УДК 621.395.019.3

Антясов И. С., Яресько А. П., Соколов А. Н.

ЗАЩИТА ИНФОРМАЦИИ В ПОМЕЩЕНИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Вследствие дешевизны фиксированной связи и простоты набора внутренних номеров, вопрос ее использования на предприятиях (в организациях) остается актуальным. Поэтому существует значительная вероятность использования злоумышленником телефонных линий для снятия конфиденциальной информации, что может привести к значительным негативным последствиям для предприятия (организации).

Рассмотрены принципы использования телефонных линий связи для конфиденциальных переговоров, возможные способы снятия конфиденциальной информации злоумышленником. Приведены методы перехвата информации в помещении с установленными телефонными аппаратами, а также средства защиты этой информации от утечки.

Ключевые слова: *технический канал утечки информации, телефонный канал связи, акустоэлектрические преобразования, средства защиты информации, высокочастотное навязывание, высокочастотное облучение.*

Antyasov I. S., Yaresko A. P., Sokolov A. N.

INFORMATION PROTECTION INDOOR AGAINST LEAKAGE THROUGH TECHNICAL CHANNELS

Due to the cheapness of fixed-line and ease set of extensions, the question of its use in enterprises (organizations) is still relevant. Therefore, there is a significant probability of using an attacker telephone lines to obtain confidential information that could lead to significant negative consequences for the enterprise (organization).

The principles of of using telephone lines for confidential negotiations, the possible ways of obtaining confidential information by an attacker. Methods of interception in the room with the established telephones, and protection of this information against leakage.

Keywords: *technical channel leakage of information, telephone communication channel, acoustic-electric conversion, means of information protection, high-frequency imposition, high-frequency radiation.*

Техническим каналом утечки информации (ТКУИ) называют совокупность технического средства разведки, объекта разведки, с помощью которого добывается информация об искомом объекте, и физической среды, в которой распространяется информационный сигнал. Под техническим каналом, по сути, понимают способ добычи разведывательной информации об объекте. При этом под разведывательной информацией имеют

ввиду сведения или совокупность данных об объектах разведки независимо от формы их представления.[1]

Материальными носителями информации являются сигналы. Сигналы могут быть:

- Электрическими;
- Электромагнитными;
- Акустическими;
- Другими. [2]

Таким образом, сигналами, зачастую, являются электромагнитные, механические и другие виды колебаний (волн), причем информация содержится в их изменяющихся параметрах. Сигналы могут распространяться только в определённых средах, в каких именно – зависит от природы сигнала. В общем случае средой распространения могут быть газовые (воздушные), жидкостные (водные) и твердые среды (конструкции зданий, токопроводящие линии, грунт, опоры).

Телефон может быть использован злоумышленником для несанкционированного доступа (НСД) к информации коммерческого и частного использования. При этом можно выделить несколько каналов утечки информации от телефона:

• Прямое прослушивание телефонных переговоров путём подключения к каналу связи.

• Акустоэлектрические преобразования (АЭП) от телефона, как от вспомогательных технических средств и систем (ВТСС). Такой способ съёма актуален, если телефон просто находится в помещении, где обсуждается конфиденциальная информация.

• Также отдельную группу ТКУИ составляют возможные утечки за счет высокочастотного облучения, навязывания или прокачки. [3]

В классическом прямом прослушивании телефонных переговоров выделяют следующие способы подключения:

• Параллельное подключение к телефонной линии. В этом случае телефонные радиоретрансляторы требуют внешнего источника питания, но труднее обнаруживаются. Эти системы основаны на индуктивном способе съёма информации при помощи специальных катушек. Так как эти системы имеют несколько каскадов усиления слабого НЧ-сигнала и имеют обязательно внешний источник питания, то они получаются громоздкими.

• Последовательное включение телефонных радиоретрансляторов в разрыв провода телефонной линии. Этот способ является самым простым и надёжным при съёме информации в телефонных линиях. Если у злоумышленников невысокий уровень технической подготовки, то часто применяется трубка телефонного ремонтника, которая подключается в распределительный ящик. Телефонную закладку можно последовательно подключить как к самому телефонному аппарату, так и к любому участку линии от абонента до АТС. В этом случае питание телефонного радиоретранслятора осуществляется от телефонной линии и на передачу он выходит с момента подъема телефонной трубки абонентом. [1]

Существует угроза прослушивания помещений через микрофон телефонного аппарата (либо от ВТСС) за счет АЭП. Стоит отметить, что данный ТКУИ является естественным и не требует закладных устройств. Микрофон является частью электронной схемы телефонного аппарата: он либо соединен с линией (через отдельные элементы схемы) при разговоре, либо отключен от нее, когда телефонный аппарат находится в ожидании вызова (трубка находится на аппарате). На первый взгляд, когда трубка лежит на аппарате, нет никакой возможности использовать микрофон в качестве источника съема информации. На самом деле это не так, посредством расшифровывания АЭП возможен перехват защищаемой информации. Данные преобразования основываются на обратном эффекте Фарадея, эффекте Веллари, емкостных эффектах, пьезоэффектах.

