Таким образом, в результате проведенного анализа уязвимых мест ИТС, возможных каналов доступа (штатных и несанкционированных) к информационным ресурсам предложен ряд методов и мероприятий, позволяющих наиболее полно перекрыть известные угрозы, и даны рекомендации по организации выполнения этих мероприятий в программно-аппаратном исполнении ПИБ.

Литература: 1. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. М. 2000. 2. Задірака В., Олексюк О. Методи захисту фінансової інформації. Київ: Вища школа, 2000. 3. Мельников Ю. Н. Защита информации в компьютерных системах. М.: Финансы и статистика; Электроинформ, 1997.

УДК 681.3

АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ И МЕТОДОВ ЗАЩИТЫ

Александр Лаврентьев
НИЦ «ТЕЗИС» НТУУ «КПИ»

Аннотация: **Приводится анализ составляющих технического канала утечки информации, классификация средств защиты, рассмотрен систематизированный подход к организации технической защиты информации.**
Summary: **The analysis of outflow, making the technical channel, of the information is resulted,Classification of means of protection, approach to organization of technical protection of the information.**
Ключевые слова: **Информация, утечка информации, технические каналы утечки информации**.

I Место противодействия техническим разведкам в системе ТЗИ

С развитием информационных технологий основной угрозой для информации с ограниченным доступом (ИсОД) стала проблема несанкционированного доступа (НСД). Однако это не уменьшает опасности несанкционированного перехвата информации и по техническим каналам. Особенно это касается информационных систем, не имеющих выхода за пределы контролируемой территории. В этом случае для разведки нет альтернативы, кроме как использование технических средств перехвата информации.

Предлагается возможный вариант подхода к классификации технических каналов утечки информации и методов защиты, которые могут лечь в основу организации системы противодействия техническим разведкам.

II Анализ структуры технических каналов утечки информации

По определению, технический канал утечки (ТКУ) информации представляет собой совокупность источника информации, среды распространения сигнала и разведаппаратуры (рис. 1).

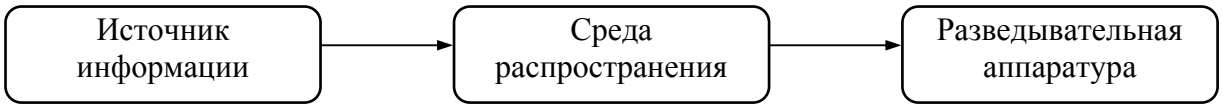

Рисунок 1

Это базовая схема технического канала утечки информации. Она не отражает существенных элементов процесса технической разведки. В конечном итоге разведывательные сообщества интересуют не поля, которые они перехватывают, а сведения, которые они могут получить на основании разведданных, полученных с помощью перехвата. Эти сведения не передаются напрямую, а претерпевают целый ряд преобразований, приводящих к возможности появления, распространения информационных полей и их перехвата и восстановления средствами технической разведки. С учетом этого ТКУ можно представить следующим образом (рис. 2).

Рисунок 2

«Преобразование информации» заключается в ее наложении на физическое поле, которое может распространяться в определенной среде и быть принято техническими средствами. Такое преобразование может осуществляться специально, например, в радиосвязи, когда высокочастотная несущая модулируется информационным сигналом. Примером непреднамеренного преобразования информационного сигнала могут служить побочные электромагнитные излучения и наводки от ЭВМ. Соответственно «восстановление информации» является обратной задачей технической разведки — восстановление сведений, ради которых ведется разведка, по полученным разведданным. Характерным примером является структура канала утечки речевой информации с использованием лазерной аппаратуры разведки:

речь – ***источник информации;***

акустические колебания воздуха – вибрация стекол – луч оптического квантового генератора – ***преобразование информации и распространение сигнала в различных средах;***

модуляция луча ОКГ – демодуляция ***– средство разведки;***

восстановление речи ***– восстановление информации.***

Естественно, что необходимым условием для возникновения возможного технического канала утечки информации с ограниченнм доступом является наличие одновременно всех трех составляющих — источника информации, среды распространения сигнала и средства разведки.

Для перекрытия возможных технических каналов утечки ИсОД можно воздействовать на любой из этих компонентов, в том числе на преобразование информации (рис. 3).

