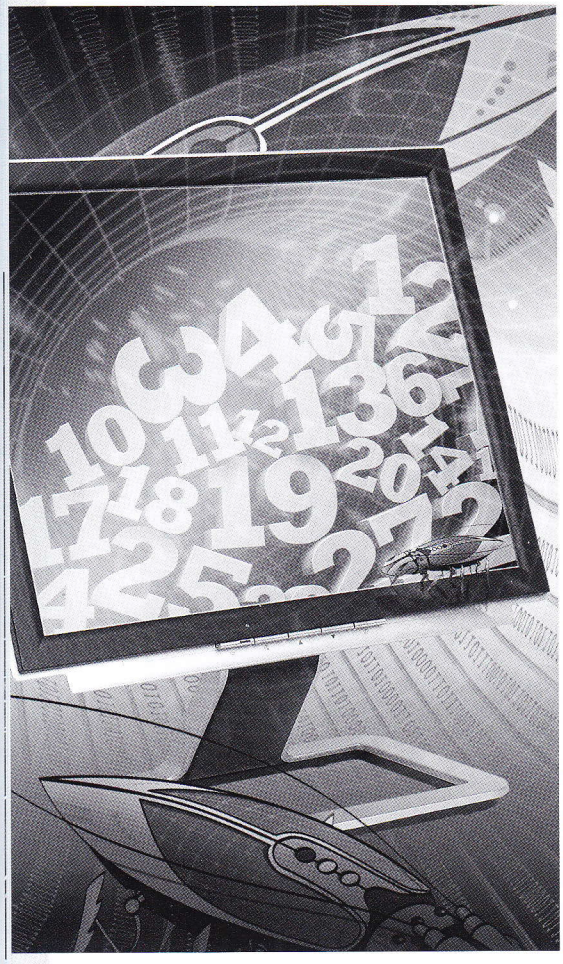
Что такое «закладочные устройства» и как с ними бороться. Часть 5

Г. А. Бузов, *кандидат военных наук, доцент, заведующий лабораторией защиты информации от утечки по техническим каналам*

Учебный центр «Информзащита»

Рассматривая вопросы выявления закладочных устройств (ЗУ), в предыдущих статьях мы уделяли основное внимание вопросам выявления радиомикрофонов как наиболее опасных и легко устанавливаемых устройств. Однако наличие в помещениях проводных линий различного назначения позволяет злоумышленникам успешно использовать их для негласного получения информации, а следовательно, есть необходимость рассмотреть вопросы выявления данных каналов. Выявление утечки информации по проводным линиям целесообразно выделить в отдельное направление, учитывая специфические особенности съема информации по линиям различного назначения.



Основными видами проводных линий, находящихся в офисах и подлежащих приборной проверке, являются: линии электросети, различные абонентские телефонные линии, линии систем пожарной, охранной сигнализации и линии неустановленного назначения.

При оценке возможностей использования проводных линий для перехвата информации необходимо определить степень угроз и возможности вероятного противника. Это в существенной мере уменьшит объем планируемых работ и позволит более целенаправленно проводить поисковые мероприятия. В любом случае основными видами поисковых работ в ходе проверки являются:

- визуальный осмотр линий и оборудования проводных коммуникаций с целью обнаружения несанкционированных подключений сетевых ЗУ;
- поиск сигналов ЗУ в проводных и кабельных линиях с помощью специальной поисковой аппаратуры.

Общая методика проверки одинакова для линий и оборудования различного назначения. Проверка реализуется в соответствии с имеющимися схемами прокладки и монтажа линий. Проверку сложной сети, имеющей большое количество отводов, обычно проводят по отдельным ее участкам.

Рассмотрим методику и особенности проверки линий различного назначения.

При проверке линий и оборудования силовой и осветительной электросети целесообразно разделить схему обследуемой сети на несколько отдельных участков, каждый из которых при проведении проверки может быть отключен от источника питающего напряжения. После этого проверка линий и оборудования проводится последовательным осмотром каждого участка.

Перед визуальным осмотром проверяемый участок сети целесообразно обесточить. Для исключения случайной подачи на него напряжения необходимо принять меры безопасности: выключить предохранители, вставить диэлектрические прокладки между контактами рубильника, магнитного пускателя, выве-

сить плакаты «Не включать, работают люди!» на рубильник и автоматы питания, изолировать отсоединенный на распределительном щите провод. При невозможности обесточить участок, а также в случаях, когда обесточивание нецелесообразно по соображениям конспирации, работы необходимо проводить не менее чем двумя членами поисковой бригады, у которых должен быть допуск к работе на электроустановках с напряжением до 1000 вольт.

