УДК 004.91

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА С ПРИМЕНЕНИЕМ ТЕХНОЛОГИИ БЛОКЧЕЙН

Юмашева Е.В., Юмашев Д.В., Тимонов Д.А.

ФГКВОУ ВО «Краснодарское высшее военное училище имени генерала армии С.М. Штеменко» Министерства обороны РФ, Краснодар, e-mail: umashevaev@mail.ru

В статье рассмотрены актуальные проблемы информационной безопасности в системе электронного документооборота в условиях постоянного информационного противоборства, динамично изменяющейся ИТ-инфраструктуры и ландшафта угроз. Обоснована необходимость повышенного контроля над оборотом документов в целях недопущения их подделки или потери/уничтожения. Для обеспечения безопасного обмена информацией авторами обоснована возможность нивелирования возникающих проблем в контексте применения технологии блокчейн, представляющей собой инновационное решение в управлении данными, их организации и хранения. Особое внимание уделено вопросам выбора алгоритмов консенсуса, которые являются важным элементом платформы распределенного реестра в СЭД, применительно к определенным сферам деятельности. Однако блокчейн-системы не лишены определенных уязвимостей, присущих объекту информатизации. В статье предложена модель оптимизации обработки и хранения информации в контексте информационной безопасности. Мероприятия по противодействию возможных угроз, в частности эффективный выбор алгоритма консенсуса, современных алгоритмов шифрования и хэш-функций, способствуют безопасности и оперативности взаимодействия. Применение защищенного децентрализованного электронного документооборота с использованием платформы распределенного реестра позволит выполнить полный цикл автоматизированного контроля системы, сократить временные затраты на обработку запросов, повысить защищенность данных, обеспечивая живучесть СЭД.

Ключевые слова: система электронного документооборота, угроза информационной безопасности, алгоритм консенсуса, уязвимость, валидация

INFORMATION SECURITY IN ELECTRONIC DOCUMENT FLOW SYSTEMS USING BLOCKCHAIN TECHNOLOGY

Yumasheva E.V., Yumashev D.V., Timonov D.A.

Krasnodar Higher Military Red Banner School named after General of the Army S.M. Shtemenko, Krasnodar, e-mail: umashevaev@mail.ru

The article deals with the current problems of information security in the electronic document management system in the context of constant information confrontation, dynamically changing IT infrastructure and threat landscape. The necessity of increased control over the circulation of documents in order to prevent their forgery or loss / destruction has been substantiated. To ensure the safe exchange of information, the authors proved the possibility of leveling the emerging problems in the context of using the distributed ledger technology, which is an innovative solution in data management, organization and storage. Particular attention is paid to the issues of choosing consensus algorithms in relation to certain areas of activity, which are an important element of the distributed ledger platform in the electronic document management system. However, blockchain systems are not devoid of certain vulnerabilities inherent in the object of informatization. The article proposes a model for neutralizing the threats of consensus algorithms. Skillful use of measures to counter possible threats, in particular, the effective choice of the consensus algorithm, modern encryption algorithms and hash functions allows ensuring the security and efficiency of interaction between the relevant authorities of the Russian Federation. The use of decentralized electronic document management on the platform provides a complete automated control system, reduces the time spent on processing requests, increases the security of data in the system, and ensures the survivability of the EDMS.

Keywords: electronic document management system, information security threat, consensus algorithm, vulnerability, validation

Внедрение системы электронного документооборота (СЭД) обладает рядом преимуществ, позволяющих оптимизировать обработку и хранение информации. Однако ее использование в настоящее время, несмотря на обеспечение необходимыми каналами связи и информационной инфраструктурой, сталкивается с рядом проблем, среди которых можно выделить несанкционированный доступ к информации, приводящий в том числе к утрате сведений, составляющих государственную тайну. Применение системы электронного документооборота с использованием блокчейн-технологии позволит минимизировать существующие уязвимости и повысить контроль над оборотом документов.

