Лекция 9. Техническая защита информации. Технические каналы утечки информации

Цель лекции: изучить техническую защиту информации; рассмотреть технические каналы утечки информации, принципы осуществления технической разведки и способы защиты от нее.

План лекции:

1. Основные понятия технической защиты информации
2. Технические каналы утечки информации
3. Принципы осуществления технической разведки

Сегодняшняя тема нашей лекции будет посвящена защите не только самой информации, как в основном было на предыдущих лекциях, сколько защите объектов обработки информации, средств и систем обработки информации от некоторых нежелательных, но неизбежных из-за их функциональных особенностей проявлений, приводящих к утечке информации, то есть мы с вами впервые, в общем-то, рассматриваем всю совокупность автоматизированной системы и помещения, в котором она расположена. Это и есть понятие объекта информатизации. Под ним будет понимать объект информатизации, на котором обработка информации происходит при помощи средств вычислительной техники.

Во-первых, техническое средство обработки информации — это техническое средство, предназначенное для приема, хранения, поиска, преобразования, отображения или передачи информации по каналам связи. К ним относятся:

- средства вычислительной техники,
- средства обработки и воспроизведения информации, например, звуковоспроизводящие устройства, различные экраны, мониторы, на которые выводятся информация,
- средства тиражирования информации, например, многофункциональные устройства, включающие свойства принтера, копира и, возможно, сканера.

А также понятие вспомогательных технических средств и систем потребуется нам для описания объекта средств вычислительной техники. Под вспомогательными техническими средствами и системами, сокращенно ВТСС, будем понимать технические средства и системы, не предназначенные для обработки важной информации, но на которые могут воздействовать электромагнитные поля побочных излучений основных технических средств. Это системы сигнализации, например, пожарные или охранные, системы электроосвещения, системы учета энергопотребления, электроприборы и

прочие системы, то есть любые, в общем-то, электрические системы, которые непосредственно не предназначены для работы с информацией, но которые неизбежно присутствуют в том или ином наборе в почти любом объекте информатизации, то есть объекте СВТ. Объект СВТ, таким образом, у нас будет состоять из следующих компонент: из технических средств обработки информации, то есть из тех средств, которые реализуют ту задачу, для которой объект СВТ создан, спроектирован и реализован; вспомогательных технических средств и систем, то есть тех средств, которые поддерживают ее функционирование, например, система электроснабжения, система пожарной сигнализации и прочие системы; системы электропитания; системы заземления; посторонних проводников.

Техническая защита информации - защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств. Важно обратить внимание, что техническая защита – это не только защита от утечки информации по техническим каналам утечки, но и защита от НСД, от математического воздействия, от вредоносных программ и т.п.

Объектами технической защиты информации могут быть:

- объект информатизации;
- информационная система;
- ресурсы информационной системы;
- информационные технологии;
- программные средства;
- сети связи.

Технические каналы утечки информации

Под ***утечкой информации*** мы будем понимать бесконтрольный и неправомерный выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация была доверена. То есть, утечка информации у нас может происходить как по вине людей, например, потому что они поделились конфиденциальной информацией с тем, кто не является авторизованным пользователем этой информации, или по каким-либо другим причинам, например, если документ, содержащий конфиденциальную информацию, попал в руки злоумышленника — случилась утечка информации, или если какой-то носитель информации, например, внешнее запоминающее устройство, попал точно так же в руки злоумышленника или был утерян.

Под **утечкой информации в задачах технической защиты информации** будем понимать несанкционированный перенос информации от ее источника к злоумышленнику.

Наконец, **под каналом утечки информации** будем понимать физическую среду несанкционированного распространения информации от источника к нарушителю, то есть ту среду, по которой распространяется информация или ее носитель, — в большинстве случаев некий сигнал, который несет информацию.

Под **техническим же каналом утечки информации** будем подразумевать такой канал утечки информации, несанкционированное получение информации с которого происходит с использованием технического средства съема информации.

