УДК 004.75

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И ЦЕЛОСТНОСТИ СЕТИ ИНТЕРНЕТ ВЕЩЕЙ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ БЛОКЧЕЙН

Лазута Л.С., аспирант,

Белорусская государственная академия связи
г. Минск, Республика Беларусь

Карпук А.А. – канд. техн. наук

Аннотация. Осуществлен анализ методов обеспечения безопасности и целостности сети Интернет вещей с использованием технологии блокчейн. Основное внимание уделено ключевым аспектам блокчейна, таким как децентрализация, неизменяемость и прозрачность данных, которые способствуют повышению безопасности данных в сетях IoT. Особое внимание уделено необходимости разработки и внедрения эффективных механизмов консенсуса и умных контрактов для обеспечения безопасности, управления и сохранения целостности данных.

Сеть Интернет вещей (Internet of Things, IoT) [1] определяется как глобальная инфраструктура для информационного общества, обеспечивающая продвинутое взаимодействие между физическими и виртуальными объектами через использование информационных и коммуникационных технологий. Концепция IoT [2] включает в себя широкий спектр устройств, от бытовых приборов до сложных промышленных инструментов, которые собирают, обмениваются и обрабатывают данные в реальном времени. Эти устройства оснащены датчиками и актуаторами и связаны через сетевые технологии, позволяющие им действовать автономно и кооперативно для достижения общих задач и улучшения качества жизни и операционной эффективности.

Эти понятия формируют фундамент, на котором строится архитектура Интернета вещей, обеспечивая его функциональность, масштабируемость и безопасность. Поскольку системы IoT включают множество устройств, обменивающихся данными и выполняющих различные функции, они сталкиваются с серьезными проблемами безопасности и целостности данных [3]. Неизбежные сбои программного и аппаратного обеспечения,

несанкционированный доступ и атаки вредоносного ПО делают системы уязвимыми. Для решения этих проблем применяются механизмы защиты, направленные на обнаружение и нейтрализацию угроз, а также восстановление системы после инцидентов. Однако, учитывая объем и разнообразие данных, обрабатываемых устройствами IoT, существующие методы часто оказываются недостаточными для обеспечения адекватной защиты [4]. Это требует внедрения более продвинутых технологий, таких как блокчейн, которые могут предложить дополнительные уровни защиты благодаря своим свойствам децентрализации и неизменяемости данных. Таким образом, для повышения безопасности и устойчивости систем IoT необходимо использовать комплексные и интеллектуальные подходы, включающие современные методы машинного обучения для анализа и обработки данных, собираемых с разнообразных устройств.

Технология блокчейн предлагает ряд методов для повышения безопасности и целостности данных в сетях IoT. Во-первых, система аутентификации устройств IoT на базе блокчейна позволяет надежно верифицировать каждое устройство в сети, используя децентрализованный и неизменяемый реестр, что значительно снижает риск несанкционированного доступа. Во-вторых, система отслеживания состояния устройств IoT обеспечивает постоянный мониторинг и запись всех изменений состояний устройств в блокчейн, что упрощает процесс обнаружения аномалий и неисправностей в режиме реального времени. Третий метод, система управления доступом к данным IoT, использует блокчейн для контроля и регулирования доступа к данным, предоставляя устойчивую к взлому платформу для хранения и обмена данными.

Авторизация представляет собой передовой метод обеспечения контроля доступа к ресурсам и управления ими [5]. Этот метод использует уникальные свойства блокчейна, такие как децентрализация, неизменяемость и прозрачность, для создания надежной системы авторизации. В блокчейне каждое устройство IoT может иметь уникальный идентификатор, ассоциированный с соответствующими ключами доступа, что позволяет точно контролировать и верифицировать права доступа без необходимости центрального управляющего узла [6].

При использовании блокчейна для авторизации, все запросы на доступ и изменения прав доступа записываются в надежный и немодифицируемый реестр, что обеспечивает полную прозрачность и отслеживаемость всех операций. Такой подход значительно усложняет несанкционированное изменение или удаление прав доступа, поскольку любые изменения в блокчейне требуют консенсуса между участниками сети. Этот метод также обеспечивает высокий уровень безопасности, поскольку изменение данных в блокчейне требует согласия большинства участников сети, что снижает риск возможных атак или мошенничества. Благодаря использованию уникальных идентификаторов устройств IoT, связанных с соответствующими ключами доступа, система обеспечивает точную верификацию прав доступа, что повышает безопасность и управляемость доступа к ресурсам.

