ***в виде файлов и файловых систем, каталогов, баз и хранилищ данных, записей и их полей в программных документах***.

При этом к носителям защищаемой информации относятся:

— **первичные носители**, которые непосредственно содержат защищаемую информацию;

— **вторичные носители**, воспроизводящие (отражающие) защищаемую информацию в своих характеристиках и/или параметрах своих физических полей в результате каких-либо преобразований (акустических, акустоэлектрических и т. д.).

К первичным носителям защищаемой информации относятся:

для распространяющейся защищаемой речевой (акустической) информации:

1) должностные лица ОИ;

2) звуковоспроизводящие устройства, входящие в состав ОТСС. В ТСОИ — это динамики радиоприемных и телевизионных устройств, магнитофонов (диктофонов) или других аудиосистем, громкоговорители (спикерфоны) телефонных аппаратов и других средств защищенной связи. В АС — звуковые колонки или встроенные динамики мониторов;

для графической (видовой) информации:

1) экраны мониторов АС, телевизионной и видеоаппаратуры ОИ, воспроизводящие защищаемую информацию;

2) экраны демонстрационной и проекционной аппаратуры, используемой на ОИ в период проведения закрытых мероприятий;

3) носители на бумажной основе — документы, содержащие защищаемую информацию (книги, плакаты, схемы, чертежи и т. д.);

для защищаемой информации, циркулирующей в ОТСС (в ТСОИ и аппаратных средствах АС):

источники ПЭМИ в ТСОИ:

1) средства защищенных видов связи (телефонной и радиосвязи) и их соединительные линии;

2) средства звукозаписи, звукоусиления и звуковоспроизведения и их соединительные линии;

3) средства телевизионного и видеооборудования, их соединительные линии и линии передачи данных;

4) средства изготовления и размножения документов;

источники ПЭМИ в АС:

1) мониторы;

2) системные блоки ПЭВМ;

3) коммутационное оборудование и средства передачи данных;

4) соединительные линии (кабели), линии передачи данных;

носители фиксированной защищаемой информации:

1) на магнитной основе (гибкие магнитные диски, съемные винчестеры, кассетные жесткие диски, носители накопителей ZIP, USB-drive, аудио- и видеокассеты, магнитные ленты и т. п.);

2) на «оптической» основе (оптические компакт-диски (CD) — CD-R (Compact Disk Recordable), CD-RW (Compact Disk Rewritable), DVD — универсальные цифровые видеодиски).

Вторичными носителями, воспроизводящими преобразованную защищаемую информацию, являются:

для речевой (акустической) информации:

1) акустические колебания в воздушной среде ОИ и за его пределами;

2) вибрационные колебания материалов ограждающих конструкций помещений ОИ (оконных стекол, стен, плит перекрытия, дверных блоков и т. д.) и выходящих за их пределы инженерных коммуникаций;

3) электрические информативные сигналы в токопроводящих цепях ОИ, создаваемые в результате акустоэлектрических преобразований;

4) собственные побочные электромагнитные излучения ОТСС и ВТСС ОИ, модулированные речевыми (акустическими) сигналами, создаваемые в результате акустоэлектромагнитных преобразований;

5) электромагнитные излучения внешних источников, модулированные речевыми (акустическими) сигналами, т. е. создаваемые в результате акустоэлектромагнитных и акустооптических преобразований;

для графической (видовой) информации:

1) отраженное первичными носителями информации излучение в видимом и/или в инфракрасном (ИК) диапазоне;

2) собственные излучения таких первичных носителей информации, как электронно-лучевые, жидкокристаллические, плазменные и др. экраны и табло;

для информации, циркулирующей в ОТСС:

1) модулированные информативным сигналом ПЭМИ ВТСС и средств обеспечения ОИ;

2) наведенные ПЭМИ ОТСС электрические сигналы (наводки) в токопроводящих цепях ОТСС, ВТСС и/или средств обеспечения ОИ;

3) отраженные от элементов ОТСС электромагнитные излучения внешнего облучающего источника, модулированные информативными сигналами ОТСС.