Таким образом, будем рассматривать технический канал утечки информации как совокупность объекта (носителя) информации, канала утечки информации и технического средства несанкционированного съема информации.

Рисунок 1 Технические каналы утечки информации

На рисунке 1 эти перечисленные нами определенные объекты выстроены в некую логическую схему. Информация исходит из некоего источника — это документ или человек, который, например, ведет разговор и таким образом распространяет информацию, или работающее устройство, на котором информация обрабатывается и, возможно, передается в канал связи. Далее, от источника информации исходит носитель информации. В большинстве случаев под ним подразумевается сигнал, который несет информацию, и вот с этого места начинается технический канал утечки информации. Далее, этот носитель информации распространяется по среде распространения информации, будь то какой-то кабель либо просто воздух: когда происходит разговор, то акустическая волна перемещается просто по открытому пространству. И, далее,

этот носитель информации через среду распространения информации попадает на техническое средство разведки, то есть на то устройство, которым оперирует нарушитель. На этом как бы заканчивается граница технического канала утечки информации, злоумышленник или нарушитель расположены на другом конце этой схемы. Таким образом, технический канал утечки информации мы будем рассматривать как структуру, состоящую их трех компонентов: источник или носитель информации (в некоторых случаях они будут отождествлены), среда распространения информации и техническое средство разведки, то есть то, что передается, та среда, по которой передается, и приемник, который принимает на другом конце этот сигнал, несущий информацию.

Источниками информации в задачах технической защиты информации являются:

- объекты наблюдения, отражающие электромагнитные волны;
- объекты наблюдения, излучающие собственные электромагнитные волны в различных диапазонах;
- устройства, создающие акустические сигналы;
- передатчики функциональных каналов связи;
- закладные устройства, а также источники побочных электромагнитных излучений и наводок, так называемые ПЭМИН.

Среда распространения информации в наших моделях — это часть пространства, в которой перемещается носитель от источника сигнала к его приемнику. Среда распространения информации определяет тот маршрут, по которому носитель информации движется в пространстве, и может быть как свободным пространством, так и направляющими линиями, например, проводами, различными инженерными коммуникациями, находящимися на объекте информатизации, какими-то другими конструкциями в зависимости от природы носителя информации и среды распространения этой информации.

Приемник информации в наших моделях — это обобщенное устройство, которое обеспечивает выполнение следующих желаемых для злоумышленника задач:

- выбор носителя с интересующей нарушителя информацией,
- усиление принимаемого сигнала,
- съем информации с сигнала-носителя и
- преобразование информации в доступную для восприятия человеком или техническим устройством форму.

То есть, приемник информации должен перехватить носитель информации, то есть сигнал, извлечь из него интересующую нарушителя информацию, возможно, усилить принимаемый сигнал до того уровня, чтобы эту информацию можно было извлечь, осуществить это извлечение и преобразовать ее в понятный для человека или технического устройства вид.

Рассмотрим три основных типа каналов утечки информации. В ряде источников приводится еще множество каналов утечки информации, технических каналов, но большинство из них могут быть представлены в качестве подтипа одного из трех перечисленных больших классов (каналов) утечки информации:

- это акустический канал, то есть канал в котором происходит утечка акустической, или звуковой, информации;
- оптический канал, по которому злоумышленник перехватывает так называемую видовую информацию, то есть информацию о внешних свойствах наблюдаемых им объектов;
- радиоэлектронный канал — это канал, по которому злоумышленник перехватывает информацию, передающуюся по тем или иным каналам связи на радиоэлектронных частотах: либо на радичастоте, либо электрические и электромагнитные сигналы перехватываются нарушителем, то есть это, скорее, канал не по природе информации, а по природе сигналоносителя.

Акустический канал утечки информации. В нашей модели он будет состоять из следующих трех компонент: источник звуковой информации, далее среда распространения сигнала и приемник звуковой информации.