Однако необходимо помнить, что в составе многих технических средств всегда штатно работают один или несколько разного рода ВЧ автогенераторов, воздействие на их элементы (конденсаторы, дроссели, системы заряженных проводников и т.д., о чем говорилось выше) механических колебаний акустических сигналов, часто приводит к изменению амплитуды и/или частоты/фазы этих колебаний, т.е. к модуляции. ВЧ колебания этих генераторов в той или иной степени излучаются в окружающее пространство и/или распространяются по отходящим от технических средств линиям, подобно побочным электромагнитным излучениям и наводкам от технических средств. Так образуются модуляционные высокочастотные каналы АЭП, которые опасны не столько сами по себе, сколько именно тем речевым сигналом, который модулирует ВЧ колебания автогенераторов. [4]

Существуют также способы искусственно улучшить свойства АЭП. С этой целью, злоу-

мышленнику нужно на один провод телефонной линии подключить высокочастотный (ВЧ) генератор, а к другому детектор амплитуд с усилителем. При этом генерируемые ВЧ-колебания проходят через элементы телефонного аппарата, обладающими «микрофонным эффектом», потом модулируются акустическими сигналами в помещении (конфиденциальной беседой). После этого модулированный сигнал демодулируется детектором амплитуд, усиливается и в результате прослушивается или записывается. Этот метод съёма информации получил название высокочастотного навязывания.

ВЧ облучение. Технический канал утечки информации с использованием «высокочастотного облучения» образуется за счет неконтактного (дистанционного, через свободное пространство) введения токов высокой частоты в нелинейные или параметрические элементы ТС. Для этих целей используется соответствующий высокочастотный генератор средства разведки. Одновременно на эти элементы воздействует акустический опасный сигнал, при этом возможна модуляция зондирующего ВЧ сигнала акустическим опасным сигналом. Затем происходит обратное переизлучение зондирующего модулированного сигнала, его прием, демодуляция и, таким образом, перехват защищаемой речевой информации. В результате воздействия акустического поля меняются параметры элементов ТС, в том числе и линейные. При этом изменяется взаимное расположение элементов схем, проводов в катушках индуктивности, значения емкостей и т.п. Это может привести к изменениям параметров переизлученного зондирующего высокочастотного сигнала, например, к модуляции его информационным сигналом. Такой механизм модуляции носит название параметрической модуляции. [5]

Защищать телефонную линию связи как канал передачи информации возможно только применением криптографических методов или полным контролем линии связи, поэтому рассмотрим защиту от утечки за счет АЭП. Среди них возможно выделить пассивные, активные и комбинированные методы и средства. Как пассивные, так и активные средства защиты имеют свои характерные преимущества и недостатки.

Достоинствами пассивных средств защиты являются:

• Малые габариты, простая электрическая схема;

• Внешнее электропитание не требуется;

• они включаются в разрыв цепей ВТСС и поэтому выход из строя некоторых элементов электрической схемы обнаруживается в процессе эксплуатации;

• невысокая стоимость относительно других типов средств.

Активные средства защиты, по сравнению с пассивными, имеют более сложное строение, высокую стоимость, а также требуют внешнего источника электропитания. Но, несмотря на эти минусы, зачастую оказывается, что эффективность активных средств защиты выше, чем у пассивных.[6]

Комбинированные средства защиты построены на основе комбинации пассивных и активных средств.

К наиболее широко применяемым пассивным методам защиты относятся:

• ограничение сигналов малой амплитуды;

• фильтрация сигналов высокочастотного навязывания;

• отключение преобразователей (источников) сигналов.

Возможность ограничения сигналов малой амплитуды основывается на нелинейных свойствах полупроводниковых элементов, главным образом диодов. В схеме ограничителя малых амплитуд используется диодный мост из включенных встречно. Такая система из двух диодов имеют сопротивление для токов малой амплитуды сотни кОм, а для токов большой амплитуды (полезных сигналов) - единицы Ом и менее, что исключает прохождение опасных сигналов малой амплитуды в телефонную линию и практически не оказывает влияние на прохождение через диоды полезных сигналов.

