ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»
(Н И У « Б е л Г У »)

ИНСТИТУТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ И ЕСТЕСТВЕННЫХ НАУК

КАФЕДРА ИНФОРМАЦИОННЫХ И РОБОТЕХНИЧЕСКИХ СИСТЕМ

АНАЛИЗ, ИССЛЕДОВАНИЕ И РАЗРАБОТКА СИСТЕМ ЦИФРОВОЙ ИДЕНТИФИКАЦИИ ТОВАРОВ

Магистерская диссертация
обучающегося по направлению подготовки
09.04.02 Информационные системы и технологии
заочной формы обучения,
группы 07001635
Черкашина Павла Викторовича

Научный руководитель
к.т.н, доцент Гахов Р.П.

Рецензент
к.т.н. доцент
Прохоренко Е.И.

БЕЛГОРОД 2018

РЕФЕРАТ

Анализ, исследование и разработка систем цифровой идентификации товаров – Черкашин Павел Викторович, диссертация на соискание учёной степени магистра, Белгород, Белгородский государственный национальный исследовательский университет (НИУ «БелГУ»)

Магистерская диссертация состоит из введения, трёх разделов, заключения и списка использованной литературы, включает 73 страниц, содержит 6 рисунок и 2 таблицы., 11 формул и приложения.

КЛЮЧЕВЫЕ СЛОВА: информационная система, криптографическая защита информации, ФГИС МДЛП, ЕГАИС.

ОБЪЕКТ ИССЛЕДОВАНИЯ: процесс цифровой идентификации товаров

ПРЕДМЕТ ИССЛЕДОВАНИЯ: метод маркировки и алгоритмы мониторинга движения товаров.

МЕТОДЫ ИССЛЕДОВАНИЯ: средства алгоритмического моделирования, технологии программирования, обоснование разработки системы.

ПОЛУЧЕННЫЕ РЕЗУЛЬТАТЫ: разработаны алгоритмы алгоритм обмена данными для системы цифровой идентификации; алгоритм формирования криптографически стойкого маркера; проведено тестирование разработанных алгоритмов в рамках работы тестового приложения.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Отечественные технологии криптографии позволяют гарантировать защиту информации. Проще говоря, цифровой код маркировки будет невозможно украсть или массово подделать. Генерирует код не производитель, который может испытывать соблазн делать что-то в третью смену, а специально уполномоченный государством единый оператор. Злоумышленник не может перехватить или скопировать коды, поскольку технологии обеспечивают их уникальность и непредсказуемость. Специалисты отмечают, что цифровая маркировка в её новом виде позволит избежать проблем, возникавших в ЕГАИС на алкогольном рынке, в котором используется американский криптографический алгоритм с открытым ключом RSA. Или сложностей в ИС «Маркировка» в фармацевтической отрасли, где недостаточная защита шифрования кода не позволяла справиться с поддельными лекарствами.

Данная работа посвящена системам цифровой идентификации товаров, основная задача данных систем — это борьба с контрафактной продукцией на рынке, защита потребителя и производителя различных ценных или жизненно необходимых товаров.

Контрафактной продукцией называется продукция, произведённая с нарушением прав на интеллектуальную собственность. Контрафактная продукция часто нарушает исключительные права на товарный знак. Контрафактной продукция становится в случае, если на ней незаконно размещают чужие товарные знаки, или схожие с ними обозначения, способные ввести покупателей в заблуждение.

Оборот на рынке контрафактной продукции наносит экономический ущерб производителям и импортёров различных товаров верхней ценовой категории. Существенно больший ущерб наносит оборот контрафактных товаров категории первой необходимости, или применяющихся в критически важных областях. Например, это детали сложных механизмов в авиации, техника

и аппаратура, применяемые в экстремальных условиях окружающей среды и условиях экстремальной нагрузки.

Также, к таковым относятся лекарственные препараты. Оборот поддельных и просроченных лекарственных препаратов наносит огромный ущерб экономике и здравоохранению. В настоящее время фармацевтический рынок Российской Федерации насчитывает 337,8 млн. упаковок лекарственных препаратов. По оценке Минэкономразвития России, подделывается примерно 10% общего оборота лекарственных средств.

По данным доклада Организации экономического сотрудничества и развития (ОЭСР):

– годовой оборот контрафактной продукции в мире в 2015 году достиг $461 млрд;
– на долю контрафактной продукции в мире приходится примерно 2,5% мирового импорта;
– на рынке стран Европейского союза подделки занимают около 5% от общего объёма торговли;
– наиболее часто подделывают продукцию из США (20%), Италии (15%), Франции и Швейцарии (по 12%), Японии и Германии (по 8%) [3].

В различных сферах экономики в Российской федерации применяются, вводятся или разрабатываются различные системы цифровой идентификации товаров, услуг, или, например, транзакций. Данные системы применяются для мониторинга движения товаров, защиты от приобретения поддельных или просроченных товаров, а также, для защиты от недобросовестных действий участников товарооборота.

Целью магистерской диссертации является совершенствование процесса цифровой идентификации товаров за счёт разработки алгоритма формирования цифрового идентификатора и алгоритма мониторинга движения товара

Задачи магистерской диссертации:

– анализ существующих систем маркировки и мониторинга движения товаров;

– обоснование значимости и актуальности объекта проектирования;

– построение моделей бизнес-процессов и обоснование разработки информационной системы для маркировки товаров и мониторинга движения товаров;

– разработка алгоритма обработки информации для систем цифровой идентификации и алгоритма формирования маркера.

– Объектом исследования выступает процесс цифровой идентификации товаров, предметом являются метод маркировки и алгоритмы мониторинга движения товаров.

Методы исследования, применяемые в диссертации средства алгоритмического моделирования, технологии программирования, обоснование разработки системы.

Магистерская диссертация состоит из введения, трёх разделов, заключения и списка использованной литературы, включает 73 страниц, 17 рисунков, 5 таблиц, 11 формул и приложения.

1 Анализ и исследование предметной области

Организация экономического сотрудничества и развития (ОЭСР) предоставила информацию о количестве контрафактной продукции в мире. По данным ОЭСР, только за 2013 год количество контрафактных товаров составило 2,5% всего мирового импорта, объем торговли подделками превысил 461 миллиард долларов. Чаще всего, как утверждают специалисты, подделываются американские, итальянские и французские бренды.

Организация экономического сотрудничества провела исследование продукции, на которую поступали жалобы на нарушение прав патентов, товарных знаков и авторских прав (за исключением интернет-пиратства). По итогам исследования выяснилось, что контрафактом являются около 5% всех товаров, импортированных на территорию Евросоюза. По приведённой статистике наиболее часто подделкам подвергаются бренды из: США (20%); Италии (15%); Швейцарии и Франции (12%); Германии и Японии (8%).

Проблема оборота на фармацевтическом рынке фальсифицированных средств приобретает характер национального бедствия во многих странах. По статистике ВОЗ, фальсификация лекарств считается четвертым злом здравоохранения после малярии, СПИДа и курения, а смертность от побочных реакций лекарств входит в первую пятёрку причин наравне с сердечно-сосудистыми, онкологическими, бронхолёгочными заболеваниями и травматизмом. За последние 40 лет поддельные лекарства в мире унесли жизни 200 тысяч человек.

Кроме того, фармацевтический контрафакт, наносит ущерб производителям легальных средств, как напрямую, посредством нечестной конкуренции, так и косвенно, посредством подрыва репутации.

Фармацевтический рынок РФ является одним из самых крупных в мире, и лидирует как по числу производителей и импортёров, так и по количеству наименований лекарственных средств. Но в отличии от фармацевтического рынка, например, Европейского союза, он весьма слабо стандартизирован, что

затрудняет применение стандартных промышленных роботов и средств проверки ЛС. Тем не менее, ответственность за распространение фармацевтического контрафакта будут нести конечные звенья системы – аптеки, часть из которых содержится за счёт бюджетных средств, а последствия отразятся в первую очередь на потребителях.

Кроме того, отечественный рынок лекарственных средств подвержен общему веянию времени – широкому распространению интернет-аптек, и магазинов фармацевтических препаратов. Это явление ухудшает криминогенную статистику данного рынка по всему миру. Диапазон поддельных изделий, поступающих на рынки, расширяется по мере увеличения коммерческого использования сети Интернет, обеспечивающей огромную и разветвлённую сеть для продажи как фирменных лекарств, так и дженериков. По данным ВОЗ, в более чем 50% случаев лекарства, приобретённые через Интернет на незаконных сайтах, скрывающих свои физические адреса, являются поддельными [7].

За первое полугодие 2017 года таможенные органы Российской Федерации выявили свыше 5,6 млн. единиц контрафактной продукции. Таможенными органами предотвращён ущерб, который мог быть нанесён правообладателям, на сумму более 1,1 млрд. рублей. Возбуждено 556 дел об административных правонарушениях, из них 545 – о незаконном использовании чужого товарного знака.

Предметами правонарушений в сфере интеллектуальной собственности чаще всего являются одежда, обувь, автозапчасти, текстиль, бижутерия, сувенирная продукция, продукты питания.

Наибольшее количество контрафактных товаров за первое полугодие 2017 года выявлено в Центральном, Северо-Западном, Южном регионах Российской Федерации.

Особое значение для защиты прав владельцев торговых марок имеет Таможенный реестр объектов интеллектуальной собственности, который ведёт Федеральная таможенная служба. По состоянию на 31 августа 2017 года в

таможенном реестре находится 4506 объектов интеллектуальной собственности, принадлежащих как зарубежным, так и российским компаниям. За 8 месяцев 2017 года в реестр было включено 211 объектов интеллектуальной собственности. В товарной структуре таможенного реестра преобладают алкогольные напитки, кондитерские изделия, спортивная одежда и обувь.

В России ежегодный объем контрафактной торговли оценивается в $4 миллиарда долларов. Согласно информации, опубликованной на сайте Таможенного информационного сервера TKS.RU, чаще всего объектами контрафакта являются лекарства, алкоголь, табачная продукция, одежда, обувь, минеральные воды и соки, автозапчасти. При этом доля незаконного оборота таких товаров в некоторых секторах доходит до 40%.

1.1 Введение в предметную область

Для отличия оригинальной продукции от подделок могут использоваться защита от вскрытия упаковки и присвоение серийного номера в сочетании с технологиями определения подлинности, что обеспечит производителям оригинальных фармацевтических продуктов несколько уровней защиты.

Защита от вскрытия упаковки – первый этап в стратегии защиты, который осуществляется с помощью разработки упаковки, например, с такими особенностями, как перфорация, предназначенная для её вскрытия. Присвоение серийного номера – второй уровень защиты: на каждую упаковку наносится уникальный серийный номер, который включается в производственную базу данных. Любые иные упаковки с тем же серийным номером будут отмечаться как подозрительные. И наконец, определение подлинности – третий уровень защиты с применением открытых, скрытых методов и методов судебной экспертизы. Открытые методы, такие как видимые голограммы или изменение цвета, используются на упаковке продукта, в то время как скрытые элементы, такие как инфракрасная и ультрафиолетовая краска, а также микротекст, доступны для считывания только с помощью специализированного оборудования. Продукция, защищённая на уровне судебной экспертизы,

например, с помощью молекулярных маркеров и биологических индикаторов, должна исследоваться в лаборатории.

До 2024 года в России должна быть создана система полной прослеживаемости оборота товаров от производителя до конечного потребителя. С 2016 года в России обязательна маркировка изделий из меха, с февраля 2017-го стартовала добровольная маркировка лекарств (обязательной она станет с 2020 года), с января 2018-го начался почти годовой экспериментальный период по маркировке табачной продукции. С 1 июня 2018 года начнётся маркировка обуви.

В декабре 2017 года президент Владимир Путин одобрил идею создания единого оператора системы цифровой маркировки товаров в России на базе ООО «Оператор-ЦРПТ», «дочки» Центра развития перспективных технологий (ЦРПТ, принадлежит структурам миллиардера Алишера Усманова, госкорпорации «Ростех» и компании инвестора Александра Галицкого). Оператор, в частности, уже участвует в эксперименте по маркировке табачной продукции.

С 1 июня 2018 года в России начнётся эксперимент по маркировке драгметаллов и камней, а также изделий из них. Соответствующее постановление премьер-министр России Дмитрий Медведев подписал 24 марта 2018 года.

Уполномоченными организациями на проведение эксперимента, который продлится до 1 ноября, являются Минфин, Федеральная таможенная служба, Федеральная налоговая служба, Росфинмониторинг, а также Гохран России и Российская государственная пробирная палата. До 1 декабря 2018 года Минфин должен провести оценку итогов эксперимента и представить отзыв в правительство, которое примет решение об эффективности введения маркировки для этой группы товаров.

В отличие от других групп товаров (табак, обувь), оператором и разработчиком интегрированной информационной системы в сфере контроля за оборотом драгоценностей будет АО «Гознак». Компания сама предложила взять

на себя эти функции и будет осуществлять их на безвозмездной основе, отмечается в постановлении. В ЦРПТ не стали комментировать наделение функциями оператора по маркировке драгоценностей Гознака. В самом Гознаке также не смогли оперативно предоставить комментарий.

До 2 апреля Гознаку предстоит определить требования к самой информационной системе и обеспечению защиты содержащихся в ней данных. Каким образом будет реализована маркировка изделий, определит Минфин. Ранее предполагалось, что на бирках ювелирных изделий будет размещён QR-код, который поможет покупателю проверить их подлинность, позже на изделиях появится нанометка.

1.2 Исследование существующих систем

Технология отслеживания и контроля представляет собой один из методов присвоения серийного номера, благодаря которому руководители могут защищать свой канал поставок от проникновения контрафактной продукции и отслеживать сроки годности товара. Преимущество такой защиты состоит в том, что существует возможность регистрировать серийный номер продукта на общем сервере или на самом продукте на любом из этапов поставки; это способствует обнаружению контрафактной продукции в канале поставок. Данный способ защиты также позволяет полностью отслеживать продукцию в глобальном масштабе.

Принцип работы таких систем заключается в нанесении уникального идентификационного кода на каждый продукт после того, как он был упакован. Код присваивается, затем активируется, проверяется и вносится в базу данных, где его можно сравнить со всеми сериализованными кодами в канале поставки.

Одним из примеров подобной системы, внедряемой в ЕС, является решение Bosch Packaging Technology по отслеживанию и контролю продукции.

Здесь используется модуль системы нанесения кода на картонные короба (CPS), состоящий из принтера, который наносит код на каждый продукт, и камеры. Для отслеживания отдельных продуктов на каждую упаковку наносится

уникальный серийный номер и дата истечения срока годности, а также номер партии и глобальный номер товара (GTIN). Система кодирует данные в машиночитаемый двухмерный матричный код. Напечатанные данные для отслеживания автоматически проверяются на точность камерой, которая считывает и распознает каждый напечатанный символ с помощью инструмента оптического распознавания и проверки символов (OCR/OCV). Пример данной маркировки приведён на рисунке 1.1.

Рисунок 1.1 – Пример маркировки, предлагаемый Bosch Packaging Technology

В течение миллисекунд она сличает понятный для человека текст с двухмерным матричным кодом. Все данные, считанные камерой, хранятся в главной базе данных, что позволяет производить контроль и отслеживать продукцию. Рисунок 1.2 демонстрирует нам внешний вид промышленного оборудования BOSCH необходимого для функционирования их системы контроля ЛС .

Рисунок 1.2 – Фотография промышленного оборудования отслеживания и контроля от компании Bosch

Однако данные технологии маркировки не регламентированы на территории Российской федерации, и их внедрение вне нашей компетенции. Как мы уже говорили в начале данного раздела, стоящая перед нами задача в значительной степени нетривиальна.

1.2.1 Система ФГИС МДЛП

С начала 2015 года в СМИ стала появляться информация, о том что министерство здравоохранения Российской федерации ведёт работы в направлении борьбы с контрафактной продукцией на Российском рынке. Принимаемые меры носят законодательно-организационный характер, например, в Августе 2015 года был издан приказ «Об утверждении Порядка осуществления выборочного контроля качества лекарственных средств для медицинского применения», позволяющий увеличить жёсткость контроля со стороны Росздравнадзора за производителями и импортёрами, и требующий от них сообщения серийных сведений обо всех поставляемых на рынок лекарственных [4].

Эти данные крайне важны для осуществления проекта Минздрава по созданию «Федеральной государственной информационной системы мониторинга движения лекарственных препаратов от производителя до конечного потребителя с использованием маркировки» (ФГИС МДЛП) аналогично существующей ЕГАИС.

Согласно концепции ФГИС МДЛП её назначением является «мониторинг движения лекарственных препаратов (ЛП) от производителя до конечного потребителя с использованием маркировки (кодификации) и идентификации упаковок лекарственных препаратов в целях обеспечения эффективного контроля качества лекарственных препаратов, находящихся в обращении, и борьбы с их фальсификацией". Для обеспечения её функционирование уже принято решение комиссии ТС, три федеральных закона, 5 постановлений правительства и издано 4 приказа министерства здравоохранения.

ФГИС МДЛП организует непрерывный мониторинг движения лекарственных препаратов от производителя до конечного потребителя с использованием индивидуальной и групповой кодированной маркировки (сериализация и агрегация) и идентификации упаковок лекарственных препаратов в целях обеспечения эффективного контроля качества лекарственных препаратов, находящихся в обращении, и борьбы с их фальсификацией.

Для идентификации конкретного ЛП, конкретной серии ЛП, конкретной упаковки ЛП, система предписывает использовать специализированные графические маркеры, такие как QR код и Data Matrix, содержащие уникальный идентификатор данной единицы ЛП или партии, а также прочие необходимые для идентификации.

Функционирование данной системы так же упрощает мониторинг срока годности ЛП и упрощает процесс изъятия из оборота бракованных партий. В конечном итоге внедрение системы должно повысить уровень лекарственной безопасности в РФ, а так же привлечь население страны к защите собственных прав и интересов [5].

