СОВРЕМЕННАЯ ПАРАДИГМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.А. Навроцкий, Л.С. Стригалев

Возникновение «интернета вещей» (Internet of Things, IoT) расширяет пространство свободы и семантические возможности современных систем. Это требует совершенствования и технологий защиты информации, поскольку аналогичные возможности приобретает и атакующая сторона, которая значительно мобильней жертвы в применении современных технологий, таких Big Data и Data Mining (Text Mining, Web Mining, Call Mining, Audio Mining, Video Mining). Возникает разрыв между технологиями атакующей защищающей систем.

Необходима доработка политики информационной безопасности системы с последующим внедрением искусственных нейронных сетей (ИНС), которые обладают возможностью обучаться и самообучаться. Современное применение ИНС в сфере информационной безопасности носит, как правило, «лоскутный» характер, в то время как необходимо структурированное иерархическое внедрение ИНС по всем «болевым» точкам системы, согласно разработанной политике информационной безопасности с возможностью последующей самоорганизации.

Технологической нишей ИНС при построении систем безопасности в настоящее время является досемантическая обработка информации, охватывающая такие аспекты технологии восприятия информации как обнаружение, распознавание и анализ. Для эффективной информационной защиты системы на современном этапе необходим симбиоз традиционных технологий [1] и ИНС.

Литература

1. Навроцкий А.А. Герман О.В., Стригалев Л.С. Методы оценки качества средств защиты информации // Технические средства защиты информации: тезисы докладов XII Белорусско-российской науч.-техн. конф. Минск, 28–29 мая 2014 г. С. 7.

ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ МЕТОДОМ DECEPTION

А.И. Наумович, А.С. Шелягович

Многочисленные публикации и открытые кейсы успешных взломов самых защищенных систем в разных странах мира свидетельствуют о том, что традиционные превентивные техники защиты информации в компьютерных сетях уже не работают. Перед направленными атаками, такими как APT или Zero-day, современные методы и стратегии защиты корпоративного периметра оказались бессильны. Кроме того, современные решения оказались недостаточно гибкими для минимизации рисков, связанных с этими угрозами. Подобные проблемы могут быть решены с применением технологии Deception. Технология Deception – это использование техник активного обмана атакующих с применением специализированных ловушек, приманок и других методов дезинформации. Применение техник обмана внутри корпоративного периметра предоставляет предприятиям возможность раннего обнаружения наиболее опасных направленных атак, которые не были отслежены превентивными механизмами, такими как межсетевые экраны, системы предотвращения вторжений и антивирусные решения. Например, если атакующий сканирует сеть или осуществляет пассивный сбор сетевых пакетов, его можно обмануть, показав множество поддельных устройств, привлекательных для атаки, на которых активны сервисы с уязвимостями. Современные Deception-решения позволяют генерировать такие ловушки, которые невозможно отличить от реальных Windows/Linux/Mac-устройств, сетевого оборудования, банкоматов, POS-устройств, SCADA-устройств, баз данных, корпоративных приложений (Oracle, SAP, CyberArk и т. п.) и даже SWIFT-инфраструктуры. Любая попытка взаимодействия с этими «сенсорами» приведет к обнаружению атакующего. В отличие от существующих средств защиты, для которых высока вероятность обхода, решения, использующие технологии ловушек – позволяют максимально быстро обнаружить злоумышленника в случае успешной атаки. Это дает возможность специалистам по информационной безопасности поймать злоумышленника фактически с поличным, остановить дальнейшее распространение атаки и предупредить кражу конфиденциальных данных в автоматическом режиме.

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