

create a digital equivalent of an identity card. Such startups include HYRP, BlockVerify, OneName and others. Copyright – the Ascribe platform uses the register in which artists, musicians, inventors can store the copyright of the encrypted identifiers. Management and law – already now there are projects like Borderless, which combine legal and economic services.

УГЛЕСОДЕРЖАЩИЕ ЭЛЕКТРОМАГНИТНЫЕ ЭКРАНЫ ДЛЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Х.А.Э. Айад, О.В. Бойправ, Л.М. Лыньков

Авторами обоснована перспективность использования порошкообразных материалов на основе активированного, древесного и кокосового углей для создания электромагнитных экранов. Установлено, что значения коэффициента передачи электромагнитного излучения (ЭМИ) в диапазоне частот 0,7–17 ГГц экранов на основе порошкообразных углесодержащих материалов – не более –7 дБ (толщина экранов – 8 мм). Значения коэффициента отражения, измеренные в режиме короткого замыкания, достигают величины –10 дБ. Определено, что в результате пропитывания до насыщения порошкообразных углесодержащих материалов водным раствором хлорида кальция можно обеспечить снижение с –7 до –35 дБ значений коэффициента передачи и с –10 до –14 дБ коэффициента отражения ЭМИ электромагнитных экранов на их основе, что связано с увеличением с $4,6 \cdot 10^{-8}$ –0,45 См/м до 0,1–70 См/м удельной проводимости таких порошков.

Таким образом, электромагнитные экраны на основе порошкообразных углесодержащих материалов могут быть использованы для обеспечения защиты информации от утечки по каналу побочного электромагнитного излучения, а также в целях снижения радиолокационной заметности наземных объектов.

ПОДГОТОВКА СПЕЦИАЛИСТОВ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ

В.М. Алефиренко

Подготовка специалистов по специальности «Техническое обеспечение безопасности», специализации «Технические средства защиты информации» осуществлялась в Белорусском государственном университете информатики и радиоэлектроники с 2002 по 2017 годы. Образовательная программа подготовки специалиста предусматривала изучение циклов социально-гуманитарных, естественнонаучных, общепрофессиональных и специальных дисциплин, дисциплин специализации, факультативные дисциплины, экзаменационные сессии, три вида практик, дипломное проектирование и итоговую государственную аттестацию [1]. Цикл общепрофессиональных и специальных дисциплин включал в себя обязательный компонент, вузовский компонент и дисциплины по выбору. Цикл дисциплин специализации включал в себя такие дисциплины как: «Первичные измерительные преобразователи и их применение в системах обеспечения безопасности», «Физические и аппаратные средства защиты информации», «Техническая защита информации в каналах утечки и вычислительных системах и сетях», «Технические и программные средства защиты информации в офисных и банковских системах» и «Проектирование электронных средств и систем обеспечения безопасности». Обучение студентов по специальности «Техническое обеспечение безопасности» предусматривало как очную (дневную), так и заочную формы обучения. При дневной форме обучения срок подготовки специалиста составлял 5 лет, а по заочной форме обучения увеличивался на 1 год. В университете осуществлялась также подготовка специалистов по заочной форме обучения для получения высшего образования, интегрированного со средним специальным образованием, что сокращало время подготовки до 4 лет. Подготовка специалистов проводилась как на бюджетной, так и на платной основе. Выпускающей кафедрой являлась кафедра «Проектирование информационно-компьютерных систем». При подготовке специалистов по специальности «Техническое обеспечение безопасности» использовались различные виды инновационных технологий, включая собственные разработки университета. За весь период подготовки по всем формам обучения по специальности «Техническое обеспечение безопасности» в Белорусском государственном

университете информатики и радиоэлектроники было выпущено более 1000 специалистов, работающих в настоящее время в различных областях, связанных с обеспечением защиты информации и безопасности объектов.

Список литературы

1. Образовательный стандарт республики Беларусь ОСРБ 1-38 02 03-2007. – Минск: МО РБ, 2007. – 36 с.

ИССЛЕДОВАНИЕ ЭКРАНИРОВАНИЯ РАДИОЗАКЛАДНЫХ УСТРОЙСТВ

В.М. Алефиренко, В.Е. Галузо

При установке радиозакладных устройств, передающих информацию по радиоканалу (радиомикрофонов), злоумышленник должен обеспечить максимальную визуальную скрытность установки, оптимальное место установки с точки зрения съема акустической информации, максимальную дальность приема информации по радиоканалу и минимальную возможность его обнаружения. Последнее условие теоретически может быть обеспечено путем экранирования радиомикрофона со стороны прослушиваемого помещения. Такой экран, установленный на определенном расстоянии от радиомикрофона, не будет являться серьезным препятствием для акустических волн, но будет экранировать радиосигнал в сторону помещения и не экранировать его в противоположном направлении – в сторону радиоприемника, установленного в соседнем помещении или снаружи здания, в котором находится прослушиваемое помещение. Для проведения исследований были выбраны следующие приборы: индикатор электромагнитного поля, интересептор, портативный частотомер ROGER RFM-31, сканирующий приемник IC-R5. В качестве закладного устройства использовался камуфлированный имитатор радиомикрофона, работающий на частоте 509,5 МГц, выполненный в виде деревянного бруска размером 160×25×15 мм [1]. В качестве экранирующего материала использовался жесткий металлический экран размером 200×300 мм, толщиной 0,5 мм и гибкая металлическая лента тонкой фольги толщиной 0,1 мм, позволяющая создавать различную форму экрана. Жесткий экран располагался перед микрофоном на различных расстояниях, на которых проводились измерения соответствующими приборами. С помощью фольги проводилось экранирование различных поверхностей самого корпуса радиомикрофона (деревянного бруска) и также проводились измерения соответствующими приборами: индикатором электромагнитного поля и интересептором (метод акустической завязки), частотомером (измерение частоты), сканирующим приемником (захват и прослушивание сигналов в помещении). Исследования показали, что когда экран (фольга) располагался вплотную только на одной тыльной стороне бруска, сигнал экранировался на расстоянии 100 мм и менее, на одной тыльной и одной торцевой стороне – на расстоянии 80 мм и менее, на одной тыльной и двух торцевых – на расстоянии 20–30 мм и менее. При этом экранирующий эффект наблюдался со всех сторон, вне зависимости от того, какая сторона экранировалась. Если брусок экранировался со всех сторон, то сигнал вообще не обнаруживался. Таким образом, проведенные исследования показали, что вне зависимости от расстояния, на котором находился экран, достичь одностороннего экранирования сигнала не удается.

Список литературы

1. Алефиренко В.М., Андрушкевич В.С. Поиск закладных устройств комбинационным методом // Тез. докл. XVI Белорусско-российской науч.-техн. конф. «Технические средства защиты информации». Минск, 5 июня 2018 г. С. 12.