УДК 681.3

В. А. Артамонов, Е.В. Артамонова

КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ
(Аналитический обзор)

Под ***техническим каналом утечки информации*** понимают совокупность источника информации, линий связи (физической среды), по которой распространяется информационный сигнал, шумов, препятствующих передаче сигнала в линиях связи, и технических и программных средств перехвата информации [1]. Источниками информации могут быть технические и программные средства информационно – коммуникационных технологий (ИКТ), непосредственно голосовой аппарат человека, излучатели систем звукоусиления, печатающие устройства, радиосистемы различного назначения и т.п.

Сигналы являются материальными носителями информации. По своей природе они могут быть ***электрическими, электромагнитными, акустическими*** *и др.* Сигналами, как правило, являются электрические, электромагнитные, акустические и другие виды колебаний (волн), причём информация содержится в изменениях их параметров.

В зависимости от природы сигналы распространяются в определённых физических средах. В общем случае средой распространения могут быть воздушные, жидкие и твёрдые среды. К ним относятся: воздушное пространство, конструкции зданий, соединительные и магистральные линии, токопроводящие элементы, грунт (земля) и т.п.

Шумы сопровождают все физические процессы и присутствуют на входе средств перехвата информации.

Средства перехвата информации служат для приёма и преобразования сигналов с целью получения информации.

1. Каналы утечки информации технических средств обработки, хранения и передачи информации

К техническим средствам приёма, обработки, хранения и передачи информации (ТСПИ) относят технические средства, непосредственно обрабатывающие конфиденциальную информацию. В их число входят ЭВМ, АТС, информационно-коммуникационные системы, системы оперативно-командной и громкоговорящей связи, системы звукоусиления, звукового сопровождения и звукозаписи и т.д.

При выявлении технических каналов ТСПИ необходимо рассматривать как систему, включающую основное оборудование, оконечные устройства, соединительные линии, структурированные кабельные линии локальных сетей, распределительные и коммутационные устройства, системы питания и заземления. Такие технические средства называют также *основными техническими средствами* ***(ОТС).***

Наряду с ТСПИ в помещениях устанавливаются технические средства и системы, непосредственно не участвующие в обработке конфиденциальной информации, но использующиеся наряду с ТСПИ и находящиеся в зоне электромагнитного поля, создаваемого ТСПИ. Такие технические средства и системы называются ***вспомогательными техническими средствами и системами (ВТСС)***. Это технические средства открытой телефонной и громкоговорящей связи, системы управления и контроля доступом, системы кондиционирования, электрификации, радиофикации, оповещения, электробытовые приборы и т.д.

В качестве канала утечки информации наибольший интерес представляют ВТСС, имеющие выход за пределы контролируемой зоны (КЗ).

Контролируемая зона *– территория (либо здание, группа помещений, помещение), на которой исключено неконтролируемое пребывание лиц и транспортных средств, не имеющих постоянного или разового допуска.*

В КЗ посредством проведения технических и режимных мероприятий должны быть созданы условия, предотвращающие утечки из неё конфиденциальной информации. КЗ определяется руководством организации, исходя из конкретной обстановки в месте расположения объекта и возможностей технических средств перехвата.

Кроме соединительных линий ТСПИ и ВТСС за пределы контролируемой зоны могут выходить провода и кабели, к ним не относящиеся, но проходящие через помещения, где установлены технические средства, а также металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции. Такие элементы называются *посторонними проводниками (ПП)*.

В зависимости от физической природы возникновения информационных сигналов, а также среды их распространения и способов перехвата, технические каналы утечки информации можно разделить на ***электромагнитные, электрические, параметрические и вибрационные***.

Электромагнитные каналы

К электромагнитным относятся каналы утечки информации, возникающие за счёт различного вида побочных электромагнитных излучений и наводок (ПЭМИН) ТСПИ:

– излучений элементов ТСПИ;

– излучений на частотах работы высокочастотных (ВЧ) генераторов ТСПИ;

– излучений на частотах самовозбуждения усилителей низкой частоты (УНЧ) ТСПИ.

Электромагнитные излучения элементов ТСПИ. В ТСПИ носителем информации является электрический ток, параметры которого (амплитуда, частота, фаза) изменяются по закону изменения информационного сигнала. При прохождении электрического тока по токоведущим элементам ТСПИ

вокруг них возникает электрическое и магнитное поля. В силу этого элементы ТСПИ можно рассматривать как излучатели электромагнитного поля, несущего информацию.

Электромагнитные излучения на частотах работы ВЧ – генераторов ТСПИ и ВТСС. В состав ТСПИ и ВТСС могут входить различного рода высокочастотные генераторы. К таким устройствам можно отнести: задающие генераторы, генераторы тактовой частоты, генераторы стирания и подмагничивания магнитофонов, гетеродины радиоприёмных и телевизионных устройств и т.п.

В результате внешних воздействий информационного сигнала (например, электромагнитных колебаний) на элементах ВЧ – генераторов наводятся электрические сигналы, которые могут вызвать паразитную модуляцию собственных ВЧ – колебаний генераторов. Эти модулированные ВЧ – колебания излучаются в окружающее пространство.

Электромагнитные излучения на частотах самовозбуждения УНЧ ТСПИ. Самовозбуждение УНЧ ТСПИ (например, усилителей систем звукоусиления и звукового сопровождения, магнитофонов, систем громкоговорящей связи и т.п.) возможно за счёт образования случайных паразитных обратных связей, что приводит к переводу усилителя в режим автогенерации сигналов. Сигнал на частотах самовозбуждения, как правило, оказывается промодулированным информационным сигналом. Самовозбуждение наблюдается, в основном, при переводе УНЧ в нелинейный режим работы, т.е. в режим перегрузки.