Целесообразно придерживаться следующей последовательности работ:

- перед осмотром с помощью тестера или другого измерительного прибора проверить отсутствие напряжения на каждом электроустановочном, коммутационном изделии и другом оборудовании коммуникаций или участка проводных (кабельных) линий с открытыми для доступа токоведущими частями;
- путем визуального осмотра выявить отсутствие новых или подмененных элементов оборудования;
- в случае подозрений на вскрытие изделия, элемента, а также при обнаружении новых, недавно установленных изделий эти изделия и элементы оборудования вскрываются, разбираются и осматриваются;
- при осмотре необходимо убедиться в стандартном расположении элементов внутреннего устройства, а также отсутствии под крышкой посторонних предметов, новых деталей или элементов неясного назначения, подключений посторонних проводников к токоведущим частям.

Выявленные подозрительные детали и элементы необходимо тщательно осмотреть и установить их истинное назначение. При осмотре особое внимание обращается на наличие признаков сложного, нестандартного внутреннего устройства обнаруженных элементов, наличие проводников, небольших отверстий, которые могут использоваться для внедрения скрытого микрофона. При необходимости для дополнительной проверки привлекаются технические средства.

Кроме того, повышенное внимание при осмотре мест установки изделий и оборудования (электрощитов, распределительных и установочных коробок, боксов, установочных ниш) необходимо уделить осмотру подходящих кабелей, проводов и элементов их скрытой подводки (кабельных каналов, электротехнических труб, металлорукавов, гофрошлангов, пазов, штроб, отверстий в стене и других ограждающих конструкциях). В процессе осмотра провода и кабели следует вытянуть из закладных труб (кабельных каналов) на максимальную длину, чтобы убедиться в отсутствии несанкционированных подключений к ним. Каналы осмотреть с использованием эндоскопа также на максимально возможную глубину.

Демонтировать крышки кабельных каналов. Визуально убедиться в отсутствии посторонних предметов и подключений на всем протяжении открытых участков прокладки кабелей и проводных линий, а также на участках их прокладки в наружных кабельных каналах (коробах).

Кроме щитов, распределительных коробок, розеток, выключателей, электропатронов и других установочных изделий необходимо разобрать и осмотреть все подключаемые к силовой и осветительной сети разветвители, переходники и потребители электроэнергии: удлинители, тройники, люстры, бра, люминисцентные светильники, настольные лампы, кондиционеры, вентиляторы, нагревательные приборы и т. д. Разборке и осмотру также подлежат сетевые штепсельные вилки потребителей электроэнергии.

Методика проверки данных проводных линий с помощью приборов практически одинакова и, как правило, проводится после визуального осмотра. Порядок подключения к линиям зависит от используемой аппаратуры и, в большинстве своем, осуществляется с использованием адаптеров и различных щупов, конфигурация которых зависит от характера проверяемой линии. Анализу подвергается, как правило, общий диапазон от 0 до 15 МГц, при этом наиболее оптимальным будет следующий порядок работы.

Проводится подготовка контролируемого помещения, для чего необходимо проверить соответствие количества и назначения реально присутствующих в нем проводных линий представленным схемам их прокладки.

Выбираются наиболее удобные наконечники к щупам применительно к типу и особенностям имеющихся проводных линий.

В процессе проверки наибольшее внимание уделяется диапазону от 40 до 2500 кГц как наиболее типичному для закладочных устройств, питающихся от напряжения проводных линий и передающих перехваченную информацию по проводам. Значительно реже встречаются закладочные устройства с частотами около 7 МГц и выше. Для обеспечения гарантированной надежности обнаружения закладочных устройств по частоте верхняя граница диапазона сканирования в приборах должна быть не менее 15 МГц.

Для выявления ЗУ в проводных и кабельных линиях с помощью поисковой аппаратуры все осветительные, бытовые приборы и другие потребители электроэнергии в проверяемом помещении должны быть подключены к электросети и приведены в рабочее состояние (включены). Это переведет в рабочее состояние возможно внедренные в эти приборы устройства ЗУ. Наличие сигналов ЗУ необходимо проверить отдельно в каждой фазе систем силовой и осветительной электросети. Для этой цели поисковый прибор с помощью входящих в его комплектацию специальных щупов (кабелей) поочередно подключается к каждой из фаз проверяемой системы.

