КАЛУЖСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО
ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Э. БАУМАНА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)»
(КФ МГТУ ИМ. Н.Э. БАУМАНА)

На правах рукописи

Беккель Людмила Сергеевна

ИДЕНТИФИКАЦИЯ БУМАЖНЫХ ДОКУМЕНТОВ ПО НЕВОСПРОИЗВОДИМОЙ МЕТКЕ, СОЗДАННОЙ СТОХАСТИЧЕСКИМ ЭЛЕКТРОРАЗРЯДНЫМ ПРОЦЕССОМ

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

ДИССЕРТАЦИЯ

на соискание ученой степени кандидата технических наук

Научный руководитель: к.т.н., доцент

Шкилев Владимир Дмитриевич

Калуга – 2019

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. Бумажные документы могут содержать как общедоступную, так и конфиденциальную информацию. Сопроводительные документы на продукцию, ценные бумаги, удостоверения личности, документы об образовании, профессиональной деятельности содержат конфиденциальную информацию, ограниченного доступа [1, 2]. Эта информация нуждается в защите от «неправомерного модифицирования, копирования» [1-4]. Средствами защиты могут служить «техническое, программное, программно-техническое средство, вещество и (или) материал» [5]. Для идентификации документов – проведения процедуры выявления их подлинности по совокупности характерных признаков (идентификаторов) – предназначены «реквизиты, позволяющие ее идентифицировать» [6].

Существующие правила идентификации бумажных документов по «наименованию и коду организации, наименованию и коду формы документа, дате, регистрационному номеру документа, подписи, печати, грифам согласования и утверждения» [7] при современном уровне развития компьютерной техники и технологий не могут обеспечить защиту бумажных документов от угроз их фальсификации. Способы защиты документов – водяные знаки, голограммы, штрихкоды не дают положительного результата, так как эти признаки воспроизводимы.

Среди способов идентификации [11, 15, 17, 23-37] широко распространен метод автоматической (бесконтактной) идентификации, для которой «используются, например, штриховые коды, радиоэтикетки, магнитные полосы, смарт-карты, звуки и сигналы, оптически распознаваемые знаки и др.» [9]. Анализ существующих способов выявил наличие их основных недостатков:

1. Невозможность применения к идентификации бумажных документов.

2. Невозможность выделения объекта из ряда ему подобных, из его же класса, из-за отсутствия уникальной метки.
3. Отсутствие сложности повторения объекта в виде его копии.

Этим объясняется направленность диссертационной работы на исследование существующих методов идентификации документов и разработку нового метода, основывающегося на создании и использовании невоспроизводимых уникальных характеристик – меток, наносимых на бумажные документы. Основное требование к метке – невозможность ее повторения на других носителях. По этой характеристике и должно осуществляться отождествление документа.

Существуют критерии, по которым можно судить о надежности защиты бумажных документов: «защита должна определять нерентабельность подделки; защита должна обеспечивать устойчивый однозначный контроль подлинности; защитный комплекс должен действовать как в условиях контролируемого, так и неконтролируемого окружения; применение защиты предполагает наличие надежной аппаратной базы контроля подлинности; надежная защита обеспечивается совокупностью разнородных защитных технологий» [52].

Анализ существующих способов, использующих стохастические физические процессы для придания объекту уникальной метки, доказал недостаточную степень проработанности задачи идентификации бумажных документов. Например, применение предложенной рядом исследователей [29-31] спектральной идентификации объектов проблематично из-за неопределенности состава изотопной метки в различные временные промежутки, вызванной ее взаимодействием со средой. Методы, основанные на использовании магнитных свойств или измерении спекл-структур [33-36], требуют применения специальных материалов и обеспечения стабильности проверяемой структуры в течение срока службы объекта. Применение каучукового опознавательного знака или магнитного чипа на бумаге требует

обеспечения условия его идеальной впечатываемости, что приведет к значительным затратам [32]. Кроме того, при использовании прикрепляемых маркеров возможно отсоединение и прикрепление маркера к другому объекту.

Отсутствие надежного метода идентификации бумажных документов приводит к распространению фальсифицированных товаров: по результатам анализа рынка охранных систем [8], 20% автосигнализаций являются контрафактом и распространяются по поддельным накладным. С каждым годом подделок становится больше, так как их выявление производится только при случайном обнаружении сайтов с объявлениями о продажах представителями фирм-производителей автосигнализаций-подлинников. ООО НПО «Телеметрия», выпускающее противоугонную автомобильную электронику под брендом «Pandora» для отечественного и иностранного потребителя (фирмы «Ниссан», «Форд») и входящее в пятерку фирм, занимающих более 70% российского рынка противоугонных средств, столкнулось с проблемой подделки их товаров. При этом предприятию, кроме финансового ущерба (по поддельным гарантийным талонам завод вынужден заменять электронные компоненты), наносится удар по имиджу. Поэтому было принято решение повысить уровень защиты бумажных документов (накладных на электронные компоненты, паспортов на выпускаемую продукцию, гарантийных талонов) за счет введения нового реквизита, позволяющего производить идентификацию с ошибками не выше 5-ти процентного значения.

Актуальность темы исследования подтверждается необходимостью поиска нового метода идентификации бумажных документов и возможности его реализации.

Степень разработанности темы исследования. Во второй половине XX века благодаря исследованиям ученых (в частности, Томской школы под руководством проф. А.А. Воробьева) получила свое развитие высоковольтная электрофизика [38]. В.Д. Шкилевым [44] было предложено использовать

электрический разряд для создания невоспроизводимой метки в электрических и диэлектрических материалах.

До настоящего времени в нашей стране метод идентификации, использующий электрический разряд для создания невоспроизводимой метки, был недостаточно изучен. Не был разработан программно-аппаратный комплекс для осуществления процедуры распознавания метки при различных условиях получения ее фотографии. Поэтому тема диссертации посвящена исследованию возможности осуществления метода идентификации бумажных документов по невоспроизводимой метке, созданной стохастическим электроразрядным процессом, использующего программный продукт – автоматизированную систему идентификации.

Целью исследования является повышение надежности отражения атак модификации и копирования информации бумажных документов за счет применения нового метода их идентификации, основанного на разнородных защитных технологиях, который позволит устанавливать подлинность документа с ошибками идентификации, не превышающими 5%-ный уровень.

Научная задача заключается в разработке модельно-методического аппарата для идентификации документа по дополнительному реквизиту – невоспроизводимой электроразрядной метке и коду документа-оригинала для повышения защищенности информации бумажных документов.

Для достижения поставленной цели в диссертации решены следующие **задачи**:

1. Теоретическое исследование существующих методов идентификации.
2. Разработка методики определения угроз безопасности информации бумажного документооборота и оценка защищенности информации бумажных документов.
3. Разработка технологии электроразрядного нанесения индивидуальной невоспроизводимой метки на бумажном носителе и выбор

средства кодирования идентификационных признаков метки для идентификации информации кода с изображением метки.

4. Разработка автоматизированной системы идентификации бумажных документов по стохастически нанесенной метке и QR-коду.

5. Экспериментальные исследования защищенности бумажных документов от подделки.

Объектом исследования являются системы защиты информации бумажных документов.

Предметом исследования являются модели, методики и алгоритмы для идентификации документа по невоспроизводимой электроразрядной метке и коду документа-оригинала.

Научная новизна результатов работы:

1. В отличие от существующих методик определения угроз безопасности информации в информационных системах, не решающих вопросы защиты системы бумажного документооборота, разработана методика, по которой составлена модель угроз безопасности информации бумажного документооборота и произведена оценка риска их реализации.

2. В отличие от существующих воспроизводимых реквизитов бумажных документов впервые применена невоспроизводимая метка, нанесенная на документ стохастическим лавинно-стримерным разрядом при рассчитанных режимах работы электроразрядной установки, что обеспечивает множество каналов разрушения, характерные признаки которых служат идентификаторами и определяются разработанной автоматизированной системой. Ранее электрический разряд в системе бумажного документооборота не использовался.

3. В отличие от существующих методов идентификации бумажных документов в разработанном методе применена процедура кодирования значений идентификационных признаков метки в виде нанесенного рядом с меткой QR-кода, что позволило при невоспроизводимости метки производить

сравнение ее признаков с информацией QR-кода документа-подлинника и тем самым обеспечить его уникальность.

Теоретическая значимость работы:

1. Разработанная методика определения угроз безопасности информации системы бумажного документооборота может быть дополнена с учетом специфики работы предприятий и организаций.

2. Разработанные технологии определения режимов электроразрядного нанесения метки и выявления ее идентификаторов автоматизированной системой при их дальнейшем развитии могут быть применены при нанесении меток на металлические и неметаллические объекты.

3. Разработанные алгоритмы кодирования информации и ее распознавания в виде автоматизированной информационной системы при их дальнейшем развитии могут быть применены к идентификации металлических и неметаллических объектов.

Практическая значимость работы состоит в следующем:

Разработанная методика определения угроз безопасности может быть применена в системе бумажного документооборота предприятий и организаций для повышения защищенности информации документов.

Предлагаемый метод идентификации, основанный на сравнении информации QR-кода и метки, нанесенной электрическим разрядом, с помощью автоматизированной информационной системы, может быть использован:

1. в системе бумажного документооборота предприятий и организаций: метка может быть нанесена на сопроводительные документы на выпускаемую продукцию;

2. в банковской сфере: при идентификации ценных бумаг – сертификатов, денежных купюр;

3. при идентификации документов об образовании, профессиональной деятельности и т.д.

По результатам работы получены два патента на изобретения.

Методология и методы исследования. В диссертации применены методы системного анализа, теории моделирования, компьютерной графики, электротехники.

Положения, выносимые на защиту:

1. Разработанная методика определения угроз безопасности информации бумажного документооборота позволяет на основе модели угроз произвести оценку защищенности информации бумажных документов и разработать сценарии дальнейшего развития событий.

2. Предложенные в работе режимы электроразрядного нанесения метки обеспечивают ее невоспроизводимость в силу стохастичности процесса и информативность из-за множества каналов разрушения, идентификационные признаки которых позволит выявлять разработанная автоматизированная система.

3. Предложенная автоматизированная система, реализующая разработанный метод идентификации, позволяет произвести кодирование и нанесение выявленных идентификаторов метки в виде QR-кода на документ для выделения его из множества подобных.

Степень достоверности научных положений и выводов, сформулированных в исследовании, подтверждается их внутренней непротиворечивостью и адекватностью физическим представлениям об исследуемом объекте, проведением экспериментальных проверок, внедрениями, выступлениями на всероссийских конференциях и публикацией результатов работы в ведущих рецензируемых изданиях.

Апробация работы. Основные результаты проделанной работы были доложены на Международном семинаре «Передовые технологии в аэрокосмической отрасли, машиностроении и автоматизации» (MIST: Aerospace-2018), научно-методических семинарах в КФ МГТУ им. Н.Э. Баумана (2016-2019 гг.), на конкурсе инновационных проектов «Startup tour»,

проходившем в г. Туле в 2016 г., на Всероссийских научно-технических конференциях «Наукоемкие технологии в приборо- и машиностроении и развитие инновационной деятельности в вузе» (МГТУ им. Н.Э. Баумана, 2015, 2016 гг.).

Публикации. Основное содержание диссертации представлено в 15 печатных работах, в том числе 3 из них – индексируемые в международных базах цитирования Scopus и Web of Science, 5 – в изданиях, входящих в перечень ВАК, 2 патента на изобретение.

Внедрение результатов работы. Полученные основные научные результаты диссертационного исследования внедрены в бумажный документооборот ООО НПО «Телеметрия» (г. Калуга), ООО «Терекс Авто» (Калужская обл., п. Товарково).

Структура и объем работы. Диссертация состоит из введения, четырех глав, заключения и библиографии. Содержит 167 страниц основного текста, 25 таблиц, 66 рисунков и список использованной литературы из 113 источников.

В **первой главе** рассмотрены научные основы идентификации объектов (продукции, услуги, бумажных документов, информации). Даны понятия функций, задач и методов идентификации. В результате теоретического исследования существующих способов идентификации подтверждена необходимость применения метода идентификации по дополнительному реквизиту бумажного документа – стохастической невоспроизводимой метки и коду метки документа-подлинника для повышения защищенности информации.

Во **второй главе** разработана методика определения угроз безопасности информации бумажного документооборота, на основе которой произведено обоснование необходимости применения идентификации бумажного документа по дополнительному реквизиту и его коду: выявлены актуальные угрозы безопасности информации бумажного документооборота; составлена модель угроз; расчетным путем обнаружено снижение риска реализации угроз фальсификации бумажного документа.

В **третьей главе** проведен анализ физической сущности электроразрядного процесса с целью непосредственного получения уникальных меток на бумажном носителе и произведен выбор средства кодирования информации о признаках метки. Для доказательства невоспроизводимого характера наносимых меток проделано исследование процесса электрического разряда в межэлектродном промежутке между мишенью метки и инструментом-электродом.

В **четвертой главе** для идентификации бумажного документа по невоспроизводимой метке, полученной электроразрядным способом разработана автоматизированная система в программной среде Visual Studio 2010, язык программирования C#. На основе разработанной модели обработки изображений метки, кодирования и распознавания информации создана система идентификации, обеспечивающая полностью автоматизированный режим работы. Автоматизированная система позволяет произвести обработку изображения метки, выявление ее идентификаторов, кодирование информации метки и важных данных документа, нанесение QR-кода на поверхности документа и идентификацию изображения метки на основе сравнения ее с QR-кодом документа-подлинника.

В **пятой главе** проведены экспериментальные исследования и анализ работы автоматизированной системы идентификации бумажных документов по стохастически нанесенной электроразрядной метке и QR-коду, содержащему информацию документа-подлинника. Фотографии меток получены в условиях различной освещенности, после длительного срока эксплуатации бумажного носителя. Проведено определение вероятности ошибок идентификации первого и второго рода. Подтверждено повышение защищенности информации бумажного документа: отсутствие принятия информационной системой изображения «чужой» метки за метку-оригинал. Информация о волновом характере распределения отверстий метки также может служить идентификатором и закодирована в QR-коде.

1 ЗАДАЧА ОБЕСПЕЧЕНИЯ ИДЕНТИФИКАЦИИ ОБЪЕКТОВ

1.1 Научные основы идентификации объектов

Бумажные документы, в том числе сопроводительные документы на продукцию, ценные бумаги, удостоверения личности, документы об образовании и квалификации весьма распространены и имеют большое значение в жизни и деятельности людей. Организация движения потоков документов, начиная с этапа их создания/получения (пункты технической обработки – машинописные бюро, копировально-множительная служба), прохождения пунктов обработки информации (руководители, структурные подразделения, отдельные исполнители) до этапа отправления документов в архив или за пределы учреждения, называется бумажным документооборотом. Несмотря на широкое внедрение электронного документооборота, в будущем сфера влияния бумажных документов сохранит свой масштаб.

Сопроводительные документы на выпускаемую продукцию, сертификаты, документы об образовании, профессиональной деятельности и т.д. содержат конфиденциальную информацию, ограниченного доступа [1, 2]. Эта информация нуждается в защите от «неправомерного модифицирования, копирования» [1-4]. Средствами защиты могут служить «техническое, программное, программно-техническое средство, вещество и (или) материал» [5]. Для идентификации документов – проведения процедуры выявления их тождественности по совокупности характерных признаков (идентификаторов) – предназначены «реквизиты, позволяющие ее идентифицировать» [6].

Существующие правила идентификации бумажных документов по «наименованию и коду организации, наименованию и коду формы документа,

дате, регистрационному номеру документа, подписи, печати, грифам согласования и утверждения» [7] при современном уровне развития компьютерной техники и технологий не могут обеспечить защиту бумажных документов от угроз их фальсификации. Существующие способы защиты документов – водяные знаки, голограммы, штрихкоды не дают положительного результата, так как эти признаки воспроизводимы.

Отсутствие надежного метода идентификации бумажных документов приводит к распространению фальсифицированных товаров: по результатам анализа рынка охранных систем [8], 20% автосигнализаций являются контрафактом и распространяются по поддельным накладным. С каждым годом подделок становится больше, так как их выявление производится только при случайном обнаружении сайтов с объявлениями о продажах представителями фирм-производителей автосигнализаций-подлинников. ООО НПО «Телеметрия», выпускающее противоугонную автомобильную электронику под брендом «Pandora» для отечественного и иностранного потребителя (фирмы «Ниссан», «Форд») и входящее в пятерку фирм, занимающих более 70% российского рынка противоугонных средств, столкнулось с проблемой подделки их товаров. При этом предприятию, кроме финансового ущерба (по поддельным гарантийным талонам завод вынужден заменять электронные компоненты), наносится удар по имиджу.

Случаи фальсификаций документов, удостоверяющих личность человека, тоже нередки. При этом полученная копия может быть выполнена на таком высоком уровне качества, что ее невозможно отличить от оригинала.

Таким образом, научная задача диссертационного исследования заключается в разработке программно-аппаратного комплекса для идентификации документа по дополнительному реквизиту – невоспроизводимой метке, наносимой стохастическим процессом на документ, и коду документа-оригинала для повышения защищенности информации бумажных документов. Поставленная задача не является тривиальной, для ее

решения необходимо выбрать способ нанесения метки на бумажный документ и разработать программно-аппаратный комплекс, включающий в себя:

- установку, с помощью которой будет нанесена уникальная метка, природа которой зависит от характера физического процесса;
- алгоритмы обработки изображения метки, кодирования информации ее характерных признаков и сравнения этих признаков с информацией метки.

Для обоснованного выбора способа нанесения метки и определения ее характерных признаков необходимо провести теоретическое исследование научных основ идентификации объектов, анализ существующих методов идентификации, выявить их положительные и отрицательные стороны.

На основании полученных результатов исследования необходимо приступить к выбору метода нанесения метки и изучению его физических основ. Для создания установки, позволяющей обеспечить информативный характер метки, следовательно, и надежность идентификации, необходимо произвести расчет параметров установки с целью получения уникальной метки.

На основании полученной информации метки необходимо провести исследования по выбору ее характерных признаков и средства их кодирования.

Затем следует разработать алгоритмы обработки изображения метки, кодирования информации ее характерных признаков и сравнения этих признаков с информацией метки. Для подтверждения надежности и достоверности разработанного метода идентификации необходимо провести экспериментальные исследования.

Обеспечение технической и информационной совместимости является одной из главных целей стандартизации [9]. Эта совместимость необходима для осуществления информационного взаимодействия между многочисленными участниками процесса производства. В настоящее время в условиях развивающихся компьютерных систем и информационных технологий решение задачи информационной совместимости становится особенно актуальным.

«Каждый объект … обладает набором признаков, определяющих его сущность и, благодаря этому, выделяющих его из множества других, часто очень похожих объектов» [10].

Для идентификации объекта по его отображениям, то есть для признания тождественности неизвестного объекта известному на основании совпадения признаков предназначен процесс идентификации. Идентификация – «установление тождественности характеристик продукции ее существенным признакам» [9]. Объекту присваивается уникальный знак, наименование, номер, условное обозначение, признак или набор признаков для его однозначного определения из множества других объектов [11].

Особенно это важно при решении задач государственного контроля и обеспечения финансовой дисциплины. Процесс идентификации также имеет большое значение для материально-технического обеспечения производства, когда нужно знать информацию об определенных марках, сортаментах, моделях, типах исполнения продукции.

При этом в качестве объектов могут выступать продукция; услуги; ценные бумаги; информация и др. [11].

Функции идентификации подразделяются на группы [12]:

- указующая, осуществляющая отождествление объекта с конкретным наименованием, типом, маркой, сортом, партией товаров;
- информационная – служащая для доведения необходимой информации до субъектов рыночных отношений;
- подтверждающая подлинность объекта, то есть соответствие его характеристики той информации, которая содержится в товарно-сопроводительных документах или указана на маркировке;
- управляющая, являющаяся одним из элементов системы качества продукции.

Идентификация позволяет решить следующие задачи:

- «однозначное определение объекта;

- распознавание объекта по его свойствам;
- группирование объектов по определенным признакам;
- выделение объекта из множества подобных и др.» [10]

Для осуществления процесса идентификации необходимо выбрать основные (несколько или один) признаки (знак, метку, свойство и т.д.). Признак – это объективное отражение свойств объекта. Для преобразования признака в идентификатор необходимо соблюсти ряд требований. Он должен обладать следующими свойствами [13]:

- индивидуальностью. Оригинальность признака означает его нетипичность, отклонение от средних величин и норм. Чем он оригинальнее, тем неопровержимее подтверждает тождество объекта;
- относительной устойчивостью – сохранением свойств (признаков) индивидуального объекта в течение длительного периода;
- достаточностью – способностью передавать информацию об объекте в полном объеме;
- отображаемостью – способностью запечатлевать в идентифицируемых объектах достаточную совокупность признаков для осуществления выводов;
- воспроизводимостью признаков – способностью к систематическому адекватному отображению. Отображение признака, воспроизводимого в каждом случае образования следа должно однозначно передавать информацию о свойствах объекта;
- выраженностью признаков – способностью доказать свое наличие.

К средствам идентификации объектов относят:

- нормативные документы (стандарт, технические условия, правила). Они регламентируют показатели качества и могут быть использованы для целей идентификации,
- технические документы, в том числе товарно-сопроводительные (сертификаты, накладные, удостоверения качества);

- маркировка, содержащая всю информацию об объекте и которую можно использовать для идентификации (наименование, вид, сорт товара, химический состав, сырье и т.д.). Штриховое кодирование относится к информационным средствам идентификации.

В таблице 1.1 приведены средства идентификации продукции, применяемые на основных этапах ее производства [14].

Процесс идентификации проходит в три этапа [15]:

1) «на этапе раздельного исследования … выделяется совокупность идентификационных признаков;

2) в ходе сравнительного исследования производится сопоставление … признаков каждого из объектов, установление среди них совпадений и различий …;

3) … оценка полученных результатов» [13].

Иногда проводят процесс предварительного исследования: проверку наличия материалов для проведения исследования и правильности их оформления; оценку их пригодности для решения поставленной задачи.

Совокупность определенного на первом этапе необходимого набора идентификаторов должна быть достаточной для проведения последующего исследования.

Идентификационные признаки могут быть изучены по отображениям объекта или по образцам, созданным в условиях, максимально приближенных к условиям получения идентифицируемого объекта.

На второй стадии идентификации для проведения сравнительного микроскопического исследования широко применяются научно-технические средства, различные измерительные приборы, фотографические методы, координационные сетки, методы совмещения изображений, наложения и др.

Таблица 1.1 – Средства идентификации, применяемые на различных этапах производства продукции [11]

Основные этапы производства продукции	**Объект идентификации**	**Средство идентификации**	**Носитель информации об идентификации**
Заключение контракта	Требования к качеству продукции	Регламентирование требований к качеству продукции	Технические условия, спецификации
Проектирование и разработка продукции	Конструкторская и технологическая документация	Кодирование документации	Кодовое обозначение каждого конструкторского и технологического документа
Закупки	Сырье, материалы, комплектующие	Маркирование, кодирование, этикетирование закупленной продукции	Товаросопроводительная документация на продукцию. Торговая марка предприятия. Штрих-код товара. Протокол входного контроля
Метрологическое обеспечение производства	Маркирование, калибровка, аттестация, юстировка средств измерений	Свидетельство, паспорт, акт, разрешение на использование средства измерения	Штамп, поверительное клеймо, пломба, идентификационный номер средства измерения
Контроль качества продукции	Качество деталей, сборочных единиц, готовой продукции	Маркирование, клеймение, этикетирование продукции	Протокол контроля (испытаний). Протокол о несоответствии

Продолжение табл. 1

Основные этапы производства продукции	**Объект идентификации**	**Средство идентификации**	**Носитель информации об идентификации**
Послепроизводственные операции	Погрузочно-разгрузочные работы, упаковка, хранение, отгрузка	Товаросопроводительная документация, маркирование, этикетирование, штриховое кодирование	Номер партии, номер контракта, число, поставщик, маркировка, получатель, место назначения, сертификат и знак соответствия, паспорт, информационная этикетка, штрих-код
Эксплуатация (применение) продукции	Качество продукции при эксплуатации	Маркирование, кодирование	Рекламация, квитанция о гарантийном ремонте, классификатор отказов, анкета для опроса потребителей

Оценка полученных результатов является самым ответственным этапом идентификационного исследования. Идентификационные признаки, совпадающие и различающиеся, оцениваются с позиции их значимости. При этом необходимо определить идентификационную значимость, устойчивость, независимость каждого различающегося признака от естественных изменений состояния идентифицируемого объекта, воздействия факторов его эксплуатации. В случае заключения о несущественном характере различающихся идентификаторов переходят к анализу совокупности совпадающих признаков. Если последние могут повториться, то

сопоставленные объекты схожи. Только на основании индивидуальной (неповторимой) совокупности идентификаторов закономерен вывод о тождестве.

При значительном объеме совпадающих признаков делается заключение о тождестве сопоставленных объектов. В противном случае, при одновременно значимой совокупности различающихся признаков, говорят об отрицательном результате исследования [15].

Заключение экспертного идентификационного исследования может носить категорический (устанавливающий тождество или различие объектов) или вероятностный характер. Вероятностные выводы экспертов могут быть вызваны несовершенством используемых экспертных методик, слабой опорой на количественные характеристики идентификационных признаков.

Для признания тождественности неизвестного объекта известному необходим выбор метода идентификации.

1.2 Анализ существующих методов идентификации объектов

Идентификация объекта предусматривает сбор информации об его характерных признаках. Объем собираемой информации зависит от характера поставленной задачи [9].

Минимально достаточный для идентификации изделия объем информации «включает наименование изделия, его условное обозначение или код и номер, обозначение нормативного или технического документа, определяющего характеристики данного изделия» [9].

В качестве дополнительной информации производится сбор данных о физических и эксплуатационных характеристиках объекта.

Среди существующих методов идентификации наиболее известны методы: «наименований; цифровых номеров; классификационный; условных обозначений; ссылочный; описательный; описательно-ссылочный; автоматической идентификации; биометрии» [9].

Для идентификации объекта при использовании метода наименований новому объекту необходимо присвоить наименование и дать его определение. Для однозначного восприятия информации разработаны стандарты на термины и определения различных объектов.

Преимущество метода – «близость к естественному разговорному языку, основной же недостаток – большое число знаков, используемых для идентификации конкретных объектов» [9].

Областью применения классификационного метода является идентификация группы однородных объектов. «Преимущество этого метода состоит в его информативности, так как позволяет из множества выделять необходимые объекты, обладающие определенными признаками» [9]. По присвоенному коду происходит полная идентификация в пределах конкретного классификатора. Комбинирование данного метода с другими способами идентификации объясняет его широкую распространенность во многих областях деятельности. Известны две разновидности классификационного метода [17]:

- иерархический способ идентификации объектов;
- фасетный способ идентификации объектов.

В основе иерархического способа разделения совокупности объектов на подмножества заложен принцип от общего к частному. Каждая соподчиненная подгруппа содержит объекты, объединенные по характерному признаку. «Недостатком метода является малая гибкость ее структуры, обусловленная фиксированностью признаков (оснований деления) и заранее установленным порядком их следования» [9]. Кроме того, в ряде случаев применение данного способа идентификации весьма затруднено из-за невозможности группирования объектов по сочетанию требуемого ряда признаков при решении конкретных задач.

Для устранения этого недостатка применяется фасетный способ классификации. В данном способе заложен принцип от частного к общему: на

основе ряда характерных признаков происходит разбиение объектов на подгруппы. Гибкость этой классификации позволяет «систематизировать объекты по необходимому набору признаков и осуществлять информационный поиск по любому сочетанию фасетов» [9].

Использование для идентификации метода цифровых номеров подразумевает, что новому объекту, кроме его наименования, необходимо присвоить цифровой номер [16]. «В сочетании с наименованием объекта его номер позволяет однозначно идентифицировать объект» [9].

В качестве разновидностей метода цифровых номеров служат порядковый и серийно-порядковый способы идентификации объектов.

Применение первой разновидности способа характерно в случае присвоения порядкового номера объекту при его появлении на основе существующего порядка. «Недостатком идентификации объектов через порядковые номера является их неинформативность, т.е. отсутствие каких-либо признаков, характеризующих объекты» [9].

Серийно-порядковый способ идентификации объектов, хотя и предусматривает дополнительную привязку к серии (например, при обозначении места проведения лекции в высшем учебном заведении происходит привязка номера аудитории к номеру корпуса), незначительно снижает неинформативность метода цифровых номеров.

Другим известным методом, использующимся при идентификации документов и продукции, является метод условных обозначений [17]. При этом применяются две его разновидности:

- мнемонический способ, с помощью которого происходит идентификация металлов и сплавов. Условный код изделия при его прочтении позволяет получить необходимые данные;
- классификационно-нумерационный способ применяется при идентификации документов на группу изделий (ТУ – технические условия и далее обозначение кода).

Следующий метод идентификации – ссылочный – подразумевает нахождение описания свойств изделия по приведенному поблизости от его наименования обозначению номера стандарта [17]. «При использовании ссылочного метода остаются не раскрытыми основные характеристики и особенности продукции» [9].

Другой метод идентификации – описательный – предлагает для отождествления объекта воспользоваться описанием его свойств. Применяется в медицине, криминалистике, геологии. «Описание объектов представлено, как правило, в нормативных и технических документах, содержащих основные показатели, свойства, характеристики, размеры, условия использования, область применения и т.п.» [9].

Областью применения описательно-ссылочного метода является идентификация продукции по ее свойствам (достаточно семи) со ссылкой на каталог [17].

Широко распространенным методом идентификации является метод автоматической (бесконтактной) идентификации, подразумевающий отказ от применения клавиатуры в процессе сбора данных [18, 19]. Это объясняется развитием электроники и созданием средств, обеспечивающих восприятие (сканирование), распознавание и обработку информации об объектах [17]. «Для автоматической идентификации используются, например, штриховые коды, радиоэтикетки, магнитные полосы, смарт-карты, звуки и сигналы, оптически распознаваемые знаки и др.» [9]. Преимуществами этих технологий являются быстрота и точность получения информации.

Технологии штрихового кодирования широко применяются при решении задач идентификации объектов. Коды представляют собой графическое изображение букв, цифр и различных знаков. Штриховое кодирование применяется для идентификации в следующих областях деятельности [17]:

- промышленное производство (идентификация готовой продукции, сборочных единиц в автостроении и электронике);

- оптовая и розничная торговля (идентификация товаров, включая печатные издания и лекарственные средства);
- транспорт и почта (идентификация грузов, почтовых отправлений, сообщений в товаросопроводительной документации, проездных документов и багажа и т.п.);
- медицина (идентификация продуктов крови, доноров, пациентов, историй болезни, больничного белья и т.д.);
- библиотечное и архивное дело (идентификация единиц и мест хранения, пользователей);
- складское хозяйство (идентификация единиц и мест хранения, поставщиков и получателей, сообщений в складской документации и пр.);
- делопроизводство (идентификация пользователей, информация о личном составе, идентификация, а также представление в виде штрихов текста документа или его аннотации).

Технология штрихового кодирования подразумевает идентификацию объекта с помощью «присвоения ему цифрового, буквенного или буквенно-цифрового кода, представление кода в виде штрихов с использованием определенной символики, нанесение штрихового кода на физические носители (товар, тару, упаковку, этикетки, документы), считывание штриховых кодов, декодирование штриховых кодов в машинные представления буквенных, цифровых или буквенно-цифровых данных и передача их в компьютер» [19].

Линейные штриховые коды, состоящие из темных штрихов и светлых пробелов между ними, могут содержать от 15 до 50 символов, подразумевают считывание информации в одном направлении – по горизонтали.

Для считывания информации с маркировки и передачи полученных данных на ПК (персональный компьютер), POS-терминал, ноутбук или кассовый аппарат применяют сканер, представляющий собой электронное устройство компактных размеров. Современный считыватель штрихкодов способен работать с кодами любых форматов. Наиболее популярными из них

являются: EAN-13 для шифрования крупногабаритных товаров (последняя цифра кода является контрольным числом, получаемым в результате вычислений над имеющимися предыдущими цифрами по определенному алгоритму (рис. 1.1)), EAN-8 для маркировки небольших товаров, UPC A, UPC E, ITF, Code 39, Code 128, ISBN и пр. [20].

Двумерные штриховые коды предназначены для повышения количества кодируемой информации – до 2000 (в некоторых случаях до 4000) символов. Расшифровка кода происходит по горизонтали и вертикали – в двух измерениях. Различают два основных вида двумерных штриховых кодов: многорядные и матричные коды.

Единое информационное сообщение многорядного кода имеет форму прямоугольника, в котором данные, используя специальные механизмы сжатия (PDF417, MaxiCode, Data Matrix, Aztec Code), наносятся в виде нескольких строчек обычных одномерных штриховых кодов (рис. 1.2).

Рисунок 1.1 – Линейный штрихкод EAN-13 [21]

Матричные коды бывают квадратными, шестиугольными и круглыми по форме, основаны на позиционном расположении темных элементов одинакового размера внутри матрицы. Могут изготавливаться и гравировкой, штамповкой на металле, других материалах. Они более надежны по сравнению с многорядными кодами, что позволяет использовать их для маркировки уникальных сертификатов, документов, присвоения ключей.

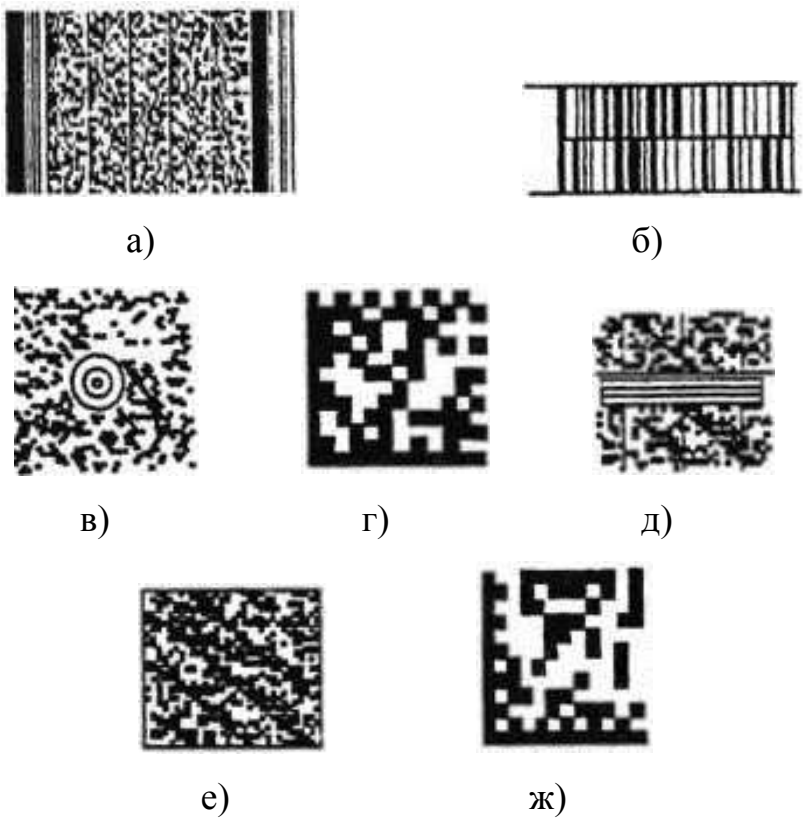


Рисунок 1.2 – Примеры двумерных штрихкодов: многорядные коды: а) PDF 417; б) Code 16K; матричные коды: в) Maxicode; г) Data Matrix; д) Code One; е) Vericode; ж) CP Code [22]

Считывать штриховые коды можно с помощью сканеров, терминалов сбора данных, мобильных телефонов со специальным установленным программным обеспечением (но с низкой производительностью).

В настоящее время распространены композитные символики, состоящие из линейного символа – ключевой информации для напечатанного над ним двумерного компонента (что позволяет существенно сократить его площадь) (рис. 1.3).

Рисунок 1.3 – Символ композитной символики [22]

Оборудование для штрихового кодирования должно выполнять следующие задачи: наносить штриховые коды; считывать их (штрихи хорошо

поглощают свет на определенных длинах волн, а фоновая поверхность хорошо его отражает, что и используется при оптическом считывании); собирать и накапливать данные; передавать их. Многие устройства выполняют несколько операций: электронные торговые весы, с помощью которых происходит взвешивание товара, печатание этикетки с нанесенным на нее штриховым кодом, ввод информации с клавиатуры, накопление данных и передача их через сеть.

Основной недостаток этого способа идентификации заключается в том, что штриховой код легко подделать.

Для определения происхождения объекта торговли или даты его изготовления применяют EPC – электронный код продукции (англ. Electronic Product Code) (рис. 1.4), хранящийся на радиочастотной метке – RFID (англ. Radio Frequency IDentification, радиочастотная идентификация) [23].

Рисунок 1.4 – Код EPC [24]

Радиочастотная идентификация является одним из способов автоматического сбора информации об объекте, местонахождении подвижных средств, животных, людей, имущества, документов, позволяет вести временной учет событий и получать информацию без вмешательства человека. Процесс осуществляется быстро и просто, с минимальным числом ошибок. Антенна радиометки улавливает радиосигнал малой мощности, испускаемый антенной устройства опроса/чтения. Этот сигнал запитывает микросхему (чип), встроенную в радиометку – RFID-метку. Далее происходит радиообмен между опросчиком и радиометкой для самоидентификации и передачи данных. поступает Контролирующий компьютер производит обработку полученной

информации и управление ею [25]. RFID-метки называют «умными этикетками» (smart labels) [26].

Данный способ идентификации имеет ряд недостатков:

- при частичном механическом повреждении метка теряет работоспособность;
- чувствительность к помехам электромагнитных полей;
- недостаточная открытость выработанных стандартов. Имеется тенденция скрывать от публики часть команд меток, в наиболее распространённых RFID-карточках может изначально содержаться закладка;
- высокая стоимость изготовления;
- низкий срок службы.

Кроме указанных недостатков, при оснащении денежных купюр RFID-метками возможно их отслеживание с помощью портативных сканеров ворами-карманниками.

Известны следующие карточные технологии (Card Technologies): технологии на основе магнитной полосы, смарт-карты, оптической карты.

Пластиковая карта с магнитной полосой имеет три дорожки: первая хранит информацию о владельце (до 76 знаков); во второй закодирован срок действия и номер карты (37 цифр); третья дорожка передает дополнительную информацию для персонализации и идентификации владельца карты, способна вместить до 104 цифровых символов. С помощью пластиковых карт можно проводить платежи, открывать сейфы и пропускные двери, пользоваться услугами, скидками или бонусами. Технология идентификации аналогична сканированию штрих-кода. Но при использовании карт применяется более дорогая технология, магнитная полоса ограничена по объему записанной на нее информации, трудно обеспечить надежность считывания и безопасность данных.

Этих недостатков лишена смарт-карта (чип карта, интегрированная карта размером с пластиковую кредитную карту). Пассивные смарт-карты содержат

только микросхему памяти для хранения информации, активные – кроме микросхемы памяти имеют микропроцессор, что делает возможным принятие решения о хранящейся информации и обеспечение различных методов для защиты доступа к информации. Но стоимость смарт-карт по сравнению с картами с магнитной полосой достаточно высока (в качестве материала проволоки от микросхемы к каждой из контактных площадок используется золото) [27].

Технология получения карт с оптической памятью (лазерных карт) основана на том же принципе, что и музыкальных дисков и CD-ROM: для хранения информации на карту прикрепляется лазерная панель (покрытая золотом), материал которой состоит из нескольких слоев и активизируется при попадании на слои лазерного луча. Лазер выжигает крошечное отверстие, его наличие означает «единицу», отсутствие – «ноль». Кроме текстовой информации можно записать графические, звуковые, программные файлы. Оптическая карта может хранить информацию объемом от 4 до 6,6 Мб, но данные на них могут быть записаны только один раз. Лазерные карты служат для хранения информации и создания банков данных в медицинских учреждениях, архивах и библиотеках. В банковских технологиях карты с оптической памятью не распространены из-за высокой стоимости карточек и считывающего оборудования.

Копии карт перечисленных видов могут быть выпущены не эмитентом похитившим заложенную в них информацию.

Биометрические технологии, основанные на измерении уникальных физиологических характеристик, способствуют идентификации живых объектов с помощью электронных приборов. Отсканированное с помощью биометрических систем изображение разных частей тела компьютер преобразует в математический цифровой код, который сравнивается с ранее сделанным кодом, хранящимся в базе данных. Биометрические технологии широко используется в случаях контроля доступа: в аэропортах, таможенных

зонах, госпиталях. «Основным критерием выбора метода является минимизация признаков, необходимых для решения задач, связанных с обработкой информации о конкретных объектах» [9].

Технологии машинного зрения наиболее распространены в медицине, биотехнологиях, военной отрасли, автомобильной промышленности. Они подразумевают преобразование данных, поступающих с устройств захвата изображения, с выполнением дальнейших операций на основе этих данных.

В систему машинного зрения входят подсистема формирования изображений; вычислительная система; алгоритмы анализа изображений [28]. В качестве первых двух компонент наиболее широко используют камеры и компьютеры. Но возможно применение «нестандартных» способов формирования изображений (использование иных, кроме видимого, спектральных диапазонов, когерентного излучения, структурированной подсветки, гиперспектральных приборов, времяпролетных, всенаправленных и быстродействующих камер, телескопов и микроскопов). Данные технологии используются лишь для распознавания и идентификации объектов и не подразумевают создания индивидуальных меток.

Использование криптографической защиты в виде нанесения на бумажные документы электронно-цифровой подписи (ЭЦП) производится не стохастическим образом, а созданием псевдослучайных величин при генерации кода. Следовательно, нельзя исключить возможность ее подделки. Кроме того, с помощью ЭЦП невозможно защитить бумажный документ от угрозы его копирования.

Все рассмотренные выше технологии либо характеризуются отсутствием создания индивидуальной метки для отдельного объекта (а не класса объектов), либо нанесенные метки может воспроизвести злоумышленник.