Перехват ПЭМИН ТСПИ осуществляется средствами радиотехнической разведки, размещёнными вне контролируемой эоны.

Электрические каналы

Электрические каналы утечки информации возникают за счёт:

– наводок электромагнитных излучений ТСПИ на соединительные линии ВТСС и посторонние проводники, выходящие за пределы КЗ;

– просачивания информационных сигналов в линии электропитания и цепи заземления ТСПИ;

– использования закладных устройств.

Наводки электромагнитных излучений ТСПИ возникают при излучении элементами ТСПИ информационных сигналов, а также при наличии гальванической связи соединительных линий ТСПИ и посторонних проводников или линий ВТСС. Уровень наводимых сигналов в значительной степени зависит от мощности излучаемых сигналов, расстояния до проводников, а также длины совместного пробега соединительных линий ТСПИ и посторонних проводников.

Случайной антенной является цепь ВТСС или посторонние проводники, способные принимать побочные электромагнитные излучения.

Случайные антенны могут быть сосредоточенными и распределёнными. *Сосредоточенная случайная антенна представляет собой компактное*

техническое средство (например, телефонный аппарат). К распределённым случайным антеннам относятся кабели, провода, металлические трубы и другие коммуникации.

Просачивание информационных сигналов в линии электропитания возможно при наличии магнитных связей между выходным трансформатором усилителя (например, УНЧ) и трансформатором блока питания. Кроме того, токи усиливаемых информационных сигналов замыкаются через источник электропитания, создавая на его внутреннем сопротивлении дополнительное напряжение, которое может быть обнаружено в линии электропитания. Информационный сигнал может проникнуть в линию электропитания также в результате того, что среднее значение потребляемого тока в оконечных каскадах усилителей зависит от амплитуды информационного сигнала, что создаёт неравномерную нагрузку на выпрямитель и приводит к изменению потребляемого тока *по закону изменения информационного сигнала.*

Просачивание информационных сигналов в цепи заземления. Кроме заземляющих проводников, служащих для непосредственного соединения ТСПИ с контуром заземления, гальваническую связь с землёй могут иметь различные проводники, выходящие за пределы КЗ. К ним относятся нулевой провод сети электропитания, экраны соединительных кабелей, металлические трубы систем водоснабжения и отопления, металлическая арматура железобетонных конструкций и т.д. Все эти проводники совместно с заземляющим устройством образуют разветвлённую систему заземления, в которую могут просачиваться информационные сигналы.

Перехват информационных сигналов возможен путём непосредственного подключения к соединительным линиям ВТСС и посторонним проводникам, проходящим через помещения, где установлены ТСПИ, а также к их системам электропитания и заземления.

Съём информации с использованием закладных устройств. Съём информации, обрабатываемой в ТСПИ, возможен путём установки в них электронных устройств перехвата – закладных устройств (ЗУ). ЗУ представляют собой мини – передатчики, излучение которых модулируется информационным сигналом. Электронные устройства перехвата информации, устанавливаемые в ТСПИ, иногда называют аппаратными закладками. Наиболее часто такие ЗУ устанавливаются в ТСПИ иностранного производства, однако возможна их установка и в отечественных средствах для ведения промышленной разведки. *Перехваченная с помощью ЗУ информация или непосредственно передаётся по радиоканалу, или сначала записывается на промежуточный носитель, а затем по команде передаётся на контрольный пункт перехвата.*

Параметрические каналы

Перехват информации возможен путём «высокочастотного облучения» («электромагнитного навязывания») ТСПИ. При взаимодействии

облучающего электромагнитного поля с элементами ТСПИ происходит переизлучение электромагнитного поля. В ряде случаев это вторичное излучение имеет модуляцию, обусловленную воздействием информационного сигнала.

Поскольку переизлученное электромагнитное поле имеет параметры, отличные от облучающего поля, данный канал утечки информации часто называют *параметрическим.*

Для перехвата информации по параметрическому каналу необходимы специальные высокочастотные генераторы с антеннами, имеющими узкие диаграммы направленности, и специальные приёмные устройства.

Вибрационные каналы

Некоторые ТСПИ имеют в своём составе печатающие устройства, для которых можно найти соответствие между распечатываемым символом и его акустическим образом.

Данный принцип лежит в основе канала утечки информации по вибрационному каналу.

2. Каналы утечки речевой информации

В случае когда источником информации является голосовой аппарат человека, информация называется *речевой.*

Речевой сигнал – сложный акустический сигнал, основная энергия которого сосредоточена в диапазоне 300 – 4000 Гц.

Голосовой аппарат человека является *первичным* источником акустических колебаний, которые представляют собой возмущения воздушной среды в виде волн сжатия и растяжения (продольных волн).

Под воздействием акустических колебаний в ограждающих строительных конструкциях и инженерных коммуникациях помещения, в котором находится речевой источник, возникают вибрационные колебания. Таким образом, в своём первоначальном виде речевой сигнал в помещении присутствует в виде акустических и вибрационных колебаний.

Различного рода преобразователи акустических и вибрационных колебаний являются *вторичными* источниками. К ним относятся: громкоговорители, телефоны, микрофоны, акселерометры др.

В зависимости от среды распространения речевых сигналов и способов их перехвата технические каналы утечки речевой информации можно разделить на: *акустические, вибрационные, акустоэлектрические, оптоэлектронные и параметрические.*

Акустические каналы

В акустических каналах утечки информации средой распространения речевых сигналов является воздух, и для их перехвата используются

высокочувствительные и направленные микрофоны, соединённые с портативными записывающими устройствами или со специальными передатчиками.