Для активизации ЗУ с акустопуском и маскирования поисковых работ в проверяемом помещении необходимо создать тестовый акустический сигнал. Нелишне напомнить о том, что создаваемый в помещении звуковой фон необходим не только для работы многих поисковых приборов, но и обеспечивает маскировку шумов и звуков, возникающих в ходе работ поисковой бригады. Для этого целесообразно создавать звуковой фон, подходящий для ситуации, возникающей в ходе скрытой

проверки помещения. Тестовый сигнал необходимо включать перед началом проведения визуального осмотра ограждающих конструкций, мебели и других предметов интерьера помещения. При этом наиболее подходящим может быть воспроизведение предварительно сделанной записи производственных шумов, доклада, делового семинара, занятий по совершенствованию профессиональной подготовки. Таким образом, создается акустический фон, не вызывающий подозрений у подслушивающего противника. Продолжительность звучания используемых записей должна быть не менее запланированной длительности поисковых и исследовательских работ.

Методика дальнейших действий определяется типом используемого для выявления сигналов ЗУ поискового прибора. Как правило, большинство приборов такого назначения имеют высокочувствительный малошумящий усилитель низкой частоты для обнаружения в линиях сигналов звукового диапазона частот и перестраиваемый приемник высокочастотных электрических сигналов. Поиск высокочастотных сигналов осуществляется вручную или автоматически путем перестройки приемника по частоте. В процессе поиска обеспечивается индикация уровней обнаруженных сигналов, их демодуляция и слуховой контроль.

При наличии в линии сигналов ЗУ через наушник прибора на выходе приемника можно услышать тестовый акустический фон обследуемого помещения. Прослушивание слабого акустического фона помещения на выходе высокочувствительного усилителя низкой частоты обычно позволяет сделать вывод о наличии в помещении устройства, обладающего «микрофонным» эффектом. Обнаружение в линии мощного ВЧ-сигнала может свидетельствовать о применении противником аппаратуры высокочастотного навязывания для прослушивания помещения.

С целью уточнения местоположение ЗУ, сигналы которого обнаружены в линии, требуется, последовательно перемещаясь вдоль контролируемой линии, изменять места подключения прибора. Если при этом (например, при включении щупов прибора в разные сетевые розетки) громкость обнаруженных сигналов возрастает, это означает, что мы приближаемся к месту подключения ЗУ. Если локализовать место установки ЗУ такими действиями не удается, используется второй способ. Поочередно отключаются от сети потребители электроэнергии (бытовые приборы и пр.). Это позволит определить, какой из них является носителем ЗУ, и подвергнуть его тщательному обследованию для обнаружения такового.

Следует помнить, что часть сетевых розеток может быть подключена к электрической сети через трансформаторы, не пропускающие сигналы ЗУ. В таких цепях поиск сигналов необходимо проводить, включая прибор в розетки, подключенные как к первичной, так и к вторичной обмотке трансформатора.

В некоторых случаях поиску сигналов ЗУ создает помеху достаточно высокий уровень низкочастотного шума в проверяемой линии. Источником такого шума могут быть регуляторы освещенности, дефектные люминисцентные лампы или блоки питания устройств бытового назначения. Для снижения уровня шума следует, не отключая шумящей цепи от проверяемой линии, вывести регулятор освещенности на максимум или удалить шумящую лампу. «Шумящий» блок питания можно определить последовательным отключением от сети потребителей электроэнергии. Найденный источник шума подвергается тщательной проверке на наличие внедренного закладного устройства.

При аппаратной проверке методом сканирования частотного диапазона рекомендуется следующий порядок действий оператора.

Сначала сканируется диапазон до 10 МГц. После завершения 2–3 циклов сканирования устанавливается верхняя граница диапазона сканирования на уровне 15 МГц. В процессе сканирования внимательно изучаются наиболее характерные особенности изображения панорамы и определяется наличие частотных составляющих, превышающих уровень общего фона.