Цель исследования: изучить особенности и специфику системы электронного документооборота, выявить основные проблемы и разработать эффективную модель оптимизации обработки и хранения информации в контексте информационной безопасности.

Материалы и методы исследования

Объект исследования – система электронного документооборота. В ходе иссле-

дования применялись методы анализа, синтеза, аналогий, обобщения.

Результаты исследования и их обсуждение

Защита системы электронного документооборота должна обеспечиваться на всех ее уровнях, включая аппаратные элементы системы, файлы системы, информацию, находящуюся внутри системы, в частности документы. В этом контексте важное место отводится организационным мерам, обеспечивающим порядок доступа к СЭД. Защищенный документооборот в определенных сферах деятельности предусматривает защиту системы в целом, в том числе информации, обеспечивая ее работоспособность, а в случае повреждений, сбоев и уничтожения – быстрое восстановление.

В СЭД обеспечиваются механизмы защиты от основных угроз: нарушение сохранности документов, безопасного доступа, подлинности документов, протоколирование действия пользователей. Основные причины потерь важной информации согласно статистике, приведенной в Cnews Analytics, представлены на рис. 1 [1].

Рис. 1. Причины потерь информации

В настоящее время существует более 100 разновидностей угроз. Угрозы информационной безопасности проявляются при воздействии на слабые элементы системы защиты, то есть через факторы уязвимости, которые возникают на любом участке архитектуры автоматизированной системы (АС). Уязвимости объекта информатизации могут быть вызваны недостатками процесса функционирования, архитектурой автоматизированных систем, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой и др.

Для нивелирования этих процессов необходима полная оценка уязвимостей, позволяющая грамотно выстроить систему защиты от угроз в информационном пространстве и сформировать рекомендации по корректировке структурно-функциональных характеристик СЭД, обеспечивающих их нейтрализацию. Модель угроз безопасности информации включает описание АС и угроз безопасности информации в контексте их структуры, модель нарушителя, возможные уязвимости, алгоритм реализации угроз безопасности информации и их последствия, штатный режим функционирования АС.

Решение вопросов информационной безопасности, в том числе технических и организационных, возможно на основе блокчейн-технологий. Платформы распределенного реестра позволяют нивелировать классические недостатки документооборота (возможность подделки или потери/уничтожения) и сохранить неизменность, прозрачность и распределенное хранение данных.

Технологии блокчейн представляют собой инновационные решения в управлении данными, их организации и хранения, обеспечивая:

– доступ каждого участника системы блокчейн ко всей информации;

– возможность разработки новых процессов, используя доступную актуальную информацию, мгновенное проведение транзакций и автопродление смарт-контрактов с определенными в реестре логическими условиями;

– формирование блоков, встраивающихся в глобальную систему блокчейн на основе транзакций, которые подлежат проверке любым независимым участником реплицированной распределенной базы данных [2].

К основным преимуществам технологии распределенного реестра можно отнести:

– отсутствие централизованного управления и посредников. Блокчейн в цифровой форме в режиме реального времени обеспечивает доступность каждому пользователю и участнику одноранговой сети копий всех записей;

– снижение риска возникновения ошибок. Достижение консенсуса в блокчейн осуществляется множеством участников сети на основе аутентификации и проверки каждого нового блока при согласии большинства о его допустимости;