Поэтому необходима разработка нового метода идентификации, основывающегося на создании и использовании невоспроизводимых уникальных характеристик – меток, наносимых на бумажные документы.

Основное требование к метке – невозможность ее повторения на других носителях. По этой характеристике и должно осуществляться отождествление документа.

Основная сложность реализации метода заключается в том, что метка должна быть создана с помощью стохастического физического процесса, но в то же время должна надежно и повторяемо считываться.

1.3 Исследование способов идентификации, использующих стохастические физические процессы для создания индивидуальной метки объекта

Для проведения процедуры идентификации в нашей стране до недавнего времени использовались методы хроматографии или классической органической хромато-масс-спектрометрии [29]. Принцип их действия основан на определении наличия или отсутствия в объектах характерных компонентов-маркеров. Но при доступности приобретения маркеров, возможно их добавление или искусственное удаление не эмитентом.

Одним из стохастических способов идентификации является маркировка объекта источниками гамма-излучения, наносимыми непосредственно на него в виде опознавательного знака. Для распознавания объекта производится регистрация его радиоактивности. Для обеспечения достоверности и надежности этой процедуры предложено в качестве уникальной характеристики «используют смеси радиоактивных изотопов с различными периодами полураспада, варьируют их соотношения в опознавательном знаке так, что число распадов каждого изотопа составляет от 10^2 до 10^6 распадов в секунду, измеряют суммарное амплитудное распределение, которое является кодом объекта в момент времени его фиксации, заносят код и дату его фиксации в долговременную память и используют их для идентификации

объекта в любой момент времени с учетом изменения амплитудного распределения за счет частичного распада радиоактивных изотопов» [30].

В способе спектральной идентификации объектов материальных ресурсов используют два независимых метода получения спектральных характеристик: от объекта и от вносимой в объект метки, представляющей собой смесь изотопов. При этом смешивание производят по закону случайных чисел. Таким образом, можно получить неограниченное число невоспроизводимых различных меток. Информацию о двух спектральных характеристиках хранят в единой ячейке базы данных, характеризующих объект материального ресурса. Идентификацию осуществляют путем сличения спектральных характеристик, снятых как с объекта, так и метки, и сравнения их с эталонными, хранящимися в базе данных [31].

Главными недостатками изотопной идентификации являются:

- взаимодействие изотопной метки со средой, в результате которого ее состав в разные промежутки времени уже может не соответствовать эталонному значению;
- объект еще до осуществления процесса нанесения метки может содержать изотопы, что также приводит к отличным от эталонных результатов.

Таким образом, способ спектральной идентификации не обеспечивает надежного отождествления объекта.

Для создания уникальной метки возможно применение различных физических эффектов. Например, один эффект заключается в измерении характеристики магнитного отклика от нанесенных магнитных материалов. Уникальность магнитного отклика каждого образца объясняется наличием естественных дефектов в магнитном материале, которые образуются невоспроизводимым образом [32].

Для получения уникальной характеристики объекта другими исследователями предложено использовать эпоксидный маркер с вкрапленными стеклянными шариками. Положение шариков после

перемешивания фиксировано и для каждого объекта уникально [33, 34]. Когерентный пучок света, испускаемый лазером, направляется на маркер объекта, и в проходящем свете образуется спекл-структура. Идентификация производится путем измерения спекл-структуры детектором, расположенным определенным образом. Для повышения надежности процедуры отождествления объекта учеными предложено получение хешированного ключа. Для этого к маркеру прикреплялся кодированный идентификатор. При прохождении пучком света пути маркер – отражение от идентификатора – маркер происходило изменение шариками спекл-структуры, и получение уникального ключа.

В 1980-х годах американские ученые исследовали возможность защиты денежных купюр с помощью использования специальной бумаги с внедренными в нее мелкими частицами оптических волокон. Подразумевалось, что идентификация купюры будет производиться путем сравнения спекл-структуры, полученной от частиц волокон, и изображения ее эталона в виде штрихкода, нанесенного на купюре [35]. Но повышенная хрупкость частиц волокон не смогла обеспечить сохранность спекл-структуры. Поэтому данный метод идентификации не являлся достаточно надежным, и его не удалось внедрить.

Для выполнения соглашения по контролю над вооружениями был предложен метод идентификации, основанный на возможности придания уникальности поверхностям капитального оборудования, например, каждому стволу пушки, с помощью небольшого заряда взрывчатого вещества [36]. Измеренная спекл-структура хранилась в файле или прикреплялась к устройству в виде цифровой подписи.

Выше приведенные методы, основанные на использовании магнитных свойств или измерении спекл-структур, требуют применения специальных материалов и обеспечения стабильности проверяемой структуры в течение срока службы объекта. Применение каучукового маркера или магнитного чипа

в бумаге или картоне требует обеспечения условия его идеальной впечатываемости, что приведет к значительным затратам. Кроме того, при использовании прикрепляемых маркеров возможно отсоединение и прикрепление маркера к другому объекту.

В декабре 2014 года нидерландские ученые разработали метод аутентификации ключа на кредитных картах [37]. Для этого на поверхность карты помещался тонкий слой прозрачного материала с наночастицами, расположение которых для каждой карты индивидуально. При попадании на карту фотонов из считывающего устройства банкомата возникала световая картина, по которой можно судить о подлинности карты. Авторы метода, утверждая о невысокой стоимости и доступности указанной технологии, предлагают его использовать не только в защите банковских карт, но и в картах-пропусках, системах охраны банковских и государственных зданий и в автомобильных ключах.

К недостаткам метода можно отнести то, что он применим не для всех объектов, в частности, банкнот, ценных бумаг, требует наличия специального маркера, содержащего наночастицы, и дорогого устройства – лазера, испускающего импульсы когерентного света.

Во второй половине XX века благодаря исследованиям ученых (в частности, Томской школы под руководством проф. А.А. Воробьева) получила свое развитие высоковольтная электрофизика [38].

«Одним из эффективных методов физического воздействия на материалы … служит … электрический разряд… Он уже давно и успешно применяется в машиностроении, химико-технологических процессах, гидроакустике, горнодобывающих отраслях, нефтедобывающих производствах» [39], силовых процессах строительной индустрии. Электроразрядная механическая обработка представляет собой процесс удаления металла быстродействующей вспышкой разряда между электродами различной полярности, при этом один из электродов прикреплен к заготовке, другой – к инструменту (расстояние между

электродами находится в пределах от 0,013 до 0,9 мм (от 0,0005 до 0,035 дюйма)). Промежуток заполнен диэлектриком и металлическими частицами, которые в результате расплавления частично испаряются и удаляются из этого промежутка [40].

В 1960-е годы ученые предложили использовать электрический разряд для разрушения твердых материалов (горных пород). Для этого пробой материала производится при импульсном высоком напряжении. Способ примечателен тем, что можно управлять эффектом разрушения твердого диэлектрика. Для этого, например, изменением величины разрядного промежутка можно получить различную глубину проникновения разряда в материал [41]. «Искровой разряд в конденсированных средах используется как рабочий инструмент в технологиях:

- разрушения железобетонных сооружений и других крупногабаритов; дробления горных пород, твердых отходов, термопластов;

- измельчения растительного сырья;

- активации растворов для усиления экстракции;

- очистки трубопроводов и других изделий от твердых отложений, активации фильтрующих материалов;

- резания щелей, бурения скважин в скальных породах;

- получения нанопорошков металлов, их оксидов и нитридов, синтезируемых при разряде в парах электрически взрываемых проводников» [38].

В настоящее время широко используются процессы размерной электроразрядной обработки металлов, базирующиеся на преобразовании энергии электрических разрядов в тепловую энергию: электроискровая (электроимпульсная) обработка, электроконтактная обработка и анодно-механическая обработка, размерная обработка электрической дугой, плазменная обработка [42].

Шкилевым В.Д. было предложено использовать электрический разряд для создания невоспроизводимой метки в электрических и диэлектрических материалах. Действие электрического разряда носит стохастический характер, невозможно его попадание в определенную точку матрицы [43]. Поэтому каждый раз можно получать разнообразный набор пятен, а, следовательно, меток.

Для придания индивидуальности объекту было предложено наносить невоспроизводимую метку в пространстве между основным и индивидуальным штриховыми и цифровыми кодами (рис. 1.5) [44].

Два независимо функционирующих струйных принтера 3 и 4, расположенные под острым углом к бумаге, оставляют разноцветные, перпендикулярные по отношению друг к другу, следы. Третий принтер 2 наносит индивидуальные штриховые и цифровые коды параллельно основным штриховому и цифровому кодам (рис. 1.6).

В патенте [44] основная часть индивидуального цифрового кода генерируется случайным образом, тогда как последняя цифра кода получается в результате применения специального алгоритма.

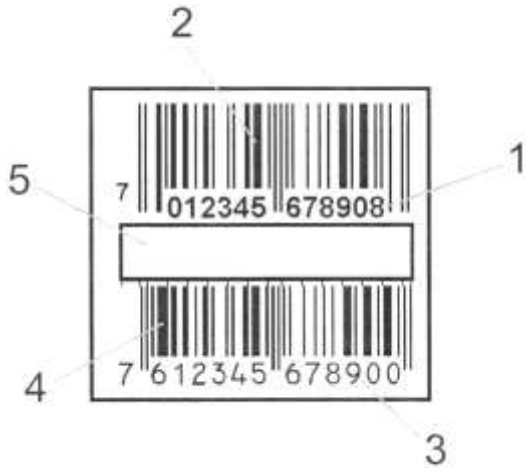


Рисунок 1.5 – Индивидуальный информационно защищенный штрих-код: 1 – основной цифровой код; 2 – штриховой код; 3 – индивидуальный цифровой код; 4 – индивидуальный штриховой код; 5 – невоспроизводимая картинка [44]

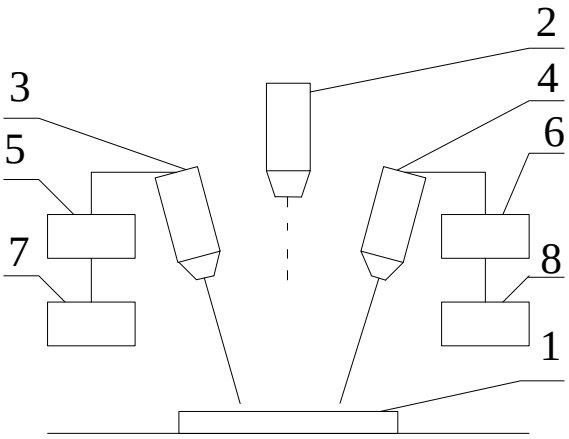


Рисунок 1.6 – Способ изготовления индивидуального штрих-кода: 2, 3, 4 – принтеры; 7, 8 – независимые блоки питания; 5, 6 – генераторы случайных чисел [44]

Невоспроизводимость картинки в пространстве 1 (рис. 1.6) объясняется наличием протяженных и уникальных наклонных следов от струйных принтеров 3 и 4 и перфораций, полученных электроразрядным методом. Наклонные следы невозможно воспроизвести не эмитенту из-за случайного характера нанесения и качества бумажного носителя: с помощью генераторов случайных чисел 5 и 6 стохастически изменяется наклон следов. Кроме того, наличие ворсистых участков бумаги способствует формированию более короткого следа, на гладком участке остается более протяженный след.

Изменение параметров электроразрядного метода производилось в следующих пределах (рис. 1.7):

энергия разряда 0,1 … 0,5 Дж,

напряжение на электродах 35 … 50 кВ,

расстояние между электродами 5 … 7 мм.

Место прожигания очередного микроскопического отверстия на бумаге предсказать невозможно, оно появляется случайным образом [45, 46].

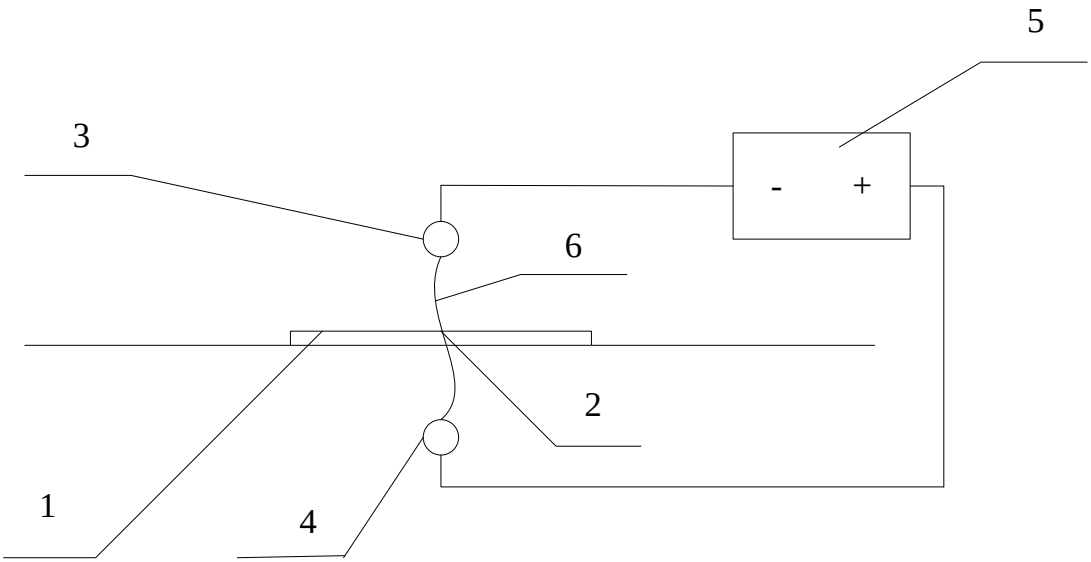


Рисунок 1.7 – Электроразрядный метод получения перфораций: 1 – невоспроизводимая картинка; 2 – перфорации; 3 и 4 – основной и дополнительный электроды соответственно; 5 – высоковольтный источник; 6 – плазменный шнур электрического разряда [44]

В настоящее время в нашей стране метод идентификации, использующий электрический разряд для создания невоспроизводимой метки, недостаточно изучен. Не разработан программно-аппаратный комплекс для осуществления процедуры распознавания образа – метки при различных условиях ее получения. Этот метод является уникальным, эффективным, не требует применения дорогостоящих оборудования и технологий.

На основе проделанного анализа существующих способов идентификации, в том числе использующих стохастические физические процессы, был выявлен метод, заслуживающий более пристального внимания для изучения и применения его на практике: идентификация диэлектрических объектов с использованием электрического разряда для создания невоспроизводимой метки.

Выводы по первой главе

1. Теоретическое исследование научной основы процесса идентификации показало, что на первом этапе проведения этой процедуры у объекта выявляется набор признаков, определяющих его сущность и выделяющих его из множества других объектов. Для преобразования признака в идентификатор он должен обладать свойствами: индивидуальностью; относительной устойчивостью; достаточностью; отображаемостью; воспроизводимостью; выраженностью признаков. При сравнительном исследовании (второй этап процесса идентификации) производится сопоставление выявленных идентификаторов каждого из объектов для установления совпадающих и различающихся признаков. Оценка полученных результатов является самым ответственным этапом идентификационного исследования. При значительном объеме совпадающих признаков делается заключение о тождестве сопоставленных объектов. В противном случае, при одновременно значимой совокупности различающихся признаков, говорят об отрицательном результате исследования.

2. Проведенный анализ существующих методов идентификации доказал отсутствие на сегодняшний момент технологии, позволяющей провести процедуру отождествления бумажных документов с высокой степенью надежности и точности. Все рассмотренные технологии либо характеризуются отсутствием создания индивидуальной метки для отдельного объекта (не класса объектов), невозможностью применения для отождествления бумажных документов, либо несложностью воспроизведения не эмитентом – лицом, не выпускающим оригиналы документов. В ходе анализа существующих методов идентификации, использующих стохастические физические процессы, самым эффективным является предложенный Шкилевым В.Д. метод создания уникальной невоспроизводимой метки на электрических и диэлектрических материалах. Метка наносится с помощью электрического разряда:

невозможность воспроизведения одной и той же метки сочетается со сравнительной простотой и низкой стоимостью технологии. Невозможность использования этого метода до настоящего времени заключалась в отсутствии программно-аппаратного комплекса, позволяющего произвести процедуру идентификации.

3. В ходе теоретического исследования был выявлен метод, заслуживающий более пристального внимания для изучения и применения его на практике: идентификация диэлектрических объектов с использованием электрического разряда для создания невоспроизводимой метки.

2 АНАЛИЗ ВОЗМОЖНОСТИ ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ БУМАЖНЫХ ДОКУМЕНТОВ ПРИ ИХ ИДЕНТИФИКАЦИИ ПО НОВОМУ РЕКВИЗИТУ

2.1 Классификация угроз безопасности информации бумажных документов

Угроза безопасности информации бумажных документов представляет собой «совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации» [5].

Классификация угроз информационной безопасности в зависимости от признака, заложенного в основу классификации, представлена в виде таблиц 2.1, 2.2 [47].

Табл. 2.1 – Классификация угроз безопасности информации по виду ее нарушаемого свойства

Угроза	Последствия
Нарушение конфиденциальности информации	Информация становится доступной пользователям, не располагающими полномочиями по ознакомлению с ней
Нарушение целостности информации	Искажение или модификация информации, потеря части данных
Нарушение доступности информации	Блокирование доступа к данным или выход из строя и сбоя функционирования технических средств и оборудования

Табл. 2.2 – Классификация угроз безопасности информации по природе возникновения

Угрозы, обусловленные человеческим фактором		Угрозы среды
случайные	преднамеренные	
Ошибки, связанные с проектированием системы защиты	Уничтожение, хищение, модификация, копирование информации – пассивные угрозы	Землетрясение
Ошибки работников при работе в системе	Незаконное получение учетных данных путем подкупа, шантажа	Наводнение
Ошибки в аппаратной платформе	Использование недекларированных возможностей средств защиты и программных закладок в программном обеспечении	Молния
Ошибки в установленном программном обеспечении	Отказ в обслуживании системы защиты	Пожар

Кроме того, существует классификация угроз в зависимости от их источника:

- внутренние угрозы – источник находится внутри контролируемой системы;
- внешние угрозы – источник за пределами системы.

Угрозы могут быть пассивными и активными. Пассивные угрозы не могут повлиять на состав и структуру системы. Активные угрозы оказывают воздействие на структурно-функциональные характеристики системы. Результатом реализации активных угроз может служить, например, отказ в обслуживании системы защиты.

2.2 Разработка модели угроз безопасности информации бумажного документооборота

Для защиты различных объектов необходимо определять и учитывать актуальные для них виды угроз. Каждая из этих угроз имеет свой уровень реализации: высокий, средний, низкий. При наличии определенного свойства объекта, обеспечивающего исполнение угрозы можно говорить об его уязвимости по отношению к этой угрозе. «Если уязвимость соответствует угрозе, то существует риск» [5]. Риск – «потенциальная опасность нанесения ущерба организации в результате реализации некоторой угрозы» [48].

Риск реализации угрозы $Р_{р.у.}$ определяется по формуле [49]:

$$Р_{р.у.} = В_{р.у.} \cdot У, \quad (2.1)$$

где $В_{р.у.}$ – вероятность или возможность (при отсутствии статистических данных) реализации угрозы, $У$ – степень причиненного ущерба (финансового, социального, политического, репутационного, технологического и др.) может быть низкой, средней, высокой.

Степень вероятности или возможности реализации угрозы определяется по таблице 2.3, может быть низкой, средней и высокой. При рассмотрении влияния на безопасность информации бумажных документов таких угроз внешней среды, как землетрясение и наводнение, вероятность их реализации можно считать низкой (значительно реже 1 раза в 5 лет). Возможности случаев возникновений пожара и последствий удара молнии в здание организации также характеризуются низкой степенью реализации. Поэтому в число актуальных угроз для организации они не входят.

Случайные ошибки в аппаратной платформе и в установленном программном обеспечении могут иметь среднюю степень вероятности реализации угрозы.

Ошибки, связанные с проектированием системы защиты даже случайного характера, наиболее опасны и могут привести к несанкционированному

доступу источника угроз к информации, не предназначенной для широкого круга лиц, и к ее разглашению, что может привести к высокой степени ущерба для организации (табл. 2.4).

Табл. 2.3 – Определение степени вероятности (возможности) реализации угрозы [49]

	Характеристика степени вероятности (возможности) реализации угрозы
Низкая	Отсутствуют объективные предпосылки к реализации угрозы безопасности информации, отсутствует требуемая статистика по фактам реализации этой угрозы (возникновения инцидентов безопасности), отсутствует мотивация для реализации угрозы, возможная частота реализации угрозы не превышает 1 раза в 5 лет
Средняя	Существуют предпосылки к реализации угрозы безопасности информации, зафиксированы случаи реализации этой угрозы (возникновения инцидентов безопасности) или имеется иная информация, указывающая на возможность реализации угрозы безопасности информации, существуют признаки наличия у нарушителя мотивации для реализации такой угрозы, возможная частота реализации угрозы не превышает 1 раза в год
Высокая	Существуют объективные предпосылки к реализации угрозы безопасности информации, существует достоверная статистика реализации этой угрозы безопасности информации (возникновения инцидентов безопасности) или имеется иная информация, указывающая на высокую возможность реализации угрозы безопасности информации, у нарушителя имеются мотивы для реализации угрозы, частота реализации угрозы – чаще 1 раза в год

Случайные ошибки работников могут привести к различного рода последствиям: к нарушению разрешительной системы доступа; неумышленному уничтожению информации, ее копированию; искажению

текста, модификации информации; разглашению ценных данных. Даже при низкой степени вероятности реализации этой угрозы организация может понести значительные убытки.

Табл. 2.4 – Определение степени возможного ущерба [49]

Степень ущерба	Характеристика степени ущерба
Высокая	В результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции
Средняя	В результате нарушения одного из свойств безопасности информации возможны умеренные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций
Низкая	В результате нарушения одного из свойств безопасности информации возможны незначительные негативные последствия. Информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств

В таблице 2.5 приведены виды и типы нарушителей (внешний злоумышленник – I тип нарушителя, внутренний – II тип нарушителя) в зависимости от их мотивации к совершению угроз безопасности информации. Преднамеренные действия по хищению, копированию, уничтожению и модификации информации могут быть совершены внешним злоумышленником

не только путем взлома системы защиты, но и путем подкупа, шантажа работников организации или добровольного сотрудничества.

Табл. 2.5 – Классификация видов нарушителей в зависимости от их мотивации [49]

№ вида	Виды нарушителя	Типы нарушителя	Возможные цели (мотивация) реализации угроз безопасности информации
1	Специальные службы иностранных государств (блоков государств)	Внешний, внутренний	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Дискредитация или дестабилизация деятельности органов государственной власти, организаций
2	Террористические, экстремистские группировки	Внешний	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Совершение террористических актов. Идеологические или политические мотивы. Дестабилизация деятельности органов государственной власти, организаций
3	Преступные группы (криминальные структуры)	Внешний	Причинение имущественногоущерба путем мошенничества или иным преступным путем. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды
4	Внешние субъекты (физические лица)	Внешний	Идеологические или политические мотивы. Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса).Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды
5	Конкурирующие организации	Внешний	Получение конкурентных преимуществ. Причинение имущественного ущерба путем обмана или злоупотребления доверием
6	Разработчики, производители, поставщики программных, технических и программно-технических средств	Внешний	Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки. Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия

Продолжение табл. 2.5

7	Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия
8	Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики)	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия
9	Пользователи информационной системы	Внутренний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия
10	Администраторы информационной системы и администраторы безопасности	Внешний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса).Месть за ранее совершенные действия. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Непреднамеренные, неосторожные или неквалифицированные действия
11	Бывшие работники (пользователи)	Внешний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Месть за ранее совершенные действия

Степень реализации угрозы хищения, копирования, уничтожения и модификации информации бумажных документов, как со стороны сотрудников организации, так и внешним злоумышленником, можно считать высокой (чаще одного раза в год), исходя из статистических данных в периодической печати.

Использование не декларированных возможностей средств защиты и отказ в обслуживании системы защиты приведут к возможности реализации угрозы несанкционированного доступа к конфиденциальной информации организации и к значительному для нее ущербу.

В зависимости от степени потенциала нарушители могут обладать разными возможностями реализации угроз (табл. 2.6), каждая из которых может быть оценена по формуле:

$$В_{р.у.} = (1 - У_з) \cdot П_н, \quad (2.2)$$

где $П_н$ – потенциал нарушителя, $У_з$ – уровень защищенности системы бумажного документооборота.

При разработке критериев уровня защищенности и системы бумажного документооборота в организации (табл. 2.7) руководствовались характеристиками защищенного документооборота и рекомендациями [49]:

- уровень защищенности бумажного документооборота может считаться высоким при соотнесении не менее 80% характеристик, указанных в таблице, к уровню «высокий» (0,8 и выше);
- средним – при соответствии не менее 90% характеристик уровню «средний» (0,6 и выше);
- низким – при несоблюдении первых пяти условий (менее 0,6).

Из формул (2.1) и (2.2) риск реализации угрозы можно оценить по формуле:

$$Р_{р.у.} = (1 - У_з) \cdot П_н \cdot У. \quad (2.3)$$

Табл. 2.6 – Возможности нарушителей в зависимости от их потенциала [49]

№	Потенциал нарушителей	Виды нарушителей	Возможности по реализации угроз безопасности информации
1	Нарушители с базовым (низким) потенциалом	Внешние субъекты (физические лица), лица, обеспечивающие функционирование информационных систем или обслуживающих инфраструктуру оператора, пользователи информационной системы, бывшие работники, лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных работ	Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы,опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему
2	Нарушители с базовым повышенным (средним) потенциалом	Террористические, экстремистские группировки, преступные группы (криминальные структуры), конкурирующие организации, разработчики, производители, поставщики программных, технических и программнотехнических средств, администраторы информационной системы и администраторы безопасности	Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы

Продолжение табл. 2.6

3	Нарушители с высоким потенциалом	Специальные службы иностранных государств (блоков государств)	Обладают всеми возможностями нарушителей с базовым и базовым повышенным потенциалами. Имеют возможность осуществлять несанкционированный доступ из выделенных (ведомственных, корпоративных) сетей связи, к которым возможен физический доступ (незащищенных организационными мерами). Имеют возможность получить доступ к программному обеспечению чипсетов (микро-программам), системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-техническим средствам информационной системы для преднамеренного внесения в них уязвимостей или программных закладок. Имеют хорошую осведомленность о мерах защиты информации, применяемых в информационной системе, об алгоритмах, аппаратных и программных средствах, используемых в информационной системе. Имеют возможность получить информацию об уязвимостях путем проведения специальных исследований (в том числе с привлечением специализированных научных организаций) и применения специально разработанных средств для анализа программного обеспечения. Имеют возможность создания методов и средств реализации угроз безопасности информации с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение в информационную систему и воздействие на нее. Имеют возможность создания и применения специальных технических средств для добывания информации,распространяющейся в виде физических полей или явлений

Табл. 2.7 – Определение уровня защищенности системы бумажного документооборота

Характеристики организации защиты бумажного документооборота	Уровень защищенности системы бумажного документооборота		
	Высокий	Средний	Низкий
Утвержден точный перечень конфиденциальных служебных бумаг и определен состав сведений, не подлежащих разглашению			
Внедрена обязательная аутентификация и использование средств ограничения доступа			
Учтены все операции в данной сфере			
Проводятся систематические проверки наличия, целостности и физического состояния ценной документации			
Положения о неразглашении сведений, относящихся к коммерческой тайне, включены в учредительную и организационную документацию, трудовые соглашения с персоналом и должностные инструкции			
Одновременное использование режимных (разрешительных, ограничительных) мер и технологических приемов, входящих в систему обработки и хранения конфиденциальных документов			
Нанесена отличительная отметка на чистый документ, в том числе сопроводительный, что позволяет выделить его в общем потоке документов			
Сформированы самостоятельные, изолированные потоки конфиденциальных документов и сделано их разделение на подпотоки в соответствии с уровнем конфиденциальности перемещаемых документов			
Используется автономная технологическая система обработки и хранения конфиденциальных документов, не соприкасающаяся с системой обработки открытых документов			
Регламентация движения документов как внутри фирмы, так и между фирмами, с момента создания документа и до передачи в архив			

Продолжение табл. 2.7

Организация самостоятельного подразделения конфиденциального делопроизводства (службы КД) или аналогичного подразделения, входящего (или не входящего) в состав службы безопасности			
Перемещение документов между руководителями, исполнителями и иным персоналом только через службу КД			

Потенциал нарушителя является функцией нескольких переменных [49]:

$$П_н = f(М, Т_з, К_т, З, В_д, О_н),$$

где М – уровень мотивации злоумышленника, $Т_з$ – затрачиваемое нарушителем время для идентификации и использования уязвимости системы, $К_т$ – техническая компетентность нарушителя, З – знание проекта и информационной системы (о системе защиты документооборота), $В_д$ – возможность доступа к информационной системе (системе документооборота), $О_н$ – оснащенность нарушителя для реализации угрозы.

Значение показателей возможностей нарушителя определяются по таблице 2.8, при этом необходимо учитывать, что:

1) Технической компетентности нарушителя присваивается значение «непрофессионал» при отсутствии необходимых знаний в области реализации угрозы; «специалист» осведомлен о мерах защиты информации; «профессионал», кроме того, обладает знаниями по выявлению новых уязвимостей системы защиты.

2) «Отсутствие знаний» о системе защиты объясняется невозможностью получения сведений о структурно-функциональных характеристиках системы (сведения доступны определенным сотрудникам); «ограниченные знания» соответствуют наличию эксплуатационной документации; «знание чувствительной информации» предполагает еще и наличие конструкторской документации.

Табл. 2.8 – Значения показателей возможностей нарушителя [49]

Показатель возможностей нарушителя		Значения при идентификации уязвимости	Значения при использовании уязвимости
Затрачиваемое время	< 0,5 час	0	0
	< 1 день	2	3
	< 1 месяц	3	5
	> 1 месяц	5	8
Техническая компетентность нарушителя	Непрофессионал	0	0
	Специалист	2	3
	Профессионал	5	4
Знание проекта и информационной системы	Отсутствие знаний	0	0
	Ограниченные знания	2	2
	Знание чувствительной информации	5	4
Возможность доступа к информационной системе	< 0,5 час или не обнаруживаемый доступ	0	0
	< 1 день	2	4
	< 1 месяц	3	6
	> 1 месяц	4	9
	Не возможно		
Оснащенность нарушителя	Отсутствует	0	0
	Стандартное оборудование	1	2
	Специализированное оборудование	3	4
	Оборудование, сделанное на заказ	5	6

3) Для реализации угрозы «стандартное оборудование» нарушитель может легко приобрести; «специализированное оборудование» потребует

небольших затрат; «оборудование, сделанное на заказ» является дорогостоящим и потребует больших временных затрат для приобретения.

Значения характеристик, приведенных в таблице 2.8, суммируются и по таблице 2.9 определяется уровень потенциала нарушителя. При наличии статистических данных о повышенной мотивации злоумышленников к реализации угрозы потенциал необходимо переводить на следующий, более высокий уровень по сравнению с первоначально определенным. При этом необходимо учитывать соотношение «затраты – выгода», т.е. рентабельность исполнения угрозы.

Табл. 2.9 – Потенциал нарушителя в зависимости от диапазона значений его характеристик [49]

Диапазон значений	Потенциал нарушителя
<10	Потенциал недостаточен для реализации угрозы безопасности
10-17	Базовый (низкий)
18-24	Базовый повышенный (средний)
>24	Высокий

Выделим актуальные угрозы безопасности информации бумажных документов, для этого применим соответствующие правила (табл. 2.10).

Табл. 2.10 – Правила определения актуальности угрозы [50]

Возможность реализации угрозы	Показатель опасности угрозы		
	низкая	средняя	высокая
низкая	неактуальная	неактуальная	актуальная
средняя	неактуальная	актуальная	актуальная
высокая	актуальная	актуальная	актуальная
очень высокая	актуальная	актуальная	актуальная

Можно считать, что угрозы среды (табл. 2.2) для информации бумажных документов не являются актуальными, эти явления природы спрогнозировать трудно и обеспечить их полное устранение невозможно.

Случайные ошибки сотрудников организации, выпускающих документы, при средней возможности их реализации и средней/высокой степени опасности, а также при низкой возможности реализации, но при высоком показателе опасности угрозы становятся актуальными.

Наибольшую угрозу несут действия злоумышленника, когда даже при низкой вероятности подкупа или шантажа сотрудника, но при высоком показателе опасности угрозы копирования, модификации, хищения, уничтожения бумажного документа становятся актуальными. При средней, высокой и очень высокой возможности реализации этих угроз их актуальность очевидна даже при среднем и низком показателях опасности. Показатели потенциала в случае повышенной мотивации к модификации и копированию документов приобретают значения:

1) затрачиваемое время – 3 (при идентификации уязвимости), 5 (при ее использовании);
2) профессионал – соответственно 5 и 4;
3) знание чувствительной информации – 5 и 4;
4) возможность доступа к системе защиты – 3 и 6;
5) стандартное оборудование – 3 и 4.

При их суммировании показывают высокий потенциал злоумышленника к совершению угрозы безопасности документа.

Для формирования мер защиты информации бумажных документов составляется модель угроз, исходящих от внешнего источника (злоумышленника) и внутреннего источника (сотрудник организации, выпускающей/хранящей документ) (рис. 2.1).

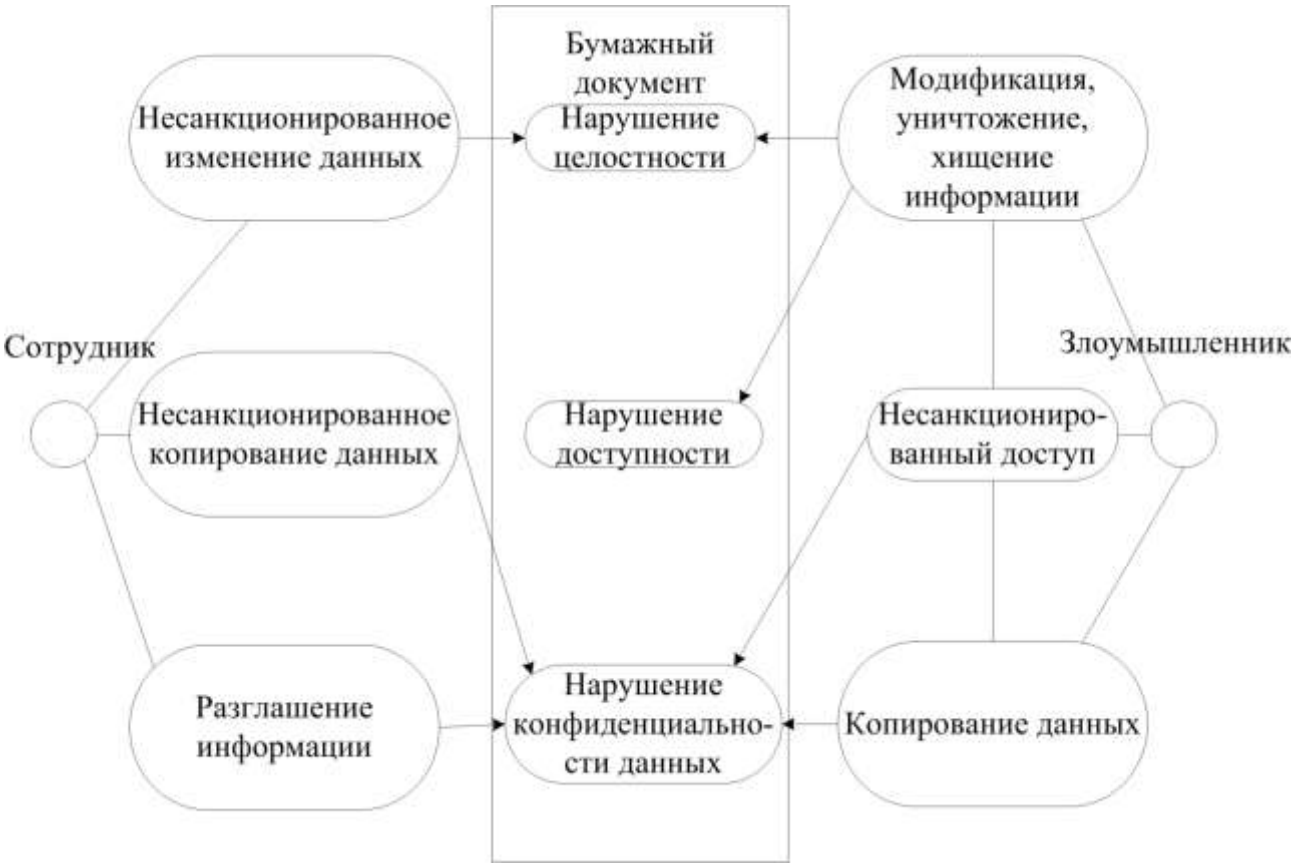


Рисунок 2.1 – Модель угроз безопасности информации бумажного документооборота

На основе анализа модели угроз можно сделать вывод, что для бумажных документов существует большой риск их модификации и копирования.

Существуют критерии, по которым можно судить о надежности защиты бумажных документов:

- «Защита должна определять нерентабельность подделки.
- Защита должна обеспечивать устойчивый однозначный контроль подлинности.
- Защитный комплекс должен действовать как в условиях контролируемого, так и неконтролируемого окружения.
- Применение защиты предполагает наличие надежной аппаратной базы контроля подлинности.
- Надежная защита обеспечивается совокупностью разнородных защитных технологий» [51].

В разрабатываемом методе идентификации предлагается использовать две разнородные технологии: стохастический электроразрядный процесс, позволяющий исключить возможность подделки метки, и нанесение кода, содержащего информацию метки документа-подлинника, при составлении которого можно внести изменения для затруднения дешифровки информации со стороны потенциального нарушителя. Тогда для защиты информации бумажных документов в организации необходимо предусмотреть, по меньшей мере, два независимо работающих подразделения, в одном из которых будет происходить нанесение электроразрядных меток на документы, в другом – будут работать пользователи со специальным программным обеспечением, позволяющим обрабатывать информацию метки и наносить код.

Показатели потенциала в момент внедрения нового метода приобретают значения:

1) затрачиваемое время – 0 (при идентификации уязвимости), 0 (при ее использовании) – в данный момент не может реализовать угрозу;
2) непрофессионал – соответственно 0 и 0;
3) отсутствие знаний – 0 и 0;
4) возможность доступа к системе защиты – 0 и 0;
5) отсутствие оборудования – 0 и 0.

Таким образом, потенциал нарушителя становится недостаточным для реализации угрозы, при этом уровень защищенности системы вырастает, тем самым обеспечивается снижение риска реализации угрозы (формула (2.3)).

Можно предположить следующие сценарии развития событий:

- нарушитель, имея повышенную мотивацию к модификации и копированию информации, приобретет высоковольтный источник, соберет электроразрядную установку, но ему также необходимо нанести код, содержащий информацию его новой метки, иначе проверку на идентификацию документ не пройдет. Значит, ему необходимо нанять программиста, затратив и

деньги, и время на декодирование, при этом его попытка может оказаться безуспешной;

- нарушитель будет пытаться путем подкупа, шантажа вступить в сговор с людьми, имеющими доступ к этим подразделениям. В этом случае необходимо обеспечить доведение до этих сотрудников правил работы с конфиденциальной информацией.

2.3 Оценка надежности идентификации бумажных документов на основе определения вероятности ошибок FRR и FAR

Для оценки надежности работы автоматизированной информационной системы необходимо определить вероятности ошибок идентификации первого (FRR – False Rejection Rate) и второго (FAR – False Acceptance Rate) рода. Ошибки первого рода появляются в тех случаях, когда при сравнении изображений одной и той же метки система ошибочно принимает их за «чужую» метку. Ошибки второго рода возникают при принятии системой «чужой» метки за метку подлинного документа [52].

На рисунке 2.2 изображен граф переходов документа Д из одного состояния в другое – от простановки метки и QR-кода до потребителя, где происходит процесс идентификации документа.