При необходимости частотный диапазон разбивается на отдельные интервалы, и их сканирование осуществляется отдельно, с тщательным изучением наиболее интенсивных составляющих частотного спектра. Проведение поиска может дополняться проведением анализа сигналов в режимах осциллограммы и спектрограммы, так как в них проявляется более детальная характеристика параметров исследуемого «опасного» сигнала. Наиболее наглядно такой анализ можно провести при использовании современных аппаратно-программных комплексов радиомониторинга, оснащенных конверторами для проверки линий различного назначения. Вариант использования такого оборудования рассмотрим на примере применения комплекса «Спектр-Professional».

Комплекс «Спектр-Professional» позволяет выявлять и детально исследовать сигналы от ЗУ с передачей данных по проводным линиям. Встроенный автоматический конвертор проводных линий комплекса обнаруживает сигналы в частотном диапазоне от 600 Гц до 10 МГц. Выбор данного частотного диапазона обусловлен следующей причиной. С одной стороны, использование частот ниже 600 Гц устройствами негласного съема информации нецелесообразно по причине высокого уровня помех в сети электропитания от бытовой техники и промышленного оборудования. С другой стороны, использование частот свыше 10 МГц устройствами негласного съема информации маловероятно по причине большого затухания сигнала в проводных линиях. Кроме того, на частотах свыше 10 МГц сами провода начинают работать как антенны, излучая сигнал в окружающее пространство, что крайне нежелательно для противника ввиду появления еще одного демаскирующего признака для выявления ЗУ. Конвертор проводных линий работает как повышающий преобразователь частоты, который переносит спектры низкочастотных сигналов в УКВ-диапазон.

Перед началом работы с конвертором проводных линий для увеличения скорости обработки инфор-

мации необходимо уменьшить частотный диапазон сканирования, установив его, например, в границах 120–240 МГц. Непременное условие, которое следует при этом соблюдать, – частота гетеродина конвертора проводных линий должна находиться в пределах этого частотного диапазона.

При сканировании указанного частотного диапазона на экране спектральных панорам (рис. 1) наблюдается следующая картина: на нем представлены сигнал от частоты гетеродина конвертора проводных линий и внутренние помехи в проводных линиях.

В случае обнаружения сигнала от ЗУ с передачей данных по проводным линиям около несущей частоты гетеродина (порядка 20 МГц) будут присутствовать гармоники и субгармоники «опасного» сигнала (рис. 2).

Для точного определения параметров обнаруженного сигнала необходимо выбрать режим экспресс-анализа управляющей программы, настроиться на частоту гетеродина конвертора проводных линий и выбрать оптимальную полосу обзора. Оптимальная полоса обзора экспресс-анализатора выбирается таким образом, чтобы в рабочей области экрана экспресс-анализатора отображалась несущая частота выявленного «опасного» сигнала.

В этом случае, как правило, на экране экспресс-анализатора (рис. 3) присутствуют:

- зеркальный канал приема;
- несущая частота гетеродина конвертора проводных линий;
- субгармоника сигнала от устройства негласного съема информации;
- несущая частота сигнала от устройства негласного съема информации.

Тогда частота выявленного «опасного» сигнала определяется по формуле:

$$F_c = F_o - F_г,$$

где F_c – действительная частота сигнала;

F_o – частота сигнала на экране Экспресс-анализатора;

$F_г$ – частота гетеродина конвертора проводных линий.