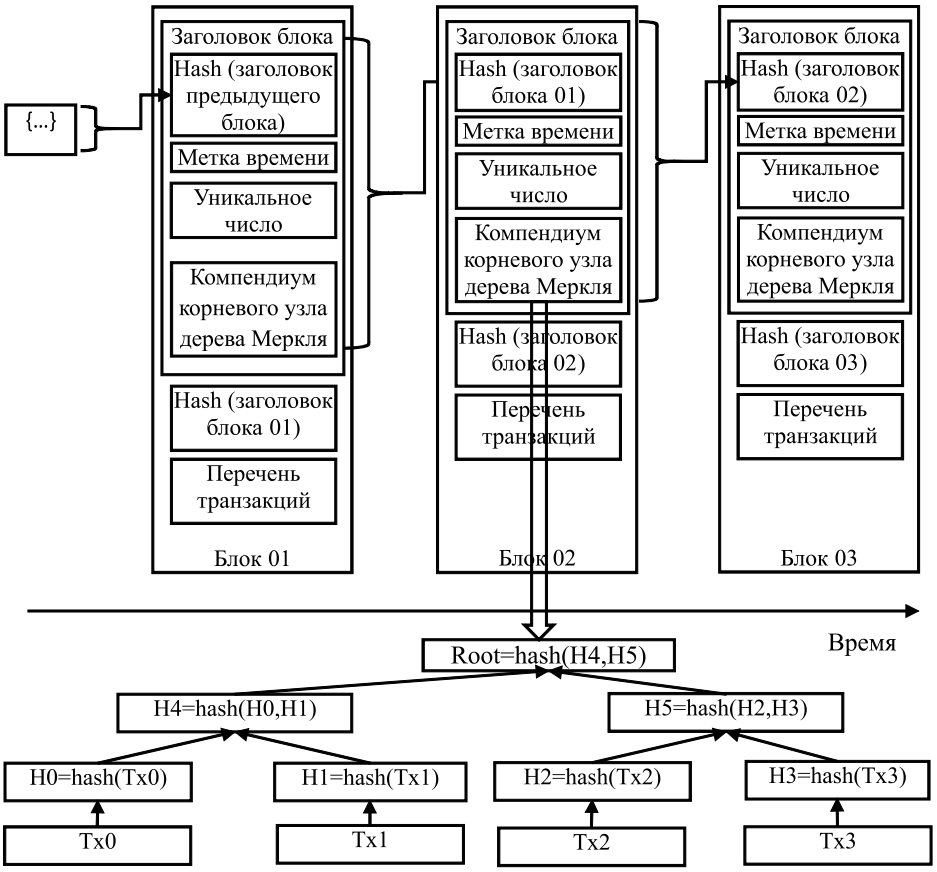

Рис. 2. Блокчейн-система на основе «дерева Меркля»

– применение новых методов шифрования, обеспечивающих безопасность и анонимность конфиденциальных данных в среде общего доступа. В блокчейн используется криптография электронной подписи (ЭП) для идентификации личности;

– отсутствие возможности подделки и изменения документов. Использование инструментов технологии блокчейн не позволяет изменить хронологические сведения, транзакция включает добавление метки времени, что позволяет отследить и проверить информацию. Внесенные данные не подлежат корректировке, за исключением случаев, когда больше 50% участников договорятся о необходимости изменения информации.

Блокчейн-система на основе «дерева Меркля» представлена на рис. 2 [3].

Безопасное и эффективное функционирование электронных систем при применении блокчейн-решений, использующих средства криптографической защиты информации, формируется в процессе их разработки и последующей сертификации или аттестации, находящихся в ведении ФСБ, ФСТЭК. Для определения класса средств криптографической защиты информации проводится оценка возможных угроз безопасности и на основе рекомендаций по стандартизации Р 1323565.1.012–2017 [4] строится модель угроз.

Важным преимуществом блокчейн-технологии является достижение консенсуса, представляющего собой механизм соглашения между всеми участниками сети относительно каждого блока данных, добавляемого в блокчейн. Алгоритмы консенсуса способствуют сохранению целостности и безопасности распределенных систем, предвидя возможные сбои в коммуникации внутри сети. В этой связи алгоритм должен быть отказоустойчивым, чтобы противостоять этому, и работать по заранее определенному консенсусу или одобрению по крайней мере от большинства машин в сети [5].

