

Анализ применимости и защищенности технологии блокчейна в беспроводных сенсорных сетях

В. А. Десницкий

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

desnitsky@comsec.spb.ru

Аннотация. Работа посвящена изучению возможностей и защищенности технологии блокчейна в применении к беспроводным сенсорным сетям (БСС), играющим важную роль в структуре современных промышленных киберфизических систем. В настоящее время наблюдается рост интереса к исследованию и внедрению блокчейна в различных БСС — как в научных исследованиях, так и в индустриальных приложениях. По мере развития БСС, характеризующихся расширением функций самоорганизации и децентрализации, сети становятся всё более восприимчивыми к комплексным атакам различного характера, использующим недостатки сетевых протоколов и программного обеспечения БСС, включая механизмы самоорганизации и децентрализации сети. Цель настоящего исследования заключается в анализе наиболее перспективных способов применения блокчейна в БСС, выявлении ключевых особенностей таких решений и вопросов их защищенности.

Ключевые слова: беспроводные сенсорные сети, блокчейн, безопасность, атаки, моделирование

I. ВВЕДЕНИЕ

В настоящее время технологии блокчейна получают все большее развитие и распространение в целях повышения защищенности, надежности и отказоустойчивости информационных систем и сетей. В [1] отмечаются такие основные преимущества использования блокчейна как улучшение процессов управления и усиление безопасности инфраструктуры. Также к наиболее распространенным направлениям, в рамках которых применяют блокчейн, относится получение следующих.

- Обеспечение неизменности данных в рамках распределенного хранилища за счет применения криптографических методов (стойких к коллизии хеш-функций) и выстраивания цепочек взаимосвязанных блоков, где несанкционированное изменение одного блока по цепочке затронуло бы и оставшиеся блоки [1]. Это способствует повышению стойкости хранимых данных к модификациям.
- Возможность согласованного добавления данных в блокчейн только при условии согласия со стороны других участников блокчейна (механизм консенсуса).
- Возможность внедрения распределенных механизмов хранения и управления данными, обладающих потенциально не меньшей степенью

защищенности чем соответствующие им аналогичные централизованные системы.

- Возможность повышения прозрачности хранилища данных в сети за счет их структуризации в виде блоков и наличия меток, определяющих время создания каждого из блоков. Также в качестве положительного побочного эффекта можно отнести потенциальное снижение затрат ресурсов за счет децентрализации с возможностью гибкого управления данными.

Самоорганизация беспроводной сенсорной сети предполагает возможность самонастройки и оптимизации сети с минимальным вовлечением оператора БСС и конечных пользователей. При этом узлы БСС способны в автономном режиме выстраивать локально оптимальные маршруты для уменьшения коммуникационных задержек, увеличения скорости передачи данных, снижения энергопотребления и др. [2]. Кроме того в соответствии с правилами самоорганизации БСС состав узлов сети может меняться динамически, в зависимости от их доступности, физического расположения и сетевых настроек. В частности, в процессе выполнения сеть способна адаптироваться как к запланированным изменениям сетевой топологии, так и к выходу из строя или потере доступности части узлов БСС.

Децентрализация БСС предполагает минимизацию роли какого-либо единого центра в общем объеме функций управления сетью, включающих функции совместной обработки и передачи данных, а также функции взаимодействия узлов [3]. При этом в рамках децентрализованного функционирования узел или группа соседних узлов способны самостоятельно принимать определенную часть решений относительно выполняемых задач. Кроме того, в зависимости от глобальных потребностей и ограничений сети, каждый узел в зависимости от текущей оперативной обстановки может выполнять ту или иную роль, как например, роль обработки данных определенного вида, после чего с течением времени передать эту роль некоторому другому узлу. Все это придает сети дополнительные возможности по повышенной надежности и отказоустойчивости.