По фактору, обусловливающему возможность возникновения угрозы, выделяются три основных вида угроз:

природные (стихийные);

техногенные;

антропогенные.

*К **природным*** угрозам относятся различные природные или физические явления (наводнения, землетрясения, пожары и т. п.), способные привести к нарушению безопасности информации.

*К **техногенным*** относятся угрозы, возникающие в процессе функционирования технических средств, способные вызвать нарушение безопасности информации. Среди техногенных угроз следует выделить два класса: *угрозы случайного помехового воздействия*, связанные с воздействием физических полей, источниками которых являются функционирующие технические средства (входящие в состав объекта информатизации или не входящие в его состав); *угрозы сбоя*, обусловленные дефектами, отказами технических средств или программного обеспечения ОИ.

*К **антропогенным*** угрозам относятся угрозы, возникающие в результате непреднамеренных или умышленных действий людей, способные привести к нарушению безопасности информации.

Непреднамеренные антропогенные угрозы, в свою очередь, разделяются на угрозы, *обусловленные неправильной организацией защиты информации на ОИ* и *ошибками персонала ОИ*. Преднамеренные антропогенные угрозы включают в себя угрозы, возникающие в результате преднамеренных деструктивных действий физических лиц или спецслужб и связанные с диверсионной деятельностью, несанкционированным доступом к информации, с ведением разведки, умышленным воздействием на ОИ по физическим полям.

По источнику угрозы все угрозы разделяются на внешние и внутренние. Под **источником угрозы** понимается субъект, материальный объект или физическое явление, физическое поле, создающее угрозы безопасности информации. Источники угроз безопасности информации разделяют на ***внешние*** и ***внутренние***. Под ***внешними источниками*** понимаются органы и подразделения разведок иностранных государств, криминальных структур, физические лица, не относящиеся к персоналу объекта информатизации, деятельность которых направлена на

нанесение ущерба безопасности информации, а также материальные объекты или физические явления, функционирование или существование которых создает опасность для информации. В отличие от внешнего источника ***внутренний источник угрозы*** безопасности информации — это субъект в составе объекта информатизации, деятельность которого наносит или может нанести ущерб безопасности информации.

По виду нарушения безопасности информации угрозы разделяются на:

· приводящие к нарушению доступности;

· приводящие к нарушению целостности;

· приводящие к нарушению конфиденциальности.

По объекту воздействия угрозы безопасности могут быть направлены на:

· информацию, которой оперирует персонал объекта информатизации;

· информацию, обрабатываемую или хранимую техническими средствами (аппаратурой в составе ОИ);

· информацию, передаваемую по линиям передачи данных.

По характеру воздействия на защищаемую информацию различают угрозы:

· утечки (хищения, разглашения);

· утраты (уничтожения);

· модификации (несанкционированное внесение изменений);

· блокирования.

По способу реализации угрозы разделяют на:

· угрозы утечки по техническим каналам;

· угрозы, связанные с НСД (угрозы НСД), в том числе угрозы программно-математического воздействия на информацию (угрозы ПМВ).

Угрозы утечки по техническим каналам в зависимости от типа информации можно разделить на три группы:

· угрозы утечки речевой (акустической) информации;

· угрозы утечки графической (видовой) информации;

· угрозы утечки информации за счет ПЭМИН.

Угрозы НСД с использованием программного обеспечения, в свою очередь, разделяются:

· по признаку удаленности субъекта от объекта доступа:

· на угрозы удаленных атак;

· на угрозы непосредственного НСД;

· по используемой ошибке:

· на угрозы, обусловленные

· неадекватностью принятых мер защиты;

· ошибками в программном обеспечении;

· ошибками пользователя;

· ошибками технического обслуживания.

По содержанию деструктивного действия угрозы НСД с применением программного обеспечения дополнительно разделяются на:

· угрозы копирования информации (хищения, ознакомления с информацией);

· угрозы ПМВ.

При этом угрозы ПМВ разделяются на угрозы модификации (подмены) данных, уничтожения информации и/или программного обеспечения, отвечающего за организацию и управление информационными процессами, блокирование информационных процессов и/или доступ авторизованных пользователей к защищаемым информационным ресурсам и службам (сервисам) информационных сетей и т. д.