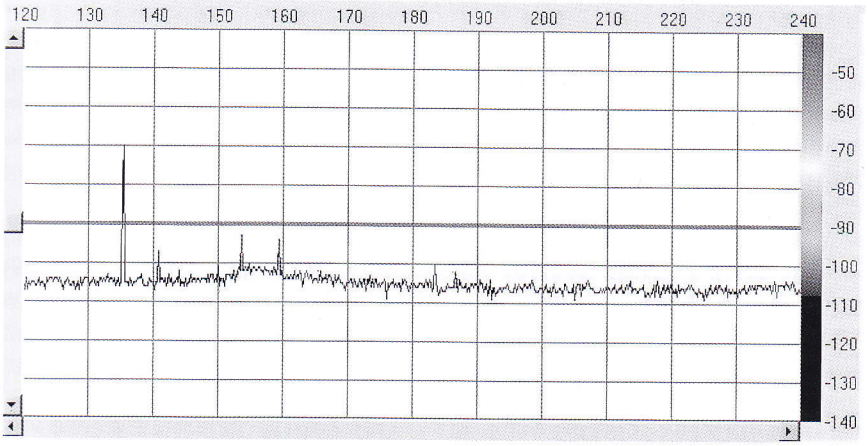


Рис. 1. ***Экран спектральных панорам при приеме сигналов от проводных линий***

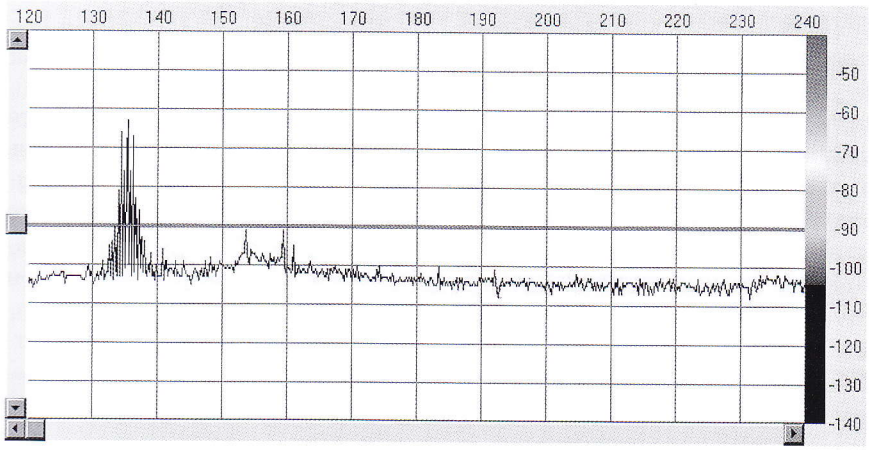


Рис. 2. ***Экран спектральных панорам при обнаружении сигнала от ЗУ с передачей данных по проводным линиям***

Следует отметить, что при увеличении полосы обзора экспресс-анализатора могут быть обнаружены гармоники несущей частоты сигнала от устройства негласного съема информации на частотах $2F_c$, $3F_c$ и т. д.

Учитывая высокую чувствительность комплекса, при поиске ЗУ с передачей данных по сети переменного тока с напряжением 220 В целесообразна работа от собственной аккумуляторной батареи ноутбука.

Если контролируемое помещение проверяется регулярно, то целесообразно сохранить в энергонезависимой памяти панораму (осциллограмму, спектрограмму) необходимых частотных интервалов.

При проверке проводных линий необходимо учитывать специфические особенности линий каждого вида. Например, проверку на наличие ЗУ в электросети целесообразно начинать с сетевых розеток, для умень-

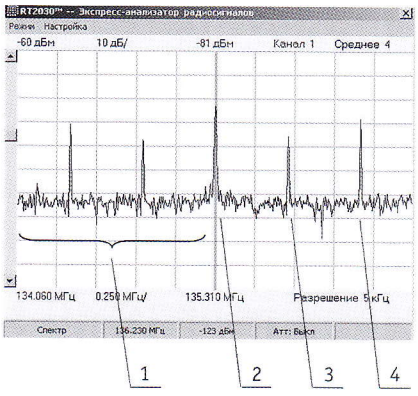


Рис. 3. ***Экран экспресс-анализатора при обнаружении «опасного» сигнала***

шения уровня фона отключив (с отсоединением от розеток) все электроприборы и аппаратуру, размещенную в контролируемом помещении. После подключения поискового прибора к сети (можно использовать для этого любую из розеток, находящихся в контролируемом помещении) необходимо провести ана-

лиз изображения панорамы. Если обнаружен сигнал, содержащий признаки модуляции акустикой помещения, то для локализации его источника может быть использован метод «акустозавязки» при поочередном подключении ко всем розеткам в проверяемом помещении.

Аналогичную проверку следует провести на элементах линий, питающих электроосветительные приборы.

После проверки силовых линий и линий, питающих осветительные приборы, необходимо проверить тройники, удлинители и другие электропотребляющие средства путем их поочередного подключения к электросети.

Проверка проводных линий систем пожарной и охранной сигнализации, а также линий неизвестного назначения аналогична проверке линий электросети, так как аналогичны сами технические средства, используемые на этих коммуникациях.

Подробнее поговорим о процедуре проверки телефонных линий. Сложность телефонных систем, их разветвленность создают повышенные объективные трудности при их обследовании. Изучая опыт проведения проверок, можно сделать вывод, что чем сложнее телефонная система, тем проще противнику установить в нее ЗУ.

