УДК 004.91

А.Б. Сизоненко, О.М. Булгаков, С.Г. Клюев

МОДЕЛЬ ЗАЩИЩЕННОЙ ПОДСИСТЕМЫ КОНТРОЛЯ ДОКУМЕНТНЫХ СИСТЕМ НА ОСНОВЕ ТЕХНОЛОГИИ «БЛОКЧЕЙН»

Федеральное государственное казенное образовательное учреждение высшего образования «Краснодарский университет Министерства внутренних дел Российской Федерации»

Проанализированы и соотнесены с требованиями обеспечения безопасности характеристики и требования к системам управления документами и подсистемам контроля. Выявлено, что основными требованиями к подсистемам контроля являются: распределение ответственности между исполнителями за их действия, фиксация времени выполнения действия, обеспечение поиска документа, контроль местоположения документа. Проанализированы способы обеспечения безопасности документных систем. Выявлено, что для построения защищенных подсистем контроля документных систем могут быть использованы возможности технологии «блокчейн». Она позволяет обеспечить распределенное хранение регистрационных данных, что снижает вероятность их утраты. Технология «блокчейн» исключает возможность внесения изменений в реестр транзакций, что не позволит отказаться от транзакции. Предложена структура регистрационной записи документа, включающая сведения об идентификационных номерах пользователя, совершаемой операции, хэш-код документа. Хэш-код записи подписывается лицом, совершающим действия в документной системе. Предложена структура блока записей и алгоритм формирования цепочки блоков. Помимо регистрационных записей, каждый блок содержит хэш-код предыдущего блока, поле со случайным числом и подписанный хэш-код текущего блока. Формирование нового блока завершается после добавления случайного числа каждым из пользователей и выработки хэш-кода. Подписывает блок тот пользователь, который выработал хэш-код, удовлетворяющий установленным критериям. Определены направления развития технологии «блокчейн» в документных системах.

Ключевые слова: электронный документооборот, система управления документами, защищенный документооборот, блокчейн.

Введение.

Анализ требований к системам управления электронным документооборотом позволяет утверждать, что в них достаточно большое значение придается вопросам безопасности информации. Традиционно безопасность информации рассматривается в совокупности трех ее составляющих: конфиденциальности, целостности и доступности.

Обеспечение требования доступности заключается в минимизации временных затрат на поиск документов и доступ к ним, т.е. пользователи и администраторы системы электронного документооборота должны знать местонахождение документа в любой момент времени. Дополнительным

требованием является обеспечение невозможности отказа от выполненных действий, что наиболее актуально при организации взаимодействия между организациями и отдельными ведомствами.

Сведения о движении документа содержатся в журналах учета. Этот элемент системы, по нашему мнению, является наиболее критичным, так как его утрата или повреждение приведет к усложнению или невозможности отслеживания пути прохождения и поиску местонахождения документов.

Одним из решений проблемы обеспечения целостности является дублирование информации, а для подтверждения действий используется электронная подпись. Для этих целей предлагается использовать популярную в настоящее время технологию «блокчейн». Распределенное хранение базы транзакций обеспечивает целостность баз и невозможность ее удаления или изменения. Для этого потребуется удалить или модифицировать все экземпляры базы, что затруднительно. Применение электронных подписей для подтверждения транзакций наряду с распределенным хранением позволит обеспечить невозможность отказа от транзакции и доступность электронных документов.

Статья является продолжением серии публикаций авторов, посвященных защищенным системам управления документами [1-3], и в ней будет рассмотрено построение распределенной подсистемы контроля в одноранговой системе управления документами.

Основная часть.

В соответствии с ГОСТ Р ИСО 15489-1-2007 [4] под документной системой или системой управления документами понимается информационная система, обеспечивающая сбор документов (включение документов в систему), управление документами и доступ к ним в течение времени. Рассмотрим требования к документным системам (рисунок 1) в соответствии с [4].

Документные системы должны обеспечивать своевременный и эффективный доступ к документам и поиск документов, необходимых для деловой деятельности и выполнения требований отчетности. Важным требованием к документным системам является способность поддерживать альтернативные варианты размещения документов. В некоторых случаях, если правовая и регулирующая среда позволяют это, документы могут физически храниться в одной организации, а ответственность и контроль управления ими могут возлагаться либо на организацию-создателя, либо на другой полномочный орган [4]. Такой порядок размещения, различающий хранение, владение и ответственность за документы, наиболее подходит для документов в электронных

документных системах. Перемещение документов может происходить в любое время, оно должно быть контролируем и документально оформленным.