Автономное устройство, конструктивно объединяющее микрофон и передатчик, называют *закладным устройством*. Перехваченная ЗУ речевая информация может передаваться по радиоканалу, сети электропитания, оптическому каналу, соединительным линиям, посторонним проводникам, инженерным коммуникациям и т.д.

Использование диктофонов и ЗУ требует проникновения в контролируемое помещение (контролируемую зону). В том случае, когда это не удаётся, для перехвата речевой информации используются направленные микрофоны.

Виброакустические каналы

В виброакустических каналах утечки информации средой распространения речевых сигналов являются ограждающие строительные конструкции помещений и инженерные коммуникации. Для перехвата речевых сигналов в этом случае используют вибродатчики (акселерометры).

Вибродатчик, соединённый с электронным усилителем называют *электронным стетоскопом (ЭС)*. ЭС позволяет осуществлять прослушивание речи с помощью головных телефонов и её запись на диктофон.

По виброакустическому каналу также возможен перехват информации с использованием ЗУ. В основном для передачи информации используется радиоканал, поэтому такие устройства часто называют радиостетоскопами. Возможно использование ЗУ с передачей информации по оптическому каналу в ближнем инфракрасном диапазоне длин волн, а также по ультразвуковому каналу (по инженерным коммуникациям).

Акустоэлектрические каналы

Акустоэлектрические каналы утечки информации возникают за счёт преобразований акустических каналов в электрические.

Некоторые элементы ВТСС, в том числе трансформаторы, катушки индуктивности, электромагниты вторичных часов, звонков телефонных аппаратов и т.п., обладают свойством изменять свои параметры (ёмкость, индуктивность, сопротивление) под действием акустического поля, создаваемого источником речевого сигнала. Изменение параметров приводит либо к появлению на данных элементах электродвижущей силы (ЭДС), либо к модуляции токов, протекающим по этим элементам в соответствии с изменениями воздействующего электрического поля.

ВТСС, кроме указанных элементов, могут содержать непосредственно акустоэлектрические преобразователи. К таким ВТСС относятся некоторые типы датчиков пожарной и охранной сигнализации, громкоговорители

ретрансляционной сети и т.п. Эффект акустоэлектрического преобразования иногда называют « микрофонным эффектом».

Перехват акустоэлектрических колебаний в данном канале утечки информации осуществляется путём непосредственного подключения к соединительным линиям ВТСС специальных высокочувствительных УНЧ. Например, подключая такие средства к соединительным линиям телефонных аппаратов с электромеханическими вызывными звонками, можно подслушивать разговоры, ведущиеся в помещениях, где установлены эти аппараты.

Технический канал утечки информации с использованием «высокочастотного электромагнитного навязывания» может быть осуществлён путём несанкционированного контактного введения токов высокой частоты от соответствующего генератора в линии, имеющей функциональные связи с нелинейными или параметрическими элементами ВТСС, на которых происходит модуляция высокочастотного канала информационным. Информационный сигнал в данных элементах ВТСС появляется вследствие акустоэлектрического преобразования акустических сигналов в электрические. Промодулированный сигнал отражается от указанных элементов и распространяется в обратном направлении или излучается.

Наиболее часто такой канал используется для перехвата разговоров, ведущихся в помещении, через телефонный аппарат, имеющий выход за пределы контролируемой зоны.

Оптико – электронный (лазерный) канал

Оптико – электронный (лазерный) канал утечки акустической информации образуется при облучении лазерным лучом вибрирующих под действием акустического речевого сигнала отражающих поверхностей помещений (оконных стёкол, зеркал и т.д.). Отражённое лазерное излучение модулируется по амплитуде и фазе и принимается приёмником оптического (лазерного) излучения, при демодуляции которого выделяется речевая информация. Для организации такого канала предпочтительным является использования зеркального отражения лазерного луча. Однако, при небольших расстояниях до отражающих поверхностей (порядка нескольких десятков метров) может быть использовано диффузное отражение лазерного излучения.

Для перехвата речевой информации по данному каналу используются сложные лазерные системы – «лазерные микрофоны», работающие, как правило в ближнем инфракрасном диапазоне длин волн.

Параметрические каналы

В результате воздействия акустического поля меняется давление на все элементы высокочастотных генераторов ТСПИ и ВТСС. При этом

изменяется взаимное расположение элементов схем, проводов в катушках индуктивности, дросселей и т.п., что может привести к изменениям параметров высокочастотного сигнала, например, к модуляции его информационным сигналом. Поэтому этот канал утечки информации называется параметрическим. Наиболее часто наблюдается паразитная модуляция информационным сигналом излучений гетеродинов радиоприёмных и телевизионных устройств, находящихся в помещениях, где ведутся конфиденциальные переговоры.

Параметрический канал утечки информации может быть организован и путём «высокочастотного облучения» помещения, где установлены закладные устройства, имеющие элементы, параметры которых (например, добротность и резонансная частота объёмного резонатора) изменяются под действием акустического (речевого) сигнала.

При облучении помещения мощным высокочастотным сигналом в таком ЗУ при взаимодействии облучающего электромагнитного поля со специальными элементами закладки (например, четвертьволновым вибратором) происходит образование вторичных радиоволн, т.е. переизлучение электромагнитного поля. А специальное устройство закладки (например, объёмный резонатор) обеспечивает амплитудную, фазовую или частотную модуляцию переотражённого сигнала по закону изменения речевого сигнала.

Для реализации возможностей такого канала необходимы специальный передатчик с направленным излучением и приёмник.

3. Каналы утечки информации при её передаче по каналам связи

Для передачи информации используются КВ, УКВ, радиорелейные, тропосферные и космические каналы связи, различные виды телефонной радиосвязи (сотовые, транкинговые, Dect, Wi-Fi и др.), а также кабельные и волоконно – оптические линии связи.

