Применение «OSCOR-5000» – проблемы и решения

Г. А. Бузов, к. в. н., доцент
А. К. Лобашев, к. т. н., доцент
Д. А. Щербаков

Борьба с внедренными на охраняемые объекты устройствами несанкционированного перехвата информации является одним из важных направлений обеспечения информационной безопасности. В настоящее время на отечественном рынке представлен широкий ассортимент средств поиска закладных устройств (ЗУ), в котором несколько обособленное место занимает спектральный коррелятор **OSCOR** (OSC-5000) (Omni Spectral Correlator) американской фирмы REI. Обособленное – прежде всего потому, что этот **прибор в числе первых был представлен на российском рынке как многофункциональный автоматизированный программно-аппаратный комплекс,** способный проводить контроль и обнаружение ЗУ в течение 24 часов, анализировать радиоэфир, инфракрасный диапазон, телефонные, проводные и силовые линии.

Преимуществом этого прибора является его удобство, быстрая «привыкаемость» пользователя к управлению прибором с помощью кнопок (клавиш) и, наконец, программное обеспечение. Да и структурные элементы (например, в OSCOR-5000E версии 5.0) постоянно совершенствуются, что также является привлекательной стороной этого прибора.

Учитывая достаточно широкое распространение этого прибора в России, в этой статье хотелось бы осветить некоторые проблемные, на наш взгляд, вопросы, касающиеся практики применения. Достаточно большой накопленный опыт применения этого прибора и преподавания слушателям основ использования OSCOR выявил следующее. **Одна из ключевых проблем** заключается в том, что из всех представленных в OSCOR исследовательских процедур, в конечном итоге, самой ответственной является **получение достоверного факта идентификации (локализации) ЗУ, в том числе и со «сложными» видами модуляции.**

Проблематика поиска «сложных» видов ЗУ занимает в последнее время все большее внимание. В связи с этим возникает необходимость анализа и осмысление накопленного опыты и разработки рекомендаций по применению прибора по обнаружению и идентификации «сложных» видов ЗУ. Для того чтобы «уйти» от наработанных на практике способов идентификации ЗУ, разработчиками устройств несанкционированного съема информации применяется большое количество способов, затрудняющих их поиск и обнаружение. **Проведенный анализ таких способов позволил выявить основные способы «ухода» от обнаружения ЗУ.**

1. **Сокращение времени** излучения закладок, что достигается, прежде всего, использованием ЗУ с **дистанционным управлением.**

2. **Применение ЗУ с накоплением информации** (и последующей импульсной передачей на приемное устройство). **Импульсные передатчики** – это устройства, которые сохраняют информацию в течение некоторого времени и периодически одним коротким импульсом передают всю накопленную информацию. Такие устройства используют

цифровую модуляцию и обычно имеют очень широкую полосу пропускания в зависимости от периодичности импульсов и рабочего цикла. **Период передачи импульсов зависит от типа устройства, он может составлять от нескольких миллисекунд до нескольких минут.** Возможно использование импульсного передатчика, передающего сигнал с периодичностью в несколько часов. **Передатчик такого типа крайне сложно обнаружить из-за длительного периода отсутствия передачи.**

3. **Использование ЗУ со скачкообразным изменением частоты излучения.** ЗУ со скачкообразной перестройкой частоты устроены таким образом, чтобы передавать информацию на одной частоте очень непродолжительное время (от 5 до 100 миллисекунд), а затем изменять частоту на новую. Такие передатчики переключаются между несколькими различными частотными каналами в пределах четко заданной полосы. Передатчик со скачкообразной перестройкой обычно передает цифровой сигнал, но может быть и аналоговым.

4. **Применение в ЗУ «закрытия» передаваемой информации с использованием различных модулирующих функций,** в частности цифровых (в том числе с «**дельта-модуляцией**»), **шумоподобных** и др. Технология шумоподобного сигнала распределяет энергию сигнала по более широкому участку спектра частот, что делает передатчик менее заметным.

Накопленный опыт применения прибора показывает, что поиск и идентификация таких ЗУ сопряжены с большими трудностями. Прежде всего следует отметить, что **в автоматическом режиме работы** OSCOR **обнаружение таких сигналов является невозможным.** Изучение тактико-технических характеристик прибора OSCOR показало, что определенные перспективы для обнаружения «сложных» видов ЗУ имеет **применение режима анализа с использованием спектра пиков.**

Проведенное детальное изучение режимов работы прибора продемонстрировало, что отображение **спектра пиков прибором является более функциональным,** чем простой режим отображения спектра. В этом режиме в приборе поддерживается постоянно обновляемый буфер памяти. Иными словами, независимо от того, какие действия пользователь выполняет с прибором, буфер памяти для спектра пиков постоянно обновляется и накапливается. То есть, если регистрируется короткий сигнал от импульсного передатчика или передатчика с изменяющейся частотой, он сохраняется в памяти в буфере развертки пиков, даже если развертка пиков в данный момент на экран не выводится. В **режиме вычитания спектров пиков и дружественного спектра** прибором обеспечивается возможность выявления разницы в развертках спектра и, таким образом, получение более точной картины спектральной характеристики на различных частотах.

