ТЕХНОЛОГИЯ МОДУЛЯЦИИ ПОЛОЖЕНИЕМ ИМПУЛЬСА КАК СРЕДСТВО РЕАЛИЗАЦИИ СКРЫТНОСТИ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ПОЛЬЗОВАТЕЛЯ

В.Т. Першин, А.Р. Буренков

Весьма перспективной в настоящее время, является технология сверхширокополосной связи (Ultra Wideband, UWB), называемой технологией импульсного радио. Традиционно термин импульсного радио в системе UWB соответствовал концепции, которая использовалась в широкополосной радиосвязи ограниченной мощности. В настоящее время связь UWB можно разделить на две категории: импульсное радио (single band) и ортогональное частотное разделение с мультиплексированием (Orthogonal Frequency Decision Multiplex, OFDM) (multi band). Такая классификация нашла поддержку в разработке стандарта IEEE 802.15.3a. Цель настоящего сообщения – показать простоту генерирования коротких импульсов и неоспоримые преимущества использования технологии импульсного радио в практике создания радио идентификаторов, которые ранее использовали криптографические средства защиты информации. По виду воздействия на исходную информацию методы криптографического преобразования можно разделить на четыре группы: шифрование, стеганография, кодирование, сжатие. Основным видом криптографического преобразования информации в современных радио идентификаторах наиболее широко используется шифрование, под которым понимается проведение обратимых математических, логических, комбинаторных и других преобразований исходной информации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов или двоичных кодов. Комплексное использование стеганографии и шифрования многократно повышает сложность решения задачи обнаружения и раскрытия конфиденциальной информации. Для шифрования используют алгоритм и ключ.

При проведении экспериментов длительность моноимпульса изменялась в пределах 0,2 – 2 пс, а период импульсной последовательности составлял от 10 до 1000 нс. В качестве главных параметров, характеризующих UWB-устройства, использовались частота повторения коротких импульсов, средняя мощность в пересчете на 1 МГц и пиковая мощность в любой полосе шириной 50 МГц.

ОБЗОР СУЩЕСТВУЮЩИХ ЭФФЕКТИВНЫХ СПОСОБОВ СКРЫТИЯ ОБЪЕКТОВ В ОПТИЧЕСКОМ ДИАПАЗОНЕ ДЛИН ВОЛН

Т.М. Печень, А.М. Прудник

Объекты, скрываемые в видимом и ИК диапазонах длин волн, могут быть легко и простыми способами обнаружены системами УФ разведки. Важно для практического значения исследовать экранирующие покрытия, созданные на основе поглощающих материалов с малым коэффициентом отражения. Одним из способов решения данной проблемы является дифракционные экраны (специальные тонкопленочные покрытия). Интерес представляют композитные материалы минимальной толщины с малым коэффициентом отражения и прохождения в максимально широком диапазоне длин волн. Известно, интегральный эффект отражения минимальный в случае использования широкополосного поглощающего покрытия. Наиболее простые материалы, имеющие малый коэффициент отражения, можно легко создать на основе пористых композитов, в которых поглотитель насыщен заданным количеством микропор. Следует отметить, что такой поглотитель характеризуется высоким коэффициентом пропускания.

Интерес представляет исследование способов снижения заметности камуфляжного материала в оптическом диапазоне длин волн. Известны разработки швейцарской компании SSZCTL по развитию технологии камуфляжа обмундирования солдат за счет снижения излучательной способности поверхности одежды путем использования металлотканых материалов, подобных шерсти, и специальных покрытий. В [1] приводятся данные, которые свидетельствуют о том, что при использовании этих материалов достигается снижение заметности объектов более чем на 60 %. Важно также отметить: эффективные наблюдаемые температуры людей, одетых в такое обмундирование, могут снижаться до 12–21 °С. Ранее в СССР, а теперь в России широко применяются однослойные маскировочные покрытия из состава табельных маскировочных комплектов МКТ-Л МКТ-Т, МКС-2, обеспечивающие снижение заметности объектов в оптическом диапазоне длин волн [2]. Данные покрытия могут быть изготовленными как из хлопчатобумажной сетчатой ткани, так и содержать основу в виде сети капроновых нитей с заполнением

поливинилхлоридной пленки с просечками или тканевыми пятнами и лентами из миткаля. Достоинством этих маскировочных покрытий является небольшая удельная масса. Из основных недостатков следует отметить следующие: слабая маскировка в ИК диапазоне, низкие физико-механические и эксплуатационные характеристики (повышенные гигроскопичность и горючесть).

