более высокая неровность края элементов и не регистрировать большое количество ложных дефектов на краях элементов топологии. Метод компенсации погрешностей рассовмещения реального и эталонного объектов предназначен для оснащения оборудования автоматического контроля топологии, включая: систему привязки координатной системы установки к эталонной координатной системе, систему динамического автосовмещения реального и эталонного изображений, систему маскирования несовпадений на краях элементов топологии. Предложенная алгоритмизация и аппаратно-программная реализация на ее основе была использована при разработке программного обеспечения компенсации погрешностей рассовмещения реального и эталонного объектов установок ЭМ-6029Б и ЭМ-6329 автоматического контроля топологии планарных структур.

Литература

1. Аваков, С.М. Автоматический контроль топологии планарных структур / С.М. Аваков. – Минск : ФУАинформ, 2007. – 168 с.

МЕТОДЫ ЭВРИСТИЧЕСКОГО АНАЛИЗА ПРИ ОБНАРУЖЕНИИ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ВЕБ-ПРИЛОЖЕНИЯХ

А.С. Цалко, П.В. Кучинский

В большинстве случаев сетевых атак злоумышленниками на веб-приложения результатом являются загруженные файлы – вредоносное программное обеспечение. Самым старым и популярным методом обеспечения защиты приложений является сигнатурный анализ. Связано это с тем, что атаки на веб-приложения в большинстве случаев производятся на основе уже известных уязвимостей с использованием готовых инструментальных средств [1].

С каждым днем исходные коды вредоносного ПО стараются замаскировать и сделать как можно более изменчивым, «полиморфным» или наоборот, сделать максимально простым и похожим на обычный скрипт. Вредоносное ПО размещается не только в новых файлах, а также и в системных файлах CMS, на которой функционирует сайт. Не редки случаи размещения исходного кода в базах данных веб-сайтов, а также в изображениях [2].

При применении злоумышленником нового метода обфускации или места размещения исходных кодов сигнатурный автоматический анализ не даст результатов. В этом случае на помощь приходят методы эвристического анализа – совокупность функций, нацеленных на обнаружение неизвестных сигнатурным базам вредоносного ПО.

Метод эвристического анализа определяет по косвенным признакам, является ли объект вредоносным. Причем в отличие от сигнатурного метода эвристик может детектировать как известные, так и неизвестные угрозы безопасности. Для того, чтобы применить методы эврестического анализа для веб-приложений (веб-сайтов), необходимо рассматривать их в качестве «черного ящика». Система, которую представляют как «черный ящик», изучается как имеющая некий «вход» для ввода информации и «выход» для отображения результатов работы, при этом происходящие в ходе работы системы процессы наблюдателю неизвестны.

Для определения набора паттернов поведения вредоносное ПО необходимо классифицировать и группировать по методам использования. В результате исследования поведения найденных с помощью сигнатурного сканирования образцов вредоносного ПО удалось выделить многие паттерны поведения и методы их детектирования.

Использование методов сигнатурного анализа позволило выявить за месяц наблюдений 8 новых произведенных атак на PHP-сайты, подконтрольные ЦИИР БГУИР. Использование данных методов наблюдения за поведением серверов и внешними изменениями вкупе с сигнатурным анализом является неотъемлемой частью обеспечения информационной безопасности веб-сайтов.

Литература

1. Anti-Malware.ru, Коробочная безопасность веб-приложений. Внутренности Web Application Firewall [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/analytics/Technology_Analysis/Web_Application_Firewall. – Дата доступа: 17.02.2017.

2. Sucuri.net, Malware Hidden Inside JPG EXIF Headers [Электронный ресурс]. – Режим доступа: https://blog.sucuri.net/2013/07/malware-hidden-inside-jpg-exif-headers.html. – Дата доступа: 17.02.2017.

МЕРА СХОЖЕСТИ НЕЛИНЕЙНОСТЕЙ ВОЛЬТАМПЕРНЫХ ХАРАКТЕРИСТИК РАДИОЭЛЕКТРОННЫХ ЗАКЛАДНЫХ УСТРОЙСТВ СЪЕМА ИНФОРМАЦИИ

В.М. Чертков, В.К. Железняк

Мера сходства играет ключевую роль при формировании классификации изучаемого множества параметров объекта и при распознавании принадлежности объектов к тому или иному классу. Специфика этих задач состоит в том, что мера сходства здесь является величиной относительной, она зависит не только от сходства объекта с определенным классом, но и от его сходства с другими классами [1]. Актуальность темы обусловлено решением проблемы определения меры схожести нелинейностей вольтамперных характеристик (ВАХ) радиоэлектронных закладных устройств съема информации, полученных на основе разработанного авторами способа распознания типа нелинейности [2]. В качестве критерия определения меры сходства известной и расчетной ВАХ, т.е. распознания типа ВАХ, выбрано средние значение среднеквадратических отклонений каждого расчетного коэффициента аппроксимирующего полинома третьей степени. В ходе проведения экспериментов определен оптимальный порог критерия меры сходства для принятия решения о соответствии задаваемой и расчетной ВАХ.

Литература

1. Количественная мера компактности и сходства в конкурентном пространстве / Н.Г. Загоруйко [и др.] // Сибирский Журнал Индустриальной Математики. – 2010. – Т. XIII. – № 1. – С. 59–71.

2. Чертков, В.М. Идентификационный портрет как основной параметр идентификации РЭС / В.М. Чертков, В.К. Железняк // Теоретические и прикладные аспекты информационной безопасности: материалы Междунар. науч.-практ. конф. Минск, 31 марта 2016 г. – С. 237–241.

ОЦЕНКА ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО ВОЛКОННО-ОПТИЧЕСКИМ ЛИНИЯМ СВЯЗИ

Д.В. Шандяло

В отличие от всех других сред передачи информации, формирование каналов несанкционированного съема на участках волоконно-оптического тракта, требует прямого доступа к оптоволокну и специальных мер отвода части излучения из оптоволокна. Извлечение информации при регистрации выведенного из волокна излучения зависит от вероятности ошибочного приема одного двоичного символа передаваемой информации и вероятности искажения кодовых комбинаций. Эти показатели зависят от вида используемых сигналов, от способов обработки сигналов, а также от длительности используемых кодовых комбинаций. В данной работе приведены вычислильная работа и концепция в виде физического эксперимента, при использовании подключения посредством метода импульсной рефлектометрии. Дается определение, описание, а также способ формирования технического канала утечки информации в волоконно-оптических технологий. Основой системы фиксации несанкционированного доступа (НД) является система диагностики состояния (СДС) оптического тракта, которая построена с анализом отраженного сигнала. На основании проведенного анализа и дальнейших исследований, предполагается обосновать соответствующие способы защиты информации в ВОЛС, а также разработать алгоритм и методику оценки защищенности ВОЛС. Методика оценки защищенности информации от несанкционированного доступа в ВОЛС описывает основные принципы, средства и методы обеспечения ИБ и может использоваться для оценки рисков нарушения ИБ

На основании исследования сделаны выводы по возможности улучшения контроля и повышения защищенности передаваемой информации по ВОЛС. В качестве возможных мер, позволяющих достичь этого, рассматривается использование постоянной и эффективной