Понятие информационной безопасности включает в себя должное обеспечение защиты любой информации от любых случайных или преднамеренных воздействий, влекущих к утечке информации, которая в свою очередь может нанести ущерб, как самой информации, включая потерю данных, так и ее владельцам или поддерживающей инфраструктуре.

Любые данные организации – это важнейший актив информационной среды в любой сфере деятельности. Состояние защищенности информационной среды организации, обеспечивающее её формирование, использование и развитие зависит от степени противодействия возможным угрозам. При обмене информации между работниками организации важно исключить ее утечку во внешнюю среду. Это достигается путем создания закрытых локальных сетей, созданием внутренней инженерно-технической инфраструктуры коммуникаций с применением различных методов технологий.

Поскольку информация не может существовать без ее носителя, то, помимо защиты информации на уровне программного обеспечения, информация, так же, подлежит аппаратной и физической защите, включая защиту пространства, которое может быть использовано для хищения информации дистанционно.

Хотелось остановиться на проблеме утечки информации на расстоянии, поскольку эта проблема очень актуальна на сегодняшний день.

В этом эссе пойдёт речь о закладных устройствах. Эти устройства фиксируют звуковые волны и передают информацию потенциальным злоумышленникам.

Основная часть

Закладное устройство – миниатюрное электронное устройство перехвата речевой информации, состоящее из микрофона и радиопередатчика, обеспечивающего передачу подслушанного звукового сигнала на достаточно значительное расстояние с помощью электромагнитных волн.

Закладные устройства являются самыми распространенными техническими средствами съема акустической информации. Их популярность объясняется

простотой использования, относительной дешевизной, малыми размерами и возможностью камуфляжа.

Радиоэлектронные закладные устройства (ЗУ) представляют собой организованный канал несанкционированного получения и передачи аудиовизуальной или обрабатываемой с помощью радиоэлектронной аппаратуры и передаваемой информации в сетях связи. Закладные устройства можно классифицировать по нескольким признакам:

- радиозакладные устройства, излучающие в эфир;

- закладные устройства, не излучающие в эфир (передача осуществляется по сетям связи, питания и т. д.);

- радиозакладные устройства с переизлучением;

- закладные устройства с передачей перехваченной информации по стандартному телефонному каналу. [4]

В первую группу входят радиозакладные устройства, предназначенные для получения аудиоинформации по акустике помещения, телевизионные закладные устройства, предназначенные для получения аудио- и визуальной информации, и радиозакладные устройства в телефонных линиях связи, устройства их обработки и передачи информации, сетях питания и т.д.. Передача перехваченной информации происходит радио- или телевизионным радиосигналом. [1]

Ко второй группе относятся устройства с передачей информации без излучения в эфир, к ним можно отнести группу закладных устройств в линиях связи, питания и охранной сигнализации с использованием этих линий связи для передачи перехваченной информации.

В ряде закладных устройств передача перехваченной информации осуществляется по стандартному телефонному каналу. Это так называемые закладки «с искусственно поднятой трубкой».

Существует целая группа закладных устройств, обеспечивающих получение информации по акустике помещения за счёт модуляции акустическим сигналом отраженного микроволнового или ИК-сигналов от элементов, на которые воздействует акустический сигнал. Это могут быть стёкла, различные перегородки, резонаторы, специальные схемы и т.д. [6]

Передача сигнала закладных устройств при их передаче различна, т.к. они могут проявляться в радиодиапазоне, как радиоизлучения с различными видами модуляции или кодирования, в ИК-диапазоне, как низкочастотные излучения в линиях связи, управления, питания, в стандартных телефонных каналах или в виде облучающих сигналов.

В зависимости от предназначения ЗУ выделяется прежде всего «зона несанкционированного получения информации». Это может быть воздушное пространство, несущие конструкции, трубы водопроводной или паровой сети для структурной акустической волны, элементы тракта обработки и передачи информации.

Простейшие закладные устройства включают три основных узла, которые определяют их тактико-технические возможности. Это: микрофон, определяющий зону акустической чувствительности жучка, радиопередатчик, определяющий дальность его действия и скрытность работы, источник электропитания, определяющий время непрерывной работы.

Закладные устройства работают как обычный передатчик. В качестве источника электропитания жучка используются малогабаритные аккумуляторы. Срок работы подобных закладных устройств определяется временем работы аккумулятора. При непрерывной работе это 1-2 суток.