В силу специфики СЭД в некоторых структурах возможно применение определенных алгоритмов консенсуса. Алгоритм Proof-of-Authority (PoA) – доказательство полномочий – выбирает ограниченное количество узлов, отвечающих

за проверку транзакций по строгим правилам, и обеспечивает безопасность сети через достижение согласия между установленными узлами. Возможность формирования узлом очередной транзакции зависит от его авторитетности. Валидаторы подтверждают свою надежность, проходя необходимые проверки. Принцип работы заключается в следующем: в блокчейн записываются по порядку появления блоки, регламентированные по размеру и состоящие из транзакций. Узлы-валидаторы проводят транзакции и записывают их в блоки. Узлы-администраторы формируют только транзакции и вносят данные в блокчейн, освобождая процесс от сложных вычислений. Узлы сети синхронизируются между собой для проверки каждой транзакции, с целью исключения недействительных. Валидирующие узлы вправе остановить определенные транзакции, приводящие к конфликтам интересов и даже ставящие под угрозу безопасность сети. Проведение постоянного контроля и мониторинга обоснованности операций в условиях недоверия, а иногда и конфликтных ситуаций между субъектами контролирующих узлов, обеспечивает стабильность системы. Алгоритм исключает дискредитацию, так как в случае злонамеренных действий узла его владелец будет наказан в соответствии с законодательством. Действия злоумышленников исключаются в связи с верификацией владельцев узлов для полноценной работы. Вместе с тем алгоритм предусматривает некую централизацию в сети, что уместно в работе некоторых структур. Алгоритм консенсуса имеет ряд преимуществ, позволяющих нивелировать недостатки блокчейн-технологии (таблица).

Блокчейн, основанный на доказательстве полномочий, в настоящее время остается надежным решением многих проблем.

Каждый блокчейн состоит из узлов, включенных в сеть, которые согласованно контролируют и перемещают данные в сети. Выполняемая одним узлом операция в целях достижения консенсуса сети согласовывается с остальными узлами. После этого данные записываются в электронный реестр, копия которого хранится у каждого узла. Протокол взаимодействия узлов, обеспечивая логику работы всей сети, позволяет выявлять потенциальные угрозы, обусловленные случайными ошибками и целенаправленными атаками, что особенно актуально для СЭД в силовых структурах.

Задачу выбора стратегии в условиях получения сообщений от разных участников, часть из которых могут быть злоумышленниками, решает алгоритм консенсуса Byzantine Fault Tolerance (BFT) – византийская отказоустойчивость. Узлы обмениваются между собой сообщениями по валидности транзакции, решая задачу византийских генералов, данные попадают в цепь при достижении консенсуса. Запечатывание транзакций в блок происходит только после их подтверждения без возможности изменения правил, по которым блок в блокчейне признается подлинным. Алгоритм позволяет прийти к консенсусу между устройствами в случае проблемных узлов в сети (передача неверной информации или некоторые из них не отвечают). С помощью алгоритма консенсуса BFT возможно предотвращение распространения ошибок и неверной информации, отправляемой вредоносными или поврежденными узлами. В случае отсутствия алгоритма одноранговый узел способен передавать и публиковать ложные транзакции, ставя под угрозу надежность блокчейна, децентрализация которого не позволяет исправить нанесенный ущерб.

Консенсус-алгоритм применим в небольших сетях с сокращением децентрализации (участники известны с момента создания сети), что позволяет достичь увеличения скорости проверки транзакций в 10 раз. Блок подписывается при условии, что 1/3 участников терпят неудачу или действуют злонамеренно. Алгоритм BFT позволяет нивелировать сбои в системе и задержки в коммуникации.