Настоящая работа ведется на стыке проблематики безопасности беспроводных сетей и технологии блокчейна, активно развивающейся в настоящее время. При этом к отличительным особенностям анализа, проводимого в данной работе, можно отнести совместный учет самоорганизующегося и децентрализованного характера БСС, с одной стороны, и

децентрализованного характера частных распределенных реестров, узлы которых располагаются на устройствах БСС, с другой стороны, что к настоящему моменту освещается в существующей открытой научно-технической литературе в недостаточной степени. В частности, к элементам новизны работы можно отнести анализ актуальных видов атак, специфичных такому виду сетей на примере систем взаимосвязанных БПЛА, анализ их выполнимости, критичности и последствий для инфраструктуры БСС.

Оставшаяся часть статьи организована следующим образом. В разделе 2 приведены результаты проведенного анализа существующих подходов и методов по использованию технологии блокчейна в качестве расширения функциональности и защищенности современных БСС. Раздел 3 представляет дискуссию о применимости наиболее важных подходов и методов. Кроме того в разделе 3 проведен анализ возможных актуальных атак на такие сети, и сформулированы основные выводы. Раздел 4 включает краткое резюме основных результатов статьи и планы дальнейших исследований по данному направлению.

II. АНАЛИЗ ПОДХОДОВ И МЕТОДОВ

В [4] блокчейн рассматривается в качестве механизма, обеспечивающего операции с данными (транзакции) в беспроводной сенсорной сети, что нацелено на предотвращение кибератак в таких сетях. На рис. 1 схематично приведены основные возможные направления применения блокчейна для совершенствования процессов функционирования БСС, к которым относятся указанные семь основных целей, охватывающих отслеживание корректности и аутентификацию узлов, обеспечение их анонимности, обеспечение скрытности и целостности данных, а также повышение безопасности и надежности узлов.

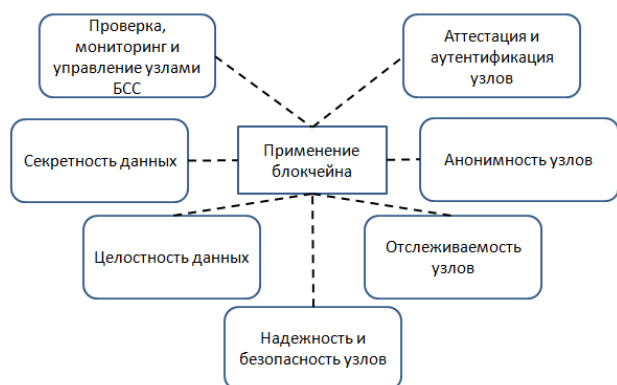


Рис. 1. Направления применения блокчейна в БСС

Отметим, что тогда как в рамках традиционных подходов к аутентификации в БСС полагаются на доверенные третьи стороны, что представляет возможную единую точку отказа, в [5] предлагается использование блокчейна в качестве средства для децентрализованной аутентификации идентичности узла. Предлагаемая многосетевая схема аутентификации БСС включает выделение трех типов иерархически связанных узлов БСС с отличающимися возможностями, а именно, базовых станций, головных кластерных узлов и узлов общего вида, которые участвуют во взаимной аутентификации в различных сценариях коммуникации. Гибридный характер данной схемы предполагает

наличие двух блокчейнов, одного локального для обеспечения аутентификации узлов общего вида и публичного – для аутентификации головных кластерных узлов. В частности, аутентификация на основе двух видов блокчейна сводится к проверке соответствия фактических аутентификационных данных узлов релевантным записям об этих узлах, хранящихся в соответствующем блокчейне.

Повышение безопасности и надежности БСС за счет применения блокчейна сводится в первую очередь к использованию преимуществ децентрализованного управления сетью [6]. Блокчейн позволяет распределять управление между несколькими узлами БСС, а также динамически перераспределять такие обязанности, что создает резервирование коммуникационно-вычислительных ресурсов и смягчает последствия некоторых видов атак, таких как flooding-атак и DDoS-атак [7]. Кроме того, как отмечается в [8], в отличие от методов, основанных на анализе идентичности, использование блокчейна совместно со смарт-контрактами позволяет блокировать передачу разведывательных и обманных сообщений дальше по сети, что делает БСС более безопасной. Это обеспечивается тем, что в записях блокчейна отсутствуют сведения от узла, внедренного в сеть атакующим. Помимо этого в [9] отмечается отслеживаемость и управление ключами, реализуемые с использованием блокчейна, которые позволяют повысить уровень защищенности БСС.

