Обзорная статья
УДК 004.738.5.056:623.746.4-519
ББК 32.52-057
Д 58
DOI: 10.53598/2410-3225-2024-3-346-71-80

Обзор концепции Интернета дронов и обеспечение безопасности выполнения полета роем БПЛА

(*Рецензирована*)

Виталий Анатольевич Довгаль

Майкопский государственный технологический университет,
Адыгейский государственный университет, Майкоп, Россия, urmia@mail.ru

Аннотация. *Проводится обзор концепции Интернета дронов как децентрализованной сети в контексте обеспечения информационной безопасности передаваемых данных. Рассматриваются основные направления использования новой технологической концепции, а также дан анализ основных угроз, исходящих от злоумышленников. Представлен анализ видов атак и нарушения обеспечения безопасной передачи данных в группе дронов, выполняющих совместный полет.*

Ключевые слова: *информационная безопасность, беспилотные летательные аппараты, Интернет вещей, Интернет дронов*

Для цитирования: *Довгаль В. А. Обзор концепции Интернета дронов и обеспечение безопасности выполнения полета роем БПЛА // Вестник Адыгейского государственного университета. Сер. : Естественно-математические и технические науки. 2024. Вып. 3* (*346*). *С. 71–80. DOI: 10.53598/2410-3225-2024-3-346-71-80*

Работа выполнена при поддержке гранта ФГБОУ ВО МГТУ (*проект № НП11-2024 «Единое интеллектуальное информационное пространство региона как фактор его устойчивого и эффективного развития»*).

Review Article

Brief review the concept of the drone Internet and ensuring the safety of UAVs swarm flight execution

Vitaly A. Dovgal

Maikop State Technological University, Adyghe State University,
Maykop, Russia, urmia@mail.ru

Abstract. *The paper reviews the concept of the drone Internet as a decentralized network in the context of ensuring information security of transmitted data. The main directions of using the new technological concept are considered, and the main threats posed by attackers are analyzed. An analysis of the types of attacks and violations of secure data transmission in a group of drones flying together is presented.*

Keywords: *information security, drones, Internet of things, Internet of drones*

For citation: *Dovgal V. A. Reviewing the concept of the drone Internet and ensuring the safety of UAV swarm flight execution // The Bulletin of the Adyghe State University. Ser. : Natural-Mathematical and Technical Sciences. 2024. Iss. 3* (*346*). *P. 71–80. DOI: 10.53598/2410-3225-2024-3-346-71-80*

The work was supported by the grant of FGBOU VO MSTU (*project No. NP11-2024* "*Common intellectual information space of the region as a factor of its sustainable and effective development*").

Введение

Беспилотные летательные аппараты (БПЛА), также известные как дроны, – это устройства, управляемые удаленным пользователем или станцией управления. До недавнего времени управление каждым отдельным беспилотником осуществлялось индивидуально, но последние технологические достижения позволяют большому количеству беспилотников взаимодействовать между собой и выполнять сложные задачи скоординированно [1], стремясь к эффективному управлению воздушным пространством [2].

Интернет дронов (Internet of Drones, IoD) – это децентрализованная сеть, осуществляющая доступ дронов к контролируемому воздушному пространству, обеспечивающая высокую адаптивность к сложным сценариям и услуги для различных приложений дронов, таких как доставка посылок, наблюдение за дорожным движением, выполнение поисково-спасательных миссий, включая навигационные услуги [3]. БПЛА в сочетании с принципами IoD обладают многочисленными преимуществами, например, высокой мобильностью, зонами покрытия беспроводной связи и способностью достигать труднодоступные места, включая значительные улучшения, такие как надежность, связь, пропускная способность и снижение задержек.