В качестве источника в таком канале могут выступать следующие объекты и явления:

- разговор, совещание, выступление, ситуация, в которой люди общаются и производят тем самым акустические колебания, акустические сигналы, которые затем могут воздействовать на какие-то другие объекты;
- звуковоспроизводящая аппаратура, которая также является источником акустических колебаний, акустических сигналов;
- работающие технические устройства, которые по своему функционалу не предназначены для того, чтобы воспроизводить какие-то звуковые осмысленные сигналы, но тем не менее их издают именно в силу своих

конструктивных особенностей, например, громко работающее оборудование, станки, производственные какие-то устройства.

Для них порождение акустических сигналов является, скорее, побочным явлением, но тем не менее оно позволяет злоумышленнику делать какие-то выводы о том, например, каков функциональный состав объекта информатизации, какое оборудование на нем используется, с какой нагрузкой оно работает, и прочие различные параметры, которые могут влиять на звуки, которые воспроизводят технические устройства.

В качестве приемников информации для данного канала утечки информации используются: самое очевидное, микрофоны, направленные и ненаправленные, диктофоны, стетоскопы и другие устройства съема звуковой информации. Микрофоны, направленные и ненаправленные, как и диктофоны, предназначены для несанкционированного перехвата акустической информации, воспроизводимой, как правило, человеческой речью либо какими-то устройствами воспроизведения звука. *Направленные микрофоны* — это такие устройства, которые характеризуются большой дальностью, на которой звук может быть перехвачен, но при этом крайне узкой областью направленности. Они часто фигурируют в различных шпионских фильмах, иногда выглядят похожими на, например, зонт, но, как правило, конструктивно они представляют собой набор узких трубочек различной длины, что обеспечивает различные частоты перехвата звука. Для того чтобы перехватить информацию, нужно очень четко направить эту нужную трубочку на источник звукового колебания и таким образом этот сигнал можно перехватить.

Оптический канал утечки информации. *В качестве источника информации* в нём будем рассматривать некий источник видовой информации, то есть объект, о котором нарушителей интересует его внешний вид, различные особенности, например, форма, цвет, факт его нахождения на какой-то территории, возможно, некие внешние признаки, выдающие его функциональные особенности.

В первую очередь здесь приходят на ум различные образцы военной техники, различные конструкторские исследования, различные постройки, сооружения. Но, тем не менее, и на территории вполне мирных объектов информатизации могут находиться какие-то объекты, факт наличия которых желательно оставить конфиденциальным, и поэтому данный канал утечки информации мы рассматриваем как актуальный и его изучаем. Далее данный источник видовой информации порождает некий носитель этой информаций, который распространяется по среде распространения сигнала, и этот сигнал поступает на оптический приёмник информации.

В качестве источников информации могут рассматриваться любые объекты либо отражающие внешний свет, либо сами являющиеся излучателями света. Здесь следует отметить, что объекты, отражающие внешний свет, по оптическому каналу утечки информации передают информацию о своих структурных свойствах, то есть о самом объекте.

А объекты, излучающие свет, как правило, передают информацию о свойствах излучаемого сигнала. В качестве среды распространения для данного канала утечки информации может выступать как воздух, так и вода и некоторые жидкости, также космос, поскольку существуют технологии разведки из космоса, существуют спутники-шпионы, которые могут фотографировать объекты на территории различных государств, то есть на земной поверхности. И отдельно выделяется оптическое волокно как канал связи функциональный, то есть используемый легальными пользователями. Тем не менее, нарушители имеют технологии, для того чтобы перехватывать информацию, передаваемую по оптическо-волоконным каналам связи. В качестве приёмника оптической информации при перехвате информации по оптическому каналу нарушителем могут использоваться такие приборы как фотоаппараты и видеокамеры, визуально-оптические приборы, то есть приборы усиления человеческого зрения, с помощью которых нарушитель ведёт непосредственное наблюдение за объектом, приборы ночного видения, тепловизоры, системы телевизионного наблюдения. Это охранные системы, обеспечивающие наблюдение за контролируемыми территориями. Нарушитель может к ним подключаться либо использовать некий аналог таких систем, размещённый им несанкционированно.