III. АНАЛИЗ ПРИМЕНИМОСТИ И ЗАЩИЩЕННОСТИ

Необходимость в проведении анализа применимости технологии блокчейна в области БСС связана в первую очередь со значительными ограничениями на ресурсы таких сетей, что существенно затрудняет внедрение блокчейна и снижает потенциальный положительный эффект от использования данной технологии. В [10] возможные применения блокчейна обуславливаются совершенствованием программных механизмов сети, для решения которых, как правило, применяются менее эффективные не распределенные способы с использованием стороннего брокера.

Проанализируем основные возможности и ограничения интеграции каждого из видов блокчейна в беспроводные сенсорные сети (табл. 1). Отметим, что по уровню возможностей и перспектив особый интерес представляют существующие и разрабатываемые гибридные блокчейны, тогда как в контексте решения актуальных задач обеспечения неизменности данных и организации эффективных распределенных механизмов хранения данных в инфраструктурах БСС наиболее релевантными тем не менее выглядят блокчейны частного типа [8].

Вместе с тем, применительно ко всем видам блокчейна, работающего в связке с БСС, в [1] дискутируется о том, что, как правило, преимущества блокчейна начинают исчезать при масштабировании конкретной сети, когда число одновременно действующих узлов начинает резко или постепенно увеличиваться. Кроме того в [1] отмечаются вероятные проблемы с нарастанием вычислительной нагрузки, потреблением энергоресурсов и исчерпанием доступного ресурса хранения по мере продолжающегося функционирования основанной на блокчейне БСС.

ТАБЛИЦА I. АНАЛИЗ ВИДОВ БЛОКЧЕЙНА ПРИМЕНИТЕЛЬНО К БСС

Вид блокчейна	Особенности применения к БСС
Публичный блокчейн	Преимущества: – При помощи публичного блокчейна БСС способна сохранять данные от сенсоров, какие-либо прикладные и системные события БСС и другую информацию Недостатки: – Несмотря на то, что такие данные могут храниться в зашифрованном виде сами данные будут доступны глобально всем пользователям такого блокчейна – Высокие вычислительные издержки и затраты на энергопотребление, необходимые для поддержки работы алгоритмов консенсуса и смарт-контрактов, значительно затрудняют фактическое применение данного вида блокчейна
Приватный блокчейн	Преимущества: – Обеспечивает большую защищенность хранимых данных и ограничивает доступ к ним авторизованными пользователями – Более низкие вычислительные и энергетические затраты для поддержания узлов функций блокчейна на узлах Недостатки: – Ограниченная доступность данных внешним по отношению к БСС сущностям, а также недостаток средств доказуемости достоверности хранимых данных внешним сущностям
Консорциальный блокчейн	Преимущества: – В значительной степени аналогичны преимуществам приватного блокчейна – По согласованию сторон консорциума предполагает дополнительную возможность большей открытости данных внешним сущностям Недостатки: – Более сложный потенциально подверженный ошибкам механизм управления таким блокчейном, в том числе потенциально более уязвим по отношению к внешним атакующим и внутренним нарушителям безопасности
Гибридный блокчейн	Преимущества: – Представляет собой более сложный гибрид публичного и приватного блокчейна, включающий, как публичные хранимые данные, так и приватные, оставляя право выбора способа хранения пользователям – Большая гибкость и настраиваемость под различные группы и интересы участников Недостатки: – Более высокая сложность архитектуры распределенного реестра, сложность поддержания инфраструктуры и необходимость согласования действий участников

Поэтому с учетом проанализированных выше подходов и методов, сформулируем основные возможные виды применения блокчейна в БСС.

- За счет использования распределенного реестра технология блокчейн обеспечивает быстрые и надежные peer-to-peer-соединения по сравнению с другими более централизованными схемами взаимодействия узлов [10]. При этом обмен данными между узлами сети осуществляется в форме сформированных блоков данных, снабженных метками времени создания этих блоков. В этом случае отсутствует необходимость проверки и координации каждой операции со стороны доверенных посредников. Кроме того за счет этого снижаются вызываемые этим временные задержки. Кроме того параллельная и, фактически, независимая

обработка взаимодействий между различными группами узлов также повышает общую среднюю скорость коммуникации в сети.