Экосистема IoD, использующая широкий спектр приложений, снижает эксплуатационные расходы, позволяя за счет повышенной гибкости, мобильности, масштабируемости и автономности решать различные задачи широкого круга потребителей (например, мониторинг угодий сельского хозяйства, ускоренная доставка посылок, ретрансляция услуг типа Интернет-сервисов в удаленные точки и т. д. [4]. При этом IoD можно рассматривать как часть Интернета вещей (Internet of Things, IoT), оснащенную взаимосвязанными физическими устройствами и подключенными к Интернету датчиками [5]. Таким образом, сеть беспилотников приобретает новые перспективы, предоставляя больше возможностей, но в то же время сохраняя ключевые свойства IoT. Как типичная сетевая архитектура, рой дронов наследует недостатки безопасности сетей IoT [6].

Цель данной статьи – обзор новой концепции Интернета дронов в контексте обеспечения информационной безопасности данных, передаваемых в сети роя.

1. Интернет беспилотных летательных аппаратов

IoD, как многоуровневая сеть контролируемого доступа к дронам с целью их координации, обеспечивает такие важные преимущества, как масштабируемость, обслуживание кодовой базы и гибкость модификации уровней с минимальными изменениями других взаимосвязанных уровней. Примерная сеть IoD состоит из трех уровней с выделенными функциями [7]:

- уровень сети управления воздушным движением;
- уровень сети сотовой связи;
- уровень Интернета.

Традиционная архитектура IoD подразделяется на определенные компоненты для корректной и эффективной работы БПЛА:

- управление и администрирование для обеспечения передачи собранных данных в нужное место назначения от узлов-источников [8];
- протоколы связи, поддерживающие передачу данных между узлами, к которым относятся MAVLink и ROSLink [9].

На практике задачи принятия решений выполняются узлами для установления необходимого поведения в сети и ускорения маршрутизации между опорными и целевыми узлами. Процесс сбора данных, их передача, стабильность и методология связи зависят от архитектурных компонентов с новыми методологиями, исследованными и проанализированными в [10, 11], а дальнейшие элементы среды IoD являются частью

слоя промежуточного программного обеспечения, разделенного на сервисные и облачные аналоги, обеспечивающие абстракцию между различными интерфейсами IoD, такими как языки программирования, операционные системы, сети и архитектуры.

Сервисное промежуточное программное обеспечение (ПО) предоставляет доступ к сети, локальную доставку сообщений, кэширование и разрешение имен для архитектуры IoD, поддерживая надежное соединение и взаимодействие для всей архитектуры Интернета дронов. Облачное промежуточное ПО быстро предоставляет ответ на запрашиваемый сервис и поддерживает различные операции приложений, например Robot Operating System (ROS), для их интеграции в сетевую архитектуру, обеспечивая при этом надежную связь между наземной сетью и БПЛА. Поскольку несколько беспилотников связаны между собой для одновременного выполнения различных операций, важным элементом инфраструктуры IoD является объединение и совместное использование данных, позволяющее обрабатывать и объединять различные источники данных для дальнейшего генерирования и пересмотра данных для задач принятия решений.

Кроме того, данные IoD можно разделить на несколько категорий:

- распределенные (мета-архитектура) данные поддерживают их переход в форму локального взаимодействия, что приводит к их масштабируемости, отказоустойчивости, совместимости, легкости перепроектирования и реконфигурации, а также безопасности от незапланированных отключений дронов;
- централизованные данные, используемые для бесперебойной работы роя дронов и обмена всей необходимой информацией через центр синтеза при поддержке других взаимосвязанных устройств сети, что приводит к получению более точной информации, связанной с задачей;
- облачные данные, контролируемые облачными интерфейсами и состоящие из различных сервисов, включая аналитику безопасности, предотвращение столкновений и операции по навигации с учетом риска.

Особую роль играет обеспечение выполнения вопросов сетевой безопасности, таких как аутентификация, конфиденциальность, доступность и обнаружение вторжений, а также соображения безопасной передачи данных, являющихся наиболее важными факторами, которые должны быть реализованы при проектировании архитектур IoD и разработке соответствующих приложений. На рисунке 1 представлена классификация соответствующих элементов и характеристик традиционной инфраструктуры IoD.