Угрозы, реализуемые без использования программного обеспечения (угрозы физического НСД к носителям информации, СВТ, элементам АС), разделяются по содержанию деструктивного действия на:

· угрозы кражи носителей и элементов оборудования;

· их подмену и/или физическое разрушение.

Угрозы непосредственного НСД к информации с использованием программного обеспечения — это угрозы, реализуемые субъектом на отдельном СВТ (отдельной ПЭВМ), отдельном АРМ без привлечения сетевых технологий. Эти угрозы разделяются по составу привлекаемого программного обеспечения на угрозы, реализуемые с применением специально разработанных для обеспечения доступа программ, и на угрозы, реализуемые с использованием системного программного обеспечения или прикладных программ общего пользования.

Угрозы удаленного доступа к информации — это угрозы доступа, реализуемые с применением сетевых технологий, т. е. угрозы сетевых атак. Под сетевой атакой понимается совокупность действий нарушителя, направленных на получение несанкционированного доступа к информационным или аппаратным ресурсам сети и реализуемых с использованием телекоммуникационной среды. Угрозы удаленного доступа к информации (угрозы сетевых атак) становятся угрозами безопасности информации, если они увязываются с определенными деструктивными действиями по отношению к защищаемой информации. Таким образом, угроза безопасности информации в данном случае включает в себя угрозу сетевой атаки и угрозу выполнения того или иного деструктивного действия с информацией.

Рассмотрим основные технические каналы утечки информации для каждого вида ОИ (ЗП, ОВТ).

Угрозы утечки речевой (акустической) информации по техническим каналам. Под **акустической** понимается информация, содержащаяся непосредственно в произносимой либо воспроизводимой речи (речевая информация), добываемая с использованием аппаратуры, регистрирующей акустические (в воздухе) и виброакустические (в упругих средах) волны, а также электромагнитные излучения и электрические сигналы, возникающие за счет акустоэлектрических преобразований в различных технических средствах под воздействием акустических волн. Восстанавливаемая нарушителем речь анализируется с целью выявления в ней конфиденциальной информации.

Для перехвата защищаемой речевой информации могут использоваться автономные закладочные устройства, портативные (носимые), возимые и стационарные средства.

Перехваченная закладочными устройствами речевая информация передается по радиоканалу, оптическому каналу (в инфракрасном диапазоне длин волн), по линиям выходящей за пределы ОИ связи, по линиям электропитания ОИ, по другим токопроводящим цепям и конструкциям (соединительным линиям ВТСС, посторонним проводникам — трубам водоснабжения и канализации, металлоконструкциям и т. п.).

Носимая аппаратура применяется для ведения перехвата в заранее определенные интервалы времени путем регистрации звуков и речи (на служебных совещаниях и т. д.) лицами, имеющими доступ на территорию организации, обслуживающей ОИ, или непосредственно на территорию ОИ. Перехват речевой информации осуществляется в выделенных помещениях (ВП) либо в непосредственной близости к нему (из смежных помещений, из коридора, извне здания). При этом средства перехвата маскируются в одежде, носимых предметах (в портфеле, сумке и т. д.). Аппаратура перехвата, как правило, представлена диктофонами (магнитофонами), работающими в автоматическом режиме. Перехваченные речевые сообщения регистрируются на магнитных или электронных носителях. Возможна одновременная передача перехваченной информации по специальному радиоканалу. Энергопитание аппаратуры производится от встроенных источников (аккумуляторных батарей).

Возимая аппаратура перехвата устанавливается на автомобилях или на других механических подвижных средствах и используется при незначительных размерах контроллируемой зоны (КЗ) ОИ и возможности парковки транспортного средства с аппаратурой в непосредственной близости от помещения ОИ. Управление возимой аппаратурой осуществляется вручную (непосредственно из автомобиля) или дистанционно.