- Обеспечение неизменности и доверия к данным между узлами БСС за счет применения блокчейна [11]. При этом необходимый уровень доверия обеспечивается фактом достижения консенсуса относительно рассматриваемых данных со стороны большей части узлов БСС в момент времени, когда эти данные были помещены в блокчейн.
- Применение заранее определенных и заслуживающих доверия правил и автоматически выполняющихся сценариев обработки данных при наступлении определенных событий в сети без прямого участия оператора и пользователей [12]. Таким образом, в момент запуска смарт-контракта соответствующие узлы БСС получают гарантии выполнения заранее согласованных условий.

Рассмотрим следующий пример, демонстрирующий использование смарт-контрактов в БСС для повышения безопасности и надежности сети. В случае обнаружения узла, функционирующего аномально совместное накопление признаков такой аномалии от некоторого достаточного числа узлов, способно запустить смарт-контракт на фактическую изоляцию данного скомпрометированного узла, которую обязаны будут соблюдать все узлы, работающие с данным блокчейном [13]. В частности, в случае систем взаимосвязанных автомобилей [14], работающих на основе инфраструктуры БСС с использованием механизмов репутации достижение пороговых значений позволяет в целях безопасности дорожного движения запустить смарт-контракт по временному запрету функционирования такого транспортного средства до момента дальнейшего выяснения обстоятельств.

Еще примером является случай киберкриминалистики системы соединенных БПЛА, функционирующей с некоторой целью, как например, для обследования местности или трубопровода [15, 16]. Каждое транспортное средство для коммуникации внутри системы использует узел БСС. При выполнении полетов группой/роем беспилотных транспортных средств каждый полет БПЛА заносится в блокчейн с фиксацией деталей маршрута, таких как пункты старта и финиша, траектория, высота и скорость полета, состояние батареи и коммуникационных интерфейсов и др. В случае инцидентов наличие цепочек блоков с логами системы с использованием блокчейна будет способствовать проведению расследования инцидента, восстановлению последовательности событий и доказательству устанавливаемых фактов. Примером смарт-контракта является случай снижения заряда батареи некоторого БПЛА ниже критического порога, зависящего от текущей дальности нахождения транспортного средства от базы. Вместе с тем смарт-контракт предписывает немедленное возвращение БПЛА для подзарядки батареи с одновременным обязательством к оставшимся беспилотникам перераспределить задачи мониторинга для недопущения пропусков в обследуемой местности/трубопроводе.

Таким образом, касательно предметной области беспроводного транспорта, функционирующего на базе инфраструктуры БСС в табл. 2 приведены четыре

типовых перспективных практических сценария применения блокчейна, их особенности и возможные сложности. В табл. 3 приведены результаты анализа актуальных видов атак для указанных 4 сценариев.

