УДК 005.92

С.Г. Исроилов[1] cptrex.si@gmail.com
С.Н. Верзунов[2]***,*** *к.т.н.* verzunov@hotmail.com
[1]*Кыргызский государственный технический университет им. И. Раззакова, Бишкек, Кыргызстан*
[2]*Институт машиноведения и автоматики НАН КР, Бишкек Кыргызстан*

РАЗРАБОТКА ЗАЩИЩЕННОЙ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА НА ОСНОВЕ БЛОКЧЕЙН-ТЕХНОЛОГИИ

В данной статье представлены результаты разработки распределенной системы документооборота для хранения и обработки данных подучетных лиц СПЭНМ ГУВД г. Бишкека на основе технологии Blockchain.

Ключевые слова: информационная безопасность, информационная система, рабочая станция, модель угроз

Введение

На сегодняшний день сотрудники МВД КР имеют в своем распоряжении недавно введенную (с 01.01.2019 года) информационную систему ЕРПП (Единый реестр преступлений и проступков), куда заносится информация о всех правонарушениях, которые фиксируются на территории Кыргызской Республики. Данная централизованная система позволяет сотрудникам всех ведомств отслеживать правонарушения на территории республики. Подобная информационная система позволяет изучать динамику преступности в стране, делать выводы и разрабатывать стратегию по предотвращению новых преступлений. Положительные отзывы о такой централизованной системе подтолкнули другие ведомства на разработку внутренней гибкой системы документооборота, которая позволяла бы собирать информацию, обрабатывать, анализировать и формировать статистические отчеты.

Однако такие информационные нововведения охватывают лишь поверхностно все структуры без возможности углубления в определенные ведомства для решения узконаправленных задач. Для улучшения качества работы сотрудников и сокращения затраты времени на работу с документацией и была разработана система хранения и обработки данных для СПЭНМ ГУВД г. Бишкека (Служба по противодействию экстремизму и незаконной миграции Главного управления внутренних дел города Бишкека, далее просто Служба).

К сожалению, помимо повышения качества работы силовых ведомств путем внедрения информационных технологий, растет и спрос на конфиденциальную информацию, которой владеют структуры, а такие технологии не редко открывают доступ злоумышленникам к нужной для них информации, если раньше вся секретная документация находилась в рукописном виде, то теперь ведомства активно пользуются информационными технологиями, что ставит под удар секретность информации. Поэтому при разработке информационной системы хранения и обработки данных Службы было принято решение уделить внимание в первую очередь обеспечению безопасности секретных данных, которыми располагают сотрудники.

Актуальность проблемы обусловлена возрастающей в настоящее время нагрузкой на сотрудников Службы, связанной с решением ряда рутинных задач. В связи с чем предлагается автоматизировать такие задачи документооборота. как обработка, хранение и передача данных подучетных лиц Службы. Кроме того, в настоящее время отсутствуют какие-либо средства защиты информации, что увеличивает вероятность

нарушения главных свойств информационной безопасности – конфиденциальности, целостности, доступности. Разработанная система позволит решить вышеперечисленные проблемы с использованием передовой технологии и вычислительных ресурсов Службы и обеспечить информационную безопасность без потери результативности работы сотрудников.

Формулировка проблемы

Целью данной работы является разработка распределенной системы документооборота для хранения и обработки данных подучетных лиц СПЭНМ ГУВД г. Бишкека с целью автоматизации работы со служебными материалами, формирования детальной отчетности и обеспечения, безопасности при помощи блокчейн-технологии.

Задачами настоящего исследования являются:

- Описание предметной области.
- Разработка политики информационной безопасности информационной системы.
- Разработка распределенной системы управления базой данных (РСУБД).
- Внедрение технологии blockchain в разработанную РСУБД.
- Разработка графического интерфейса пользователя к системе.
- Разработка механизмов защиты информации, обрабатываемой системой.

Блокчейн-технология в системах электронного документооборота

Блокчейн (blockchain или block chain) – выстроенная определенным образом непрерывная последовательная цепочка блоков, содержащих информацию. Цепь блоков строится по правилам, которые задает разработчик системы, куда внедряется данная технология. На каждом узле блокчейн-системы хранятся копии всей базы данных в целом, и они сверяются между собой. Это придает системе жизнеспособность даже в случае успешных хакерских атак на ее одиночные узлы. Для проверки информации, хранящейся в цепи блоков, используются полные узлы сети. На рис. 1 демонстрируется, как устроена цепь blockchain. Цепь blockchain формируется из блоков, которые неразрывно связаны между собой хэшем предыдущего блока. Самый первый блок в цепи называется генезис-блоком и формируется отдельно по особому алгоритму, который задаст разработчик, а последующие уже согласно технологии. Блок может формироваться по разным критериям, с соблюдением некоторых правил, которые перечислены ниже [1]:

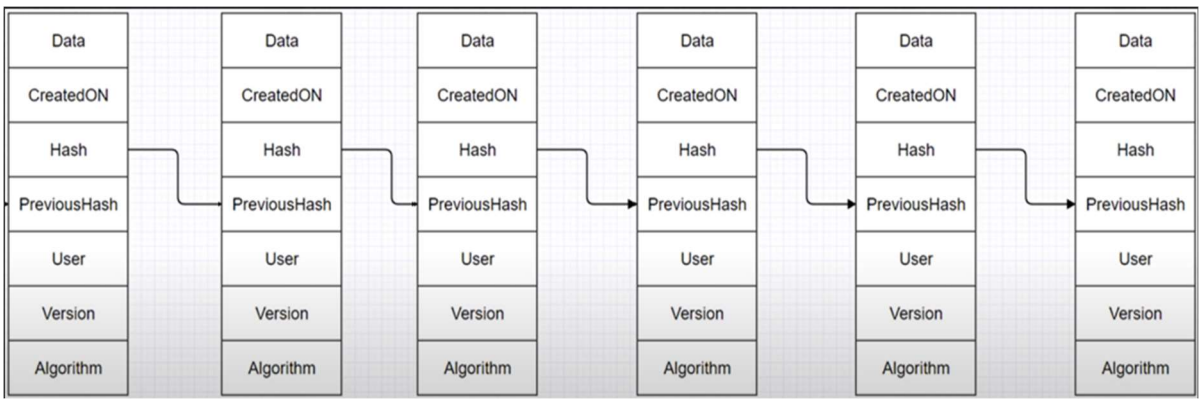

Рис. 1. Цепочка блоков информации технологии Blockchain

1. Блок должен нести в себе хэш предыдущего блока.
2. Блок должен нести в себе собственный хэш, который формируется по собственному алгоритму разработчика.
3. Блок должен нести в себе все данные, которые участвуют в образовании хэша блока.