Однако же в тексте не говориться о каких-либо системах безопасности кроме доступа к сервисам системы межведомственного электронного взаимодействия (СМЭВ) посредством с использованием технологий электронной цифровой подписи (ЭП). Тем не менее, система с такой высокой общественной важностью и экономическим эффектом, обязана гарантировать достоверность сведений, содержащихся в маркировке ЛП и групповых кодах транспортной тары (ГК). Система в существующем виде остаётся уязвимой для недобросовестных участников её работы и крипто аналитиков, способных расшифровать алгоритм генерации индивидуальных кодов упаковки ЛП.

Рисунок 1.3 приводит концепцию организационной структуры функционирования будущей системы, взятую из проектной документации Росздравнадзора.

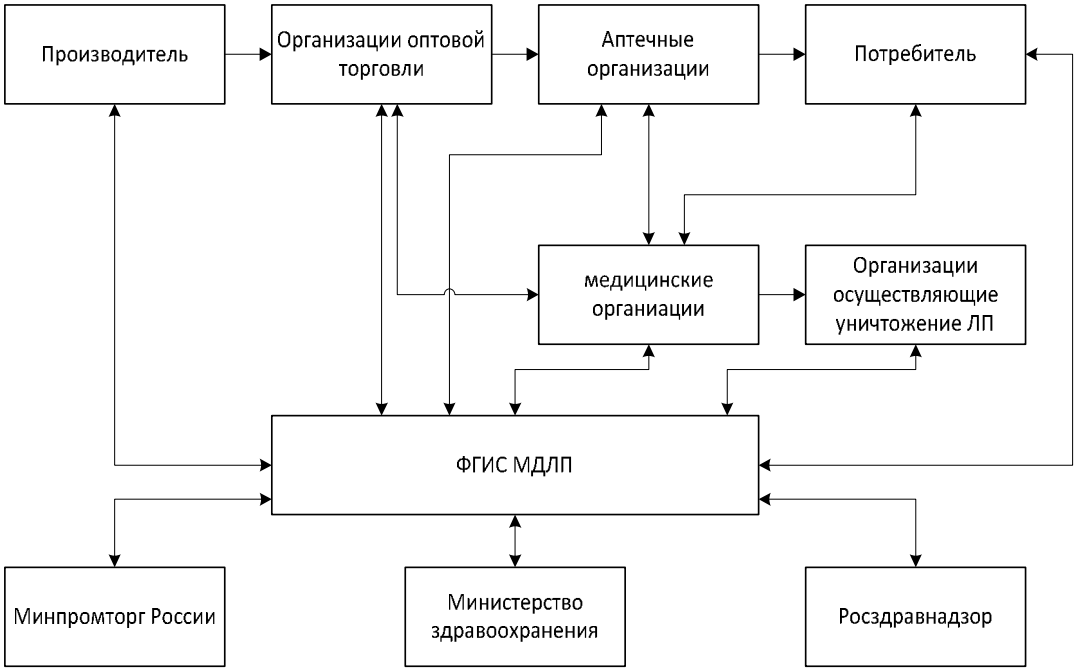

Рисунок 1.3 – Краткая организационная диаграмма информационного взаимодействия участников системы ФГИС МДЛП

На данный момент, ситуация с окончательным видом данной системы не определена. Пилотный проект по внедрению маркировки лекарств продлён до конца 2018 года. Согласно постановлению правительства Российской Федерации от 24 января 2017 года «О проведении эксперимента по маркировке

контрольными (идентификационными) знаками и мониторингу за оборотом отдельных видов лекарственных препаратов для медицинского применения» оператором информационной системы, осуществляющим обеспечение эксперимента, была определена Федеральная налоговая служба.

Росздравнадзор определил этапы подключения различных групп лекарственных препаратов к информационной системе «Маркировка».

Упомянутый федеральный закон предусматривает возможность поэтапного введения маркировки лекарственных препаратов. Этапы будут определяться правительством Российской Федерации.

Добровольный эксперимент по маркировке контрольными (идентификационными) знаками и мониторингу оборота отдельных видов лекарственных препаратов для медицинского применения проводился в рамках реализации приоритетного проекта «Лекарства. Качество и безопасность». В нем принимают участие более 1200 участников, которые уже промаркировали более 4 миллионов упаковок лекарств. С августа 2017 года первые маркированные лекарства появились в аптеках. В рамках эксперимента ФНС России доработала информационную систему «Маркировка» в целях использования её для мониторинга движения лекарств, а также разработала специальное мобильное приложение, позволяющее покупателям проверять их легальность. Эксперимент позволил определить эффективность и технические возможности системы, а также наметить направления её развития.

Согласно приказу Минздрава №866, аптечные и медицинские организации должны иметь рабочие места, оснащенные персональными компьютерами, устройствами считывания специальной маркировки, а также иметь ключи электронной подписи (ЭП), которые требуются для информационного взаимодействия с ФГИС МДЛП. Для работы с системой должно быть обеспечено подключение к Интернету. В случае отсутствия такой возможности информация может накапливается на компьютерном оборудовании аптечных и медицинских организаций и затем передаваться по определенному графику офлайн.

И, что совершенно логично, требуется доработать информационные системы аптечных и медицинских организаций в целях интеграции с ФГИС МДЛП для организации контроля на местах получения и отпуска лекарственных препаратов. Информация о всех операциях в процессе оборота ЛП должна автоматически передаваться из таких систем в ФГИС МДЛП. Для этого ФНС уже разработала и опубликовала описания интеграционных профилей для разработчиков учетных систем.

В частности, на данное время доступны:

– протокол обмена интерфейсного уровня, версия 2.6;

– схемы и форматы для разработчиков учетных систем.

Схема работы пользователей в режиме интеграции учетной системы с ФГИС МДЛП выглядит следующим образом:

Пользователь аптечного учреждения (или подразделения МО) получает лекарственный препарат от поставщика и сканирует маркировку (код коробки SSCC, код упаковки sGTIN).

Учётная система передаёт эти сведения в ФГИС МДЛП и получает от неё ответ.

Если ФГИС МДЛП «бракует» препарат – то сведения о нем автоматически фиксируются в системе, и он выводится из оборота. Такой препарат должен быть возвращён поставку для уничтожения – это подделка;

Если ФГИС МДЛП возвращает положительный ответ, то информация о таком поступлении фиксируется в учётной системе, с ней можно работать, в том числе осуществлять выписку и выдачу препарата пациентам.

В случае, если препарат перемещается между подразделениями аптечной или медицинской организации, эти сведения передаются в ФГИС МДЛП.

Как только препарат фактически израсходован (аптечная организация продала препарат пациенту или выдала его по льготному рецепту, или в стационаре осуществили расход препарата по врачебному назначению и т.д.) – учётная система должна передать эти сведения в ФГИС МДЛП, при этом

персональные данные пациента не передаются. Этим шагом учётная система выводит препарат из оборота в ФГИС МДЛП.

Отметим, что сервисы электронного взаимодействия на текущий момент находятся на стадии тестирования, что означает возможное изменение протоколов обмена — об этом красноречиво свидетельствуют информационные сообщения на сайте ФНС. Ожидается, что после завершения анализа результатов эксперимента методологические рекомендации к внедрению и использованию системы МДЛП могут быть расширены и дополнены, а также, что немаловажно для разработчиков, задействованных учётных систем, будут уточнены и технические детали интеграции.

В связи с этим мы рекомендуем в настоящее время проводить предварительные (начальные) мероприятия по оснащению и автоматизации аптечных и медицинских организаций в части учёта лекарственных препаратов, включая следующее:

Ознакомиться с актуальными НПА и описанием схемы работы системы, отслеживать изменения (тут рекомендуем пользоваться специализированными ресурсами ФНС и Росздравнадзора).

Разработать и издать приказ по организации о назначении ответственного за внедрение системы и создании соответствующей рабочей группы.

Осуществить подготовку рабочих мест сотрудников: оснастить их необходимым количеством персональных компьютеров (ПК), сканеров, закупить и установить усиленную квалифицированную электронную подпись (УКЭП), ПО для работы с ней, провести базовое компьютерное обучение.

Определиться и внедрить программный продукт для учёта движения ЛП, если это ещё не сделано.

Зарегистрироваться в системе по адресу mdlp.markirovka.nalog.ru. Для работы с системой придётся учесть технические требования: Операционная система — не старше Microsoft Windows 7 или Mac OS X 10.8, браузер не ниже Internet Explorer 10 или Safari, плагин и программное обеспечение «КриптоПро» по версии 3.6.7777 или позднее.

По возможности, провести работы с ФГИСЗ МДЛП хотя бы в тестовом режиме.

Для разработчиков аптечных систем и МИС МО реализация интеграции соответствующих учётных систем с ФГИСЗ МДЛП, на наш взгляд, пока является несколько преждевременной, по крайней мере, до публикации результатов эксперимента и официального утверждения финальных версий интеграционных механизмов. После того как эксперимент будет завершён и все необходимое программное обеспечение и сопроводительная документация ФГИСЗ МДЛП будут окончательно отлажены, можно будет приступить к детальной проработке данного вопроса и доработкам в части интеграции. Тем не менее, аптечным и медицинским организациям, а также разработчикам соответствующих информационных систем уже сейчас необходимо «подготовить почву» и активно готовиться к предстоящим работам.

Для уточнения вопросов и консультирования участников проекта (аптек и медицинских организаций) в регионах России созданы специализированные «Центры компетенций». Информацию о таком центре в своём регионе можно найти здесь.

Следует понимать, что внедрение системы затронет все бизнес-процессы, связанные с получением, реализацией и списанием лекарственных препаратов. Поэтому, если пока данные процессы не автоматизированы внутри самой медицинской организации, то данный вопрос следует решить в самое ближайшее время. Для этого предлагаем обратить внимание на продукт «КМИС.Аптека», позволяющий в полной мере решить данные задачи.

Полностью налаженные и автоматизированные процессы лекарственного обеспечения внутри организации с помощью «КМИС.Аптека» позволят в будущем сделать подключение МО к ФГИС МДЛП незаметным для пользователей. Для сотрудников АСУ значительно упростится решение технической стороны вопроса – после завершения отладки протоколов интеграции со стороны ФНС, МО, которая использует в своей работе

«КМИС.Аптека», вместе с обновлением получит новую версию продукта с готовым к эксплуатации интеграционным протоколом интеграции с МДЛП.

О перспективах развития системы. В планах развития системы, как отмечает министр здравоохранения России Вероника Скворцова, также стоит интеграция ФГИС МДЛП с информационно-аналитической системой (ИАС) мониторинга и контроля в сфере государственных и муниципальных закупок лекарственных препаратов, которая введена в промышленную эксплуатацию с 1 января 2018 г. Внедрение связки данных систем, совместно с использованием персонифицированного учета лекарственных средств, позволит взять под контроль весь процесс лекарственного обеспечения в рамках всей страны. При этом для работы этой системы Минздравом на основании Государственного реестра лекарственных средств (ГРСЛ) разработан единый справочник классификатор лекарственных препаратов (ЕСКЛП), а также выработаны единые принципы ведения и передачи соответствующих структурированных сведений. В настоящий момент, функционирование системы организованно так, что розничная торговля, выполняя функции фильтра, берет на себя и вину за появление контрафакта, этим фильтром выявленного, хотя при этом никак в этом не участвует.

1.2.2 Система ЕГАИС.

Данную аббревиатуру следует расшифровывать как «Единая государственная автоматизированная информационная система». Она предназначена для того, чтобы формировать базу данных об организациях, которые изготавливают алкогольную продукцию, а также предприятиях, которые заняты в сфере её реализации. Данная система производит учёт всех спиртных напитков. Собираются данные о том, где они были произведены, а также куда позже поставляются и, соответственно, в каких объёмах. Как работает ЕГАИС в рознице? Рассматриваемая программа предоставляет возможность контроля всего рынка производства и сбыта алкогольной продукции. В свою очередь, это помогает существенно уменьшить уровень

реализации несертифицированных товаров. Как система ЕГАИС начал работать двенадцать лет назад, однако только до начала прошлого года с ней приходилось сталкиваться исключительно поставщикам и фирмам-производителям. Согласно актуальному законодательству, с тех пор абсолютно все предприниматели и компании, которые заняты в сфере реализации сидра, пива, пуаре и медовухи, также вынуждены отчитываться в рассматриваемой программе. Это необходимо делать в процессе получения продукции от поставщика, впоследствии же, в момент продажи, дальнейший учет обязательным не является.

Основной функциональной целью системы ЕГАИС является обеспечение информационной и технологической поддержки задач, установленных Федеральным законом от 22 ноября 1995 г. № 171-ФЗ «О государственном регулировании производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции Продукты »:« ... Государственное регулирование в области производства и оборота этилового спирта, спиртовой и спиртосодержащей продукции направлено на защиту экономических интересов Российской Федерации, обеспечение потребностей потребителей в указании продукции Анны, а также улучшить его качество и осуществлять контроль за соблюдением законов, правил и положений в регулируемом районе ».

Согласно утверждениям производителя, ЕГАИС позволяет:

– обеспечивать полноту и достоверность учёта производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции; с возможностью детализации до субъекта РФ, производителя, вида, наименования продукции, крепости, объёма, правильности начисления акциза;

– обеспечивать ведение учёта импорта спирта и алкогольной продукции с контролем правильности начисления акциза;

– обеспечивать учёт федеральных специальных марок и акцизных марок;

– производить анализ состояния и тенденций развития производства и оборота этилового спирта и алкогольной продукции на территории РФ и её регионов;

– затруднить сбыт контрафактной продукции за счёт проверки сопроводительных документов, удостоверяющих законность производства и оборота этилового спирта и алкогольной продукции.

Основные компоненты ЕГАИС.

АСИиУ (автоматические средства измерения и регистрации концентрации безводного спирта в готовой продукции) является источником данных, зарегистрированных в EGAIS предприятием, которое покупает алкоголь (спиртосодержащее сырье), производит спирт или алкогольную продукцию. Примеры автоматизированных многофункциональных комплексов АСИиУ Basis 2006M, они не только учитывают спиртосодержащие продукты, но и способны решать дополнительные задачи, автоматизируя процесс производства алкоголя. Комплексы АСИиУ могут одновременно использоваться для передачи данных в EGAIS и для внутреннего контроля. Комплексы Basis T предназначены для учета алкогольной и алкогольной продукции во время транспортировки.

UTM - универсальный транспортный модуль. Программа, созданная участником алкогольного рынка и используемая для передачи данных между EGAIS и учётной системой участника.

При отправке партии алкоголя отправляющий участник обязан передать сообщение о отгруженном алкоголе в TMU, которое, в свою очередь, передаст эту информацию в центральную базу данных EGAIS.

При приёме алкоголя участник-получатель обязан принимать алкоголь только при наличии информации о доставке в ЕГАИС. С этой целью получатель также имеет UTM, который автоматически получает данные из EGAIS. При получении партии алкоголя принимающая сторона должна подтвердить получение, отправив сообщение в UTM.

Технически, TMU - это 3 службы: Transport, Transport-Updater и Transport-Monitoring, а также база данных для хранения сообщений.

Транспорт - основной сервис, который обменивается с сервером EGAIS. Это веб-сервис с Java-апплетами, который обменивается 8080 сообщениями на

порту с учётной системой участника и отправляет / принимает эти файлы на сервер EGAIS.

Transport-Updater - это сервис, предназначенный для обновления основных сервисных модулей. Когда служба останавливается, Transport автоматически останавливается.

Transport-Monitoring - это служба, предназначенная для мониторинга первых двух служб и автоматического запуска их в случае выключения. Эта услуга не критична для работоспособности, TMU работает, даже если Transport-Monitoring не работает.

В качестве СУБД UTM использует Apache Derby.

Ссылка на установочный пакет последней версии модуля УТМ доступна только в личном кабинете ЕГАИС.

В личный кабинет можно попасть только в случае наличия аппаратного ключа. Система ЕГАИС в розничном сегменте введена для того, чтобы перекрыть канал сбыта «контрафактной» продукции и тем самым повысить собираемость акцизов на алкоголь. Слово «контрафактной» взято в кавычки потому, что под этим термином понимается вся продукция, информации о которой нет в системе ЕГАИС. А это не только опасная для здоровья потребителя разлитая кустарным образом подделка, но и самый настоящий качественный алкоголь, разлитый на самом настоящем заводе, но его производитель просто решил не платить за него акциз и не регистрировать факт выпуска в системе. Вот всю такую контрафактную продукцию и призвана выявлять и запрещать к продаже система ЕГАИС, к которой сейчас должны быть подключены кассы всех розничных магазинов в городах нашей страны. Раз контрафакт невозможно будет безопасно продать, то и пропускать «мимо акциза» смысла не будет.

Продавец на кассе должен отсканировать акцизную марку, а касса при этом должна связаться через интернет с серверами ЕГАИС и передать им информацию о продаже этой конкретной бутылки алкогольной продукции. При этом примерно с середины февраля 2017 года система в течении 3 секунд должна

вернуть на кассу ответ о том, что продукция легальна, числится на остатках магазина, акциз за неё оплачен и её продажа разрешена.

А данной концепции кассы магазинов становятся своеобразными фильтрами, не позволяющими продать покупателю контрафакт. Если фильтр сработал правильно и выявил такой контрафакт. Согласно пункту 6 статьи 12 Федерального закона «О государственном регулировании производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции и об ограничении потребления (распития) алкогольной продукции» за правильность нанесения и за подлинность федеральных специальных марок и акцизных марок несут ответственность собственники (владельцы) алкогольной продукции, осуществляющие её производство, импорт, поставки или розничную продажу. Как только магазин подписал приходные накладные на алкогольную продукцию он стал её владельцем.

При выявлении контролирующими органами алкогольной продукции, находящейся в нелегальном обороте, возбуждается дело об административном правонарушении, выявленная продукция изымается из оборота. По решению суда на юридическое лицо может быть наложен штраф (от 40 000 руб. до 50 000 руб. по ч. 2 ст. 15.12 КоАП РФ, от 50 000 руб. до 100 000 руб. по ч. 4 ст. 14.17 КоАП РФ), а вся партия алкогольной продукции будет подлежать конфискации и дальнейшему уничтожению. Также лицензирующий орган обязан обратиться в суд с заявлением об аннулировании лицензии выданной организации, у которой данная продукция была обнаружена.