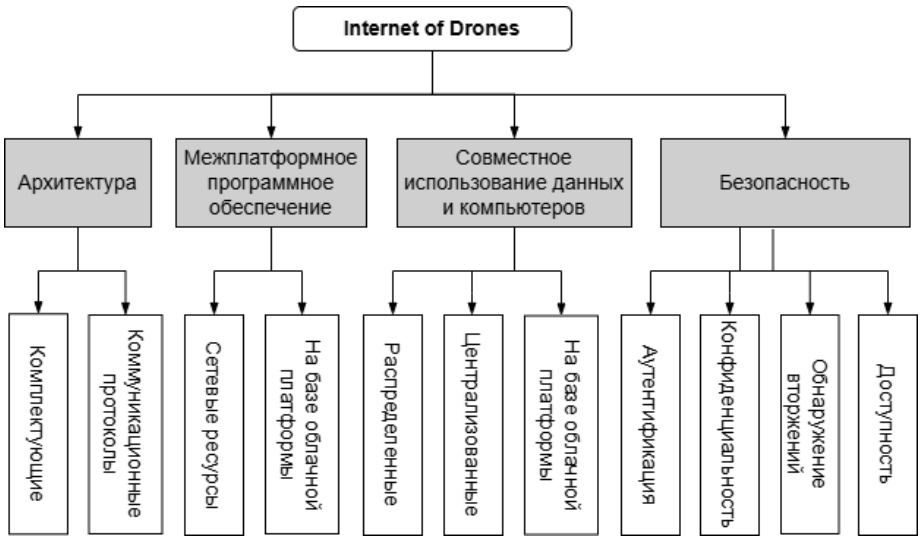

Рис. 1. Основные элементы и функции IoD

Fig. 1. Main elements and functions of IoD

Основные требования к IoD можно разделить на требования к связи и безопасности, поскольку беспилотники являются основным функциональным компонентом соответствующей технологии. На рисунке 2 представлены соответствующие ключевые требования к IoD.

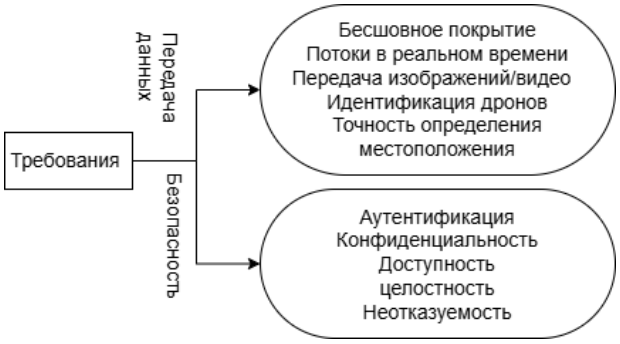

Рис. 2. Ключевые требования к IoD

Fig. 2. Key requirements for IoD

Требованиями к передаче данных являются:

1. Бесшовное покрытие, поддерживающее работу беспилотников на разных высотах в отличие от сетей. Например, для обеспечения защиты растений используется покрытие на высоте до 10 м, для обследования линий электропередач – 50–100 м, а для картографирования сельскохозяйственных угодий рекомендуется использовать высоты в диапазоне 200–300 м [12].

2. Для контроля условий полета, задач беспилотника и оборудования, а также для управления в чрезвычайных ситуациях используются дистанционные контроллеры в режиме реального времени, в зависимости от условной задержки и требований к скорости передачи данных.

3. Передача изображений и видео высокой четкости обеспечивает высокую скорость передачи данных по восходящей линии связи от дрона к станции в зависимости от их размера и качества соответственно. Кроме того, сети 5G поддерживают такие услуги, как высокая скорость передачи данных (10 Гбит/с), низкие задержки, увеличение дальности беспроводной связи, а также дополнительные функции в рамках применения дронов, включая дополненную и виртуальную реальность.

4. Мобильные сети идентифицируют и контролируют беспилотники посредством поддержки:

- регистрации серийных номеров и законности управления полетом;
- обнаружения и мониторинга соединений и передачи данных беспилотников, при этом в режиме реального времени устанавливаются дополнительные протоколы регулирования;
- чувствительной к времени оценки и предупреждения о полетах для предотвращения рисков, связанных с траекториями полетов, движением и координацией [13].