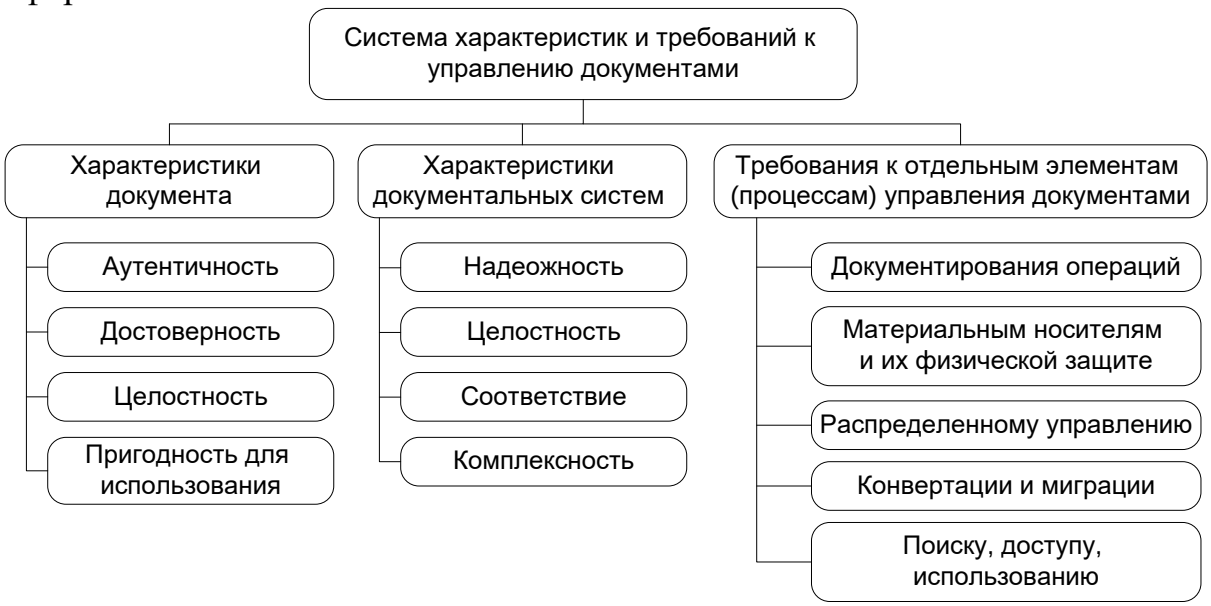

Рисунок 1 – Система требований к документам и документным системам

Документная система должна быть подготовлена к чрезвычайным ситуациям так, чтобы определять и уменьшать риски. Вовремя и после восстановления деятельности организации, пострадавшей от чрезвычайных ситуаций, система должна сохранить свою целостность и продемонстрировать это.

В документных системах непосредственно за создание документа, включение его в систему и сохранение информации о его движении отвечает подсистема контроля (рисунок 2) [4].

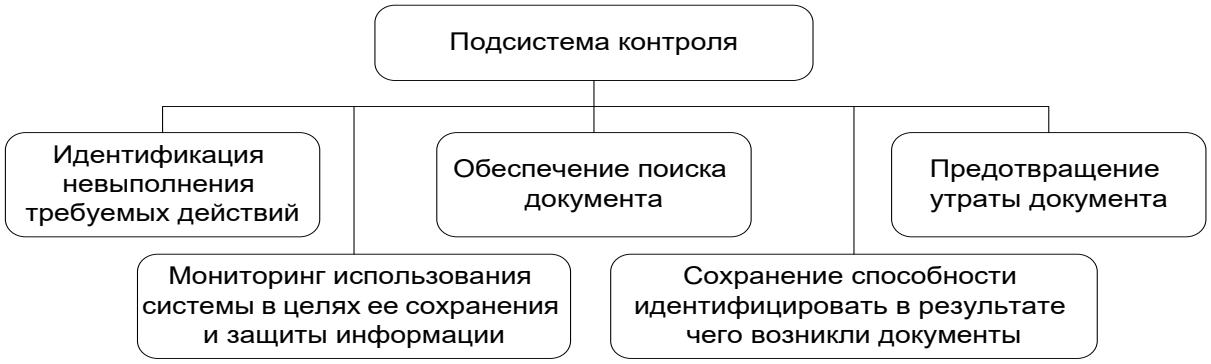

Рисунок 2 – Функции подсистемы контроля документной системы

Контроль действий определяет этапы выполнения решений или операций, зафиксированных в документе, распределяет между

исполнителями ответственность за действия, фиксирует даты предполагаемого и реального выполнения действий [4].