Поэтому если система ЕГАИС вернула на кассу отказ в регистрации продажи кассир должен отложить такую бутылку и не допустить её дальнейшего оборота (продажи, списания, перемещения, возврата). Если ЕГАИС не успел вернуть отказ в регистрации в установленный срок и чек продажи был успешно закрыт, а покупатель унёс «контрафактную» бутылку с собой, то письмо о такой операции все равно «найдёт своего героя» в личном кабинете ЕГАИС. А если таких операций с одним и тем же наименованием алкогольной продукции будет много, то на место будут отправлены сотрудники контрольного управления РАР.

Их задачей станет выявление на остатках магазина других таких бутылок из этой «левой» партии, оформление их изъятия, составление протоколов и передача материалов дела в суд. Что и стало происходить в массовом порядке в конце прошлого и в 2017 года:

– Решение № 12-1170/2016 12-75/2017 от 25 января 2017 г. по делу № 12-1170/2016 (Череповец)

– Решение № 71-81/2017 от 8 февраля 2017 г. по делу № 71-81/2017 (Свердловская обл.)

– Решение № 7А-118/2017 от 8 февраля 2017 г. по делу № 7А-118/2017 (Ставрополь)

– Постановление № 5-46/2017 от 1 февраля 2017 г. по делу № 5-46/2017 (Екатеринбург)

Суть этих решений судов примерно одинакова – предприятие должно приложить все необходимые усилия для того, чтобы не допустить оборота контрафактной продукции. Если продажа такой продукции выявлена системой ЕГАИС, то значит усилий было недостаточно. И даже тот факт, что почти во всех материалах дела указано, что при приёмке акцизные марки на алкогольной продукции проходили визуальную проверку и выборочную проверку специальными приборами контроля (например, «ДЕВИС-А36»), не указывает на то, что такие меры были достаточными, а значит не освобождает предприятие от санкций.

На сайте «Межрегионального управления Росалкогольрегулирования по Уральскому федеральному округу» размещена информация о тех мерах, которые служба рекомендует принимать предприятиям розничной торговли для выявления продукции с «поддельными» акцизными марками. Кроме визуального осмотра, который, как выяснилось, почти не помогает выявлять контрафакт, необходимо проверять информацию о марке, содержащуюся в ЕГАИС, при помощи ресурса «Проверка марок», размещённого в личном кабинете на официальном сайте Федеральной службы по регулированию алкогольного рынка (www.fsrar.ru).

Схема функционирования системы ЕГАИС в товарообороте изображена на рисунке 1.4.

Что ещё можно сделать, чтобы минимизировать риски розницы? В первую очередь действительно организовать тщательную проверку акцизных марок. Сделать это можно при помощи специальных терминалов сбора данных, которые умеют подключаться к ЕГАИС и оперативно получать информацию о результатах проверки. К счастью, за последний год появились достаточно бюджетные модели терминалов, приспособленные под такие задачи.

Если помарочное сканирование всей продукции с проверкой марки в личном кабинете ЕГАИС невозможно, то нужно хотя бы визуально убедится, что наклеенная марка соответствует тому, на что она наклеена и сопроводительным документам. Главное, что по системе ЕГАИС вам отгрузили именно то, что привезли по факту.

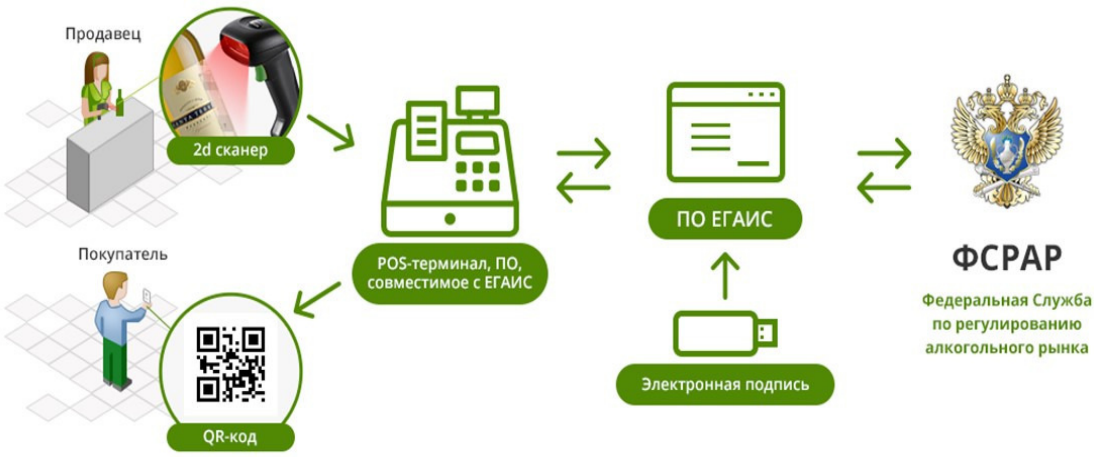

Рисунок 1.4 – Схема мониторинга товарооборота в системе ЕГАИС

Второй контур контроля – оперативное выявление дублей марок при регистрации продажи в системе ЕГАИС. Важно по каждому случаю появления такого дубля (письма в личном кабинете или запрета продажи на кассе) разобраться в его причинах. Самые распространённые из них это ошибки сотрудников предприятия – отсканировали не то, вернули на полку уже просканированный товар и т.д. В этом случае возникает «внутренний дубль» - повторная продажа марки в одном и том же торговом объекте. Если это

единичный случай, то проблемы в этом нет. Если дубли марок идут постоянно и по одной и той же позиции нужно срочно проверять все остатки этого наименования – нелегал мог напечатать зеркальную марку на всю партию и выпустить её в розницу. Ваша задача как можно скорее выявить такую партию и прекратить её розничный оборот.

Если обнаружен дубль марки, проданной в другом торговом объекте (другого региона, города, торговой сети), то также нужно срочно снимать с продажи всю партию и проверять остатки.

По закону предприятие не имеет права ничего сделать с выявленными остатками. Предприятие обязано сообщить в правоохранительные органы о факте выявления признаков правонарушения, дождаться проверки, получить протокол и решение суда о штрафе, а может и об отзыве лицензии. Это в том случае, если на предприятии действительно осталась в наличии такая продукция. Потому что если ничего нет, то установить факт подделки акцизной марки без самой акцизной марки и без продукции, на которую она наклеена проверяющим будет проблематично.

Вернуть такую продукцию поставщику невозможно, потому что «возврат», это тоже «оборот контрафактной алкогольной продукции».

В итоге, самый безопасный способ защитить себя от чужого правонарушения, это не допустить попадания сомнительной алкогольной продукции в собственность, т.е. на остатки предприятия. При этом даже помарочная проверка такой продукции в личном кабинете не даёт полной гарантии, что где-то в стране на остатках какого-то другого магазина не ждут своего часа дубли тех марок, которые прямо сейчас проверяются. Ведь другой «магазин» мог ещё не оприходовать остатки «дублей», в момент проверки на предприятии, они могли до него банально не доехать от поставщика и информации о дубле в личном кабинете вы не будет отображена. Если партия «дублей» будет продана через ЕГАИС первой, то имеющиеся в наличии у других участников рынка товары автоматически станут контрафактом, и никто этого не узнает пока не начнёт их реализацию.

По статистике с введением ЕГАИС сократилось число розничных предприятий, имеющих лицензию на торговлю алкогольной продукцией. Это означает, что часть мелкой розницы ушла «в тень», приторговывая алкоголем совсем без лицензии и уж конечно, без ЕГАИС. Такие «серые» точки могут выявить и наказать только местные органы власти.

Основные принципы работы с данными в этой системе ЕГАИС. В системе существует два регистра (места хранения) информации об остатках. Первый регистр («Склад») хранит сведения в разрезе алкокодов, кода справки формы А и кода справки формы Б. Это означает, что каждой реальной бутылке (или нескольким бутылкам одной партии) соответствует одна запись, в которой заполнены все три этих поля.

В системе ЕГАИС в качестве идентификатора используется Код алкогольной продукции (код АП). Это 19-ти значный код, созданный в системе при регистрации в ней новой элемента. Этот код создаётся по заявке поставщика или импортёра алкогольной продукции для каждого наименования. Одна и та же продукция, выпускаемая на разных заводах, может иметь одинаковый код EAN (классический штрих-код продукции), одинаковое наименование, бутылку и этикетку, но разные коды алкогольной продукции.

Код формы А. «Номер партии», зафиксированный в ЕГАИС поставщиком или производителем при регистрации в системе акцизных марок на продукцию. Код формы А для всей партии (диапазона номеров) данной алкогольной продукции будет одинаковым и неизменным.

Код формы Б. «Код транзакции» присвоенный документу товародвижения в ЕГАИС. Каждая отгрузка, каждое перемещение продукции между контрагентами в ЕГАИС формирует новый код формы Б.

Алкокод содержится в акцизной марке, его можно считать сканером и как-то распознать. Код формы А и код формы Б никак нельзя определить по акцизной марке. Они содержаться только в сопроводительных документах.

Получается, что каждое товародвижение по первому регистру ЕГАИС выполняется только при полном указании всех трёх кодов. И их легко

определить при оптовой поставке, т.к. они сопровождают каждую такую отгрузку и создаются (заполняются) теми, кто её осуществляет. В розничной торговле код формы А и код формы Б конкретной бутылки определить фактически невозможно, т.к. внешне все бутылки одинаковы.

Поэтому ФСРАР создал отдельный регистр в ЕГАИС («Торговый зал»), с которого и осуществляется розничная продажа алкогольной продукции в системе. И в этом регистре вся продукция хранится только в разрезе алкокода. Коды формы А и код формы Б при этом теряются.

1.2.3 Независимый проект Buydentity

Проект Buydentity это альтернативный децентрализованный проект, который позволяет повысить надёжность с помощью обновления информации о товаре на каждом этапе его жизненного цикла от производителя к покупателю понять его характеристики, статус, задействованных контрагентов и исключить продажу подделки или повторную продажу уже реализованного товара.

Для реализации этой идеи каждый товар должен обладать уникальным кодом отслеживания, который позволит в любой момент времени однозначно идентифицировать его. Например, в самом простом случае это может быть QR-код (также могут применяться NFC-метки), который наклеен на товар. Код связан с идентификационными данными о товаре (цвет, вес, номер изделия, номер партии, фото, дата и место производства, производитель и прочее), которые записаны в приватный блокчейн Ethereum (платформа для создания децентрализованных онлайн-сервисов на базе блокчейна). Такая запись данных о продукции не позволяет изменить его характеристики в любой момент времени, и вы сможете проследить весь путь движение товара.

Описанным выше способом можно пометить все товары и решить проблему их однозначной идентификации. Однако, указанная реализация не решает проблему создания контрафакта. Кто-нибудь может купить один настоящий продукт, копировать и тиражировать QR-код на аналогичные поддельные товары. Выход в данной ситуации следующий: в блокчейн

необходимо разместить статус товара и его владельца, который будет меняться в зависимости от стадии его жизненного цикла. Для реализации, описанной выше логики в проекте была развернута сеть Ethereum на основе Azure Blockchain as a Service. Они позволили гибко настраивать правила передачи собственности от одного участника к другому.

Для реализации, описанной выше логики в проекте была развернута сеть Ethereum на основе Azure Blockchain as a Service, что позволило гибко настраивать правила передачи собственности от одного участника к другому [6]. Общая схема функционирования приведена на рисунке 1.5.

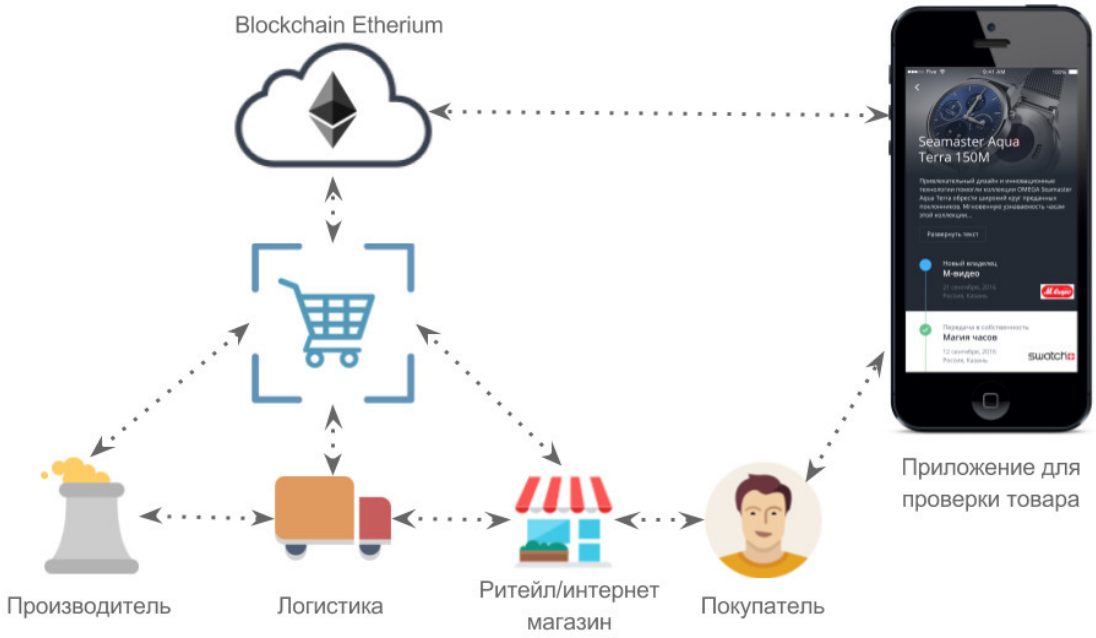

Рисунок 1.5 – Схема работы системы цифровой маркировки Bydentity

Прототип платформы позволяет отслеживать на базе blockchain весь жизненный цикл товара, что даёт возможность исключить создание подделки и проверить подлинность товара в любой момент времени.

Возможности проекта для бизнеса:

– получение аналитики сбыта товара по всему миру;

– с помощью технологии blockchain исключение подделки товаров;

– информация о местонахождении товара находится в текущий момент;

– процесс изготовления и реализация товара прозрачны;

– контроль контрагентов на каждом этапе жизненного цикла товара;

– Надёжные и долгосрочные взаимоотношения с покупателями.

Мобильное приложение buydentity даёт возможность исключить покупку подделки и проверить подлинность товара в любой момент времени. Преимущества для пользователей:

– защита от покупки подделки;

– просмотр паспорта товара и его истории;

– сохранение гарантии и сервисного обслуживания;

– проверка любого товара в 0 кликов.

Для работы с сетью Ethereum команда воспользовалась клиентом Geth, который позволяет подключаться и осуществлять транзакции по протоколу http. Для тестирования и отладки был развернут приватный блокчейн, однако, при попытке доступа к интерфейсу управления с помощью .NET-библиотеки Nethereum, постоянно возникала ошибка подключения к клиенту. Проблема оказалась в устаревшей версии клиента Geth. Кстати, обновления можно найти в репозитории на GitHub.

Следующая проблема, которая оказалась относительно простой, возникла с подключением клиента Geth к удаленному клиенту в виртуальной машине Microsoft Azure. Как оказалось, она скрывалась не только в клиенте, но и в настройке фаервола виртуальной машины. С этой проблемой можно разобраться с помощью материала по настройке конечных точек виртуальных машин. Для доступа к клиенту Geth извне достаточно указать флаг --wsaddr “0.0.0.0” (по умолчанию localhost).

Смарт-контракты Ethereum были выбраны не случайно — синтаксис языка Solidity несложный, очень похож на JavaScript и можно сказать, что подобен языку C. Поэтому первая версия контракта была быстро реализована и проверена с помощью веб-IDE.

1.3 Выводы по первому разделу

В данном разделе, была изучена ситуация с оборотом контрафакта на современном внутреннем и международном рынке, и борьба с ним. Были рассмотрены принципы работы систем цифровой идентификации и мониторинга движения товаров. В результате можно сделать следующие выводы:

– Существующие на сегодняшний день государственные системы в Российской федерации не обеспечивают полного контроля за оборотом продукции, оставляя уязвимыми тех или иных участников рынка. В течении 2017 года неоднократно происходили случаи, когда розничные сети несли убытки, в связи с попаданием на их склад контрафактной продукции.

– Существует опасность «вброса» дублирующей подлинную контрафактной продукции в оборот.

– Данные проблемы отчасти решены в системе Bydentity, но архитектура blockchain не подходит для государственного регулирования ввиду меньшего быстродействия и избыточной распределённости вычислений и хранения информации.

Выходом из данной ситуации может является разработка системы, ведущей мониторинг каждого изменения статуса продукции в обороте и гарантирующей подлинность собранных данных.

2 Разработка моделей цифровой идентификации товаров

При проектировании больших и сложных систем возникают проблемы, связанные не только со свойствами их составных частей – элементов и подсистем, но также и с закономерностями функционирования объекта в целом, рассматриваемые как общесистемные проблемы. Следствием этого является необходимость решения широкого круга специфических задач, к которым относятся: определение общей структуры системы и требований к элементам и подсистемам, организация взаимодействия между ними, выбор оптимальных режимов функционирования, оптимальное управление протекающими в системе процессами, учёт влияния внешней среды и т.п. По мере усложнения систем всё более значимыми становятся общесистемные вопросы, теория сложных систем, системотехника, моделирование.

Правительство РФ утвердило базовые принципы модели функционирования системы маркировки товаров средствами идентификации. Они предусматривают идентификацию каждой единицы товара путём присвоения уникального кода, создание единой информационной системы маркировки, в которой будет храниться вся информация, генерируемая участниками системы маркировки. Создание, развитие и обеспечение бесперебойного функционирования единого каталога товаров и системы цифровой маркировки, а также организация механизмов общественного контроля, поручены единому оператору системы. Также определен перечень первых товаров, подлежащих обязательной маркировке: табачная продукция, обувь, духи, различные предметы одежды, фотокамеры и др.