Кроме того, большое значение имеет точное вертикальное или горизонтальное позиционирование, однако оно зависит от области применения

Требования к конфиденциальности и безопасности возникают в самой сети, например, из-за ошибок локализации. Следовательно, необходимо уделить дополнительное внимание аутентификации устройств, узлов и пользователей для предотвращения несанкционированного доступа к конфиденциальной информации, включая взаимную аутентификацию между дроном и наземной станцией управления. Такие меры противодействия достигаются за счет использования ключей безопасности, обеспечивающих абсолютную секретность и конфиденциальность при защите беспроводных каналов связи от несанкционированного разглашения информации, доступность данных,

контроль доступа, целостность собранных данных и неотказуемость, направленная на обнаружение скрытых действий.

2. Фундаментальная архитектура IoD

IoD, как сетевая архитектура, контролирует воздушное пространство путем развертывания взаимосвязанных БПЛА и установления их постоянной координации, которая достигается за счет создания наземной станции (НС) и распределенных беспилотников [2]. Важнейшей задачей БПЛА является сбор и хранение данных и информации из определенной зоны полета (Fly Zone, FZ), которые затем передаются на назначенную НС с помощью модулей беспроводной связи, основанных на технологиях IoT. В частности, воздушное пространство делится на множество конкретных FZ и групп дронов, направленных на мониторинг конкретной среды для эффективного сбора данных, которые передаются на управляющий сервер (УС) НС. На сервер управления возложены дополнительные обязанности (хранение конфиденциальной информации, относящейся к пользователю, дрону и воздушному пространству). С помощью диспетчерского пульта (ДП) пользователь наблюдает за заранее заданной средой IoD, при этом все участники сети регистрируются до развертывания дрона в запланированной полетной зоне.

После регистрации беспилотники в режиме реального времени собирают данные в соответствующей зоне и передают их на сервер управления, при этом они могут делиться собранными данными со своими соседями. Кроме того, ДП может передать дронам через УС инструкции для выполнения любой необходимой задачи. Беспроводная связь обеспечивается сотовыми сетями 5G в конкретной FZ, в отличие от подключения между НС и беспроводными точками доступа, которое осуществляется проводным способом. На рисунке 3 представлена концептуальная модель сети IoD с коммуникациями и разделением обязанностей в среде IoD.

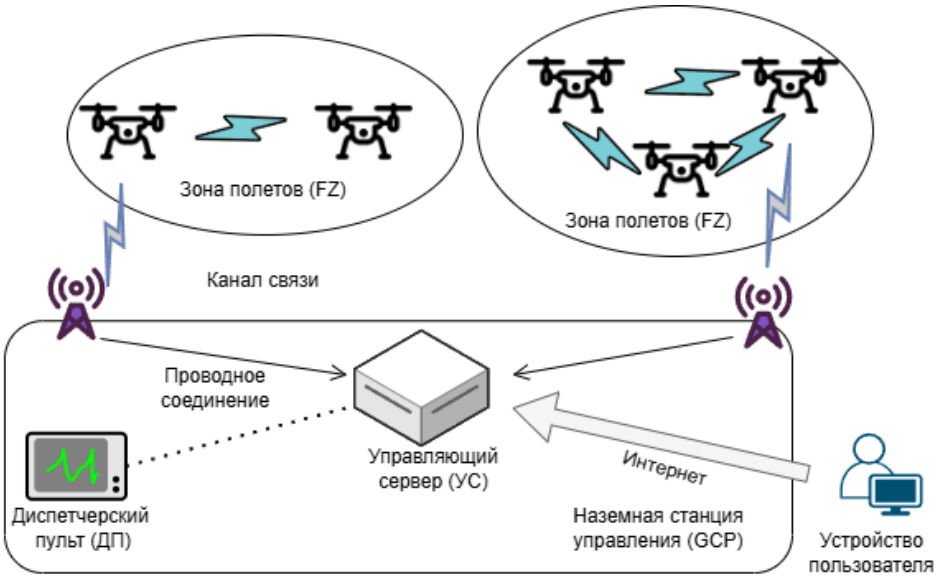

Рис. 3. Концептуальная модель сети Интернета дронов

Fig. 3. A conceptual model of the drone Internet network

3. Безопасность в IoD

С развитием индустрии беспилотных летательных аппаратов растет количество приложений на базе БПЛА. Соответственно, растут и различные риски и уязвимости. Система IoD подвержена многим проблемам безопасности и защиты, которые могут существенно повлиять на выполнение поставленной задачи, данные (получение, связь,