Документальная фиксация движения документов требуется для обеспечения их обнаружения при любой необходимости. Механизмы контроля могут предусматривать фиксацию идентификатора документа, его заголовка, сотрудника или подразделения, обладающего документом, и времени (даты) перемещения документа. Система должна контролировать выдачу, передачу между сотрудниками и возврат документов на место их расположения или хранения, а также их изъятие из документной системы для уничтожения либо передачи другой уполномоченной сторонней организации, в том числе архивным органам для дальнейшего хранения [4].

Среди множества возможных решений рассмотренных проблем и способов выполнения перечисленных требований остановимся на отождествлении операций, произведенных с документом, путем обеспечения достоверности месторасположения документов и идентификации пользователей и совершенных с документом действий.

Существует множество способов решения указанных проблем. Для контроля целостности применяются различные коды, включая помехоустойчивое кодирование и хэширование, создаются резервные копии. Для подтверждения и невозможности отказа от авторства применяют электронные подписи. В настоящее время нашла применения технология «блокчейн» (от англ. block – блок, chain – цепочка). Основным принципом функционирования новой технологии является прозрачность совершаемых операций с невозможностью их изменения лицами, не имеющими к ней санкционированного доступа [5].

Блокчейн является распределенной защищенной базой транзакций без централизованного контролирующего органа, т.е. позволяет автоматизировать транзакции без привлечения третьей стороны, является системой распределенного согласия и доверия, представляет собой инфраструктуру, обеспечивающую подтверждение подлинности. Факт принятия транзакции или отказа от нее является результатом распределенного консенсуса, а не решения централизованного органа [5].

Таким образом, можно сделать вывод, что технология «блокчейн» может быть применена для решения указанных задач.

Во-первых, хранение учетных данных будет происходить распределено, что обеспечивает целостность учетного журнала. Создается большое количество резервных копий. При непреднамеренном или несанкционированном удалении одной или даже нескольких копий учетного журнала, у других пользователей останутся копии. Это значительно снижает вероятность утраты учетных данных.

Во-вторых, обеспечивается доказательства проведения операций и невозможность отказа от операции.

Перейдем к рассмотрению технологии «блокчейн» применительно к документным системам. Предлагается следующая структура регистрационной записи в защищенных распределенных журналах учета для систем управления документами на основе технологии «блокчейн» (рисунок 3).

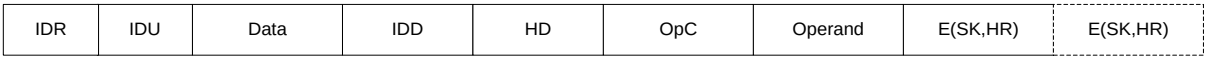

Рисунок 3 – Структур записи блока

На рисунке 3 введены следующие обозначения:
IDR – идентификатор записи.
IDU – идентификатор пользователя.
Data – дата выполнения операции.
IDD – идентификатор документа.
HD – хэш-код документа.
OpC – код операции.
Operand – операнд.
SK – ключ подписи пользователя.
HR – хэш-код записи.
E(SK,HR) – подписанный хэш-код записи.

Формирование записи происходит следующим образом. Поля IDR, IDR, Data, IDD формируются автоматически при регистрации документа. Причем предполагается, что документ имеет в распределенной системе единый идентификационный номе IDD. Помимо самого документа его хэш-код (HD) также вносится в регистрационную запись. Это является дополнительной мерой защиты целостности документа и практически исключит возможность несанкционированного внесения в него изменений.

В поле OpC кодируется технологическое действие, которое выполняется с документом. Им может быть создание, отправка, получение, уничтожение, передача на доклад, исполнение, уничтожение документа. Поле Operand содержит реквизиты, необходимые для однозначного выполнения операции. Например, если выполняется отправка документа, то в поле Operand должно содержать адресата (адресатов), если документ направляется на хранение – ссылка на его местонахождение.