Ниже приведены примеры отображения спектров пиков различных импульсных сигналов и спектров реального времени (в режиме вычитания) для модификации прибора OSCOR-5000 E (версии 5.0).

На рис. 1 в верхней части показаны развертка дружественного спектра и спектра пиков. График в нижней части отражает разницу между этими двумя развертками. В данном примере в обследуемую среду были введены **два закладных устройства (с перестройкой частоты и импульсного передатчика),** а также сигналы сотовой и пейджинговой связи для демонстрации функций OSCOR. Эти сигналы помечены на графике.

Опыт использования прибора показывает, что при анализе сложных сигналов основной принцип идентификации – распознавание различий между развертками спектра и изучение каждого случая вручную. На рис. 1 показан диапазон частот от 5 до 1505 МГц. При наличии помех этот участок спектра может оказаться значительно более загруженным, поэтому при проведении анализа можно увеличить масштаб развертки и рассмотреть каждый участок спектра по отдельности, изучая их по необходимости.

Изучение опыта применения прибора показывает, что в целом **базовый алгоритм выявления таких ЗУ заключается в следующем:**

- сохраняется дружественный спектр;
- с помощью определенных манипуляций с основными органами управления прибором при входе в обследуемое помещение очищается память спектра пиков;
- далее изучаются все обнаруженные «подозрительные» сигналы вручную (опыт показывает, работа прибора в этом режиме может продолжаться от нескольких минут до одного часа).

Рассмотрим примеры, как различные радиопередатчики идентифицируются при исследовании прибором «сложных» сигналов с использованием экрана развертки пиков. Так, при выявлении сигналов с использованием технологии **ШПС** энергия сигнала распределяется по широкому участку спектра частот (что делает ЗУ менее заметным на общем фоне развертки). В случае исследования прибором ШПС-си-

Рис. 1. ***Отображение спектра пиков и дружественного спектра***

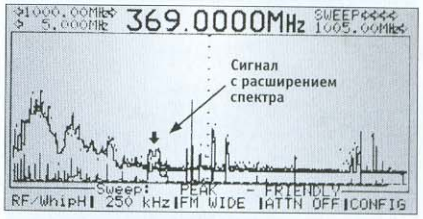

Рис. 2. ***Изображение сигнала с расширением спектра при развертке 5–1005 МГц***

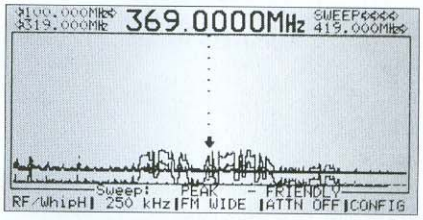

Рис. 3. ***Изображение сигнала с расширением спектра при развертке 319–419 МГц***

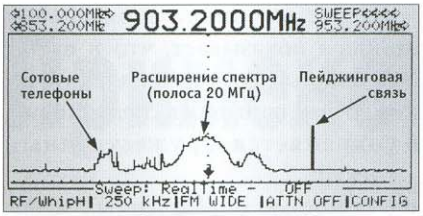

Рис. 4. ***Изображение ШПС-сигнала в сравнении с сигналами сотовой и пейджинговой связи***

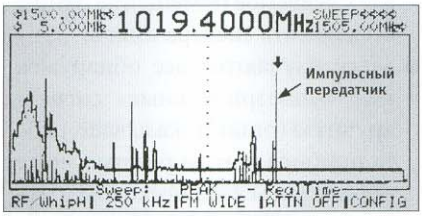

Рис. 5. ***Изображение импульсного радиопередатчика при развертке 5–1005 МГц***

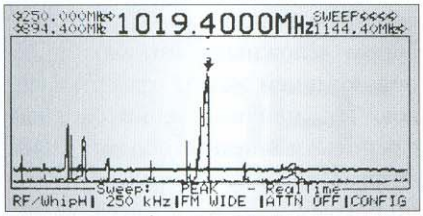

Рис. 6. ***Изображение импульсного радиопередатчика при развертке 894–1144 МГц***

Рис. 7. ***Изображение импульсного радиопередатчика при развертке 969,4–069,4 МГц***