В зависимости от вида канала связи технические каналы перехвата (утечки) информации можно разделить на ***электромагнитные, электрические и индукционные.***

Электромагнитные каналы

Электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться портативными средствами радиоразведки.

Данный канал утечки наиболее широко используется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым средствам связи и радиорелейным и спутниковым линиям связи.

Электрические каналы

Электрический канал перехвата информации, передаваемой по кабельным линиям связи, предполагает контактное подключение аппаратуры перехвата к кабельным линиям связи.

Контактный способ используется в основном для снятия информации с коаксиальных и низкочастотных кабелей связи (через согласующие устройства). Для кабелей, внутри которых поддерживается повышенное давление воздуха, применяются устройства, исключающие его снижение, для предотвращения срабатывания специальной сигнализации.

Электрический канал наиболее часто используется для перехвата телефонных разговоров, но может использоваться и для перехвата данных. Устройства, подключаемые к телефонным линиям и совмещённые с устройствами передачи по радиоканалу, иногда называют телефонными закладками.

Индукционный канал

Наиболее часто используемый способ контроля проводных линий связи, не требующий контактного подключения – индукционный. В индукционном канале используется эффект возникновения вокруг кабеля связи электромагнитного поля при прохождении по нему информационных электрических сигналов, которые перехватываются специальными индукционными датчиками.

Индукционные датчики применяются в основном для съёма информации с симметричных высокочастотных кабелей.

Современные индукционные датчики способны регистрировать информацию с кабелей, защищённых не только изоляцией, но и двойной бронёй из стальной ленты и стальной проволоки, плотно обвивающей кабель. Менее подвержены подобному съёму информации волоконно – оптические кабели.

Для бесконтактного съёма информации с незащищённых телефонных линий связи могут использоваться специальные высокочувствительные низкочастотные усилители, снабжённые магнитными антеннами, в ряде случаев оборудованными радиопередатчиками для передачи информации на контрольный пункт перехвата.

4. Технические каналы утечки видовой информации

Наряду с информацией, обрабатываемой в ТСПИ, и речевой информацией важную роль играет *видовая информация,* получаемая техническими средствами перехвата информации в виде изображений.

В зависимости от характера информации можно классифицировать следующие способы её получения:

– наблюдение за объектами;

– съёмка объектов;
– снятие копии документов.

Наблюдение и съёмка объектов и документов

В зависимости от условий наблюдения и освещения для наблюдения за объектами могут использоваться различные технические средства. Для наблюдения днём – оптические приборы (монокуляры, оптические трубы, бинокли, телескопы и т.д.), телевизионные камеры, для наблюдения ночью – приборы ночного видения, телевизионные камеры, тепловизоры.

Для наблюдения с большого расстояния используются средства аэро – и космической кино – фото съёмки, длиннофокусные оптические системы, а для наблюдения с близкого расстояния – камуфлированные скрытно установленные телевизионные камеры. При этом изображение с телевизионных камер может передаваться на мониторы как по кабелю, так и по радиоканалу.

Съёмка объектов проводится для документирования результатов наблюдения и более подробного изучения объектов. Для съёмки объектов используются телевизионные и фотографические средства, включая аэро – космические.

Съёмка документов осуществляется, как правило, с использованием портативных фотоаппаратов.

5. Каналы утечки информации, создаваемые атаками извне и внутри корпоративных систем ИКТ (объекта информатизации)

Атаки на системы ИКТ можно разделить на следующие группы:
– операционных систем;
– сетевого программного обеспечения;
– систем управления базами данных.

Атаки и каналы утечки информации СУБД

В большинстве случаев несанкционированный доступ осуществляется преодолением защиты компьютерных систем на уровне операционных систем, что позволяет получить доступ к файлам СУБД с помощью средств операционной системы. Однако, в ряде случаев, для высокоорганизованных СУБД существуют средства самих систем для защиты от вторжений, включая криптографические (Oracle и др.).

Атаки на уровне операционной системы

Защита операционных систем (ОС) является сложной задачей. Дело в том, что структуры современных ОС, чрезвычайно сложны, и поэтому

соблюдение адекватных политик безопасности на практике является довольно трудной задачей.

Возможные атаки, как внешние, так и внутренние, в виде несанкционированного доступа (НСД) могут порождать технические каналы информации, характеристики и параметры которых в значительной степени зависят от архитектуры и конфигурации конкретных ОС. Однако существуют общие для всех методы НСД, которые сводятся к следующим характерным атакам:

– кража пароля или другой идентификационной информации;

– получение пароля из файла, в котором он был сохранён пользователем; кража внешнего носителя парольной информации и т.д.;

– сканирование жёстких дисков компьютера;

– сборка «мусора» (если средства ОС позволяют восстанавливать ранее удалённые объекты);

– превышение полномочий (используются ошибки в программном обеспечении или администрировании ОС);

– отказ в обслуживания (Denial of Service – DoS).

Атаки на уровне сетевого программного обеспечения

Распределённые структуры и сети являются наиболее уязвимыми по части атак проводимых злоумышленниками, потому что канал связи, по которому циркулирует сетевой трафик, чаще всего не защищён, и всякий, кто может иметь доступ к нему, соответственно может перехватывать сообщения и отправлять свои собственные. На уровне сетевого программного обеспечения (СПО) возможны следующие виды атак, в том числе, приводящим к образованию технических каналов утечки информации [2]:

– прослушивание сегмента локальной сети;

– перехват сообщений на маршрутизаторе и создание ложного маршрута (на сленге хакеров маршрутизатор – «лучший друг»);

– навязывание сообщений – *снифферы пакетов* (отправляя в сеть сообщения с ложным обратным адресом, злоумышленник переключает на свой компьютер уже установленные сетевые соединения и в результате получает права пользователей);

– распределённый отказ в обслуживании (DDoS – distributed DoS);

– атаки типа *«человек посредине»* (Man – in – the – Middle). Для атак этого типа часто используют снифферы пакетов, транспортные протоколы и протоколы маршрутизации. Атаки проводятся с целью кражи информации, перехвата текущей сессии и получения доступа к частным сетевым ресурсам, для получения информации о сети, её пользователях и анализе сетевого трафика, для проведения атак типа DoS/DDoS, искажения передаваемых данных и ввода несанкционированной информации в сетевые сессии.