В целом, процесс исследования телефонного оборудования заключается в проведении следующих мероприятий:

- предварительного контроля и исследования системы с целью определения ее сложности, а также типа необходимого для контроля оборудования;
- разработки плана по проведению проверки;
- визуальной проверки оснащения, проводов и кабелей телефонной системы, анализа всей системы с точки зрения ее соответствия спецификации;
- проверки всех проводов (в парах и раздельно) каждой входной линии акустическим усилителем и соответствующими приемниками радиочастот с целью обнаружения передачи во время нормальной работы системы;
- исследования проверяемой линии на наличие проводов, идущих мимо контролируемой контактной колодки (с этой целью необходимо обследовать телефонный кабель на всем его протяжении вплоть до окончания в колодках);
- проверки с помощью измерительной аппаратуры принадлежности каждого провода (каждый провод нужно проверить со всеми остальными проводами и заземлением);
- обследования с помощью приборов всех устройств, приводящих в действие данное оборудование (необходимо провести осмотр всех деталей телефонной системы, он должен включать демонтаж аппаратов, соединений, а также присоединенных приборов);
- проверки на наличие линейного высокочастотного навязывания, признаком которого является наличие в линии немодулированного стабильного зондирующего сигнала на частотах более 150 кГц (при этом порядок подключения приборов и процедура анализа не отличаются от изложенного применительно к проверке линий электросети).

Проверка офисной и абонентской телефонной сети осуществляется следующим образом. Визуальный осмотр линий и оборудования заключается в поиске несанкционированных подключений к телефонным проводам и телефонному оборудованию, поиске посторонних предметов и вызывающих подозрение деталей в телефонных аппаратах, вилках, розетках, распределительных коробках, оборудовании офисной АТС, в телефонном шкафу.

Проводимые исследования и поисковые мероприятия позволяют сделать вывод, что до 70 % ЗУ, обнаруженных в ходе проведения поисковых работ, составляют средства, непосредственно снимающие информацию с телефонной линии либо использующие телефонную линию для передачи информации, перехваченной другим способом. При этом во многих случаях используются комбинированные ЗУ, осуществляющие перехват телефонных переговоров при снятой телефонной трубке, а в паузах между ними – контроль и съем акустической информации из помещения. Необходимо помнить, что устройства бесконтактного (индуктивного) съема информации с телефонных линий в настоящее время практически не обнаруживаются ни одним типом поисковых приборов. Следовательно, визуальный осмотр телефонных аппаратов, другого телефонного оборудования и самих телефонных линий должен проводиться с предельной тщательностью.

При вскрытии телефонных аппаратов прежде всего необходимо искать нестандартные или чем-либо выделяющиеся, наспех установленные элементы и узлы, нарушение лакокрасочного покрытия монтажных плат. При этом разборке и осмотру также подлежат и телефонные трубки. Особенно детально следует осмотреть телефонный шкаф, так как именно в нем наиболее просто осуществляется несанкционированное подключение к линии. Осмотр телефонных линий целесообразно проводить на всем протяжении от телефонных аппаратов до городской АТС. Учитывая, что доступ посторонних лиц на АТС и в телефонные колодцы запрещен, обычно ограничиваются проверкой линии до места их соединения с многожильным магистральным кабелем в телефонном щите.

Изложенные положения позволяют сделать вывод, что исследование линий связи на наличие ЗУ – очень трудоемкая и дорогостоящая задача, требующая применения различных приборов. Сложности заключаются в том, что ЗУ может быть установлено на большом расстоянии от телефона, а методы съема информации очень разнообразны.

Необходимо помнить, что любое контактное подключение к линии приводит к изменению ее электрических параметров, выявление которых требует применения сложной аппаратуры. Для регистрации электрических параметров линии применяют телефонные анализаторы, с помощью которых можно измерить напряжение, величину тока в линии, сопротивление и ток утечки и, сравнив полученные значения с параметрами линии в нормальном

состоянии, сделать заключение о наличии и характере (параллельное или последовательное) несанкционированных подключений. При этом следует помнить, что параметры линии в нормальном состоянии при некачественном (это случается очень часто) ее монтаже могут произвольно меняться от погодных и других внешних факторов в очень широком диапазоне. Пользователям защищенных телефонных аппаратов можно дать совет более часто обращать внимание на дисплей прибора защиты телефонной линии, который регистрирует ее напряжение. Целесообразно завести журнал, в который ежедневно заносить показания дисплея прибора, а затем анализировать эти значения.

