management systems – Guidance. // International Organization for Standardization. URL: https://www.iso.org/standard/63417.html (дата доступа: 17.05.2017).

3. СТБ ISO/IEC 27001:2016. Системы менеджмента информационной безопасности. Требования. Введ. 2016-01-10. Минск: БелГИСС, 2016. 28 с.

ОБЪЕКТНО-ОРИЕНТИРОВАННЫЙ ПОДХОД АНАЛИЗА ДЕФЕКТОВ ПРИ КОНТРОЛЕ ПЛАНАРНЫХ СТРУКТУР

Е.А. Титко

В работе представлены быстродействующие алгоритмы эффективного обнаружения дефектов планарных структур, возникающих при изготовлении из СБИС. Они основаны на объектно-ориентированном подходе анализа дефектов с помощью сегментированных алгоритмов с минимальной логической сложностью [1]. При этом достигается расширении структурных информационных данных о топологии при некотором изменении аппаратной операции оборудовании автоматического контроля разных модификаций одного семейства. Это достигается за счет большого запаса по производительности, в результате которого появляется возможность иметь оригинальные, но унифицированные с точки зрения исполняемого кода, алгоритмы для различных типов топологии и, соответственно, различных топологических слоев, а также для различных типов дефектов. При этом настройка на конкретный тип топологии или дефекта осуществляется за счет смены базы данных алгоритма, а сам алгоритм может оставаться, практически, неизменным.

В результате применения разработанных алгоритмов обнаружения дефектов достигается высокая производительность автоматического оборудования, повышение субпиксельного разрешения, возможность специализации алгоритмов по типам обрабатываемой топологии и группам дефектов, упрощение аппаратной реализации путем распараллеливания и совмещения во времени операций, выполняемых за один такт.

Самостоятельное значение имеет возможность определения фотолитографической значимости дефектов в режиме реального времени. В некоторых случаях возможность определения фотолитографической значимости дефектов в режиме реального времени позволяет также автоматически принимать решение о критичности дефекта и, соответственно, выполнять пакетную обработку шаблонов в автоматическом режиме.

Литература

1. Титко, Е.А. Универсальная система получения субпиксельного разрешения / Е.А. Титко, С.А. Манин, Г.А. Зубов // Информационные технологии и системы 2016 : материалы Междунар. науч. конф., Минск, Респ. Беларусь, 26 окт. 2016 г. / Белорус. гос. ун-т информатики и радиоэлектроники. – Минск, 2016. – С. 88–89.

МЕТОД КОМПЕНСАЦИИ ПОГРЕШНОСТЕЙ РАССОВМЕЩЕНИЯ РЕАЛЬНОГО И ЭТАЛОННОГО ОБЪЕКТОВ

Д.С. Титко

В работе рассматривается метод автоматизированного контроля топологии планарных структур, который основан на системе динамического автосовмещения реального и эталонного изображений [1]. Метод основан на алгоритмической минимизации количества ложных дефектов.

Разработанный метод предназначен для системы маскирования ложных дефектов, которая работает на основании информации, получаемой от устройства распознавания края элемента, которое на каждом шаге работы детектора дефектов вырабатывает признак края элемента, который принимает значение «1» при компарировании края элемента и значение «0» – в противном случае. Эта система, при вводе соответствующего признака оператором-технологом, позволяет маскировать несовпадения реального и искусственного изображений в диапазоне ±1 или ±2 пикселя относительно положения края элемента искусственного изображения. В результате появляется возможность снизить чувствительность установки на краях элементов, что позволяет контролировать топологию изделий для которых допускается

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.