

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. – Р. 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 отключенном 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.