Центр развития перспективных технологий, определённый оператором Единой национальной системы цифровой маркировки и прослеживаемой, готов обеспечить все обозначенные в документе требования к системе и её функционированию. ЦРПТ совместно с представителями бизнеса в каждой товарной категории проработает оптимальные механизмы маркировки для минимизации затрат участников оборота и комфортного перехода на

обязательную цифровую маркировку. ЦРПТ считает важным исследование особенностей каждой группы для поиска наименее затратного и не нарушающего операционные процессы способа внедрения. Данный подход доказал свою эффективность в проекте по маркировке табачной продукции, где менее чем за три месяца – с января по апрель 2018 года – система цифровой маркировки заработала в полную силу: от нанесения на производстве до продажи промаркированной легальной продукции в магазинах.

Принятая Правительством РФ модель функционирования подразумевает идентификацию каждой единицы товара путём присвоения уникальных цифровых кодов, защищённых криптографией. Код товара состоит из 2 частей – код идентификации и код проверки. Код идентификации содержит код товарной позиции в создаваемом едином каталоге товаров и уникальный код единицы товара. Код проверки формируется с использованием российских криптографических технологий. ЦРПТ обеспечит необходимый уровень доступа к единой системе органам государственной власти и местного самоуправления, участникам оборота товаров и потребителям.

Национальная система маркировки – один из важнейших проектов на ближайшие годы, направленный на создание цифровой экосистемы, позволяющей государству, бизнесу и потребителю контролировать путь любого товара от конвейера до кассы в торговой точке. Это платформа для построения в стране экономики доверия. Цифровая маркировка и прослеживаемость – наиболее эффективный механизм противодействия незаконному обороту продукции.

Для решения проблем, обозначенных в предыдущем разделе необходимо разработать средства системного характера, способные предотвратить негативные явления, связанные с оборотом контрафактной продукции, и не добросовестным ведением торговых операций. Системы мониторинга движения товаров и системы цифровой идентификации товаров существуют уже продолжительное время, включая системы, действующие и разрабатываемые в Российской федерации. Однако нашей задачей является совершенствование

принципа работы данных систем, поэтому необходимо разработать функциональные и логические модели системы, способной выполнять задачи систем данного класса с дополнительной криптографической защитой информационной составляющей товарооборота.

В первую очередь, информационная безопасность данной подсистемы значительно повысится от применения защищённых каналов связи по протоколам SSL и SSH, что повышает устойчивость системы к атакам типа «человек посередине», которые особенно критичны при получении ответа пользователем приложения на мобильной платформе. Так же необходимо разработать специальный протокол, обмена данными, рассматривающий каждую упаковку товара или группу упаковок в таре как отдельное сообщение, отправляемое между участниками рынка. На каждом этапе должна быть возможность убедиться в достоверности этого сообщения. Протокол ориентируется на принципы “End to End” шифрования. Реализация данного протокола обмена затруднительна без использования согласованного с алгоритмом обмена данными протокола формирования маркера.

2.1 Средства проектирования.

При проектировании системы необходимо построение логических и функциональных моделей разных блоков системы. Основным средством для этого являются следующие пакеты прикладных программ:

- AllFusion Process Modeler 7
- ERwin Data Modeler
- MS Visio.

AllFusion Process Modeler 7 или как он ранее назывался BPwin - мощный программный продукт с помощью которого, можно проводить моделирование, анализ, описание и последующую оптимизацию бизнес-процессов. С помощью BPwin можно создавать графические модели бизнес-процессов. Графическое изображение схемы выполнения работ, организации документооборота, обмена различными видами информации позволяет визуализировать существующую

модель организации бизнеса. Это дает возможность использовать передовые инженерные технологии для решения задач управления организацией.

AllFusion Process Modeler r7, совмещает в одном инструменте средства моделирования функций (IDEF0), потоков данных (DFD) и потоков работ (IDEF3), координируя эти три основных аспекта бизнеса для соответствия потребностям аналитиков и системных аналитиков. AllFusion Process Modeler r7, позволяет повторно использовать ключевую информацию моделирования с точки зрения базовых аспектов, чтобы определить точки конфликтов и, в конечном счёте, достичь их согласования.

IDEF0 - методология функционального моделирования. С помощью наглядного графического языка IDEF0 изучаемая система предстает перед разработчиками и аналитиками в виде набора взаимосвязанных функций (функциональных блоков - в терминах IDEF0). Как правило, моделирование средствами IDEF0 является первым этапом изучения любой системы. С помощью функционального моделирования (нотация IDEF0), можно провести систематический анализ бизнеса, сосредоточившись на регулярно решаемых задачах (функциях), свидетельствующих об их правильном выполнении показателях, необходимых для этого ресурсах, результатах и исходных материалах (сырье).

IDEF3 — методология моделирования и стандарт документирования процессов, происходящих в системе. Метод документирования технологических процессов представляет собой механизм документирования и сбора информации о процессах. IDEF3 показывает причинно-следственные связи между ситуациями и событиями в понятной эксперту форме, используя структурный метод выражения знаний о том, как функционирует система, процесс или предприятие.

ERwin Data Modeler – CASE-средство для проектирования и документирования баз данных, которое позволяет создавать, документировать и сопровождать базы данных, хранилища и витрины данных. Модели данных помогают визуализировать структуру данных, обеспечивая эффективный

процесс организации, управления и администрирования таких аспектов деятельности предприятия, как уровень сложности данных, технологий баз данных и среды развёртывания.

2.2 Построение модели системы цифровой идентификации и мониторинга движения товаров

Концепция большинства систем цифровой идентификации товаров не предусматривает систем безопасности кроме доступа к сервисам системы межведомственного электронного взаимодействия (СМЭВ) с использованием технологий электронной цифровой подписи (ЭП). Данной меры достаточно для обеспечения безопасности и целостности данных передаваемых между участниками системы (государственными органами, производителями, импортёрами и фарм. предприятиями).

Однако в существующем виде система остаётся уязвимой для недобросовестных участников её работы. Передаваемые в открытой форме на упаковке индивидуальные коды позволяют расшифровать алгоритм своей генерации и внедрять контрафакт на пути следования ЛП подобно атаке «человек посередине». Добавление контрольного хэша ЭЦП полученного по индивидуальному коду ЛП и групповому коду также не даёт полной гарантии так как существует уязвимость любого хэша к коллизиям. А передача его совместно с кодируемыми данными в открытом виде приводит так же к возможности проведения «атаки большими данными» [7].

В связи с этим, на следующем этапе исследования разработан проект системы маркировки лекарственных препаратов с гарантированной подлинностью для предотвращения оборота фальсифицированных и контрафактных ЛП.

На рисунке 2.1 изображена контекстная диаграмма организационного функционирования системы мониторинга движения товаров. В данном случае, учитываются требования, предъявляемые к существующим или проектируемым государственными информационным системам.

Функционал системы условно распределяется на три основных функции, это аккредитация производителей и импортёров, маркировка продукции, и обслуживание мониторинга.

Функции аккредитации заключаются в организационной работе по лицензированию и управлению процессом получения поставщиками рынка документации, в том числе и ключевой необходимой для работы в системе. А также в лицензировании продукции, поставляемой на рынок.

Рисунок 2.1 – Функциональная диаграмма функционирования ИС

На рисунке 2.2 Функциональное предназначение блока «Маркировка продукции» заключается в выполнении операций по формированию цифрового идентификатора, наносимого на маркируемую продукцию, регистрационная информация о товарах и поставщиках фармацевтической продукции, исходящей информацией выступают ответы на запросы статуса, реестры товаров, маркировочные товары, управлением выступают законы и решения правительства Российской информации и стандарты, протоколы, технические характеристики, в свою очередь механизмами являются программное и аппаратное обеспечение, предполагается что это будет QR-код. Входящей

информацией являются товары. Детализация данных функций рассмотрена подробнее далее.

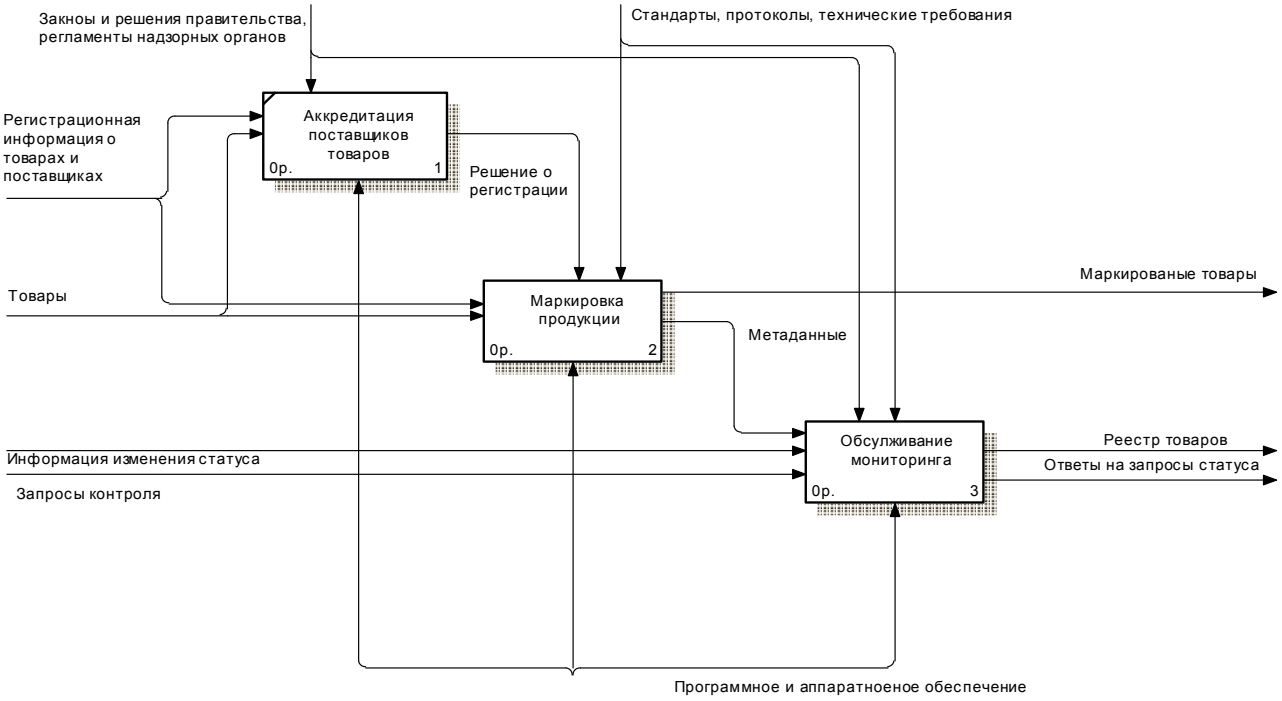

Рисунок 2.2 – Декомпозиция функциональной диаграммы ИС

Функционал «Обслуживание мониторинга» заключается в обслуживании запросов проверки товаров, и транзакций по отражению изменений статусов товаров и также рассматривается ниже. Поток данных происходит следующим образом: регистрационная информация о поставщиках и товарах относятся аккредитации поставщиков товаров (без аккредитации никакая фармацевтическая компания не имеет право работать на Российском рынке), затем регистрируются товары и производится маркировка продукции, метаданные поступают в обслуживание мониторинга из которого формируется реестр товаров и ответы на запросы статуса. Результатом выполнения данного функционала являются данные для реестра товаров, физические товары, несущие маркеры, а также, статистическая информация о контролируемом товарообороте.

На рисунке 2.3 приведена декомпозиция блока маркировки продукции. В рамках выполнения данного функционала выполняются действия по формированию данных о поставщике и товаре в блоке «Формирование

метаданных». Функционал формирования ключей осуществляет формирование ключей для формирования подписи маркера и осуществления верификации транзакций поставщика или владельца товара. Ключевая пара формируется на основании данных о поставщике продукции, и в качестве входных данных принимается в следующем функционале «Формирование маркера».

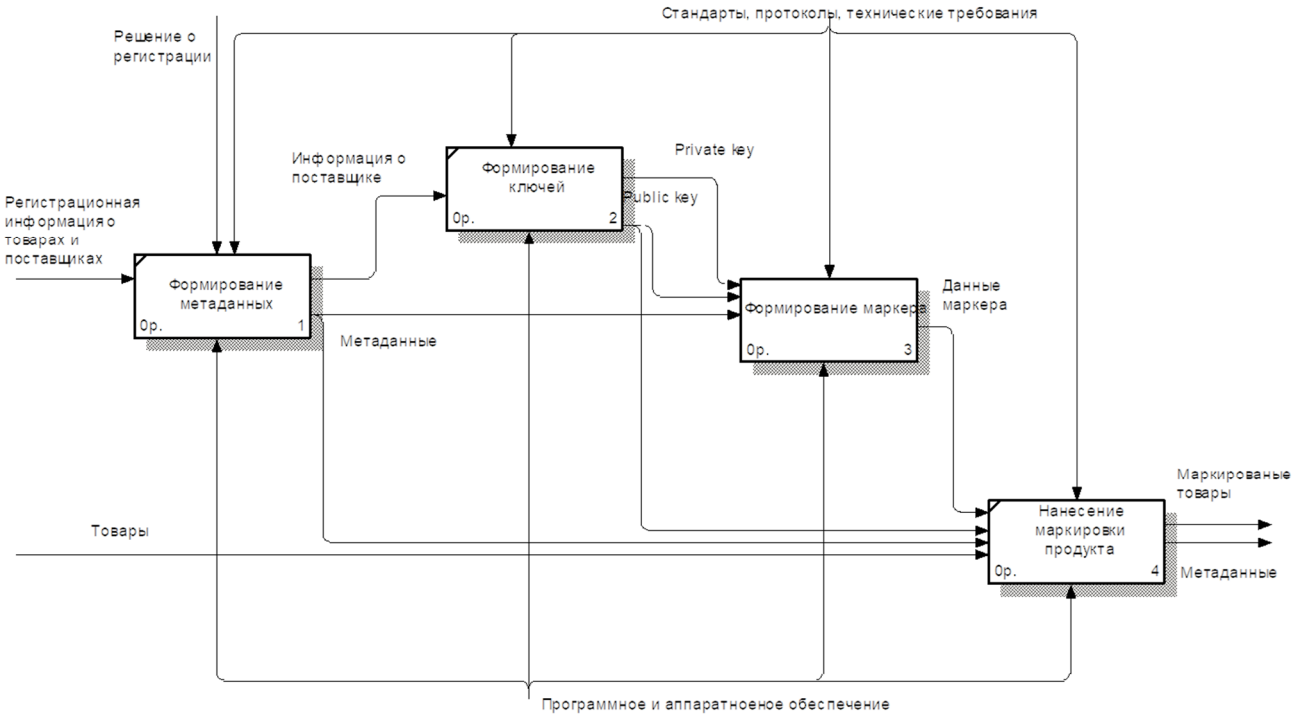

Рисунок 2.3 – Детализация функционального блока маркировки продукции

Функциональный блок «Формирование маркера» предназначен для выполнения операций создания цифрового идентификатора и занесения маркируемой продукции в регистры. Изначально формируются метаданные, затем ключи, маркеры и происходит нанесение маркировки продукта, исходящей информацией выступят маркированные товары. Данный сформированный цифровой идентификатор передаётся в блок «Маркировка продукции» в котором осуществляется непосредственное физическое нанесение маркера.

На рисунке 2.4 приведена детализация блока обслуживание мониторинга. Задача обслуживания мониторинга заключается в функциях получения данных, для ответа на запросы о товарах, и выполнении функций формирования записей.

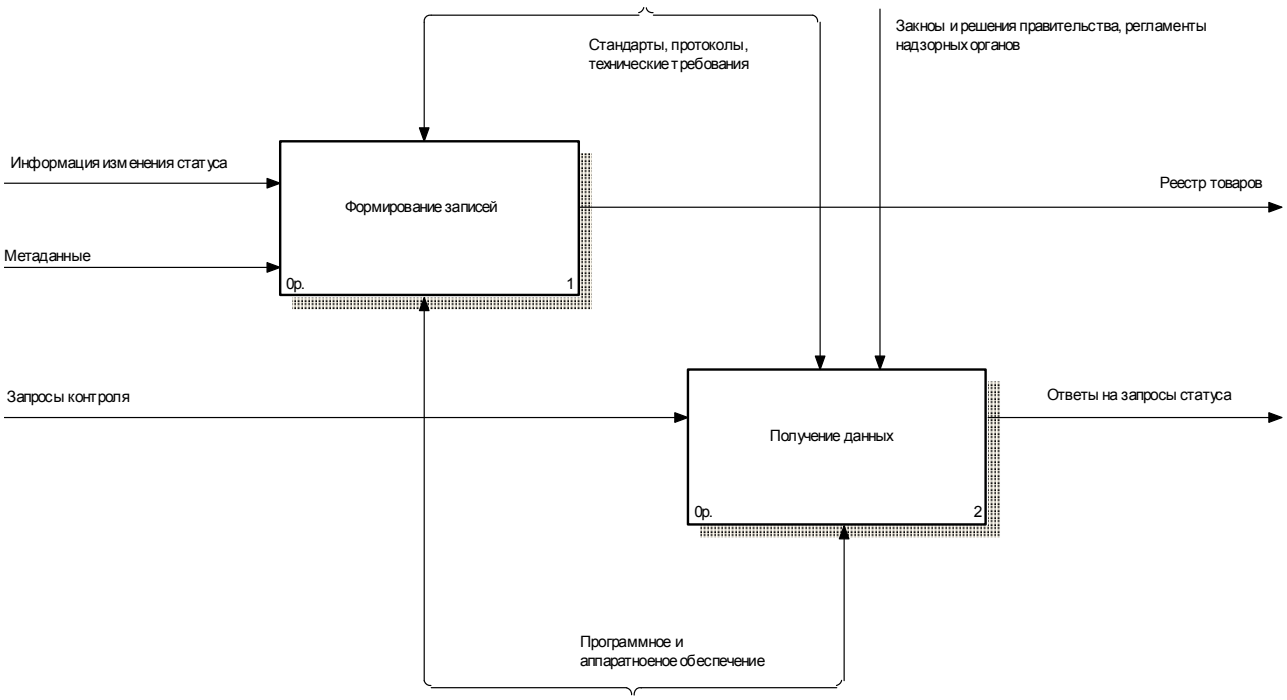

Рисунок 2.4 – Детализация блока «обслуживание мониторинга»

Функционал формирования записей на входе получает метаданные о товаре и информацию о его статусе. В качестве выходных данных, приведённый на изображении блок возвращает записи в реестр состояний. Также, в данном блоке происходит контроль подлинности данных транзакций. Данный блок будет декомпозирован более детально в последующем подразделе.

