ПОВЫШЕНИЕ СКРЫТНОСТИ И ИНФОРМАТИВНОСТИ СРЕДСТВ ОХРАННОЙ СИГНАЛИЗАЦИИ

В.В. Платон

В настоящее время в сигнализационных комплексах наиболее широко используются датчики серии РЛД-94. Изделия используют физический принцип, основанный на преобразовании в сигнал тревоги изменений параметров электромагнитного поля на входе приемного устройства при появлении нарушителя в зоне обнаружения.

РЛД-94 обеспечивает высокую вероятность обнаружения нарушителя >0,98, наработку на ложное срабатывание не менее 3000 час, наработку на отказ – 30000 ч. Устойчиво к воздействию ливневых дождей и практически не реагирует на мелких животных. Корпус антенного блока выполнен из неподверженного коррозии алюминия, что обеспечивает длительный срок службы и резко уменьшает воздействие внешних электромагнитных помех, механическую прочность при резких колебаниях температур от –50 до +65 градусов.

Разнообразие моделей РЛД-94 (УМ-50-18 – до 50 м; УМ-150-18 – до 150 м; УМ-300-18 – до 300 м) позволяет потребителю оптимизировать затраты на организацию сигнализационного блокирования рубежа различной протяженности и конфигурации за счет рационального использования возможностей моделей и разницы в их цене [1].

С точки зрения повышения информативности и электромагнитной совместимости целесообразен переход к системам просветной радиолокации, реализующих не монохроматический, а линейно-частотномодулированный сигнал. В этом случае возможно измерение дальности, получение дальномерного портрета цели, снижение влияния мешающих отражений, повышение скрытности и характеристик электромагнитной совместимости.

Также повышения скрытности можно достичь снижением спектральной плотности при заданной мощности передающего устройства, оно достигается расширением спектра зондирующего сигнала, что также повышает разрешающую способность РЛС по дальности [2–4].

Список литературы

1. Лавриненко А.В. Периметровые средства обнаружения: современное состояние // Специальная техника. 2001. № 5. С. 14–18.

2. Сальников И.И. Чернышев М.Н. Определение размера и скорости движения нарушителя в двухпозиционных охранных системах ближней радиолокации // Известия высших учебных заведений. Поволжский регион. Технические науки. 2011. № 1 (17). С. 96–105.

3. Смирнова Д.М. Обнаружение и измерение координат движущихся наземных объектов в многопозиционной просветной радиолокационной системе: автореф. дис. …к-та техн. наук. Нижний Новгород, 2014. 16 с.

4. Зубков А.Н. Радиолокационная система обнаружения наземных целей в коротковолновой части ММ диапазона // Сб. докл. НТК по миллиметровой технике. Львов, ЛНИРТИ, 1986.

ОБУЧЕНИЕ СЛУШАТЕЛЕЙ КУРСОВ ПЕРЕПОДГОТОВКИ ОСНОВАМ ЗАЩИТЫ ИНФОРМАЦИИ

В.А. Полубок, А.А. Косак

В настоящее время фраза Н. Ротшильда «Кто владеет информацией, тот владеет миром» стала как никогда актуальной. Огромный прогресс в области информационных технологий привел к тому, что компании и частные лица как никогда стали зависимыми от информационных систем и их безопасности. В настоящее время вопрос информационной безопасности становится одним из основных аспектов при разработке информационных систем.

Анализ подхода к обучению слушателей переподготовки по специальностям, связанным с информационными технологиями, свидетельствует о недостаточной подготовке в области технологий обеспечения информационной безопасности. Результаты анализа показывают, что необходима фундаментализация обучения слушателей технологиям защиты

информации, что позволит познакомить их с фундаментальными основами теории защиты информации, общей схемой обеспечения информационной безопасности, со структурой унифицированной концепции и стратегией защиты информации. Рассмотрение фундаментальных основ теории защиты информации позволит сформировать представление о подходах к защите информации, инвариантных относительно развития разных информационных технологий [1].

Обучение основам защиты информации в рамках курсов переподготовки по ИТ-специальностям можно разделить на два направления: программное и техническое. Если технические методы защиты информации рассматриваются слушателями в рамках курса «Компьютерные сети», то программные методы защиты информации в рамках специальности не рассматриваются. В настоящее время прорабатывается возможность введения в рамках курса, где слушатели изучают основы алгоритмизации и программирования, темы «Основы защиты информации», в которой будут рассматриваться как основы защиты информации на уровне программного обеспечения, так и основные алгоритмы шифрования данных (например: AES, DES, RSA, RC4), будут описываться основные преимущества и недостатки и приводится варианты их применения на практике. Для закрепления полученных знаний слушателям, в рамках практических занятий, будет предложено реализовать один из алгоритмов шифрования. Полученные теоретические и практические навыки в дальнейшем помогут выпускникам переподготовки быть более конкурентоспособными на рынке труда.

Список литературы

1. Димов Е.Д. Методика обучения студентов вузов технологиям защиты информации в условиях фундаментализации образования: автореф. дис. ... канд. пед. наук. Москва, 2013. 25 с.

МОНИТОРИНГ ЭЛЕКТРОМАГНИТНЫХ ПОЛЕЙ, СОЗДАВАЕМЫХ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКОЙ

В.А. Попов, А.В. Потапович, П.Л. Прудников

В условиях стремительно развивающейся современной вычислительной техники, переноса на ЭВМ большинства количества и видов анализа и обработки информации, возникла и начала развиваться киберпреступность. Одной из ее разновидностей является перехват обрабатываемой на ЭВМ информации путем внедрения в агрегаты вычислительной машины аппаратной закладки, считывающей обрабатываемые в памяти компьютера данные и передаче ее по радиоканалу с помощью встроенных в вычислительную технику недекларированных возможностей. Встроенные недекларированные возможности в вычислительную технику могут быть организованы как программным путем с использованием не основных по функциональному назначению свойств элементной базы, так и аппаратно-программным путем. Такие встроенные недекларированные возможности вычислительной техники могут эпизодически кратковременно организовывать передачу информации в сжатом виде на некоторой частоте по радиоканалу. Исходя из этого, становится очевидным один из методов обнаружения подобных устройств несанкционированного съема информации – мониторинг электромагнитного излучения вычислительной техники.

Важнейшим показателем мониторинга электромагнитного излучения является выбор необходимого диапазона частот. При выборе частотного диапазона мониторинга исходили из предпосылок наиболее простого и доступного метода организации получения информации. Частотный диапазон предлагается выбрать от 10 МГц до 10 ГГц с разбиением его на 10 октавных полос.

Устройство мониторинга может применяться на рабочих местах, в машинных залах предприятий, осуществляющих обработку конфиденциальной информации на ЭВМ. Сигнал тревоги от устройства мониторинга послужит основанием для выполнения работ с целью проверки узлов и агрегатов ЭВМ на предмет наличия недекларированных возможностей.