Рассмотрим подробнее переходы документа в разные состояния. Вероятность того, что метка М нанесена на документ эмитентом и является истинной, обозначим $P_{\text{М}_\text{и}}$. При предположении, что злоумышленник может также нанести метку своим техническим устройством, появляется вероятность возникновения на документе фальшивой метки – $P_{\text{М}_\text{ф}}$. При нанесении QR кода по информации метки на документ возможны также различные состояния:

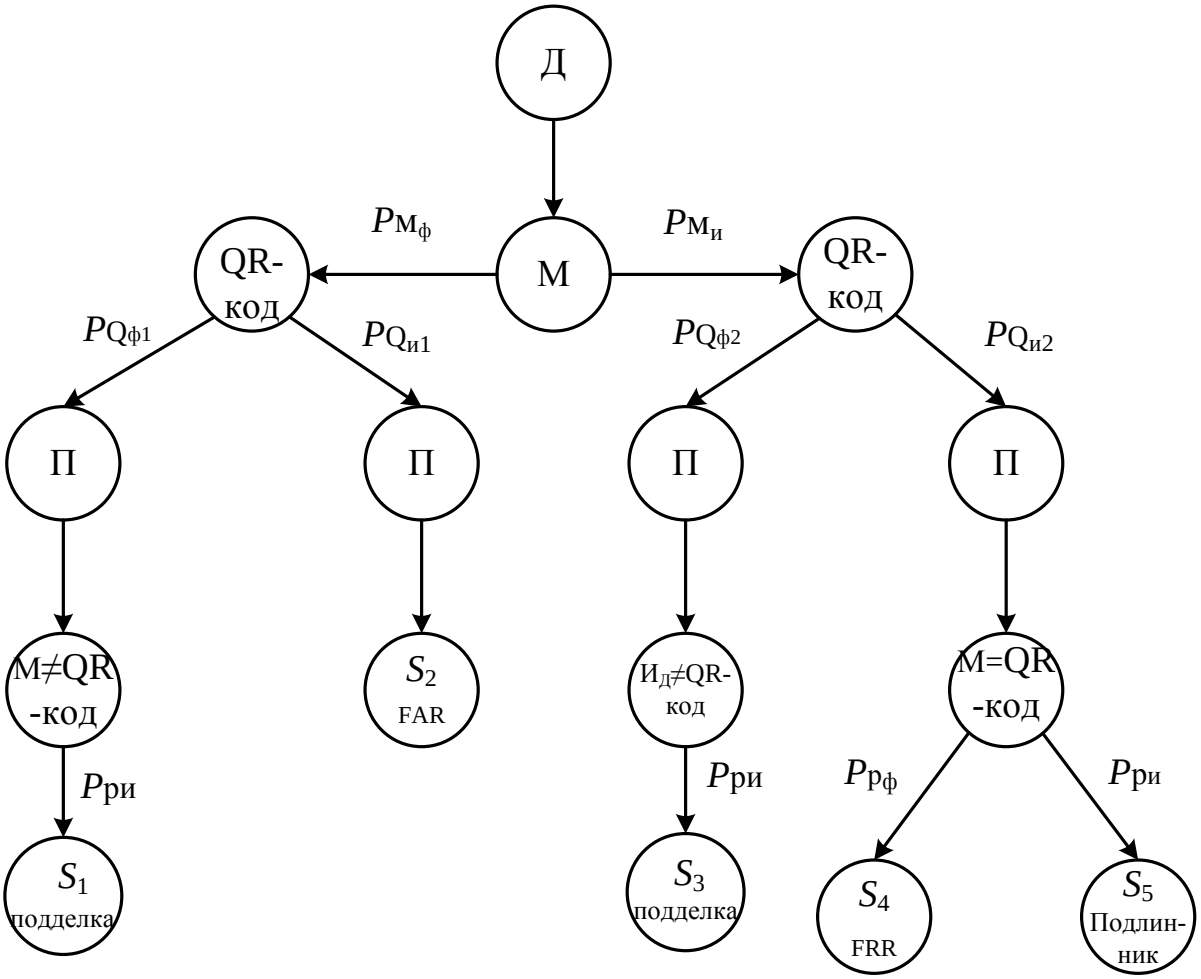


Рисунок 2.2. – Граф переходов

- метка проставлена эмитентом, и QR-код с вероятностью $P_{Q_{и2}}$ также нанесен в этом учреждении, и при совпадении информации метки и QR-кода автоматизированная информационная система с вероятностью распознавания $P_{р_и}$ выдает решение о том, что у потребителя документ-подлинник (на рисунке 2.2 это состояние S_5);
- метка проставлена эмитентом, и QR-код с вероятностью $P_{Q_{и2}}$ также нанесен в этом учреждении, но при распознавании информации метки и QR-кода автоматизированная информационная система с вероятностью распознавания $P_{р_ф}$ ошибочно принимает решение о несовпадении идентификационных признаков (нечеткое изображение метки при

сканировании для распознавания) – появляются ошибки первого рода FRR (состояние S_4);

- метка проставлена эмитентом, но злоумышленником с вероятностью $P_{Q_{\text{ф}2}}$ внесены изменения в текст документа. Важная информация документа $\text{И}_\text{Д}$ не совпадет с информацией QR-кода, и автоматизированная система выдаст решение, что у потребителя подделка (состояние S_3);
- метка проставлена не эмитентом, и с вероятностью $P_{Q_{\text{ф}1}}$ на документ злоумышленником нанесен фальшивый QR-код. При несовпадении информации метки и QR-кода автоматизированная система выдает решение, что у потребителя подделка (на рисунке 2.2 это состояние S_1);
- метка проставлена не эмитентом, и с вероятностью $P_{Q_{\text{и}1}}$ злоумышленник знает алгоритм внесения информации в QR-код. При совпадении информации метки и QR-кода потребитель ошибочно принимает подделку за подлинник – возникает ошибка второго рода FAR(состояние S_2) .

Так как все эти события независимы во времени [53], то сумма $\sum_1^5 P(S_i)$ вероятностей всех состояний равна единице:

$$\sum_1^5 P(S_i) = 1.$$

Тогда вероятность безошибочной идентификации $P_{\text{б.и.}}$ автоматизированной системой определяется по формуле:

$$P_{\text{б.и.}} = P(S_1) + P(S_3) + P(S_5), \qquad (2.4)$$

где $P(S_1)$, $P(S_3)$, $P(S_5)$ – соответственно вероятности перехода документа в состояние S_1, S_3, S_5. Погрешность идентификации документа ε возникает при появлении ошибок идентификации первого и второго рода, т.е.:

$$\varepsilon = P(S_2) + P(S_4),$$

где $P(S_2)$, $P(S_4)$ – соответственно вероятности наступления события S_2, S_4.

Вероятность перехода документа в состояние S_1 определяется по формуле:

$$P(S_1) = P_{\text{М}_\text{ф}} \cdot P_{Q_{\text{ф}1}} \cdot P_{\text{р}_\text{и}} . \qquad (2.5)$$

Вероятность наступления состояния S_3:

$$P(S_3) = P_{\text{М}_\text{и}} \cdot P_{Q_{\text{ф}2}} \cdot P_{\text{р}_\text{и}}. \quad (2.6)$$

Вероятность перехода документа в состояние S_5 определяется по формуле:

$$P(S_5) = P_{\text{М}_\text{и}} \cdot P_{Q_{\text{и}2}} \cdot P_{\text{р}_\text{и}}. \quad (2.7)$$

При подстановке формул (2.5) – (2.7) в (2.4) получим:

$$P_{\text{б.и.}} = P_{\text{М}_\text{ф}} \cdot P_{Q_{\text{ф}1}} \cdot P_{\text{р}_\text{и}} + P_{\text{М}_\text{и}} \cdot P_{Q_{\text{ф}2}} \cdot P_{\text{р}_\text{и}} + P_{\text{М}_\text{и}} \cdot P_{Q_{\text{и}2}} \cdot P_{\text{р}_\text{и}} = P_{\text{р}_\text{и}} \cdot$$

$$\left(P_{\text{М}_\text{ф}} \cdot P_{Q_{\text{ф}1}} + P_{\text{М}_\text{и}} \cdot \left(P_{Q_{\text{ф}2}} + P_{Q_{\text{и}2}}\right)\right) = P_{\text{р}_\text{и}} \cdot \left(P_{\text{М}_\text{ф}} \cdot P_{Q_{\text{ф}1}} + 1 - P_{\text{М}_\text{ф}}\right) = P_{\text{р}_\text{и}} \cdot$$

$$\left(P_{\text{М}_\text{ф}} \cdot \left(P_{Q_{\text{ф}1}} - 1\right) + 1\right) = P_{\text{р}_\text{и}} \cdot \left(1 - P_{\text{М}_\text{ф}} \cdot P_{Q_{\text{и}1}}\right). \quad (2.8)$$

Вероятность точного распознавания зависит $P_{\text{р}_\text{и}}$ от точности сканирования изображений и составляет 0,999 [54].

Вероятность нанесения злоумышленником фальшивой метки $P_{\text{М}_\text{ф}}$ зависит от его способностей определить способ получения метки, собрать установку и верно рассчитать режимы электроразрядного процесса. Известно, что за шесть месяцев 2019 года в России раскрыто 122,8 тыс. преступлений мошеннического характера [55]. При условии, что доля физиков-теоретиков среди преступников составляет не более 30% [56], а численность населения России – 146,8 млн. чел. [57], то за пять лет вероятность нанесения метки составит:

$$P_{\text{М}_\text{ф}} = \frac{122{,}8 \cdot 30 \cdot 10}{146{,}8 \cdot 10^3 \cdot 100} = 0{,}0025.$$

Вероятность расшифровки алгоритма внесения информации в QR-код $P_{Q_{\text{и}1}}$ определим из условия, что изучение кода нарушителем высшей квалификации [58] происходит по экспоненциальному распределению [59] с параметром $\beta_{\text{вз}}$:

$$\beta_{\text{вз}} = \frac{1}{\overline{t_{\text{вз}}}},$$

где $\overline{t_{\text{вз}}}$ – среднее время расшифровки кода.

Время взлома кода с перестановкой определяется по формуле:

$$t_{\text{вз}} = \frac{K!}{\alpha_{\text{п}}},$$

где K – длина ключа перестановки, $\alpha_{\text{п}}$ – интенсивность подбора ключа (6 кодов в минуту, исходя из нормативов скорости чтения – 0,1 в секунду). При длине ключа перестановки 15:

$$t_{\text{вз}} = \frac{15!}{0{,}1} = 1{,}308 \cdot 10^{13}(\text{с}) = 15{,}2(\text{лет}).$$

Тогда среднее время расшифровки кода примет значение:

$$\overline{t_{\text{вз}}} = \frac{t_{\text{вз}}}{2} = 7{,}6 \text{ (лет)}.$$

Зная, что плотность вероятности случайной величины X экспоненциального распределения $f(X)$ имеет вид:

$$f(X) = \beta_{\text{вз}} \cdot e^{-\beta_{\text{вз}} \cdot x} = \frac{1}{7{,}6} \cdot e^{-\frac{1}{7{,}6} \cdot x},$$

определим вероятность расшифровки нарушителем алгоритма внесения информации в QR-код $P_{Q_{\text{и}1}}$ в течение пяти лет, взяв интеграл от плотности вероятности:

$$P_{Q_{\text{и}1}} = \int_0^5 \beta_{\text{вз}} \cdot e^{-\beta_{\text{вз}} \cdot x}\, dx = \int_0^5 \frac{1}{7{,}6} \cdot e^{-\frac{1}{7{,}6} \cdot x}\, dx = -e^{-0{,}1316 \cdot 5} - (-e^{-0{,}1316 \cdot 0}) = 0{,}482.$$

При подстановке определенных значений вероятностей $P_{\text{р}_{\text{и}}}$, $P_{\text{М}_{\text{ф}}}$, $P_{Q_{\text{и}1}}$ в формулу (2.8) вероятность безошибочной идентификации примет вид:

$$P_{\text{б.и.}} = 0{,}999 \cdot (1 - 0{,}0025 \cdot 0{,}482) = 0{,}998.$$

Тогда вероятность ошибок идентификации первого и второго рода при правильно выбранном пороге чувствительности автоматизированной системы составит:

$$\varepsilon = 1 - P_{\text{б.и.}} = 1 - 0{,}998 = 0{,}002 = 0{,}2\% < 5\%.$$

Следовательно, разрабатываемый метод идентификации можно применить для повышения защищенности информации бумажных документов.

Выводы по второй главе

1. В результате исследования видов угроз и их источников произведена классификация угроз безопасности информации бумажного документооборота.
2. Выявлены актуальные угрозы безопасности информации бумажного документооборота:

- случайные и преднамеренные ошибки персонала и внешнего нарушителя, приводящие к несанкционированному доступу к конфиденциальной информации, вследствие чего происходит хищение, уничтожение, модификация, копирование и разглашение информации;
- ошибки, связанные с проектированием и обслуживанием системы защиты бумажного документооборота.

3. На основе разработанной методики определения угроз безопасности информации бумажного документооборота составлена модель угроз и обосновано применение метода идентификации бумажного документа по дополнительному реквизиту и его коду для повышения защищенности документа:

- предлагается использовать разнородные технологии: стохастический электроразрядный процесс, позволяющий исключить возможность подделки метки и нанесение кода, содержащего информацию метки документа-подлинника, при составлении которого можно внести изменения для затруднения дешифровки информации со стороны потенциального нарушителя.
- на момент внедрения нового метода потенциал нарушителя становится недостаточным для реализации угрозы;
- в результате рассмотрения сценариев развития событий также наблюдается трудность реализации нарушителем угроз фальсификации документов;

при определении на основе теории графов надежности идентификации бумажных документов было выявлено, что ошибки идентификации не превысят 5%-ного уровня.

3 ОПРЕДЕЛЕНИЕ ПАРАМЕТРОВ ПРОЦЕССА ЭЛЕКТРОРАЗРЯДНОГО НАНЕСЕНИЯ МЕТКИ И СРЕДСТВА КОДИРОВАНИЯ ЕЕ ИНФОРМАЦИИ

3.1 Физические основы стохастического электроразрядного процесса

В большинстве случаев коммутаторами генераторов мощных наносекундных импульсов служат искровые разрядники [60]. Разряд в газе характеризуется следующими стадиями: пробой, искра и дуга. Пробой – совокупность явлений, нарушающих электрическую изоляцию промежутка между электродами. Искра – совокупность самоподдерживающихся процессов, приводящих к росту тока в межэлектродном промежутке. Дуга – третья стадия разряда, характеризуемая относительно небольшим падением напряжения и стационарным током, определяемым параметрами разрядной цепи и приложенным напряжением [60].

Различают несамостоятельный и самостоятельный разряды в газах. Несамостоятельный разряд протекает только в условиях воздействия внешней ионизации. Самостоятельный разряд возможен при приложении к электродам статического пробивного напряжения $U_{\text{пр}}$, зависящего от внешних условий: давления и температуры, примесей молекул других веществ, влаги, сорта газа, конфигурации электродов, длины межэлектродного промежутка, внешнего облучения и т.д. При этом длительность процесса повышения напряжения до значения $U_{\text{пр}}$ существенно превышает время установления предпробойного тока.

Иначе происходит импульсный пробой. Для его осуществления на электроды подается импульс напряжения, длительность фронта которого много

меньше времени развития разряда [61]. Для характеристики перенапряжения введен коэффициент $k_{\text{п}}$:

$$k_{\text{п}} = \frac{U_{\text{а}}}{U_{\text{пр}}}, \quad (3.1)$$

где $U_{\text{а}}$ – амплитуда импульса.

На формирование импульсов (прямоугольных, ступенчатых и т.д.) влияют процессы, протекающие в плазме разрядного промежутка, тип которой зависит от стадии искрового разряда [60]:

- в начальной стадии образуется слабоионизованная плазма типа плазмы тлеющего разряда. Столкновение электронов, средняя энергия которых значительно превышает тепловую энергию молекул, происходит в основном с нейтральными частицами, но не друг с другом и не с ионами;
- сильно ионизованная квазиравновесная плазма типа дуговой, состояние которой ближе к термически равновесному.

Между моментами приложения напряжения к электродам и осуществления пробоя, характеризуемого резким спадом напряжения, проходит некоторое время запаздывания $t_{\text{з}}$. Оно состоит из статистического времени запаздывания $t_{\text{с}}$, в течение которого в межэлектродном промежутке должен появиться инициирующий электрон, и времени формирования разряда $t_{\text{р}}$. На второй стадии происходит развитие разрядных структур, приводящих к формированию «проводящего мостика» между электродами, и затем к пробою.

Использование искрового разряда приводит к уменьшению статистического времени запаздывания пробоя. При движении электрона к аноду происходит ударная ионизация атомов и молекул газа. В течение времени $t_{\text{р}}$ появляется первичная электронная лавина (при числе начальных электронов N_{e0}=1), следует нарастание ионизации, что приводит к развитию пробоя.

Движение появившихся в результате ионизации электронов и ионов определяется как сумма хаотического перемещения со средней тепловой

скоростью $v_т$ и направленного вдоль электрического поля напряженности E дрейфового движения со скоростью v_e [60]:

$$v_e = \frac{eE}{m\vartheta} = \mu_e E,$$

где e – заряд электрона,

m – масса электрона,

μ_e – подвижность электронов,

ϑ – частота упругих столкновений электронов с молекулами:

$$\vartheta = n v_т \overline{\sigma},$$

где n – плотность газа,

$\overline{\sigma}$ – сечение рассеяния.

Длина свободного пробега электрона между столкновениями определяется следующим образом [60]:

$$\lambda = \frac{v_т}{\vartheta} = \frac{1}{n\overline{\sigma}} \sim \frac{1}{p},$$

где p – давление газа [60]:

$$p = nkT,$$

где k – постоянная Больцмана,

T – температура газа.

По закону подобия (при разрешенных процессах в плазме: ионизация при однократных столкновениях; прилипание, отрыв, дрейф, диффузия, фотоэмиссия электронов; вторичная эмиссия электронов при ударе ионов о катод) для газовых разрядов существует взаимосвязь между характеризующими разряд комплексами величин. Энергия, приобретаемая электроном на пути $\lambda \sim \frac{1}{p}$, составляет $eE\lambda \sim \frac{E}{p}$ (напряженность электрического поля и давление газа входят в виде комплекса $\frac{E}{p}$). Также имеет место комплекс для давления газа и длины межэлектродного промежутка – pd, коэффициента ударной ионизации $\propto$ – $\frac{\propto}{p}$, времени – pt, плотности тока разряда j – $\frac{j}{p^2}$.

Плотность тока [60]

$$j = \sigma E,$$

где σ – проводимость, $\sigma = 2{,}82 \cdot 10^{-4}$.

Вторичная эмиссия электронов с катода происходит в результате его бомбардировки не только положительными ионами, но и фотонами, вызывающими фотоионизацию газа, или метастабильными атомами. Положительные ионы могут вырывать электроны с поверхности катода в результате упругого взаимодействия и при появлении сильного электрического поля вблизи катода. На рисунке 3.1 изображен механизм потенциального вырывания электронов положительными ионами [62]. Под воздействием сильного электрического поля, созданного оказавшимся вблизи катода положительным ионом, с поверхности катода вырывается электрон. Перемещаясь к иону, электрон рекомбинирует с ним, выделившаяся при этом часть энергии в виде кванта света ($h\nu$) может вызвать эмиссию еще одного электрона с поверхности катода.

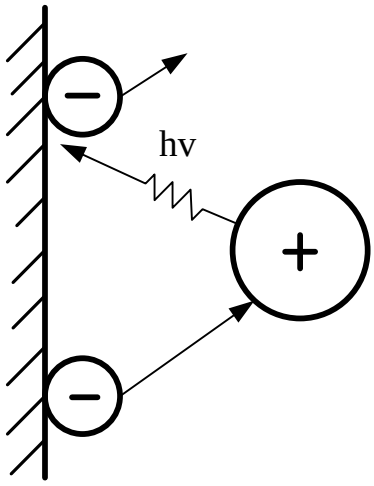


Рисунок 3.1 – Механизм потенциального вырывания электронов положительными ионами [62]

При импульсном воздействии напряжения на развитие разряда значительное влияние оказывает эмиссия электронов под воздействием фотонов, участвующих в рождении электронов, с которых начинается лавинообразная ионизация.

Электронная лавина, развиваясь во времени и в пространстве, испускает фотоны из всего объема лавины при переходе возбужденных частиц (электрон молекулы находится на более удаленной неустойчивой орбите) в нормальное состояние или в результате рекомбинации электронов и ионов (рис. 3.2).

Число актов ионизации N_e в 1 см^3 за 1 с [62]:

$$\frac{dN_e}{dt} = \vartheta_i N_e,$$

где ϑ_i – частота ионизации, главная характеристика скорости процесса.

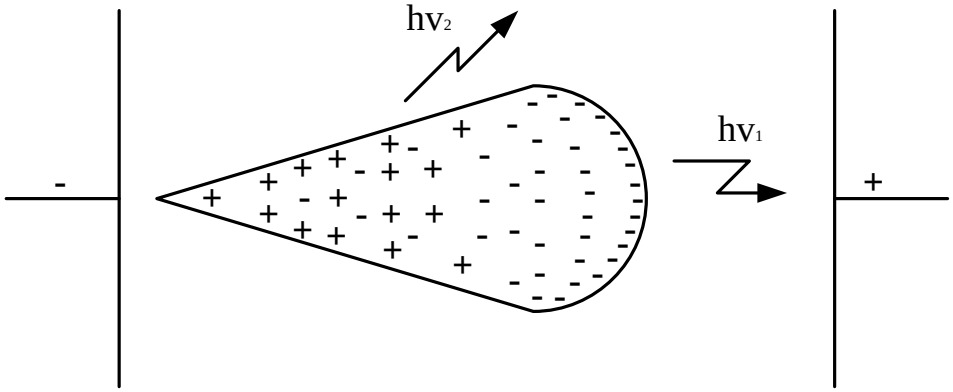


Рисунок 3.2 – Схема электронной лавины [62]

Так как все рождающиеся электроны в лавине перемещаются с одинаковой скоростью, то скорость ионизации характеризуется коэффициентом ударной ионизации $\propto$ – числом актов ионизации, совершаемых электроном на 1 см пути вдоль поля E, определяется по формуле Таунсенда [60]:

$$\propto = Ap \cdot exp\left(-\frac{Bp}{E}\right),$$

где A – коэффициент, зависящий от состава газа,

B – коэффициент, зависящий от энергии ионизации газа.

Константы в вышеприведенной формуле могут быть выбраны на основе экспериментальных данных. Например, в воздухе A=15 $(\text{см} \cdot \text{мм рт. ст.})^{-1}$, B=365 $\text{В}/(\text{см} \cdot \text{мм рт. ст.})$ при $100 < \frac{E}{p} < 800$ $\text{В}/(\text{см} \cdot \text{мм рт. ст.})$ [60].

Минимальное количество энергии, получаемое электроном от электрического поля и требуемое для ионизации [60]

$$\varepsilon_{min} = \mathrm{e}e\frac{B}{A},$$

где e – основание натурального логарифма,

e – заряд электрона.

ε_{min} достигается при $\frac{E}{p} = B$ [60].

Число электронов N_e через промежуток времени t определяется по формуле [60]:

$$N_e = N_{e0}e^{\propto v_e t}.$$

Каждому появившемуся электрону соответствует ион, перемещающийся в сторону катода со скоростью v_i.

При N_{e0}=1 можно определить число ионов в лавине [60]:

$$N_i = e^{\propto x} - 1,$$

где $x = v_e t$ – длина пути.

Бомбардировка катода ионами вызывает вторичную эмиссию электронов. Обобщение экспериментальных данных позволяет определить скорости движения электронов и ионов [60]:

$$v_e = c_1\left(\frac{E}{p}\right)^n,$$

$$v_i = c_2\left(\frac{E}{p}\right)^{1/2},$$

где c_1, c_2 – параметры, зависящие от сорта газа. Значения параметров c_1, c_2 формулы (3) выбираются из таблиц [60]. Скорость движения электронов намного выше скорости ионов, поэтому ионы образуют в лавине объемный заряд, напряженность электрического поля которого E' направлена в сторону, противоположную напряженности поля дрейфового перемещения электронов E (кружки – центры разноименных пространственных зарядов) (рис. 3.3). Число электронов $N_{e\text{кр}}$, при котором $E' \sim E$ и в лавине практически не будет происходить рост количества электронов, называется критическим. При этом критическими будут длина лавины $x_{\text{кр}}$ и время ее развития $t_{\text{кр}}$.

В зависимости от длины межэлектродного промежутка d и критической длины электронной лавины $x_{кр}$ возможен один из трех видов разряда. При таунсендовском разряде $x_{кр}$>d, объемный заряд одиночной лавины не искажает электрическое поле в межэлектродном промежутке [60]:

$$\left(lnN_{екр}\right)/\propto > d.$$

По теории Таунсенда условие возникновения разряда [60]:

$$\gamma e^{\alpha d} \approx 1,$$

где γ – число вторичных электронов с катода, приходящихся на один положительный ион.

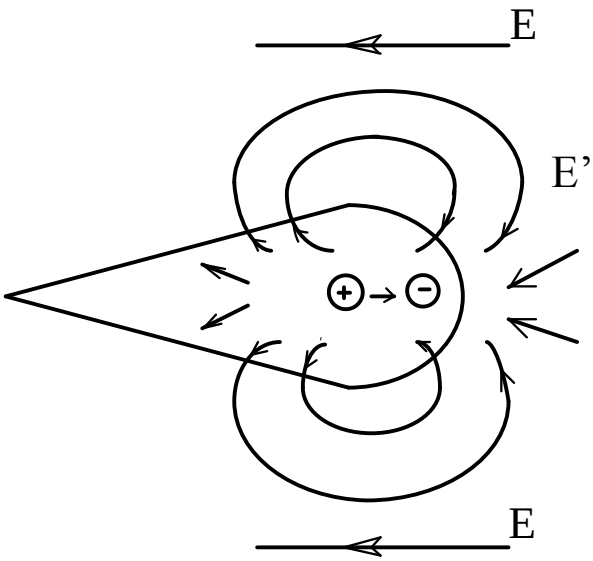


Рисунок 3.3 – Схематичное изображение одиночной лавины [60]

Если длина межэлектродного промежутка превышает критическую длину электронной лавины $x_{кр}$ ($x_{кр}$<d), то возникает стримерный разряд – первичная лавина переходит в стример, затем в разрядный канал [60]:

$$\left(lnN_{екр}\right)/\propto \leq d.$$

Для осуществления этого типа разряда необходимо излучение лавиной числа фотонов или убегающих электронов, достаточного для ионизации молекул газа вблизи головки лавины. Коэффициент перенапряжения $k_{п}$ (3.1) имеет важное значение при переходе от таунсендовского к стримерному разряду [63]. Кривая, изображенная на рисунке 3.4, является границей двух областей, соответствующих разным условиям протекания разряда: область,

лежащая выше кривой, соответствует стримерному разряду, ниже – таунсендовскому.

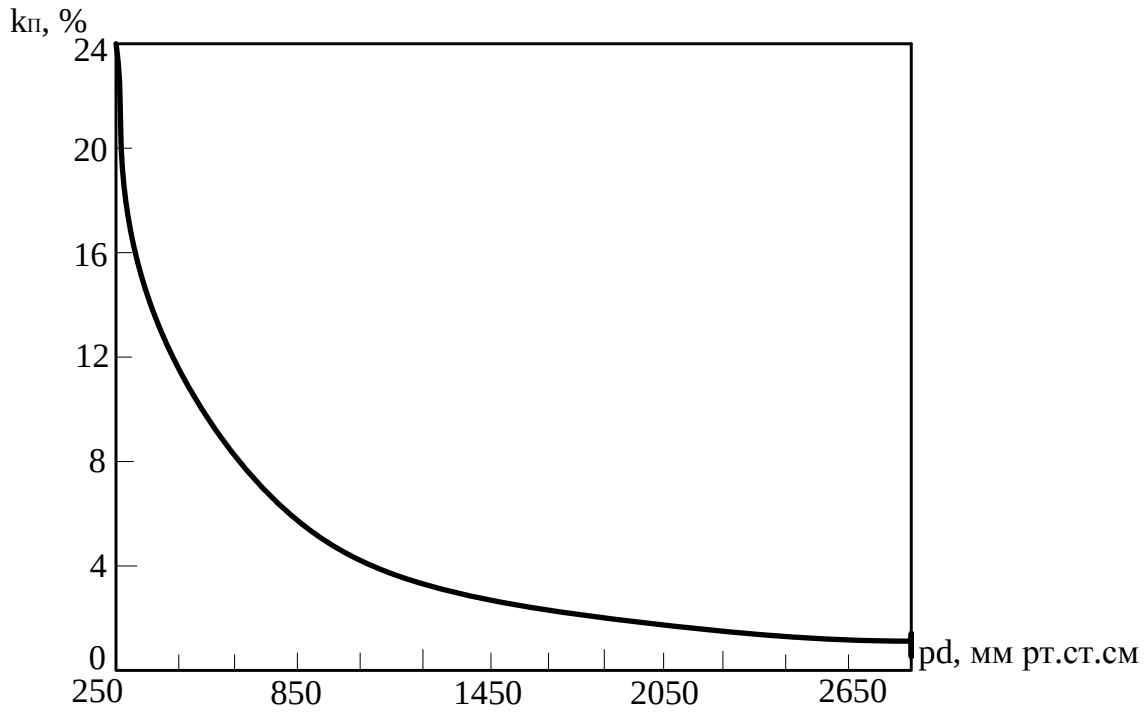


Рисунок 3.4 – Кривая, разделяющая области развития разряда в воздухе по стримерному и таунсендовскому механизмам [60]

Условием появления многолавинного разряда является большое перенапряжение, длина межэлектродного промежутка намного превышает критическую длину электронной лавины $x_{кр}$ ($x_{кр} \ll d$) [60]:

$$\left(lnN_{e\text{кр}}\right)/\propto \ll d.$$

Введение диэлектрика в межэлектродный промежуток представляет собой пробой газа, происходящий в условиях, характеризующихся специфичными факторами: вид неоднородности электрического поля, материал, диэлектрическая проницаемость, толщина подложки, смачиваемость, проводимость ее поверхности [64].

Возникают «тройные точки» (электрод – газ – твердый диэлектрик), приводящие к облегчению инициирования разряда [65]. Под действием нормальной составляющей напряженности электрического поля движущиеся заряды прижимаются к поверхности диэлектрика, при этом выделяющееся в результате движения тепло вызывает дополнительную термическую

ионизацию. При значительном отличии диэлектрических проницаемостей твердого ε_1 и газообразного ε_2 диэлектриков поле «вытесняется в газообразный диэлектрик», что приводит к протеканию разряда при более низких напряжениях [64].

Диффузия заряженных частиц по шести координатным направлениям приводит к уносу частиц из разрядного промежутка и способствует расширению канала разряда после спада напряжения. Эйнштейном получено соотношение между коэффициентом диффузии D и подвижностью электронов μ_e [62]:

$$\frac{D}{\mu_e} = \frac{kT}{e}.$$

Геометрия электродов и наличие макронеоднородностей проводимости влияют на траектории разрядных каналов. Рост разрядных структур, образованных разветвленными плазменными каналами, носит нерегулярный, стохастический характер. Характеристики разрядных структур (форма, скорость роста, величина регистрируемого тока, характер и спектр излучения разрядных каналов и другие) сильно зависят от условий осуществления разряда [66].

Неустойчивость процесса разряда и существующие микронеоднородности газовой среды, – все это приводит к стохастическому ветвлению и изгибу каналов. Вероятность роста токового канала «$P_n(M)$ в направлении n из точки M, принадлежащей разрядной структуре, электроду или проводящему включению» [38] определяется по формуле (3.2):

$$P_n(M) = \begin{cases} \frac{1}{Z}(E_n(M)^2), E_n(M) \geq E_{max} \\ 0, E_n(M) < E_{max} \end{cases}, \quad (3.2)$$

где Z – нормировочный множитель, $Z = \sum_{n,M} E_n(M)$,

$E_n(M)^2$ – квадрат проекции локальной напряженности электрического поля на данное направление,

E_{max} - критическая величина напряженности электрического поля.

Суммирование в формуле (3.2) происходит по всем возможным направлениям и точкам роста.

Наличие в воздухе в пределах межэлектродного промежутка проводящих включений приводит к отклонению траектории канала разряда от кратчайшего пути (рис. 3.5).

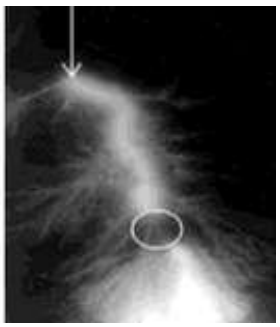


Рисунок 3.5 – Траектория разряда при наличии проводящих включений [67]

Для создания невоспроизводимой метки на бумажном документе было принято решение о создании в межэлектродном промежутке системы «электрод – воздух – бумага – электрод» лавинно-стримерного разряда. Это привело к необходимости расчета требуемого напряжения электрического поля, приложенного к электродам, величина которого значительно превысит минимально необходимое напряжение пробоя промежутка. С помощью лавинно-стримерного разряда на поверхности материала образуется множество расположенных в стохастическом порядке каналов разрушения, на размеры которых большое влияние оказывает энергия разряда [68].

3.2 Проектирование параметров экспериментальной установки для получения идентификационной метки

Форма катода оказывает влияние на величину электронного тока: замена плоской формы на острие приводит к усилению тока [61].

При применении в качестве электродов плоскостей с закругленными краями или сфер при расстоянии между ними не более их диаметра

устанавливается однородное электрическое поле. Величина напряжения пробоя зависит от температуры и давления газа. При достаточной мощности источника напряжения внезапно возникшая искра переходит в дугу. При давлении 0,1 МПа, температуре воздуха 20℃ и длине межэлектродного промежутка 1 см электрическая прочность воздуха составляет 3,2 $\frac{\text{МВ}}{\text{м}}$ [62, 69]. При повышении давления она возрастает ($eE\lambda \geq E_c$), так как уменьшаются расстояние между молекулами и длина свободного пробега электронов. При понижении давления электрическая прочность сначала понижается, но при некотором значении давления возрастает, так как при значительных расстояниях между молекулами уменьшается вероятность столкновений электронов с ними. На рисунке 3.6 приведена зависимость максимального пробивного напряжения от произведения давления газа на длину межэлектродного промежутка.

В настоящее время не существует достоверных теоретических расчетов напряжения пробоя газового промежутка, поэтому для ориентировочного определения пробивного напряжения воздуха при давлении 760 мм рт. ст., температуре 20 °С и частоте 50 Гц используются следующие зависимости [70]:

1) при использовании плоских электродов, удаленных друг от друга на величину d, не превышающего 1 см:

$$U_{\text{пр}} = E_{\text{пр}} d, \text{ кВ}, \tag{3.3}$$

где $E_{\text{пр}}$ – электрическая прочность воздушного промежутка, кВ/см,

d – величина межэлектродного промежутка, см. При $d < 1$ см

$$E_{\text{пр}} = (E_{\text{пр0}} + \frac{\alpha}{d}), \text{ кВ/см}, \tag{3.4}$$

где $E_{\text{пр0}} = 30$ кВ/см – электрическая прочность воздушного промежутка в однородном электрическом поле при нормальных условиях (p_0 = 760 мм рт. ст. и T_0 = 293°К), $\alpha = 1{,}35$ кВ – константа.

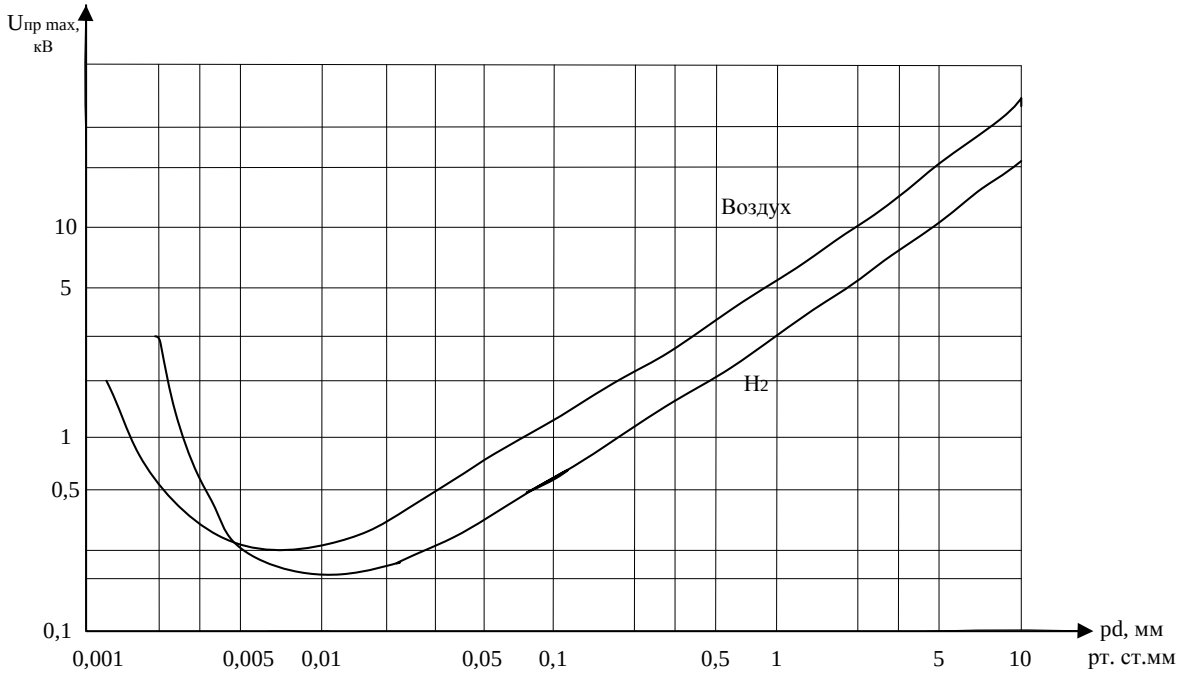


Рисунок 3.6 – Зависимость максимального пробивного напряжения при частоте 50 Гц и температуре 20℃ от произведения давления газа на длину межэлектродного промежутка для воздуха и водорода [70]

При расстоянии между электродами d в пределах от 1 до 20 см

$$U_{\text{пр}} = 24{,}5d\delta\left(1 + \frac{0{,}28}{\sqrt{d\delta}}\right), \text{ кВ}, \tag{3.5}$$

где δ - относительная плотность газа при давлении p (мм рт. ст.) и абсолютной температуре T (в градусах Кельвина), отличных от нормальных p_0 и T_0 (760 мм рт. ст. и 293°К), вычисляется по формуле:

$$\delta = \frac{p}{p_0} \cdot \frac{T_0}{T} = \frac{p}{760} \cdot \frac{273+20}{T} = 0{,}386 \cdot \frac{p}{T}. \tag{3.6}$$

2) при применении симметричного поля двух сфер, кратчайшее расстояние между которыми d находится в пределах $r < d < 2r$ (малая степень неоднородности) напряжение пробоя определяется по формуле:

$$U_{\text{пр}} = \frac{E_{\text{пр}} d}{f}, \text{ кВ}, \tag{3.7}$$

где

$$E_{\text{пр}} = 27{,}2\delta\left(1 + \frac{0{,}54}{\sqrt{r\delta}}\right), \text{ кВ/см}, \tag{3.8}$$

где d – кратчайшее расстояние между сферами, см,

r – радиус сферы, см,

f – геометрический фактор, учитывающий снижение напряжения пробоя вследствие неравномерности электрического поля

$$f = 0{,}25\left[\frac{d}{r} + 1 + \sqrt{\left(\frac{d}{r} + 1\right)^2 + 8}\right]. \quad (3.9)$$

Неоднородное электрическое поле создается в случаях, когда в качестве электродов применяются острие и плоскость, два острия, два провода, сферические поверхности при расстоянии между ними, превышающем радиус сферы. Особенность пробоя заключается в том, что при критических значениях напряженности электрического поля появившийся частичный разряд приобретает вид короны. При повышении напряжения корона переходит в искровой разряд и дугу [69]. Для ориентировочного определения пробивного напряжения воздуха при давлении 760 мм рт. ст., температуре 20°С и частоте 50 Гц используются следующие зависимости [70]:

1) для поля двух параллельных цилиндрических проводов при значении отношения d/r, не превышающем 30,

$$U_{\text{пр}} = 2E_{\text{пр}} \cdot r \cdot ln\frac{d}{r}, \text{ кВ}, \quad (3.10)$$

где $E_{\text{пр}} = 30\delta\left(1 + \frac{0{,}301}{\sqrt{r\delta}}\right)$, кВ/см,

d – расстояние между осями проводов, см,

r – радиус провода, см,

$U_{\text{пр}}$ – напряжение на проводе относительно нейтрали, кВ;

2) напряжение пробоя для электродной системы «острие – острие» при резко неоднородном поле может быть вычислено по приближенной формуле:

$$U_{\text{пр}} = U_{\text{пр}} = (14 + 3{,}16d)\delta, \text{ кВ}. \quad (3.11)$$

3) напряжение пробоя для электродной системы «острие – плоскость» при резко неоднородном поле может быть вычислено по приближенной формуле:

$$U_{\text{пр}} = (7 + 3{,}36d)\delta, \text{ кВ}. \quad (3.12)$$

При положительно заряженной игле электродной системы острие – плоскость для пробоя потребуется меньшее напряжение, чем при использовании иглы в качестве катода (рис. 3.7).

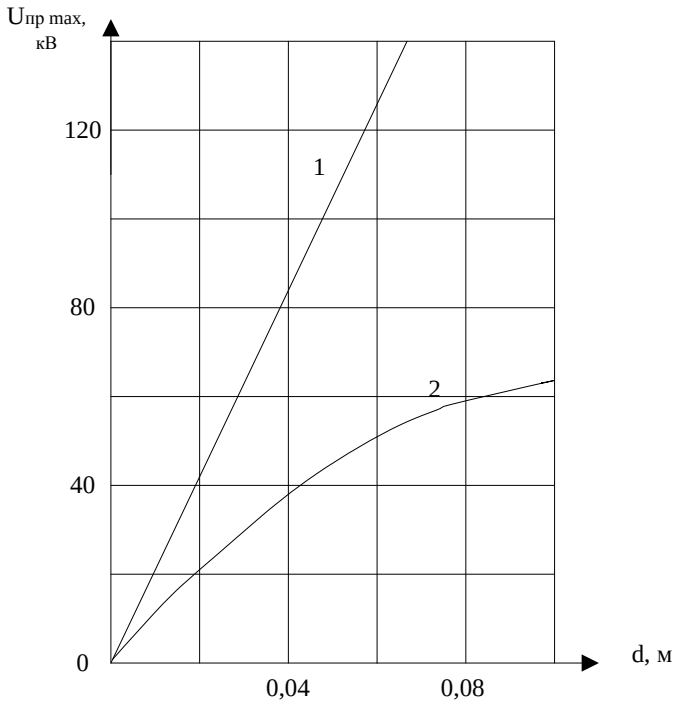


Рисунок 3.7 – Зависимость максимального пробивного напряжения от длины межэлектродного промежутка при положительной (кривая 2) и отрицательной полярности (кривая 1) на игле [71]

Это объясняется тем, что при любой полярности в районе иглы напряженность электрического поля будет наибольшей, следовательно, там будет происходить ионизация. Электроны быстро нейтрализуются на аноде, а вблизи катода наблюдается облако малоподвижных ионов – объемный заряд. При положительной полярности иглы наличие объемного заряда является ее продолжением, ослабляет напряженность поля вблизи нее, создает благоприятные условия для дальнейшей ионизации [71].

При отрицательной полярности на игле происходит снижение напряженности поля в неионизированной области, поэтому дальнейшая ионизация требует более высокого напряжения. Облако малоподвижных ионов

является экраном, сглаживающим максимальные неоднородности поля в межэлектродном промежутке.