2.3 Разработка алгоритма верификации цифрового идентификатора товара

В рамках решения поставленных задач, необходимо разработать алгоритм, позволяющий сформировать цифровой идентификатор, однозначно идентифицирующий товар и позволяющий удостовериться в подлинности маркера и товара.

Реализовать данные функции невозможно без журналирования статуса и состояния товара. Данный функционал необходим для подтверждения подлинности товара, и валидации операций при перемещении товаров.

На рисунке 2.5 изображена функциональная декомпозиция процессов связанных с обслуживанием мониторинга. В виде действующих процессов получения данных выступают запросы, выполняемые по требованию пользователей или контролирующих организаций.

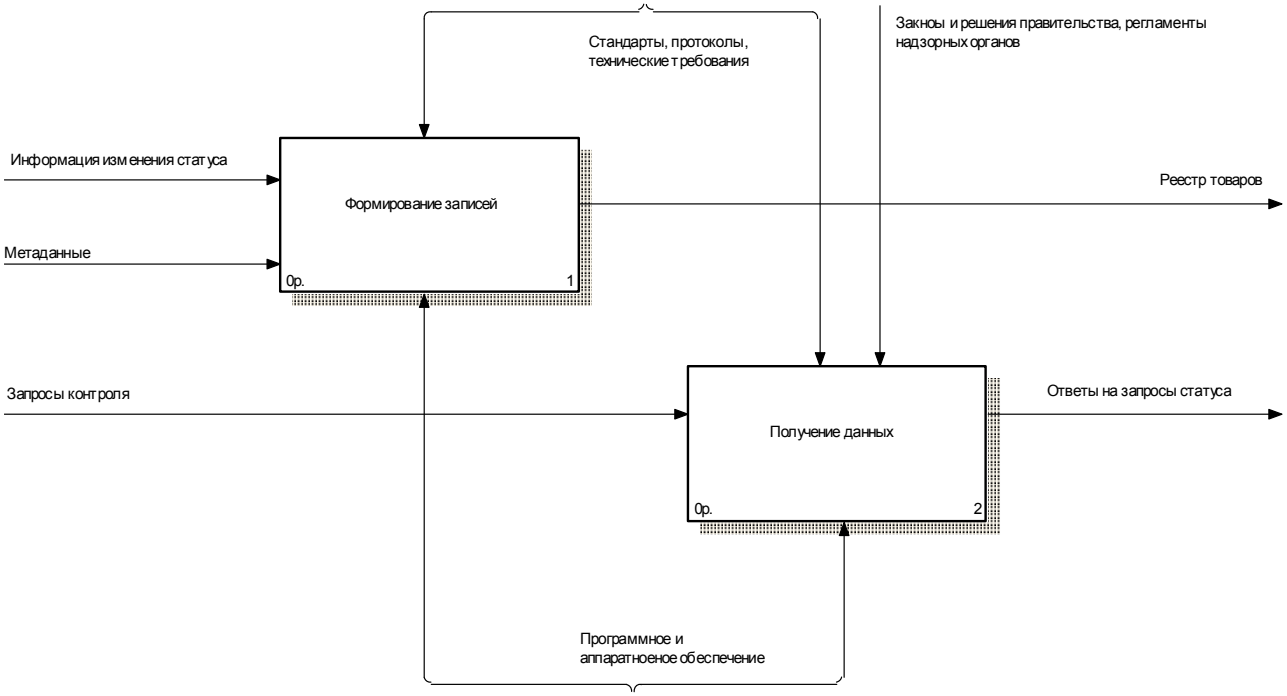

Рисунок 2.5 – Функциональная модель процесса «обслуживание мониторинга»

Второй функциональный блок, формирование записей – отвечает за создание записей о введении в оборот на рынке и перемещении товаров между участниками рынка.

На рисунке 2.6 представлена логическая модель детализирующая процесс формирования записей, в которой методом асинхронного и происходит идентификация владельца товара, и идентификация объекта (товара), при идентификации владельца происходит получение из БД открытого ключа, и формирование контрольной строки которая шифруется при помощи открытого ключа, и отправляется владельцу на подтверждение. Получив данную строку, владелец товара расшифровывает её при помощи своего закрытого ключа отправляет полученный ответ на сервер. В зависимости от того, правильная ли получена строка, методом исключающего или происходит ветвление исполнения функций.

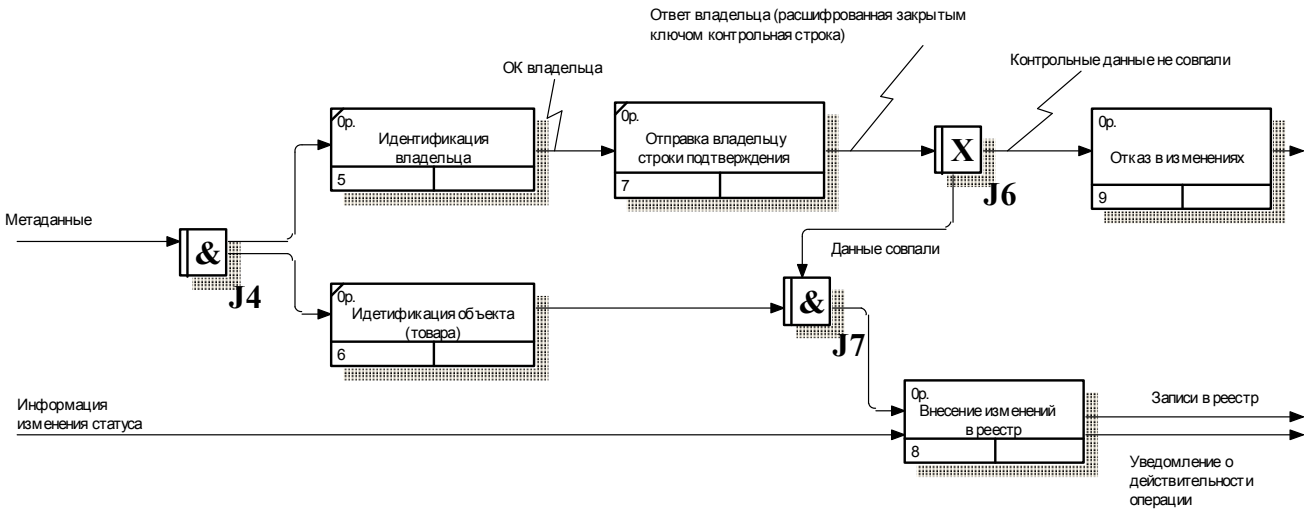

Рисунок 2.6 – Логическая модель детализирующая процесс формирования записей

Происходит отказ в изменениях, или, если данные совпали, происходит внесение изменений в реестр, для идентифицированного товара. В результате реестр добавляются новые записи о изменениях статуса товара и отправляется уведомление о действительности произведённой операции её участникам.

На рисунке

Рисунок 2.7 подробно представлена детализация процесса внесения изменений.

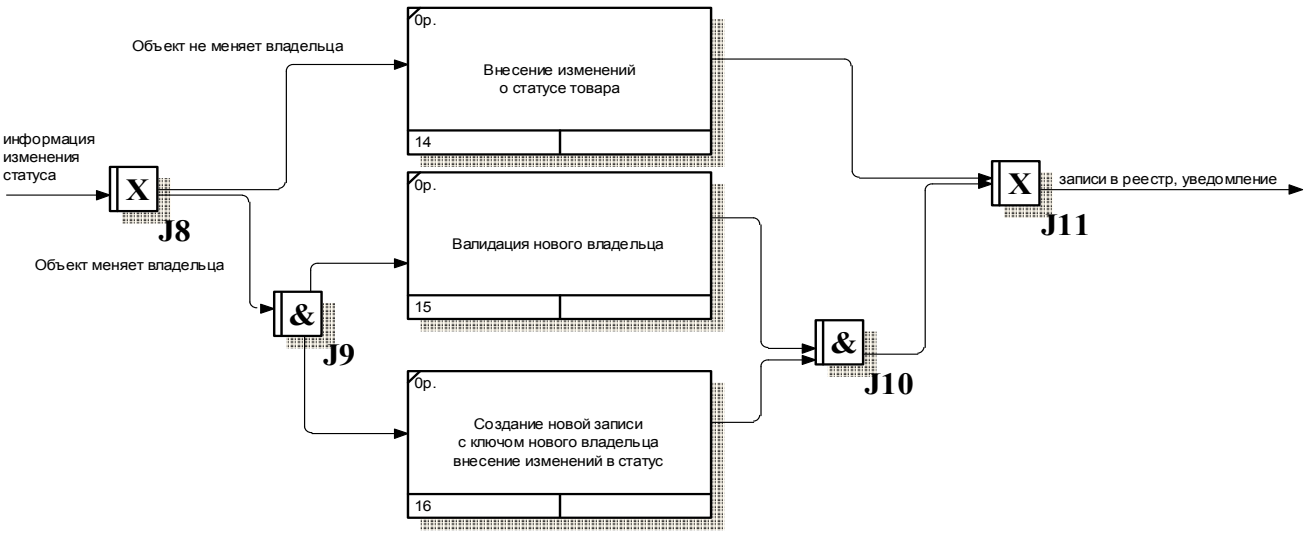

Рисунок 2.7 – Детализация процесса внесения изменений

Если внесение изменений совершается со сменой владельца, то происходит два действия одновременно (синхронное и): валидация нового владельца или создание новой записи с ключом нового владельца и внесение изменений в статус товара.

2.4 Разработка алгоритма формирования маркера

Для более чёткого представления о том, как происходит маркировка фармацевтической продукции указано на рисунке 2.8. Функциональная блок-схема процесса маркировки продукции состоит из четырёх блоков: формирование метаданных, формирование ключей, формирование маркера, а также нанесения маркировки продукта.

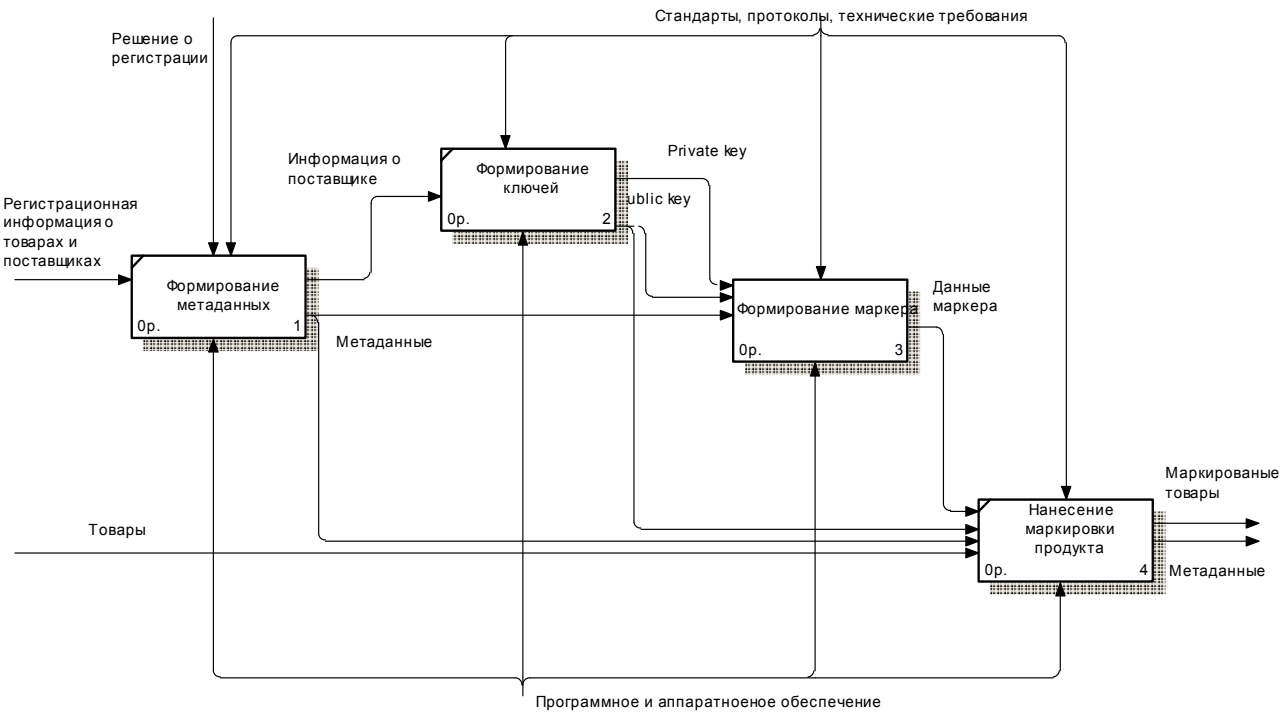

Рисунок 2.8 – Функциональная блок-схема процесса маркировки продукции

Стоит обратить внимание на логическую модель процесса формирования маркера, отображённую на рисунке 2.9, она показывает каким образом формируется маркер. Данная модель состоит из трёх блоков: формирование полезной нагрузки, хеширование с ключом и формирование данных маркера.

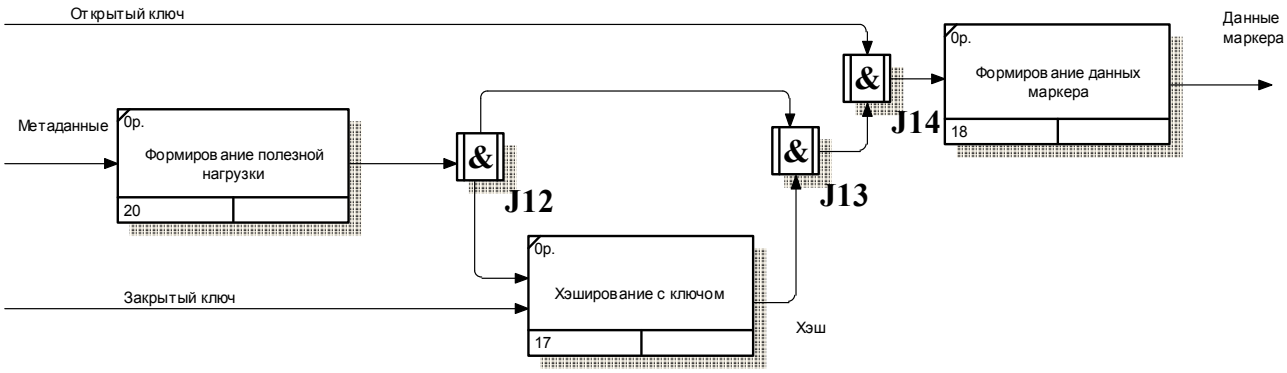

Рисунок 2.10 – Логическая модель процесса формирования маркера

2.5 Выводы по второму разделу

Во втором разделе разработаны и проанализированы модели функционирования системы мониторинга движения товаров применяющей предлагаемый способ цифровой идентификации.

В ходе проектирования были разработаны организационные и логические модели применения криптографических алгоритмов для обеспечения информационной безопасности процесса мониторинга движения товаров. Так же, были смоделированы основные функции связанные с обеспечением «ведения» промаркированных цифровым идентификатором товаров в процессе мониторинга.

3 Программная реализация

Для того чтобы было возможно провести испытания самой важной, части проекта, функционала по формированию стойкого маркера и

3.1 Исследование средств криптографической защиты информации, применимых для решения задач

При современном темпе развития компьютерных и цифровых технологий мы не в состоянии воспринимать свою жизнь вне информационного потока окружающего нас. Процессы обработки, хранения, передачи и использования информации становятся главенствующими в жизни современного общества, любая наша деятельность достаточно тесно связана с этими процессами.

Не существует абсолютно стойких криптоалгоритмов, за исключением одноразового блокнота. Все известные криптоалгоритмы построены не на знании, а на незнании. Стойкость шифра ещё никому не удалось математически доказать, зато удалось доказать нестойкость большинства из придуманных когда-либо шифров. Поэтому стойким считается тот шифр, для которого пока что не придумали практичного метода взлома. Однако если такого метода ещё не придумали, то это не значит, что его не придумают никогда, хотя применительно к хорошо изученным шифрам (AES, Twofish, Serpent) вероятность взлома в ближайшие 10 лет пренебрежительно мала. Существует мнение, что АНБ имеет в своём распоряжении неизвестные широкой общественности методы криптоанализа, однако это не более, чем слухи. Никаких доказательств этого факта нет. Однако не следует считать, что зашифрованные сейчас данные не будут вскрыты никогда. Я считаю, что максимальный срок, на который можно засекретить данные это 10–20 лет. Вы должны это четко понимать и всегда помнить.

Единственно возможной сейчас атакой на стойкие криптоалгоритмы является перебор всех возможных вариантов ключей. На данном этапе развития техники возможен подбор 64 битного ключа, и теоретически 70 битного.

Минимально безопасной является длина ключа в 80 бит. В случае создания квантового компьютера, длину ключа для симметричных шифров следует удвоить для достижения идентичного уровня безопасности. Поэтому 128 битные ключи теоретически могут быть взломаны на КК, но 256 битные ключи не будут взломаны прямым перебором никогда, так как полный перебор такого числа комбинаций упирается в ограничения, поставленные законами физики. Следует также следить за тем, чтобы ваш пароль имел не меньшую стойкость, чем ключевое пространство используемого алгоритма шифрования, в противном случае данные могут быть вскрыты подбором пароля.

Суммируя вышесказанное сделаем вывод, что успешные лобовые атаки крайне маловероятны, однако не стоит сбрасывать их со счетов. Также не стоит пользоваться криптоалгоритмами с ключом короче 256 бит, но и ключи длиннее тоже не имеют особого смысла.