Технология blockchain включает в себя такие важные составные, как:

- распределенное хранение данных;
- доказательство работы (PoW)/доказательство доли (PoS);
- консенсус.

Распределенное хранение данных подразумевает, что каждый узел сети будет иметь собственную копию данных. Нет единого централизованного хранилища. Согласно источнику [1]: «Полные узлы – точки, отвечающие за отправку и получение данных в блокчейн-сети. Они поддерживают и обеспечивают безопасность blockchain-сети. Эти узлы также называются полными проверяющими узлами (validating nodes), поскольку участвуют в процессе проверки транзакций и блоков системы. Полные узлы также могут ретранслировать новые транзакции и блоки в блокчейне».

Консенсус, алгоритм консенсуса – способ решения задачи, поставленной сервером (например, добавление нового блока, проверка другой цепи блоков, может определяться как механизм, с помощью которого blockchain-сеть достигает консенсуса. Он удостоверяет, что соблюдаются все правила проверок, и гарантирует, что целостность блока или цепи блоков не нарушена.

Доказательство работы (PoW) – алгоритм консенсуса, который используется для подтверждения операции в системе и передачи новых блоков цепи серверу. Проще говоря, как только произойдет операция, которая требует модификации существующей информации или же добавление новой, сервер попытается сформировать блок данных и после успешного формирования (прохождения всех этапов проверки) узел, который сформировал этот блок, отправит цепь блоков на проверку другим участникам сети (другим полным узлам), которые в свою очередь подтвердят целостность данных инициатора- узла.

Таким образом, блокчейн – выстроенная по определённым правилам непрерывная последовательная цепочка (связный список) блоков, содержащих информацию [2]. Впервые термин появился как название полностью реплицированной распределённой базы данных, реализованной в системе Биткойн, из-за чего блокчейн часто относят к базовым технологиям криптовалют, однако система цепочек блоков может быть распространена на любые взаимосвязанные информационные блоки и может использоваться в самых разных отраслях нашей жизни: управление поставками, логистика, защищенный документооборот [3].

Информация, хранящаяся в блокчейне, существует как общая и постоянно сверяемая база данных. Такой способ использования сети имеет очевидные преимущества. База данных блокчейна не хранится в каком-то единственном месте, а это означает, что он сохраняет записи действительно публично, и они легко проверяются. Не существует централизованной версии этой информации, которую можно было бы

повредить. Копии хранятся на миллионах носителей одновременно, и ее данные доступны для всех пользователей во внешней сети [4].

Основная задача технологии блокчейн – доверительная передача собственности на цифровые активы в недоверительной сети без посредников. Ключевым понятием блокчейна является транзакция – единственный способ изменить состояние данных. Блок – это структура данных, позволяющая хранить список транзакций. Узлы блокчейн-сети создают транзакции, обмениваются ими и изменяют состояние блокчейн-сети. Чаще всего копии цепочек блоков хранятся и обрабатываются независимо друг от друга на различных компьютерах. Фактически блокчейн представляет собой логику хранения данных, не зависящую от какого-либо центра – отдельного сервера или группы серверов. Блокчейн отличает неизменность хранимых данных, которая достигается за счет приемов криптографии, а не за счет доверия к кому-либо. Два простейших криптографических алгоритма, используемых в блокчейне, – это хеш-функции и электронные подписи, обеспечивающие целостность транзакций и отвечающие за авторизацию. Участники блокчейн-сети не являются равноправными: почти в любой реализации этой технологии введено следующее распределение ролей: − валидаторы – участники, пишущие транзакции в журнал; − аудиторы – участники, не записывающие транзакции, а только проверяющие их правильность; − легкие клиенты – участники, не хранящие полные копии блокчейна, а взаимодействующие с сетью через другие узлы. Глобальные вложения, связанные с блокчейн-технологиями, в 2021 году могут достичь 9,7 млрд долларов США. Размер рынка рассчитывается на основе прогнозируемых доходов от внедрения решений блокчейн, а также предоставления услуг и сервисов на его основе. При этом предполагается, что среднегодовой темп роста в период до 2022 года составит от 79,6% до 81,2%, однако ряд регионов будет наращивать темпы роста в области блокчейн-индустрии опережающим образом: Япония – 127,3%, Латинская Америка – 152,5% , Анализ мировых трендов патентования технологий блокчейн за последние 5 лет выявил 2565 патентных документов, сгруппированных в 1804 патентных семейства. До 2013 года активность практически отсутствовала, начиная с 2014 года и далее наблюдается увеличение количества поданных патентных документов. Согласно статистике, приведённой Всемирной организацией интеллектуальной собственности WIPO, за 2014 год было сделано 84 запроса на патентирование блокчейн-проектов, за 2015 год – 229 запросов, 2016 год – 455, ещё больше за 2017-й – более 1500. Несмотря на непродолжительный период патентования технологий блокчейн, доля выданных патентов высока и составляет более 10%. Принимая во внимание то, что более 75% патентных документов опубликованы после 2015 года, а также продолжительный срок экспертизы патентных заявок (около двух лет в Европейском патентном ведомстве и до нескольких лет в США), такая большая доля выданных патентов свидетельствует о зрелости и высокой значимости технологий [5].

Во многих организациях осуществляется обмен информацией: с деловыми партнерами, государственными служащими, региональными партнерами. Значительная часть информации передается в виде документов на традиционных носителях. Но в последнее время значительный объем информации поступает по информационно-цифровым каналам, посредством которых передаются электронные документы. Даже

традиционный (бумажный) документооборот сегодня немыслим без использования электронных документов и электронного документооборота [6].

Если обратиться к областям применения блокчейн, то одной из наиболее перспективных представляется технология защищенного документооборота, который может стать намного безопаснее – в первую очередь за счёт ведения децентрализованного реестра документов, который невозможно изменить или подправить. Пользователи смогут работать с документами, имея полную уверенность в их авторстве и подлинности. Таким образом, решается множество проблем, связанных с несовершенством бюрократического аппарата, опасностью махинаций и подделки документов. На данный момент в мире уже существует множество реализаций подобной технологии, например, сервис BlockSign (США), разработанный нью-йоркской компанией Basno, представляющей собой общедоступный регистр, в котором хранятся подписанные электронным способом документы [7].