Стационарная аппаратура устанавливается в помещении (в кабинете, в квартире; в подвале; на чердаке здания и т. п.) и используется для постоянного ведения перехвата речевой информации в непосредственной близости к ОИ (в одном здании, в рядом расположенных зданиях и т. п.). Управление стационарной аппаратурой осуществляется вручную или дистанционно.

Угрозы перехвата защищаемой графической (видовой) информации по техническим каналам. Перехват (просмотр) защищаемой графической (видовой) информации осуществляется посторонними лицами путем ее непосредственного наблюдения при НСД в помещение ОИ либо на расстоянии прямой видимости из-за пределов ОИ с использованием оптических (оптико-электронных) средств.

Для перехвата защищаемой графической (видовой) информации могут использоваться следующие виды портативных (носимых), возимых и стационарных средства перехвата графической (видовой) информации:

— оптические средства и системы, позволяющие увеличить дальность наблюдения (бинокли, телескопы, зрительные трубы и т. п.);

— аппаратура, позволяющая расширить диапазон приема (спектральную чувствительность), — приборы ночного видения и источники ИК-подсветки (облучения объекта наблюдения ИК-лучами);

— устройства регистрации изображений (фотоаппараты, блоки электронной (цифровой) памяти фото-, теле- и видеооборудования).

Если доступ в помещение контролируется, но имеется возможность его посещения техническим персоналом (электрики, уборщицы и т. п.), не исключена установка видеосистем, закамуфлированных под находящиеся в помещении предметы, например книгу или настольные часы. Такие системы имеют непродолжительное время работы и устанавливаются, как правило, для видеозаписи отдельных мероприятий (например, совещания). Миниатюрные камеры можно скрытно установить практически в любом месте, например в бамбуковом стержне, воткнутом в цветочный горшок и используемом для подвязки комнатного растения (видеомагнитофон или видеопередатчик устанавливается непосредственно в цветочном горшке), или в автомобильной антенне.

Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок. К угрозам утечки защищаемой информации в ОТСС по ТКУИ относятся:

— угрозы утечки защищаемой информации по каналам побочных электромагнитных излучений ОТСС;

— угрозы утечки защищаемой информации по каналам электрических наводок, возникающим в токопроводящих цепях ОТСС.

ТКУИ по ПЭМИ возникают в результате излучений гармоник следующих элементов ОТСС:

— имеющих в своем составе ВЧ-генераторы (процессор, материнская плата ЭВМ и др.);

— низкочастотных (НЧ) усилителей звуковых колонок (динамиков) на частотах их самовозбуждения;

— генератора развертки электронно-лучевой трубки монитора ЭВМ;

— соединительных элементов (разъемов, портов) системного блока и периферийных устройств ЭВМ.

ТКУИ по ПЭМИ возникают также в результате модуляции информативными сигналами внешнего облучающего излучения (метод ВЧ-навязывания), воздействующего на нелинейные элементы ОТСС.

Прием сигналов ПЭМИ осуществляется радио- и радиотехническими средствами перехвата, размещенными вне КЗ, или специальными закладочными устройствами.

ТКУИ в ОТСС возникают также в результате преобразования ПЭМИ элементов ОТСС, содержащих информативные сигналы, в электрические наводки в следующих токопроводящих цепях, выходящих за пределы помещения ОИ и/или за пределы КЗ:

— в соединительных линиях блоков и устройств, входящих в состав ОТСС;

— в линиях ВТСС (средств служебной связи и др.);

— в линиях средств обеспечения ОИ;

— в шинах заземления ОИ;

— в линиях электропитания ОТСС и помещения ОИ;

— в токопроводящих проводниках инженерных коммуникаций ОИ.

Прием информативных электрических сигналов, наводимых в токопроводящих цепях, осуществляется путем непосредственного подключения приемных устройств к данным линиям, размещенным вне помещения ОИ и/или выходящим за пределы КЗ ОИ.

