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

позволяет повысить качество и эффективность подготовки специалистов. К таким инструментам относится электронный учебно-методический комплекс (ЭУМК), представляющий собой программно-методический обучающий комплекс, включающий систематизированные учебные, научные и методические материалы по учебной дисциплине и призван обеспечить реализацию учебных целей и задач на всех этапах образовательного процесса.

В данной работе авторы рассматривают использование материалов авторского ЭУМК как возможные пути повышения эффективности учебного процесса в рамках перехода на двухуровневую систему высшего образования «бакалавр-магистр».

Дисциплина «Квантовые системы для обеспечения информационной безопасности» II-ой ступени высшего образования заочной формы обучения учреждения образования «Белорусская государственная академия связи» специальности 1-98 80 03 «Аппаратное и программно-техническое обеспечение информационной безопасности» призвана формировать у обучающихся теоретические знания и практические навыки, необходимые для разработки и проектирования квантовых систем безопасности различного уровня и назначения.

ЗАЩИТА ИНФОРМАЦИИ ПРИ ОБРАБОТКЕ ЭЛЕКТРОННЫХ МЕДИЦИНСКИХ КАРТ

В.И. Пачинин, В.А. Пуйдак, Г.В. Сечко, М.А. Тимонович, И.С. Харкевич

Рассматривается защита конфиденциальной персональной информации пациентов в белорусских медицинских учреждениях. Источником такой информации может быть электронная медицинская карта (ЭМК), широкое внедрение которой в поликлиниках Минска началось в 2018 г. и согласно планам Министерства здравоохранения Республики Беларусь должно полностью завершиться к 2020 г. По мнению авторов доклада, внедрение ЭМК в Беларуси будет осложнено отсутствием белорусского закона «О персональных данных», проект которого Национальное собрание Республики Беларусь планирует обсуждать только в 2019 г. Таким образом, сегодня в Беларуси никто не требует у пациента согласия на обработку его персональных данных из ЭМК, что предусмотрено статьей 6 (пункт 1 подпункт 1.1) закона Российской Федерации «О персональных данных» от 27.07.2006 № 152-ФЗ. Следовательно, доступ к персональным данным пациента при обработке ЭМК автоматически получает целый круг медицинских работников, обрабатывающих данные [1], а правовой гарантии защиты этих данных в Беларуси пока нет. В этом аспекте в России у пациента больше возможностей: не согласившись на обработку своих данных без своего участия пациент может разместить эти данные в архиве, доступ к которому будет иметь только он с помощью системы распознавания личности по радужной оболочке глаза (РОГ) [1]. Стоимость такой системы в последние годы резко снижается за счет сканирования РОГ с помощью смартфона. Обработку данных из архива медицинский работник сможет вести только в присутствии пациента и под его контролем (либо в присутствии доверенного лица пациента, имеющего доступ к архиву). Тем самым пациент получит высокий уровень защиты своих данных (если ему это, конечно, необходимо).

Литература

1. Ситник, М. Ю. Состояние защиты персонифицированных медицинских данных в Беларуси в 2018 году // Материалы 54-й науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8 «Информационные системы и технологии». Минск, 21 апреля 2018 г. С. 92–94.

ИСПОЛЬЗОВАНИЕ МОДУЛЯЦИИ ПОЛОЖЕНИЕМ ИМПУЛЬСА В ТЕХНОЛОГИИ РАДИОЧАСТОТНОЙ ИДЕНТИФИКАЦИИ ОБЪЕКТОВ

В.Т. Першин

Система радиочастотной идентификации (Radio Frequency IDentification, RFID) объектов в общем случае содержит три компонента: считыватель (ридер), идентификатор (карта, метка, тег) и компьютер. Считыватель излучает в окружающее пространство электромагнитную энергию. Идентификатор принимает сигнал считывателя и формирует