хранение) и сеть, принимая во внимание передачу конфиденциальной и критической информации, поскольку инфраструктура IoD становится целью для многих враждебных кибератак [14].

Все атаки можно разделить на следующие группы [15]:

- атаки на устройства, направленные на имитацию конфиденциальных учетных данных для доступа к компонентам беспилотников;
- сетевые атаки, при которых потоки данных подменяются и изменяются;
- программные атаки, при которых в беспилотники или наземные станции внедряются вредоносные данные.

Таким образом, сохранение конфиденциальности, целостности, доступности, аутентичности и конфиденциальности являются ключевыми требованиями к IoD, чтобы правильно отразить ее возможности и функции в борьбе с угрозами и нарушениями безопасности:

- конфиденциальность беспроводных каналов связи предотвращает утечку данных;
- целостность гарантирует неизменность собранных данных;
- доступность услуг для авторизованных пользователей сохраняется даже в случае проникновения;
- аутентификация проверяет личность перед доступом или обменом данными, а конфиденциальность предотвращает раскрытие личных данных злоумышленниками без разрешения.

Кроме того, сети IoD уязвимы к физическим угрозам, что сильно влияет на их безопасность и, как следствие, на требования дронов к выполнению поставленных перед ними задач. Значительными примерами физических угроз являются кражи и вандализм, неблагоприятные погодные условия (в зависимости от размера работающего дрона), столкновения между дронами из-за природы IoD-приложений и совместной работы беспилотного флота, а также возможные сенсорные сбои.

3.1. Атаки, основанные на ошибках локализации.

Одной из основных категорий атак на системы IoD являются атаки, основанные на ошибках локализации. В частности, отсутствие локализации для киберфизических систем, таких как IoD, приводит к значительным ошибкам, возникающим из-за препятствования оценке безопасного местоположения дронов. На рисунке 4 представлена классификация атак на IoD, основанная на соответствующей категории.

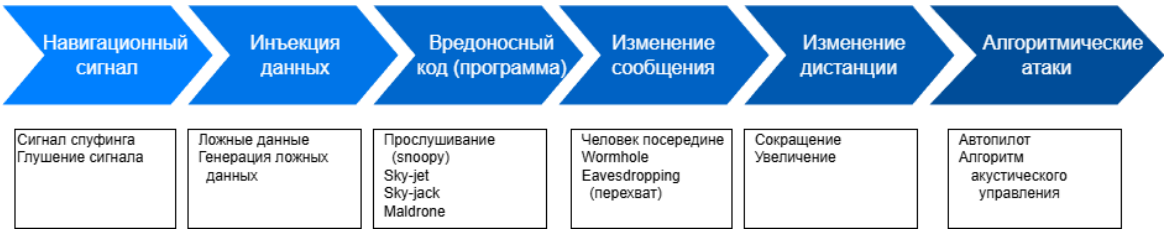

Рис. 4. Атаки на основе ошибки локализации

Fig. 4. Attacks based on localization error

Первый блок атак – навигационный сигнал – использует необходимость роя дронов определять точное местоположение с помощью навигационных сигналов, включая глобальную систему позиционирования (GPS), глобальные навигационные спутниковые системы (GNSS) и наземные сигналы управления (GCS). К ним относятся:

- атаки спуфинга GPS, направленные на обработку сигналов GPS с помощью специализированных генераторов, значительно задерживающих сигнал, что приводит к нарушению координации и возможным столкновениям дронов в воздухе;

- глушение каналов, нарушающих связь путем использования сигналов GNSS, принимаемых дронами, для предоставления неверных направлений, в то время как в случае с НС третьи лица передают ложные сигналы, направляющие дроны в определенные места.