Другие наиболее дорогие приборы – кабельные локаторы. Принцип их действия заключается в посылке коротких импульсов в линию. Достигая точки неоднородности в линии (контактное подключение), импульс отражается и регистрируется прибором. По времени задержки отраженного сигнала можно определить расстояние до нелинейности. Ранее трудности в применении данных приборов были связаны, как правило, с их значительными габаритными размерами, массой и высокой стоимостью. В настоящее время в связи с миниатюризацией комплектующих основными недостатками этих приборов можно считать следующие: относительно высокая стоимость, часть приборов требует обесточивания линии, наличие скруток на линии зачастую воспринимается прибором как нелинейность.

Разнообразие приборов для проверки телефонных линий вызывает необходимость проведения наиболее тщательной и детальной оценки вероятного противника, что позволяет реально оценить его возможности по использованию тех или иных видов ЗУ, а соответственно, и необходимость применения той или иной аппаратуры для выявления установленных ЗУ.

В данной статье были рассмотрены основные подходы к выявлению ЗУ, использующих для передачи информации проводные линии различного назначения. При этом необходимо помнить, что решение о проведении поисковых мероприятий в каждом конкретном случае принимается руководителем организации в зависимости от выявленных угроз безопасности информации.

В последующих статьях будут рассмотрены основные характеристики и особенности применения нелинейных локаторов в современных условиях. ■

ЛИТЕРАТУРА

1. Болдырев А. И., Василевский И. В., Сталенков С. Е. Методические рекомендации по поиску и нейтрализации средств негласного съема информации. – М.: ЗАО НПЦ Фирма «НЕЛК», 2001. – 138 с.

2. Бузов Г. А., Практическое руководство по выявлению специальных технических средств несанкционированного получения информации. – М.: Горячая линия-Телеком, 2010. – 240 с.

НОВОСТИ

Группа компаний МАСКОМ: 23 года на страже информационной безопасности

В начале девяностых годов прошлого века в России была выстроена новая современная система лицензирования в области технических средств защиты. Базисом системы стали организации-лицензиаты ФСТЭК России, среди которых видное место занимал Центр безопасности МАСКОМ, образованный 15 мая 1991 года.

На протяжении своей деятельности компания смогла не только усовершенствовать существовавшие на тот момент средства для защиты информации, но и на основе полученных знаний и опыта создать абсолютно новые, непревзойденные в своем направлении системы защиты информации. Многие разработки стали прорывом в сфере обеспечения безопасности. Группа компаний МАСКОМ имеет ряд наград, полученных на международных форумах.

Сегодня в состав Группы компаний МАСКОМ входят такие организации, как ООО ЦБИ «МАСКОМ», НОУ УЦБИ «МАСКОМ», ООО «МК-Спецмонтаж», Дальневосточный холдинг «МАСКОМ Восток». Именно в данных подразделениях на волнах передовых технологий силами квалифицированных специалистов создается дух компании, который вносит свой вклад в развитие средств защиты российских информационных ресурсов.

23-ю годовщину со дня основания ГК МАСКОМ встречает расширяя и развивая такие направления деятельности, как:

- разработка, производство и поставка средств защиты информации, обнаружения каналов утечки информации, систем оценки защищенности, специальных технических средств;
- оказание услуг по обеспечению защиты информации, составляющей государственную, служебную, коммерческую тайну, безопасности персональных данных и конфиденциальной информации;
- образовательные услуги в области ИБ для органов государственной власти, местного самоуправления, лицензиатов и соискателей лицензий ФСТЭК и ФСБ, руководителей и сотрудников служб безопасности предприятий;
- консалтинговые и аудиторские услуги в области защиты речевой информации и информационной безопасности АС;
- проектирование и монтаж инженерно-технических систем безопасности и обеспечения жизнедеятельности;
- специальные экспертизы соискателей лицензий ФСТЭК и ФСБ России;
- организация и управление строительством и реконструкцией специальных объектов и объектов общего назначения;
- научно-исследовательские и опытно-конструкторские работы в области защиты информации.