В общем случае *несанкционированный доступ* не может считаться отдельным типом атаки. Большинство сетевых атак проводятся ради получения НСД к ресурсам ИКТ. Например, чтобы подобрать логин Telnet, злоумышленник должен сначала получить подсказку Telnet на своей системе. После подключения к порту Telnet на экране появится сообщение *«authorization required to use this resource»* («для пользования этим ресурсом нужна авторизация»). Если после этого «хакер» («инсайдер») продолжит попытки доступа, они будут считаться несанкционированными. Источник таких атак может находиться как внутри сети, так и снаружи.

Для противодействия указанным методам НСД следует максимально использовать защиту систем коммуникаций и СПО с целью затруднения (в идеале предотвращения) доступа к ресурсам ИКТ неавторизованным (нелигитимным) пользователям. В качестве таких мер используют создание демилитаризованных и доверенных зон методами межсетевого экранирования, методы и системы активного аудита на основе систем обнаружения и предотвращения вторжений (IDS/IPS – системы), виртуальные частные сети – VPN, системы доверенной первоначальной загрузки и разграничения полномочий (ролевое управление, дискреционный и мандатный доступ к ресурсам ИКТ).

Сетевая разведка

Под сетевой разведкой подразумевается сбор информации о сети с помощью общедоступных данных и приложений. При подготовки атаки против какой либо сети злоумышленник, как правило, пытается получить о ней как можно больше информации. Сетевая разведка проводится в форме запросов *доменных сетевых имён – DNS,* эхо – тестирования и сканирования портов.

Запросы DNS помогают понять, кто владеет тем или иным доменом и какие адреса этому домену присвоены.

Эхо – тестирование (ping sweep) адресов, раскрытых с помощью DNS, позволяет увидеть, какие хосты реально работают в данной среде. Получив список хостов, хакер использует средства сканирования портов, чтобы составить полный список услуг, поддерживаемых этими хостами.

Избавиться от сетевой разведки невозможно. К примеру, отключив эхо –ISMP и эхо – ответ на периферийных маршрутизаторах, избежав тем самым эхо – тестирования, теряются данные, необходимые для сетевых сбоев. Кроме того, сканировать порты можно и без предварительного эхо – тестирования. Просто это займёт больше времени, т.к. придётся сканировать и несуществующие IP – адреса. Системы IDS/IPS на уровне сети и хостов обычно хорошо справляются с задачей уведомления администратора безопасности (офицера безопасности) о ведущейся сетевой разведке, что в свою очередь, позволяет лучшему противодействию сетевой атаке и оповещению провайдера (ISP) из сети которого замышляется атака.

Атаки на уровне приложений

Атаки на уровне приложений могут проводиться несколькими способами. Самый распространённый из них состоит в использовании уязвимостей серверного ПО (sendmail, HTTP, FTP). Используя эти уязвимости злоумышленники могут получить доступ к компьютеру от имени авторизованного пользователя, работающего с приложением (как правило, это бывает не простой пользователь, а привилегированный администратор с правами системного доступа). Сведения об атаках на уровне приложений, как правило, публикуются, чтобы дать возможность администраторам безопасности («офицерам безопасности») произвести корректировку с помощью «патчей» (заплат). Однако, эти публикации доступны в том числе и хакерам.

Главная проблема с атаками на уровне приложений состоит в том, что они часто пользуются портами, которым разрешён проход через демилитаризованную зону (DMZ) или отдельно стоящий межсетевой экран (МЭ).

К примеру, хакер, эксплуатирующий уязвимость, часто использует в ходе атаки TCP порт 80. Поскольку WEB–сервер предоставляет пользователям WEB – страницы, МЭ должен предоставлять доступ к этому порту. При этом, с точки зрения МЭ, атака расценивается как нормальный трафик порта 80.

Полностью исключить атаки на уровне приложений невозможно, свидетельством тому являются постоянные публикации хакеров и системных аналитиков об обнаружении новых уязвимостей тех или иных приложений. Поэтом, здесь необходимо сконцентрировать внимание на разработку подробной политики безопасности и скрупулёзной её выполнимости. В качестве примера, приведём некоторые установки политики безопасности, которые необходимо выполнять для снижения уязвимостей для атак данного типа:

- *читайте лог – файлы операционных систем и сетевые лог – файлы и/или анализируйте их с помощью специальных приложений;*
- *подпишитесь на услуги по рассылке данных о слабых местах прикладных программ: Bugtraq (http://www.securityfocus.com/archive/1)*
- *пользуйтесь самыми свежими версиями ОС и приложений и самыми последними коррекционными модулями (патчами);*
- *кроме системного администрирования, пользуйтесь системами распознавания атак (IDS).*

Существуют две взаимодополняющие друг друга технологии IDS:

– сетевая система IDS (NIDS) отслеживает все пакеты, проходящие через определённый домен. Когда система NIDS видит пакет или серию пакетов, совпадающих с сигнатурой известной или вероятной атаки, она генерирует сигнал тревоги и/или прекращает сессию;

– хост-система IDS (HIDS) защищает хост с помощью программных агентов. Эта система борется с атаками против одного хоста;