К простейшим изделиям, в которых реализован метод ограничения сигналов малой амплитуды, является устройство защиты аналоговых двухпроводных телефонных аппаратов (ТА) “Корунд” . Диодные ограничители устройства обеспечивают подавление низкочастотных сигналов малой амплитуды на частоте 1 кГц в сторону абонентской линии (АТС) более чем на 60 дБ. При ведении телефонных переговоров устройство практически не влияет на качество разговора (затухание речевых сигналов менее 2 дБ).

Метод фильтрации высокочастотных сигналов используется главным образом для защиты телефонных аппаратов от “высокочастотного навязывания”.[4]

Простейшим фильтром является конденсатор, устанавливаемый в звонковую цепь телефонных аппаратов с электромеханическим звонком и в микрофонную цепь всех аппаратов. Емкость конденсаторов выбирается такой величины, чтобы зашунтировать сигнал высокой частоты, подаваемый в линию и не оказывать существенного влияния на качество телефонных разговоров. Более сложное фильтрующее устройство представляет собой многозвенный LC-фильтр нижних частот.

Отключение преобразователей (источников) сигналов от линии при положенной трубке телефонного аппарата является наиболее эффективным методом защиты информации. [4]

Самый простой способ реализации этого метода защиты заключается в установке в корпусе телефонного аппарата или телефонной линии специального ручного переключателя. Более удобным в эксплуатации является установка в телефонной линии устройства защиты, автоматически отключающего телефонный аппарат от линии при положенной телефонной трубке. К типовым устройствам, реализующим данный метод защиты, относится устройство защиты двухпроводных телефонных линий связи "Барьер-М1"

Активные методы защиты от утечки информации за счет АЭП предусматривают подачу в линию при положенной телефонной трубке маскирующего сигнала речевого диапазона частот (как правило, основная мощность помехи сосредоточена в диапазоне частот стандартного телефонного канала: 300 - 3400 Гц). При снятии трубки телефонного аппарата подача в линию шумового сигнала прекращается. К устройствам, реализующим активные методы защиты, относится генератор шума "Гранит-12".

Устройство защиты «Прокруст- 2000» применяется с целью обеспечения защиты городской телефонной линии до АТС методом постановки активной помехи, подавляющей действие телефонных закладок во время разговора. Устройство предотвращает съем и передачу информации по телефонной линии в промежутках между телефонными переговорами, а также осуществляет обнаружение подключенных телефонных закладок и контролирует постоянную составляющую напряжения в телефонной линии.

При использовании активных средств защиты важно помнить, что постоянное использование таковых средств в активном режиме может привести к демаскированию защитного средства. Рекомендуется включать зашумление или кодирование линии только на время важных и конфиденциальных переговоров, поскольку если злоумышленник подключится в этот момент у линии, он услышит неразборчивый или малоразборчивый шум. Если же защита и зашумление будут включены постоянно, то злоумышленник поймет, что важная линия защищается и будет искать другой способ для добывания информации.

Несмотря на то, что телефонная проводная связь становится всё менее актуальной, важность её защиты остаётся на высоком уровне, поскольку большая часть государственных структур, а также крупные коммерческие компании внутри своих подразделений ведут переговоры именно по проводной телефонной связи, которую необходимо защищать должным образом.

Примечания

1. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1 Технические каналы утечки информации: учеб. пособие. – М.: Гостехкомиссия РФ, 1998. – 320 с.

2. Торокин А.А. Основы инженерно-технической защиты информации.— М.: Издательство «Ось-89», 1998 г. — 336 с.

3. Каторин. Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.

4. Бузов, Г.А. Защита от утечки информации по техническим каналам / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев. – М.: Горячая линия – Телеком, 2005. – 416 с.

5. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., МещеряковР.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО«Издательство Машиностроение», 2009 – 508 с.

6. Хорев А.А. Защита вспомогательных технических средств и систем от утечки по ним речевой информации [Электронный ресурс] // журнал «Специальная Техника» № 2, 2006 год. . – URL:http://www.ess.ru/sites/default /files/files/articles/2006/02/2006_02_08.pdf (дата обращения: 01.09.2015)

Соколов Александр Николаевич, к. т. н., доцент, зав. кафедрой безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет», г. Челябинск. E-mail: ANSokolov@inbox.ru

Антясов Иван Сергеевич, аспирант кафедры безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет», г. Челябинск. E-mail: antyasov@gmail.com

Яресько Антон Павлович, студент кафедры безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет).

Alexander Sokolov, a. M. N., Associate Professor, Head. the Department of Information Systems Security "South Ural State University", Chelyabinsk. E-mail: ANSokolov@inbox.ru

Antyasov Ivan, postgraduate Department of Information Systems Security "South Ural State University", Chelyabinsk. E-mail: antyasov@gmail.com

Yaresko Anton, students of the department of information systems security «South Ural State University» (National Research University).