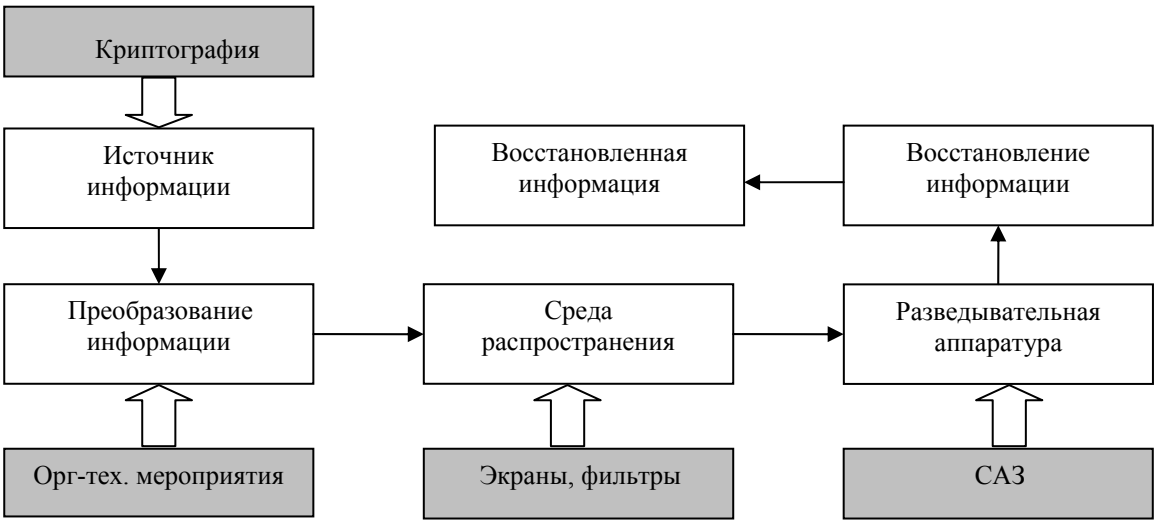

Рисунок 3

Таким образом, меры по технической защите информации можно условно разделить на три основные группы, исходя из того, на какую составляющую канала утечки информации они воздействуют.

Воздействие на *источник информации* заключается в ее преобразовании в вид, исключающий или существенно затрудняющий возможность ее несанкционированного восстановления. Наиболее распространенным способом такого воздействия является шифрование информации (криптография). Применяется также метод создания неопределенности относительно истиных значений скрываемого сигнала.

Кроме того, можно воздействовать на *преобразование*, исключив его организационными или техническими мерами. Например, при наличии паразитной генерации, которая может возникнуть в техническом средстве, это средство дорабатывают или заменяют.

В качестве средств перекрытия канала утечки информации путем воздействия на *среду ее распространения* используются, в основном, экраны, фильтры, маски. Этот метод широко применяется при осуществлении радиотехнической, оптической маскировки и т. д. Это достаточно известные меры и подробно описывать их нецелесообразно. Достаточно отметить, что они направлены на изменение среды, препятствующее распространению информационного сигнала, с целью снижения уровня сигнала до нормированных значений.

Воздействие на *техническое средство разведки* может быть реализовано путем его удаления (например, ликвидация закладных устройств) или достигается применением средств активной защиты (САЗ). САЗ предназначены для формирования на входе разведаппаратуры такого соотношения сигнал/помеха, которое не позволяет восстановить информацию.

Возможный технический канал утечки информации считается перекрытым, если на границе контролируемой зоны (в месте возможного размещения средств разведки) выполняются требования действующих норм эффективности защиты для объекта соответствующей категории.

Анализ технических каналов утечки информации позволит не только выбрать адекватные по цене и эффективности меры защиты, но и правильно их применить. Например, существует заблуждение, что средства активной защиты подавляют информационный сигнал, например от ЭВМ, и, исходя из этого, стараются разместить САЗ как можно ближе к объекту защиты. В документации на некоторые САЗ оговаривается зона их действия, например, 10 м. Очевидно, что это технически неграмотный подход к применению систем активной защиты. Наиболее оптимальное размещение САЗ, обеспечивающее необходимую эффективность защиты при минимальном уровне помех, – между объектом защиты и зоной возможного размещения средств разведки. При этом, чем ближе к средству разведки размещены САЗ, тем эффективнее их действие при минимальном уровне помехи. Кроме того, такое размещение САЗ позволяет обеспечить защиту нескольких объектов (например, ЭВТ). При выборе места размещения антенн САЗ необходимо исключить возможность пространственной селекции излучений от объекта разведки и САЗ (рис. 4).

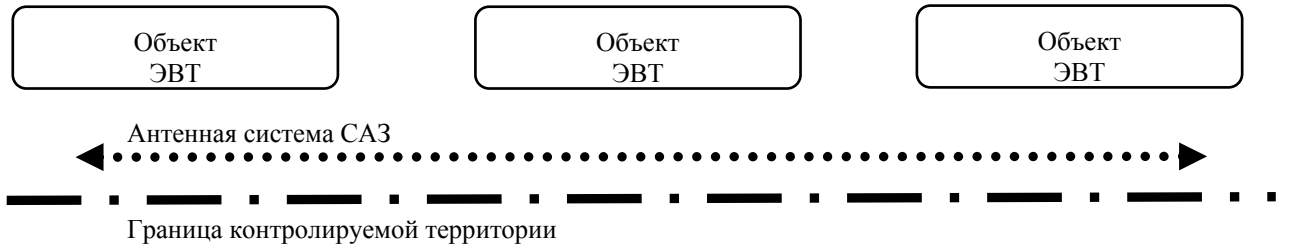

Рисунок 4

На практике встречаются также другие типичные ошибки, возникающие при организации защиты в связи с незнанием структуры ТКУ и его физического смысла. Например, необоснованным является требование по организации защиты ИсОД от утечки по техническим каналам хранилищ 1 отделов. В этом случае имеется информация с ограниченным доступом (документы), но нет преобразования в поле, способное ее передавать.