Возможности и опасности алгоритма консенсуса Proof-of-Authority

Возможности алгоритма	Опасности алгоритма
Отсутствие возможности проведения атаки ввиду строгой проверки валидаторов при получении ими полномочий и их надежности	Отказ от децентрализации, так как в валидации блоков принимает участие ограниченное количество субъектов
Значительное сокращение потребляемой энергии	Алгоритм более применим как решение для частных сетей, а не публичных блокчейнов
Увеличение скорости проверки транзакции, снижение стоимости проведения операций, возможности горизонтального масштабирования, объединяя несколько сетей в одну	Допустимы мошеннические манипуляции со стороны третьих лиц ввиду знания личности валидатора

В настоящее время отсутствует идеальный механизм консенсуса. Применяемые в блокчейне алгоритмы обладают как преимуществами, так и недостатками. Консенсусный механизм Proof-of-Authority жертвует децентрализацией в пользу высокой пропускной способности и масштабируемости. Алгоритм консенсуса Byzantine Fault Tolerance способен предотвращать распространение ошибок и неверной информации, которые ставят под угрозу надежность блокчейна, в то же время применим в большей степени для частных блокчейн-приложений. Алгоритмы консенсуса Byzantine Fault Tolerance и Proof-of-Authority по своим принципам и сущности являются наиболее удачными для применения в СЭД в определенных структурах, позволяя учесть их специфику.

Вместе с тем следует обратить особое внимание на уязвимости, связанные с реализацией алгоритма консенсуса**,** которые можно отнести к фундаментальным, так как легитимность новых блоков зависит от эффективности алгоритма и его устойчивости к возможным угрозам.

Большое значение в СЭД отводится эффективности функционирования инфраструктуры. Автоматизированный контроль инфраструктуры системы электронного документооборота на основе технологии распределенных реестров осуществляется в следующей последовательности:

– генерация уникального цифрового отпечатка для каждого регистрируемого электронного документа;

– проверка проекта электронного документа (ЭД) узлом делопроизводства;

– сохранение проекта электронного документа с соответствующей ему электронной подписью как регистрируемый ЭД;

– проведение транзакции запроса смарт-контракта абонента-подписанта с удостоверяющим центром с целью получения сведений о текущем статусе сертификата проверки ключа электронной подписи (ЭП) абонента-подписанта;

– формирование транзакции запроса на регистрацию ЭД в делопроизводстве после согласования проекта;

– обеспечение автоматической проверки ключа ЭП абонента-подписанта на каждом активном узле в СЭД с кодом положительного ответа о значении текущего статуса сертификата проверки ключа электронной подписи, или с кодом ошибки, реплицируемой всеми узлами в СЭД с указанием времени ее записи после проверки на корректность;