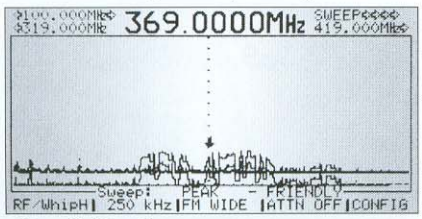

Рис. 8. ***Изображение импульсного радиопередатчика при развертке 970,000–1070,00 МГц (в режиме перевернутого графика разностей)***

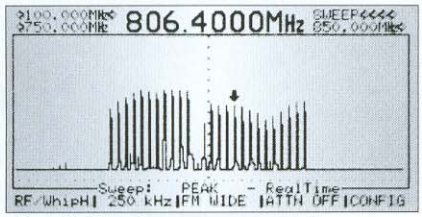

Рис 9. ***Изображение передатчика со скачкообразной перестройкой частоты***

гнала с цифровым кодированием может обнаружиться несколько слабых сигналов со скачкообразной перестройкой частоты.

На рис. 2 показан сигнал с расширением спектра при развертке 5–1005 МГц. На рис. 3 показан тот же сигнал с расширением спектра при развертке 319–419 МГц. Уменьшение развертки дает возможность более детальной оценки спектральных составляющих исследуемого сигнала.

На рис. 4. показан спектр изображения ШПС-сигнала (с полосой пропускания 20 МГц) в сравнении с сигналами сотовой и пейджинговой связи.

В приведенном ниже примере (рис. 5 и 6) показано зафиксированное изображение импульсного радиопередатчика с использованием анализа спектра пиков при различных видах разверток (5–1005 МГц и 894–1144 МГц).

На рис. 7 и 8 приведен пример изображения импульсного радиопередатчика с использованием анализа спектра пиков при различных видах разверток (969,4–1069,4 МГц и 970,000–1070,00 МГц). На рис. 8 показано изображение импульсного радиопередатчика в режиме перевернутого графика разностей.

Другой тип «сложных» видов ЗУ – **устройства со скачкообразной перестройкой частоты.** Анализ функционирования таких устройств показывает, что такие ЗУ рассчитаны на передачу на одной частоте лишь в течение короткого промежутка времени (от 5 до 100 миллисекунд), после чего они меняют частоту передачи на новую, кажущуюся случайной. Такие передатчики переключаются между несколькими различными частотными каналами в пределах четко заданной полосы.

На рис. 9 показан факт регистрации прибором **устройств со скачкообразной перестройкой частоты.** Для подтверждения данных о наличии опасного сигнала необходимо применить метод разнесенного приема с фиксацией амплитуд ЗЛ-сигналов (и их сравнении) в проверяемом помещении и за его пределами.

Таким образом, в статье рассмотрены некоторые проблемные, на наш взгляд, вопросы, которые касаются тактико-технических основ применения прибора OSCOR для идентификации «сложных» видов ЗУ с учетом последних программно-технических новаций прибора OSCOR. К сожалению, объем статьи не позволяет раскрыть более подробно некоторые частные «детали» работы с прибором, но они достаточно подробно изложены в описании рассматриваемого прибора. Нам представляется, что предложенный в статье материал поможет более продуктивно использовать прибор для решения задач поиска каналов несанкционированного съема информации. ■

ЛИТЕРАТУРА

1. Хорев А. А. Защита информации от утечки по техническим каналам. Ч. 1. Технические каналы утечки информации. Учебное пособие. – М.: Гостехкомиссия России, 1998.

2. Барсуков В. Блокирование технических каналов утечки информации //Jet Info. Информационный бюллетень. 1998. № 5–6. С. 4–12.

3. Хорев А. А. Классификация и характеристика технических каналов утечки информации, обрабатываемой ТСПИ и передаваемой по каналам связи // Специальная техника, 1998, № 2, Май – июнь, с. 41–46.

4. Хорев А. А. Технические каналы утечки акустической (речевой) информации // Специальная техника, 1999, № 1, Март – апрель, с. 48–55.

5. «Шпионские штучки» и устройства для защиты объектов и информации: Справочное пособие. – СПб.: Лань, 1996.

6. НПО «Защита информации». Каталог 2004 г.

7. НПО «НЕЛК». Каталог 2004 г.

8. НПО «Смерш Техникс». Каталог 2004 г.

9. ЦБИ «МАСКОМ». Каталог 2005 г.

10. Лобашев А. К., Лосев Л. С. Современное состояние и тактические возможности применения индикаторов электромагнитных излучений // Специальная техника, № 6, 2004.

11. Бузов Г. А.., Лобашев А. К., Лосев Л. С. «Легальные жучки»: суровая реальность и меры противодействия» // Специальная техника, № 1, 2005.

12. Бузов Г. А., Лобашев А. К., Лосев Л. С. Современный взгляд на решение проблемы применения «легальных жучков» // «Защита информации. Инсайд» , № 2, 2005.