Некорректная реализация криптографических программ. Даже самый надёжный алгоритм шифрования может оказаться бессилен, если он реализован с ошибками, или используется неправильно.

Ошибки и неправильное применение криптографии — это болезнь проприетарного софта. Особенно на этой почве прославилась небезызвестная компания Microsoft. Практически каждое созданное ими криптографическое решение содержало серьёзные уязвимости, а зачастую было тривиально взламываемым. За примерами далеко ходить не надо, это Kerberos, шифрование документов MS Office, PPTP VPN, протокол аутентификации NTLM, Syskey, EFS шифрование в Windows 2000, ГСЧ в windows 2000/XP/Vista. Как показывает история, эта компания не способна учиться на своих ошибках, поэтому лучше использовать что угодно, но только не криптографию от Microsoft, ибо худшей чем у них репутации вы при всём желании не найдёте.

Проприетарное ПО и аппаратные криптографические средства помимо ошибок могут содержать преднамеренные закладки, или их производитель может нагло врать об их свойствах. В качестве примера могу привести винчестеры с аппаратным шифрованием от Drecom, производитель которых

заявлял о шифровании с помощью AES, но на самом деле там оказался тривиально взламываемый XOR. Подробно прочитать об этом вы можете здесь. Из всего этого можно сделать вывод — нельзя никогда верить словам производителя. Всегда требуйте доказательств его слов, и проверяйте их собственноручно, или интересуйтесь мнением профессионалов, если не имеете достаточной квалификации.

Вредоносное программное обеспечение, в случае если применяется правильный криптографический софт, то это устраняет вышеописанные опасности, но не устраняет все опасности до конца. Одной из серьёзнейших опасностей является попадание к вам троянского ПО, которое может перехватывать вводимые пароли, ключи шифрования, или даже отсылать сами данные. Защита от вредоносного ПО это отдельная большая тема, и я не буду её здесь освещать. Но запомните — вы должны исключить возможность попадания любого недоверенного ПО в вашу систему. В противном случае шифрование данных не имеет никакого смысла. Если вы занимаетесь обработкой действительно секретной информации, то лучше всего это делать на не подключенной к интернету системе, и держать на ней лишь минимум необходимого софта.

Физические атаки или прямой доступ к системе. Физические атаки всегда связаны с прямым физическим доступом к системе, или возможностью наблюдения за ней. В частности, возможно удалённое наблюдение, установка жучков. Существует техника, позволяющая считать изображение с вашего монитора на расстоянии в сотню метров. Существует способ считывания вводимого через клавиатуру текста по звукам нажатия клавиш, которые могут быть получены с помощью жучка или лазерного микрофона. Помимо этого, противник, имеющий физический доступ к вашей системе, может установить в неё программную закладку или аппаратный кейлогер. Ключи шифрования и конфиденциальные данные могут быть считаны из памяти компьютера несколькими способами, включая заморозку и перенос модулей памяти, или подключение считывающего устройства к шинам компьютера. Содержимое

памяти может быть считано даже через некоторые внешние порты, например, Firewire с помощью обычного ноутбука, без применения спецтехники.

Важное замечание: злоумышленник ни в коем случае не должен получить физический доступ к включённой системе, в памяти которой находятся конфиденциальные данные. В противном случае любое шифрование может быть легко взломано. Организация работы с конфиденциальными данными обязательно должна включать в себя физическую безопасность. Идеально иметь для этого специальную комнату, которая экранирована от ЭМИ-утечек, не имеет окон, имеет звукоизоляцию, средства постановки радиопомех, и обязательно крепкие железные двери. Эта комната должна охраняться, и доступ в неё должен быть регламентирован пропускным режимом. Контроль доступа должен дублироваться, т.е. желательно одновременное применение механических и электронных замков, а также наличие поста охраны. В случае невозможности принятия таких мер, нужно озаботиться хотя бы средствами обнаружения попыток несанкционированного доступа, и средствами поиска установленных закладок. Все это не пустая паранойя, это необходимо для защиты ваших данных от сильного противника. Советую вам серьёзно задуматься над вышесказанным.

Программные утечки информации и данных. Программные утечки информации и данных. Применительно к дисковому шифрованию, в некоторых случаях возможно вскрытие зашифрованных данных без применения троянов и без физического доступа к включённой системе. Виной этому являются утечки конфиденциальных данных в ряд незашифрованных системных файлов. Наиболее опасными файлами в Windows являются реестр, файлы подкачки, crash dump и файл гибернации (hiberfil.sys). В файл подкачки пишется большая часть памяти пользовательских приложений, в том числе и обрабатываемые ими конфиденциальные данные. DiskCryptor препятствует попаданию ключей и паролей в файл подкачки благодаря хранению их в неподкачиваемой памяти. К тому же пароли и ключи не хранятся дольше, чем это нужно для их обработки, после чего занимаемая ими область памяти зануляется.

Подобная защита есть во всех адекватных Open Source криптографических продуктах, но её не всегда достаточно для сведения риска утечек к нулю. Наиболее опасными являются утечки в hiberfil.sys и в crash дампы, так как при этом на диск сохраняется всё содержимое памяти, включая неподкачиваемые области. Положение сильно осложняется тем, что механизм записи дампов и hiberfil.sys полностью недокументирован, и поэтому большинство существующих средств шифрования дисков не могут зашифровать эти файлы и они пишутся в открытом виде в сектора диска! Подобная уязвимость была в DriveCrypt Plus Pack старых версий, и даже в TrueCrypt 5.1. Последствия этого катастрофичны, так как сохранение дампа памяти в открытом виде однозначно приводит к вскрытию всей зашифрованной информации в течение нескольких минут.

В общем товарищи из Microsoft подложили нам такую свинью, что и никаких бекдоров в криптософте не надо. Наверняка этой особенностью Windows умеют пользоваться спецслужбы, откуда и пошли соответствующие слухи. Наиболее простым решением является отключение дампов и гибернации, о чём кстати сказано в документации к TrueCrypt. Проблема только в том, что большинство пользователей документацию не читают, и получают не безопасность, а только иллюзию таковой. В DiskCryptor начиная с версии 0.2.5 введены меры, препятствующие утечкам ключевых данных:

Если ваш системный раздел зашифрован, то DiskCryptor будет шифровать дампы и hiberfil.sys;

Если не зашифрован, то при наличии подключённых криптодисков вход в гибернацию и запись дампов при крахе системы будут блокироваться, а если подключённых криптодисков нет, то перед входом в гибернацию или записью дампа будет автоматически очищаться хэш паролей в памяти.

Таким образом программа препятствует попаданию ключевых данных на диск в открытом виде. Но учтите, что всегда остается вероятность утечки данных по вине стороннего приложения. Например, если у вас стоит ПО, перехватывающий ввод с клавиатуры (это могут быть различные переводчики,

программы автоматический смены раскладки клавиатуры, кейлогеры), либо вы передаёте пароли через буфер обмена, то пароли могут быть сохранены в неконтролируемом DiskCryptor участке памяти, и попасть во всевозможные места утечки данных, вплоть до сохранения пароля в клавиатурный лог. Чтобы защититься от утечек, вызываемых сторонним софтом, вам будет достаточно зашифровать все разделы, на которые может идти сохранение подобной информации. Практических способов расшифровки данных предостаточно. Их список не ограничивается всем вышеописанным.

Поэтому запомните — защита конфиденциальных данных не должна сводиться только к шифрованию, крайне важно не забывать о физической защите и организационной стороне вопроса. Но тем не менее, вышеописанное не отменяет необходимости пользоваться шифрованием, так как его использование в любом случае увеличивает затраты атакующего.

В условиях всеобщей информатизации, вопросы информационной безопасности и защиты информации становятся наиболее актуальными. Наука о тайные передачи информации, недоступной или непонятной для посторонних лиц, произошло и стало развиваться в тот момент, когда человечество осознало необходимость обеспечения защиты информации. Криптография – одна из старейших наук, её история насчитывает несколько тысяч лет, развиваясь вместе с человеком, она претерпела огромное количество изменений, постоянно совершенствуясь и дополняясь.

3.1.1 Симметричное шифрование

Симметричное шифрование — это способ шифрования, в котором для зашифрования и расшифрования применяется один и тот же криптографический ключ. Ключ алгоритма должен сохраняться в секрете как отправителем, так и получателем сообщения. Ключ алгоритма выбирается сторонами до начала обмена сообщениями.

Симметричные шифры бывают следующих видов:

блочные шифры. Обрабатывают информацию блоками определённой длины (64, 128 бит и т.д.), применяя к блоку ключ в установленном порядке, как правило, несколькими циклами перемешивания и подстановки, называемыми раундами. Результатом повторения раундов является лавинный эффект ¾ нарастающая потеря соответствия битов между блоками открытых и зашифрованных данных.

поточные шифры, в которых шифрование проводится над каждым битом либо байтом исходного (открытого) текста с использованием гаммирования. Поточный шифр может быть легко создан на основе блочного (например, ГОСТ 28147-89 в режиме гаммирования), запущенного в специальном режиме. Гаммирование — это процесс "наложения" определённой последовательности (гамма-последовательности) на открытый текст. Например, это может быть операция "исключающего ИЛИ". При расшифрования операция проводится повторно, в результате получается открытый текст.

Параметры алгоритмов шифрования: стойкость, длина ключа, число раундов, длина обрабатываемого блока, сложность аппаратной/программной реализации.

Примеры симметричных алгоритмов: DES (Data Encryption Standard, стандарт шифрования данных), ГОСТ 28147-89.

3.1.2 Ассиметричное ширование

Двухключевые криптосистемы (криптосистемы открытого ключа, ассиметричное шифрование) используют на различных этапах два вида ключей: закрытый и открытый. Такие системы применяются для шифрования и цифровой подписи. В ассиметричных криптосистемах для шифрования и расшифровывания информации используются разные ключи. В таких системах каждый пользователь получает пару ключей: открытый ключ, которым информация зашифровывается, и закрытый ключ, которым информации расшифровывается.

Причём открытый ключ публикуется открыто, а закрытый ключ сохраняется владельцем в секрете. Таким образом, необходимость передачи секретной информации исчезает. Однако, более подробней о криптосистемах открытого ключа мы поговорим в 4 главе нашей книги.

Электронно-цифровая подпись (ЭЦП) используется физическими и юридическими лицами в качестве аналога собственноручной подписи для придания электронному документу юридической силы, равной юридической силе документа на бумажном носителе, подписанного собственноручной подписью правомочного лица и скреплённого печатью.

Электронный документ – это любой документ, созданный и хранящийся на компьютере, будь то письмо, контракт или финансовый документ, схема, чертёж, рисунок или фотография. ЭЦП обеспечивает:

– проверку целостности документов;
– конфиденциальность документов;
– установление лица, отправившего документ.

При формировании электронной подписи под сообщением, отправляемым неким абонентом в той же информационной системе, отправитель подписывает послание своим секретным ключом. На самом деле пользователь вычисляет контрольную сумму сообщения, шифрует её секретным ключом и присоединяет шифрограмму к сообщению.

Виды асимметричных шифров:

– RSA (Rivest-Shamir-Adleman)
– DSA (Digital Signature Algorithm)
– Elgamal (Шифросистема Эль-Гамаля)
– Diffie-Hellman (Обмен ключами Диффи — Хелмана)
– ECDSA (Elliptic Curve Digital Signature Algorithm) — алгоритм с открытым ключом для создания цифровой подписи.
– ГОСТ Р 34.10-2012.

3.1.3 Доказательство с нулевым разглашением

Доказа́тельство с нулевы́м разглаше́нием (информа́ции) в криптографии (англ. Zero-knowledge proof) — интерактивный криптографический протокол, позволяющий одной из взаимодействующих сторон («The verifier» — проверяющей) убедиться в достоверности какого-либо утверждения (обычно математического), не имея при этом никакой другой информации от второй стороны («The prover» — доказывающей). Причём последнее условие является необходимым, так как обычно доказать, что сторона обладает определёнными сведениями в большинстве случаев тривиально, если она имеет право просто раскрыть информацию. Вся сложность состоит в том, чтобы доказать, что у одной из сторон есть информация, не раскрывая её содержание. Протокол должен учитывать, что доказывающий сможет убедить проверяющего только в случае, если утверждение действительно доказано. В противном случае сделать это будет невозможно, или крайне маловероятно из-за вычислительной сложности.

Под интерактивностью протокола подразумевается непосредственный обмен информацией сторонами [1,2].

Понятие 'нулевое разглашение' было впервые предложено в 1980-х специалистами MIT Шафи Голдвассером, Сильвио Микали и Чарльзом Ракофф. (Shafi Goldwasser, Silvio Micali и Charles Rackoff). Эти исследователи работали над проблемой, которая относится к интерактивным системам доказательства - теоретическим системам, в которых первый участник (назовём его 'Испытатель' (Prover) обменивается сообщениями со вторым участником 'Контролёр' (Verifier) чтобы убедить контролёра, что некоторое математическое утверждение верно. *

До Голдвассера и других, большинство работ в этой области фокусировались на системах доказательства правильности. То есть, на случаях, когда злоумышленник - Испытатель пытается провернуть трюк с Контролёром, подсовывая ему ложное значение. Но Голдвассер, Микали и Ракофф рассмотрели противоположную сторону этой проблемы. Вместо того, чтобы беспокоится

только об Испытателе, они спросили: что произойдёт, если вы не доверяете Контролёру?

Особо их обеспокоила возможность утечки информации. Конкретно, они задались вопросом, сколько дополнительной информации получит Контролёр в ходе доказательства самого факта, что утверждение верно?

Важно отметить, что это не просто теоретический интерес. Есть реальные, практические приложения, в которых эти вещи важны.

Вот одно из них: представьте, что клиент в реальном мире хочет войти на веб-сервер, используя пароль. Стандартный подход к проблеме 'в реальном мире' включает в себя хранение хэшированной версии пароля на сервере. Логин в такой системе рассматривается как вид 'подтверждения', что хэш предоставленного пароля это выход хэширующей функции действующего пароля. И, что более важно, как 'подтверждение' того, что клиент действительно знает пароль.

Большинство систем в реальном мире реализуют это 'подтверждение' наихудшим образом из возможных. Клиент просто передаёт оригинальный пароль на сервер, который повторно вычислят хэш пароля и сравнивает его с сохранённым значением. Проблема здесь очевидна: сервер получает мой пароль в самом притягательном для хакеров виде 'чистый текст'. А пользователь может только молится о том, что защита сервера не скомпрометирована.

То, что предложили Голдвассер, Микали и Ракофф, стало надеждой на появление новых методов подтверждения. В случае полной реализации, доказательства с нулевым разглашением смогут дать подтверждение в описанной выше задаче. При этом не разгласив ни одного бита информации, которая соответствует тому, что 'это утверждение верно'.

Таким образом, рассматриваемый протокол требует наличия интерактивных исходных данных (interactive input) от проверяющего, как правило, в виде задачи или проблемы. Цель легального доказывающего (имеющего доказательство) в этом протоколе — убедить проверяющего в том, что у него есть решение, не выдав при этом даже части «секретного»

доказательства («нулевое разглашение»). Цель проверяющего же — это удостовериться в том, что доказывающая сторона «не лжёт» [14,15].

Также были разработаны протоколы доказательства с нулевым разглашением [15,16], для которых не требовалось наличия интерактивных исходных данных, при этом доказательство которых, как правило, опирается на предположение об идеальной криптографической хеш-функции, то есть предполагается, что выход однонаправленной хеш-функции невозможно предсказать, если не известен её вход [21].

Рассмотренные выше алгоритмы применимы для шифрования данных в различных информационных системах. Применимо к создаваемой системе данные алгоритмы способны повысить криптографическую стойкость маркера, а также, предоставляют механизм удостоверения текущего владельца товара.

На рисунке 3.1 представлена даталогическая модель проектируемой системы. Даная модель является минимально необходимой, так как для функционирования полноценной системы может потребоваться большее количество сущностей. Сущности реестров хранят текущие данные о владельцах, объектах (товарах), и состояниях объектов. Сущность «связь объектов-субъектов» необходима для хранения текущей информации о ключевых данных подтверждающих текущее состояние объекта.

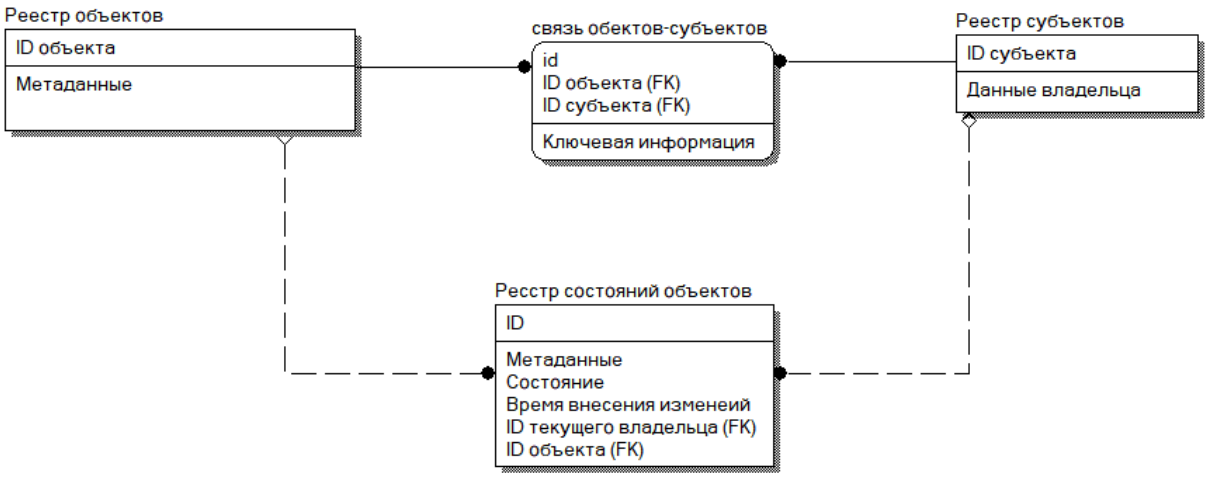

Рисунок 3.1 – Даталогическая модель системы цифровой идентификации товаров

3.2 Реализация Алгоритма формирования маркера

На рисунке 3.2 представлена схема формирования данных для цифрового идентификатора товара. На данной схеме условно отображена информация о товаре, и преобразования, которым она подвергается.