Микрофон - устройство, улавливающее акустические колебания, распространяющиеся в воздушном пространстве. Микрофоны, позволяют улавливать негромкую речь на дальности 5 -10 метров.

Радиопередатчик осуществляет передачу информации с помощью электромагнитных волн в определенном радиодиапазоне. Для передачи информации используются VHF (метровый), UHF (дециметровый) и GHz (ГГц) диапазоны длин волн. Наиболее часто используются диапазоны частот: 130-174 МГц, 350-450 МГц, 850-950 МГц и 1100-1300 МГц. Однако не исключено использование и других диапазонов. [3]

Для приема информации, передаваемой закладным устройством, необходим приемник. Лучше использовать специальный приемник, но если нет средств на его приобретение, можно воспользоваться обычным радиоприемником, но тогда закладное устройство должно использовать частоту передачи в диапазоне, выделенном для радиовещания. Но тогда передаваемый сигнал смогут принимать все обладатели радиоприемников (настроенных на частоту радиозакладки),

находящиеся в радиусе действия закладного устройства. А это не только демаскирует деятельность злоумышленника, но и в значительной мере способствует его обнаружению.

Скрытность работы закладных устройств обеспечивается небольшой мощностью передатчика, выбором частоты излучения, ограничением времени непрерывной работы (использование системы дистанционного управления). Для повышения скрытности работы в некоторых закладных устройствах используется разделение этапов съема и передачи информации (радиозакладки с промежуточным накоплением). Они имеют в своем составе цифровой накопитель, приемник сигналов дистанционного управления и специальный передатчик для ускоренной передачи информации. В таких закладных устройствах в течение некоторого времени осуществляется перехват акустической информации, преобразование ее в цифровой вид и запись во внутреннюю память закладки. Передача информации в эфир осуществляется через определенные промежутки времени или по команде дистанционного управления. Соотношение времени накопления и времени передачи может составлять от 40:1 до 120:1.

Для закрытия радиоканала применяются различные способы кодирования: аналоговое скремблирование речевого сигнала (как правило, инверсия спектра) и цифровое кодирование, заключается в преобразовании речевого сигнала в цифровой вид с последующим шифрованием по одному из алгоритмов. [2]

Заключение

Утечка информации чревата губительными последствиями.

Для противодействия потенциальным угрозам информационной безопасности в организации должен быть разработан и реализован набор процедур по предотвращению потенциальных дистанционных угроз и минимизации ущерба в том случае, если такая ситуация всё-таки возникнет.

Итак, при разработке внутренней инженерно-технической инфраструктуры коммуникаций необходимо учитывать множество аспектов, для того, чтобы защитить информацию от несанкционированного доступа. Так, например, телефонные аппараты (даже при положенной трубке) могут быть использованы для прослушивания разговоров, ведущихся в помещениях, где они установлены. Так же, прослушивание разговоров возможно путем размещения закладных

устройств в зонах, предназначенных для ведения конфиденциальных переговоров, электронных устройств перехвата речевой информации.

Следовательно, методы и средства защиты инженерно-технической инфраструктуры коммуникаций организации должны быть направлены на исключение использования закладных устройств в конфиденциальных зонах.

Список литературы

1. Викторов, А.Д. Способы перехвата информации, обрабатываемой техническими средствами / А. Д. Викторов, В.И.Гене, Э.В.Гончаров // М.: Полиграф. – 2005. – С. 85-100.
2. Катарин, Ю.Ф. Большая энциклопедия промышленного шпионажа / Ю.Ф. Катарин, Е.В. Куренков, А.В. Лысов, А.Н. Остапенко // СПб.: ООО «Издательство Полигон». – 2000. – С.15-22.
3. Соболев, А.Н. Физические основы технических средств обеспечения информационной безопасности: Уч. Пособие / А.Н. Соболев, В.М. Кириллов // М.: Гелиос АРВ. – 2004. – С. 75-80.
4. Специальные проверки служебных помещений [Электронный ресурс] Аналитика. Средства защиты информации [сайт] 2006 – 2014. – Оежим доступа:http://www.analitika.info/poisk.php?page=1&full=block_article37&articlepage=5
5. Торокин, А.А. Инженерно-техническая защита информации. – М.: Гелиос АРВ, 2005. – С. 102-108, 652-657, 809-816.
6. Хорев, А.А. Способы перехвата информации, обрабатываемой техническими средствами // Защита информации. Инсайд. – 2008. – №1. – стр. 28 – 36.