Другой тип атак ошибок локализации – традиционная инъекция данных, в результате которой модифицируются инструкции для изменения запрограммированного маршрута беспилотника:

- вредоносная атака типа Snoopy, позволяющая третьим лицам проводить сбор данных, связанных с использованием Wi-Fi в системе IoD, что приводит к навигационному контролю над дроном;
- атака sky-jet, связанная с установкой программного обеспечения для деактивации стандартных и запрограммированных средств управления навигацией;
- атака sky-jack, позволяющая злоумышленникам обнаружить используемые беспроводные сети и проникнуть в них;
- атака Maldrone, нарушающая связь между системой управления полетом дрона и его сенсорными устройствами и позволяющая удаленно захватывать БПЛА.

Атаки изменения сообщений позволяют нарушить передачу данных и сообщений для эффективного управления дронами:

- атака «человек посередине» основана на получении несанкционированного доступа к потокам навигационных данных, передаваемых между дроном и соответствующей системой навигационного управления;
- атака сетевого уровня Vormhole, связанная со вмешательством, предполагает физическое или цифровое изменение аппаратного или программного обеспечения дрона, приводящее к несанкционированному управлению, краже данных или даже повреждению дрона;
- атака «прослушивание» – это перехват навигационных сообщений между интересующим дроном и его контроллером по незащищенным каналам связи.

Группа атак, связанных с изменением дистанции, позволяет сфальсифицировать данные о расчете расстояния, изменяя данные об определении положения компонентов IoD по размеру или содержанию.

Атаки на основе алгоритмов – последний тип проникновений, основанных на ошибках локализации, определяемый внедренными алгоритмами, которые приводят к существенному искажению функциональности автопилота и искажают алгоритм акустического управления положением путем изменения резонансной частоты гироскопа дрона.

3.2. Атаки, основанные на требованиях безопасности и конфиденциальности – категория атак IoD, основанная на требованиях безопасности и конфиденциальности, нацеленных на такие важные принципы, как целостность, доступность, аутентичность, конфиденциальность и неразглашение, как показано на рисунке 5.

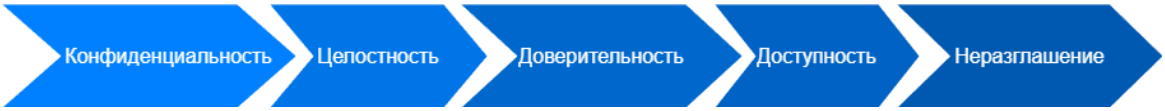

Рис. 5. Атаки на требования IoD к безопасности и конфиденциальности

Fig. 5. Attacks on IoD security and privacy requirements

Конфиденциальные данные, собираемые и обрабатываемые с помощью механизмов IoD, могут быть украдены или искажены злоумышленниками с помощью таких стратегий нападения, как анализ трафика, путем получения информации об устройствах и сетях IoD, включая местоположение, подключенные сенсорные устройства и захваченные ими данные, которые распределяются между сетью IoD и GCS, что в ре-

зультате приводит к перехвату сетевого трафика.

Другая категория атак связана с целостностью, то есть точностью, достоверностью и непротиворечивостью данных. Целостность IoD нарушается путем введения ложных данных в систему связи путем модификации, фальсификации, подмены и инъекции данных с целью введения в заблуждение пользователей беспилотников.

Конфиденциальность нарушается в результате несанкционированного доступа нелегитимных пользователей к компонентам сети IoD для получения целевой информации. Показательными примерами являются подмена идентификации, когда злоумышленник выдает себя за легитимного пользователя путем подмены идентификационных данных; несанкционированный доступ к серверу и сервисам IoD с использованием взломанных учетных записей или дублирования идентификаторов; атаки повторного воспроизведения путем обхода и воспроизведения установленных механизмов безопасности и запросов; подслушивание для перехвата коммуникаций IoD в режиме реального времени с целью извлечения конфиденциальной информации [16].