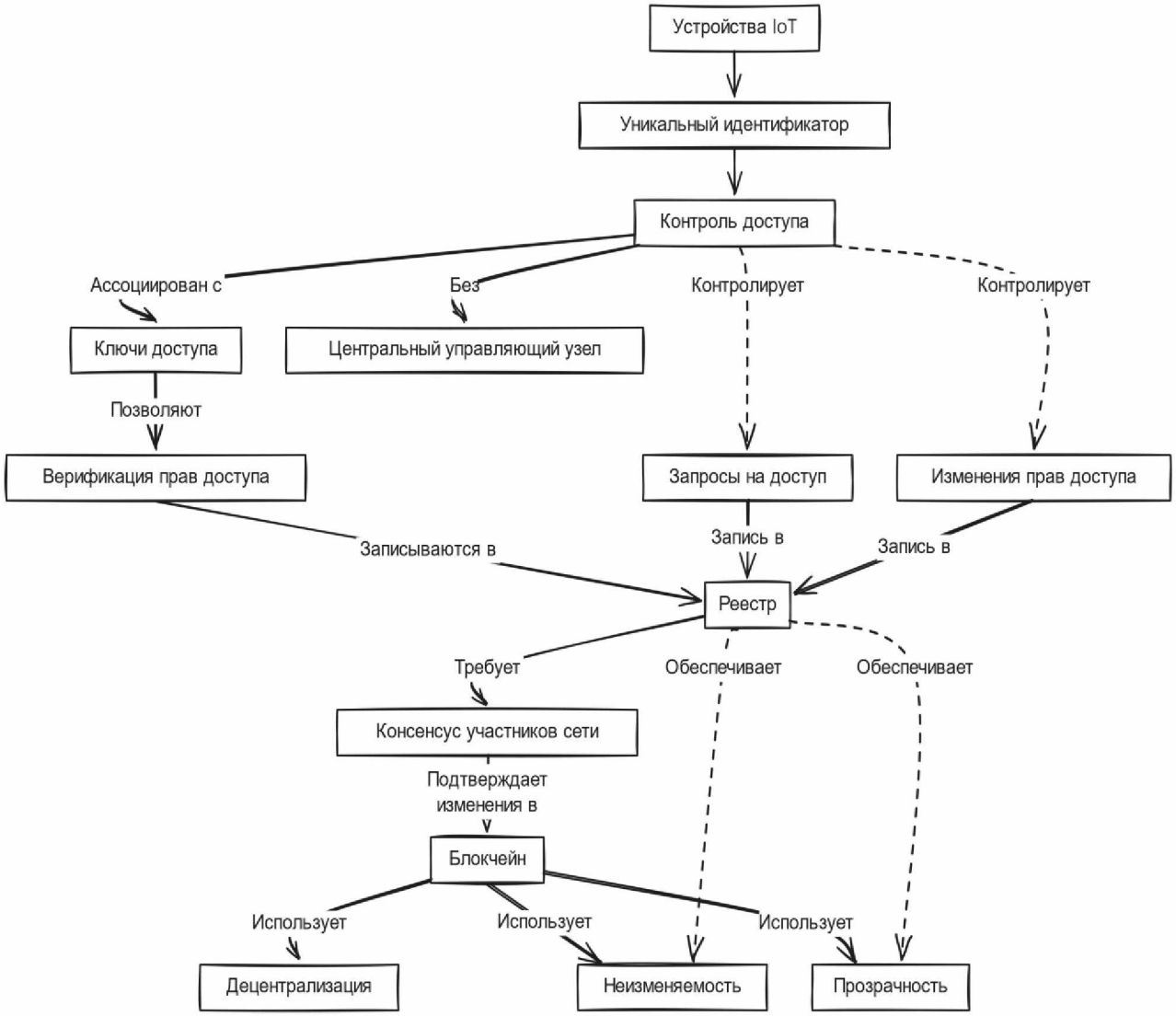

Рисунок 1 – Авторизации на основе блокчейна для управления доступом устройств IoT

Мониторинг и обновление систем в рамках IoT являются критически важными процессами для поддержания безопасности, стабильности и функциональности устройств. Эти процессы включают сбор и анализ данных о состоянии устройств, что позволяет оперативно выявлять неисправности или уязвимости. Системы мониторинга должны обеспечивать непрерывное слежение за параметрами работы устройств, такими как использование памяти, загрузка процессора, температура и сетевая активность. Данные, собранные в процессе мониторинга, анализируются для определения отклонений от нормы, которые могут указывать на возможные сбои или попытки безопасностных нарушений. Процесс обновления включает разработку и распространение патчей или новых версий программного обеспечения, что обеспечивает исправление обнаруженных уязвимостей и добавление новых функций. Обновления должны распространяться автоматизированно и безопасно, чтобы минимизировать перерывы в работе и предотвратить возможность внедрения вредоносного кода в процессе их установки. Важно, чтобы процедуры мониторинга и обновления были интегрированы в единую систему управления, что позволяет обеспечить централизованное контролирование и управление всеми аспектами работы устройств IoT.

Список использованных источников:

1. Aliu, O.G. "A Survey Of self Organisation in Future Cellular Networks." IEEE Communications Surveys Tutorials. Vol. 15. 2013. P. 336-361.

2/ Klaine P.V. "A Survey of Machine Learning Techniques Applied to Self-Organizing Cellular Networks." IEEE Communications Surveys Tutorials. Vol. 19, no. 4. 2017. P. 2392–2431.

3. Аверченко, И.Б. "Блокчейн технологии в индустрии интернета вещей." Гарвардское бизнес-ревью. 2017. № 3. С. 45-49.

4. Джонсон, Д. "Блокчейн технологии для интернета вещей." IoT Solutions World Congress. 2016.

5. Дориан, Н. "Blockchain: Blueprint for a New Economy." Sebastopol: O'Reilly Media, 2015. 152 p.

6. Бутерин, В.Э. "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform." GitHub. 2014.