С появлением новой технологии многие зарубежные компании начали внедрять её в свои организации. Так, китайская консалтинговая компания PwC поделилась результатами исследования, проведенного в 2018 г., по теме: «Технология блокчейн и ее применение». В процессе исследования было опрошено 600 руководителей из 15 крупных организаций. Их спрашивали, применяют ли они систему блокчейн и в чем видят её потенциал. Итоги опроса позволили сделать вывод, что Китай в скором времени может стать блокчейн-державой. Также нельзя оставить без внимания и Бразилию. Ведь именно в данной стране произошла первая сделка по продаже недвижимости при помощи блокчейн-технологии. Она была заключена всего лишь за 20 минут вместо 30 требуемых дней. США и страны Европы также не остались в стороне. Так, в США данная технология применятся уже не только в финансовой сфере, но и для обмена медицинскими данными. А в Испании создают блокчейн-систему контроля поставок древесины [8]. Успешные примеры внедрения технологии блокчейн в бизнес-процессы различных компаний дают надежду и системам электронного документооборота. Но способен ли блокчейн действительно улучшить архитектуру подобных систем? Прежде всего следует оценить технологию по ключевым параметрам: юридической значимости и актуальности для бизнес-процессов. Несмотря на сдерживающие факторы (технические сложности внедрения и высокие финансовые издержки) повсеместного перехода документооборота организации на технологию бокчейн, данная технология полностью оправдывает себя в действии. Она позволяет не только оптимизировать различные бизнес-процессы, но и сэкономить миллиарды долларов. По данным международного агентства Accenture, к 2025 г. экономия на операционных расходах с учетом внедрения блокчейна составляет от 8 до 12 млрд. долларов [9]. По многочисленным исследованиям, проведённым в зарубежных организациях, было выявлено, что технология решает огромный спектр задач начиная от оптимизации документооборота, проведения платежей, обмена документацией в рамках различных сделок до контроля цепочек поставок и сокращения временных затрат на исполнение бизнес-сделок как внутри компании, так и на стороне контрагентов. Отсюда можно сделать вывод, что данная технология достаточно эффективна и имеет ряд преимуществ в электронном документообороте, таких как:

- снижение правовых рисков;

- увеличение скорости и точности обработки информации;
- уменьшение затрат при хранении данных и при обмене платежами;
- эффективно организованную поисковую систему документов;
- исключение дублирования информации;
- исключение возможности потери/кражи или вовсе уничтожения какого-либо документа или его фрагмента;
- отсутствие постоянной нужды в улучшении технических средств и наращивании технических объёмов.

Таким образом, резюмируя всё вышесказанное, можно сделать следующий вывод, что технология блокчейн позволит не только сократить время проведения различных бизнес-операций, но и также оптимизировать и обезопасить документооборот организации. Работоспособность данной технологии в системе электронного документооборота уже доказана на практике, поэтому остаётся лишь подобрать подходящие области для её применения и предусмотреть соответствующие механизмы контроля и управления, препятствующие её использованию в противоправных целях.

Предлагаемое решение и его теоретическое обоснование

СЭД (система электронного документооборота) насчитывает в настоящем времени 15 пользователей с разными правами доступа к хранящейся информации. Пользователи могут просматривать информацию, которая доступна им, а редактировать только ту информацию, которая был внесена автором.

На всю группу сотрудников (5 человек) выделено по три персональных компьютера. В помещении находится три сетевых принтера, один сетевой коммутатор, один сетевой маршрутизатор. Существует локальная сеть, доступ в интернет отсутствует.

Только на служебных компьютерах имеется возможность для редактирования информации пользователем в системе. С других устройств в сети пользователи смогут только просматривать информацию и отправлять на печать.

Пользователи имеют доступ к своей информации, у руководителя Службы есть возможность скрывать информацию и делать ее доступной определенному пользователю. Права администратора СЭД будут отсутствовать у пользователей, которые являются сотрудникам. Учетная запись администратора будет существовать отдельно и по умолчанию не будет использоваться. Возможность использования такой учетной записи будет доступна только начальнику Службы или отдельному техническому сотруднику.

Для того, чтобы воспользоваться возможностями СЭД, сотрудник должен авторизоваться в операционной системе, а затем подключиться к СЭД. После этого сотруднику будут открыты возможности согласно его правам доступа. Авторизованные сотрудники могут внести новую информацию. Для этого необходимо заполнить все обязательные пункты и подтвердить добавление информации или изменение существующей. Помимо этого, сотрудники могут просматривать существующую информацию, отслеживать статистику и распечатывать необходимую информацию. Сотрудники могут вносить заметки и оставлять комментарии для своих коллег, чтобы те обратили внимание на определенные детали.

Главной задачей такой системы является обеспечение безопасности хранения информации для дальнейшего удобного использования. Система нацелена на быстрый поиск нужной информации и выдачу информации на основе выставленных фильтров.

Таким образом следует выделить следующие возможности системы:

- обработка досье подучетных лиц Службы;
- доступ к досье подучетных лиц Службы;
- хранение досье подучетных лиц Службы;
- распечатка досье подучетных лиц Службы.

Основная цель информационной безопасности СЭД – обеспечение стабильной работы Службы и защита от непреднамеренного (неправильного, незаконного) изменения информации в системе, а также хранение, защита от раскрытия, потери, утечки.

Анализ требований. В процессе проведения анализа требований к разрабатываемой системе была создана модель в виде диаграммы IDEF0 (рис.2). Данная диаграмма показывает бизнес-процессы, которые протекают внутри Службы. Однако для более детального описания бизнес-процессов была составлена декомпозиция основной диаграммы описания бизнес-процессов IDEF0 (рис. 3), что позволяет более детально рассмотреть проблемы и правильно определить требования к разрабатываемой системе.