В качестве материала для электродов применяют медь М1, М2; латунь ЛС-62; алюминий и его сплавы Д1, Ал3, Ал5; чугун; углеграфитированный материал марки ЭЭГ; вольфрамомедные композиционные металлокерамические сплавы [72]. Основными факторами, влияющими на выбор материала, являются их износ, величина межэлектродного промежутка, температурные деформации технологической системы. Следовательно, материал электрода должен быть выбран, исходя из следующих требований [72]: высокая эрозионная стойкость; способность к обеспечению стабильности процесса электроразрядной обработки; возможность применения несложного технологического процесса для получения электрода требуемой формы и необходимых размеров; относительно небольшая стоимость электрода.

Медные электроды при высокой стоимости материала и трудоемкости процесса их изготовления обеспечивают самые высокие показатели стабильности процесса протекания разряда.

Повышенным износом характеризуются электроды, изготовленные из латуни, алюминия и его сплавов при невысокой их стоимости. Кроме того, алюминий характеризуется малым диапазоном режимов работы.

Область применения серого чугуна ограничивается его возможностью работы в режимах малой энергии импульсов.

Углеграфитированный материал марки ЭЭГ обладает самой высокой износостойкостью, легкой обрабатываемостью, способностью к обеспечению стабильности протекания процесса при разных режимах электроразрядной обработки. Область применения этого материала – электроды-инструменты сложной формы.

Несмотря на высокую эрозионную стойкость вольфрамомедных и композиционных металлокерамических сплавов, эти материалы имеют

высокую стоимость. Поэтому их применение оправданно только в случае изготовления электродов сложной формы и небольших размеров.

Величина пробивного напряжения также зависит от материала электродов (табл. 3.1).

Таблица 3.1 – Пробивное напряжение вакуумного промежутка при электродах, изготовленных из различных материалов [73]

Материал	**Пробивное напряжение, кВ**
Сталь	122
Нержавеющая сталь	120
Никель	96
Алюминий	41
Медь	37

Для проведения экспериментов была собрана установка [74-79]. В качестве материала электродов была выбрана медь из-за наилучших показателей процесса протекания разряда, сравнительно небольшой величины напряжения пробоя, несмотря на высокую стоимость материала.

В течение экспериментальных исследований использовались электроды различной формы, для расчета напряжения пробоя были применены эмпирические зависимости (3.3) – (3.12) и графики рисунков 3.6 и 3.7. В частности, рассматривалась коническая форма электрода с разными углами заточки.

В результате была выбрана схема установки (рис. 3.8), в которой один из электродов (поз. 2) представляет собой плоскость, форма второго (поз. 1) – острие. На плоский электрод для нанесения невоспроизводимой метки помещался бумажный документ.

В ходе проведения экспериментов была определена оптимальная длина межэлектродного промежутка, которая составила 10 мм. Газовые разряды производились в воздухе, атмосферное давление менялось в пределах 740 – 760

мм рт. ст., температура воздуха – 20±3℃, величина максимального пробивного напряжения – 50 кВ.

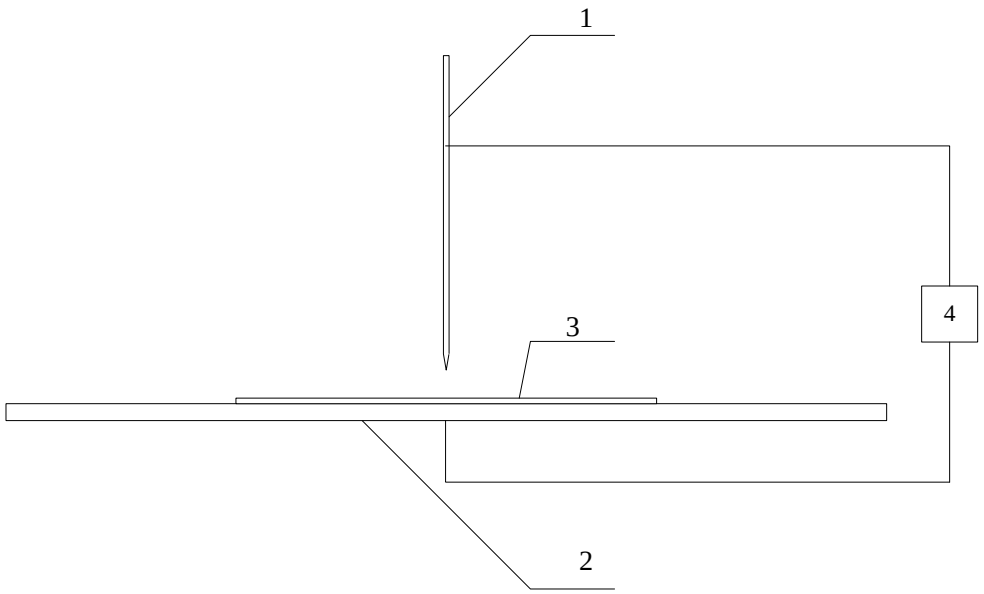


Рисунок 3.8 – Схема нанесения невоспроизводимой метки: 1, 2 – электроды, 3 – бумажный документ с нанесенной мишенью и индивидуальным кодом (серийным номером), 4 – высоковольтный источник

В результате проведения экспериментов на бумажных носителях с нанесенными черным цветом мишенями на них электроразрядным способом были получены метки в виде ряда отверстий, расположенных стохастическим образом. Размеры отверстий зависели от энергии разряда. Кроме того, каждой мишени был присвоен свой индивидуальный код, который располагался внизу, под мишенью (рис. 3.9).

Полученная электроразрядным способом стохастическая метка с индивидуальным кодом является невоспроизводимой и может быть нанесена на бумажный носитель (документ особой секретности, сертификат, денежная купюра) или металл (например, двигатель самолета, автомобиля). Затем информация с метки и кода должна быть закодирована в виде двумерного графического кода, например, QR-кода и для определения подлинности объекта необходимо произвести распознание закодированной информации [74, 77].

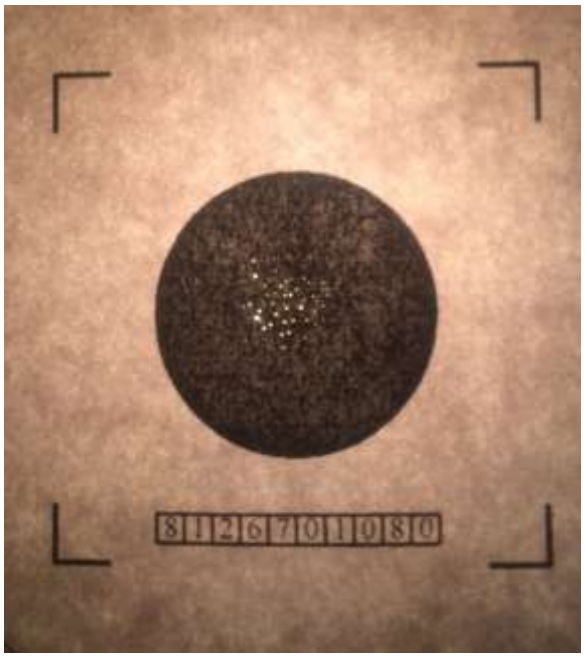


Рисунок 3.9 – Стохастическая метка и ее индивидуальный код

3.3 QR-код как средство кодирования идентификационных признаков изображения метки

Для осуществления процедуры идентификации бумажного документа по созданной электрическим разрядом метке необходимо провести сравнение информации об ее идентификационных признаках с эталонной информацией метки-оригинала. В качестве идентификаторов метки были выбраны ее индивидуальный код – серийный номер, количество прожженных электрическим разрядом отверстий на мишени, координаты центров масс отверстий (по двум осям – *X* и *Y*), размеры отверстий (их площади в пикселях). Совокупность выбранных идентификационных признаков содержит информацию о метке в полном объеме и отвечает всем требованиям, предъявляемым к идентификаторам [12]:

- индивидуальность метки отражается описанием только ей присущих данных: индивидуальный код, число отверстий на мишени, координаты их центров масс и площади отверстий меток отличаются друг от друга;

- устойчивость признаков обеспечивается сохранностью их свойств в течение срока службы документа (экспериментально проверено);
- для проведения идентификации метки достаточно совокупности перечисленных признаков, полностью ее описывающих;
- все идентификаторы отвечают требованию допустимости – они могут быть измерены с помощью алгоритмов предварительной обработки изображения метки, разработанных в третьей главе;
- все признаки являются воспроизводимыми – они обеспечивают неоднократное отображение информации о свойствах метки в полном объеме;
- каждый идентификатор обладает выраженностью – доказывает свое существование.

При небольшом количестве документов значения признаков меток-оригиналов могут храниться в базах данных. Но хранение информации большого объема документов исключает такую возможность.

Поэтому в новом методе идентификации предлагается на бумажном документе кроме метки, созданной стохастическим электрическим разрядом, поблизости от нее нанести двумерный штрихкод, хранящий эталонную информацию о значениях ее идентификаторов [79]. Запись большого объема информации в этом коде и считывание ее сканирующим оборудованием дает возможность отказаться от использования баз данных. Сравнение признаков метки с закодированными эталонными значениями, хранящимися в двумерном штрихкоде, позволяет сделать вывод о подлинности документа.

В настоящее время доступно использование более двадцати разных двумерных кодов. Среди них наиболее популярны: Aztec code, MaxiCode, ShotCode, Ez code, Micro QR code, QR код, Data Matrix, Microsoft Tag (HCCB), MicroPDF417, PDF417, Codablock-F, BeeTagg [15].

При выборе средства кодирования были учтены следующие характеристики штрихкодов [22]:

- внешний вид;

- автономность считывания кода;
- возможность черно-белой печати;
- возможность осуществления оптимизации кода при существующих технологиях печати;
- возможность нанесения кода на материалы разного рода;
- величина максимального объема данных при максимальном уровне коррекции ошибок;
- существование кодов коррекции ошибок;
- размер кода;
- возможность пространственного распознавания кода;
- открытость формата;
- поддержка индустрией.

Характер нанесенной метки требует принятия величины максимального объема кодируемых данных в качестве одного из главных критериев выбора средства кодирования информации. Это объясняется тем, что на мишени электрическим разрядом прожигается от 60 до 80 отверстий. Описание количества, размеров и координат центров масс этих отверстий требует большой емкости данных.

Анализ характеристик технологий перечисленных двумерных штрихкодов привел к отсеиванию на первом же этапе исследования четырех символик: ShotCode, Ez code, Microsoft Tag (HCCB), BeeTagg [22, 80-82]. Исключение их из дальнейшего рассмотрения вызвано необходимостью обращения при считывании кода к интернет-серверу. Кроме того, Microsoft Tag (HCCB) требует при своем использовании цветные: принтер, видеоконтрольное устройство, снимающую камеру. Код характеризуется закрытостью формата, что резко снижает область применения. В настоящее время его технология проходит этап тестирования. Возможность его распознавания зависит от качества и чистоты рамки данного кода, угла видимости его сканирующим устройством.

Остальные коды позволяют производить автономное считывание. MaxiCode (рис. 1.2) создан в 1992 году фирмой United Parcel Service для грузоотправительных и грузоприемных систем, не рассматривается как средство кодирования идентификаторов, так как использование его технологии защищено патентами [83, 84]. Кроме того, недостатками данного штрихкода является небольшая величина максимального объема кодируемых данных: алфавитно-цифровых знаков – 93, цифровых знаков – 138 [85]. Для своего применения код требует использования сканеров с высоким разрешением.

Кодирование информации с помощью многорядного кода Codablock-F (рис. 3.10) похоже на построчное заполнение символов с разрывом строки текстового редактора [22]. Всего может быть от 2 до 44 строк, соответственно максимальное количество символов – 2725. Количество строк, знаков в строке, плотность печати для оптимального размещения идентификационных признаков должны быть рассчитаны программой печати символа. Возможность коррекции ошибки отсутствует.

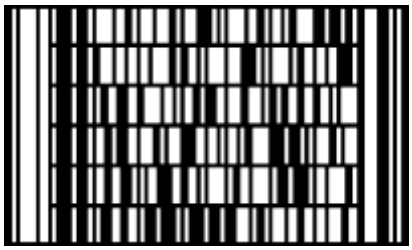


Рисунок 3.10 – Пример двумерного штрихкода Codablock-F [22]

В результате анализа остальных двумерных штрихкодов для кодирования информации, предоставляемой стохастически нанесенными метками, предложено использовать наиболее популярный среди них QR-код (табл. 3.2). Это матричный код, имеющий вид двумерного штрихкода и статус опубликованного стандарта ISO/IEC 16022:2006 [86, 87].

Таблица 3.2 – Сравнение характеристик двумерных штрихкодов [88]

Характеристики двумерных штрихкодов		**QR-код** 	**PDF417** 	**DataMatrix** 
Разработчик		DENSO Wave	Symbol Texnologies	RVSI ACUTY CiMatrix
Вид		матричный	многорядный	матричный
Объем данных	Цифровых	7089	2710	3116
	Буквенно-цифровых	4296	1850	2355
	Двоичных	2953	1018	1556
	Японских, китайских, корейских символов	1817	554	778
Преимущества		Большой объем данных, маленький размер, высокая скорость сканирования	Большой объем данных	Маленький размер
Область применения		Все категории	Автоматизация делопроизводства	Автоматизация производства
Стандарты		AIM, JIS,ISO	AIM, ISO	AIM, ISO

Преимущество применения QR-кода по сравнению с другими матричными кодами заключается в способности надежного кодирования значительно большего объема цифровой и текстовой информации, практически на любой поверхности. Кроме того, код имеет сравнительно небольшой размер (при кодировке 7089 цифр, 4296 цифр и букв) [88]. Использование другого

распространенного двумерного матричного штрихкода Data Matrix производить кодировку 7001 цифры и 4208 прописных букв (рис. 1.2) [89].

Другой известный код Aztec code позволяет записать 3832 числовых или 3067 буквенных символов (рис. 3.11) и также уступает QR-коду [90].

Рисунок 3.11 – Пример двумерного штрихкода Aztec code [22]

Для QR-кода разрешение играет не столь важную роль, как, например, для двумерных штрих-кодов PDF417 (рис. 1.2) (число цифр в одном коде – 2710, цифр и букв – 1850), поэтому для распознавания не требуется дорогостоящее оборудование [91, 92].

Доступная функция избыточного кодирования QR-кода позволяет получить информацию из поврежденного до 30% кода при уровне коррекции ошибок: 7, 15, 25, 30%. При этом распознавание кода возможно при повороте на произвольный угол, зеркальном отражении, выворотке – обратной замене цвета фона и текста [22].

Запись большого объема информации в этом коде дает возможность отказаться от использования баз данных, предназначенных для хранения эталонной информации, содержащейся в получаемых метках. Кроме того, QR-код характеризуется высокой скоростью распознавания сканирующим оборудованием, определяющим код как двумерное изображение.

Выводы по третьей главе

1. В результате анализа физической сущности электроразрядного способа нанесения уникальных меток на бумажный носитель и исследования процесса электрического разряда в межэлектродном промежутке между мишенью метки и инструментом-электродом было получено доказательство невоспроизводимого, стохастического характера наносимых меток.

Неустойчивость процесса разряда и наличие в воздухе в пределах межэлектродного промежутка проводящих включений приводит к отклонению траектории канала разряда от кратчайшего пути.

2. Рассчитаны параметры и режимы работы электроразрядного устройства, необходимого для получения невоспроизводимой метки. Для определения оптимальных режимов пробоя межэлектродного промежутка проведены исследования влияния формы, полярности, материалов электродов на процесс нанесения метки на бумажный носитель. Выбрана электродная система острие – плоскость, положительный электрод – игла. В качестве материала для электродов предложено применить медь из-за наилучших показателей процесса протекания разряда. На электрод-плоскость был помещен бумажный документ с нанесенной мишенью с индивидуальным кодом – серийным номером. Оптимальная длина межэлектродного промежутка составила – 10 мм. Газовые разряды производились в воздухе, атмосферное давление менялось в пределах 740 – 760 мм рт. ст., температура воздуха – 20±3℃. Произведен расчет необходимого максимального напряжения пробоя межэлектродного промежутка – 50 кВ. Полученные с помощью собранной установки метки также показали неустойчивый характер электрического разряда: метки имели вид отверстий, расположенных стохастическим образом. Размеры отверстий зависели от энергии разряда.

3. Для осуществления процедуры идентификации бумажного документа по созданной электрическим разрядом метке был обоснован выбор

ее идентификаторов. В качестве идентификационных признаков метки приняты ее индивидуальный код – серийный номер, количество прожженных электрическим разрядом отверстий на мишени, координаты центров масс отверстий, размеры отверстий. Совокупность выбранных идентификационных признаков содержит информацию о метке в полном объеме и отвечает всем требованиям, предъявляемым к идентификаторам. Для кодирования информации, предоставляемой стохастически нанесенными метками, предложено использовать технологию написания QR-кода. Преимущество его применения по сравнению с другими матричными кодами заключается в способности надежного кодирования значительно большего объема цифровой и текстовой информации, практически на любой поверхности. Кроме того, QR-код характеризуется высокой скоростью распознавания сканирующим оборудованием, определяющим код как двумерное изображение.

4 РАЗРАБОТКА МОДЕЛИ ИДЕНТИФИКАЦИИ НЕВОСПРОИЗВОДИМОЙ МЕТКИ, ПОЛУЧЕННОЙ ЭЛЕКТРОРАЗРЯДНЫМ СПОСОБОМ

4.1 Алгоритмы предварительной обработки изображения метки для подготовки к кодированию значений идентификаторов

Для последующего кодирования информации метки, полученной стохастическим способом, необходимо применить алгоритмы предварительной обработки ее изображения. Это вызвано следующими причинами. Полученные электроразрядным способом отверстия мишени имеют малые размеры, и для четкого изображения на фотографии требуют подсветки. Подсветка приводит к выявлению неоднородности окраски мишени – на фотографии видны более светлые пятна, которые затем программой могут быть восприняты за несуществующие отверстия. Кроме того, бумага имеет нерегулярную структуру (волокна бумаги располагаются на разных расстояниях), разреженность также может привести к получению неточной информации. Все это вызывает необходимость применения алгоритмов предварительной обработки изображения метки.

Изображение имеет растровый формат, поэтому возможен попиксельный доступ для считывания и установки значения цвета. Растровое изображение на мониторе и других отображающих устройствах состоит из сетки пикселей – прямоугольных цветных точек [93].

Изображение каждой метки хранится в формате RGB – аддитивной цветовой модели, широко используемой в технике. В данной модели цвета образуются добавлением (англ. addition) к чёрному цвету. Модель описывает способ синтеза цвета для цветовоспроизведения. Выбор красного, зеленого и

синего цветов (аббревиатура которых и дала ей название) в качестве основных компонент обусловлен особенностями физиологии восприятия цвета сетчаткой человеческого глаза [94]. Синтез цветов Ц при освещении экрана двумя цветными прожекторами в этой модели обозначается:

$$Ц = (r_1 + r_2, g_1 + g_2, b_1 + b_2),$$

где (r_1, g_1, b_1) – обозначение цвета одного цветного прожектора,

(r_2, g_2, b_2) – выражение цвета второго цветного прожектора.

Изображение в трехканальной цветовой модели RGB получается с помощью синтеза основных цветов. Смешивание двух компонент позволяет получить пурпурный (M – magenta), жёлтый (Y – yellow), циановый (C – cyan) цвета. Синтез всех трёх цветовых компонентов обеспечивает получение белого цвета (W – white).

В большом количестве приложений пространство RGB имеет вид куба 1×1×1. Интенсивность каждой из трех компонент цвета может принимать значения от 0 до 1 на соответствующей оси координат (r, g или b).

В компьютерной технике чаще используется гамма-компенсированное цветовое пространство sRGB. Области значений каждой из координат представляются в виде одного октета, имеющего значения целых чисел от 0 до 255 включительно (0 – минимальная, 255 – максимальная интенсивность).

При подготовке изображения метки к кодированию необходимо получить максимальную яркость каждого пикселя. Можно различными способами перевести изображение из цветовой модели RGB в другие известные системы для выделения яркости. Предлагается осуществить перевод (конверсию) изображения из модели RGB в YUV – цветовую модель, синтезирующую цвет из яркости (Y) и двух цветоразностных компонент (U и V) [95]. Именно модель YUV разработана для выделения яркостной компоненты изображений.

Получение полутонового изображения метки с помощью осуществления конверсии из модели RGB в модель YUV производится при применении формул (4.1):

$$Y = 0{,}299R + 0{,}587G + 0{,}114B,$$
$$U = -0{,}14713R - 0{,}2886G + 0{,}436B + 128, \quad (4.1)$$
$$V = 0{,}615R - 0{,}51499G - 0{,}10001B + 128,$$

где R, G, B – соответственно интенсивности красной, зеленой и синей компонент цвета [96],

Y – яркостная компонента,

U и V – цветоразностные компоненты.

Составляющие U и V несут в себе информацию для восстановления требуемого цвета, их значения варьируются в пределах: U – [-0.436, 0.436], V – [0.615, 0.615] [97]. Y изменяется в диапазоне [0, 1]. В яркостной компоненте содержится черно-белое изображение (в оттенках серого цвета).

К полутоновому изображению метки применяется сегментация, являющаяся одной из главных задач обработки изображений. В результате применения данной операции изображение метки разбивается на области, используя определенный критерий однородности [98]. Каждая область представляет собой совокупность элементов, объединенных по общему свойству. Сегментация предназначена для выделения границ на изображении для упрощения его дальнейшего анализа.

Для осуществления процесса сегментации предлагается использовать один из основных и простых способов – разделение изображения на области с помощью порога – заданной величины яркости. В ходе порогового разделения производится сравнение значения яркости каждого пикселя изображения с заданным значением порога.

Для четкого разграничения светлых (отверстия) и черных областей (фон) проведена бинаризация – операция порогового разделения по методу Оцу [99, 100]. Выбор этого метода из существующих способов обусловлен наиболее качественным уровнем бинаризации при работе с метками, нанесенными стохастическим образом. В основе метода лежит использование гистограммы

распределения значений яркости пикселей растрового изображения. Она строится по величинам, используя формулу (4.2):

$$p_i = \frac{n_i}{N}, \tag{4.2}$$

где p_i – значения яркости пикселей, N – общее количество пикселей на изображении, n_i – число пикселей с уровнем яркости i [99, 100]. Разделение диапазона яркостей на два класса осуществляется с помощью пороговой величины уровня яркости $k_{\text{ц}}$, представляющего собой целое значение от 0 до L. Относительные частоты каждого класса яркости $\omega_0(k_{\text{ц}}), \omega_1(k_{\text{ц}})$ определяются по формулам (4.3):

$$\omega_0(k_{\text{ц}}) = \sum_{i=1}^{k_{\text{ц}}} p_i\,,\ \omega_1(k_{\text{ц}}) = \sum_{i=k_{\text{ц}}+1}^{L} p_i = 1 - \omega_0(k_{\text{ц}}). \tag{4.3}$$

Для каждого из двух классов рассчитываются средние уровни изображения $\mu_0(k_{\text{ц}}),\ \mu_1(k_{\text{ц}})$ по формулам (4.4):

$$\mu_0(k_{\text{ц}}) = \sum_{i=1}^{k_{\text{ц}}} \frac{ip_i}{\omega_0},\ \mu_1(k_{\text{ц}}) = \sum_{i=k_{\text{ц}}+1}^{L} \frac{ip_i}{\omega_1}. \tag{4.4}$$

Определяется максимальное значение оценки качества разделения изображения на две части по формуле (4.5):

$$\eta(k_{\text{ц}}) = max_{1 \le k_{\text{ц}} \le L-1} \left(\frac{\sigma^2_{\text{кл}}(k_{\text{ц}})}{\sigma^2_{\text{общ}}} \right), \tag{4.5}$$

где $(\sigma_{\text{кл}})^2 = \omega_0\omega_1(\mu_1 - \mu_0)^2$ – межклассовая дисперсия, $(\sigma_{\text{общ}})^2$ – общая дисперсия для всего изображения целиком.

По полученному значению порога производится бинаризация (4.6):

$$Y'(x,y) = \begin{cases} 0,\ Y(x,y) < k_{\text{ц}} \\ 1,\ Y(x,y) \ge k_{\text{ц}} \end{cases} \tag{4.6}$$

Все значения больше критерия становятся 1, в данном случае 255 (белый) и все значения пикселей, которые меньше порога $k_{\text{ц}}$ – 0 (черный).

В результате проведенной бинаризации получено бинарное изображение метки с четко выраженными границами отверстий. Для отверстий установлен один цвет, для мишени – другой (рис. 4.1) [101].

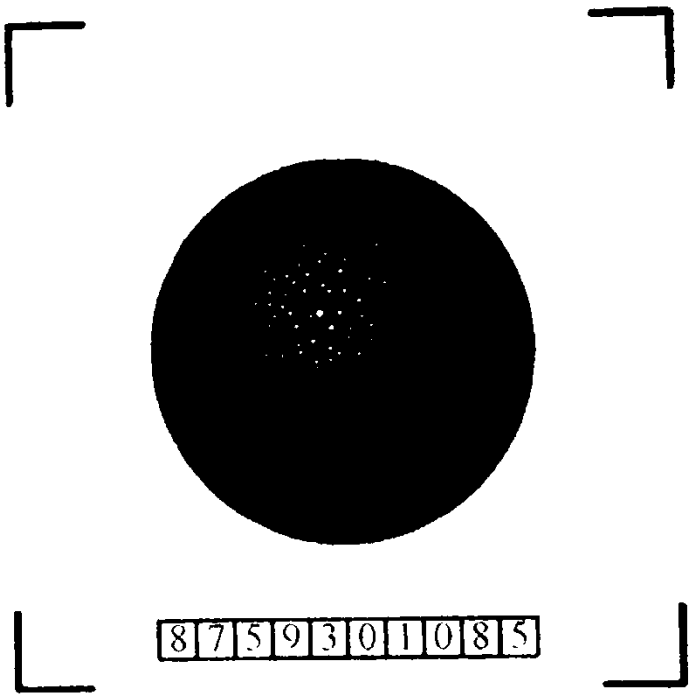


Рисунок 4.1 – Бинарное изображение метки

Для определения месторасположения мишени на изображении (нахождение четырех ограничителей в виде уголков) применен попиксельный обход по вертикали и горизонтали (рис. 4.1) с отбором точек – вершин уголков при удовлетворении следующих критериев:

1) яркость точки меньше заранее вычисленного порога яркости по изображению:

$$Y(x, y) < k_{\text{ц}};$$

2) у двух соседних с ней точек яркость больше порога;

$$\begin{cases} Y(x+1, y) > k_{\text{ц}} \\ Y(x, y+1) > k_{\text{ц}} \end{cases}, \text{ или}$$

$$\begin{cases} Y(x, y+1) > k_{\text{ц}} \\ Y(x-1, y) > k_{\text{ц}} \end{cases}, \text{ или}$$

$$\begin{cases} Y(x-1, y) > k_{\text{ц}} \\ Y(x, y-1) > k_{\text{ц}} \end{cases}, \text{ или}$$

$$\begin{cases} Y(x, y-1) > k_{\text{ц}} \\ Y(x+1, y) > k_{\text{ц}} \end{cases}.$$

3) обнаружение по направлению оставшихся двух сторон линий, состоящих из точек, у которых значения яркости ниже пороговой величины.

Координаты вершин записываются в принятые переменные leftTopX, leftTopY, rightTopX, rightTopY, leftBottomX, leftBottomY, rightBottomX, rightBottomY. Вспомогательные переменные leftTop, rightTop, leftBottom, rightBottom сохраняют расстояние от этих точек до углов изображения. Для каждой точки-претендента проводится проверка по величине расстояния от каждого угла до нее:

$$leftTop = x + y$$
$$leftTopX = x \ , \ x + y < leftTop;$$
$$leftTopY = y$$

$$rightTop = (Width - x) + y$$
$$rightTopX = x \ , \ (Width - x) + y < rightTop;$$
$$rightTopY = y$$

$$leftBottom = x + (Height - y)$$
$$leftBottomX = x \ , \ x + (Height - y) < leftBottom;$$
$$leftBottomY = y$$

$$rightBottom = (Width - x) + (Height - y)$$
$$rightBottomX = x \ ,$$
$$rightBottomY = y$$

$$(Width - x) + (Height - y) < rightBottom\ .$$

Таким образом, определены координаты вершин четырех уголков по окончанию обхода изображения.

С целью исключения зависимости результата идентификации от точности позиционирования метки при захвате ее камерой в алгоритмы обработки включена процедура компенсации поворота изображения метки относительно границ кадра.

При попытке вычисления угла поворота изображения метки и последующего обратного поворота получим погрешности из-за ресурсоемких нецелочисленных вычислений. Для того, чтобы упростить вычисления и уменьшить погрешность, преобразован один из старейших алгоритмов машинной графики – алгоритм Брезенхема растеризации отрезка [94].

Оригинальная версия алгоритма определяет точки двумерного растра, подлежащие закрашиванию, для получения приближения прямой линии, заданной крайними точками с координатами (x_1, y_1) и (x_2, y_2). Основная идея алгоритма заключается в том, что одна из координат (разность по которой больше) изменяется на единицу, а изменение второй координаты зависит от величины накопленной ошибки – расстояния между действительным положением отрезка и ближайшими координатами сетки растра. Для этого вычисляются разности по формулам (4.7):

$$dx = x_2 - x_1\,,$$
$$dy = y_2 - y_1. \qquad (4.7)$$

Большая по модулю разность определяет, по какой координате будет идти дальнейший цикл вычислений. Согласно формуле прямой получаем выражения (4.8):

$$y(x) = y_1 + \left({(y_2 - y_1)}\Big/{(x_2 - x_1)}\right) * (x - x_1) = y_1 + \left({dy}\Big/{dx}\right) * (x - x_1)$$

или (4.8)

$$x(y) = x_1 + \left({(x_2 - x_1)}\Big/{(y_2 - y_1)}\right) * (y - y_1) = x_1 + \left({dx}\Big/{dy}\right) * (y - y_1)$$

Достаточно на каждом шаге изменять координату, по которой выявлена большая разность координат, на 1, а вторую оставлять прежней или изменять на 1 в зависимости от величины ошибки, изменяющейся на значение углового коэффициента (система выражений (4.9)):

$$\frac{y_2 - y_1}{x_2 - x_1} = \frac{dy}{dx} \text{ или}$$
$$\frac{x_2 - x_1}{y_2 - y_1} = \frac{dx}{dy}$$

$$y_{i+1} = y_i + Sign(dy)$$

$$x_{i+1} = \begin{cases} x_i, & e_{i+1} = e_i + \dfrac{dx}{dy} < 0.5 \\ x_i + Sign(dx), & e_{i+1} = e_i + \dfrac{dx}{dy} \geq 0.5 \end{cases}$$

$$e_{i+1} = \begin{cases} e_{i+1}, & e_{i+1} = e_i + \dfrac{dx}{dy} < 0.5 \\ e_{i+1} - 1, & e_{i+1} = e_i + \dfrac{dx}{dy} \geq 0.5 \end{cases}$$

или

$$x_{i+1} = x_i + Sign(dx)$$

$$y_{i+1} = \begin{cases} y_i, & e_{i+1} = e_i + \dfrac{dy}{dx} < 0.5 \\ y_i + Sign(dy), & e_{i+1} = e_i + \dfrac{dy}{dx} \geq 0.5 \end{cases} \quad (4.9)$$

$$e_{i+1} = \begin{cases} e_{i+1}, & e_{i+1} = e_i + \dfrac{dy}{dx} < 0.5 \\ e_{i+1} - 1, & e_{i+1} = e_i + \dfrac{dy}{dx} \geq 0.5 \end{cases}$$

Если ошибка превысит 0.5, то координата изменяется на 1, и ошибка уменьшается на 1. Целочисленным алгоритм становится при умножении значения ошибки на 2 для ее сравнения с 1 и умножении на величины dx или dy (система уравнений (4.10)).

$$y_{i+1} = y_i + Sign(dy)$$

$$x_{i+1} = \begin{cases} x_i, & e_{i+1} = e_i + 2dx < 1 \\ x_i + Sign(dx), & e_{i+1} = e_i + 2dx \geq 1 \end{cases}$$

$$e_{i+1} = \begin{cases} e_{i+1}, & e_{i+1} = e_i + 2dx < 1 \\ e_{i+1} - 1, & e_{i+1} = e_i + 2dx \geq 1 \end{cases}$$

или

$$x_{i+1} = x_i + Sign(dx)$$

$$y_{i+1} = \begin{cases} y_i, & e_{i+1} = e_i + 2dy < 1 \\ y_i + Sign(dy), & e_{i+1} = e_i + 2dy \geq 1 \end{cases} \quad (4.10)$$

$$e_{i+1} = \begin{cases} e_{i+1}, & e_{i+1} = e_i + 2dy < 1 \\ e_{i+1} - 1, & e_{i+1} = e_i + 2dy \geq 1 \end{cases}$$

Для осуществления поворота вместо вывода точки на экран, предусмотренного в оригинальной версии алгоритма, значения ее координат передаются процедуре, производящей смещение пикселей изображения по горизонтали или вертикали на разность между координатой начальной точки и выданной алгоритмом Брейзенхема. Для получения ровного изображения необходимо задать в качестве входных значений поочередно две пары точек-уголков (верхние и левые) и при этом учесть изменения координат уголков после первого преобразования.

В результате обхода исключается из рассмотрения все, что располагается за пределами ограничителей.

Требованием дальнейшей обработки изображения является определение положения цифрового кода для правильной ориентации метки. Для нахождения местоположения индивидуального (серийного) номера метки применен обход изображения, ограниченного уголками с четырех сторон, из середины каждой стороны. При этом яркость встречаемых пикселов сравнивается с порогом. Первый встреченный пиксель с яркостью ниже порога дает подозрение на то, что он является частью ограничительной рамки цифрового кода. Если процедура поиска углов, примененная для части изображения, подозреваемой на наличие цифрового кода, выделит четыре разных угла, то подтвердится его наличие. В противном случае обход продолжится.

После нахождения крайнего пикселя рамки цифрового кода станет понятно расположение метки: если код расположен под ней, то она правильно ориентирована, в остальных случаях для обеспечения правильной ориентации необходимо осуществить поворот изображения на 90, 180 или 270 градусов в зависимости от расположения кода. Из изображения правильно ориентированной мишени с цифровым кодом последний выделяется в отдельное изображение и удаляется из исходного.

Затем попиксельным обходом определяется местонахождение мишени. В результате все, что находится вне мишени, удаляется, и остаются два изображения – мишени и кода.

В полученном изображении находим крайние точки мишени и удаляем часть изображения, находящегося за ее пределами, сохраняя размер мишени для последующей записи (рис. 4.2).

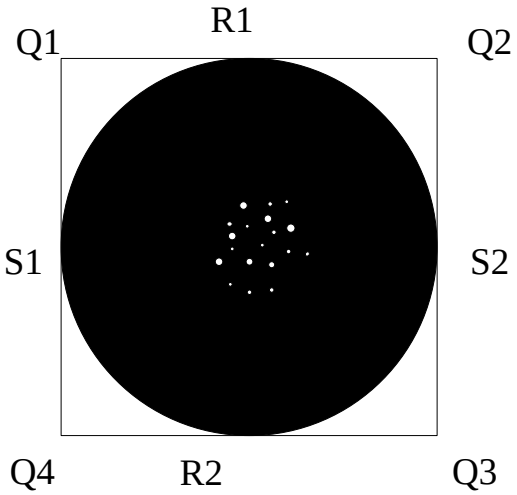


Рисунок 4.2 – Изображение мишени

Для упрощения дальнейшего обхода мишени в поисках отверстий заполняем углы вокруг мишени черным цветом, используя алгоритм затравки по отрезкам. С целью осуществления процесса заливки с затравкой в программе использован алгоритм короеда. Свое название он получил вследствие последовательного «выедания» – попиксельного закрашивания области, подлежащей заливке [94]. Эта область может быть задана в виде многоугольника. В разработанной программе она определяется цветом границы. В программе используется модификация алгоритма: на каждой итерации закрашивается не один пиксель, а строка. В качестве структуры данных используется стек с упорядоченным набором элементов, поддерживающий операции добавления и извлечения элемента. Заполнению подлежали области Q1R1S1, Q2R2S2, Q3R3S3, Q4R4S4.

После получения четких контуров светлых и темных областей изображения автоматизированная система идентификации переходит к

кодированию информации метки. Для поиска идентификаторов (в их качестве приняты признаки метки – количество отверстий, координаты их центров масс и размеры как удовлетворяющие требованиям к их устойчивости, оригинальности, однозначной передачи информации о свойствах метки) производится обход изображения. При обнаружении отверстия (его цвет – белый) запускается процедура его обработки. В ходе ее работы отверстие перекрашивается методом затравки (для исключения повторного расчета его размеров при дальнейшем обходе). Для этого применен алгоритм короеда с 4-связной областью.

Также рассчитываются площадь отверстия в пикселях и находится его центр масс – геометрическая точка, характеризующая распределение масс в системе отверстия [102].

Известны следующие способы определения координат центров масс твердых тел, расположенных на плоскости:

- Аналитический метод производится путем интегрирования.

При невозможности разбить плоское однородное тело на конечное число частей с известными положениями их центров тяжести координаты центра масс тела x_c и y_c рассчитываются по следующим формулам:

$$x_c = \frac{S_x}{A}, y_c = \frac{S_y}{A},$$

$$I_x = \iint_D xdxdy, \qquad (4.11)$$

$$I_y = \iint_D ydxdy,$$

где $A = \iint_D dxdy$ – площадь области D [103],

S_x, S_y – статические моменты тела относительно координатных осей.

- Метод симметрии может применяться при наличии у однородного тела плоскости, или оси, или центра симметрии. В этом случае его центр масс находится соответственно либо в плоскости симметрии, либо на оси симметрии, либо в центре симметрии.

- Разбиение. Сложную и асимметричную фигуру разбивают на конечное число частей таким образом, чтобы для каждой из них положение центра тяжести и площадь были бы известны (формулы (3.12)):

$$x_c = \frac{\sum_{i=1}^{n} A_i x_i}{\sum_{i=1}^{n} A_i} = \frac{A_1 x_1 + A_2 x_2 + A_3 x_3 + \ldots}{A_1 + A_2 + A_3 + \ldots},$$

$$y_c = \frac{\sum_{i=1}^{n} A_i y_i}{\sum_{i=1}^{n} A_i} = \frac{A_1 y_1 + A_2 y_2 + A_3 y_3 + \ldots}{A_1 + A_2 + A_3 + \ldots}, \quad (4.12)$$

где $A_1, A_2, A_3, \ldots$ - площади простейших фигур, вписанных в контур, $x_1, x_2, x_3, \ldots$, $y_1, y_2, y_3, \ldots$ - координаты центров тяжести простейших фигур контура относительно выбранных осей координат [104].

Аналитический способ определения площади фигуры заключается в том, что по известным координатам x_i, y_i (i = 1, 2, 3, … n) вершин замкнутого многоугольника с применением формул геометрии, тригонометрии и аналитической геометрии можно определить площадь закрашенного участка [104]:

$$A = \frac{1}{2}\sum x_i (y_{i+1} - y_{i-1}) \text{ или}$$

$$A = \frac{1}{2}\sum y_i (x_{i-1} - x_{i+1}),$$

где i=1, 2, 3, …n. $S = \frac{1}{2}\sum x_i (y_{i+1} - y_{i-1})$.

В разработанной программе принят факт, что прожженные электрическим разрядом стохастически расположенные отверстия изображения метки состоят из пикселей. Площадь каждого пикселя равна 1, поэтому центр масс каждого отверстия, учитывая формулы (3.11), (3.12) рассчитывается по формулам (3.13):

$$x_c = \frac{\sum_{i=1}^{n} x_i}{n},$$

$$y_c = \frac{\sum_{i=1}^{n} y_i}{n}, \quad (4.13)$$

где x_i, y_i – координаты пикселей, попавших в область отверстия,

n – количество пикселей отверстия.

В результате обхода изображения система получает и сохраняет информацию о количестве отверстий, координатах их центров масс и производит быструю сортировку по размерам отверстий (рис. 4.3, 4.4).