ТАБЛИЦА II. АНАЛИЗ ТИПОВЫХ СЦЕНАРИЕВ ПРИМЕНительно К СИСТЕМАМ БЕСПИЛОТНОГО ТРАНСПОРТА

Сценарий применения	Особенности сценария
Координация и управление полетами роя БПЛА	– При помощи блокчейна происходит согласование полетов БПЛА на местности для минимизации инцидентов физической безопасности и оптимизации процессов выполнения миссии – Непрерывная фиксация в блокчейне данных о местоположении БПЛА позволяет с минимальными задержками получать сведения о соседних БПЛА и строить локально оптимальные маршруты движения – К сложностям реализации можно отнести ограниченность вычислительных ресурсов и энергоресурсов на бортовых микроконтроллерах, а также возможные задержки в доставке данных в связи с несовершенством используемых беспроводных технологий
Надежный и защищенный обмен данными телеметрии	– Ввиду высокой критичности данных от сенсоров БПЛА и данных об их местоположении блокчейн обеспечивает повышенную их защищенность от возможных фальсификаций – Кроме того в блокчейне доступ к данным предоставляется только авторизованным сущностям – К ограничениям относится некоторая избыточность в хранении исторических данных, в особенности в случае дублирования сенсоров – Еще одним ограничением является постоянное подключение узлов к коммуникационной сети, что увеличивает расход энергоресурсов
Мониторинг физической промышленной и логистической инфраструктуры	– Возможность индивидуального и группового анализа состояния элементов инфраструктуры (трубопровод, промышленный цех и др.) с использованием БПЛА для выявления неисправностей приборов и нарушений функционирования – Блокчейн позволяет фиксировать изменения состояния оборудования с учетом цепочек исторических событий на узлах БСС – Использование смарт-контрактов для уведомления всех связанных узлов о выявленных инцидентах и необходимости ремонтных мероприятий – Возможные риски по рассогласованию фактического местоположения и состояния узлов при выполнении смарт-контрактов и снижению производительности БСС
Сбор, агрегация и анализ больших объемов данных транспортной инфраструктуры	– Использование алгоритмов снижения размерности и агрегации больших объемов данных от БПЛА, а также алгоритмов машинного обучения в условиях слабо предсказуемого движения и функционирования БПЛА – Наличие риска потери существенных данных и неточности проводимого анализа в результате уменьшения объемов данных и их агрегации. Необходимость достижения баланса между полнотой собираемых и обрабатываемых данных, а также размерами блоков блокчейна

ТАБЛИЦА III. АНАЛИЗ АКТУАЛЬНЫХ ВИДОВ АТАК ПРИМЕНительно К СИСТЕМАМ БЕСПИЛОТНОГО ТРАНСПОРТА

Сценарий применения	Анализ актуальных видов атак
Координация и управление полетами роя БПЛА	– атаки внедрения ложных узлов, в том числе на основе Sybi-атаки [17], направленные на изменение траекторий БПЛА и использующие возможности самоорганизации для принятия

Сценарий применения	Анализ актуальных видов атак
	- новых идентичностей узлов – DoS и flooding-атаки [18], перегружающие сеть и направленные на нарушение доступности БПЛА
Надежный и защищенный обмен данными телеметрии	– Replay-атаки, включающие повторную отправку ранее полученных данных и команд, в том числе команд инициирующих передачу функциональных ролей между узлами в рамках децентрализованного управления БСС – Основанная на Man-in-the-Middle атака перехвата и подмены данных перед их добавлением в блокчейн – Атака нарушения секретности хранимых в блокчейне данных и их раскрытия внешним сущностям
Мониторинг физической промышленной и логистической инфраструктуры	– Poisoning-атака, включающая внесение ложных, не проверенных или скомпрометированных данных в блокчейн за счет манипуляций по необоснованному динамическому перераспределению функций мониторинга, что приводит к неправильной диагностике оборудования – DoS и flooding-атаки со стороны скомпрометированных узлов в рамках децентрализованной самоорганизующейся БСС
Сбор, агрегация и анализ больших объемов данных транспортной инфраструктуры	– Атака нарушения координации БПЛА за счет препятствования скомпрометированным узлам БСС установлению консенсуса при добавлении новых данных в блокчейн – Атака прослушивания каналов передачи данных для нарушения приватности первичных и агрегированных данных – Атака необоснованного разделения сети на изолированные части, препятствующего эффективному обмену данными и анализу

В качестве одного из выводов из проведенного анализа отметим, что для повышения применимости и эффективности блокчейна в БСС, в том числе в самоорганизующихся децентрализованных сетях, целесообразно применять и адаптировать различные модели работы с данными. Сложность или даже практическая невозможность помещения в блокчейн всей полноты данных, возникающих и циркулирующих в сети, обуславливается необходимостью их существенного сокращения и агрегации, но, во-первых, с сохранением их фактической используемости в бизнес-процессах сети и, во-вторых, с возможностью валидации их корректности и неизменности.