- *в своей работе системы IDS пользуются сигнатурами атак, которые представляют собой профили конкретных атак либо их типов. Сигнатуры определяют условия, при которых трафик считается хакерским. Аналогами IDS в мире физической защиты объектов можно считать систему предупреждения или камеру наблюдения. Самым большим недостатком IDS является её способность генерировать ложные сигналы тревоги. Чтобы минимизировать количество ложных срабатываний и добиться корректного функционирования системы IDS в сети, необходима тщательная её настройка.*

Злоупотребление доверием

В общем случае, этот тип действий не является атакой. Он представляет собой злонамеренное использование отношений доверия, существующих в сети. Классическим примером такого злоупотребления является ситуация в пограничной части корпоративной сети. В этом сегменте часто располагаются серверы DNS, SMTP, HTTP. Поскольку все они принадлежат к одному и тому же сегменту, взлом одного из них приводит к взлому и всех остальных, так как эти серверы доверяют другим системам своей сети. Другим примером является система, установленная с внешней стороны межсетевого экрана, имеющая отношения доверия с системой, установленной с внутренней стороны МЭ. В этом случае, взлом внешней системы приводит к риску проникновения в систему, защищённую МЭ.

Риск злоупотребления доверием можно снизить за счёт более жёсткого контроля уровней доверия в пределах своей сети (например, использованием дискреционного и мандатного методов доступа) и более тщательного сегментирования серверных частей сети с помощью коммутаторов. Системы, расположенные вне демилитаризованных зон, никогда не должны пользоваться абсолютным доверием со стороны защищённых МЭ систем. Отношения доверия должны ограничиваться определёнными протоколами и, по возможности, аутентифицироваться не только поIP – адресам, но и по другим параметрам.

Переадресация портов представляет собой разновидность злоупотребления доверием, когда взломанный хост используется для передачи через межсетевой экран трафика, который в противном случае был бы отбракован. Представим себе МЭ с тремя интерфейсами, к каждому из которых подключён определённый хост. Внешний хост может подключаться к хосту общего доступа (DMZ), но не к хосту, установленному с внутренней стороны МЭ. Хост общего доступа может подключаться и к внутреннему, и к внешнему хосту. Если хакер захватит хост общего доступа, он сможет установить на нём программное средство, перенаправляющее трафик с внешнего хоста прямо на внутренний хост. Хотя при этом, не нарушается ни одно правило, действующее на МЭ,

внешний хост в результате переадресации получает прямой доступ к защищённому хосту.

Основным способом борьбы с переадресацией портов является использование надёжных моделей доверия. Кроме того, помешать хакеру установить на хосте свои программные средства может хост – система IDS (HIDS).

Вирусы и приложения типа «червь» и «троянский конь»

Рабочие станции конечных пользователей в значительной степени уязвимы относительно вирусных атак и вредоносных программ типа «червь» и «троянский конь».

Вирус – программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам. Под вирусом чаще всего понимается не "традиционный" вирус, а практически любая вредоносная программа. Это приводит к путанице в терминологии, осложненной еще и тем, что практически все современные антивирусы способны выявлять указанные типы вредоносных программ, таким образом ассоциация "вредоносная программа-вирус" становится все более устойчивой. Исходя из этого, а также из назначения антивирусных средств, в дальнейшем, если это не будет оговорено отдельно, под вирусами будут подразумеваться именно вредоносные программы.

Вредоносная программа – компьютерная программа или переносной код, предназначенный для реализации угроз информации, хранящейся в компьютерной системе (КС), либо для скрытого нецелевого использования ресурсов КС, либо иного воздействия, препятствующего нормальному функционированию КС.

К вредоносным программам относятся компьютерные вирусы, трояны, сетевые черви и др. Компьютерные вирусы, трояны и черви являются основными типами вредоносных программ.

Для активации вируса необходимо, чтобы зараженный объект получил управление. Деление вирусов происходит по типам объектов, которые могут быть заражены:

Загрузочные вирусы – вирусы, заражающие загрузочные сектора постоянных и сменных носителей.

Файловые вирусы – те, которые непосредственно работают с ресурсами операционной системы.

Макровирусы – вирусы, написанные на языке макрокоманд и исполняемые в среде какого-либо приложения. В подавляющем большинстве случаев речь идет о макросах в документах Microsoft Office.

Скрипт-вирусы – вирусы, исполняемые в среде определенной командной оболочки: раньше – bat-файлы в командной оболочке DOS, сейчас чаще VBS и JS - скрипты в командной оболочке Windows Scripting Host (WSH).

Червь (сетевой червь) – тип вредоносных программ, распространяющихся по сетевым каналам, способных к автономному преодолению систем защиты автоматизированных и компьютерных сетей, а также к созданию и дальнейшему распространению своих копий, не всегда совпадающих с оригиналом, и осуществлению иного вредоносного воздействия.

Сетевые черви – черви, использующие для распространения протоколы Интернет и локальных сетей. Обычно этот тип червей распространяется с использованием неправильной обработки некоторыми приложениями базовых пакетов стека протоколов tcp/ip.

Почтовые черви – черви, распространяющиеся в формате сообщений электронной почты.

IRC-черви – черви, распространяющиеся по каналам IRC (Internet Relay Chat).

P2P-черви — черви, распространяющиеся при помощи пиринговых (peer-to-peer) файлообменных сетей.

IM-черви – черви, использующие для распространения системы мгновенного обмена сообщениями (IM, Instant Messenger – ICQ, MSN Messenger, AIM и др.). Сегодня наиболее многочисленную группу составляют почтовые черви. Сетевые черви также являются заметным явлением, но не столько из-за количества, сколько из-за качества: эпидемии, вызванные сетевыми червями зачастую отличаются высокой скоростью распространения и большими масштабами. IRC-, P2P- и IM-черви встречаются достаточно редко, чаще IRC, P2P и IM служат альтернативными каналами распространения для почтовых и сетевых червей.