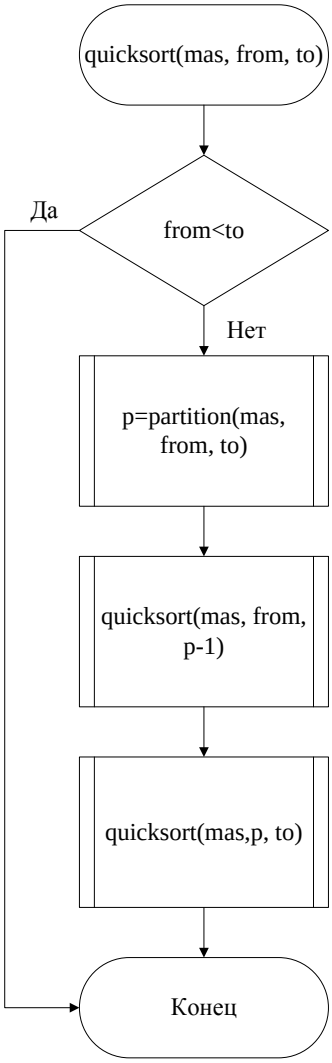


Рисунок 4.3 – Блок-схема процедуры быстрой сортировки

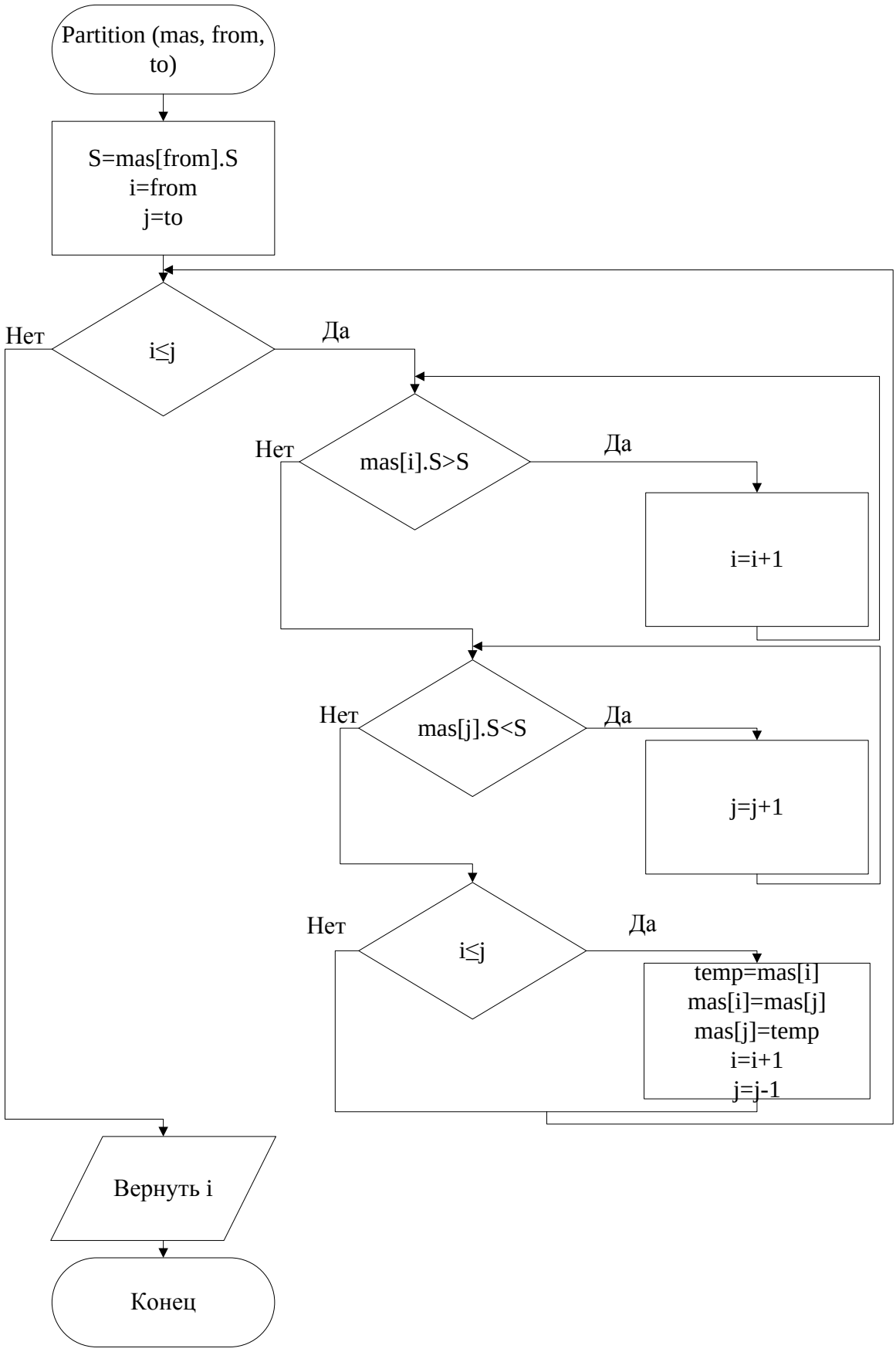


Рисунок 4.4 – Вспомогательная процедура для быстрой сортировки

Принцип работы сортировки заключается в том, что сначала в качестве опорного элемента выбирается размер первого отверстия. Затем, при вызове вспомогательной процедуры (рис. 4.4) происходит сравнение всех остальных размеров с размером опорного элемента.

В результате образуются два подмассива, один из которых содержит элементы, размеры которых больше размера опорного элемента, в другом подмассиве – элементы меньшего размера. Далее в каждом подмассиве выбирается свой опорный элемент, и процедура повторяется до тех пор, пока в подмассиве не останется один элемент. Таким образом, происходит сортировка элементов по размеру отверстий для определенного порядка занесения информации в QR-код.

4.2 Алгоритмы кодирования информации изображения метки в QR-код

Идентификационные признаки стохастически нанесенной метки, полученные после прохождения ряда подготовительных этапов (рис. 4.5), должны быть подвергнуты дальнейшей обработке: нанесению в виде QR-кода на бумажный носитель поблизости от метки.

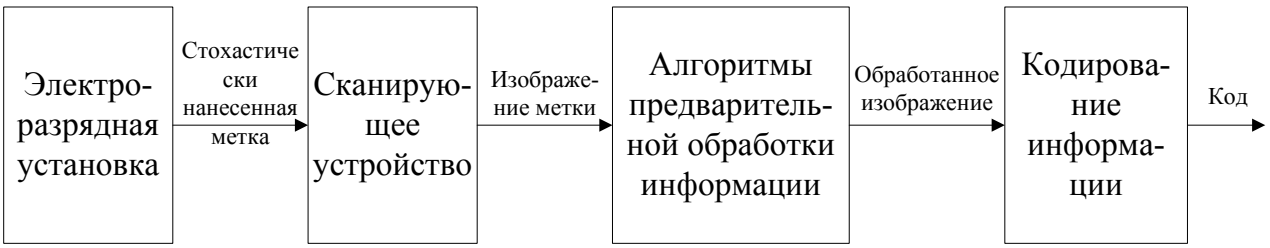


Рисунок 4.5 – Подсистема подготовки и кодирования информации [75]

Существует четыре основных способа кодирования информации в QR-код [105]:

- цифровое кодирование;
- кодирование Кандзи;
- байтовое кодирование;
- алфавитно-цифровая кодировка.

Из возможных видов кодировок QR-кодов выбираем алфавитно-цифровую кодировку. Этот выбор обусловлен тем, что кроме кодирования цифровой информации (например, размер отверстий метки, прожженных электрическим разрядом) возникает необходимость шифрования букв: для бумажных (денежных, в том числе) документов в качестве исходной информации может служить буквенное обозначение номера серии. Алфавит кодирования состоит из 45 символов, значения которых приведены в таблице 4.1. Каждая пара символов преобразуется в 11-битное число по правилу:

$$45 \cdot a + b,$$

где a и b – соответственно нечетный и четный символы. Непарный нечетный символ преобразуется в 6-битное число. Полученные числа составляют последовательность бит информации.

Таблица 4.1 – Значения символов в буквенно-цифровом кодировании [105]

0	1	2	3	4	5	6	7	8	9
0	1	2	3	4	5	6	7	8	9
A	B	C	D	E	F	G	H	I	J
10	11	12	13	14	15	16	17	18	19
K	L	M	N	O	P	Q	R	S	T
20	21	22	23	24	25	26	27	28	29
U	V	W	X	Y	Z	Пробел	$	%	*
30	31	32	33	34	35	36	37	38	39
+	-	.	/	:					
40	41	42	43	44					

После выбора вида кодировки необходимо задаться уровнем коррекции, зависящим от принятого допустимого уровня повреждения QR-кода. На этом уровне код еще можно восстановить, применив код Рида-Соломона с восьмибитным кодовым словом [105]. Существуют 4 уровня коррекции: L-уровень допускает не больше 7% повреждений, M-уровень – 15%, Q-уровень – 25%, H-уровень – 30%. При большем уровне повреждения кода можно записать

меньшее количество информации. В качестве допустимого уровня повреждения QR-кода выбираем уровень M, так как он является наиболее распространенным.

При выбранном уровне коррекции в коде записывается полезная и служебная информация (в битах), максимальное количество которой зависит от номера версии QR-кода (табл. 4.2).

Таблица 4.2 – Максимальное количество информации в зависимости от версии и уровня коррекции [105]

	Номер версии									
Уровень коррекции	1	2	3	4	5	6	7	8	9	10
L	152	272	440	640	864	1088	1248	1552	1856	2192
M	128	224	352	512	688	864	992	1232	1456	1728
Q	104	176	272	384	496	608	704	880	1056	1232
H	72	128	208	288	368	480	528	688	800	976
	11	12	13	14	15	16	17	18	19	20
L	2592	2960	3424	3688	4184	4712	5176	5768	6360	6888
M	2032	2320	2672	2920	3320	3624	4056	4504	5016	5352
Q	1440	1648	1952	2088	2360	2600	2936	3176	3560	3880
H	1120	1264	1440	1576	1784	2024	2264	2504	2728	3080
	21	22	23	24	25	26	27	28	29	30
L	7456	8048	8752	9392	10208	10960	11744	12248	13048	13880
M	5712	6256	6880	7312	8000	8496	9024	9544	10136	10984
Q	4096	4544	4912	5312	5744	6032	6464	6968	7288	7880
H	3248	3536	3712	4112	4304	4768	5024	5288	5608	5960
	31	32	33	34	35	36	37	38	39	40
L	14744	15640	16568	17528	18448	19472	20528	21616	22496	23648
M	11640	12328	13048	13800	14496	15312	15936	16816	17728	18672
Q	8264	8920	9368	9848	10288	10832	11408	12016	12656	13328
H	6344	6760	7208	7688	7888	8432	8768	9136	9776	10208

Определим номер версии QR-кода по количеству информации в битах, которую он должен будет содержать. Количество информации в символах С:

$$\mathrm{C} = \mathrm{C}_{\text{н}} + \mathrm{C}_{\text{д}} + 1 + nC_{\text{от}},$$

где $C_{\text{н}}$ – количество символов серийного номера (максимум принимаем 16),

$\mathrm{C}_{\text{д}}$ – количество символов диаметра метки (максимум принимаем 4),

1 – пробел между ними,

n – количество отверстий (до 100),

$\mathrm{C}_{\text{от}}$ – количество символов, описывающих одно отверстие.

$$\mathrm{C}_{\text{от}} = \mathrm{C}_{\text{от1}} + \mathrm{C}_{\text{от2}} + \mathrm{C}_{\text{от3}} + 3,$$

где $\mathrm{C}_{\text{от1}}$ – количество символов в значении координаты x центра масс отверстия (4),

$\mathrm{C}_{\text{от2}}$ – количество символов в значении координаты y центра масс отверстия (4),

$\mathrm{C}_{\text{от3}}$ – количество символов в значении площади отверстия (4),

3 – пробелы между данными.

$\mathrm{C}_{\text{от}} = 4 + 4 + 4 + 3 = 15$, $\mathrm{C} = 16 + 4 + 1 + 100 * 15 = 1521$ символ.

Так как каждая пара символов кодируется 11 битами, а последний одиночный символ – 6 битами, получаем

$$(1520/2) * 11 + 1 * 6 = 8366 \text{ бит}.$$

Тогда при уровне коррекции М выбираем версию кода – 26.

Запись способа кодировки требует 4 бит служебного поля и для буквенно-цифрового кодирования имеет значение 0010 (для цифрового кодирования – 0001, для побайтового кодирования – 0100). Требуемая длина поля количества данных определяется по таблице 3.3 в зависимости от версии QR-кода и способа кодирования и дописываются недостающие нули.

Таким образом, получаем запись информации, выполненную в следующей последовательности: способ кодирования – количество данных – данные.

Далее последовательность байт разбиваем на блоки (табл. 4.4).

Таблица 4.3 – Длина поля количества данных [105]

	Версия QR-кода		
Способ кодирования	1-9	10-26	27-40
Цифровое	10 бит	12 бит	14 бит
Буквенно-цифровое	9 бит	11 бит	13 бит
Побайтовое	8 бит	16 бит	16 бит

Таблица 4.4 – Определение количества блоков [105]

	Номер версии									
Уровень коррекции	1	2	3	4	5	6	7	8	9	10
L	1	1	1	1	1	2	2	2	2	4
M	1	1	1	2	2	4	4	4	5	5
Q	1	1	2	2	4	4	6	6	8	8
H	1	1	2	4	4	4	5	6	8	8
	11	12	13	14	15	16	17	18	19	20
L	4	4	4	4	6	6	6	6	7	8
M	5	8	9	9	10	10	11	13	14	16
Q	8	10	12	16	12	17	16	18	21	20
H	11	11	16	16	18	16	19	21	25	25
	21	22	23	24	25	26	27	28	29	30
L	8	9	9	10	12	12	12	13	14	15
M	17	17	18	20	21	23	25	26	28	29

(*Продолжение табл. 4.4*)

Q	23	23	25	27	29	34	34	35	38	40
H	25	34	30	32	35	37	40	42	45	48
	31	32	33	34	35	36	37	38	39	40
L	16	17	18	19	19	20	21	22	24	25
M	31	33	35	37	38	40	43	45	47	49
Q	43	45	48	51	53	56	59	62	65	68
H	51	54	57	60	63	66	70	74	77	81

В нашем случае получим 23 блока (версия 26, уровень коррекции M).

Для создания байтов коррекции к каждому блоку данных применяется алгоритм Рида-Соломона [106]. Количество создаваемых байтов коррекции, приходящееся на один блок, определяется по таблице 4.5.

Таблица 4.5 – Определение числа байтов коррекции в зависимости от версии и уровня коррекции [106]

	Номер версии									
Уровень коррекции	1	2	3	4	5	6	7	8	9	10
L	7	10	15	20	26	18	20	24	30	18
M	10	16	26	18	24	16	18	22	22	26
Q	13	22	18	26	18	24	18	22	20	24
H	17	28	22	16	22	28	26	26	24	28
	11	12	13	14	15	16	17	18	19	20
L	20	24	26	30	22	24	28	30	28	28
M	30	22	22	24	24	28	28	26	26	26
Q	28	26	24	20	30	24	28	28	26	30
H	24	28	22	24	24	30	28	28	26	28
	21	22	23	24	25	26	27	28	29	30

(*Продолжение табл. 4.5*)

L	28	28	30	30	26	28	30	30	30	30
M	26	28	28	28	28	28	28	28	28	28
Q	28	30	30	30	30	28	30	30	30	30
H	30	24	30	30	30	30	30	30	30	30
	31	32	33	34	35	36	37	38	39	40
L	30	30	30	30	30	30	30	30	30	30
M	28	28	28	28	28	28	28	28	28	28
Q	30	30	30	30	30	30	30	30	30	30
H	30	30	30	30	30	30	30	30	30	30

Для версии 26 и уровня коррекции M получим 28 байтов коррекции. Для дальнейшего кодирования воспользуемся таблицей 4.6.

Согласно таблице для версии 26, уровня коррекции M, 28 байтов коррекции получен генерирующий многочлен

168, 223, 200, 104, 224, 234, 108, 180, 110, 190, 195, 147, 205, 27, 232, 201, 21, 43, 245, 87, 42, 195, 212, 119, 242, 37, 9, 123

Для дальнейшего вычисления данных в алгоритме Рида-Соломона применяется поле Галуа длиной 256 (табл. 4.7) и обратное поле Галуа (табл. 4.8) [107].

Для осуществления следующего цикла следует провести подготовку массива. Его длина принимается равной суммарному значению количества байтов текущего блока и числа байтов коррекции. В начале массива записываются байты текущего блока, в конце помещаются нули.

Таблица 4.6 – Генерирующие многочлены [107]

Количество байт коррекции	Генерирующий многочлен
7	87, 229, 146,149, 238, 102, 21
10	251, 67, 46, 61, 118, 70, 64, 94, 32, 45
13	74, 152, 176, 100, 86, 100, 106, 104, 130, 218, 206, 140, 78
15	8, 183, 61, 91, 202, 37, 51, 58, 58, 237, 140, 124, 5, 99, 105
16	120, 104, 107, 109, 102, 161, 76, 3, 91, 191, 147, 169, 182, 194, 225, 120
17	43, 139, 206, 78, 43, 239, 123, 206, 214, 147, 24, 99, 150, 39, 243, 163, 136
18	215, 234, 158, 94, 184, 97, 118, 170, 79, 187, 152, 148, 252, 179, 5, 98, 96, 153
20	17, 60, 79, 50, 61, 163, 26, 187, 202, 180, 221, 225, 83, 239, 156, 164, 212, 212, 188, 190
22	210, 171, 247, 242, 93, 230, 14, 109, 221, 53, 200, 74, 8, 172, 98, 80, 219, 134, 160, 105, 165, 231
24	173, 125, 158, 2, 103, 182, 118, 17, 145, 201, 111, 28, 165, 53, 161, 21, 245, 142, 13, 102, 48, 227, 153, 145, 218, 70
28	168, 223, 200, 104, 224, 234, 108, 180, 110, 190, 195, 147, 205, 27, 232, 201, 21, 43, 245, 87, 42, 195, 212, 119, 242, 37, 9, 123
30	41, 173, 145, 152, 216, 31, 179, 182, 50, 48, 110, 86, 239, 96, 222, 125, 42, 173, 226, 193, 224, 130, 156, 37, 251, 216, 238, 40, 192, 180

Таблица 4.7 – Поле Галуа

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	2	4	8	16	32	64	128	29	58	116	232	205	135	19	38
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
76	152	45	90	180	117	234	201	143	3	6	12	24	48	96	192
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
157	39	78	156	37	74	148	53	106	212	181	119	238	193	159	35
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
70	140	5	10	20	40	80	160	93	186	105	210	185	111	222	161
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
95	190	97	194	153	47	94	188	101	202	137	15	30	60	120	240
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
253	231	211	187	107	214	177	127	254	225	223	163	91	182	113	226
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
217	175	67	134	17	34	68	136	13	26	52	104	208	189	103	206
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
129	31	62	124	248	237	199	147	59	118	236	197	151	51	102	204
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
133	23	46	92	184	109	218	169	79	158	33	66	132	21	42	84
144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
168	77	154	41	82	164	85	170	73	146	57	114	228	213	183	115
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
230	209	191	99	198	145	63	126	252	229	215	179	123	246	241	255
176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
227	219	171	75	150	49	98	196	149	55	110	220	165	87	174	65

(*Продолжение таблицы 4.7*)

192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
130	25	50	100	200	141	7	14	28	56	112	224	221	167	83	166
208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
81	162	89	178	121	242	249	239	195	155	43	86	172	69	138	9
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
18	36	72	144	61	122	244	245	247	243	251	235	203	139	11	22
240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255
44	88	176	125	250	233	207	131	27	54	108	216	173	71	142	1

Таблица 4.8 – Обратное поле Галуа

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
-	0	1	25	2	50	26	198	3	223	51	238	27	104	199	75
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
4	100	224	14	52	141	239	129	28	193	105	248	200	8	76	113
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
5	138	101	47	225	36	15	33	53	147	142	218	240	18	130	69
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
29	181	194	125	106	39	249	185	201	154	9	120	77	228	114	166
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
6	191	139	98	102	221	48	253	226	152	37	179	16	145	34	136
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
54	208	148	206	143	150	219	189	241	210	19	92	131	56	70	64
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
30	66	182	163	195	72	126	110	107	58	40	84	250	133	186	61
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
202	94	155	159	10	21	121	43	78	212	229	172	115	243	167	87
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
7	112	192	247	140	128	99	13	103	74	222	237	49	197	254	24

(*Продолжение таблицы 4.8*)

144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
227	165	153	119	38	184	180	124	17	68	146	217	35	32	137	46
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
55	63	209	91	149	188	207	205	144	135	151	178	220	252	190	97
176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
242	86	211	171	20	42	93	158	132	60	57	83	71	109	65	162
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
31	45	67	216	183	123	164	118	196	23	73	236	127	12	111	246
208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
108	161	59	82	41	157	85	170	251	96	134	177	187	204	62	90
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
203	89	95	176	156	169	160	81	11	245	22	235	122	117	44	215
240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255
79	174	213	233	230	231	173	232	116	214	244	234	168	80	88	175

Затем из массива выбирается первый элемент, оставшиеся элементы сдвигаются на ячейку влево, в качестве последнего элемента записывается нуль. По таблице 4.8 находим значение, соответствующее значению первого выбранного элемента (соответствующее значение располагается под величиной выбранного элемента). Затем производим суммирование каждого значения генерирующего многочлена с величиной, определенной по таблице 4.8. В случае превышения одного из полученных суммарных значений числа 254 используется его остаток при делении на 255. Далее для каждого суммарного значения генерирующего многочлена определяется соответствующее ему значение (располагается под ним) по таблице 4.8. Затем проводится операция побитового сложения по модулю 2 каждого значения, полученного из таблицы 4.8, со значениями подготовленного массива.

Количество повторов данного цикла равно числу байтов данных текущего блока. При равенстве нулю значения первого элемента массива все эти действия не производятся.

Первые несколько байтов массива, таким образом, являются байтами коррекции.

Далее последовательность байтов (из блоков исходных данных и коррекции) кодируется в QR-код (рис. 4.6).

Рисунок 4.6 – Составляющие QR-кода [84]

Поисковые узоры и расположенные по полю в зависимости от номера версии более мелкие синхронизирующие квадраты – выравнивающие узоры служат для нормализации размера и ориентации изображения.

Координаты расположения выравнивающих узоров представлены в таблице 4.9. Началом системы отсчета является точка – верхний левый угол с координатами (0; 0). Для удобства представления в таблице приведена одна из координат каждого выравнивающего узора [108].

Таблица 4.9 – Координаты расположения выравнивающих узоров

1	2	3	4	5	6	7	8	9	10
-	18	22	26	30	34	6,22,38	6,24,42	6,26,46	6,28,50
11	12	13	14	15	16	17	18	19	20
6, 30,54	6, 32, 58	6, 34, 62	6, 26, 46,66	6, 26, 48,70	6, 26, 50,74	6, 30, 54, 78	6, 30, 56, 82	6, 30, 58, 86	6, 34, 62, 90
21	22	23	24	25	26	27	28	29	30
6,28, 50,72, 94	6,26, 50,74, 98	6,30, 54,78, 102	6,28, 54,80, 106	6,32, 58,84, 110	6,30, 58,86, 114	6, 34, 62, 90, 118	6,26, 50, 74, 98,122	6,30, 54, 78, 102, 126	6, 26, 52, 78, 104, 130
31	32	33	34	35	36	37	38	39	40
6, 30, 56, 82, 108, 134	6, 34, 60, 86, 112, 138	6, 30, 58, 86, 114, 142	6, 34, 62, 90, 118, 146	6, 30, 54,78, 102, 126, 150	6, 24, 50,76, 102, 128, 154	6, 28, 54, 80, 106, 132, 158	6, 32, 58, 84, 110, 136, 162	6, 26, 54, 82, 110, 138, 166	6, 30, 58, 86, 114, 142, 170

Для версии 26 запись 6, 30, 58, 86, 114 (табл. 4.9) означает следующие места расположения центров модулей:

(6, 6), (6, 30), (6, 58), (6, 86), (6, 114), (30, 6), (30, 30), (30, 58), (30, 86), (30, 114), (58, 6), (58, 30), (58, 58), (58, 86), (58, 114), (86, 6), (86, 30), (86, 58), (86, 86), (86, 114), (114, 6), (114, 30), (114, 58), (114, 86), (114, 114).

Для выполнения требования об отсутствии наложения выравнивающих узоров на поисковые узоры (начиная с седьмой версии) из рассмотрения должны быть исключены следующие координаты:

(6, 6), (6, 114), (114, 6).

Для определения кода версии необходимо воспользоваться таблицей 4.10, в которой представлены коды для версий с номерами 7 – 40.

В нашем случае для версии 26 ее код выглядит следующим образом:

110101 101111 011100.

Таблица 4.10 – Коды версии в зависимости от ее номера [108]

Версия	7	8	9	10	11	12	13	14	15
Код версии	000010 011110 100110	010001 011100 111000	110111 011000 000100	101001 111110 000000	001111 111010 111100	001101 100100 011010	101011 100000 100110	110101 000110 100010	010011 000010 011110
Версия	16	17	18	19	20	21	22	23	24
Код версии	011100 010001 011100	111010 010101 100000	100100 110011 100100	000010 110111 011000	000000 101001 111110	100110 101101 000010	111000 001011 000110	011110 001111 111010	001101 001101 100100
Версия	25	26	27	28	29	30	31	32	33
Код версии	101011 001001 011000	110101 101111 011100	010011 101011 100000	010001 110101 000110	110111 110001 111010	101001 010111 111110	001111 010011 000010	101000 011000 101101	001110 011100 010001
Версия	34	35	36	37	38	39	40		
Код версии	010000 111010 010101	110110 111110 101001	110100 100000 001111	010010 100100 110011	001100 000010 110111	101010 000110 001011	111001 000100 010101		

На рисунке 4.7 изображен код версии 26, помещенный в QR-коде. Информация об идентификационных признаках метки заносится в свободное пространство холста, разбитое на столбцы шириной два модуля. Полосы синхронизации и выравнивающие узоры необходимо пропустить. Начало заполнения данных – правый нижний угол правого крайнего столбца, направления заполнения – справа налево, снизу вверх (1 – черный модуль, 0 – белый). При достижении верха столбца данные заносятся в следующий столбец, расположенный левее в направлении справа налево, сверху вниз. При заполнении этого столбца маршрут занесения данных аналогичен направлениям заполнения первого столбца. Таким образом, все данные заполняют пространство холста. При недостатке данных в пространство заносят нулевые модули.

а) б)

Рисунок 4.7 – Код версии 26 в QR-коде: а) слева от верхнего правого узора; б) над нижним левым поисковым узором

Код маски и уровня коррекции (рис. 4.6) служит для инвертирования цвета модуля коррекции данных для исключения появления артефактов, мешающих процессу декодирования. В таблице 4.11 приведены коды маски в зависимости от их номера и уровня коррекции [108].

Для определения необходимости инвертирования цвета проводят проверку координат каждого модуля коррекции данных по правилам, приведенным в таблице 4.12 [108]. В этой таблице имеются обозначения:

mod – остаток от деления,

/ – целочисленное деление.

Условием инвертирования цвета модуля является равенство нулю результата таблицы.

Выбор номера маски является интерактивным процессом: необходимо для каждого изображения метки сгенерировать QR-код с наложением каждой из восьми масок (от нулевого до седьмого номера).

Таблица 4.11 – Код маски в зависимости от ее номера и уровня коррекции

Уровень коррекции	Номер маски	Код
L	0	111011111000100
	1	111001011110011
	2	111110110101010
	3	111100010011101
	4	110011000101111
	5	110001100011000
	6	110110001000001
	7	110100101110110
M	0	101010000010010
	1	101000100100101
	2	101111001111100
	3	101101101001011
	4	100010111111001
	5	100000011001110
	6	100111110010111
	7	100101010100000
Q	0	011010101011111
	1	011000001101000
	2	011111100110001
	3	011101000000110
	4	010010010110100
	5	010000110000011

(*Продолжение таблицы 4.11*)

	6	010111011011010
	7	010101111101101
H	0	001011010001001
	1	001001110111110
	2	001110011100111
	3	001100111010000
	4	000011101100010
	5	000001001010101
	6	000110100001100
	7	000100000111011

Определение оптимального номера маски происходит по правилу штрафных баллов [101]:

2. При нахождении на основном поле не менее пяти модулей одного цвета по горизонтали или вертикали начисляются штрафные баллы, количество которых равно уменьшенной на два модуля длине этого участка (минимальное значение – 3 балла).

3. Каждый квадрат модулей одного цвета размером 2x2 добавляет 3 балла.

4. При обнаружении по вертикали или горизонтали следующего чередования цветов модулей – черный, белый, черный, черный, черный, белый, черный – начисляются 40 баллов.

5. Определяется процентное соотношение черных и белых модулей основного поля. Граничным считается соотношение 55% черных модулей на 45% белых модулей. При отклонении процентного состава черных модулей в меньшую сторону от 55% добавляются 10 баллов за дополнительный процент вариации.

Таблица 4.12 – Правило проверки модуля коррекции данных в зависимости от номера маски

Номер маски	Номер маски в двоичном представлении	Маска
0	000	$(X+Y)\ mod\ 2$
1	001	$X\ mod\ 2$
2	010	$Y\ mod\ 3$
3	011	$(X+Y)\ mod\ 3$
4	100	$(X/2+Y/3)\ mod\ 2$
5	101	$(X \cdot Y)mod2 + (X \cdot Y)mod3$
6	110	$\big((X \cdot Y)mod2 + (X \cdot Y)mod3\big)mod2$
7	111	$\big((X \cdot Y)mod3 + (X \cdot Y)mod2\big)mod2$

Определенные по пунктам 1 – 4 баллы суммируются, и выбирается номер маски, обеспечивающей минимальное количество штрафных баллов. Код маски и уровня коррекции записывается в предусмотренные стандартом места QR-кода по горизонтали и вертикали (дублирование производится для возможности восстановления утерянной информации).

В результате проделанных процедур сгенерированы QR-коды изображений меток, содержащие данные – значения идентификационных признаков: серийный номер метки, ее диаметр, количество полученных электрическим разрядом отверстий на мишени, координаты центров масс отверстий (по двум осям – *X* и *Y*), размеры отверстий (их площади в пикселях). На рисунке 4.8 приведен QR-код одной из стохастически созданных меток.

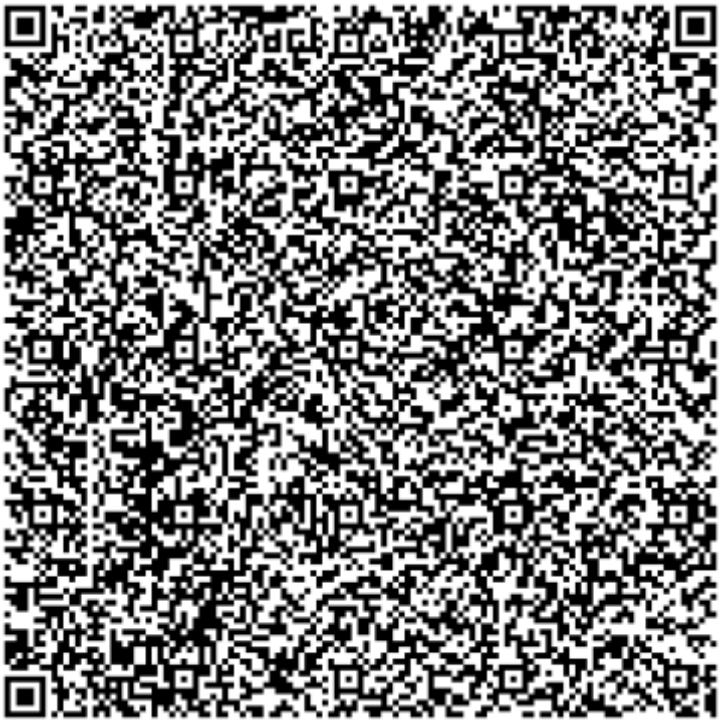


Рисунок 4.8 – Сгенерированный QR-код

4.3 Алгоритмы распознавания информации

На рисунке 4.9 показана разработанная подсистема идентификации объекта, содержащая этапы распознавания информации, хранящейся в QR-коде [75]. Идентификация производится сопоставлением информации метки с данными, записанными в виде кода.

Для осуществления сравнения сканированной информации метки со значениями идентификаторов, хранящимися в коде, разработаны алгоритмы, использующие методы компьютерной графики.

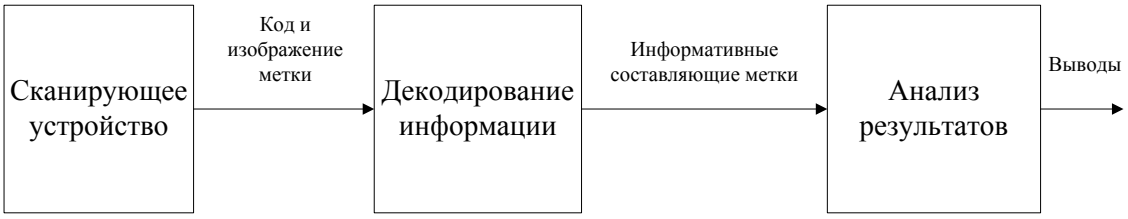


Рисунок 4.9 – Подсистема распознавания информации

Для идентификации используется принцип отображения множеств (4.14):

$$x \in A, y \in B,$$
$$f(x) = y, \qquad (4.14)$$

где A – множество меток; x – набор признаков метки; B – множество QR-кодов меток; y – QR-код, содержащий набор признаков, конкретной метки; f – функция отображения – создания QR-кода, содержащего признаки метки. f^{-1} – процедура проверки соответствия набора признаков, зашифрованных в QR-коде, набору признаков проверяемой метки. При выполнении условия

$$f^{-1}(y) = x$$

идентификация метки считается успешной. В обратном случае, при

$$f^{-1}(y) \neq x$$

метка «чужая».

Полученное с помощью сканирующего устройства изображение метки подвергается процедуре предварительной подготовки. Для этого применяются вышеописанные алгоритмы, используемые при подготовке изображения к кодированию.

Затем, с помощью процедуры поиска углов, автоматизированная система идентификации определяет местонахождение QR-кода на изображении. Аналогично ранее описанным алгоритмам обработки изображения метки производится компенсация поворота кода.

После осуществления бинаризации определяется размер ячейки с помощью попиксельного обхода изображения. Далее QR-код считывается из изображения побитно благодаря известному размеру ячейки. Информация заносится в битовый двумерный массив в зависимости от того, каких пикселей в квадрате больше: белых или черных.

Декодирование информации, записанной в QR-коде, производится в порядке, обратном кодированию. Происходит считывание информации об уровнях коррекции ошибок и шаблоне маски, после чего шаблон маски

применяется ко всем битам данных. При необходимости осуществляется процедура исправления ошибок.

Из полученного варианта кода считывается служебная и полезная информация в том порядке, в каком она была записана. Таким образом, после установления режима (буквенно-цифровой), становится известным размер мишени на образце, с которого получен QR-код (он необходим для масштабирования), количество отверстий, координаты их центров, размеры отверстий, серийный номер метки. Первым сравнивается серийный номер, так как в случае его несовпадения дальнейшая проверка не понадобится. Далее, при проходе в цикле по массиву отверстий метки, описанных в QR-коде, проводятся следующие проверки:

1) находится ли на проверяемой метке отверстие в том месте, указание о координатах центра которого содержится в QR-коде (с учетом разницы размеров изображений проверяемой метки и метки из кода);

2) если отверстие нашлось, определяется его центр и площадь (как и при их определении для записи в QR-код) и с учетом масштаба определяется, совпадает ли центр с центром отверстия из QR-кода и одинаковой ли эти отверстия площади.

Таким образом, к выводу готовятся три значения: количество попаданий в отверстие (hit), количество совпадающих центров отверстий и количество отверстий, совпадающих по площадям.

Принцип работы автоматизированной системы можно проследить по ее блок-схеме, приведенной на рисунке 4.10.

Вначале, применяя к изображению метки алгоритмы предварительной обработки, система переводит его из цветовой модели RGB в YUV. Далее, проводя пороговую бинаризацию, система добивается четкого разграничения светлых и темных областей.

Затем при выборе действия «Создать QR-код» (это действие выполняется при обработке изображения новой метки и отсутствии QR-кода с информацией

об ее идентификационных признаках) система приступает к его созданию: определяет идентификаторы метки, запоминает их значения и заносит всю необходимую информацию в QR-код.

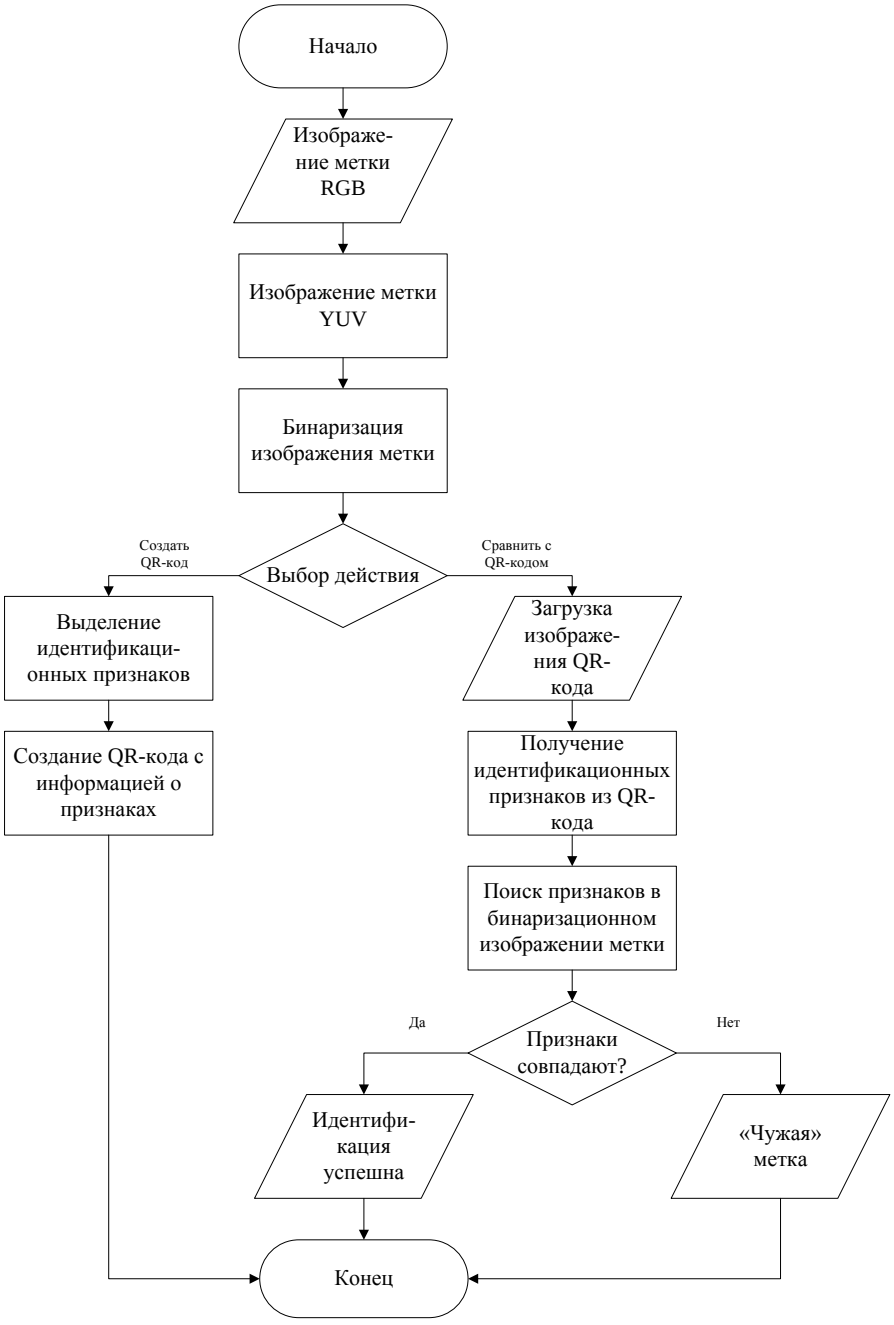


Рисунок 4.10 – Блок-схема автоматизированной системы идентификации стохастически созданных меток [109]

При необходимости сравнения изображения метки с QR-кодом документа (нанесенного поблизости от метки или документа-оригинала) выбирается действие «Сравнить с QR-кодом». Тогда происходит загрузка изображения QR-

кода, с помощью процедуры декодирования значения идентификаторов извлекаются из кода. Путем обработки сфотографированного изображения метки система осуществляет поиск и считывание величин идентификационных признаков. При совпадении значений (при условии не превышения допустимого порога отклонений) автоматизированная система выдает результат об успешной идентификации. В противном случае, приходит к выводу о наличии «чужой» метки.

Таким образом, разработанная модель процесса идентификации и созданная на ее основе автоматизированная система позволяет производить отождествление бумажного документа по метке, стохастически нанесенной электроразрядным способом. Для подтверждения этого произведены экспериментальные исследования надежности и адекватности нового метода идентификации.

Выводы по четвертой главе

1. В качестве начального этапа разработки модели идентификации невоспроизводимых, стохастически нанесенных меток применены алгоритмы предварительной обработки их изображений для исключения влияния на результаты идентификации нерегулярной структуры бумажного носителя и неоднородности окраски мишени. Для получения полутонового изображения метки произведена конверсия из модели RGB в YUV.

В работе применено построение сегментации с помощью порога – сравнение значения яркости каждого пикселя изображения с пороговым значением.

Для определения месторасположения мишени на изображении применен попиксельный обход по вертикали и горизонтали. С целью исключения зависимости результата идентификации от точности позиционирования метки при захвате ее камерой в алгоритмы обработки включена процедура

компенсации поворота изображения метки относительно границ кадра: преобразование оригинальной версии алгоритма Брезенхема растеризации отрезка.

Для нахождения местоположения индивидуального (серийного) номера метки применен обход изображения, ограниченного уголками с четырех сторон, из середины каждой стороны. При неправильной ориентации метки (нахождение кода не под ней) автоматизированная система осуществит поворот изображения на 90, 180 или 270 градусов в зависимости от расположения кода.

Полученный цифровой код выделяется в отдельное изображение. Затем определяется местонахождение мишени. В результате попиксельного обхода остаются два изображения – мишени и кода.

Для четкого разграничения светлых (отверстия) и черных областей (фон) проведена бинаризация – операция порогового разделения по методу Оцу.

После получения четких контуров светлых и темных областей изображения автоматизированная система идентификации переходит к кодированию информации метки. В качестве идентификаторов приняты признаки метки – индивидуальный номер, количество отверстий, координаты их центров масс и размеры. Все идентификаторы удовлетворяют требованиям к их устойчивости, оригинальности, однозначно передают информацию о свойствах метки, и совокупность признаков позволяет сделать выводы о результатах процедуры по выявлению тождественности метки.

В результате обхода изображения система обнаруживает отверстие и запускает процедуру его обработки. В ходе ее выполнения отверстие перекрашивается методом затравки для исключения его повторной обработки. Определяются площадь отверстия в пикселях и его центр масс, для которых с помощью алгоритма быстрой сортировки устанавливается определенный порядок занесения их информации в QR-код.

2. В процессе диссертационного исследования были сгенерированы QR-коды, хранящие значения идентификаторов стохастически нанесенных меток.

