Литература

1. Интернет-портал Российской Федерации [Электронный ресурс]. – URL: https://www.anti-malware.ru (дата обращения: 10.05.2018).
2. Интернет-портал Dark Reading [Электронный ресурс]. – URL: https://www.darkreading.com (дата обращения: 10.05.2018).

ЭЛЕКТРОМАГНИТНЫЕ ЭКРАНЫ НА ОСНОВЕ ЖЕЛЕЗОСОДЕРЖАЩИХ ПОРОШКООБРАЗНЫХ МАТЕРИАЛОВ

Н.А. Неверов, О.В. Бойправ, Н.В. Богуш, Т.В. Полуян

Один из путей предотвращения утечки информации по каналу побочного электромагнитного излучения заключается в электромагнитном экранировании устройств, с помощью которых выполняется обработка этой информации. Для этого используются материалы, обеспечивающие ослабление напряженности электромагнитного излучения. Основной недостаток таких материалов заключается в их высокой стоимости. В настоящей работе для получения низкостоимостных электромагнитных экранов предложено использование железосодержащей пыли, являющейся отходом различный стадий производства лифтовых изделий:

– лазерная резка металла;

– рихтовка направляющих лифтовых изделий;

– двухступенчатая дробеметная очистка металлических изделий.

Определено, что указанная железосодержащая пыль характеризуется высокими значениями относительной магнитной проницаемости (от 30 до 90 отн. ед. в зависимости от того, в результате реализации какой стадии производства она была получена).

Выполнен синтез электромагнитных экранов на основе железосодержащей пыли. Для этого реализованы ее смешивание со связующим веществом (цементным раствором) и формовка полученной смеси в плиты с плоской поверхностью. Исследованы характеристики передачи и отражения электромагнитного излучения (ЭМИ) синтезированных экранов. Установлено, что величина коэффициента передачи ЭМИ в диапазоне частот 0,7…17 ГГц экранов на основе железосодержащей пыли, полученной в результате лазерной резки металла, изменяется в пределах от –2 до –14 дБ, а экранов на основе железосодержащей пыли, полученной в результате рихтовки направляющих лифтовых изделий и двухступенчатой дробеметной очистки металлических изделий – соответственно от –2 до –12 дБ и от –2 до –25 дБ (при толщине, равной 1 см). Средняя величина коэффициента отражения ЭМИ указанных экранов составляет –8 дБ (при условии их закрепления на металлических подложках).

На основе представленных результатов можно сделать вывод о перспективности применения железосодержащей пыли в целях изготовления устройств для архитектурного электромагнитного экранирования.

ОРГАНИЗАЦИОННЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

Т.С. Немов, Ю.А. Скудняков

Для обеспечения защиты информации необходимо строгое разделение обязанностей на предприятии. В зависимости от степени секретности необходимо наличие особых служб безопасности, которые подчиняются непосредственно руководству организации и контролируют соблюдение всех правил. Залог успеха в борьбе с несанкционированным доступом к информации – это четкое представление о каналах утечки информации. В общем виде необходимо разделить весь комплекс мер по защите информации на 3 больших блока: 1) ограничение доступа; 2) разграничение доступа; 3) контроль доступа. Ограничение доступа должно осуществляться в зависимости от степени секретности. Наиболее простым способом контроля является введение пропускной системы, при которой каждый отдел работает в ограниченной изолированной зоне [1]. Разграничение доступа заключается в распределении узких функциональных задач. Каждый сотрудник должен выполнять строго определенные функции [2]. Ограничение полномочий каждого пользователя позволит защитить информацию в случае проникновения злоумышленника в отдельно взятый отдел. Даже если один участок

будет уязвим, вся система продолжит функционировать в нормальном режиме. Контроль доступа должен быть основан на идентификации. В этом случае необходимо присваивать каждому субъекту уникальный образ, имя и число. В обязанности службы безопасности входит проверка соответствия всем требованиям. Приведенные выше организационные методы являются лишь базовыми для обеспечения защиты информации на предприятии. Данный список может дополняться в зависимости от конфиденциальности информации, которая используется при работе предприятия, объема выполняемых работ и опыта работы сотрудников предприятия в сфере защиты информации. Эффективность каждого блока полностью зависит от руководства предприятия, которое должно обеспечить предприятие финансовыми и человеческими ресурсами. Финансовые вложения позволяют обеспечить предприятие необходимыми техническими и криптографическими средствами защиты информации.

Литература

1. Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа. М.: Гелиос АРВ, 2006. 376 с.

2. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. Кн. 1. М.: Энергоатомиздат, 1994. 400 с.

ПРОГРАММНОЕ СРЕДСТВО ПРЕДПРОСМОТРА НАСТРОЕК ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ MICROSOFT DYNAMICS AX

В.Н. Нестеренко

В работе представлено расширение для модуля «Безопасность» ERP-системы Microsoft Dynamics AX [1], позволяющее осуществлять предпросмотр отдельных частей интерфейса системы с учетом привилегий конкретного пользователя.

Разработанное программное средство предназначено для оптимизации процесса обеспечения безопасности путем определения прав доступа пользователей ERP-системы. С его помощью разработчики и менеджеры безопасности могут увидеть, как будет выглядеть та или иная форма для указанного пользователя Microsoft Dynamics AX в соответствии с предоставленными ему привилегиями. Программное средство позволяет учитывать общие настройки доступа пользователей, особенности отображения форм, связанные с привилегиями точки входа, а также воздействия «Record-level security». Для случаев, когда вызов формы осуществляется из родительской формы, предусмотрена возможность настройки и передачи необходимых входных данных в вызываемую форму, в том числе привилегии формы-родителя, что позволяет в полной мере эмулировать такого рода ситуации. Расширение представлено графическим интерфейсом, выполненным в соответствии с правилами, принятыми для Microsoft Dynamics AX. В ходе работы были реализованы алгоритмы обхода элементов форм, определения действующих прав доступа к элементам форм на основе ролей пользователя и установленной привилегии точки входа, фильтрации данных по правилам «Record-level security» с учетом текущих ролей пользователя и других особенностей этой технологии. Для этого использовались встроенный фреймворк для обработки узлов дерева объектов Microsoft Dynamics AX, стандартные методы и классы модуля «Безопасность», а также утилиты для работы с «Record-level security». В результате удалось получить эффективное средство для контроля проделываемой работы по установке привилегий пользователей.

Литература

1. The Microsoft Dynamics AX Team. Inside Microsoft Dynamics AX 2012 R3. Redmond: Microsoft Press, 2014. 371 p.

МЕТОДИКА ТЕСТИРОВАНИЯ АНТИВИРУСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Омуару Алвелл Эллингтон, Е.С. Белоусова

С быстрым развитием технологий меняется и характер вирусных угроз для данных. Технологии, которые должны обеспечить защиту от этих угроз, должны адаптироваться.