Радиоэлектронный канал утечки информации.

Для того чтобы говорить о радиоэлектронном канале утечки информации, определим сначала понятие побочных электромагнитных излучений и наводок, или сокращенно ПЭМИН. Под этим термином будем подразумевать демаскирующие побочные электромагнитные излучения, возникающие при работе входящих в состав объекта информатизации технических средств.

По уже известной нам модели в данном канале утечки информации у нас существует источник сигнала, именно сигнала, а не какой-то информации, как

раз в данном случае они как бы отождествляются у нас, носитель и источник информации, среда распространения такого сигнала и приемник этого сигнала, из которого затем нарушитель может извлечь смысловую информацию.

В качестве носителя информации в данном случае у нас может рассматриваться электрический ток, из которого нарушитель может перехватывать смысловую информацию, и электромагнитное поле, порожденное различными устройствами в составе объекта информатизации.

В качестве источников информации здесь могут рассматриваться передающие устройства, то есть устройства, которые используются легальными пользователями, но при этом нарушитель также может перехватывать информацию от них.

Простой пример — радиопередатчик. Легальные пользователи обмениваются информацией, но при этом нарушитель не имеет никаких препятствий для того чтобы несанкционированно эту информацию перехватывать. Источники паразитных электромагнитных излучений и наводок — объекты, отражающие излучения, и объекты, являющиеся источниками собственных излучений.

В качестве среды распространения здесь рассматриваются, подобно предыдущим каналам, воздух, космическое пространство и различные направляющие линии, то есть каналы связи, силовые каналы и кабели на территории объекта информатизации, например, кабели электропитания.

Ну в качестве приемников информации здесь нарушителем используются различного рода приемники, действующие на частотах радиоканала, на радиочастотах. В рамках данного канала нарушитель реализует следующие действия: перехватывает радиосигналы, перехватывает электрические сигналы, осуществляет радиолокационные и радиотеплолокационные наблюдения за интересующим его объектом. Особенностями радиоэлектронного канала утечки

информации являются независимость от времени суток: в отсутствие освещения и в его присутствии данный канал одинаково удобен для нарушителя, если он обладает соответствующей аппаратурой. Данный канал минимально зависит от метеоусловий по сравнению с двумя другими рассмотренными нами каналами. Он обладает высокой информативностью, поскольку как минимум часть информации, передаваемой по данному каналу, исходит непосредственно от аппаратуры обрабатывающей информацию, нарушитель достигает высокой оперативности и высокой информативности получения информации, вплоть до режима реального времени, то есть вплоть до одновременности с легальным получателем.

Принципы осуществления технической разведки

Прослушивание акустических сигналов микрофонами, направленными и ненаправленными, возможно, в комплексе со звукозаписывающими устройствами или устройствами передачи по радиоканалу или иным каналам связи. Данные устройства используются для перехвата информации по прямому акустическому каналу, то есть человеческой речи чаще всего, и в данном случае нарушитель может использовать комплекс устройств, которые сами записывают информацию либо передают её далее по радиоканалу для того, чтобы она была принята другими устройствами.

В данном случае это уже специальные закладные устройства, так называемые жучки, радиозакладки и прочие шпионские устройства, часто показываемые в соответствующих кинофильмах.

Кроме того, злоумышленник может *использовать перехват акустических сигналов* электронными стетоскопами, возможно, в комплексе с аналогичными устройствами передачи информации по различным каналам связи, если речь идёт о перехвате информации, которая извлекается нарушителем из колебаний каких-то конструкций зданий, из колебаний каких-то сред, например, водопровода или различных конструкций здания, системы вентиляции, системы центрального отопления и прочих систем.