После формирования записей, они группируются в блоки (рисунок 3). Критерии завершения внесения записей в блок определяются

правилами, заданными при разработке распределенной подсистемы контроля, и могут основываться на истечении определенного времени, достижении определенного размера блока или количества записей.

После завершения внесения записей в блок к нему добавляется хэш-код предыдущего блока (H_{n-1}) и рассылается всем пользователям. Каждый пользователь генерирует случайное число и записывает его в поле RND, после этого формирует хэш-код блока (H_n). Тот пользователь, у которого сформированный хэш-код окажется наиболее точно удовлетворяющим установленному критерию (например, минимальный, максимальный или входящий в заданный системой диапазон) подписывает хэш-код блока своей электронной подписью ($E(H_n)$).

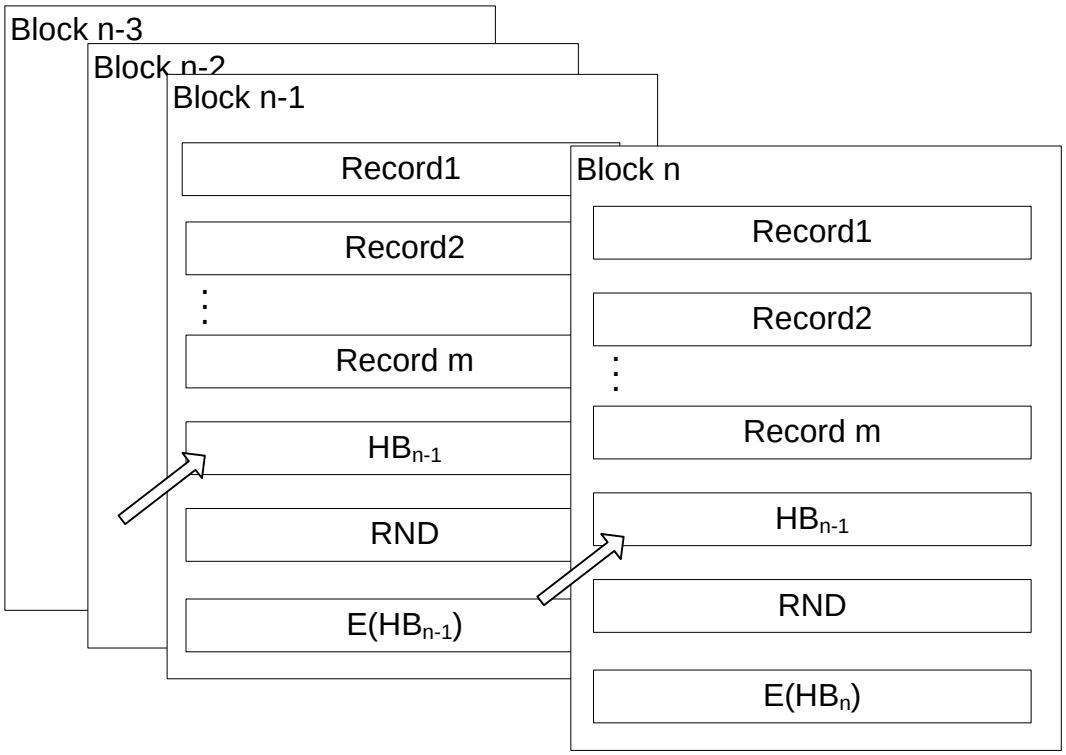

Рисунок 3 – Модель формирования блоков распределенной подсистемы контроля

Таким образом, блок считается сформированным и добавляется в цепочку блоков. Такой механизм, упрощенный по сравнению с «блокчейнами» криптовалют, позволяет решить проблему обеспечения доверия к выполненным операциям, не прибегая к трудоемким вычислениям.

Заключение.

Предложенная модель построения подсистемы контроля документных систем (в том числе предназначенных для обработки документов ограниченного доступа) позволит обеспечить целостность

регистрационных данных и доступность документов, обеспечить юридическую значимость выполняемых действий и невозможность отказа от них. В рамках детализации модели может быть рассмотрена конкретная спецификация записей с кодировкой и форматом представления конкретных операций. Разработанный протокол может быть использован в комбинированных системах документооборота, в которых пересылка документов происходит традиционным способом, а подсистема контроля является электронной. Дальнейшим развитием темы будет являться разработка тестовой подсистемы контроля с использованием открытых «блокчейн» систем.