Технология написания кода была немного изменена для будущего сокрытия информации о значениях идентификаторов метки от злоумышленников. Из возможных видов выбрана алфавитно-цифровая кодировка: для бумажных документов в качестве исходной информации может служить буквенное обозначение номера серии. В качестве допустимого уровня повреждения кода выбран уровень M для обеспечения записи большого объема информации. Расчетным путем получен номер версии кода – 26. Информация записывается в последовательности: способ кодирования – количество данных – данные. Определено количество создаваемых байтов коррекции, для создания которых к каждому блоку данных применен алгоритм Рида-Соломона. Блоки исходных данных и блоки коррекции объединены в один поток байт.

3. На основе разработанной модели обработки изображений метки, кодирования и распознавания информации создана система идентификации, обеспечивающая полностью автоматизированный режим работы. Автоматизированная система позволяет произвести идентификацию изображения метки на основе сравнения ее с QR-кодом. С этой целью применены алгоритмы распознавания информации, использующие обязательные поля QR-кода для декодирования.

5 ЭКСПЕРИМЕНТАЛЬНЫЕ ИССЛЕДОВАНИЯ ЗАЩИЩЕННОСТИ БУМАЖНЫХ ДОКУМЕНТОВ ОТ ПОДДЕЛКИ ПРИ ИСПОЛЬЗОВАНИИ РАЗРАБОТАННОГО МЕТОДА ИДЕНТИФИКАЦИИ

5.1 Анализ результатов сравнения изображений меток с QR-кодами их эталонов

Собранная электроразрядная установка представляла собой два электрода, один из которых был плоским для удобства расположения бумажного носителя, форма второго – острие с углом заточки 45^{o} (рис. 3.8). Материал электродов – медь. Расстояние между электродами – 10 мм. К электродам был подключен высоковольтный источник. Величина максимального пробивного напряжения – 50 кВ. Газовые разряды производились в воздухе, атмосферное давление менялось в пределах 740 – 760 мм рт. ст., температура воздуха – $20\pm3℃$.

Автоматизированная система идентификации разработана в программной среде Visual Studio 2010, язык программирования C#.

В экспериментах на документ 1 электроразрядным способом наносили уникальную метку 2 в виде совокупности стохастически расположенных отверстий. На рисунке 5.1 показан алгоритм работы автоматизированной системы идентификации, запатентованный автором совместно с научным руководителем [110].

На бумажный документ дополнительно был нанесен серийный номер 3, QR-код 4, содержащий буквенно-цифровые коды, серийный номер, размер метки, количество, координаты и размер отверстий. Использование двумерного штрихкода для хранения эталонных значений, содержащихся в получаемых наборах перфораций, позволяет производить запись большого объема

информации и отказаться от применения баз данных, работа с которыми была бы крайне затруднительной.

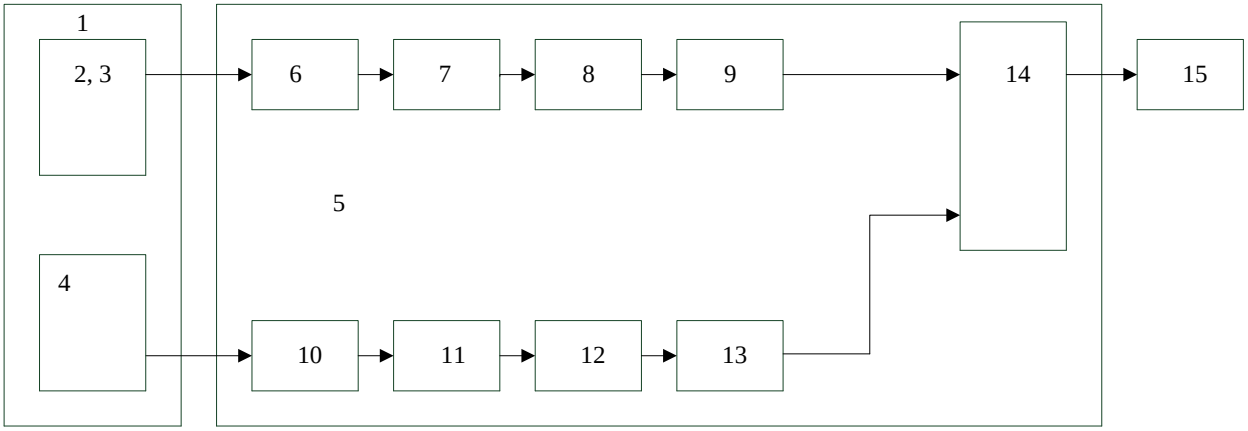


Рисунок 5.1 – Последовательность операций по выявлению подлинности документа

Последовательность операций по проверке индивидуальности документа производилась следующим образом:

1. Сканирующее и обрабатывающее устройство 5 производило сканирование метки 2 и серийного номера 3 и сохранение их изображений в памяти устройства 6. В качестве такого устройства можно применить один из серийно выпускаемых смартфонов, планшетов, наладонных компьютеров (PDA). Устройство должно быть оснащено цифровой камерой требуемого разрешения и набором специальных прикладных программ для считывания и обработки изображений. Также в качестве устройства можно применить персональный компьютер с подключенным к нему сканером. В экспериментах фотографии меток были получены с помощью камер обычных смартфонов торговых марок iPhone и Sony.

2. Изображение метки 2, хранящееся в памяти устройства 6, подвергалось сегментации (на рисунке 5.1 это процедура 7).

3. Бинаризация изображения метки – процедура 8.

4. Выделение идентификаторов из полученного в предыдущей процедуре изображения метки – процедура 9.

5. Процедура 10 – сканирование двумерного кода 4, обеспечивает его считывание и сохранение в памяти устройства 5.

6. Бинаризация и сегментация двумерного кода 4, несущего информацию о подлинной метке 2 (процедура 11).

7. Процедура 12 – выделение байтов информации двумерного кода 4 и при необходимости исправление его ошибок.

8. Выделение идентификаторов из двумерного кода – процедура 13.

9. Процедура 14 – сравнение идентификаторов метки 2 и двумерного кода 4. Если они совпадают с определенной точностью, то документ признается подлинным.

10. Процедура 15 – решение о подлинности документа. Реализуется в виде сообщения, формируемого устройством 5.

В ходе проведения серии экспериментов были получены результаты идентификации бумажных документов.

Первый этап экспериментальных исследований был посвящен подтверждению возможности применения нового метода идентификации и анализу качества процесса, производимого разработанной автоматизированной системой. Каждая метка, полученная с помощью электроразрядной установки, проходила процедуру изготовления QR-кода ее эталонного изображения. Для этого сканированное изображение метки подвергалось предварительной обработке системой идентификации. Значения идентификаторов, определенные системой, помещались в QR-код, наносимый на бумажный носитель (рис. 5.2).

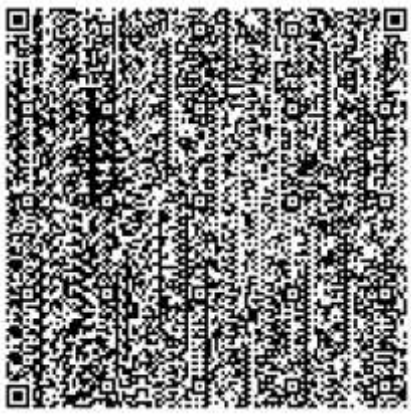


Рисунок 5.2 – QR-код одной из меток, созданный автоматизированной системой

В ходе диссертационного исследования учитывалось, что при установлении истинности документа (документа об образовании и повышении квалификации, накладной на товар, удостоверения личности, сертификата) у проверяющего субъекта может отсутствовать сканирующее устройство высокой чувствительности. Поэтому особенно важно обеспечить надежность идентификации изображения метки, сделанного камерой обычного сотового телефона, при сравнении с QR-кодом ее эталонного изображения.

Для получения фотографий меток были выбраны два смартфона разных торговых марок (iPhone и Sony) средней ценовой категории, один из них был в употреблении два года, другой – четыре года. Фотографирование меток проводилось в течение одного часа при одинаковых условиях внешней среды: одна и та же степень освещенности. Камерами этих телефонов, не приспособленных для профессионального использования, были получены фотографии каждой метки (при подсветке) для сравнения с QR-кодами их эталонных изображений (рис. 5.3).

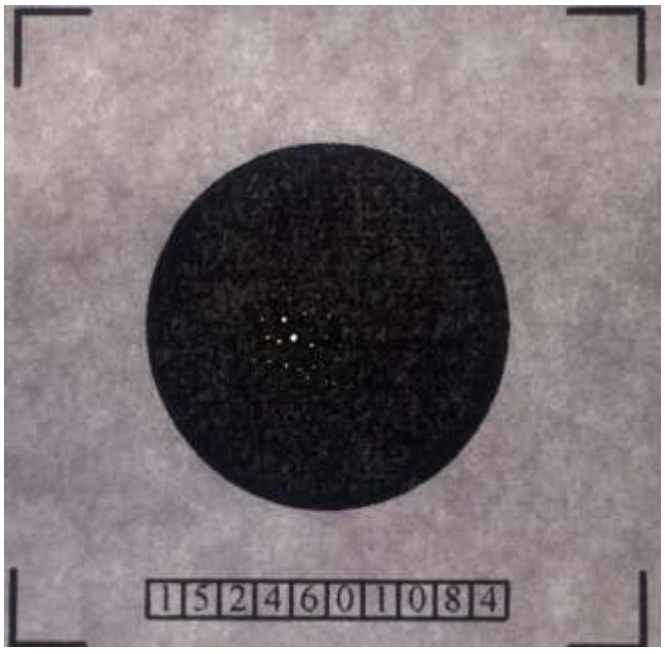


Рисунок 5.3 – Фотография метки

Автоматизированной системой была произведена обработка фотографий, осуществлено определение значений идентификаторов (с учетом масштабирования) и сравнение их с информацией QR-кода эталонных

изображений. Один из результатов сравнения значений идентификационных признаков, взятых из изображения метки, с информацией QR-кода приведен на рисунке 5.4.

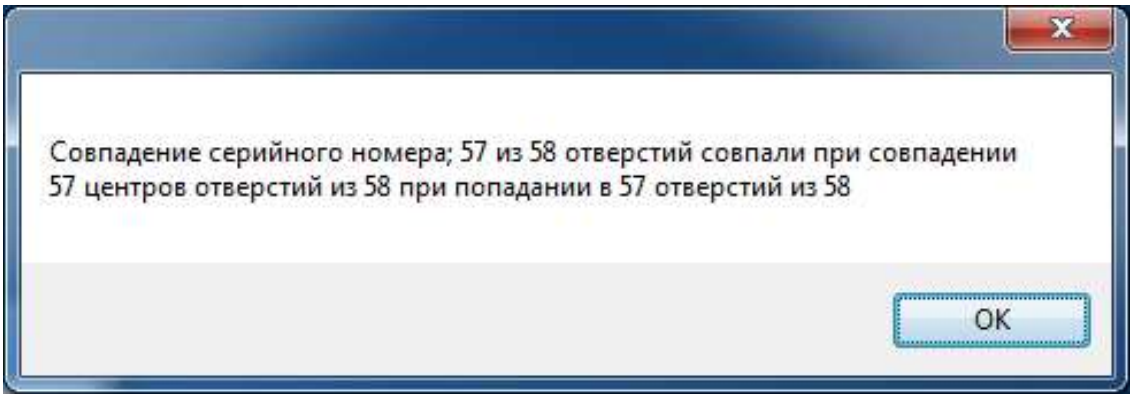


Рисунок 5.4 – Результат сравнения фотографии метки с QR-кодом ее эталонного изображения

Построение диаграммы, изображенной на рисунке 5.5, произведено по результатам работы автоматизированной системы. Выбранные метки имели различное количество отверстий, прожженных электроразрядным способом. По горизонтальной оси отложены номера столбцов – результатов идентификации, по вертикальной оси рисунка – значение числа нанесенных отверстий.

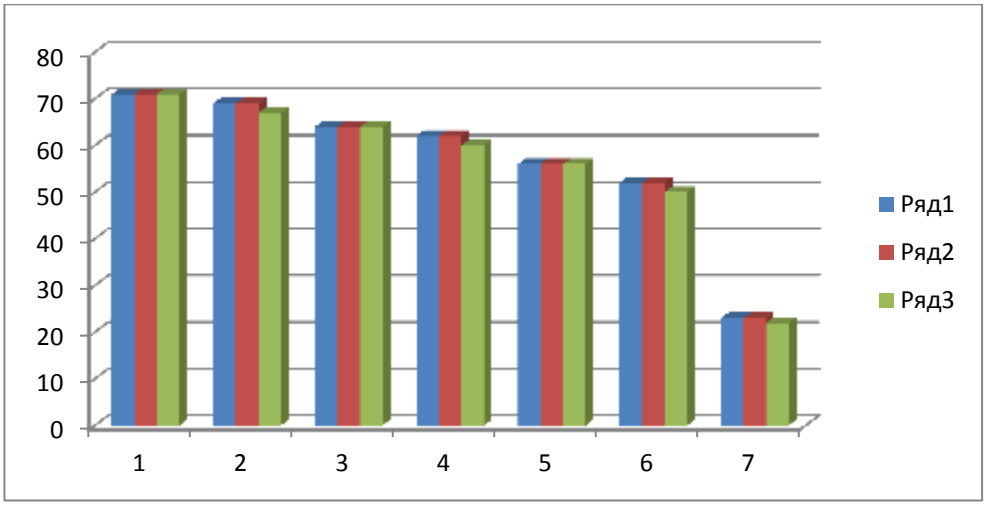


Рисунок 5.5 – Диаграммы результатов идентификации фотографий меток с QR-кодами их эталонных изображений

Каждый столбец диаграммы состоит из трех составляющих и иллюстрирует результаты отождествления метки по совпадению значений ее

идентификаторов: количества нанесенных отверстий на мишени (составляющая – Отверстие), координат центров масс отверстий (составляющая – Центр), размеров отверстий (составляющая – Размер).

Столбцы 1, 3, 5 иллюстрируют результаты сравнения фотографий меток, сделанных камерой одного смартфона, 2, 4, 6, 7 – другого телефона. При этом величина отклонения сравниваемых значений от полного совпадения не превысила допустимого порога – 5%.

Результаты проведенных исследований, таким образом, доказали возможность и успешность проведения автоматизированной системой процедуры идентификации, несмотря на среднюю чувствительность камер смартфонов.

Для проведения статистики ошибок первого рода необходимо задаться массивом выборки:

$$M_{FRR} = i \cdot n, \tag{5.1}$$

где i – количество меток, n – число фотографий одной и той же метки.

Массив выборки для определения ошибок второго рода определяется по формуле:

$$M_{FAR} = i \cdot (i-1) \cdot (n+1). \tag{5.2}$$

Порог сравнения t_{com} может принимать значения от нуля до единицы. При величине $t_{com} = 0$ все изображения метки, не только «свои», но и «чужие», становятся «своими». В этом случае *FRR*=0, *FAR*=100%. При $t_{com} = 1$ все сравнения изображений меток с QR-кодом документа-оригинала будут ниже порога чувствительности и тогда *FAR*=0, *FRR*=100% [104]. Вероятность ошибок первого рода определяются по формуле:

$$FRR = \frac{m_{FRR}}{M_{FRR}} \cdot 100\%,$$

где m_{FRR} – количество ошибок первого рода (число изображений метки, «не узнанных» системой).

Вероятность ошибок второго рода можно вычислить следующим образом:

$$FAR = \frac{m_{FAR}}{M_{FAR}} \cdot 100\%,$$

где m_{FAR} – количество ошибок второго рода (число «чужих» изображений метки, признанных системой своими).

График зависимости вероятности ошибок первого рода от порога чувствительности автоматизированной системы представлен на рисунке 5.6.

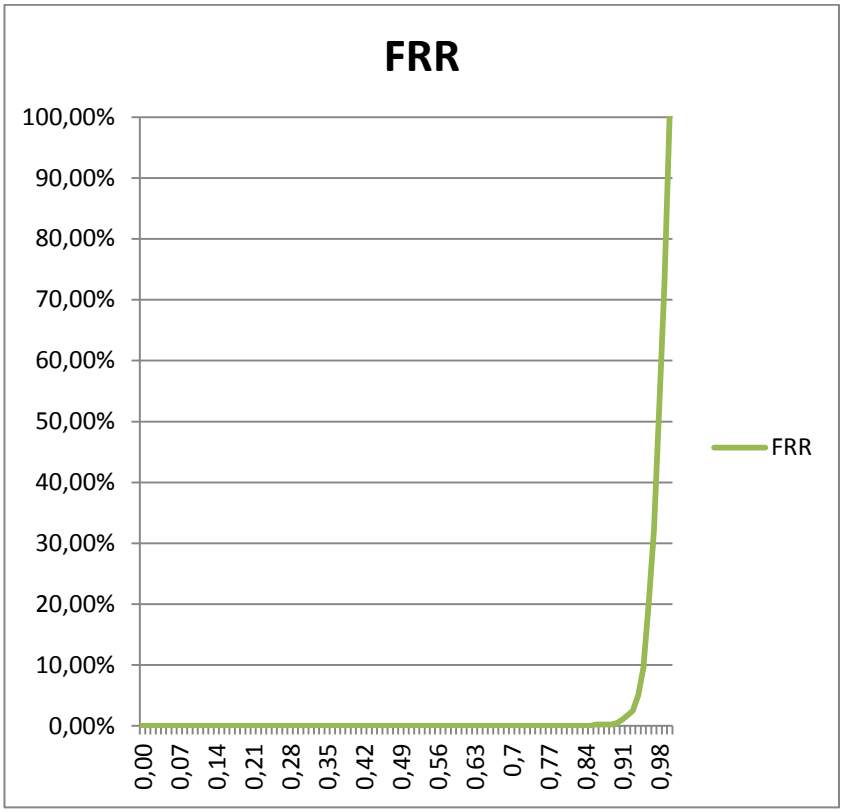


Рисунок 5.6 – Определение вероятности появления ошибок первого рода при обработке фотографий меток, сделанных в условиях хорошей освещенности

По оси абсцисс нанесены значения порога чувствительности автоматизированной системы от 0 до 1, по оси ординат – вероятность отказа от признания «своей» метки за метку документа – оригинала. При $i = 400$, $n = 10$, массив выборки по формуле (5.2):

$$M_{FRR} = 400 \cdot 10 = 4000.$$

При пороге $0{,}85 < t_{com} \leq 1$ появляются ошибки идентификации первого рода.

Для оценки надежности работы автоматизированной системы определим ошибки идентификации первого рода в условиях влияния факторов внешней среды на получение качественного изображения метки и последующей ее идентификации.

5.2 Анализ влияния факторов внешней среды на процесс идентификации метки, полученной стохастическим электроразрядным способом

Для проведения анализа результатов работы автоматизированной системы по идентификации изображения метки в качестве факторов внешней среды были выбраны:

- степень освещенности метки при получении фотографии ее изображения;
- длительность периода эксплуатации бумажного документа с нанесенными на него меткой и QR-кодом.

При проведении данного этапа экспериментальных исследований предполагалось, что для осуществления процедуры идентификации бумажных документов может быть задействовано сканирующее устройство различной степени чувствительности. Следовательно, возможность применения камеры обычного смартфона для идентификации изображения метки с QR-кодом ее эталонного изображения подтвердит надежность работы автоматизированной системы и нового метода идентификации.

Поэтому каждая метка была сфотографирована в различное время суток, в разные дни при пасмурной и ясной погоде. Степень освещенности, таким образом, варьировалась, качество фотографий изображений метки также сильно отличалось.

Вывод о тождественности изображения метки при сравнении ее с QR-кодом производился на основе анализа совпадающих значений совокупности

идентификаторов – серийного номера метки, количество прожженных электрическим разрядом отверстий на мишени, координаты центров масс отверстий, размеры отверстий.

Полное совпадение значений или небольшое их отклонение (в пределах 5 %) позволяет судить об успешности процедуры идентификации меток. Если значения идентификационных признаков изображения метки значительно отличаются от их записанных в QR-коде величин, то можно сделать вывод об отрицательном результате тождественности объектов.

При проведении экспериментальных исследований для фотографирования меток была использована камера обычного сотового телефона среднего класса, бывшего в употреблении два года, не приспособленная для профессионального фотографирования.

В ходе работы автоматизированной системы были сгенерированы QR-коды эталонных изображений множества меток. Полученные при различной степени освещенности фотографии каждой из меток также были обработаны автоматизированной системой. Для определения надежности работы автоматизированной системы идентификация метки производилась по трем критериям – совпадение количества отверстий, координат их центров и их площадям. Совпадение по серийному номеру не учитывалось. Формула определения массива выборки принимает значение:

$$M_{FRR} = i \cdot (n + m), \tag{5.3}$$

где m – дополнительное количество фотографий метки, сделанное при пасмурной погоде камерами телефонов.

При $i = 400$, $n = 10$, $m = 12$ массив выборки по формуле (5.3):

$$M_{FRR} = 400 \cdot (10 + 12) = 8800.$$

Для иллюстрации работы автоматизированной системы по идентификации изображений метки, полученных в условиях различной освещенности, в диссертационном исследовании отобрана метка с серийным номером 8126701080. На рисунке 5.7 приведен QR-код эталонного изображения

метки, созданный автоматизированной системой. На рисунке 5.8 показана фотография метки, служащая в качестве оригинала для сравнения ее идентификационных признаков с идентификаторами фотографий этой же метки, произведенными в условиях разной степени освещенности.

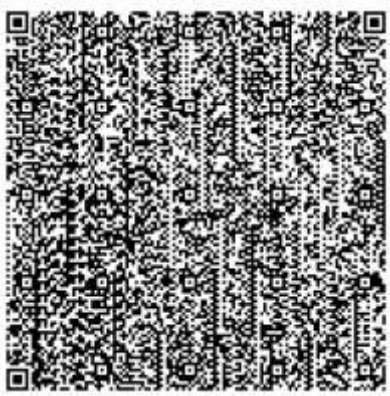


Рисунок 5.7 – QR-код метки № 8126701080, созданный автоматизированной системой

Рисунок 5.8 – Фотография метки [90]

В ходе проведения исследования автоматизированная система выдавала результаты сравнения значений идентификационных признаков, взятых из фотографий метки, с величинами идентификаторов QR-кода оригинала. Один из результатов сравнения с фотографиями метки приведен на рисунке 5.9. По результатам идентификации метки с серийным номером 8126701080, произведенным автоматизированной системой, была построена диаграмма, представленная на рисунке 5.10. Такие же показатели характерны и для меток с другими серийными номерами. По горизонтальной оси отложены номера

столбцов – результатов идентификации, по вертикальной оси диаграммы – значение количества нанесенных отверстий.

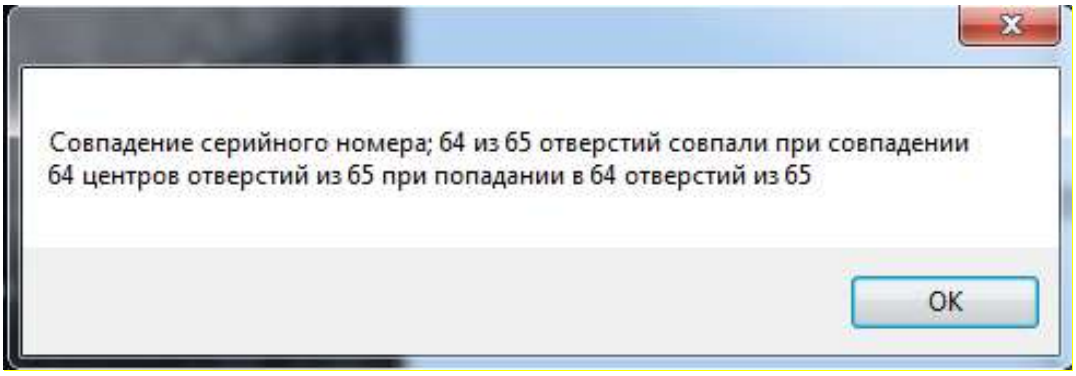


Рисунок 5.9 – Результат сравнения фотографии метки с QR-кодом ее эталонного изображения

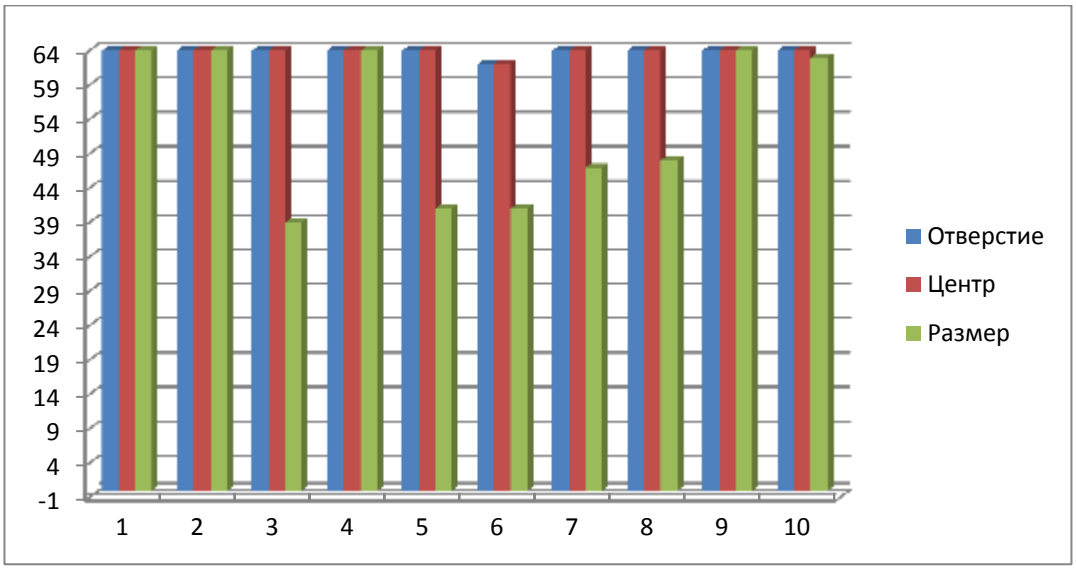


Рисунок 5.10 – Диаграммы результатов идентификации фотографий меток с QR-кодами их эталонных изображений

Столбцы 1, 2, 4, 9, 10 отражают результаты проведения процедуры идентификации фотографий метки, полученные в ясные дни при яркой степени освещенности.

Столбцы 3, 5, 6, 7, 8 построены по показателям процедуры идентификации метки, сфотографированной в пасмурные дни при разной степени освещенности.

Показатели столбцов 7 и 8 характерны для идентификации, проведенной в дневное время пасмурных суток, результаты столбцов 3, 5, 6 получены при сравнении с фотографиями, сделанными в вечерние часы.

Из проведенного исследования видно, что степень освещенности оказывает существенное влияние на результаты идентификации: невысокое качество полученных при слабой освещенности фотографий искажает величину размеров отверстий. Если по координатам центров и количеству отверстий идентификация проходит успешно при работе автоматизированной системы с фотографиями меток, сделанных даже в условиях невысокой степени освещенности, то по идентификатору – площадь отверстий наблюдается отклонение от совпадения значений, превышающее допустимый порог. Из этого следует, что данный идентификатор весьма зависим от фактора внешней среды – степени освещенности метки при получении фотографии ее изображения.

По результатам исследований построен график зависимости вероятности ошибки первого рода от порога чувствительности автоматизированной системы (рис. 5.11). По оси абсцисс нанесены значения порога чувствительности автоматизированной системы от 0 до 1, по оси ординат – вероятность отказа от признания «своей» метки за метку документа – оригинала.

По графику рисунка 5.11 видно, что ошибки идентификации первого рода появляются при пороге чувствительности $0{,}2 < t_{com} \leq 1$.

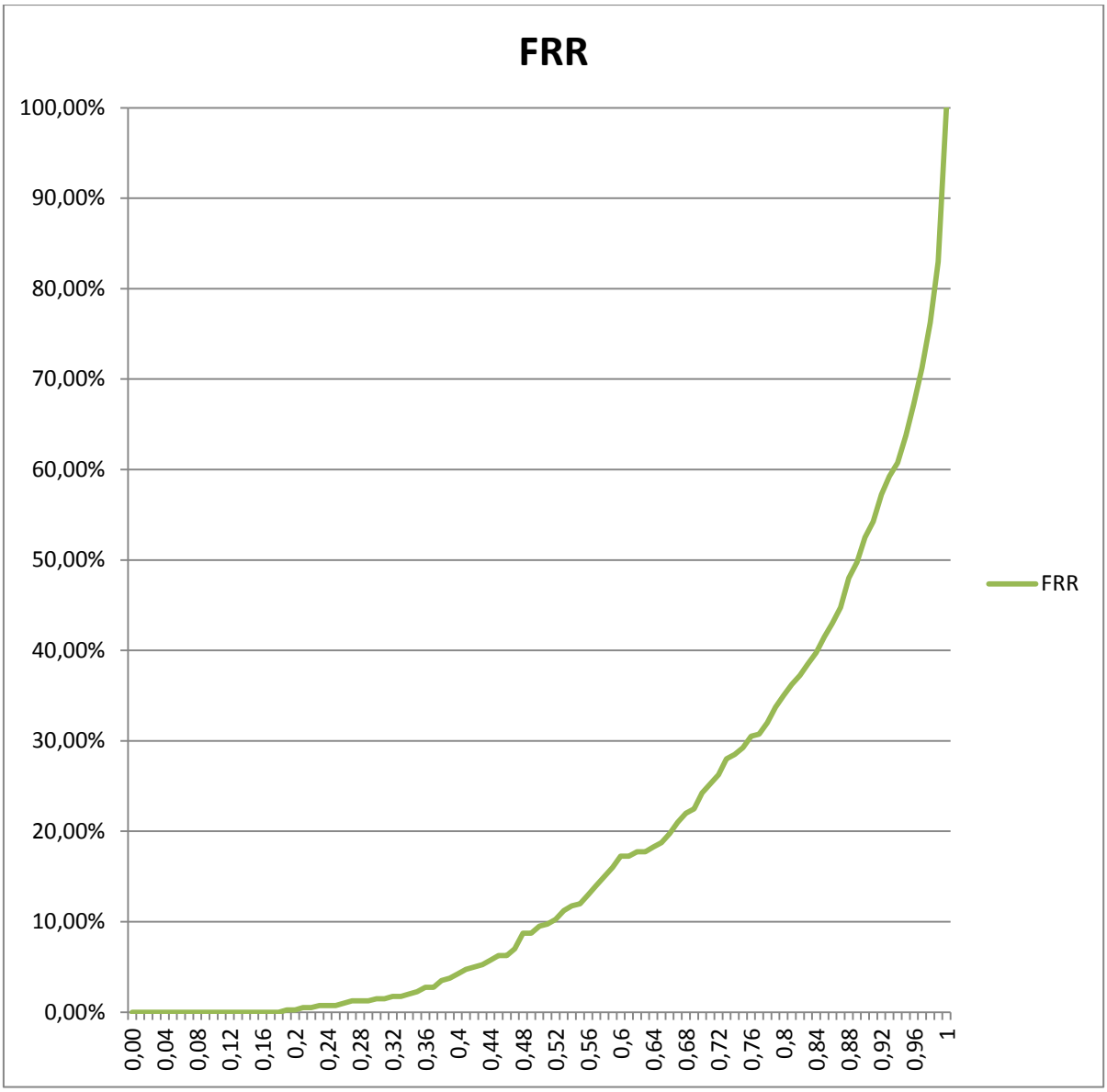


Рисунок 5.11 – Определение вероятности появления ошибок первого рода при обработке фотографий меток, сделанных в разных условиях освещенности

Кроме того, на данном этапе экспериментальных исследований было выявлено влияние еще одного фактора внешней среды – длительности периода эксплуатации бумажного документа с нанесенными на него меткой и QR-кодом – на надежность процедуры идентификации, осуществляемой автоматизированной системой.

На каждом бумажном носителе с помощью электроразрядной установки прожигалась метка и поблизости от нее автоматизированная система наносила QR-код со считанной ею и зашифрованной информацией о значениях идентификационных признаков метки.

В начале исследования были сделаны фотографии каждой метки камерой сотового телефона и произведена генерация QR-кодов меток-оригиналов, изображения которых были получены сканирующим устройством.

Все носители в течение полугода активно эксплуатировались: принимали участие в демонстрации результатов работы автоматизированной системы идентификации, проводимых на заседаниях кафедры и конференциях.

Полученные электроразрядным способом метки подвергались тщательному рассмотрению коллегами, контакту (метки трогали руками).

После шестимесячного периода активной эксплуатации были сделаны фотографии каждой метки, и автоматизированной системой произведено сравнение информации изображения метки с QR-кодом ее оригинала.

На рисунках 5.12 – 5.18 в виде диаграмм представлены результаты сравнения идентификаторов изображений метки, полученных из фотографий, сделанных в начале эксперимента, с изображениями метки, полученными после полугодового периода эксплуатации. При этом для иллюстрации были выбраны метки с разным количеством нанесенных отверстий – от 23 до 88. По горизонтальной оси отложены номера столбцов, по вертикальной оси – количество нанесенных электроразрядным способом отверстий метки.

На этих рисунках каждый столбик изображен в виде двух составляющих:

- левая составляющая – показатель, полученный после обработки и идентификации изображения метки до эксплуатации;
- правая составляющая содержит значение идентификатора, выданное системой в результате обработки фотографии, сделанной после полугодового периода эксплуатации, и сравнения с QR-кодом.

Столбец под номером 1 иллюстрирует совпадение с информацией QR-кода – оригинала по количеству нанесенных отверстий на мишени. Столбец под номером 2 отражает количество отверстий, у которых совпали координаты центров масс отверстий по сравнению с оригиналом. Столбец 3 показывает

число отверстий, у которых одинаковые с оригиналом площади соответствующих отверстий.

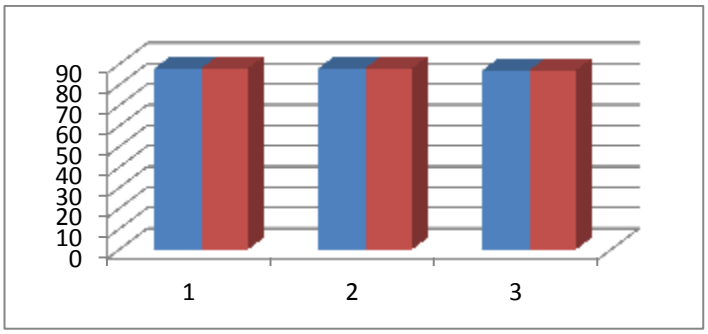


Рисунок 5.12 – Диаграмма результатов сравнения фотографий метки с числом отверстий 88 с ее QR-кодом – оригиналом

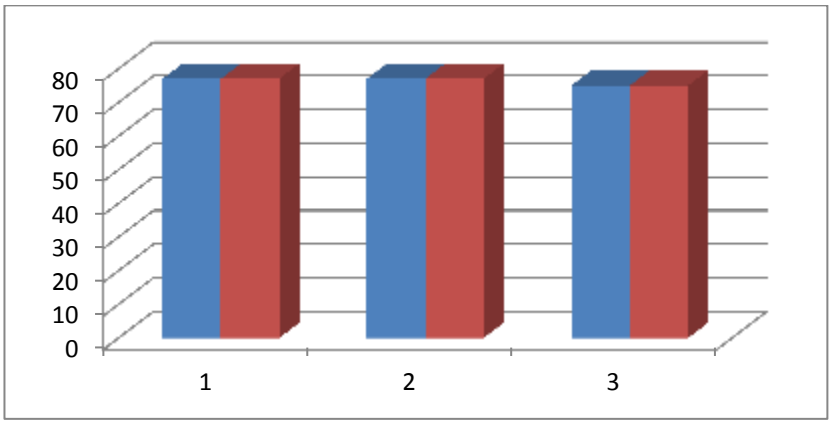


Рисунок 5.13 – Диаграмма результатов сравнения фотографий метки с числом отверстий 77 с ее QR-кодом – оригиналом

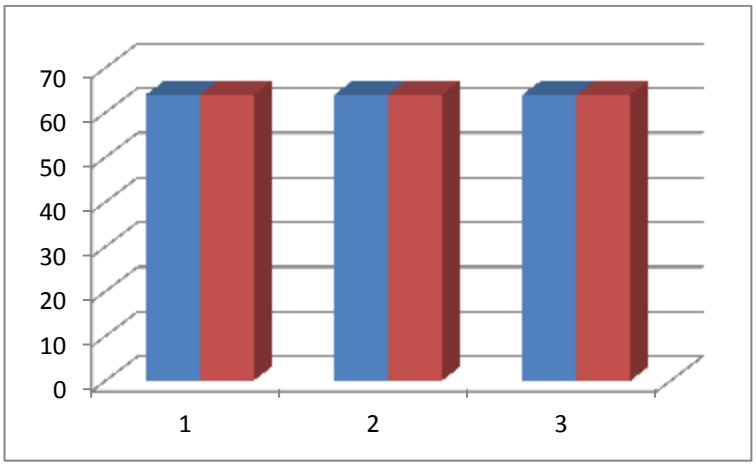


Рисунок 5.14 – Диаграмма результатов сравнения фотографий метки с числом отверстий 64 с ее QR-кодом – оригиналом

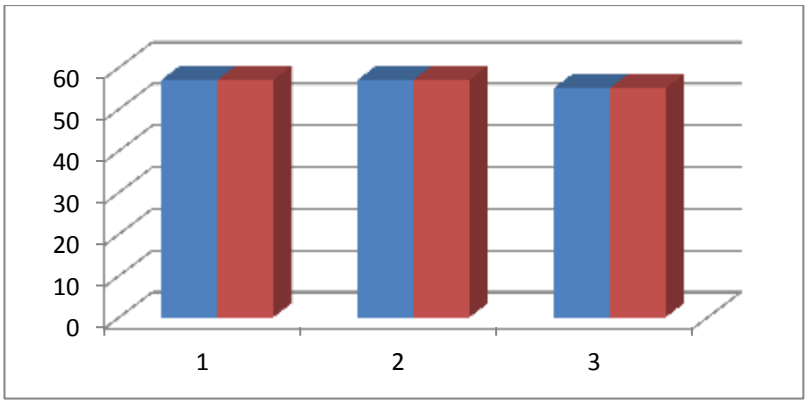


Рисунок 5.15 – Диаграмма результатов сравнения фотографий метки с числом отверстий 57 с ее QR-кодом – оригиналом

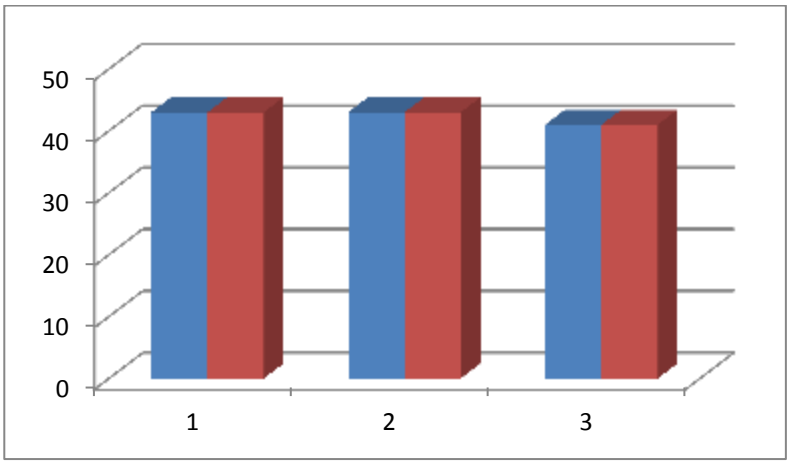


Рисунок 5.16 – Диаграмма результатов сравнения фотографий метки с числом отверстий 43 с ее QR-кодом – оригиналом

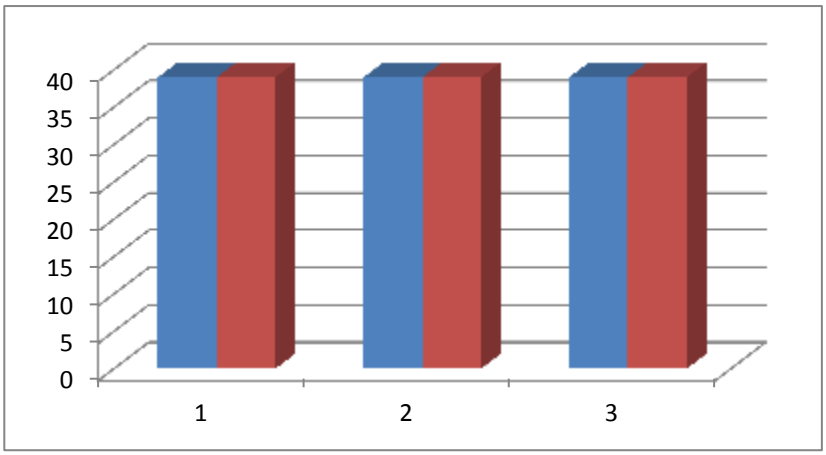


Рисунок 5.17 – Диаграмма результатов сравнения фотографий метки с числом отверстий 39 с ее QR-кодом – оригиналом

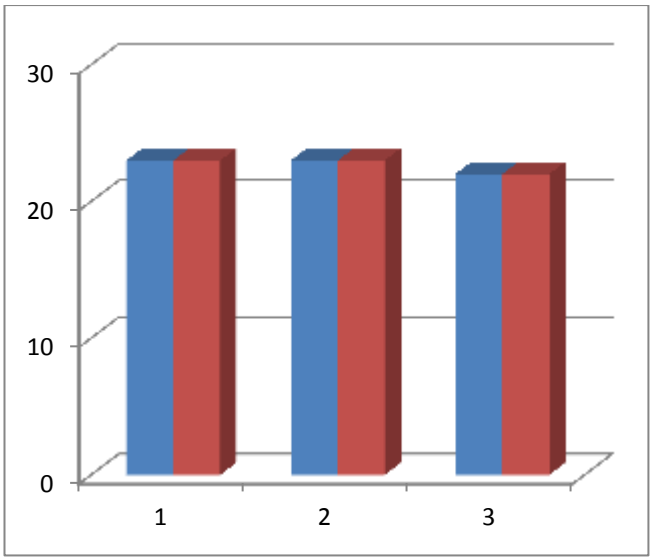


Рисунок 5.18 – Диаграмма результатов сравнения фотографий метки с числом отверстий 23 с ее QR-кодом – оригиналом

Анализ результатов данного исследования позволяет сделать вывод о том, что данный фактор внешней среды – период эксплуатации бумажного носителя не оказал влияния на итог идентификации. Каждая метка после контакта и попытки ее загрязнения осталась узнаваемой для автоматизированной системы идентификации. Все ее идентификационные признаки, как видно из рисунков 5.12 – 5.18, совпали по значениям, полученным после обработки фотографий, сделанных до и после эксплуатации.

