УДК 04.056(075.8)

С.В. Дзюин, К.В. Мухин

Аппаратные средства контроля при проведении аудита информационной безопасности

В статье предлагается использование набора средств радиоконтроля для проведения аудита. Рассматриваются различные зоны радиоконтроля.

Одним из важнейших направлений решения проблем обеспечения адекватного уровня информационной безопасности является проведение аудита информационной безопасности.

При проведении аудита информационной безопасности контролируемых зон важной задачей является определение технических каналов утечки информации, в частности электромагнитных каналов. Для эффективного решения этой задачи необходимо проведение тщательного радиомониторинга контролируемой зоны с составлением карты радиоэфира.

Параллельно с проверкой проводных коммуникаций при аудите радиомониторинг обеспечивает выявления информационных побочных излучений оргтехники и сигналов СНСИ (средств несанкционированного съема информации) (радиозакладки), использующих радиоканал для передачи перехваченной информации.

Сложной проблемой современного радиомониторинга является выявление СНСИ со специальными видами сигналов (например, шумоподобными сигналами с фазовой манипуляцией, сигналами со сверхширокополосной частотной модуляцией или скачкообразным изменением несущей частоты (псевдослучайная перестройка рабочей частоты (ППРЧ). Данные сигналы в силу своих свойств (возможность усиления обработки) могут работать на очень малых мощностях, соизмеримых с шумами, т.е. их излучение может быть не более средних уровней индустриальных шумов. Это определяет их высокую скрытность, в том числе и для средств радиоконтроля. Поэтому существующие стандартные средства радиоконтроля не позволяют автоматически идентифицировать такие излучения с сигналами СНСИ, а в ряде случаев вообще не могут определить факт их наличия и соответственно факт работы разведрадиосистемы.

В этой связи для радиомониторинга зон контроля наиболее подходят такие автоматизированные комплексы, которые позволяют оператору при необходимости самому проводить детальный анализ принимаемых сигналов или комплексы, интегрированные с ПК, имеющими соответствующие алгоритмы обработки. При аудите необходимо учитывать, что стоимость этих СНСИ весьма высока, она свидетельствует о высокой квалификации злоумышленника, высоком уровне потенциальных возможностей его разведсредств и, таким образом, разведпотенциале в целом. Эти СНСИ закладываются профессионально, надолго и с особой тщательностью.

Непосредственное измерение показателей, характеризующих уровни излучения в каналах и помеховую обстановку в каналах с учетом возможных алгоритмов работы СНСИ требует значительных аппаратурных затрат. Значительные временные задержки, возникающие при работе алгоритмов измерителя, делают результат измерения в момент использования недостоверным. Это не позволяет обеспечить оперативного определения признаков функционирования СНСИ нарушителя и, следовательно, резко снижает эффективность работы алгоритмов обманных систем. Знание текущего состояния каналов, определяемое анализатором качества канала, позволяет избежать этого.

Для реализации функции анализа качества канала удобно пользоваться информационными методами. Возможность использования структуры информационного сигнала для контроля качества канала вытекает из факта, что его основные характеристики – длина блока, скорость передачи, среднее значение веса кодовой комбинации – являются известными величинами. Поэтому если сигнал на выходе канала имеет параметры, отличные от априорно известных, то это служит признаком наличия ошибок в канале.

В информационных системах на сигналы воздействует комплекс помех, возникающих в канале. В состав канала включаются среда распространения сигнала и аппаратура, участвующая в обработке сигнала до решающего или управляющего устройства. В связи с этим помехи, приводящие к искажению сигналов, поступающих на вход решающего устройства, имеют разную природу. Во-первых, возникновение ошибок вызвано условиями распространения сигналов. Во-вторых, сама аппаратура вносит дополнительные искажения, что также определяет характер ошибок на выходе информационной системы. В состав аппаратуры, участвующей в формировании цифрового сигнала, входят исполнительные механизмы, приемное устройство, демодулятор, декодер и устройство принятия решения. В-третьих, ошибки связаны с работой СНСИ, возникающих при несанкционированном доступе [1–3]. Однако независимо от своей природы ошибки проявляются одинаково в виде трансформации кодового вектора состояния канала. При этом характер изменения вектора состояния канала вследствие шумов и сосредоточенных помех и вследствие несанкционированного доступа отличается.

Поэтому при радиомониторинге для оценки состояния радиоэфира возможно использовать сравнение реального веса определенного числа принятых кодовых посылок с априорным значением веса. Анализаторы качества канала построены на этом принципе. Точность измерения ошибок в канале с помощью таких анализаторов определяется длиной выборки измерения при некоррелированных отсчетах. Кроме того, с ростом объема выборки растет и время реакции анализаторов на изменение состояния канала, т.е. падает скорость измерений. Существует возможность избежать «жесткого» размена точности на скорость измерений за счет специальных алгоритмов. Они состоят в том, что в начальные моменты или в моменты резких изменений состояния канала измерения проводятся с повышенной точностью на основании увеличенной выборки (уменьшение скорости). В установившихся режимах объемы выборки уменьшаются и скорость текущих измерений состояния канала возрастает.

На базе описанного материала поставлены практические курсы для изучения специальных дисциплин специальности 090105 «Комплексное обеспечение информационной безопасности в автоматизированных системах»

Литература

1. Дзюин С.В. и др. Анализатор качества канала: А.с.1713110 СССР, МКИ Н04В3/46 // Бюл. – 1992. – № 6.
2. Дзюин С.В. Устройство для контроля качества канала: А.с.1555876 СССР, МКИ Н04В3/46 // Бюл. – 1990. – № 13.
3. Дзюин С.В. Анализатор качества канала. Решение на выдачу патента 12.12.2005.

Дзюин Сергей Витальевич
Ижевский государственный технический университет
К.т.н., доцент кафедры систем и технологий информационной безопасности

Мухин Константин Вячеславович
Ижевский государственный технический университет, аспирант
Тел.: (3412) 59 24 17
Эл. почта: sam@istu.ru

S.V. Dzuin, K.V. Muhin
Hardware of the control over carrying out of audit of information safety

In papers use of a set of radiocontrols means the over carrying out of audit is offered. Various zones of the radiocontrol are considered.