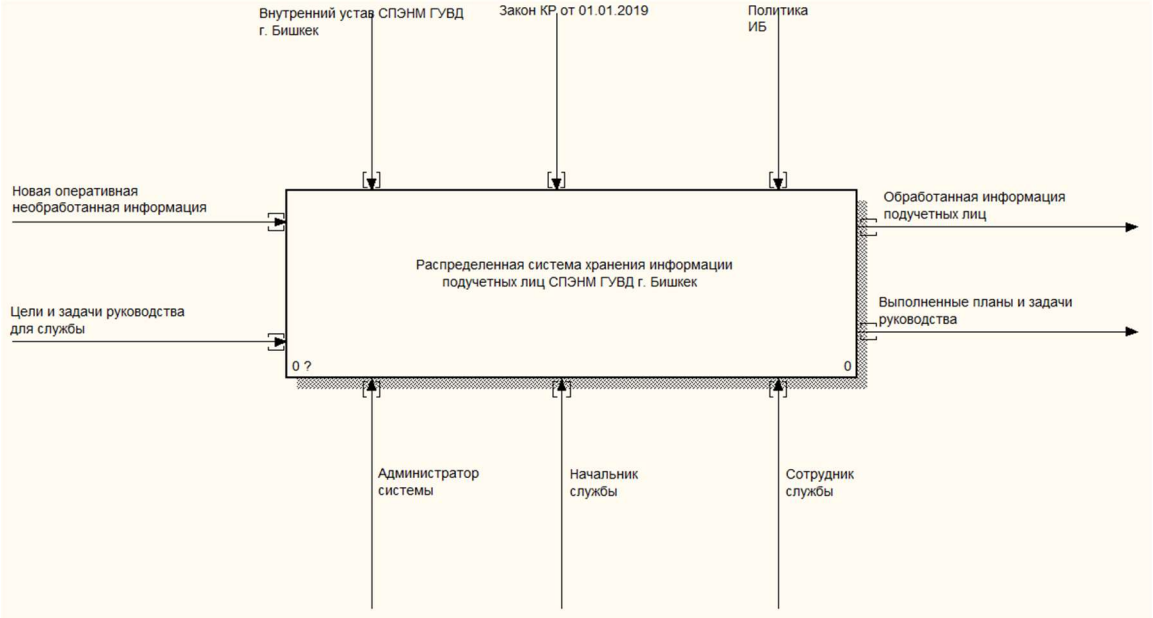

Рис. 2. Диаграмма описания бизнес-процессов в СЭД

В процессе определения требований к разрабатываемой системе были выявлены основные свойства, которыми она должна обладать.

Концептуальная модель. Для того чтобы графически отобразить общие требования к функциональному поведению проектируемой системы, была разработана концептуальная модель в виде UML – диаграммы вариантов использования (USE CASE). Данная модель предоставляет список всех пользователей системы, а также цели, которые они преследуют при использовании.

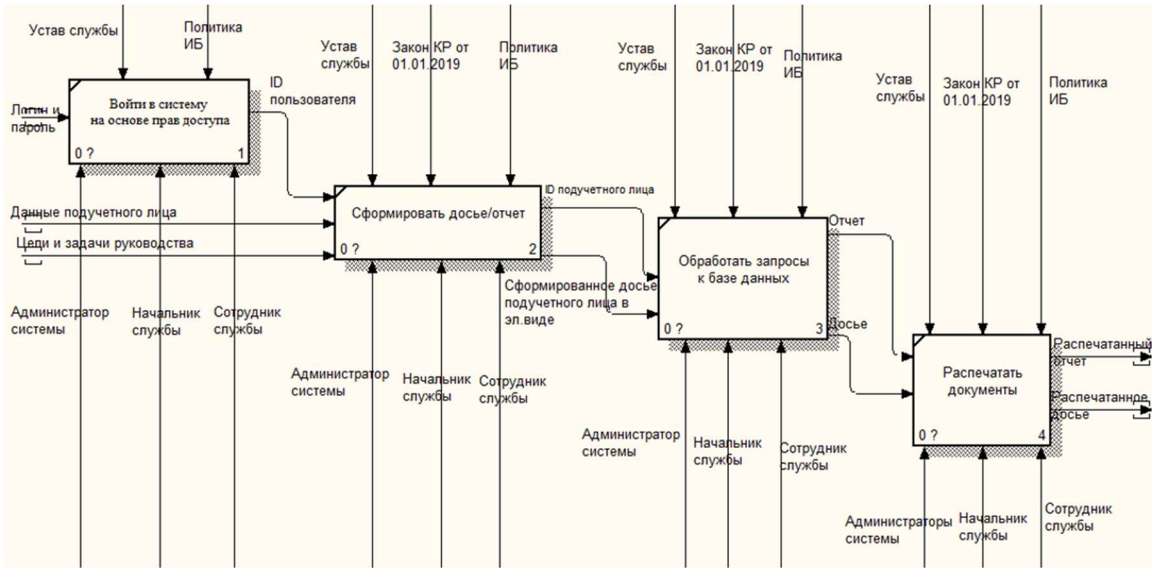

Рис. 3. Декомпозиция основного процесса СЭД

На рис. 4 представлена диаграмма вариантов использования. В системе предусмотрены следующие роли: «Администратор системы», «Начальник службы»,

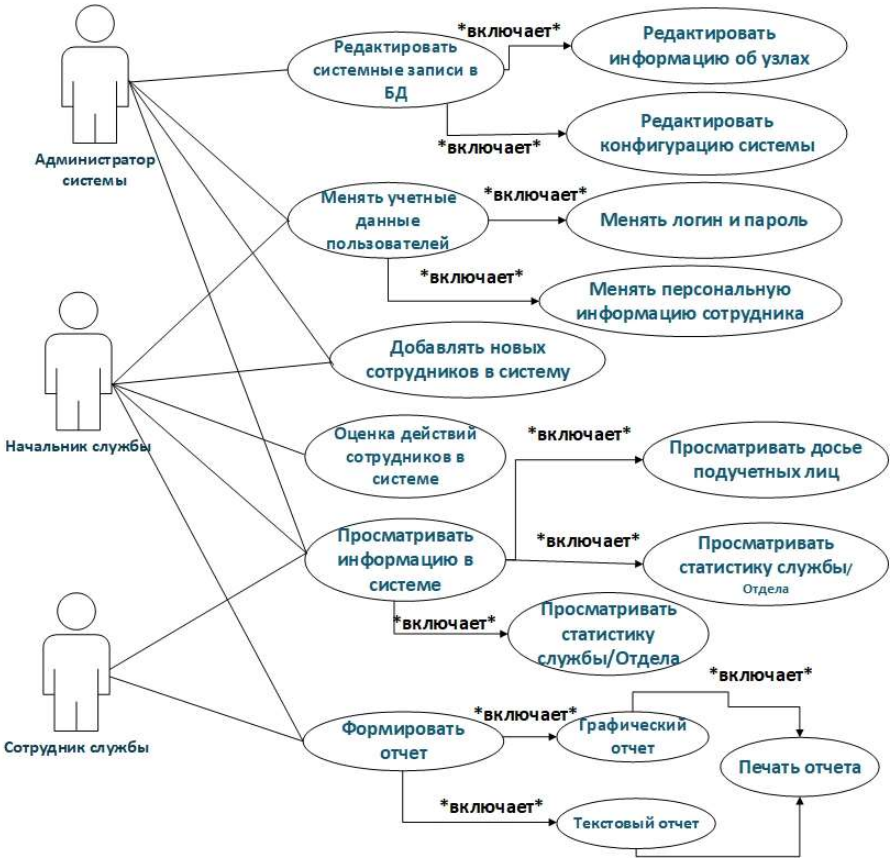

Рис. 4. Концептуальная модель Use-Case

«Сотрудник службы». На диаграмме показаны три актера, которые являются необходимыми для работы СЭД. Их роли определяются следующим образом: Актер «Администратор системы» – лицо, которое следит за работоспособностью системы: все ли узлы обрабатывают блоки данных или нет. Также вводит данные об уровнях доступа

пользователей, проводит мониторинг инцидентов, регистрирует новых сотрудников в системе. Актер «Начальник службы» – лицо, которое следит за работой. Актер «Сотрудник службы» – лицо, которое выполняет рутинные операции, обеспечивающие работу Службы.