Другой пример. Устанавливаются средства защиты на линии, не имеющие выхода за пределы контролируемой территории. В данном случае есть источник информации, возможно преобразование информационного сигнала в электрическое поле, но нет среды распространения сигнала до средства разведки. Также может отсутствовать средство разведки при наличии остальных составляющих, например, когда негде установить лазерное средство съема речевой информации.

Предложенная схема возможных ТКУ является универсальной и может быть применена к любой информации и любому техническому каналу – будь то ПЭМИ, наводки, речевая информация или другое. Важно грамотно провести анализ информационных потоков, выявить места возможного возникновения ТКУ, оценить их реальную угрозу, выбрать и принять адекватные меры защиты.

III Алгоритм защиты

Понимание физического смысла всех элементов технического канала утечки информации позволит объективно их выявить, оценить степень угрозы, подобрать оптимальные средства защиты. При организации защиты информации от утечки по техническим каналам необходимо:

1. Определить, в каком виде циркулирует информация на объекте. Это может быть речевая информация на совещании, в устройствах звукоусиления и звукозаписи; это может быть информация, копируемая с бумажных носителей, обрабатываемая на ЭВМ и так далее. Необходимо учесть даже механические, электрические и, тем более, электронные пишущие машинки, на которых изготавливаются документы, содержащие ИсОД.
2. Установить потенциальную возможность преобразования информационного сигнала внутри источника информации в поля и сигналы, способные распространяться за пределы контролируемой территории. Это может быть паразитная генерация, модуляция встроенных (функциональных) генераторов информационным сигналом, побочные электромагнитные излучения и другое.
3. Установить, на какие элементы объекта и его оборудования в принципе может воздействовать информационный сигнал. Результатами такого воздействия могут быть вибрации строительных конструкций, вызванные речью, наводки в проводах и кабелях и т. п.
4. Определить наличие среды распространения сигнала за пределы контролируемой территории. Так, наводка информационного сигнала в линию не представляет опасности, если линия не выходит за пределы контролируемой территории.
5. Провести анализ реальности угрозы перехвата информационного сигнала с учетом возможностей технических средств разведок. Так, например, если соседнее с выделенным помещение принадлежит той же фирме (организации), то считается, что в нем применение технических средств перехата исключено, и меры защиты не требуются. Если напротив окон выделенного помещения невозможно размещение лазерных средств съема речевой информации, то нет необходимости в виброзащите стекол. Целесообразно провести предварительный технический контроль для инструментального подтверждения наличия или отсутствия возможного технического канала утечки информации.
6. Выбрать и установить оптимальные с точки зрения цены и эффективности средства защиты. Необходимо учесть, что в ряде случаев возможно воздействие средствами защиты не на все каналы утечки информации. Например, нельзя зашифровать речевую информацию при проведении совещаний. При выборе средств защиты нужно учитывать как техническую, так и информационную перспективы развития объекта. Выбор уровня защиты с учетом перспективы позволит перейти к обработке более важной информации без принятия дополнительных мер. Ряд средств защиты позволяет также осуществлять техническую модернизацию в рамках действующей системы защиты. К ним можно отнести экранированные сооружения, средства активной защиты и т. д.
7. Провести инструментальный контроль эффективности принятых мер защиты. Все технические средства защиты после монтажа на объекте обязательно должны пройти технический контроль, подтверждающий выполнение требований действующих норм эффективности защиты. Такой контроль проводится независимо от того, имеется ли сертификат на средство защиты (защищенное средство), были ли проведены специальные обследования в лабораторных условиях и т. д. По результатам контроля разрабатываются соответствующие документы, дающие право на обработку (обсуждение и пр.) ИсОД.
8. Организовать сопровождение системы защиты информации. Система защиты информации будет жизнеспособна только при условии постоянного контроля за ее функционированием. Контроль может быть повседневным, периодическим и внеплановым. Он может осуществляться с проведением инструментальных измерений и без них. Повседневные проверки проводятся, как правило, без использования технических средств контроля. Они заключаются в проверке соответствия состава и размещения технических средств на объекте требованиям соответствующих эксплуатационных документов, наличия и работоспособности средств защиты и т. д. Сроки проведения периодического контроля определяются требованиями действующих нормативно-методических документов и включают инструментальную проверку эффективности мер защиты. Например, для выделенных помещений и объектов ЭВТ установлена периодичность технического контроля в один год. Внеплановый контроль проводится при ремонте и замене оборудования, которое может участвовать в формировании ТКУ информации, или после устранения недостатков, выявленных в ходе проверок.