В частности, один из примеров такой модели данных представлен в работе [6], где каждые 10 минут создается новый блок, который агрегирует все основные данные, которые должны быть сохранены в блокчейне. Это позволяет сократить объемы хранимых данных и повысить применимость блокчейна в рамках БСС. Это также позволяет оптимизировать не только, собственно, ресурс хранения, но также и ресурс обработки и коммуникационный ресурс сети. Кроме того целесообразно применять различные подходы к кластеризации в БСС, которая сокращает количество активных каналов внутри сети, и это позволяет снизить объемы хранимых данных [19].

Еще один релевантный пример представлен в [7], где новый блок формируется и добавляется в блокчейн только по мере накопления новой информации в локальной базе данных БСС. Таким образом, в рамках актуальных прикладных задач перспективным представляется подход, при котором лишь ограниченный объем данных фактически сохраняется в блокчейн,

причем сохраняемые в рамках блока транзакционные данные или слепки первичных данных характеризуют состав и состояния всех действующих узлов БСС. Например, это было бы возможно при помощи генерации контрольных сумм первичных и агрегированных данных и использовании других криптопримитивов.

Кроме того отметим, что в сравнении с альтернативными работами в данной предметной области, в частности [1, 4, 20], помимо анализа применимости и защищенности технологии блокчейна в БСС, в рамках настоящей работы особое внимание уделяется также проблематике самоорганизации и децентрализации БСС и их влиянию на способы организации блокчейна в БСС и защищенности таких решений. В частности, в данной работе учитываются децентрализация БСС, возможные ролевые модели узлов и связанные с этим актуальные виды атак.

IV. ЗАКЛЮЧЕНИЕ

Проводимая работа посвящена исследованию особенностей использования технологии блокчейна в БСС, выявлению угроз кибербезопасности, связанных с использованием блокчейна с учетом свойств самоорганизации и децентрализации БСС. В качестве направлений дальнейших исследований рассматривается решение задач моделирования и программно-аппаратной реализации распределенных механизмов управления безопасностью в БСС с учетом применимости блокчейна и методов интеллектуального анализа данных.