Модель потоков данных. С помощью модели потоков данных приведем описание того, как будут в системе преобразоваться потоки данных, используя разрабатываемую систему (модель TO-BE). Данная модель описывает процесс преобразования данных от ее входа до выдачи пользователю. Модель потоков данных начинается с построения диаграммы работы Службы. Она включает в себя три внешние сущности: «Начальник службы», «Сотрудник службы», «Администратор службы» (рис. 5). Весь функционал системы представлен в виде декомпозиции диаграммы потоков данных.

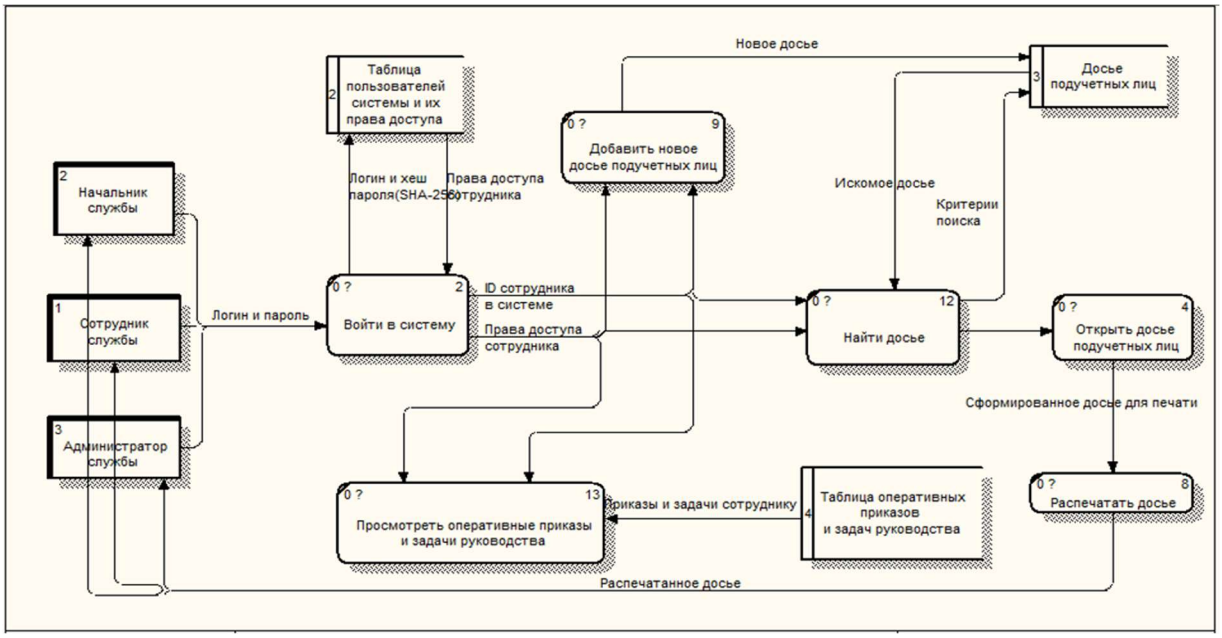

Рис. 5. Диаграмма потоков данных TO-BE

Ролевая модель безопасности объекта. В процессе исследования деятельности Службы была выбрана ролевая модель безопасности как наиболее гибкая, максимально точно подошедшая под спроектированную распределенную СЭД, обеспечивающую хранение данных подучетных лиц. Как сказано в работе [10]: «Ролевая модель безопасности появилась как результат развития дискреционной модели. Однако она обладает новыми по отношению к исходной модели свойствами: управление доступом в ней осуществляется как на основе определения прав доступа для ролей, так и путем сопоставления ролей пользователям и установки правил, регламентирующих использование ролей во время сеансов. В ролевой модели понятие «субъект» замещается понятиями «пользователь» и «роль».

Пользователь – человек, работающий с системой и выполняющий определенные служебные обязанности. Роль – это активно действующая в системе абстрактная сущность, с которой связан набор полномочий, необходимых для выполнения определенной деятельности. Подобное разделение хорошо отражает особенности деятельности различных организаций, что привело к распространению ролевых политик безопасности. При этом как один пользователь может быть авторизован

администратором на выполнение одной или нескольких ролей, так и одна роль может быть сопоставлена одному или нескольким пользователям. При использовании ролевой политики управление доступом осуществляется в две стадии»:

- для каждой роли указывается набор полномочий (разрешений на доступ к различным объектам системы);

- каждому пользователю сопоставляется список доступных ему ролей.

При определении ролевой политики безопасности используются следующие множества и функции:

- U – множество пользователей;
- R – множество ролей;
- P – множество полномочий (разрешений) на доступ к объектам системы;
- S – множество сеансов работы пользователя с системой.
- user: S -> U – функция, определяющая для сеанса s ∈ S текущего пользователя u ∈ U: user(s) = u;
- roles: S -> {R} – функция, определяющая для сеанса s ∈ S набор ролей из множества R, доступных в данном сеансе:
- permissions : S -> {P} – функция, задающая для сеанса s ∈ S набор доступных в нём полномочий (иначе говоря, совокупность полномочий всех ролей, доступных в данном сеансе).

Согласно работе [10]: «В качестве критерия безопасности ролевой модели используется следующее правило: система считается безопасной, если любой пользователь системы, работающий в сеансе $s \in S$, может осуществлять действия, требующие полномочия p ∈ P, только в том случае, если p ∈ $permissions(s)$. Существует несколько разновидностей ролевых моделей управления доступом, различающихся видом функций user, roles и permissions. В частности, может определяться иерархическая организация ролей, при которой роли организуются в иерархии, и каждая роль наследует полномочия всех подчиненных ей ролей. Могут быть определены взаимоисключающие роли (т. е. такие роли, которые не могут быть одновременно назначены одному пользователю). Также может вводиться ограничение на одновременное использование ролей в рамках одной сессии, количественные ограничения при назначении ролей и полномочий, может производиться группировка ролей и полномочий». В системе предусмотрено три роли:

Сотрудник Службы – основная роль, которая позволяет пользователю взаимодействовать с системой (просматривать и редактировать досье согласно полномочиям).