И уже упоминавшийся сегодня перехват акустических сигналов путём *высокочастотного облучения соответствующих закладных устройств*. Для перехвата информации по различным акустопреобразовательным каналам нарушитель может использовать:

- приём и детектирование побочных электромагнитных импульсов,
- перехват акустических сигналов через устройства, обладающие микрофонным эффектом, путём подключения к их соединительным линиям. В этом случае нарушитель отслеживает изменения параметров электрического сигнала, вызванные микрофонным эффектом, который имеет место для тех или иных устройств, не обязательно устройств обработки информации, возможно, вспомогательных устройств и систем.

- Облучение оконных стёкол лазерными стетоскопами также входит в арсенал нарушителя и применяется для перехвата информации, порождаемой внутри помещения, например, при ведении переговоров в закрытом кабинете.

Несмотря на то, что на территорию кабинета сам нарушитель попасть не может, если существуют оконные стёкла, не защищённые специальным оборудованием, они испытывают вибрацию, которая возникает за счёт воздействия звуковой волны, неизбежно порождаемой при ведении переговоров, и в этом случае нарушитель, облучая или зондируя, говоря другим словом, оконные стёкла с помощью лазерных стетоскопов, может эти колебания считывать, то есть регистрировать, и преобразовывать их затем в звуковой сигнал, из которого извлекать смысловую информацию, то есть содержание разговора.

При перехвате информации по оптическому каналу утечки информации нарушитель может осуществлять наблюдение за объектом при помощи оптических приборов, например, биноклей, перископов и прочих приборов усиления зрения.

Может он также реализовывать перехват информации из волоконно-оптических каналов связи описанным ранее способом, а также осуществлять:

- скрытую съёмку объекта информатизации, то есть того объекта, за которым он ведёт наблюдение, при помощи фотоаппаратуры и видеоаппаратуры, как портативной, то есть носимой самим нарушителем, например, посетителем, который пришёл на территорию объекта информатизации в качестве клиента, контрагента, приглашённого сотрудника какой-нибудь службы поддержки, например, электромонтёра или сотрудника организации, которая осуществляет размещение противопожарной сигнализации или
- других коммуникационных средств, аппаратуры, установленной на территории объекта вычислительной техники, объекта СВТ, то есть аппаратуры, установленной нелегально, различных закладных устройств и
- прочих устройств несанкционированного съёма информации, аппаратуры, установленной на транспортных средствах, включая летательный аппараты, в том числе беспилотные.

В современном мире беспилотные летательные аппараты получают всё более и более широкое распространение, поэтому возможность того, что для наблюдения за тем или иным объектом информатизации будет использовано подобное средство, следует считать актуальной и предпринимать соответствующие меры защиты от такой угрозы. А также аппаратуры, установленной на космических аппаратах. Данный вид аппаратуры больше всего применяется, наверное, для наблюдения за различными стратегическими объектами, такими как военные объекты различные, объекты общегосударственной инфраструктуры.

Список использованной литературы

1. Adam Shostack. “Threat Modeling: Designing for Security”. Published by John Wiley & Sons, Inc., Canada 2014.- 626 p.

2. Richard Bejtlich. “The Practice of Network Security Monitoring”. Published by No Starch Press, Inc., USA 2013. – 380 p.

3. Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams and Abdul Aslam. “Enterprise Cybersecurity: how to build a successful Cyberdefense program against advanced threats”. Published by Apress, 2015. – 508 p.

4. Хорев А. А. Организация защиты конфиденциальной информации в коммерческой структуре // Защита информации. Инсайд : журнал. — 2015. — № 1. — С. 14—17. — ISSN 2413-3582

5. Morris J. Dworkin. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions (англ.) // Federal Inf. Process. Stds. (NIST FIPS) - 202. — 2015-08-04.