СПИСОК ЛИТЕРАТУРЫ

- [1] Nguyen V.-C., Nguyen M.T., Trang T.L.H., Tran T.A. Blockchain Technology in Wireless Sensor Network: Benefits and Challenges // *Proceedings of the XXXX conference*. 2021. С. 1–5.
- [2] Rajesh M.V., Acharya T.A., Hajiyeve H., Lydia E.L., Alshahrani H.M., Nour M.K., Mohamed A., Duhayyim M.A. Blockchain Driven Metaheuristic Route Planning in Secure Wireless Sensor Networks // *Computers, Materials and Continua*. 2023. Vol. 74, №1. С. 933–949. DOI: 10.32604/cmc.2023.027344.
- [3] Gupta V., De S. An Energy-Efficient Edge Computing Framework for Decentralized Sensing in WSN-Assisted IoT // *IEEE Transactions on Wireless Communications*. 2021. Vol. 20, №8. С. 4811–4827. DOI: 10.1109/TWC.2021.3062568.
- [4] Ismail S., Dawoud D.W., Reza H. Securing Wireless Sensor Networks Using Machine Learning and Blockchain: A Review // *Future Internet*. 2023. Vol. 15, No. 6. Art. No.: 200. DOI: 10.3390/fi15060200.
- [5] Cui Z., Hue F., Zhang S., Cai X., Cao X., Zhang W., Chen J. A Hybrid Blockchain-Based Identity Authentication Scheme for Multi-WSN // *IEEE Transactions on Services Computing*. 2020. Vol. 13, №2. С. 241–251. DOI: 10.1109/TSC.2020.2964537.
- [6] Rehman A. et al. Ensuring Security and Energy Efficiency of Wireless Sensor Network by Using Blockchain // *Applied Sciences*. 2022. Vol. 12, №21. Art. No.: 10794. DOI: 10.3390/app122110794.
- [7] Guerrero-Sanchez A.E., Rivas-Araiza E.A., Gonzalez-Cordoba J.L., Toledano-Ayala M., Takacs A. Blockchain Mechanism and Symmetric Encryption in a Wireless Sensor Network // *Sensors*. 2020. Vol. 20, №10. Art. No.: 2798. DOI: 10.3390/s20102798.
- [8] Dener M., Orman A. BBAP-WSN: A New Blockchain-Based Authentication Protocol for Wireless Sensor Networks // *Applied Sciences*. 2023. Vol. 13, No. 3. Art. No.: 1526. DOI: 10.3390/app13031526.
- [9] Nguyen M.D., Nguyen M.T., Chien T.V., Ta T.M. A Comprehensive Study on Applications of Blockchain in Wireless Sensor Networks for Security Purposes // *Journal of Computing Theories and Applications*. 2024. Vol. 2, №1. С. 102–117. DOI: 10.62411/jcta.10486.
- [10] Ramasamy L.K., Firoz Khan K.P., Imoize A.L., Ogbemor J.O., Kadry S., Rho S. Blockchain-Based Wireless Sensor Networks for Malicious Node Detection: A Survey // *IEEE Access*. 2021. Vol. 9. С. 128765–128785. DOI: 10.1109/ACCESS.2021.3111923.
- [11] Yasin M.R., Syed H.J., Shuja J. An Efficient Approach for Tampering Attack Detection in WSN Using Blockchain / 2024 International Wireless Communications and Mobile Computing (IWCMC). Ayia Napa, Cyprus : IWCMC, 2024. С. 156–161. DOI: 10.1109/IWCMC61514.2024.10592565.
- [12] She W., Liu Q., Tian Z., Chen J.-S., Wang B., Liu W. Blockchain Trust Model for Malicious Node Detection in Wireless Sensor Networks // *IEEE Access*. 2019. Vol. 7. С. 38947–38956. DOI: 10.1109/ACCESS.2019.2902811.
- [13] Nouman M. et al. Malicious Node Detection Using Machine Learning and Distributed Data Storage Using Blockchain in WSNs // *IEEE Access*. 2023. Vol. 11. С. 6106–6121. DOI: 10.1109/ACCESS.2023.3236983.
- [14] Chiasserini C.F., Giaccone P., Malnati G., Macagno M., Sviridov G. Blockchain-based Mobility Verification of Connected Cars / 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC). Las Vegas, NV, USA : CCNC, 2020. С. 1–6. DOI: 10.1109/CCNC46108.2020.9045104.
- [15] Wang J., Liu Y., Niu S., Song H.H. Blockchain Enabled Verification for Cellular-Connected Unmanned Aircraft System Networking // *Future Generation Computer Systems*. 2021. Vol. 123. С. 233–244. DOI: 10.1016/j.future.2021.05.002.
- [16] Karam S. N., Bilal K., Shuja J., Khan L.U., Bilal M., Khan M.K. Intelligent IoT- and UAV-Assisted Architecture for Pipeline Monitoring in OGI // *IT Professional*. 2024. Vol. 26, №3. С. 46–54. DOI: 10.1109/MITP.2023.3339448.
- [17] Benadla S., Merad-Boudia O.R., Senouci S.M., Lehsaini M. Detecting Sybil Attacks in Vehicular Fog Networks Using RSSI and Blockchain // *IEEE Transactions on Network and Service Management*. 2022. Vol. 19, №4. С. 3919–3935. DOI: 10.1109/TNSM.2022.3216073.
- [18] Embarak O.H., Zitar R.A. Securing Wireless Sensor Networks against DoS Attacks in Industrial 4.0 // *Journal of Intelligent Systems & Internet of Things*. 2023. Vol. 8, №1. Art. No.: 080106. DOI: 10.54216/JISIoT.080106.
- [19] Verma S., Zeadally S., Kaur S., Sharma A.K. Intelligent and Secure Clustering in Wireless Sensor Network (WSN)-Based Intelligent Transportation Systems // *IEEE Transactions on Intelligent Transportation Systems*. 2022. Vol. 23, №8. С. 13473–13481. DOI: 10.1109/TITS.2021.3124730.
- [20] Singh T., Vaid R., Sharma A. Security Issues in Blockchain Integrated WSN: Challenges and Concerns / 2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICES). Chennai, India : ICSES, 2022. С. 1–5. DOI: 10.1109/ICES55317.2022.9914006.