ЛИТЕРАТУРА

1. Сизоненко, А.Б. Новая форма представления электронных документов / А.Б. Сизоненко, С.Г. Клюев // Спецтехника и связь. – 2014. – №. 2. – С. 60-63.
2. Клюев, С.Г. Вопросы стандартизации форм представления информации ограниченного доступа в системах электронного документооборота / С.Г. Клюев, А.Б. Сизоненко // Моделирование, оптимизация и информационные технологии [Электронный ресурс]. – 2017. – № 3(18). – Режим доступа: http://moit.vivt.ru/wp-content/uploads/2017/08/KluevSizonenko_3_1_17.pdf.
3. Клюев, С.Г. Протокол создания и передачи документов ограниченного доступа в системах электронного документооборота // Моделирование, оптимизация и информационные технологии. Научный журнал – 2017. – №4(19). – Режим доступа: https://moit.vivt.ru/?cat=3745&lang=ru.
4. Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования: ГОСТ Р ИСО 15489-1-2007. – Введ. 12.03.2007 – М.: Стандартинформ, 2017. – 23 с.
5. Лелу, Лоран Блокчейн от А до Я. Все о технологии десятилетия / Лоран Лелу ; [пер с фр. А.Н. Степановой]. – М.: Эксмо, 2018. – 256 с.

A.B. Sizonenko, O.M. Bulgakov, S.G. Klyuev

MODEL OF PROTECTED TRACKING SUBSYSTEM OF RECORDS SYSTEM BASED ON BLOKCHEIN TECHNOLOGY

Federal State Public Educational Establishment of Higher Educaton «Krasnodar University of the Ministry of the Interior of the Russian Federation»

The characteristics and requirements for document management systems and control subsystems have been analyzed and correlated with security requirements. It is revealed that the main requirements for the control subsystems are: the distribution of responsibility between performers for their actions, fixing the time of the action, ensuring the search for a document, monitoring the location of the document. The ways of ensuring the security of document systems are analyzed. It has been revealed that the possibilities of blockchain technology can be used to build protected control subsystems of document systems. It allows for the distributed storage of registration data, which reduces the likelihood of their loss. The blockchain technology excludes the possibility of making changes to the transaction register, which will not allow to refuse the transaction. The structure of the registration record of the document is proposed, including information on the user's identification numbers, the transaction being performed, and the hash code of the document. The hash code of the record is signed by the person performing the actions in the document system. The structure of the block of records and the algorithm for forming the chain of blocks are proposed. In addition to the registration records, each block contains the hash code of the previous block, the random number field, and the signed hash code of the current block. The formation of a new block is completed after adding a random number to each of the users and generating a hash code. The subscriber subscribes the unit, which has developed a hash-code that meets the established criteria. The directions of the development of blockchain technology in document systems are determined.

Keywords: electronic document management, records system, protected workflow, blockchain.

REFERENCES

1. Sizonenko, A.B. Novaya forma predstavleniya e`lektronny`x dokumentov / A.B. Sizonenko, S.G. Klyuev // Specztexnika i svyaz`. – 2014. – No. 2. – pp. 60-63.
2. Klyuev, S.G. Voprosy` standartizacii form predstavleniya informacii ogranichennogo dostupa v sistemax e`lektronnogo dokumentooborota / S.G. Klyuev, A.B. Sizonenko // Modelirovanie, optimizaciya i informacionny`e texnologii [E`lektronny`j resurs]. – 2017. – No. 3(18). – Rezhim dostupa: http://moit.vivt.ru/wp-content/uploads/2017/08/KluevSizonenko_3_1_17.pdf.
3. Klyuev, S.G. Protokol sozdaniya i peredachi dokumentov ogranichennogo dostupa v sistemax e`lektronnogo dokumentooborota // Modelirovanie, optimizaciya i informacionny`e texnologii. Nauchny`j zhurnal – 2017. – No.4(19). – Rezhim dostupa: https://moit.vivt.ru/?cat=3745&lang=ru.
4. Sistema standartov po informacii, bibliotechnomu i izdatel`skomu delu. Upravlenie dokumentami. Obshhie trebovaniya: GOST R ISO 15489-1-2007. – Vved. 12.03.2007 – M.: Standartinform, 2017. – 23 p.
5. Lelu, Loran Blokchejn ot A do Ya. Vse o texnologii desyatiletiya / Loran Lelu ; [per s fr. A.N. Stepanovoj]. – M.: E`ksmo, 2018. – 256 p.