Это в очередной раз подтвердило надежность и успешность процедуры отождествления изображения метки при использовании нового метода и автоматизированной системы.

5.3 Анализ результатов работы автоматизированной системы идентификации по выявлению подлинности документа из совокупности объектов

Данный этап экспериментальных исследований посвящен подтверждению применимости разработанной автоматизированной системы идентификации в случае отождествления истинного документа с помощью

сравнения изображения его метки и QR-кода документа-оригинала. На предыдущих этапах производилось распознавание изображений метки, полученных при обработке ее фотографий, по QR-коду ее же оригинала. В данном параграфе произведен анализ результатов процедуры идентификации каждой метки по фотографиям этой метки и множества других – «чужих» меток с помощью нового разработанного метода.

При защите бумажных документов наиболее важной проблемой является снижение ошибок второго рода – запрет признания автоматизированной системой «чужой» метки за метку документа – подлинника.

Для выявления способности автоматизированной системы выделять истинный бумажный документ по стохастически нанесенной метке из совокупности других, «поддельных» документов, проводились экспериментальные исследования с использованием большого числа бумажных носителей с прожженными метками (400 штук, вариантов изображений каждой метки – 10). Массив выборки по формуле (5.1) составил:

$$M_{FAR} = (400 - 1) \cdot (10 + 1) \cdot 400 = 1755600.$$

Сканированные изображения каждой метки сначала подвергались процедуре предварительной обработки, поиску и считыванию значений идентификаторов. Затем системой были созданы QR-коды эталонных изображений.

С помощью камеры сотового телефона были получены фотографии каждой метки.

Для иллюстрации работы автоматизированной системы вначале рассмотрена процедура распознавания метки с серийным номером 8126701080 (рис. 5.8) по фотографиям множества других меток, в том числе и по ее фотографии. На рисунке 5.19 изображена фотография одной из «чужих» меток с серийным номером 8759301085. Для проведения процедуры идентификации автоматизированной системой были созданы QR-коды всех участвующих в

эксперименте меток. На рисунке 5.20 изображен код одной из них с серийным номером 8759301085.

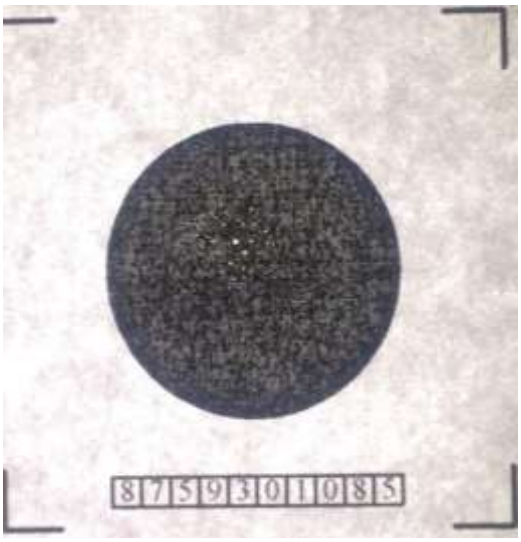


Рисунок 5.19 – Стохастически нанесенная метка № 8759301085

После выполнения процедур обработки изображений меток, считывания значений их идентификационных признаков, кодирования информации в виде QR-кодов и распознавания метки, автоматизированная система сделала вывод о полном несовпадении значений идентификаторов «чужих» меток по сравнению с величинами признаков, записанными в QR-коде метки – оригинала. На рисунке 5.21 приведен один из полученных автоматизированной системой результатов сравнения «чужой» метки с эталонной.

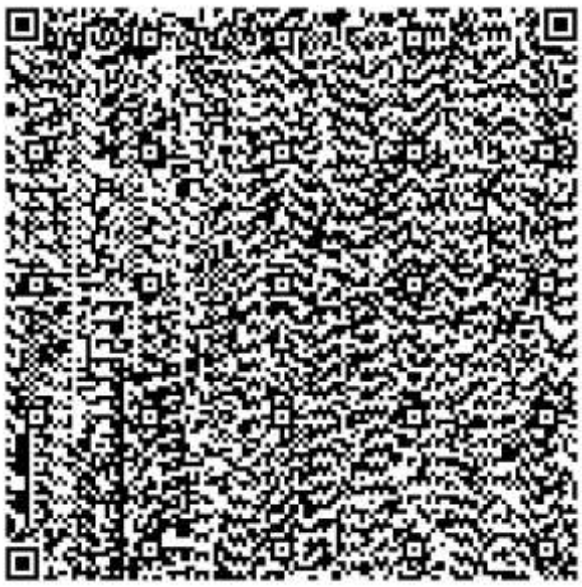


Рисунок 5.20 – QR-код метки № 8759301085

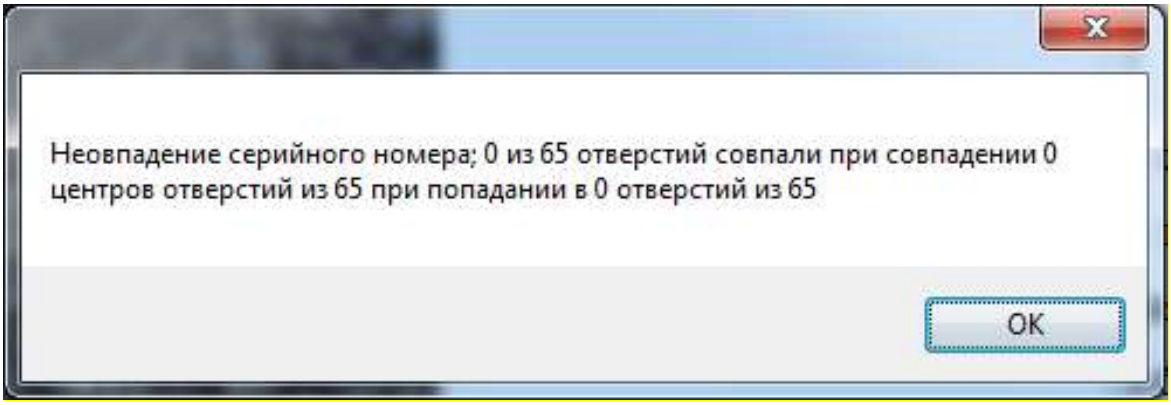


Рисунок 5.21 – Результаты сравнения QR-кода метки № 8759301085 с бинарным изображением эталонной метки

Приведенный результат распознавания «чужой» метки отражает значительное отличие от результата сравнения значений идентификационных признаков истинной метки с информацией QR-кода ее оригинала (рис. 5.9). Несовпадение серийного номера, отсутствие совпадения по количеству прожженных отверстий, по координатам их центров масс и величинам площадей исключает возможность выдачи «поддельного документа» с нанесенной «чужой» меткой даже при копировании QR-кода метки-оригинала подлинника.

Для иллюстрации работы автоматизированной системы по идентификации метки с серийным номером № 8759301085 среди множества «чужих» меток на рисунке 5.22 приведена диаграмма. Для ее построения из совокупности обработанных данных наряду с нулевыми результатами были отобраны и ненулевые итоги процедуры идентификации.

По горизонтальной оси диаграммы отложены номера столбцов – результатов процедуры идентификации, по вертикальной оси – количество отверстий.

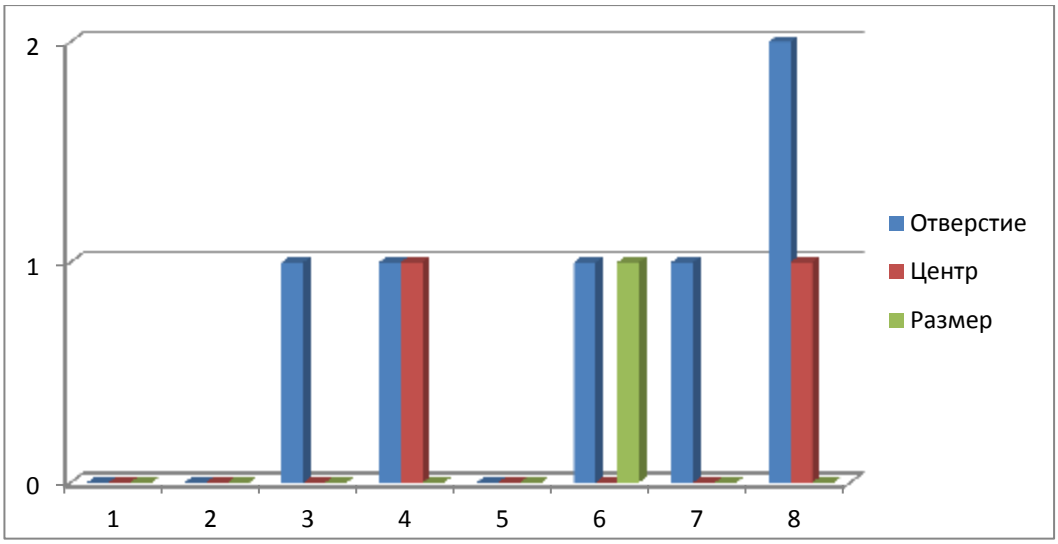


Рисунок 5.22 – Диаграмма результатов сравнения QR-кода метки № 8759301085 с бинарными изображениями «чужих» меток

Из приведенной диаграммы следует, что сравнение идентификационных признаков «чужих» меток с информацией QR-кода оригинала дает совпадение по максимальному значению у одной из них – частей двух отверстий из 65 отверстий метки – оригинала (столбец 8). Но площади частей этих отверстий отличаются от эталонных значений, и произошло совпадение по координатам центра масс одного отверстия при сравнении с координатами 65 отверстий оригинальной метки.

Столбец 4 иллюстрирует пересечение одного отверстия «чужой» метки с частью одного из 65 отверстий эталонной метки при совпадении координат центра масс одного отверстия.

Столбец 6 показывает общность показателей – части одного отверстия и площади при полном отличии значений координат центров масс.

Столбцы 3 и 7 отражают пересечения одного отверстия «чужой» метки и метки – оригинала.

Отсутствие столбцов под номерами 1, 2, 5 показывает отличие величин идентификационных признаков «чужих» меток при сравнении с идентификаторами QR-кода эталонной метки.

На рисунках 5.23 – 5.32 приведены диаграммы, построенные на основе результатов работы автоматизированной системы по идентификации меток с

разными серийными номерами, различным числом прожженных электроразрядным способом отверстий. Для иллюстрации процедуры идентификации отобраны наряду с нулевыми и ненулевые показатели. Выявление подлинности каждой из них также определялось автоматизированной системой в ходе сравнения величин идентификационных признаков всех участвующих в эксперименте меток со значениями, записанными в QR-коде метки – оригинала.

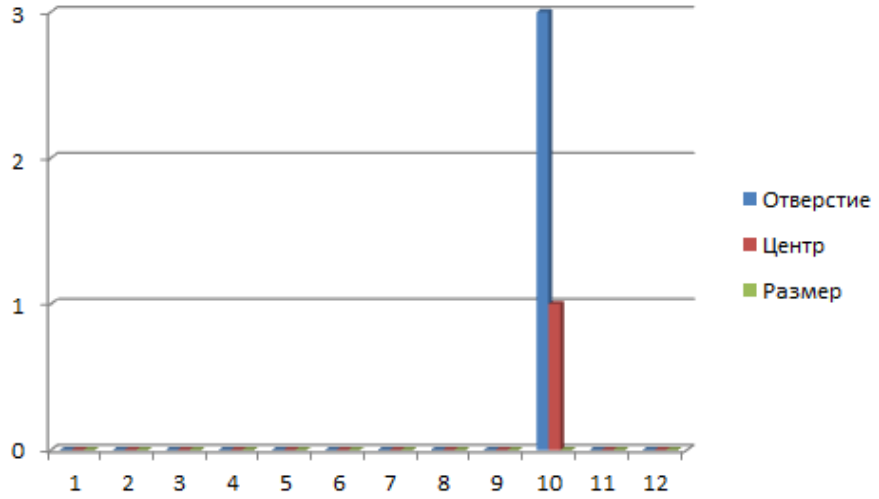


Рисунок 5.23 – Диаграмма результатов сравнения QR-кода метки № 3326751080 с бинарными изображениями «чужих» меток

Сравнение значений идентификационных признаков метки с серийным номером 3326751080 с величинами идентификаторов «чужих» меток дало наряду с отрицательными результатами (отсутствие столбцов под номерами 1 – 9, 11, 12) совпадение частей трех отверстий (у метки – оригинала 87 отверстий) при одинаковых координатах центра масс одного отверстия (рис. 5.23). Результат работы автоматизированной системы по выявлению подлинности бумажного носителя с нанесенной меткой с серийным номером 4426502088 представлен на рисунке 5.24.

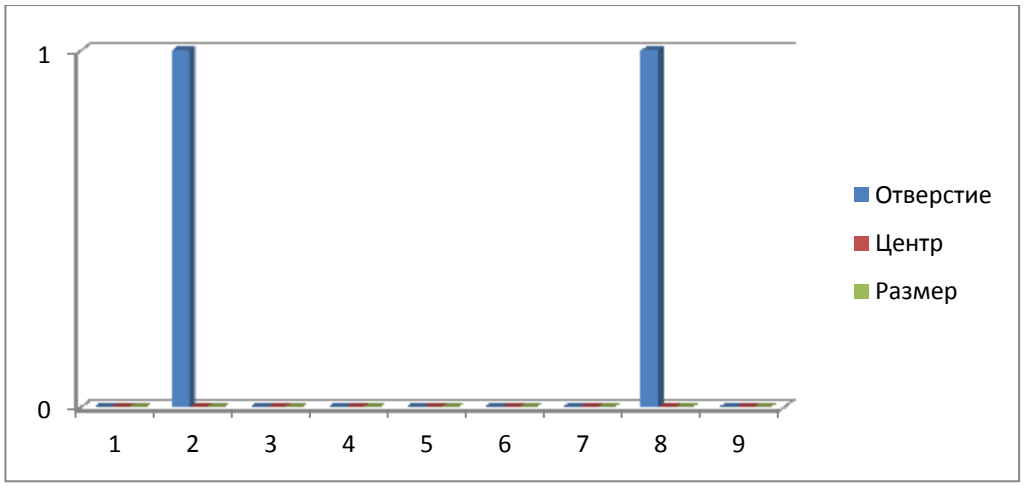


Рисунок 5.24 – Диаграмма результатов сравнения QR-кода метки № 4426502088 с бинарными изображениями «чужих» меток

Как видно из диаграммы, максимальное совпадение произошло при пересечении одного отверстия «чужой» и эталонной меток. При этом координаты центра масс отличны. Отсутствие столбцов под номерами 1, 3 – 7, 9 показывает отрицательные результаты идентификации «чужих» меток при сравнении с идентификаторами QR-кода эталонной метки.

Сравнение значений идентификационных признаков метки с серийным номером 6135730065 с величинами идентификаторов «чужих» меток дало наряду с отрицательными результатами (отсутствие столбцов под номерами 1, 2, 5, 7, 8, 11) совпадение частей двух отверстий при одинаковых координатах центра масс одного отверстия (рис. 5.25).

Столбцы 3, 4, 6, 10, 12 иллюстрируют общность части одного отверстия у «чужой» и эталонной меток.

Диаграмма рисунка 5.26 также отображает совпадение частей двух отверстий (столбец 9), части и координат центра масс только одного отверстия – столбцы 2 – 7 и отсутствие совпадения по этим показателям – нулевая высота столбца 1.

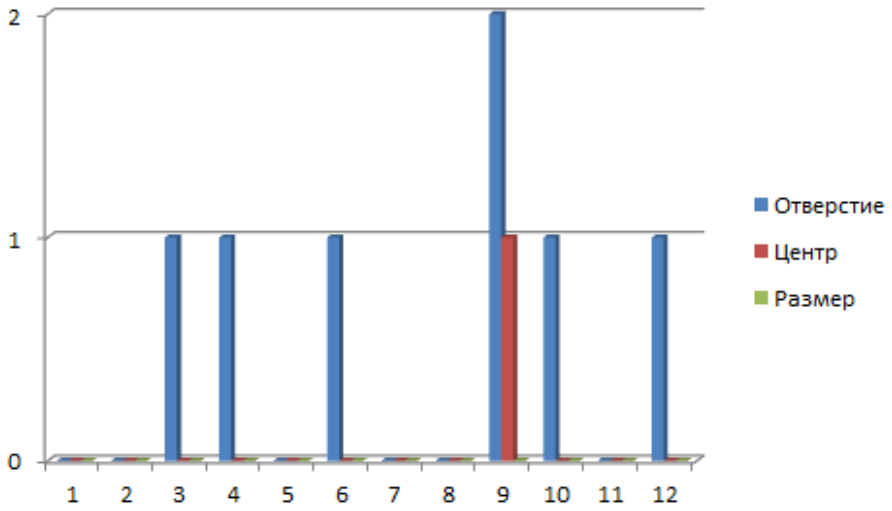


Рисунок 5.25 – Диаграмма результатов сравнения QR-кода метки № 6135730065 с бинарными изображениями «чужих» меток

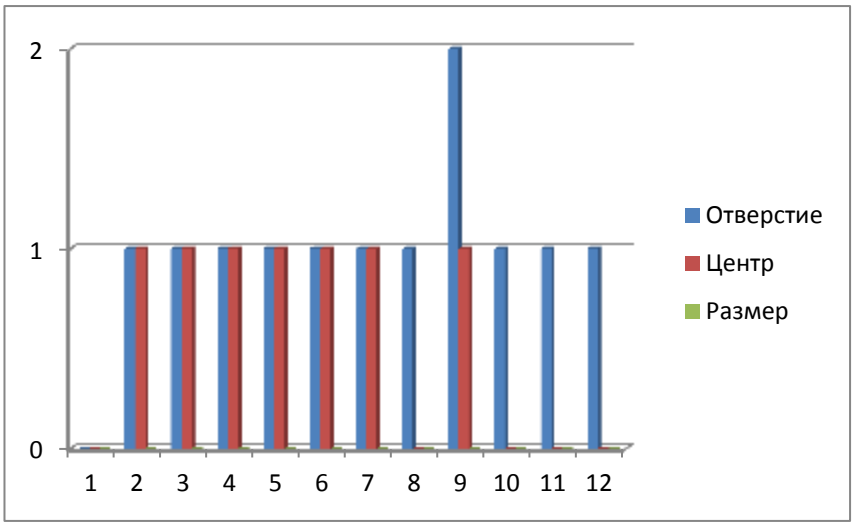


Рисунок 5.26 – Диаграмма результатов сравнения QR-кода метки № 0354850017 с бинарными изображениями «чужих» меток

На рисунке 5.27 представлена диаграмма, построенная по результатам идентификации метки с серийным номером 0058935588, имеющей 94 отверстия. Как видно из диаграммы, максимальное количество совпадений происходит у одной из «чужих» меток – по общим частям пяти отверстий (столбец 8). Но при этом совпадение координат центра масс возможно только у одного отверстия. Столбец 6 иллюстрируют общность частей двух отверстий «чужой» и эталонной меток, совпадение площадей одного отверстия и отсутствие совпадения координат центров масс. Столбцы 3 и 5 показывают

общность показателей – части и координат центров масс одного отверстия при полном отличии значения его площади. Столбцы 9 и 10 отражают совпадение по частям двух отверстий, при этом координаты центра масс одинаковы у двух отверстий (столбец 9) и у одного отверстия (столбец 10). Остальные столбцы показывают на общность части одного отверстия «чужой» и эталонной меток.

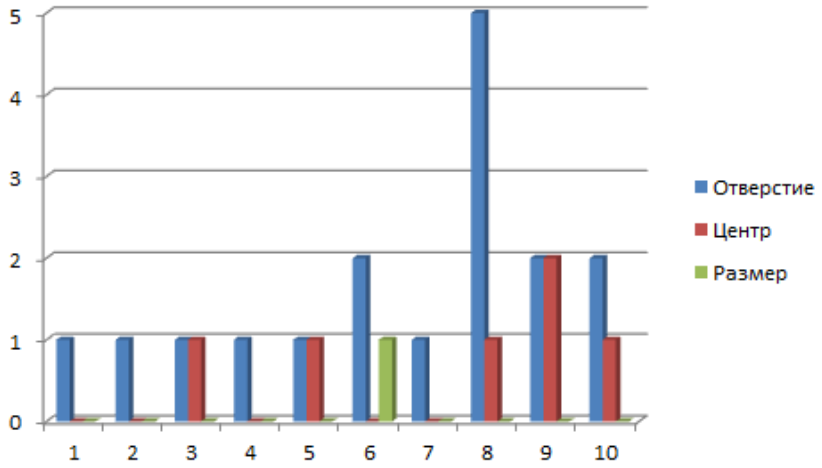


Рисунок 5.27 – Диаграмма результатов сравнения QR-кода метки № 0058935588 с бинарными изображениями «чужих» меток

Сравнение значений идентификационных признаков метки с серийным номером 7177701080 с величинами идентификаторов «чужих» меток дало совпадение частей четырех отверстий (столбец 1) при одинаковых координатах центра масс трех отверстий (эталонная метка имела 92 отверстия) (рис. 5.28). Столбцы 4, 5, 6 показывают общность частей трех отверстий «чужой» метки и метки – оригинала. При этом совпадение координат центров масс двух отверстий замечено только у одной из этих меток (столбец 6). Столбцы 2 и 3 отражают общность показателей – частей и координат центров масс двух отверстий при полном отличии значений их площадей. Столбцы 7 и 8 иллюстрируют совпадение части и координат центров масс одного отверстия. По одному показателю произошло совпадение у двух «чужих» меток – общей части одного отверстия (столбец 9), двух отверстий (столбец 10).

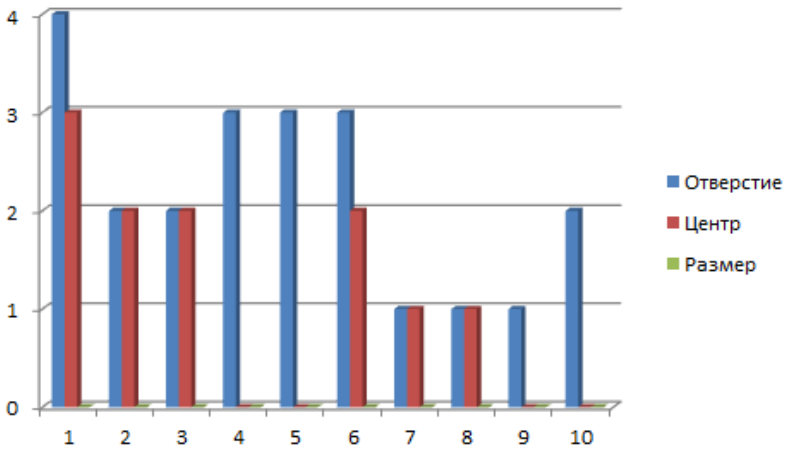


Рисунок 5.28 – Диаграмма результатов сравнения QR-кода метки № 7177701080 с бинарными изображениями «чужих» меток

На рисунке 5.29 изображена диаграмма, построенная по результатам идентификации метки с серийным номером 5122701560, имеющей 87 отверстий. Как видно из диаграммы, максимальное количество совпадений происходит у одной из «чужих» меток – по общим частям четырех отверстий (столбец 3). При этом совпадение координат центра масс и площади возможно только у одного отверстия (совпадения могут быть по разным отверстиям). Столбец 2, 6, 10, 11 иллюстрируют общность частей двух отверстий «чужой» и эталонной меток, совпадение площади одного отверстия отражает столбец 11, координат центров масс одного отверстия – столбцы 2 и 10. Столбцы 7 – 9, 12 показывают общность показателей – части одного отверстия и координат центров масс при полном отличии значения его площади. Столбцы 9 и 10 отражают совпадение по частям двух отверстий, при этом координаты центра масс одинаковы у двух отверстий (столбец 9) и у одного отверстия (столбец 10). Остальные столбцы показывают на общность части одного отверстия «чужой» и эталонной меток.

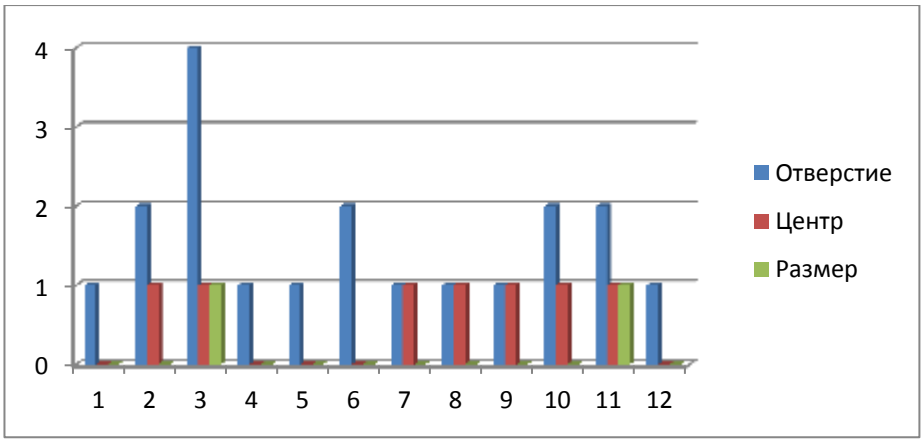


Рисунок 5.29 – Диаграмма результатов сравнения QR-кода метки № 5122701560 с бинарными изображениями «чужих» меток

По диаграмме, представленной на рисунке 5.30, можно судить о совпадении частей трех отверстий при сравнении метки – оригинала с серийным номером 8126401533 и одной из «чужих» меток (столбец 8). При этом координаты центров масс совпали только у двух отверстий. Столбцы 1 – 7 иллюстрируют общность частей одного отверстия, при этом одинаковые координаты центра масс одного отверстия отмечаются у четырех «чужих» меток (столбцы 1, 2, 4, 5). Отсутствие столбцов под номерами 9 и 10 свидетельствует о различии величин идентификационных признаков «чужих» меток при сравнении с идентификаторами QR-кода эталонной метки.

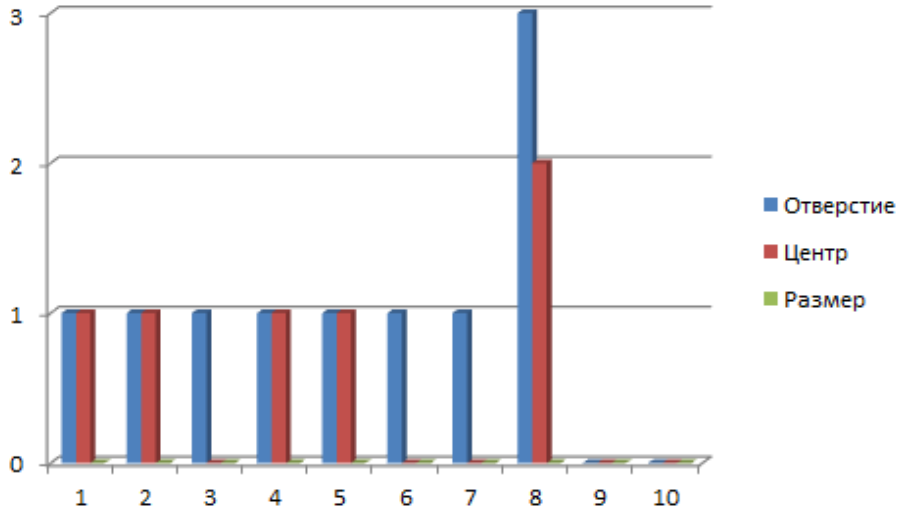
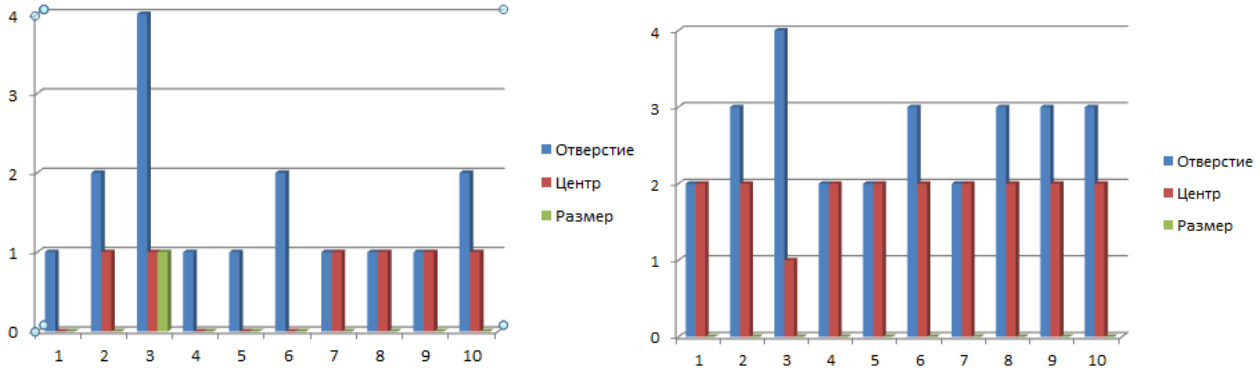


Рисунок 5.30 – Диаграмма результатов сравнения QR-кода метки № 8126401533 с бинарными изображениями «чужих» меток

Диаграмма рисунка 5.31, а построена по результатам совершенной автоматизированной системой идентификации метки с серийным номером 3144561077. Исследования показали, что максимальное количество совпадений с эталонной меткой происходит только у одной из «чужих» меток – по общим частям трех отверстий (столбец 8). Но при этом совпадение координат центра масс возможно у двух отверстий. Столбцы 1 – 7 отражают общность частей одного отверстия, при этом одинаковые координаты центра масс одного отверстия отмечаются у четырех «чужих» меток (столбцы 1, 2, 4, 5). Нулевая высота столбцов 9 и 10 указывает на отсутствие совпадений значений идентификаторов метки – оригинала и «чужих» меток.



а) б)

Рисунок 5.31 – Диаграмма результатов сравнения QR-кода: а) метки № 3144561077 с бинарными изображениями «чужих» меток; б) метки № 2155706880 с бинарными изображениями «чужих» меток

На рисунке 5.31, б изображена диаграмма, построенная по результатам идентификации метки с серийным номером 2155706880, имеющей 98 отверстий. Сравнение значений идентификационных признаков метки – оригинала с величинами идентификаторов «чужих» меток дало совпадение частей четырех отверстий (столбец 3) при одинаковых координатах центра масс одного отверстия. Столбцы 2, 6, 8 – 10 показывают общность частей трех отверстий «чужой» метки и метки – оригинала. При этом совпадение координат центров масс произошло у двух отверстий, при отсутствии совпадения величин площадей прожженных отверстий у всех участвующих в эксперименте

«чужих» меток. Столбцы 1, 4, 5, 7 отражают совпадение частей и координат центров масс двух отверстий.

В результате экспериментов построен график зависимости вероятности ошибок идентификации второго рода от порога чувствительности автоматизированной системы (рис. 5.32). По оси абсцисс нанесены значения порога чувствительности автоматизированной системы от 0 до 1, по оси ординат – вероятность признания «чужой» метки за метку документа – оригинала. Даже при пороге чувствительности 0,03 все «чужие» метки не будут признаны системой за метку-подлинник.

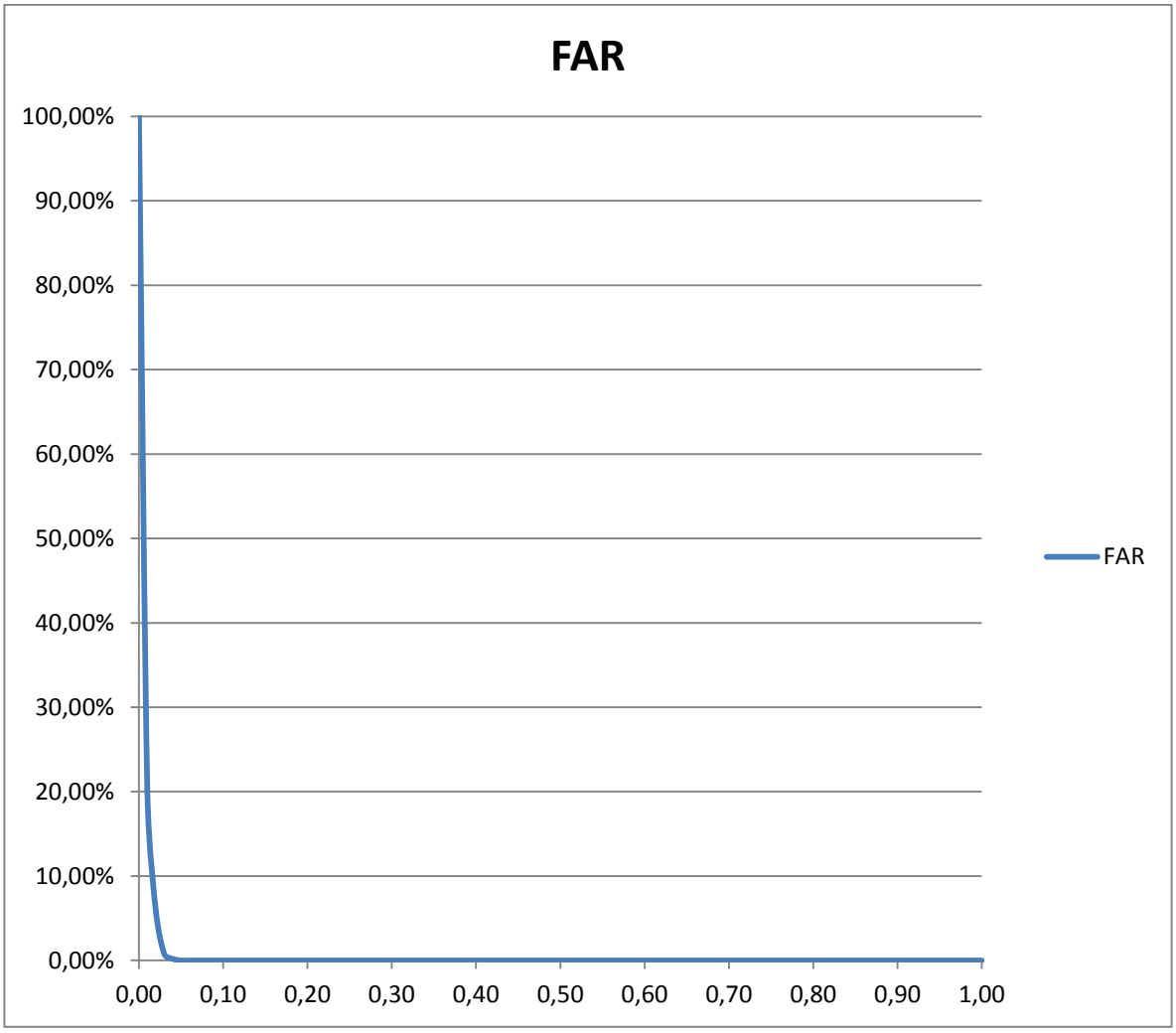


Рисунок 5.32 – Определение вероятности появления ошибок второго рода

Для определения значения порога чувствительности автоматизированной системы для идентификации бумажных документов построен график, на котором совмещены зависимости вероятностей ошибок первого (при хорошей

освещенности меток при их фотографировании) и второго рода от порога чувствительности (рис. 5.33). По графику рисунка 5.33 t_{com} можно выбирать в пределах от 0,04 до 0,85. Но с учетом влияния разной степени освещенности на качество идентификации меток величину порога следует определить по рисунку 5.34. По этому графику видно, что при пороге $t_{com} = 0{,}2$ все «чужие» метки не будут пропущены, а все «свои» подтвердят свою истинность.

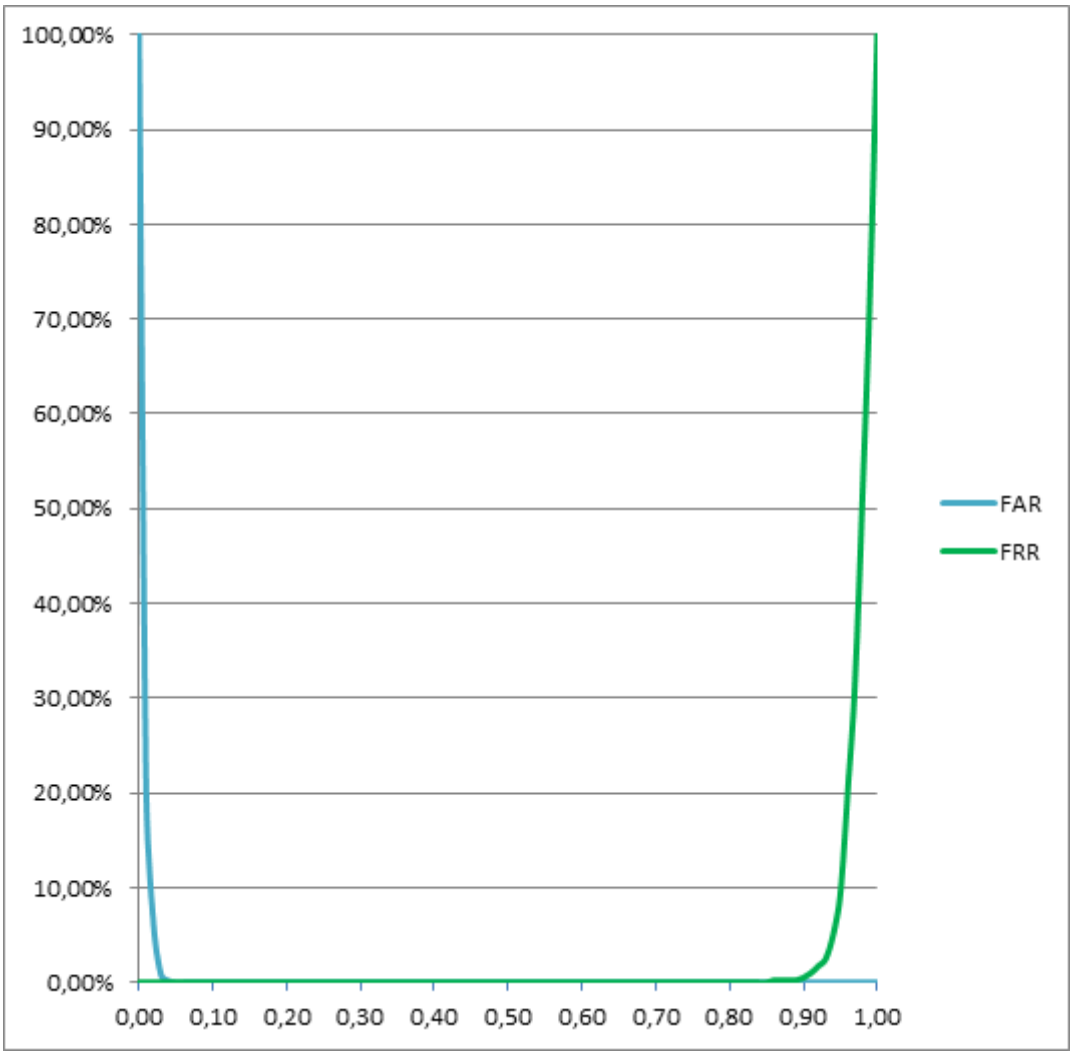


Рисунок 5.33 – Определение порога чувствительности автоматизированной системы идентификации при хорошей освещенности меток

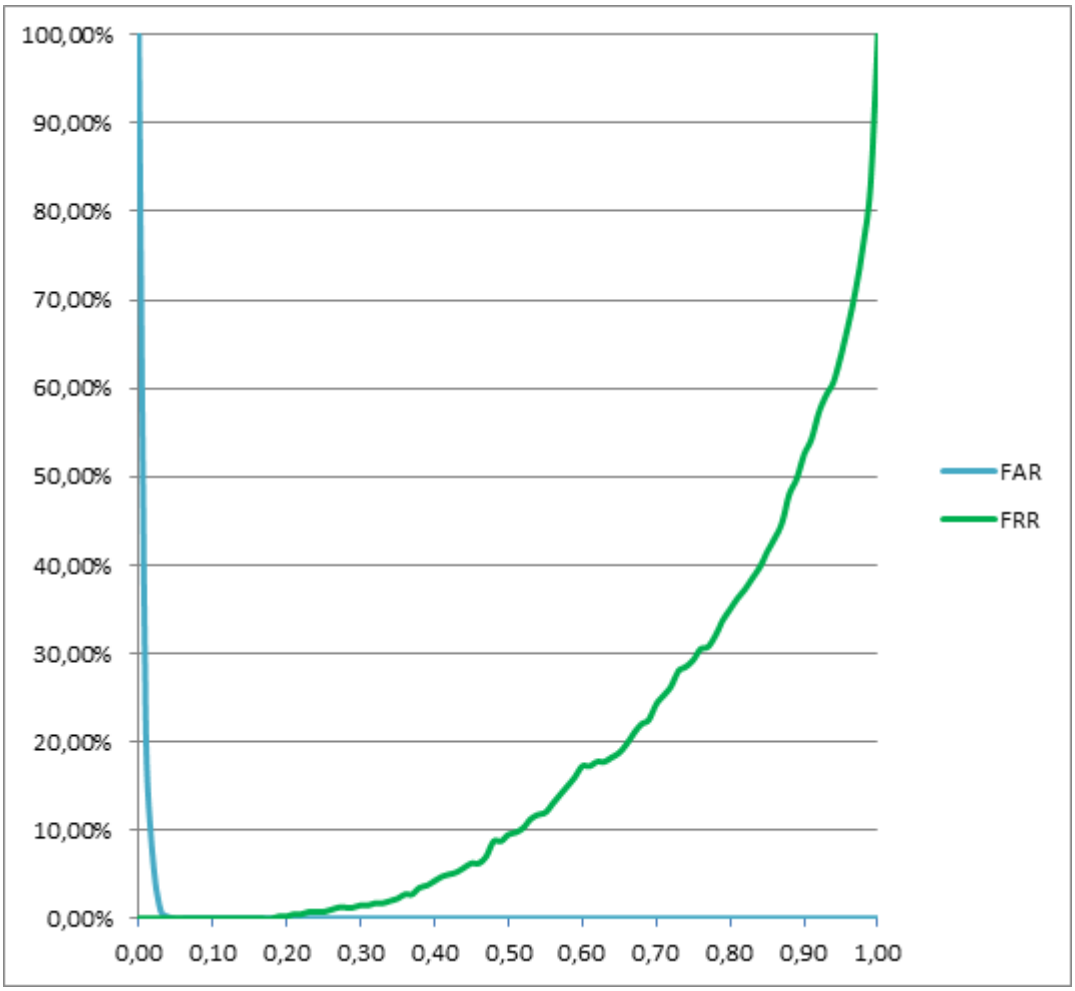
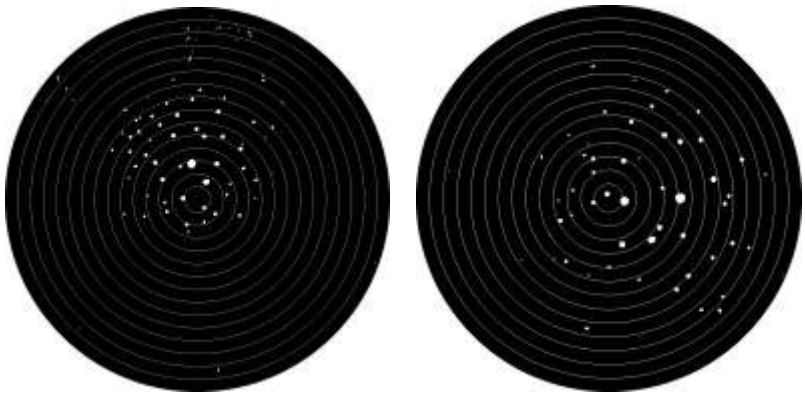


Рисунок 5.34 – Определение порога чувствительности автоматизированной системы идентификации с учетом влияния разной степени освещенности при фотографировании меток

Анализ результатов проведенных экспериментальных исследований доказал адекватность и надежность предлагаемого метода идентификации бумажных документов, основанного на применении разработанной автоматизированной системы [111-113].