В состав технических средств обработки и передачи защищаемой информации, размещенных на типовом объекте информатизации и не относящихся к средствам вычислительной техники и автоматизированным системам, входят:

— средства и системы защищенных видов связи (проводные, беспроводные);

— средства и системы звукоусиления, звукозаписи и звуковоспроизведения защищаемой информации;

— электронные демонстрационные системы для воспроизведения защищаемой информации;

— средства и системы телевизионного и видеооборудования;

— средства изготовления и размножения документов.

К средствам и системам защищенных видов связи относятся:

— использующие метод аналогового скремблирования;

— осуществляющие дискретизацию речевого сигнала с последующим шифрованием.

К защищаемой информации в ТСОИ систем защищенных видов связи относятся речевая информация и электрические информативные сигналы, передаваемые по каналам связи.

К угрозам безопасности информации, представленной электрическими информативными сигналами, относятся угрозы возникновения ПЭМИ от телефонных аппаратов (самовозбуждение НЧ-усилителей), просачивания и наводок электрических информативных сигналов в токопроводящие цепи самих ОТСС, наводок в цепи других технических средств ОИ (ВТСС и средств обеспечения) в результате магнитных, емкостных и/или индуктивных связей при совместном прохождении соединительных линий.

К средствам и системам телевизионного и видеооборудования, обрабатывающим защищаемую информацию, относятся:

— средства регистрации речевой информации (микрофоны);

— средства регистрации изображений (графической информации) — оптические системы теле- и видеокамер;

— средства записи защищаемой информации (цифровые и аналоговые магнитофоны, устройства магнитной записи и блоки памяти видеомагнитофонов и видеокамер и т. п.);

— средства отображения графической информации (мониторы, экраны телевизионных приемников, демонстрационные устройства и т. п.);

— средства отображения акустической информации (звукоусилительные и звуковоспроизводящие устройства — НЧ-усилители и звуковые колонки соответственно);

— соединительные линии и линии передачи информации (для ОИ, расположенных в разных помещениях).

К защищаемой информации в ТСОИ систем телевизионного и видеооборудования относится акустическая информация, графическая (видовая) информация и электрические информативные сигналы, передаваемые по их соединительным линиям.

К средствам и системам изготовления и размножения документов, обрабатывающим защищаемую информацию, относятся:

— средства изготовления и размножения защищаемой аудиоинформации (студии звукозаписи и т. п.);

— средства изготовления и размножения защищаемой видеоинформации (кино- и телестудии);

— средства изготовления и размножения защищаемой графической информации, представленной на бумажных носителях (типографии, множительные аппараты — ксероксы и т. п.).

К защищаемой информации в ТСОИ систем и средств изготовления и размножения документов относятся акустическая информация и графическая (видовая) информация.

Перехват защищаемой информации, циркулирующей в ОТСС объекта информатизации, возможен по ТКУИ.

Прием сигналов ПЭМИ осуществляется ВЧ и НЧ радиоприемными устройствами и радио- и радиотехническими средствами перехвата, размещаемыми за пределами контролируемой зоны ОИ.

Прием информации, передаваемой закладочными устройствами, может осуществляться на специальные приемные устройства, работающие в соответствующем диапазоне длин волн.

Перехваченная с помощью закладочных устройств информация или непосредственно передается по радиоканалу, или записывается на специальное запоминающее устройство, а передается на запросивший ее объект по специальной команде.

Электромагнитные излучения элементов ОТСС обусловлены тем, что при прохождении электрического тока, параметры которого изменяются по закону информационного сигнала, по токоведущим элементам ОТСС вокруг них в окружающем пространстве возникают электрическое и магнитное поля. В силу этого элементы ОТСС можно рассматривать как излучатели электромагнитного поля, модулированного по закону изменения информационного сигнала.

Электромагнитные излучения на частотах работы высокочастотных генераторов в составе ОТСС и ВТСС (задающих генераторов, генераторов тактовой частоты, генераторов стирания и подмагничивания магнитофонов, гетеродинов радиоприемных и телевизионных устройств, генераторов измерительных приборов и т. д.) обусловлены наведением информационных сигналов на элементы генераторов. Наведенные электрические сигналы могут вызвать непреднамеренную модуляцию собственных колебаний генераторов. Эти промодулированные высокочастотные колебания излучаются в окружающее пространство.