Руководство Службы – роль для пользователей с повышенными правами. Данная роль игнорирует полномочия и позволяет просматривать всю информацию в системе.

Администратор Службы – роль для сотрудников информационной безопасности Службы. Не имеет ограничений. Открыт доступ к системным записям.

В системе предусмотрено три уровня (полномочий) доступа (рис. 6):

Уровень 1 – основной уровень, данным уровнем располагают все сотрудники Службы.

Уровень 2 – присваивается отдельным пользователям в системе. Позволяет просматривать информацию уровнем ниже.

Уровень 3 – присваивается к досье высокого уровня секретности. По умолчанию имеют доступ роли «Руководство Службы».

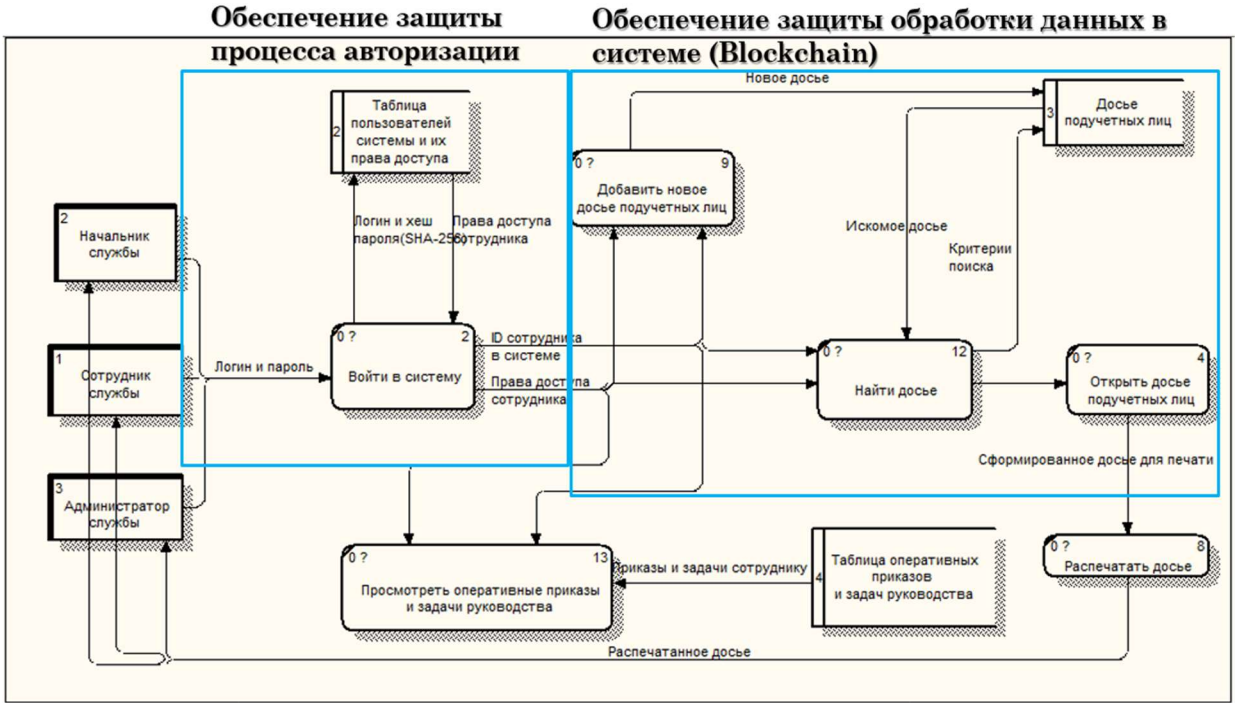

Рис. 6. Схема расположения защитных механизмов в СЭД

Методы и технологии для защиты системы

При решении вопроса о защите информационной системы внимание акцентировалось на достижение трех фундаментальных понятий информационной безопасности, таких как:

- Конфиденциальность
- Целостность
- Доступность

Эти три понятия не перекрывают друг друга по уровню значимости и всегда находятся на одной ступени. Для того, чтобы достичь обеспечения всех трех условий информационной безопасности, было принято решение сменить архитектуру с централизованной системы на распределенную. Такой подход позволит снизить финансовые затраты на оборудование и повысить отказоустойчивость и доступность данных. Однако этого недостаточно, так как остальные механизмы безопасности (правовые документы, технические ограничения и т.д.) не обеспечивают достижения целостности в полной мере при заданных условиях работы информационной системы.

Проанализировав функционирование Службы и сделав выводы о специфике работы, для достижения целостности было принято решение взять за основу принцип работы технологии blockchain.

Распределенная система хранения данных. Распределенная система хранения данных – это комплексное программно-аппаратное решение по организации надёжного хранения информационных ресурсов и предоставления гарантированного доступа к ним.

Плюсы:

1. Разделимость и локальная автономность.
2. Повышение доступности данных.
3. Повышение надежности.
4. Повышение производительности.
5. Экономические выгоды.
6. Модульность системы.

Использование блокчейн-технологии в СЭД. Блокчейн-технология внедрена в СЭД Службы для обеспечения одного из главных свойств информационной безопасности – целостности данных.

Загрузка блоков в цепь blockchain. При включении одного из серверов системы серверная машина выгружает из базы данных блоки с информацией. Каждый блок состоит из (рис. 7) таких элементов, как:

1. ID – идентификатор блока.
2. Дата создания блока.
3. Хэш блока (заранее просчитанный перед добавлением в базу данных).
4. Данные (досье), которые хранит в себе блок.
5. Предыдущий хэш блока (заранее просчитанный перед добавлением в базу данных).
6. Адрес сервера, который был инициатором добавления блоков.

Рис. 7. Таблица блоков данных цепи blockchain

Проверка целостности блока данных. Перед добавлением блока данных в основную цепь blockchain блок проходит проверку на целостность данных внутри блока. Блок, выгруженный из базы данных, имеет свой заранее просчитанный хэш, а также данные, которые он предназначен хранить (досье). Сервер, используя данные блока, заново просчитывает хэш, используя алгоритм шифрования SHA 256, и сверяет его с изначальным хэшем блока. Создание хэша происходит по следующей формуле:

Hash = SHA256 (ID + PreviousHash + Data).

Hash – сформированный хэш блока.

ID – идентификатор блока (присваивается автоматически сервером в момент его формирования. Уникален).

PreviousHash – хэш предыдущего блока.

Data – данные системы, которая содержит в себе блок (досье подучетного лица).

SHA256() – криптографический алгоритм необратимого преобразования произвольной длины сообщения в фиксированную длину потоков символов.

В случае, если только что сформированный хэш равен хэшу блока, то проверка считается пройденной, и сервер переходит к следующему этапу.