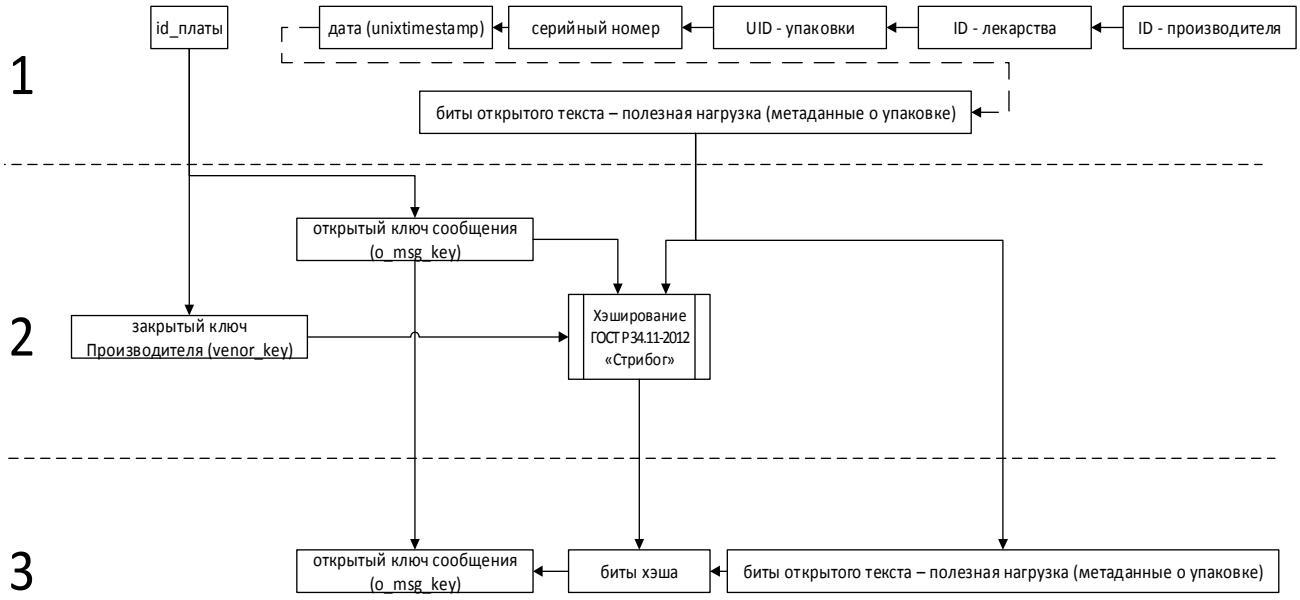

Рисунок 3.2 – Алгоритм создания цифрового идентификатора

Каждый идентификатор, фактически нанесённый на упаковку товара в виде маркера QR или DataMatrix представляет из себя набор полей, приведённый на таблице ниже.

Таблица 1 – Поля сообщения в двоичном виде

соль	Открытый Ключ	Хэш	МЕТА	выравнивание
128-бит	16256 - бит макс. для DM	23496 - бит макс. для QR		0-15 - бит

В нашей работе мы подразумеваем что «МЕТА» – это данные о упаковке ЛП (индивидуальный номер, серийный, код препарата, код производителя, дата выпуска и прочее), часть из этих данных перечисляются на упаковке, для визуального сопоставления покупателем, но также важно, что часть этих данных известна только лицензиату данного ЛП и «серверу» системы. Количество бит

отводимых для полезной информации зависит от того какого типа маркер будет применяться. Максимальная вместимость Data Matrix 2кб и около 3 кб (2953 байт) QR кода.

Открытый ключ Ключ – это ключ при помощи которого пользователь может расшифровать зашифрованный хэш и сравнить его с хэшем открытого сообщения.

Для обеспечения работы системы протокол предполагает наличие у экспортёра/производителя его личного закрытого ключа. Надёжнее всего будет кодировать его аппаратно, и хранить в форме ПЛИС (программируемой логической интегральной схемы). Данная схема будет включаться в состав маркирующего оборудования. Данный ключ является закрытым ключом производителя.

Как видно, в данном виде сообщения реализован принцип криптографии с открытым ключом и формирования электронной цифровой подписи в виде шифрованного хэша передаваемого сообщения.

На рисунке 3.3 представлен интерфейс тестового приложения реализующего формирование такого маркера. В тестовом приложении мы используем алгоритм формирования ЭЦП на основе алгоритма RSA а не отечественного ГОСТ 34-11. 2012 применение которого предполагается в действующей системе. На рисунке 3.4 изображён скриншот тестового приложения считывающего цифровой идентификатор и производящего его верификацию.

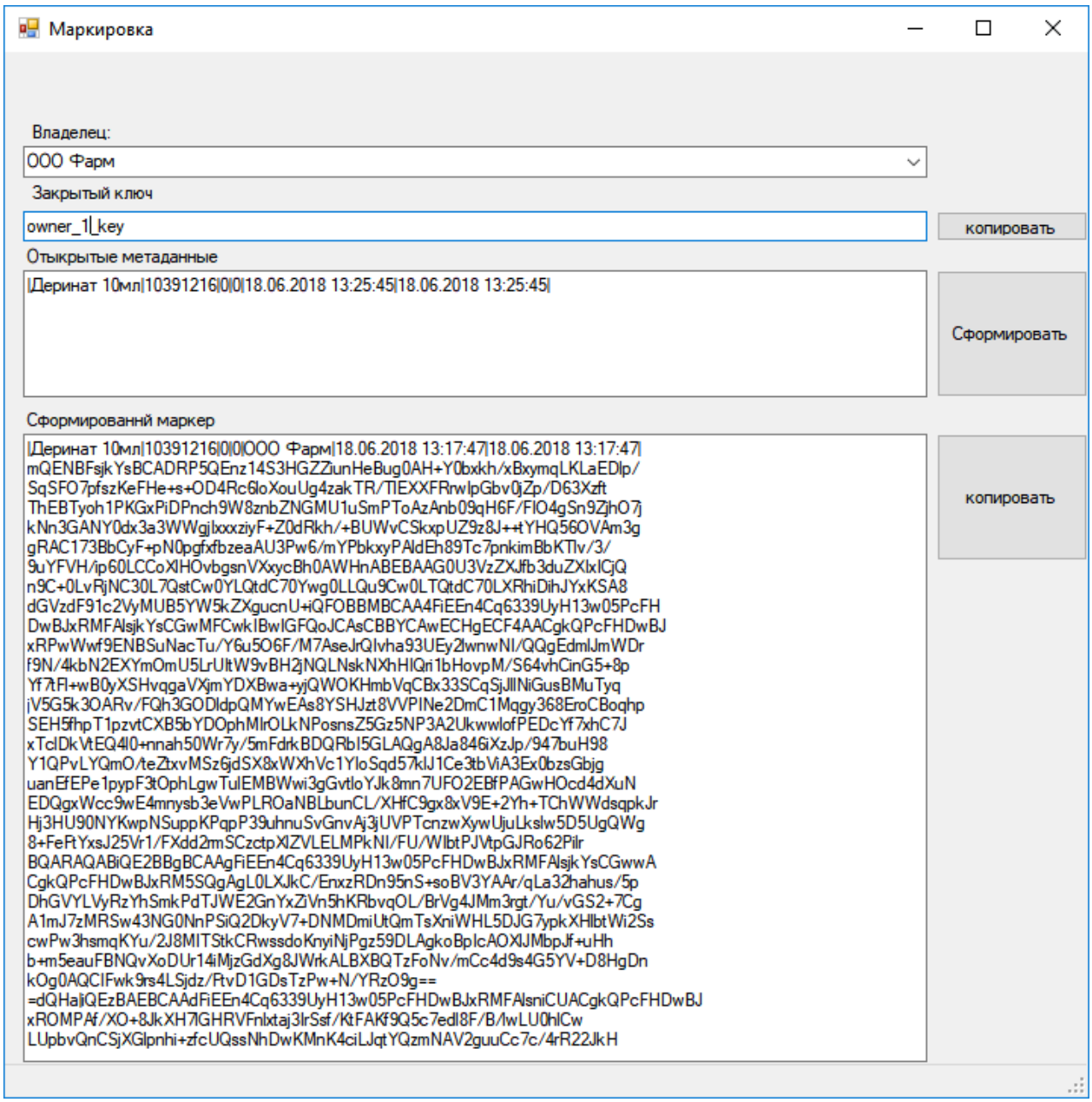

Рисунок 3.3 – Интерфейс тестового приложения формирующего цифровой идентификатор

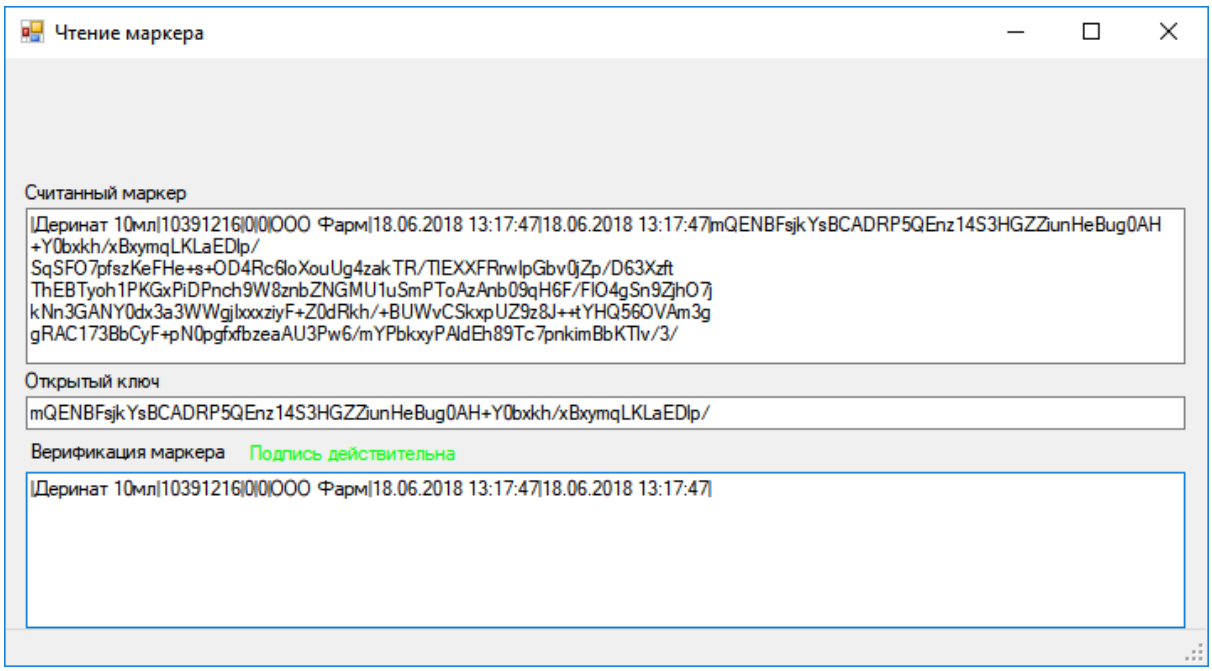

Рисунок 3.4 – Интерфейс тестового приложения проверяющего цифровой идентификатор

3.3 Реализация протокола верификации и мониторинга движения товара

Разрабатываемая система призвана защитить население от нелегальных лекарственных средств и предоставить гражданам и организациям возможность оперативной проверки их легальности.

Для осуществления движения товаров между участниками рынка необходимо при каждом перемещении осуществлять запись об изменении состояний объекта. Перемещение товара со склада на склад, передача между юридическими лицами, отправка в розничную продажу. Данная информация необходима для подтверждения достоверности того, что данный товар является той самой единицей товара которая в данный момент времени находится перед покупателем или представителем контролирующего органа.

На рисунке 3.5 изображён интерфейс приложения в поле которого введён цифровой идентификатор. Из идентификатора извлечён открытый ключ и с его помощью зашифрована контрольная стока содержащая символы: «test_string». В зашифрованном виде данная строка отправлена владельцу товара для расшифровки его закрытым ключом.

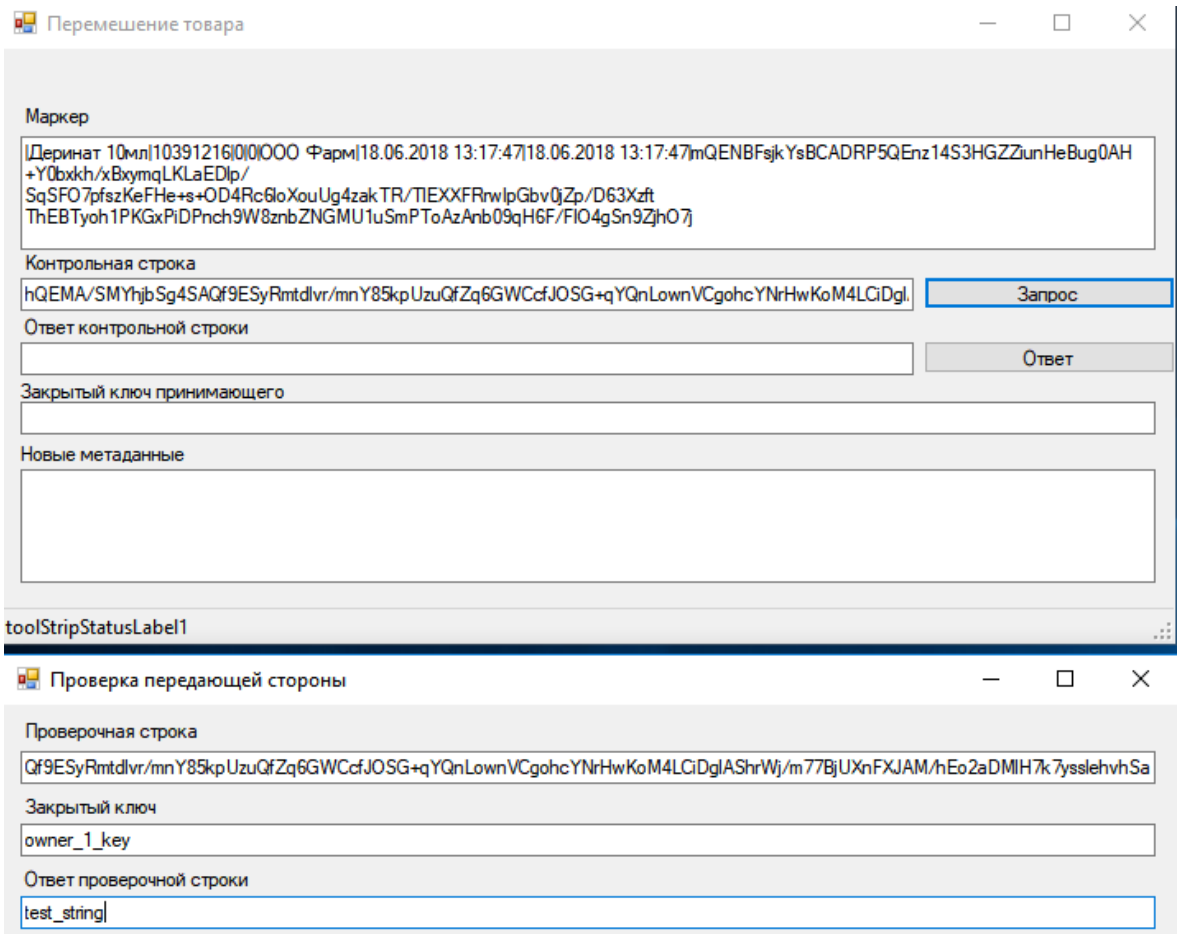

Рисунок 3.5 – Скриншот тестового приложения осуществляющего поверку условного владельца товара

На рисунке 3.6 изображён интерфейс приложения после подтверждения исходного владельца. В нём формируется новый идентификатор. Он может быть снова нанесён на товар при определённых условиях, но в любом случае он будет занесён в базу данные, и при последующем перемещении именно эта информация будет передана при проверке потребителем. И уже открытый ключ первого владельца будет применяться при контроле последующей транзакции. Данный механизм контроля реализуется при помощи алгоритма ассиметричного шифрования RSA с 1024 битным ключом.

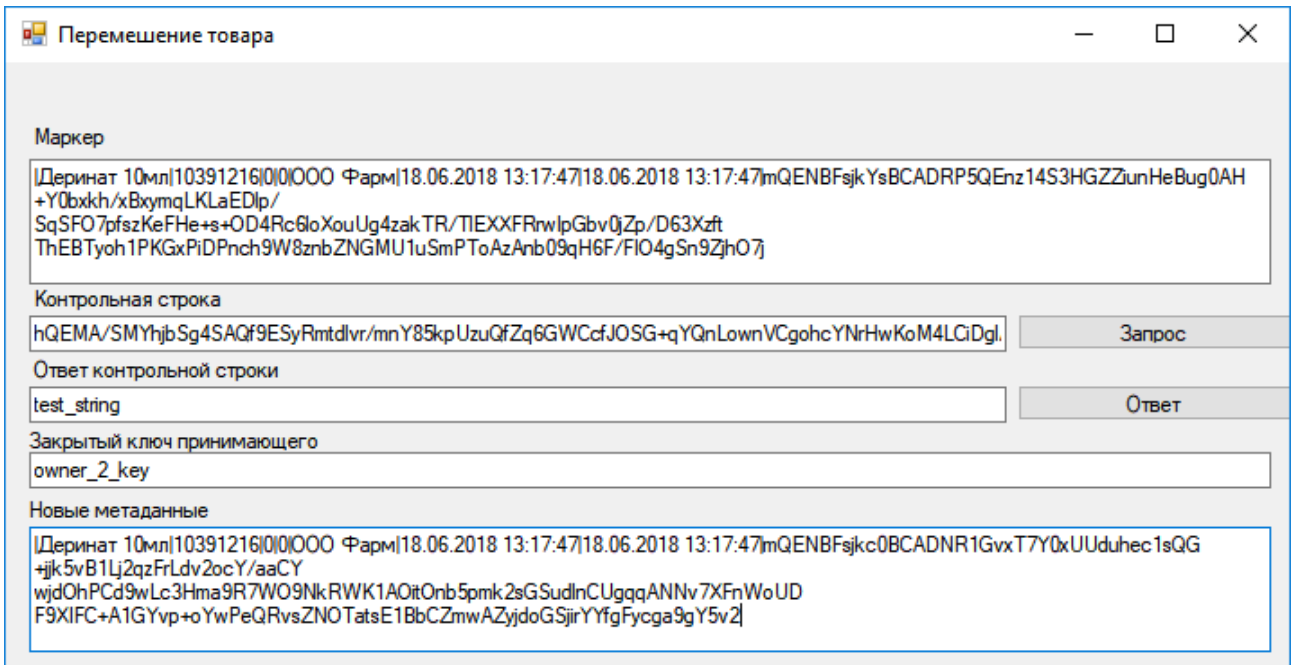

Рисунок 3.6 – Скриншот приложения осуществившего проверку и внёсшего изменения в метаданные.