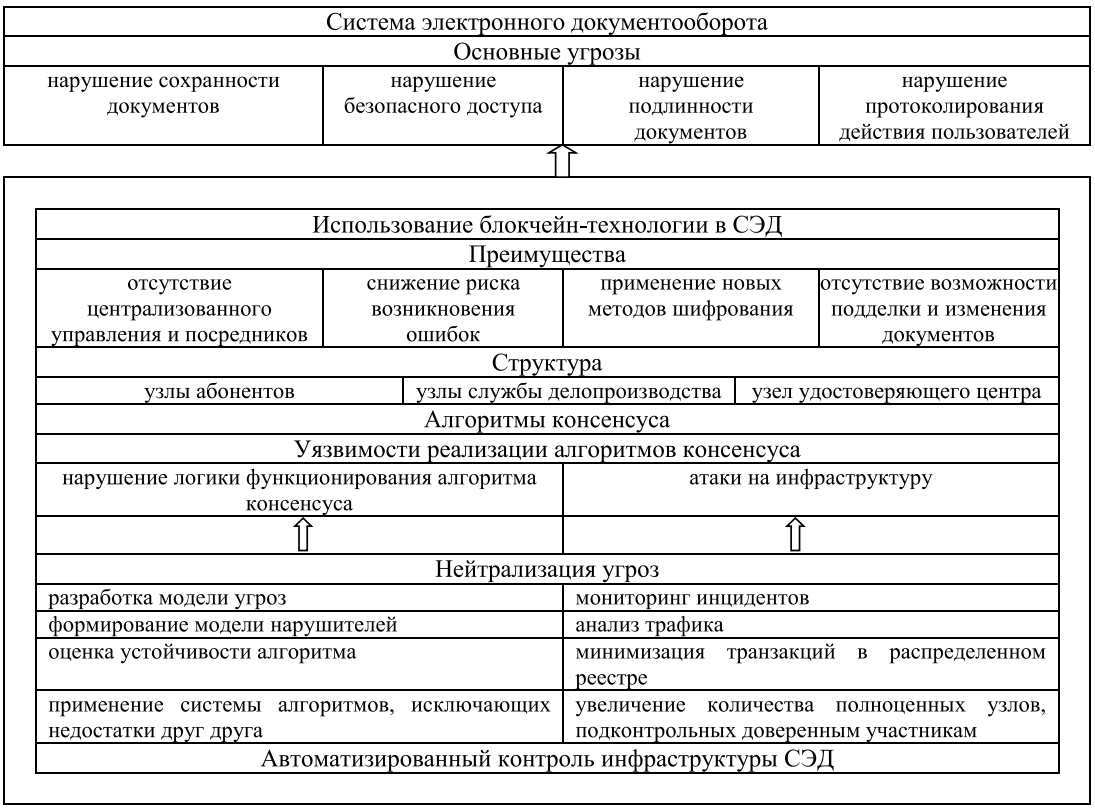

Рис. 3. Модель нейтрализации угроз информационной безопасности в СЭД

– формирование транзакции ответа о регистрации ЭД с кодом транзакции запроса, кодом положительного ответа о принятии проекта или с кодом ошибки, кодом статуса сертификата проверки ключа ЭП;

– фиксация в случае подписания проекта ЭД несколькими подписантами электронной подписи каждого подписанта в соответствующей транзакции ответа;

– проверка смарт-контрактом абонента с делопроизводством транзакции ответа о текущем статусе сертификата проверки ключа ЭП после положительного кода ответа о регистрации проекта ЭД, и формирование в случае «действительного» кода статуса транзакции ответа о регистрации ЭД в делопроизводстве;

– вычисление абонентом-получателем для проверки подлинности ЭП хэш-кода ЭД и поиск на его основе по соответствующей транзакции хэш-кода цифрового отпечатка ЭД. После нахождения осуществляется проверка ЭД на его подлинность и на предмет корректности используемого ключа проверки ЭП;

– проверка факта регистрации ЭД в делопроизводстве абонентом-получателем. При положительном результате проверки он делает вывод о подлинности ЭП.

Таким образом, проверяющий абонент в СЭД блокчейн получает подтверждение в технической и юридической целостности ЭД.

Модель нейтрализации угроз информационной безопасности в СЭД представлена на рис. 3.

Выводы

Применение защищенного децентрализованного электронного документооборота на платформе блокчейн имеет огромный потенциал использования в современном информационном мире, в особенности в определенных областях деятельности. Стоит помнить, что большую роль во внедрении этой технологии играют именно нюансы ее построения. Эффективная архитектура и применение определенных алгоритмов консенсуса позволит значительно повысить информационную безопасность СЭД.

Список литературы

1. Cnews Analytics Обзоры и рейтинги [Электронный ресурс]. URL: ИТ-рынка https://www.cnews.ru/reviews/free/ (дата обращения: 11.01.2021).

2. Крячко А.А. Актуальные возможности применения технологий распределенного реестра для защиты СЭД в рамках муниципального управления // Международный научно-технический журнал «Теория. Практика. Инновации». 2018. № 5 (29). С. 12–21.

3. Будзко В.И., Мельников Д.А. Информационная безопасность и блокчейн // Системы высокой доступности. 2018. № 3. Т. 14. С. 5–12.

4. Рекомендации по стандартизации Р 1323565.1.012-2017 Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации [Электронный ресурс]. URL: https://meganorm.ru/Data2/1/4293739/4293739817.pdf (дата обращения: 11.01.2021).

5. Мурзин П.Е. Основные подходы к разработке протокола консенсуса в распределенных реестрах // Вестник современных цифровых технологий. 2019. № 1. С. 26–36.