Кроме того, было замечено, что при исследовании характера расположения каналов разрушения (отверстий метки) наблюдалась интерференционная картина. Для ее выявления на бумажном носителе по разработанной программе на мишени выделялась область в виде окружности, охватывающей набор перфораций, затем в этой области был проведен ряд концентрических окружностей на равных расстояниях друг от друга. На

рисунке 5.35 приведены примеры меток с нанесенными концентрическими окружностями.



а) б)

Рисунок 5.35 – Нанесение концентрических окружностей на невоспроизводимых поверхностях: а) № 8759301085; б) № 8132201086

Далее информационной системой производился подсчет количества центров перфораций, попавших в каждую кольцевую подобласть мишени и в центровую окружность самого малого радиуса. На графиках рисунка 5.36 по оси абсцисс отложены номера подобластей. Например, 1 – центровая часть малого радиуса, 2 – кольцевая часть между центровой и следующей за ней окружностью большего радиуса и т. д. По оси ординат отложено количество перфораций, попавших в конкретную область.

Исследования проводились при разбивании перфорированной области мишени на различное количество колец. На рисунке представлены графики, полученные при одном и том же количестве колец для каждого набора перфораций. Дальнейший анализ результатов разных наборов перфораций, проделанный с помощью разработанной информационной системы, показал волновой характер распределения центров отверстий, не совпадающий с функцией нормального распределения.

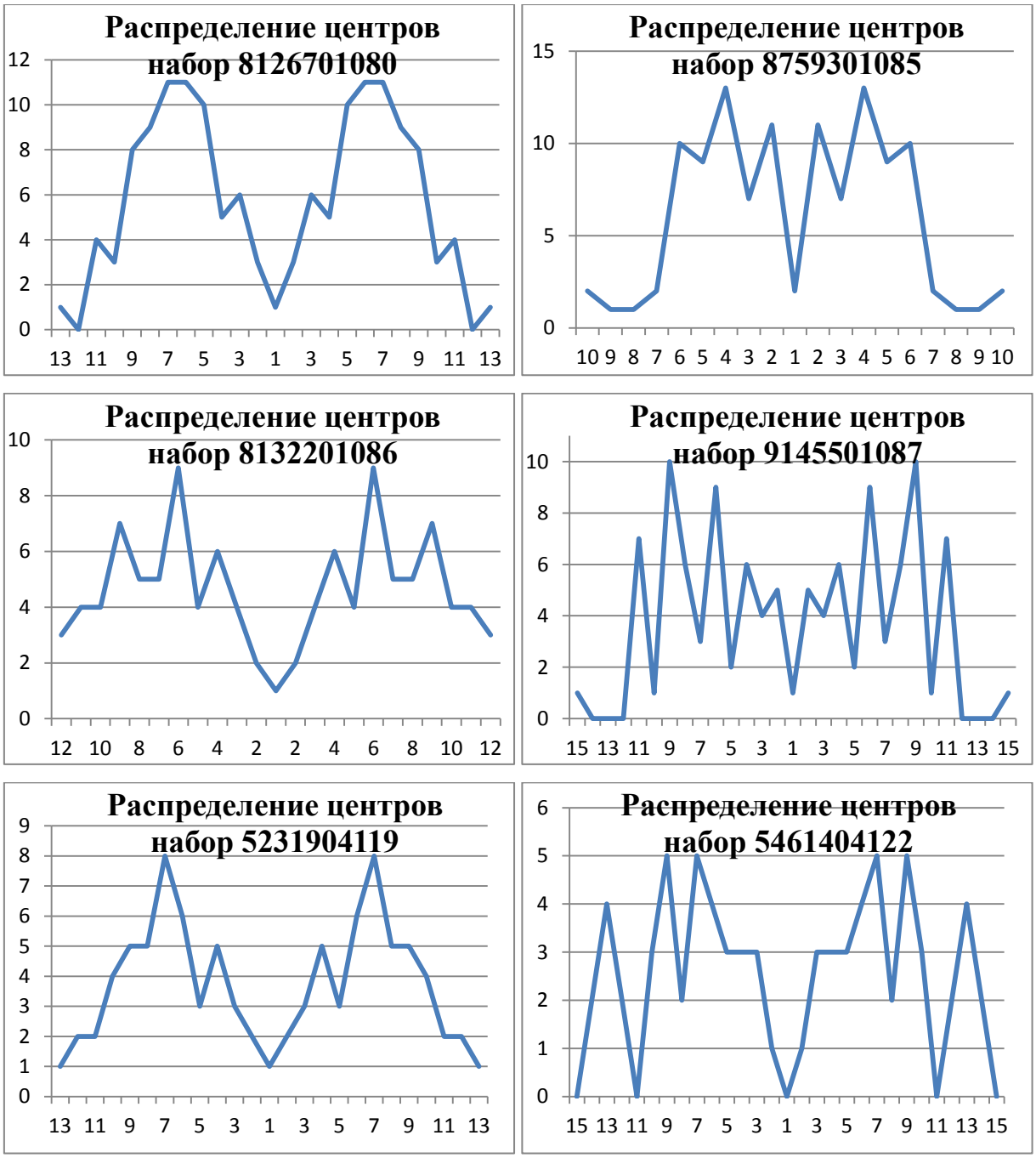


Рис. 5.36 – Характер распределения центров перфораций для наборов № 8126701080, 8759301085, 8132201086, 9145501087, 5231904119, 5461404122

Анализ характера представленных на графиках волн показал интерференционную картину: максимальная амплитуда волн в четыре раза превышает среднее значение. Таким образом, при идентификации метки интерференционный характер расположения отверстий можно также считать дополнительным доказательством ее подлинности.

Выводы по пятой главе

1. В результате проведения первого этапа экспериментальных исследований было получено подтверждение возможности применения нового метода идентификации, производимого разработанной автоматизированной системой. Каждая метка, полученная с помощью электроразрядной установки, прошла процедуру изготовления QR-кода ее эталонного изображения. В ходе диссертационного исследования учитывалось, что при установлении истинности документа у проверяющего субъекта может отсутствовать сканирующее устройство высокой чувствительности. Поэтому для получения фотографий меток были выбраны два смартфона, не приспособленных для профессионального использования.

Результаты проведенных исследований доказали возможность и успешность проведения автоматизированной системой процедуры идентификации, несмотря на среднюю чувствительность камер смартфонов.

2. Второй этап экспериментальных исследований был посвящен проведению анализа влияния факторов внешней среды на процесс идентификации метки, полученной стохастическим электроразрядным способом. В качестве факторов внешней среды были выбраны:

- степень освещенности метки при получении фотографии ее изображения;
- длительность периода эксплуатации бумажного документа с нанесенными на него меткой и QR-кодом.

Каждая метка была сфотографирована в различное время суток, в разные дни при пасмурной и ясной погоде. Полученные при различной степени освещенности фотографии каждой из меток также были обработаны автоматизированной системой. Ею произведено сравнение значений

идентификаторов. Построена зависимость вероятности ошибок идентификации первого рода от порога чувствительности системы.

Анализ результатов проведенного исследования свидетельствует о существенном влиянии степени освещенности на результаты идентификации: невысокое качество полученных при слабой освещенности фотографий искажает величину размеров – площадей отверстий. Если по координатам центров и количеству отверстий идентификация проходит успешно при работе автоматизированной системы с фотографиями меток, сделанных даже в условиях невысокой степени освещенности, то по идентификатору – площадь отверстий наблюдается отклонение от совпадения значений, превышающее допустимый порог. Но даже низкое качество фотографий метки позволяет сделать вывод об ее тождественности.

Также на данном этапе экспериментальных исследований было выявлено влияние длительности периода эксплуатации бумажного документа с нанесенными на него меткой и QR-кодом на надежность процедуры идентификации, осуществляемой автоматизированной системой. В начале исследования были сделаны фотографии каждой метки камерой сотового телефона и произведена генерация QR-кодов меток-оригиналов, изображения которых были получены сканирующим устройством.

Все носители в течение полугода активно эксплуатировались: подвергались тщательному рассмотрению коллегами, контакту (метки трогали руками). После шестимесячного периода активной эксплуатации были сделаны фотографии каждой метки, и автоматизированной системой произведено сравнение информации изображения метки с QR-кодом ее оригинала.

Анализ результатов данного исследования позволяет сделать вывод о том, что период эксплуатации бумажного носителя не оказал влияния на итог идентификации. Каждая метка после контакта и попытки ее загрязнения осталась узнаваемой для автоматизированной системы идентификации. Это в очередной раз подтвердило надежность и успешность процедуры

отождествления изображения метки при использовании нового метода и автоматизированной системы.

3. Третий этап экспериментальных исследований был посвящен подтверждению применимости разработанной автоматизированной системы идентификации по выявлению подлинного документа по стохастически нанесенной метке из совокупности других, «поддельных» документов с помощью сравнения изображений меток и QR-кода документа-оригинала. После выполнения процедур обработки изображений меток, считывания значений их идентификационных признаков, кодирования информации в виде QR-кодов и распознавания метки, автоматизированная система делала вывод о соотношении значений идентификаторов «чужих» меток по сравнению с величинами признаков, записанными в QR-коде метки – оригинала.

Весьма малый процент совпадения значений идентификационных признаков – общность частей одного-пяти отверстий, одинаковые значения координат центра масс одного-трех отверстий, площади одного отверстия – свидетельствует о повышении защищенности информации бумажного документа: отсутствие принятия информационной системой изображения «чужой» метки за метку – оригинал. Построенные зависимости вероятностей ошибок идентификации первого и второго рода позволили определить значение порога чувствительности автоматизированной системы, при котором все «чужие» метки не будут пропущены, а все свои подтвердят свою истинность.

Информация о волновом характере распределения отверстий метки также может служить идентификатором и закодирована в QR-коде.

Таким образом, новый метод электроразрядного получения метки и его реализация в виде разработанной автоматизированной системы может быть применен для идентификации бумажных документов.

ЗАКЛЮЧЕНИЕ

В диссертационной работе решена научная задача разработки модельно-методического аппарата для идентификации документа по дополнительному реквизиту – невоспроизводимой электроразрядной метке и коду документа-оригинала для повышения защищенности информации бумажных документов. Основными результатами являются:

1. Разработана методика определения угроз безопасности информации бумажного документооборота, позволяющая на основе модели угроз произвести оценку защищенности информации бумажных документов и разработать сценарии дальнейшего развития событий.

2. Для защиты информации бумажных документов впервые применена невоспроизводимая метка, нанесенная на документ стохастическим лавинно-стримерным разрядом при рассчитанных режимах работы электроразрядной установки, что обеспечивает множество каналов разрушения, характерные признаки которых служат идентификаторами и определяются разработанной автоматизированной системой.

3. В новом методе идентификации применена процедура кодирования автоматизированной системой значений идентификационных признаков метки в виде нанесенного рядом с меткой QR-кода, что позволяет при невоспроизводимости метки с высокой степенью точности производить сравнение ее признаков с информацией QR-кода документа-подлинника и тем самым обеспечить его уникальность. Ошибки идентификации не превышают 5%-ный уровень.

Таким образом, все поставленные задачи выполнены, цель исследования достигнута.

Рекомендации по применению результатов работы для идентификации бумажных документов включают в себя указания по применению нового

метода идентификации: использованию методики определения угроз безопасности информации бумажного документооборота для оценки защищенности информации бумажных документов и разработки сценариев дальнейшего развития событий; назначению режимов работы электроразрядной установки для нанесения меток; применению автоматизированной системы идентификации бумажных документов, позволяющей определять значения идентификаторов меток, кодировать их, наносить в виде QR-кода на документ и производить его идентификацию на основе сравнения информации метки и QR-кода. Основываясь на сформулированных рекомендациях, представляется вероятной возможность применения полученных результатов для идентификации бумажных документов, так как разработанный метод идентификации позволяет выявить подлинный документ из множества ему подобных с высокой степенью точности.

Перспективы дальнейшей разработки темы исследования заключаются в адаптации разработанного метода к идентификации полимерных и металлических изделий.

Соответствие паспорту специальности. Положения, выносимые на защиту, соответствуют паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»:

«4. Системы документооборота (вне зависимости от степени их компьютеризации) и средства защиты циркулирующей в них информации» (результаты 1-3);

«6. Модели и методы формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования» (результаты 1-3);

«13. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности» (результаты 1-3).

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Об информации, информационных технологиях и о защите информации (с изм. и доп., вступ. в силу с 29.03.2019 г.): федер. закон от 27.07.2006 № 149-ФЗ, ред. 29.03.2019. [Электронный ресурс]. – Режим доступа:: http:// www.consultant.ru/document/cons_doc_LAW_61798/. (дата обращения 30.04.2019).

2. Об утверждении перечня сведений конфиденциального характера (с изм. и доп., вступ. в силу с 13.07.2015 г.): указ Президента РФ от 06.03.1997 № 188 [Электронный ресурс]. – Режим доступа: http://base.garant.ru/10200083/. (дата обращения 30.04.2019).

3. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России от 11.02.2013. № 17, ред. 15.02.2013. [Электронный ресурс]. – Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17. (дата обращения 30.04.2019).

4. Об утверждении Правил делопроизводства в федеральных органах исполнительной власти: постановление Правительства РФ от 15.06.2009 № 477, ред. от 26.04.2016. [Электронный ресурс]. – Режим доступа: http://base.garant.ru/195767/. (дата обращения 30.04.2019).

5. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=418509#06630855403017148. (дата обращения 30.04.2019).

6. ГОСТ Р 7.0.8-2013. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200108447. (дата обращения 30.04.2019).

7. ГОСТ Р 6.30-2003. Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200031361. (дата обращения 30.04.2019).

8. Рынок охранных систем [Электронный ресурс]. – Режим доступа: http://ai-media.ru/news/rynok-ohrannyh-sistem/.(дата обращения 23.10.2019).

9. О техническом регулировании (с изменениями на 29 июля 2017 г.) [Электронный ресурс]: федер. закон от 29.07.2017 № 243-ФЗ, ред. от 29.07.2017. – Режим доступа: http:// www.pravo.gov.ru. (дата обращения 10.02.2018).

10. Берновский, Ю.Н. Основные методы идентификации объектов [Электронный ресурс] / Ю.Н. Берновский // Стандарты и качество. – 2000. – № 9. – Режим доступа: https://ria-stk.ru/stq/adetail.php?ID=5817 (дата обращения 15.03.2015).

11. Омельченко, Е.В. Товароведение, экспертиза и стандартизация в вопросах и ответах: учебное пособие для подготовки к экзамену/ Е.В. Омельченко. – М.: АНО ВПО Российская академия предпринимательства, 2013. – 65 с.

12. Идентификация и фальсификация непродовольственных товаров: учебное пособие/ Под общ. ред. д.э.н., проф. И.Ш. Дзахмишевой. – 2-е изд., доп. и перераб. – М.: «Дашков и К°», 2013. – 360 с.

13. Ищенко, Е.П. Криминалистика: учебник / Е.П. Ищенко. – М.: Юридическая фирма «Контракт»: Волтерс Клувер, 2011. – 512 с.

14. Свиткин, М.З. Менеджмент качества и обеспечение качества продукции на основе международных стандартов ИСО/ М.З. Свиткин, В.Д. Мацута, К.М. Рахлин. – СПб.: Изд-во СПб картфабрики ВСЕГЕИ, 1999. – 403 с.

15. Ищенко, Е.П. Криминалистика: учебник. – 2-е изд., доп. и перераб./ Е.П. Ищенко, А.А.Топорков; под общ. ред. д.ю.н., проф. Е.П. Ищенко. – М.: Юридическая фирма «КОНТРАКТ», «ИНФРА-М», 2006. — 748 с.

16. Стандартизация и управление качеством продукции: учебник для вузов/ В.А. Швандар [и др.]; под общ. ред. проф. В.А. Швандара. — М.: ЮНИТИ-ДАНА, 2001. — 487 с.

17. Берновский, Ю.Н. Основы идентификации продукции и документов: учеб. пособие/ Ю.Н. Берновский. – М.: ЮНИТИ-ДАНА, 2012. – 351 с.

18. Алесинская Т.В. Основы логистики. Функциональные области логистического управления/ Т.В. Алесинская. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – 116 с.

19. Востриков, А.А. Штриховое кодирование: учеб. пособие / А.А. Востриков, А.М. Сергеев. – СПб.: ГУАП, 2011. – 59 с.

20. Малявкина, Л.И. Технология штрихового кодирования в торговых розничных сетях [Электронный ресурс] / Л.И. Малявкина, Т.С. Старцева// Экономическая среда. – 2013г. – №2. – Режим доступа: http://docplayer.ru/36080900-L-i-malyavkina-t-s-starceva-tehnologiya-shtrihovogo-kodirovaniya-v-torgovyh-roznichnyh-setyah.html. (дата обращения 15.03.2015).

21. Гаджинский, А.М. Логистика: учебник [Электронный ресурс] / А.М. Гаджинский. – М.: «Дашков и К», 2006. – 432 с. – Режим доступа: https://www.booksite.ru/fulltext/logist/text.pdf. (дата обращения 23.10.2017).

22. Adams, R. Specifications For Popular 2D Bar Codes [Электронный ресурс] / R. Adams. – Режим доступа: http://www.adams1.com/stack.html. (дата обращения 23.05.2015).

23. Музипов, Х.Н. Новые технологии идентификации объектов / Х.Н. Музипов, С.Э. Литвинов, Д.Д. Канев // Автоматизация, телемеханизация и связь в нефтяной промышленности. - 2013. - № 4. - С. 16-19.

24. Власов, М. RFID: 1 технология – 1000 решений: Практические примеры использования RFID в различных областях / М. Власов. – М.: Альпина Паблишер, 2014. – 218 с.

25. Финкенцеллер, К. RFID-технологии. Справочное пособие [Электронный ресурс] / К. Финкенцеллер; пер. с нем. Сойунханова Н.М. – М.: Додэка-XXI, 2010. – 496 с. Режим доступа:

http://www.kazus.ru/forums/attachment.php?attachmentid=49767&d=1374440757. (дата обращения 25.05.2015).

26. Bonsor, K. How RFID Works [Электронный ресурс] / K. Bonsor, W. Fenlon – Режим доступа: http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/rfid3.htm . (дата обращения 20.08.2015).

27. Rankl, W. Smart Card: handbook/ W. Rankl, W. Effing. – Chichester: John Wiley&Sons, Ltd, 2010. – 1088 p.

28. Желтов, С.Ю. Обработка и анализ изображений в задачах машинного зрения / С.Ю. Желтов [и др.]. – М.: Физматкнига, 2010. – 672 с.

29. Лебедев, А.Т. Масс-спектрометрия в органической химии [Электронный ресурс] / А.Т. Лебедев. – М.: БИНОМ. Лаборатория знаний, 2003. – 493 с. – Режим доступа: http://kipinfo.ru/files/dokl_piter_12.ppt (дата обращения 18.11.2015).

30. Пат. 2064697 Российская Федерация, МПК G 21 H 5/02. Способ маркировки и идентификации объектов // Ляпидевский В.К.; заявитель и патентообладатель Ляпидевский В.К. - № 2000131736/09; заявл. 20.05.1993; опубл. 27.07.1996, Бюл. № 23 (II ч.). - 3 с.: ил.

31. Пат. 014299 Евразийская патентная организация, МПК G 06 K 9/76. Способ спектральной идентификации объектов материальных ресурсов // Шкилев В.Д. (MD), Каранфил В.Г. (MD); заявитель и патентообладатель Шкилев В.Д. (MD), Каранфил В.Г. (MD). – № 200600768; заявл. 27.04.2007; опубл. 29.10.2010, Бюл. № 5. - 5 с.: ил.

32. Пат. 2064697 Российская Федерация, МПК G 06 K 7/14 . Способы и устройства для создания печатных изделий с возможностью установления их подлинности и с последующей их проверкой// Кауберн Р.П.; заявитель и патентообладатель Инджениа Текнолоджи Лимитед (GB). – № 2006136024/09; заявл. 09.03.2005; опубл. 27.01.2010, Бюл. № 6. - 13 с.: ил.

33. Пат. US 6584214 B1 G 07 B 17/00. Identification and verification using complex, three-dimensional structural features // Pappu R., Gershenfeld N., Smith J.R.; Massachusetts Institute Of Technology. – № US 09/419,756; заявл. 19.10.1999; опубл. 24.06.2003, Бюл. - 5 с.: ил.

34. Smalley, E. Plastic tag makes foolproof ID [Электронный ресурс] / E. Smalley // Technology Research News. – 2002. – Режим доступа: http://www.trnmag.com/Stories/2002/100202/Plastic_tag_makes_foolproof_ID_100202.html (дата обращения 14.10.2015).

35. Kravolec, E. Plastic tag makes foolproof ID / E. Kravolec // Technology Research News. – 2002. – Vol. 2. – P.75–85.

36. Anderson, R. Security Engineering: a guide to building dependable distributed systems/ R. Anderson// Wiley. – 2001. – P. 251 – 252.

37. Goorden, S.A. Quantum-Secure Authentication of a Physical Unclonable Key / S.A. Goorden // Optica.– 2014. – Vol, issue 1. – N. 6. – P. 421-424.

38. Лопатин, В.В. Электрический разряд и его технологические применения/ В.В. Лопатин, И. И. Сквирская // Известия Томского политехнического университета". – 2003. – Т. 306. – № 1. – С. 128-132.

39. Малюшевская, А.П. Электроразрядная обработка сырьевых компонентов для изготовления облегченных строительных изделий/ А.П. Малюшевская, П.П. Малюшевский // Электронная обработка материалов. –2012. – № 48(5). – С. 112–119.

40. Металлы и сплавы. Справочник/ Под редакцией Ю.П. Солнцева. – СПб.: НПО «Профессионал», НПО «Мир и семья». – 2003. – 1066 с.

41. Усов А.Ф. Исследования в области разработки электроимпульсных технологий / Усов А.Ф. // Проблемы энергетики запада Европейского Севера России. – Апатиты: КНЦ РАН. – 1999. – С. 70 – 86.

42. Носуленко В.И. Размерная обработка металлов электрической дугой / В.И. Носуленко // Электронная обработка материалов. – 2005. – № 1. – С. 8-17.

43. Шкилев В.Д., Адамчук А.Н. Об уникальности набора пятен, полученных электроразрядным способом / В.Д. Шкилев, А.Н. Адамчук // Электрическая размерная обработка материалов. – Т.44. – №5. – 2009. – С. 4 – 5.

44. Пат. 2408929 Российская Федерация, МПК G 06 K 1/12. Способ изготовления штрих-кода [Электронный ресурс] / Шкилев В.Д.; заявитель и патентообладатель Шкилев В.Д. – № 2000131736/09; заявл. 18.12.2008; опубл. 10.01.2011, Бюл. N 23. - 7 с.: ил.

45. Беккель, Л.С. Принцип Паули и возможности его применения в макромире / Л.С. Беккель, В.Д. Шкилев // Наукоемкие технологии в приборо- и машиностроении и развитие инновационной деятельности в вузе: сб. тр. Всеросс. науч.-техн. конф. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2015. – Т. 4. – С. 203-207.

46. Шкилев, В.Д. О методологии исследования стохастических процессов / В.Д. Шкилев, Л.С. Беккель // Наукоемкие технологии в приборо- и машиностроении и развитие инновационной деятельности в вузе: сб. тр. Всеросс. науч.-техн. конф. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2015. – Т. 5. – С. 281-284.

47. Классификация угроз информационной безопасности [Электронный ресурс] – Режим доступа: https://rvision.pro/blog-posts/klassifikatsiya-ugroz-informatsionnoj-bezopasnosti/ (дата обращения 08.07.2019).

48. ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий (с Поправкой) [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200048398. (дата обращения 30.04.2019).

49. Методика определения угроз безопасности информации в информационных системах (ФСТЭК России): Утв. 2015 г. [Электронный ресурс]. – Режим доступа: https://fstec.ru/component/attachments/download/812. (дата обращения 08.07.2019 г.).

50. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных: Утв. ФСТЭК России от 14.02.2008. [Электронный ресурс]. – Режим доступа:

http://www.consultant.ru/document/cons_doc_LAW_77814/. (дата обращения 04.07.2019).

51. Бубнова, М.С. Этикетка и упаковка – признак идентификации подлинности товара/ М.С. Бубнова // Регионы России: защита от контрафакта. 1-я Всероссийская выставка-форум. – 2003. – С. 19.

52. Сущенок, О.А. Оценка эффективности работы биометрических систем [Электронный ресурс] / О.А. Сущенок // Системи обробки інформації. – 2011. – № 4(94). – Режим доступа: https:// www.hups.mil.gov.ua › periodic-app › article › soi_2011_4_22 (дата обращения 15.03.2019).

53. Беккель, Л.С. Определение вероятностей ошибок первого и второго рода при использовании нового метода идентификации бумажных документов/ Л.С. Беккель // Системы высокой доступности. – 2019. - № 4. – С. .

54. Сравнительный анализ сканеров Graphtec CS510EN и Contex [Электронный ресурс]. – Режим доступа: http://www.jetcom.ru/articles/graphtec-vs-contex.html. (дата обращения 28.11.2019).

55. Мошенники успешно освоили IT-технологии [Электронный ресурс]. – Режим доступа: http://www.ng.ru. (дата обращения 28.11.2019).

56. Одаренные дети – ресурс человеческого потенциала современной России [Электронный ресурс]. – Режим доступа: http://www.iq.hse.ru. (дата обращения 28.11.2019).

57. Население России: численность, динамика, статистика [Электронный ресурс]. – Режим доступа: http://www.statdata.ru. (дата обращения 28.11.2019).

58. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации (ФСТЭК России): Утв. 30.03.1992 г. [Электронный ресурс]. – Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/387-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g4. (дата обращения 28.11.2019 г.).

59. Иванов, В.П. Математическая оценка защищенности информации от несанкционированного доступа [Электронный ресурс]. – Режим доступа: https://docplayer.ru/38529736-Matematicheskaya-ocenka-zashchishchennosti-informacii-ot-nesankcionirovannogo-dostupa.html. (дата обращения 28.11.2019 г.)

60. Месяц, Г.А. Импульсная энергетика и электроника / Г.А. Месяц. – М.: Наука, 2004. – 704 с.

61. Месяц, Г.А. Генерирование мощных наносекундных импульсов / Г.А. Месяц. – М.: Сов. Радио. – 1974.

62. Воробьев, Г.А. Физика диэлектриков (область сильных полей). Учебное пособие/ Г.А. Воробьев [и др.] – Томск: Изд-во Томского ун-та, 2003. – 242 с.

63. Allen, K.L. Mechanism of Spark Breakdown / K.L. Allen, L. Philips // Electrical Rev. – 1963. – Vol. 173. – N 3. – P. 779-783.

64. Григорьев, А.Н. Электрический разряд по поверхности твердого диэлектрика. Ч. 1. Особенности развития и существования поверхностного разряда/ А.Н. Григорьев [и др.] // Известия Томского политехнического университета. – 2006. – Т. 309. – № 1. – С. 66 – 69.

65. Krile, J.T. DC flashover of a dielectric Surface in atmospheric conditions / J.T. Krile [e.a.] // IEEE Trans. Plasma Sci. – 2004. – V. 32. –N. 5. – P. 1828-1834.

66. Карпов, Д.И. Моделирование инициирования и роста разрядных структур в жидких диэлектриках: автореф. дисс. … канд. физ.-мат. наук: 01.04.07 / Карпов Денис Иванович – Томск, 2003. – 20 с.

67. Курец, В.И. Электроразрядные технологии обработки и разрушения материалов. Учебное пособие. / В.И. Курец [и др.] – Томск: Изд-во ТПУ, 2012. – 272 с.

68. Саушкин, Б.П. Электрический разряд в жидких и газовых средах – основа нового поколения методов и технологий машиностроительного производства / Б.П. Саушкин //Электронная обработка материалов. – 2004. – № 1. – С. 4–17.

69. Мак-Доналд, А. Сверхвысокочастотный пробой в газах/ А. Мак-Доналд; пер. с англ. Савченко М.М., Франк А.Г. – М. : Мир, 1969. – 206 с.

70. Бутенко, В.А. Техника высоких напряжений. Учебное пособие./ В.А. Бутенко [и др.] – Томск: Изд-во ТПУ, 2008. – 118 с.

71. Прахова, М.Ю. Электротехнические материалы: учеб. пособие / М.Ю. Прахова, Н.А. Ишинбаев. – Уфа: Изд-во УГНТУ, 2000. – 139 с.

72. Поляков, З.И. Электрофизические и электрохимические методы обработки. Учебное пособие / З.И. Поляков [и др.]. – 2-е изд., перераб. и доп. – Челябинск: Изд-во ЮУрГУ, 2006. – 89 с.

73. Тарасова, Л.В. Современные представления о механизме электрического пробоя в высоком вакууме/ Успехи физических наук. – 1956. – Т. LVIII. – Вып. 2. – С. 321–346.

74. Шкилев, В.Д. О некоторых особенностях формирования идентификационных меток, полученных электроразрядным способом / В.Д. Шкилев, Л.С. Беккель // Наукоемкие технологии в приборо- и машиностроении и развитие инновационной деятельности в вузе: сб. тр. Всеросс. науч.-техн. конф. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2016. – Т. 4. – С. 70-74.

75. Беккель, Л.С. Концепция разработки метода идентификации объекта по его невоспроизводимой стохастически нанесенной метке / Л.С. Беккель, В.Д. Шкилев //XXI век: итоги прошлого и проблемы настоящего плюс. Научно-методический журнал. – 2016. – №06 (34). – С. 184-187.

76. Шкилев, В.Д. Универсальный метод идентификации объектов материальных ресурсов / В.Д. Шкилев, Л.В. Лысенко, А.К. Горбунов, Л.С. Беккель // Электронный журнал: наука, техника и образование. – 2017. – №01 (10). – С. 90-100.

77. Шкилев, В.Д. О барьерном разряде и квантово-волновых дорожках / В.Д. Шкилев, Л.С. Беккель // Электронный журнал: наука, техника и образование. – 2017. – № СВ1 (11). – С. 164-171.

78. Пат. на изобретение 2639176 Российская Федерация, МПК С 21 С 7/00 , С 22 С 1/00. Способ легирования металлов и сплавов// Шкилев В.Д., Хайченко В.Е., Филиппова И.А., Беккель Л.С., Головачева Ю.Г.; заявитель и патентообладатель Шкилев В.Д., Хайченко В.Е., Филиппова И.А., Беккель

Л.С., Головачева Ю.Г. – № 2006136024/09; заявл. 02.11.2016; опубл. 20.12.2017, Бюл. № 35. - 7 с.: ил.

79. Пат. на изобретение RU 2647375 Российская Федерация, МПК G 07 D 7/00. Денежная купюра, способ ее изготовления и способ подтверждения ее истинности и индивидуальности // В.Д. Шкилев, Л.С. Беккель, Д.В. Шкилев. заявл. 04.03.2016; опубл. 15.03.2018. Бюл. № 8. – 7 с.: ил.

80. Официальный сайт ShotCode [Электронный ресурс]. – Режим доступа: http://web.archive.org/web/20060412031020/http://www.shotcode.com:80/ (дата обращения 15.12.2015).

81. Официальный сайт Ez code [Электронный ресурс]. – Режим доступа: http://www.scanlife.com/ (дата обращения 15.12.2015).

82. Официальный сайт Microsoft Tag [Электронный ресурс]. – Режим доступа: http://tag.microsoft.com/consumer/index.aspx (дата обращения 15.12.2015).

83. Ла, Море Роберт де. Штриховые коды и другие системы автоматической идентификации: учеб. пособие / Ла Море Р. де; пер. с англ. Л. Леймонта. – М.: Изд-во МГУП, 1999. – 195 с.: ил.

84. Silver Bay Software. Maxicode Encoder. Programmer's Manual [Электронный ресурс]. – Режим доступа: http://www.silverbaytech.com/files/maxicode/maxi_api.pdf (дата обращения 23.11.2015).

85. ГОСТ Р 51294.6-2000 (ИСО/МЭК 16023-2000) Автоматическая идентификация. Кодирование штриховое. Спецификация символики MaxiCode (Максикод) [Электронный ресурс]. – Режим доступа: http://engenegr.ru/gost-r-51294-6-2000 (дата обращения 25.12.2015).

86. Сайт компании Denso-Wave [Электронный ресурс]. – Режим доступа: http://www.denso-wave.com/en/index.html (дата обращения 05.01.2016).

87. ГОСТ Р ИСО/МЭК 18004-2015 Информационные технологии. Технологии автоматической идентификации и сбора данных. Спецификация символики штрихового кода QR Code [Электронный ресурс]. – Режим доступа: http://www.internet-law.ru/gosts/gost/60057/ (дата обращения 05.02.2016).

88. Грошев, А.С. Информатика: учеб. для вузов/ А.С. Грошев, П.В. Закляков. – 3-е изд., перераб. и доп. М.: ДМК Пресс, 2015. – 588 с.: ил.

89. ГОСТ Р ИСО/МЭК 16022-2008 Автоматическая идентификация. Кодирование штриховое. Спецификация символики Data Matrix [Электронный ресурс]. – Режим доступа: http://gostexpert.ru/gost/gost-16022-2008 (дата обращения 05.01.2016).

90. ГОСТ Р ИСО/МЭК 24778-2010 Информационные технологии. Технологии автоматической идентификации и сбора данных. Спецификация символики штрихового кода Aztec Code [Электронный ресурс]. – Режим доступа:http://vsegost.com/Catalog/49/49839.shtml (дата обращения 05.01.2016).

91. QR Code Essentials [Электронный ресурс] / Denso ADC. – Режим доступа: http://www.nacs.org/LinkClick.aspx?fileticket=D1FpVAvvJuo%3D&tabid=1426&mid=4802 (дата обращения 17.02.2016).

92. ГОСТ Р 51294.9-2002 (ИСО/МЭК 15438-2001) Автоматическая идентификация. Кодирование штриховое. Спецификации символики PDF417 (ПДФ417) [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200030464 (дата обращения 05.01.2016).

93. Иванов, Д.В. Алгоритмические основы растровой машинной графики/ Д.В. Иванов [и др.]. – М.: Бином. Лаборатория знаний, 2013. – 284 с.

94. Роджерс, Д.Ф. Алгоритмические основы машинной графики / Д.Ф. Роджерс; пер. с англ. Баяковского Ю.М., Галактионова В.А. – М.: Книга по Требованию, 2013. – 512 с.

95. Демин, А.Ю. Основы компьютерной графики: учеб. пособие / А.Ю. Демин. – Томск: Изд-во Томского политехнического университета, 2011. – 191 с.

96. Keith, J. Video Demystified: A Handbook for the Digital Engineer / J. Keith. – 5-th ed. – Burlington: Newnes, 2013. – 889 p.

97. Poynton, C. Digital Video and HDTV. Chapter 24/ C. Poynton. – Waltham: Morgan Kaufmann, 2012. – 709 p.

98. Shapiro, L. G. Computer Vision / Linda G. Shapiro, George C. Stockman. – New Jersey, PrenticeHall, 2001. – Pp. 279–325.

99. Otsu, N. A threshold selection method from gray-level histogram/ N. Otsu// IEEE Transactions on System Man Cybernetics. – 1979. – Vol. SMC-9. – No. 1. – Pp. 62-66.

100. Liao, P. A Fast Algorithm for Multilevel Thresholding / P. Liao, T. Chen, P. Chung // Journal of Information Science and Engineering. – 2001. – Vol. 17 (5). – Pp. 713–727.

101. Беккель, Л.С. Анализ и обработка изображений стохастически нанесенных меток / Л.С. Беккель, В.Д. Шкилев //XXI век: итоги прошлого и проблемы настоящего плюс. Научно-методический журнал. – 2016. - №06 (34). – С. 30-34.

102. Центр масс [Электронный ресурс] // Словари и энциклопедии на Академике. – Режим доступа: https://dic.academic.ru/dic.nsf/bse/148615/ (дата обращения 14.04.2015).

103. Василенко, С.Л. Центр масс плоских фигур в точках золотого сечения [Электронный ресурс] / С.Л. Василенко // «Академия Тринитаризма». – 2010. – № 77-6567. – Режим доступа: http://www.trinitas.ru/rus/doc/0016/001c/1661-vs.pdf (дата обращения 15.05.2015).

104. Олофинская, В.П. Техническая механика / В.П. Олофинская. – М.: Форум Инфа-М, 2005. – 349 с.

105. Brown, J. QR Code Demystified – Part 3 [Электронный ресурс] / J. Brown. – Режим доступа: https://www.matchadesign.com/news/blog/qr-code-demystified-part-3/ (дата обращения 15.04.2015).

106. Сагалович, Ю. Л. Введение в алгебраические коды/ Ю. Л. Сагалович. – М.: МФТИ, 2007. — 262 с.

107. Brown, J. QR Code Demystified – Part 4 [Электронный ресурс] / J. Brown. – Режим доступа: https://www.matchadesign.com/news/blog/qr-code-demystified-part-4/ (дата обращения 15.04.2015).

108. Brown, J. QR Code Demystified – Part 5 [Электронный ресурс] / J. Brown. – Режим доступа: https://www.matchadesign.com/news/blog/qr-code-demystified-part-5/ (дата обращения 15.04.2015).

109. Беккель, Л.С. Алгоритм работы автоматизированной системы для нового метода идентификации бумажных документов / Л.С. Беккель, В.Д. Шкилев //XXI век: итоги прошлого и проблемы настоящего плюс. Научно-методический журнал. – 2017. - №04 (38). – С. 47-53.

110. Беккель, Л.С. Расчет напряжения электрического поля для пробоя промежутка «воздух – твердый диэлектрик»/ Л.С. Беккель, В.Д. Шкилев, А.П. Коржавый // Электромагнитные волны и электронные системы. – 2018. - № 8. - С. 46-52.

111. Беккель, Л.С. Анализ результатов работы автоматизированной системы идентификации изображений стохастически нанесенных меток / Л.С. Беккель, В.Д. Шкилев //XXI век: итоги прошлого и проблемы настоящего плюс. Научно-методический журнал. – 2017. - №04 (38). - С. 54-58.

112. Беккель, Л.С. Исследование явления интерференции при электрическом пробое твердого диэлектрика/ Л.С. Беккель, В.Д. Шкилев, А.П. Коржавый //Электромагнитные волны и электронные системы. – 2018. - №6. - С. 25-29.

113. Beckel, L.S. Non-replicable object surface development for its automatic identification / L.S. Beckel, V.D. Shkilev // IOP Conference Series: Materials Science and Engineering, 450(5) 052013, 2018. – 5 p.

Приложение 1

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАТЕНТ

НА ИЗОБРЕТЕНИЕ

№ 2647375

ДЕНЕЖНАЯ КУПЮРА, СПОСОБ ЕЕ ИЗГОТОВЛЕНИЯ И СПОСОБ ПОДТВЕРЖДЕНИЯ ЕЕ ИСТИННОСТИ И ИНДИВИДУАЛЬНОСТИ

Патентообладатели: ***Шкилев Владимир Дмитриевич (RU), Беккель Людмила Сергеевна (RU), Шкилев Дмитрий Владимирович (RU)***

Авторы: ***Шкилев Владимир Дмитриевич (RU), Беккель Людмила Сергеевна (RU), Шкилев Дмитрий Владимирович (RU)***

Заявка № **2016107875**
Приоритет изобретения **04 марта 2016 г.**
Дата государственной регистрации в Государственном реестре изобретений Российской Федерации **15 марта 2018 г.**
Срок действия исключительного права на изобретение истекает **04 марта 2036 г.**

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев