Разработчики антивирусных программ утверждают, что они обеспечивают эффективное реагирование на компьютерные вирусные инциденты. Однако в настоящее время мало указаний относительно наилучшего способа оценки эффективности таких требований. Поэтому особенно актуальным является разработка тестов антивирусных программных продуктов, которые измеряют эффективность функциональных возможностей антивируса. Используя этот подход, была разработана методика тестирования выполнения требований к функциональности антивирусных программ. В настоящее время существует 4 метода тестирования антивирусных программ: статическое тестирование, динамическое тестирование; тестирование скорости реакции, ретроспектива. Тесты продолжают развиваться по мере развития отрасли, продукты становятся более сложными, требуются более сложные тесты. важно расширить методологию тестирования в областях, которые наиболее важны для защиты пользователей, используя индикаторы, которые важны как для пользователей, так и для разработчиков.

Методика тестирования антивирусных продуктов заключалась в диагностики сканирующих механизмов, защиты от вредоносных веб-приложений, фишинга, дополнительных сканеров. Для тестирования были выбраны следующие программные продукты: Kaspersky, Avira, Avast, Eset NOD32. На основе проведенных тестов можно заметить, что не один из тестируемых продуктов не обнаружил 100 % зараженных файлов, при этом все продукты осуществляли попытку лечения некоторых файлов, а не просто удалять обнаруженные ими угрозы. Антивирусный продукт Kaspersky обнаружил 97,65 % зараженных файлов, при этом из них более 60 % было удалено. Антивирусный продукт Eset NOD32 обнаружил 77,88 % зараженных файлов, восстановлено было около 55 % файлов.

ЗАЩИТА АВТОРСКИХ ПРАВ ИЗОБРАЖЕНИЯ С ИСПОЛЬЗОВАНИЕМ ЦВЗ

Н.В. Орлов

1. *Проблема.* Вопрос защиты авторских прав на цифровые изображения актуален в наше время, т.к. графические материалы, разработанные автором, могут быть легко скопированы или распространены. Простота кражи чужих графических изображений привело к тому, что каждый день увеличивается их хищение. Исходя из этого, проблема защиты авторских прав на графические изображения актуальна в наше время, и техническим решением данной проблемы является программный продукт, предотвращающий копирование, искажение или распространение авторских материалов.

2. *Метод решения.* Для защиты графических материалов широко используется применение цифровых водяных знаков. Таким образом, для защиты графических материалов от копирования и распространения используется программное обеспечение, основанное на графической защите с применением ЦВЗ на основе криптографического метода Куттер-Джордона-Боссена.[1]

В данном методе ЦВЗ внедряются с помощью изменения цветовых компонентов пикселя. Отдельно взятые биты ЦВЗ неоднократно внедряются в изображение с помощью изменения показателей синего канала в пикселе. Внедрение информации производится по одному биту в один пиксель контейнера. С помощью секретного ключа задаются координаты пикселей, в которые будет произведено встраивание. При внедрении цветовые показатели красного и зеленого цветов остаются неизменными, а цветовые показатели синего – будут изменяться по следующей формуле: $Bx,y^* = \begin{cases} Bx,y + \lambda Yx,y, \text{ при } Mi = 1 \\ Bx,y - \lambda Yx,y, \text{ при } Mi = 0 \end{cases}$, где $\lambda = 0{,}1$; $Yx,y = 0{,}3*Rx,y+0{,}59*Gx,y+0{,}11*Bx,y$. Обозначения: Bx,y – показатель яркости синего цвета с координатами (x, y); Bx,y^* – показатель изменения яркости синего цвета пикселя; Yx,y – показатель яркости пикселя; Mi – i-й бит встраиваемой информации; λ – коэффициент, задающий энергию встраиваемого бита данных [2].

3. *Эффективность.* ЦВЗ должен отвечать следующим свойствам: незримость для человеческого глаз, стойкость к искажению контейнера. Метод Куттера-Джордана-Боссена выполняет необходимые свойства. Достижение незримости для человеческого глаза осуществляется с помощью внедрения битов ЦВЗ именно в синий канал пикселя, так как к данному цвету, человеческий глаз обладает наименьшей чувствительностью.

Достижение стойкости к изменениям графического материала достигается с помощью неоднократного внедрения битов ЦВЗ в разных частях защищаемого изображения.[3]

Таким образом, программное обеспечение, основанное на графической защите с применением ЦВЗ на основе криптографического метода Куттера-Джордана-Боссена, позволяет решать задачу защиты авторской графической информации от несанкционированных кражи и распространения.

Литература

1. Стеганографические системы. Критерии и методическое обеспечение / под ред. В.Г. Грибунина. Саров, ФГУП «РФЯЦ-ВНИИЭФ», 2016. С. 10–29

2. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. М.: ДМК-Пресс, 2006. С. 106–110

3. Грибунин Г.Ф., Пузыренко А.Ю., Туринцев И.В. Цифровая стеганография. Москва: СОЛОН-ПРЕСС, 2009. С. 8–15.

ТОНКОПЛЕНОЧНАЯ МИКРОСБОРКА С ПОВЫШЕННЫМ ТЕПЛООТВОДОМ И ПОМЕХОЗАЩИЩЕННОСТЬЮ БЕСКОРПУСНЫХ КРИСТАЛЛОВ

А.С. Осипович, А.Г. Черных, В.В. Шульгов

Малый удельный вес, высокие коэффициент теплопроводности, электрические и прочностные свойства алюминиевых анодированных подложек (ААП) наиболее полно удовлетворяют жестким требованиям, предъявляемым к массогабаритным характеристикам и тепловым режимам функционирования схем[1]. Применение ААП при создании микроэлектронных устройств позволяет компоновать их без дополнительного основания.

Основанием разработанной микросборки является анодированная алюминиевая подложка с несквозными углублениями, размеры которых с допуском в большую сторону соответствуют размерам монтируемых в них кристаллов. На дне углубления анодный оксид алюминия отсутствует. Предварительное лужение дна углубления позволяет осуществить пайку кристаллов низкотемпературной припойной пастой, обеспечивая при этом хороший электрический и тепловой контакт. Один уровень металлизации обеспечивает электрическую разводку схемы и возможность монтажа поверхностно-монтируемых компонентов на подложку (SMT) и кристаллов в одном цикле.

Углубление имеет высоту, равную сумме толщины кристалла и толщины припойной прокладки. Это сделано с целью автоматизации процесса разварки кристаллов. После монтажа всех кристаллов и SMD компонентов микросборка закрывается гибкой крышкой из безадгезивного алюминий-полиимидного лакофольгового диэлектрика типа ФДИ-А (ЫУО.037.042 ТУ) производства ООО «Тэтраэдр» (г. Москва, Россия) и соединяется с основанием сваркой в местах, свободных от полиимида. Предпочтительна установка микросборки в герметизированных отсеках(аппаратуре).

Литература

1. Sokol V., Shulgov V. Aluminiumunterlagen für die mikroelektronischen Einrichtungen / 9.Chemnitzer Fachtagung Mikromechanik & Mikroelektronik, Chemnitz, 5./6. November 2009. S. 138–140.

ОБУЧАЮЩИЙ КОМПЛЕКС ПО ДИСЦИПЛИНЕ «КВАНТОВЫЕ СИСТЕМЫ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

С.А. Павлюковец, М.П. Патапович, И.В. Бычек

В современных условиях инновационного развития Республики Беларусь, перехода к экономике знаний, научные исследования в учреждениях высшего образования и их связь с потребностями реального сектора экономики приобретают особую значимость, так как, являясь составной частью учебного процесса, они в первую очередь обеспечивают основу образования и его практико-ориентированную направленность.

Совокупность инфокоммуникационных технологий и проводимых научных исследований