Сравнение хэша с другими блоками. После успешного прохождения проверки хэша блока сервер начинает проверку хэша предыдущего блока с хэшем текущего блока. Если хэш совпадает, то данный блок добавляется в основную цепь блокчейна системы.

Проверка всей цепи блоков других серверов (узлов) в сети показана на рис. 8. После успешного формирования цепи блоков сервер запрашивает другие сформированные цепи блоков узлов в сети. Каждый узел в сети проверяет все доступные цепи блоков. Если хотя бы одна цепь блоков не пройдет проверку, работа в сети будет невозможна, так как в этом случае возникает вероятность нарушения целостности данных системы.

Практическое исследование и выводы

Вход в систему. Для входа необходимо запустить соответствующее приложение на рабочем столе. После запуска перед пользователем откроется окно авторизации приложения (рис. 9).

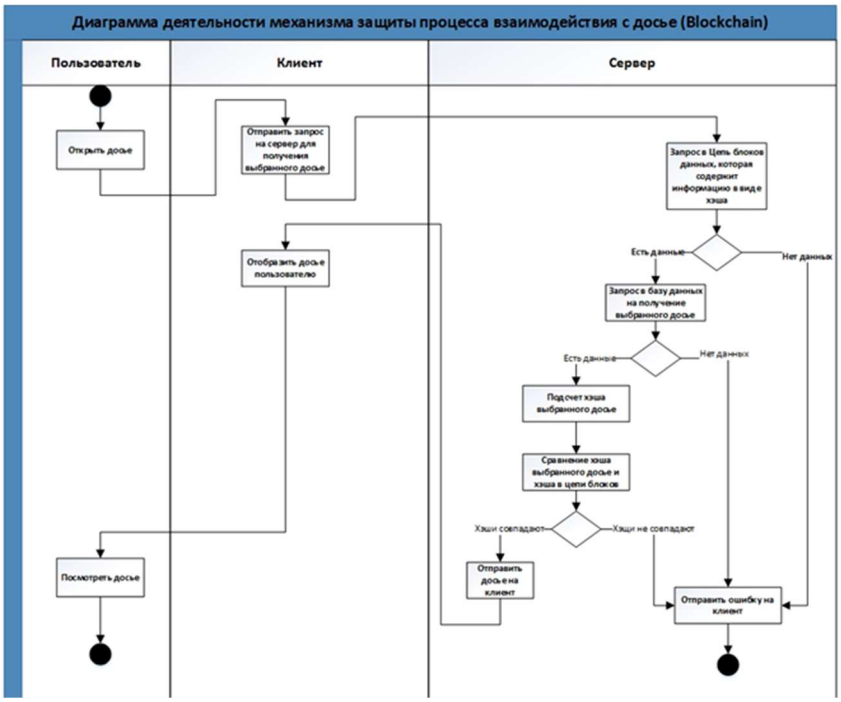

Рис. 8. Диграмма деятельности процесса защиты информации в системе с использованием Blockchain

Профиль сотрудника. Завершив процесс авторизации в системе, пользователю становится доступно окно профиля сотрудника, которое содержит информацию о сотруднике, а также меню выбора операций в системе (рис.10).

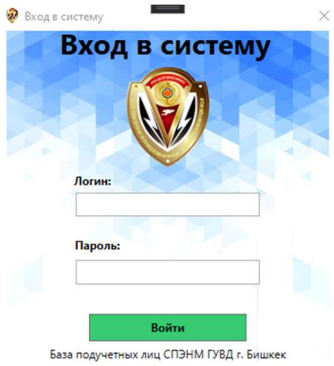

Рис. 9. Окно авторизации приложения

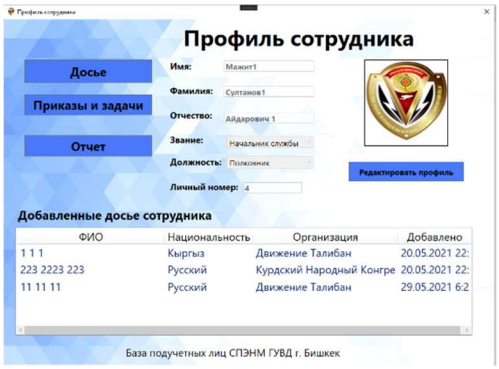

Рис. 10. Профиль сотрудника

Досье подучетных лиц. После нажатия на кнопку «Досье» перед пользователем открывается окно приложения, содержащее список доступных досье для просмотра, редактирования или печати (рис. 11). Нажав ЛКМ (левая кнопка мыши) на доступную запись, сотрудник откроет данное досье.

Просмотр досье. При просмотре досье сотруднику доступна полная информация о подучетном лице. Пользователь может распечатать досье, а также отредактировать информацию (рис. 12).

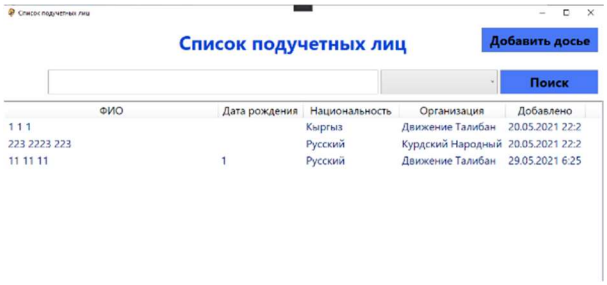

Рис.11. Список досье подучетных лиц

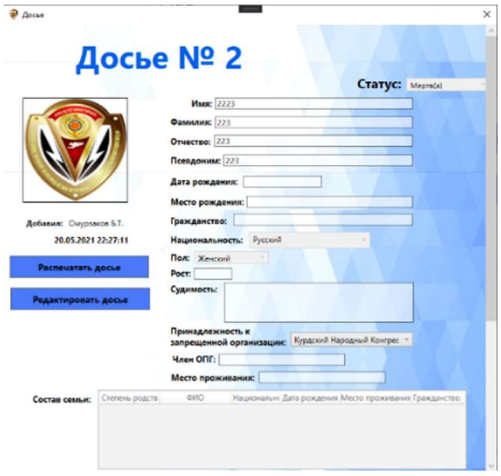

Рис.12. Просмотр досье

Поиск досье. Для поиска соответствующего досье существуют определенные критерии поиска. Выбрав один из них и заполнив поле текста, пользователь может осуществить поиск (рис. 13).