Атаки, связанные с доступностью IoD, направлены на нанесение физического ущерба структуре беспилотника или его аппаратным компонентам, например, путем прерывания работы сети (Denial-of-Service, DoS), включая рассылку пакетов во всё порты, кроме исходного, в целях перегрузки злоумышленником сети беспилотников, отправкой большого количества ненужного и нежелательного трафика. Перегрузка сети дронов приводит к снижению производительности или даже полному отключению и нарушению работы сервера нормального трафика (Distributed Denial-of-Service, DDoS), путем подмены GPS и глушения каналов, что препятствует доступу законных пользователей к услугам и важным ресурсам.

Кроме того, возникновение рисков на этапах разработки и развертывания, связанных с неправильной конфигурацией и ограниченным включением механизмов безопасности, заменой прошивки в процессе обновления или фальсификацией механизмов IoD, может привести к утечке данных, влияя на доверительность данных. Среди других стратегий стоит упомянуть кейлоггеры, используемые для передачи конфиденциальных данных непосредственно злоумышленникам, или нарушения нормативных требований доверенными третьими лицами, приводящие к финансовым потерям и потерям интеллектуальной собственности.

Таким образом, исследование технологической концепции IoD показывает, что обеспечение безопасности функционирования роя требует отказа от использования традиционных децентрализованных механизмов и подключения дополнительных технологий, например, искусственного интеллекта или вычислительных вариаций для дальнейшего дополнения таких требований, как автоматизация, распределение задач для повышения эффективности и улучшение скорости передачи данных.

Примечания

1. Dovgal V. A. Making decisions about the placement of unmanned aerial vehicles based on the implementation of an artificial immune system in relation to information processing // Proceedings – 2021 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM 2021), Sochi, May 17–21, 2021. Sochi, 2021. P. 828–833.
DOI: 10.1109/ICIEAM51226.2021.9446353

2. Dovgal V. A. Decision-making for placing unmanned aerial vehicles to implementation of analyzing cloud computing cooperation applied to information processing // Proceedings – 2020 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM 2020), Sochi, May 18–22, 2020. Sochi : Institute of Electrical and Electronics Engineers Inc. 2020. P. 9111975.
DOI: 10.1109/ICIEAM48468.2020.9111975

3. Singh M. P., Aujla G. S., Bali R. S. Blockchain for the Internet of Drones: Applications, Challenges and Future Directions // IEEE Internet Things Mag. 2021. No. 4. P. 47–53.

4. Довгаль В. А., Куижева С. К. Использование технологии больших данных для охра-

ны окружающей среды // Фундаментальные и прикладные аспекты геологии, геофизики и геоэкологии с использованием современных информационных технологий : материалы VI Междунар. науч.-практ. конф., Майкоп, 17–21 мая 2021 г. Майкоп : Кучеренко В. О., 2021. Ч. 1. С. 86–94.

5. Довгаль В. А., Довгаль Д. В. Обзор возможностей интеграции облачных вычислений и Интернета вещей // Вестник Адыгейского государственного университета. Сер. : Естественно-математические и технические науки. 2019. Вып. 4 (251). С. 81–86.
URL: http://vestnik.adygnet.ru

6. Dovgal V. A., Dovgal D. V. Security analysis of a swarm of drones resisting attacks by intruders // Distance Learning Technologies (DLT 2020): Selected Papers of the 5th International Scientific and Practical Conference. Yalta, Crimea, September 22–25, 2020. Yalta, Crimea, 2021. P. 316–323.

7. The Internet of Drones: AI Applications for Smart Solutions / A. Solanki, S. Tarar; S. P. Singh, A. Tayal // CRC Press : Boca Raton, 2022. 450 p.

8. A multidomain virtual network embedding algorithm based on multiobjective optimization for Internet of Drones architecture in Industry 4.0 / P. Zhang, C. Wang, Z. Qin, H. Cao // Softw. Pract. Exp. 2022. No. 52. P. 710–728.

9. Dronemap Planner: A service-oriented cloud-based management system for the Internet-of-Drones / A. Koubâa, B. Qureshi, M.-F. Sriti [at al.] // Ad Hoc Netw. 2019. No. 86. P. 46–62.