Таким образом, постоянное развитие современных и эффективных методов обнаружения объектов средствами оптической разведки требует от исследователей поиска новых способов скрытия.

Литература

1. *Peach M.* // Infrared Imaging News. – 2012. № 6. – P. 2 – 7.

2. *Минин И. В., Минин О. В., Харитошин Н. А.* // ИНТЕРЭКСПО ГЕО-СИБИРЬ. – 2015. Т. 5., № 1. – С. 85 – 88.

ОЦЕНКА ТЕКУЩЕГО СОСТОЯНИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

М.Ю. Пимошенко

Целью аудита является предоставление независимой и объективной комплексной оценки текущего состояния защищенности информационной системы, позволяющей систематизировать угрозы информационной безопасности и предложить рекомендации по их устранению. Задачи, которые решаются В ходе аудита защищенности информационной системы решаются следующие задачи: анализ структуры, функций, используемых технологий автоматизированной обработки и передачи информации в информационной системе, анализ бизнес-процессов, нормативно-распорядительной и технической документации; выявление значимых угроз информационной безопасности и путей их реализации, выявление и ранжирование по степени опасности существующих уязвимостей технологического и организационного характера в информационной системе; составление неформальной модели нарушителя, применение методики активного аудита для проверки возможности реализации нарушителем выявленных угроз информационной безопасности; проведение теста на проникновение по внешнему периметру IP-адресов, проверка возможности проникновения в информационную систему при помощи методов социальной инженерии; анализ и оценка рисков, связанных с угрозами безопасности информационных ресурсов; оценка системы управления информационной безопасностью на соответствие требованиям СТБ ISO/IEC 27001-2011 и разработка рекомендаций по совершенствованию системы управления информационной безопасностью; разработка предложений и рекомендаций по внедрению новых и повышению эффективности существующих механизмов обеспечения информационной безопасности.

Комплексная проверка позволяет увидеть полную картину состояния информационной безопасности на предприятии, локализовать имеющиеся проблемы и слабые места системы защиты и разработать эффективную программу построения системы информационной безопасности предприятия. Результатом независимой оценки текущего состояния системы информационной безопасности, устанавливающей уровень ее соответствия определенным критериям, является предоставление результатов в виде рекомендаций.

ОБ ЭКСПЕРИМЕНТАЛЬНОМ ПОДТВЕРЖДЕНИИ ВРЕМЕНИ ХРАНЕНИЯ ИНФОРМАЦИИ ИНТЕГРАЛЬНЫХ МИКРОСХЕМ EEPROM ПОСЛЕ ОТКЛЮЧЕНИЯ ПИТАНИЯ

В.И. Плебанович, С.М. Боровиков, А.В. Будник

Электрически стираемые перепрограммируемые постоянные запоминающие устройства (в англоязычной редакции EEPROM – Electrically Erasable Programmable Read Only Memory) для запоминания данных используют эффект хранения заряда на плавающем затворе МОП-транзистора при отключённом питании. Одной из важнейших эксплуатационно-технических характеристик является продолжительность хранения информации после отключения питания [1]. Актуальным является вопрос о подтверждении гарантированного в ТУ значения этой характеристики.

Для кристаллов интегральных микросхем (ИМС) EEPROM предлагается способ прогнозирования времени хранения информации после отключения питания. Прогнозирование выполняется с использованием ускоренных испытаний [2], в качестве которых рассматриваются температурные воздействия, сопровождающие технологические операции помещения кристалла в корпус и сборки ИМС.