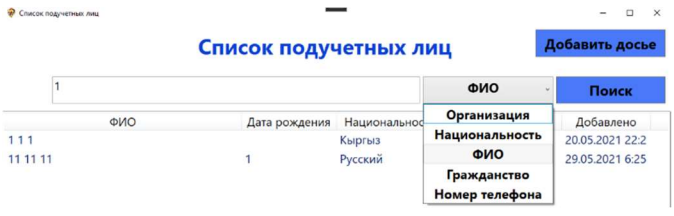

Рис. 13. Поиск досье

Добавление нового досье. Добавление нового досье доступно всем авторизованным сотрудникам в системе. После добавления происходит проверка согласно реализованной технологии блокчейн в системе (рис. 14).

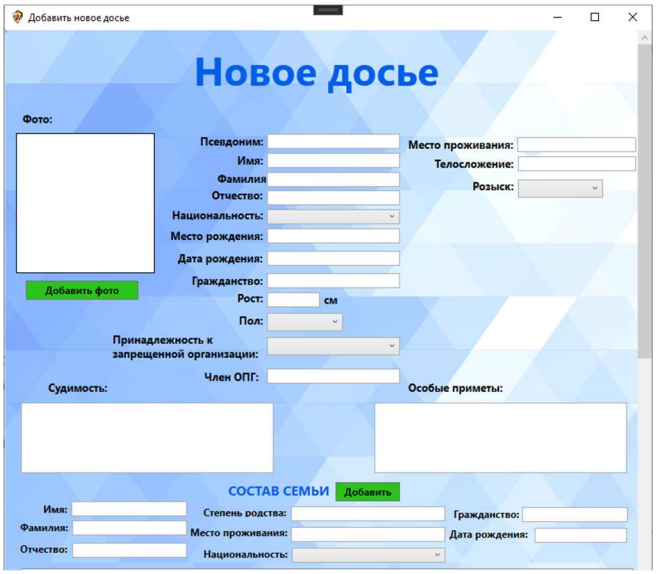

Рис. 14. Добавление нового досье

Запуск сервера. Запуск сервера происходит путем открытия .exe- файла в папке с сервером (рис. 15).

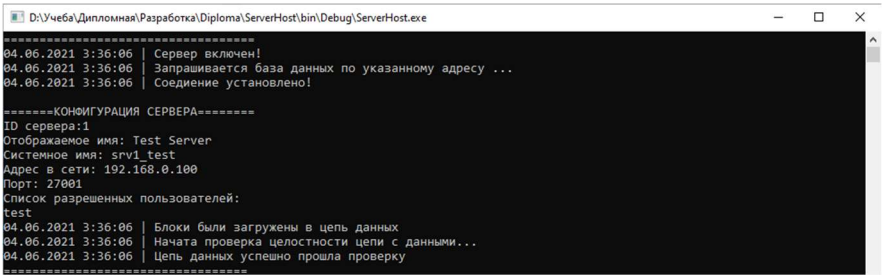

Рис. 15. Информация о запуске сервера

Добавление нового досье в систему. После добавления досье сервер уведомляет об успешном добавлении (рис.16).

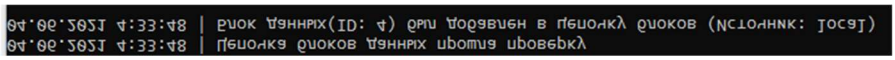

Рис. 16 . Информация о добавлении нового досье в СЭД

Просмотр досье в системе. При просмотре досье сервер проверяет целостность данных досье, если сформированный хэш совпадает с хэшем блока, то досье доступно для просмотра (рис. 17).

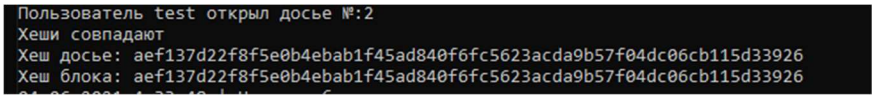

Рис. 17 .Информация о просмотре досье пользователем

Таким образом, хранение данных в блокчейне позволяет обеспечить наличие таких принципов СЭД, как высокий уровень доверия к системе, максимальная защищенность

данных, доступность СЭД для всех участников и временная привязка электронных документов.

Заключение

Для хранения данных была исследована блокчейн-технология, которая в основном используется в финансовом секторе для хранения транзакций. Было проведено исследование возможности адаптировать данную технологию, в частности, метод хранения данных к описанному объекту защиты, а именно системы электронного документооборота для ведения распределенной базы хранения подучетных лиц. Так, были спроектированы диаграммы основного процесса работы системы документооборота. Была разработана политика информационной безопасности. Есть плюс и минусы использования данной технологии. Минус заключается в сложной интеграции блокчейн-технологии в уже работающие бизнес-процессы, отсюда вытекает значительное расходование средств на внедрение. Ещё одним минусом можно назвать не слишком быструю работу блокчейн, так как при подтверждении транзакции необходимо обойти все узлы сети и проверить каждую цепочку блоков. Однако существенное влияние вышеописанный минус технологии на распределенную систему не оказывает, потому что данная СЭД не подразумевает миллионные транзакции, чтобы он стал ощутим. Плюсом является высокая отказоустойчивость, невозможность нарушения целостности информации.

Литература

1. https://www.investopedia.com/terms/b/blockchain.asp (дата обращения: 15.04.2021)
2. Пескова О.Ю., Половко И.Ю., Захарченко А.Д. Применение блокчейн-технологий в системах электронного документооборота: анализ и программная реализация // Инженерный вестник Дона. – №3. –2019. – http://ivdon.ru/ru/magazine/archive/n3y2019/5801
3. Генкин Артем, Михеев Алексей. Блокчейн. Как это работает и что ждет нас завтра. – М.: Альпина Паблишер, 2017. – 592 с.
4. Chris Skinner Value Web // K. Information technologies. – 2016 – С. 150 – 175.
5. Технологии блокчейн: Современное состояние и ключевые инсайты https://www.fips.ru/vse-uslugi/patent-analytics/report-blockchain.pdf (дата обращения: 10.07.2021)
6. Бафанова В.Е, Миленькая Н.В, Сергиенко Н.Л. Применение информационной технологии блокчейн в системе электронного документооборота // Научные труды КубГТУ. – № 3. – 2020. – С. 791 – 798.
7. BlockSigh: How it all works https://blocksign.com/about (дата обращения: 10.07.2021)
8. Федотова В.В., Емельянов Б.Г., Типнер Л.М. Понятие блокчейн и возможности его использования // European science2018. – № 1 (33). – С. 40 – 48.
9. http://nbj.ru/publs/banki-i-biznes/2019/11/26/kompanija-mindsmith-provela-masshtabnoe-issledovanie-otechestvennogo-blokchein-rynka/index.html (дата обращения: 10.07.2021)

http://veteranov.net/content/seti-teoriya/basesecuretyautosystem/42-part2-6 (дата обращения: 03.05.2021)