Троян (троянский конь) — тип вредоносных программ, основной целью которых является вредоносное воздействие по отношению к компьютерной системе. *Трояны* отличаются отсутствием механизма создания собственных копий. Некоторые *трояны* способны к автономному преодолению систем защиты КС, с целью проникновения и заражения системы. В общем случае, *троян* попадает в систему вместе с вирусом либо *червем*, в результате неосмотрительных действий пользователя или же активных действий злоумышленника. В силу отсутствия у *троянов* функций размножения и распространения, их жизненный цикл крайне короток – всего три стадии: проникновение на компьютер, активация, выполнение заложенных функций. Это, само собой, не означает малого времени жизни *троянов*. Напротив, *троян* может длительное время незаметно находиться в памяти компьютера, никак не выдавая своего присутствия, до тех пор, пока не будет обнаружен антивирусными средствами. Задачу проникновения на компьютер пользователя *трояны* решают обычно одним из двух следующих методов.

Маскировка – *троян* выдает себя за полезное приложение, которое пользователь самостоятельно загружает из Интернет и запускает. Иногда

пользователь исключается из этого процесса за счет размещения на Web-странице специального скрипта, который используя дыры в браузере автоматически инициирует загрузку и запуск *трояна*.

Кооперация с вирусами и червями – *троян* путешествует вместе с червями или, реже, с вирусами. В принципе, такие пары *червь-троян* можно рассматривать целиком как составного *червя*, но в сложившейся практике принято троянскую составляющую червей, если она реализована отдельным файлом, считать независимым трояном с собственным именем. Кроме того, *троянская* составляющая может попадать на компьютер позже, чем файл *червя*.

Борьба с вирусами «червями» и «троянскими конями» ведётся с помощью эффективного антивирусного программного обеспечения, работающего на пользовательском уровне, реже на уровне сети. В общем случае, теоретически доказано, что задача обнаружения вирусов является неразрешимой. В реальной жизни антивирусная программа считается качественной, если она обнаруживает все жизнеспособные экземпляры вируса, желательно также его нежизнеспособные ответвления, и при этом характеризуется сравнительно небольшим числом ложных срабатываний. Следует избегать лишь тех ложных срабатываний, которые затрагивают существующие программы, используемые в повседневной работе различными пользователями. Ложные срабатывания на искусственных примерах, появление которых на компьютерах пользователей близко к нулю, вполне допустимы. Большинство вирусов, червей и троянов обнаруживаются современными антивирусными средствами с довольно высокой вероятностью, при условии регулярного обновления сигнатурных баз и эвристических алгоритмов распознавания.

Программные закладки

Программная закладка (ПЗ) – недокументированный модуль, внедряемый в общесистемные программные средства, прикладные программы и аппаратные средства ИКТ.

Существует три основные группы деструктивных действий, которые могут осуществляться ПЗ:

– копирование информации пользователей ИКТ (паролей, криптографических ключей, кодов доступа, конфиденциальных электронных документов, находящихся в оперативной или внешней памяти этих систем;

– изменение алгоритмов функционирования системных, сетевых, прикладных и служебных программ;

– навязывание определённых режимов работы (например, блокирование записи на диск при удалении информации, при этом информация, которую требуется удалить, не уничтожается и может быть в последствии скопирована или передана по электронной почте на пункт перехвата).

Бороться с ПЗ чрезвычайно сложно. Для этого при поставке ПО для критически важных объектов необходимо требовать от поставщика

(«вендора») алгоритмы программ и / или их исходные тексты (объектные модули). Затем следует этап проверки (верификации) и тестирования ПО на соответствие представленным документам. Данную процедуру обычно выполняют специальные, аккредитованные органом по сертификации испытательные центры (лаборатории), с выдачей сертификата соответствия продукта или системы ИТ нормам информационной безопасности на соответствие которым проводились испытания.

Инсайдерские каналы утечки информации

Утечка конфиденциальных корпоративных данных может нанести серьезный вред бизнесу компании [3]. Утрата таких данных в результате кражи по заказу конкурентов или небрежности собственных сотрудников компании неизбежно влечет потерю конкурентного преимущества, наносит вред репутации компании, вызывает отток клиентов и приводит к санкциям со стороны регулирующих органов, начиная от предупреждений и штрафов и заканчивая отзывом лицензий на основные виды бизнеса. Как правило, подобным видом деятельности занимается определённая, мотивированная (в том числе и методами «социальной инженерии») группа людей – *инсайдеры*.

Инсайдер (англ. insider) – член какой-либо группы людей, имеющей доступ к информации, недоступной широкой общественности. Термин используется в контексте, связанном с секретной, скрытой или какой-либо другой закрытой информацией или знаниями: инсайдер – это член группы, обладающий информацией, имеющейся только у этой группы.

Ни для кого не секрет, что информация сейчас занимает первое место в конкурентной борьбе и соответственно утечка информации за пределы компании может нанести непоправимый ущерб репутации и финансовому положению организации. В связи с этим сейчас ведутся активные споры насчет реализации политики информационной безопасности в компаниях, а также обсуждаются проблемы инсайдерства. Пока же ясно одно – для того, чтобы защищать информацию, нужно контролировать потоки ее передачи и способы использования.