Электромагнитные излучения на частотах самовозбуждения усилителей ОТСС (систем звукоусиления и звукового сопровождения, магнитофонов, систем громкоговорящей связи и т. п.) возникают за счет случайных преобразований отрицательных обратных связей в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов. Сигнал на частотах самовозбуждения, как правило, оказывается промодулированным информационным сигналом. Это наблюдается в основном при переводе усилителя низкой частоты (УНЧ) в нелинейный режим работы, т. е. в режим перегрузки.

Технические каналы утечки информации, обусловленные наводками, образуются за счет соединительных линий ОТСС, ВТСС и посторонних проводников (в том числе цепей электропитания и заземления).

Наводки электромагнитных излучений ОТСС возникают при излучении элементами ОТСС информационных сигналов при наличии емкостной, индуктивной или гальванической связи соединительных линий ОТСС, линий ВТСС и посторонних проводников. В результате на случайных антеннах (цепях ВТСС или посторонних проводниках) наводится информационный сигнал.

Прохождение информационных сигналов в цепи электропитания возможно при наличии емкостной, индуктивной или гальванической связи источника информационных сигналов в составе аппаратуры ОТСС и цепей питания. Информационный сигнал может проникнуть в цепи электропитания также в результате того, что среднее значение потребляемого тока в оконечных каскадах усилителей в большей или меньшей степени зависит от амплитуды информационного сигнала, что создает неравномерную нагрузку на выпрямитель и приводит к изменению потребляемого тока по закону изменения информационного сигнала.

Прохождение информационных сигналов в цепи заземления обусловлено наличием емкостной, индуктивной или гальванической связи источника информационных сигналов в составе аппаратуры ОТСС и цепей заземления. При этом кроме заземляющих проводников, служащих для непосредственного соединения ОТСС с контуром заземления, гальваническую связь с данным контуром могут иметь различные проводники, выходящие за пределы контролируемой зоны (нулевой провод сети электропитания, экраны соединительных кабелей, металлические трубы систем отопления и водоснабжения). Все эти проводники совместно с заземляющим устройством образуют разветвленную систему заземления, на которую могут наводиться информационные сигналы.

Перехват информационных сигналов по электрическим каналам утечки информации возможен с применением специальных емкостных или индукционных съемников, а также путем непосредственного подключения к соединительным линиям ВТСС и посторонним проводникам, проходящим через помещения, где установлены ОТСС, к их системам электропитания и заземления.

Параметрический канал утечки информации возникает в результате высокочастотного облучения элементов технических средств передачи информации (ТСПИ), в которых производится обработка информационных сигналов. В результате нелинейных явлений возникает угроза утечки информации (образуются каналы утечки информации на частоте облучающего сигнала и его гармониках за счет модуляции информационным сигналом). При съеме информации по параметрическому каналу для исключения взаимного влияния облучающего и переизлученного сигналов используется временная или частотная развязка.

(Продолжение статьи в следующем номере журанала)

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 1996 г. № 149-ФЗ. Ст. 3, 9, 16.

2. Федеральный закон «Об участии в международном информационном обмене» от 4 июля 1996 г. № 85-ФЗ. Ст. 9, 17.

3. Распоряжение Президента Российской Федерации «Об утверждении Доктрины информационной безопасности Российской Федерации» от 9 сентября 2000 г. № р-1895.

4. Указ Президента Российской Федерации «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17 марта 2008 г. № 351.

5. Указ Президента Российской Федерации «Об утверждении Концепции национальной безопасности Российской Федерации» от 17 декабря 1997 г. № 1300. Разд. 2.

6. Постановление Совета Министров — Правительства Российской Федерации «Об утверждении Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам» от 15 сентября 1993 г. № 912-51. Разд. 1, ст. 9; 10, разд. 2, ст. 7; разд. 3, ст. 24, 25.

7. *Громыко И. А., Оспищев Е. Я., Кильмаев С. Ю.* Будущее за упреждающими системами защиты // Вопросы защиты информации. 2007. № 2. С. 11–14.