продуктами почти не ведется или эти вопросы обсуждаются только в профессиональной среде. До рядового пользователя существующие угрозы в популярных продуктах информационных технологий и возможные последствия их использования не доходят. Вообще говоря, даже лица в обязанности, которым вменено обеспечивать информационную безопасность, далеко не всегда осведомлены с существующими проблемами в сфере защиты информационных ресурсов и тем более защиты личности.

В настоящее время перед обществом встает серьезная проблема ликбеза в сфере защиты личности и информационных ресурсов, как общества в целом, так и отдельных пользователей. На государственном уровне этой проблеме достаточного внимания не уделяется. Необходимо выработать концептуальные основы повышения осведомленности общества в проблемах информационной безопасностью, и самым серьезным образом подойти к проблемам информационного зомбирования. Промедление в решении этих вопросов может серьезно повлиять на мотивационное поведение масс, защищенность государства от внешнего вмешательства в управление и устойчивое экономическое и политическое развитие государства.

СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК ОСНОВА ДЛЯ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ОРГАНИЗАЦИИ

М.В. Сороко, А.М. Прудник

Рассматриваются практические аспекты внедрения системы менеджмента информационной безопасности (СМИБ) в соответствии со стандартом ISO/IEC 27001:2013 [1]. СМИБ – это часть общей системы управления организации, которая основана на оценке рисков, и которая предназначена для реализации, эксплуатации, мониторинга и совершенствования ИБ.

Перед разработкой СМИБ должно быть получено одобрение руководства для организации; должен быть разработан план проекта, который, в частности, предполагает определение области применения; определены требования, которым должна соответствовать СМИБ, должны быть определены информационные активы организации и получены данные по текущему состоянию ИБ в рамках области применения СМИБ; должна быть определена методология оценки рисков, сама оценка рисков и выбор вариантов действий с рисками (уменьшение, передача, принятие), а также выбор средств управления ими.

Собственно разработка СМИБ предполагает разработку конечной структуры организации с описанием ролей и сфер ответственности; разработку политик ИБ; разработку процедур обеспечения ИБ; разработку систем ИБ информационных и коммуникационных технологий и физических объектов, в том числе план внедрения средств управления; разработку средств управления; план проверок, проводимых руководством, т.е. список исходных данных для осуществления проверки и ее процедуры, включая аспекты аудита, мониторинга и измерения; разработку программы обучения, образования и информирования персонала организации в области ИБ, в т.ч. материалы для обучения в области ИБ, само обучение в области ИБ, включая разъяснение функций и ответственности, планы обучения и записи результатов обучения, образования и информирования в области ИБ и разработку конечного плана проекта СМИБ.

После разработки и внедрения СМИБ организации надлежит выполнить процедуры мониторинга и анализа, провести внутренний и внешний аудиты, произвести измерение результативности средств управления с целью определения их соответствия требованиям безопасности, а также выполнить оценки рисков.

Заключительными действиями являются разработка процедур по корректирующим и предупреждающим действиям, произвести проверку полного соответствия СМИБ по контрольной таблице стандарта ISO/IEC 27003 [2] и, при необходимости сертификации по национальному стандарту [3], провести внешний аудит.

Литература

1. ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements // International Organization for Standardization. URL: https://www.iso.org/standard/54534.html (дата доступа: 17.05.2017).

2. ISO/IEC 27003:2017 Information technology – Security techniques – Information security

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