Проблема защиты информации от инсайдерских угроз сейчас стоит очень остро. За последнее время обсуждение этого явления идет активнее, чем полемика по вопросам антивирусной защиты, хакерских атак или спама. Проходит огромное количество конференций, посвященных этой проблеме, эксперты в области информационной безопасности спорят, какой из способов защиты информации от инсайдеров надежнее – аппаратный или программный. Но все мнения сходятся в одном: для того, чтобы защищать коммерчески важную информацию, необходим контроль. Этот контроль может выражаться в ограничении прав доступа различных групп пользователей к документам и приложениям, а также в построении эффективной системы безопасности компании на основе тщательно выверенной и постоянно обновляемой политики безопасности. Некоторые эксперты отмечают, что в настоящее время одной из проблем при реализации

стратегии (политики) информационной безопасности в компании является то, что далеко не всегда можно провести грань между тайной личной жизни сотрудника и его служебными обязанностями.

Участившиеся случаи инсайдерства в России, странах СНГ и за рубежом доказывают, что теперь нужно беспокоиться не только о защите от угроз, исходящих извне, из Интернета и т.д., но и защищать секретную информацию от недобросовестных сотрудников собственной компании. В зависимости от потребностей, способа организации работы в компании и/или корпоративной сети, можно выбрать программные или аппаратные средства защиты информации, а также применять особый режим политики безопасности организации.

В первую очередь для борьбы с инсайдерством в компании необходимо наладить четкую систему контроля и аудита за использованием тех или иных документов в работе сотрудников. Для этого нужно использовать специальные настройки программного обеспечения для ограничения доступа группам пользователей к отдельным частям корпоративной сети и к документам (дискреционный и /или мандатный доступ). Для различных сотрудников компании должны быть утверждены, соизмеримые с их ролью, стандарты политики безопасности. Так, в некоторых компаниях реализовано такое решение при работе с корпоративными приложениями: ограничен доступ к внутренним ресурсам и происходит ограничение функционала при работе с приложениями. Например, есть документы, которые пользователь может только просматривать, но не может изменять или печатать. Кроме того, может быть установлено ограничение на время работы с документом (например, не более 8 часов в день или 1 часа непрерывно), или ограничение на количество запусков приложения. Есть несколько подобных решений, которые могут помочь осуществить защиту информации от инсайдеров в рамках корпоративной сети.

В последнее время наибольшее распространение для борьбы с инсайдерскими утечками информации получили так называемые DLP (Data Leak Prevention) – системы или системы предотвращения утечек конфиденциальной информации, которые позволяют контролировать обращение информации, защитить ее от несанкционированного доступа и распространения.

DLP-решение позволяет бороться не только с утечками информации, но со всей совокупностью угроз, связанных с обращением информации:

– нецелевое использование инфраструктуры;

– использование каналов связи во вред компании;

– нарушение политики информационной безопасности.

Однако, повсеместному применению DLP–систем препятствуют некоторые нюансы, которые не всегда учитываются потребителями.

В отличие от антивируса, DLP, по определению, не может быть готовым продуктом. Это – некая платформа, которую можно использовать с разными целями и по различным сценариям, и которая непременно должна поддерживаться процессами внутри организации. И

вот это-то внедрение в бизнес – процессы компании зачастую становится тормозом к внедрению этих технологий в инфраструктуру поддержки бизнеса этих компаний. Клиенту хотелось бы решить все свои проблемы одним махом: купил, настроил, забыл. И вот незадача – оказывается, DLP «из коробки» не работает. У всех компаний собственные бизнес-процессы, уникальная система движения информации, индивидуальный набор каналов коммуникаций, совершенно разный набор терминов и что особенно – требований к конфиденциальной информации. Все эти аспекты должны быть проанализированы на этапе внедрения проекта, по результатам написана методика использования системы внутри компании, под нее должны быть подстроены управленческие акты внутри компании и пр.

Более подробно о DLP – системах и о технологиях их использования см. на сайте [4].

Заключение

Как следует из приведенного обзора, количество и природа технических каналов утечки информации велико и, к большому сожалению, непрерывно возрастает. Рынок систем и технологий конфиденциального съёма и получения информации (в большей части нелегальный или находящийся в арсенале спецслужб) огромный, что в свою очередь побуждает к развитию сервисов и систем информационной безопасности. Таким образом, извечное противоборство «снаряда и брони» перманентно продолжается. В ряде случаев бытует мнение (или кем - то «ненавязчиво» внушается), что методы инженерно – технической разведки (ПЭМИН, акустика, электромагнитное навязывание и т.д.) ушли в прошлое как атрибут «холодной войны» и являются «шпионскими страшилками». К большому сожалению, это всё не так. Законы рыночной экономики, конкурентная борьба (зачастую недобросовестная), в ряде случаев толкают субъекты хозяйствования и физические лица к применению подобных технологий. Поэтому, в условиях повсеместного использования программно – технических методов и средств обеспечения ИБ не следует забывать и о физической и инженерно – технической защите активов компании. Все эти моменты, включая и мотивацию, должны быть тщательно прописаны в политике безопасности организации (повсеместное использование IDS/IPS и DLP – систем мотивируют нарушителей ИБ на использование иных методов и технологий съёма информации).

Литература

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

2. Решения компании Cisco Systems по обеспечению безопасности корпоративных сетей (издание II). [Электронный ресурс]. – Минск, 2012. – Режим доступа: http://itzashita.ru/. – дата доступа: 27. 08. 2012 г.

3. Утечки корпоративной информации и конфиденциальных данных. [Электронный ресурс]. – Минск, 2012. – Режим доступа: http://itzashita.ru/. – дата доступа: 27. 08. 2012 г.
4. Как работают DLP – системы: разбираемся в технологиях предотвращения утечки информации. [Электронный ресурс]. – Минск, 2012. – Режим доступа: http://itzashita.ru/. – дата доступа: 27. 08. 2012 г.