3.4 SWOT анализ. Оценка целесообразности применения проектируемой системы

Система имеет возможность автоматизировать следующие процессы:

– процесс распознания фармацевтического препарата;
– идентификацию его серийного номера;
– контроль срока годности, подлинности и качества препарата;

Грамотное применение возможностей системы, в свою очередь позволит достичь следующих эффектов:

– оптимизация защиты потребителей от покупки некачественного или контрафактного товара. Быстрый и удобный способ определения подлинности лекарства;
– защита производителей и импортёров фармацевтических препаратов от недобросовестной конкуренции на рынке со стороны производителей контрафактной продукции;

– автоматизация и ускорение складских и аптечных операций за счёт обеспечения провизора индивидуальными средствами распознания, и за счёт подключения складских роботов к системе;

Разработанная система. позволит оперативно выявлять контрафактную и бракованную продукцию в обороте. Каждый человек при помощи своего устройства сможет противодействовать обороту контрафактных лекарственных средств. Таким образом, общество инструмент, с помощью которого оно может защитить себя и свои права потребителя от недобросовестных участников рынка. Данное явление можно назвать Crowd control.

Таблица 3.2 содержит SWOT-матрицу анализа сильных и слабых сторон разрабатываемой системы. В таблице рассматриваются потенциальные возможности системы и связанные с её применением трудности.

Таблица 3.2 – SWOT-матрица анализ сильных и слабых сторон системы

Сильные стороны	Возможности		Угрозы.		Итого
	1. Улучшение обстановки на рынке фарм. продукции	2. Совершенствование разработки	1. Компрометация данных	2. Быстрое моральное устаревание	
1. Низкая стоимость разработки	++	0	0	++	+3
2. Широкая сфера применения	++	++	+	++	+7
3. Обеспечение сопровождения	++	+	+	+	+5
Итого	+6	+3	+2	+5	+16
Слабые стороны					
1. Повышение накладных расходов торговых процессов	–	–	–	– –	–5
2. Нехватка квалифицированных кадров	– –	– –	– –	– –	–8
Итого	–3	–3	–3	–4	–13
Общий итог	+3	0	-1	+1	+3

Анализ сильных и слабых сторон проекта показывает, что, как и внедрение любой подобной системы, его внедрение приведёт к росту расходов на реализацию и соответственно, может привести к росту цен для потребителя.

С точки зрения производителя, расходы на внедрение подобной системы окупаются за счёт нивелирования последствий от недобросовестной конкуренции на рынке.

Так же, во внедрении подобных систем заинтересованно государство, его расходы на устранения последствий оборота контрафакта, с учётом долгосрочной перспективы влияния данного эффекта так же, можно отнести к расходам, окупающимся со временем. Кроме того, для внедрения некоторых систем государство уже сейчас предлагает субсидиальные программы.

Кабинет министров утвердил правила предоставления субсидий из федерального бюджета на создание системы мониторинга движения лекарственных средств. Применение данной системы поможет защитить население от фальсифицированных медицинских препаратов и способствовать оперативному выведению из оборота контрафактных и недоброкачественные препараты.

Документ опубликован на сайте правительства. Создателям данной системы, которому будут доступны субсидии из фона на реализацию государственной программы "Развитие фармацевтической и медицинской промышленности" на 2013 - 2020 годы, станет Российский фонд технологического развития.

Фонд из полученных им субсидий будет предоставлять целевые займы российским компаниям на приобретение оборудования и программного обеспечения для модернизации производства лекарственных препаратов и их маркировки.

3.5 Выводы по третьему разделу.

В данном разделе был рассмотрен процесс тестирования основных идей, предложенных в предыдущем разделе. Была проведена разработка приложения

Формирующего цифровой идентификатор товара с цифровой подписью. Так же было разработано приложение моделирующее движение маркированного товара на рынке, и производящего верификацию владельца товара посредством проверки факта владения им закрытым ключом.

Разработанная система. позволит оперативно выявлять контрафактную и бракованную продукцию в обороте. Каждый человек при помощи своего устройства сможет противодействовать обороту контрафактных лекарственных средств.

ЗАКЛЮЧЕНИЕ

В результате выполнения магистерской диссертации поставленные цели были достигнуты. Были выполнены следующие задачи:

– проведён сравнительный анализ существующих систем маркировки, идентификации, мониторинга товаров;

– предложен алгоритм обмена данными для системы цифровой идентификации;

– предложен алгоритм формирования криптографически стойкого маркера.

В качестве перспективы развития разработанной системы предполагаются государственные системы контроля и мониторинга, такие как ФГИС МДЛП и ЕГАИС, так же, данные алгоритмы и протоколы применимы в системах документооборота.

Разработанные алгоритмы позволит применять их как в частных, так и в государственных информационных системах цифровой маркировки и контроля оборота товаров и с достоверной точностью идентифицировать подлинность того или иного товара. Кроме того, систему подобной маркировки возможно применить для контроля документооборота или в сфере оказания услуг. А также данный функционал позволит контролирующим органам в режиме реального времени получать доступ к сведениям об участниках эксперимента, их продукции, данным о сгенерированных кодах и их передвижении.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Доклад секретариата шестьдесят второй ассамблеи здравоохранения Контрафактные изделия медицинского назначения [Текст]: доклад / ВОЗ. – 2009г. – 30 апр.- 7 с.

2. Фармацевтический рынок России – 2015 отчёт DSM Group [Текст] : отчёт – М. DSM Group, 2015 – 29 с.

3. Фармацевтический рынок России – 2013 отчёт DSM Group [Текст] : отчёт – М. DSM Group, 2013 – 71 с.

4. Bagozzi, D. Коалиция по борьбе с поддельными лекарствами под руководством ВОЗ изучает технологии по профилактике подделок [Электронный ресурс] / Daniela Bagizzi, Режим доступа: http://www.who.int/mediacentre/news/releases/2007/pr07/ru/

5. Российская Федерация. Законы. Федеральный закон от 12.04.2010 «Об обращении лекарственных средств» – 68 с.

6. Корнюшин, В. Автоматизация аптеки: борьба за товар [Электронный ресурс] / В. Конюшин // Фармацевтический Вестник. – Вып. 20. – 2011. – 14 июня. – Режим доступа: http://www.pharmvestnik.ru/publs/staryj-arxiv-gazety/avtomatizatsija-apteki-borjba-za-tovar.html

7. Людвиг, Ф. Глобальная борьба с контрафактной фармацевтической продукцией. Сочетание нормативного регулирования и технологий в качестве главной стратегии этой борьбы [Текст] / Ф. Людвиг // Фармацевтическая отрасль. – 2011 - №6. – с. 73 – 76.

8. Благовещенский, А. Россияне проверят подлинность лекарств через смартфон [Текст] / А. Благовещенский // Российская газета. – 2013 г. – 25 декабря. - Режим доступа: https://rg.ru/2013/12/25/lekarstvo-smartphone-site.html

9. Panasonic показала самые легкие наладонные бизнес-планшеты [Электронный ресурс] // Вести Hi-tech, Режим доступа : http://hitech.vesti.ru/news/view/id/8741

10. Штрих-код [Электронный ресурс] // Энциклопедия экономиста Grandars.ru, – Режим доступа : http://www.grandars.ru/college/tovarovedenie/shtrih-kod.html

11. ГОСТ 34.601-90 «Автоматизированные системы. Стадии создания»

12. ГОСТ 34.602-89 «Техническое задание на создание автоматизированной системы».

13. ГОСТ 34.603-92 «Виды испытаний автоматизированных систем»

14. ГОСТ Р ИСО/МЭК ТО 12182-2002 Классификация программных средств.

15. ГОСТ Р ИСО/МЭК 12119-2000 «Пакеты программ. Требования к качеству и тестированию».

16. Федеральный закон «О патентных поверенных» от 30.12.2008 № 316-ФЗ

17. ГОСТ 7.32-2001 «Отчет о научно-исследовательской работе. Структура и правила оформления».

18. Гатченко Н.А., Исаев А.С., Яковлев А.Д. «Криптографическая защита информации» – СПб: НИУ ИТМО, 2012. – 142 с.

19. Фастовцев Э. Сервис-ориентированные технологии интеграции информации [Электронный ресурс]. URL: http://khpi-iip.mipk.kharkiv.edu/library/sotii/lectures/Lecture5.pdf.

20. Вступили в силу требования о предоставлении сведений о сериях и партиях ЛС, поступающих в оборот // gmpnews.ru. 2016. № 15.01.2016.

21. Министерство здравоохранения Российской Федерации. Приказы. №866 от 30 ноября 2015 г. «Об утверждении Концепции создания Федеральной государственной информационной системы мониторинга движения лекарственных препаратов от производителя до конечного потреби // 2015.

22. Buydentity: Борьба с контрафактом // Habrahabr [Электронный ресурс]. URL: https://habrahabr.ru/company/microsoft/blog/312054/.

23. Ломакин В.В. Программирование и программное обеспечение информационных технологий / В.В. Ломакин, Белгород: НИУ БелГУ, 2014.

24. Петров А.А. Компьютенрная безопасность. Криптографические методы защиты. / А.А. Петров, Москва: ДМК, 2000. 448 с.

25. ГОСТ Р 34.12-2015 Информационная технология. Криптографическая защита ифнормации. Блочные шифры. 2015.

26. ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хеширования. 2012.

27. Маторин С.И., Зимовец О.А. Теория систем и системный анализ // : ИД Белгород.

28. Благодатских, В.А. Стандартизация разработки программных средств: Учебное пособие / Под ред. О. С. Разумова. — М.: Финансы и статистика, 2014. – 210с.

29. Вендров, А.М. Проектирование программного обеспечения экономических информационных систем: Учебник для студентов экономических вузов, обучающихся по спец. «Прикладная информатика (по областям)» и «Прикладная математика и информатика».-М.:Финансы и статистика, 2015.-544 с.

30. Аверченков, В. И. Организационная защита информации: учеб. пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - Брянск: БГТУ, 2005.

31. Баричев, С. Г. Основы современной криптографии / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. - Москва: СИНТЕГ, 2011. - 176 с.

32. Зиндер, Е.З. Бизнес-реинжиниринг и технологии системного проектирования. [Текст]: Учебное пособие. / Е. З. Зиндер.- М., Центр Информационных Технологий, 2015г.- 346с.

33. Когаловский, М. Р. Технология баз данных на персональных ЭВМ. [Текст]: учебное пособие. / М. Р. Когаловский. - М.:Финансы и статистика, 2016 г.- 123 с.

34. Хоффман, Л. Д. Современные методы защиты информации / Л.Д. Хоффман; под ред. В.А. Герасименко. – М.: Сов. радио, 1980. – 264 с.

35. Домарев, В.В. Энциклопедия безопасности информационных технологий. Методология создания системы защиты информации/ В.В. Домарев. – Киев: ТИД «ДС», 2001. – 668 с.

36. Жданов, О. Н. Методика выбора ключевой информации для алгоритма блочного шифрования / О.Н. Жданов. - М.: ИНФРА-М, 2015. - 607 с.

37. Черёмушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. М.: Изд. центр «Академия», 2009. 272 с.

38. Шумский, А.А. Системный анализ в защите информации / А.А. Шумский. - Москва: СПб.: Питер, 2005. - 224 с.

39. Муромцев, В.В. Проектирование информационных систем: Учебное пособие для студентов вузов заочной формы обучения по спец. «Прикладная информатика в экономике».-Белгород:БелГУ,2007.-160 с.

40. Силантьев, Н.Б. CASE-средства ERWin. – М.: Финансы и статистика, 2014. – 215с.

41. Федоров, Н.В. Проектирование информационных систем на основе современных CASE-технологий. [Текст]: учебное пособие. / Н. В. Федоров.- МГИУ, 2015 г.-128с.

42. Федорова, Е.Н. Теоретические основы программирования. [Текст]: учебное пособие. / Е.Н. Федорова.- МГИУ, 2016 г.-214с.

43. Форсайт, Д., Понс, Ж. Компьютерное зрение. Современный подход. – М.: Издательский дом «Вильямс», 2014.-928 с.

44. Черкашин П. В. Проблема выбора оптимального средства распознавания образов для идентификации лекарственных средств [Текст] / П. В. Черкашин, А. А. Литвинова, Р. П. Гахов // Новое слово в науке: перспективы развития : материалы IX Междунар. науч.–практ. конф. (Чебоксары, 7 авг. 2016 г.) / редкол.: О. Н. Широков [и др.]. — Чебоксары: ЦНС «Интерактив плюс», 2016. — № 3 (9). — С. 108–115. — ISSN 2411-8133.

45. Спичак И.В., Гахов Р.П., Порядин В.Е., Черкашин П.В., Чеботарёв А.А. Разработка мер по повышению информационной безопасности федеральной государственной информационной системы мониторинга

движения лекарственных препаратов [Текст] / И.В. Спичак, Р.П. Гахов, В.Е. Порядин, П.В. Черкашин, А.А. Чеботарёв // Фармацевтический кластер как интеграция науки, образования и производства: сборник материалов 6-й международной научно-практической телеконференции, г. Белгород, 5 октября 2016 г. / отв. ред. И.В. Спичак. – Белгород: ИД «Белгород» НИУ «БелГУ», 2016. – 138 с. -С. 133-137. — ISBN 978-5-9571-2235-7

46. Черкашин П. В. Разработка средств противодействия фармацевтическому контрафакту с использованием технологий машинного зрения [Текст] / П. В. Черкашин, Р. П. Гахов // Научные исследования: от теории к практике : материалы XI Междунар. науч.-практ. конф. (Чебоксары, 12 февр. 2017 г.) / редкол.: О. Н. Широков [и др.]. — Чебоксары: ЦНС «Интерактив плюс», 2017. — № 1 (11). — ISSN 2413-3957. Режим доступа :https://interactive-plus.ru/ru/article/118180/discussion_platform

47. Гахов Р.П., Черкашин П.В. Разработка системы идентификации продукта с гарантированной надёжностью [Текст] / Р.П. Гахов, П.В. Черкашин // Наука и образование: отечественный и зарубежный опыт : междуна-родная научно-практическая заочная конференция (26 мая 2017 г. Белгород): сборник статей/[орг. ком.: Гиричев А.В., Линник – Ботова С. И., Косогорова Л. В.] – г. Белгород: Издательство ООО «ГиК», 2017. – 185 с. Режим доступа :http://gikprint.ru/wp-content/uploads/2017/06/gikkonf-26-05-2017.pdf

48. Irina V. Spichak, Roman P. Gahov, Pavel V. Cherkashin, Vladimir E. Poryadin, Igor S. Friz DEVELOPMENT OF THE PHARMACOLOGICAL PRODUCT IDENTIFICATION SYSTEM WITH GUARANTEED RELIABILITY [Text] // International Journal of Green Pharmacy, 2017. Режим доступа :http://greenpharmacy.info/index.php/ijgp/article/view/1171

49. Черкашин П.В. Применение средств машинного зрения в системе идентификации маркировки и номерных знаков / П.В. Черкашин, А.И. Шепелев, О.Г. Худасова [и др.] // Наука, образование, общество: тенденции и перспективы развития : материалы IX Междунар. науч.-практ. конф. (Чебоксары, 12 февр.

2018 г.) / редкол.: О.Н. Широков [и др.] – 2018. – Чебоксары: ЦНС «Интерактив плюс», 2018.

50. Черкашин П.В. Проектирование системы распознавания номерных знаков государственной регистрации транспортных средств. Систематизация образов номерных знаков, применяемых в Российской Федерации / П.В. Черкашин, А.И. Шепелев, О.Г. Худасова [и др.] // Наука, образование, общество: тенденции и перспективы развития : материалы IX Междунар. науч.-практ. конф. (Чебоксары, 12 февр. 2018 г.) / редкол.: О.Н. Широков [и др.] – 2018. – Чебоксары: ЦНС «Интерактив плюс», 2018

51. Черкашин П.В. Применение средств машинного зрения в системе идентификации маркировки и номерных знаков / П.В. Черкашин, А.И. Шепелев, О.Г. Худасова [и др.] // Наука, образование, общество: тенденции и перспективы развития : материалы IX Междунар. науч.-практ. конф. (Чебоксары, 12 февр. 2018 г.) / редкол.: О.Н. Широков [и др.] – 2018. – Чебоксары: ЦНС «Интерактив плюс», 2018.

52. Черкашин П.В. Применение различных типов IP-АТС в корпоративной сети / К.Д. Исхакова, Е.А. Зайцева, П.В. Черкашин / науч. рук. Д.И. Ушаков // Наука, образование, общество: тенденции и перспективы развития : материалы IX Междунар. науч.-практ. конф. (редкол.: О.Н. Широков [и др.] – 2018. – Чебоксары: ЦНС «Интерактив плюс», 2018.

Магистерская диссертация выполнена мной совершенно самостоятельно. Все использованные в работе материалы и концепции из опубликованной научной литературы и других источников имеют ссылки на них.

«07» июня 2018 г.

_____ Черкашин П.В.