10. Collaborative Data Acquisition for UAV-Aided IoT Based on Time-Balancing Scheduling / M. Ren, X. Fu, P. Pace [at al.] // IEEE Internet Things J. 2024. No. 11. P. 13660–13676.

11. Huang X., Fu X. Fresh Data Collection for UAV-Assisted IoT Based on Aerial Collaborative Relay // IEEE Sensors J. 2023. No. 23. P. 8810–8825.

12. Communication and networking technologies for UAVs: A survey / A. Sharma, P. Vanjani, N. Paliwal [at al.] // J. Netw. Comput. Appl. 2020. No. 168. P. 102739.

13. Security and Privacy for the Internet of Drones: Challenges and Solutions / C. Lin, D. He, N. Kumar [at al.] // IEEE Commun. Mag. 2018. No. 56. P. 64–69.

14. Довгаль В. А., Довгаль Д. В. Анализ уязвимостей и угроз безопасности роя дронов с поддержкой Wi-Fi, противостоящего атакам злоумышленников // Вестник Адыгейского государственного университета. Сер. : Естественно-математические и технические науки. 2020. Вып. 3 (266). С. 67–73. URL: http://vestnik.adygnet.ru

15. Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations / N. Neshenko, E. Bou-Harb, J. Crichigno [at al.] // IEEE Commun. Surv. Tutorials. 2019. No. 21. P. 2702–2733.

16. Довгаль В. А., Довгаль Д. В. Обнаружение и предотвращение атаки «злоумышленник в середине» в туманном слое роя дронов // Вестник Адыгейского государственного университета. Сер. : Естественно-математические и технические науки. 2020. Вып. 2 (261). С. 53–59. URL: http://vestnik.adygnet.ru

References

1. Dovgal V. A. Making decisions about the placement of unmanned aerial vehicles based on the implementation of an artificial immune system in relation to information processing // Proceedings – 2021 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM 2021), Sochi, May 17–21, 2021. Sochi, 2021. P. 828–833.
DOI: 10.1109/ICIEAM51226.2021.9446353

2. Dovgal V. A. Decision-making for placing unmanned aerial vehicles to implementation of analyzing cloud computing cooperation applied to information processing // Proceedings – 2020 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM 2020), Sochi, May 18–22, 2020. Sochi : Institute of Electrical and Electronics Engineers Inc. 2020. P. 9111975.
DOI: 10.1109/ICIEAM48468.2020.9111975

3. Singh M. P., Aujla G. S., Bali R. S. Blockchain for the Internet of Drones: Applications, Challenges and Future Directions // IEEE Internet Things Mag. 2021. No. 4. P. 47–53.

4. Dovgal V. A., Kuizheva S. K. Utilizing big data technology for environmental protection // Fundamental and applied aspects of geology, geophysics and geoecology using modern information technologies : Proceedings of 4th International Scientific and Practical Conference, Maykop, May 17–21, 2021. Maykop : Kucherenko V. O., 2021. Part 1. P. 86–94.

5. Dovgal V. A., Dovgal D. V. A survey of the integration possibilities of cloud computing and Internet of things // The Bulletin of the Adyghe State University. Ser. : Natural-Mathematical and Technical Sciences. 2019. Iss. 4 (251). P. 81–86. URL: http://vestnik.adygnet.ru

6. Dovgal V. A., Dovgal D. V. Security analysis of a swarm of drones resisting attacks by in-

truders // Distance Learning Technologies (DLT 2020): Selected Papers of the 5th International Scientific and Practical Conference. Yalta, Crimea, September 22–25, 2020. Yalta, Crimea, 2021. P. 316–323.

7. The Internet of Drones: AI Applications for Smart Solutions / A. Solanki, S. Tarar; S. P. Singh, A. Tayal // CRC Press : Boca Raton, 2022. 450 p.

8. A multidomain virtual network embedding algorithm based on multiobjective optimization for Internet of Drones architecture in Industry 4.0 / P. Zhang, C. Wang, Z. Qin, H. Cao // Softw. Pract. Exp. 2022. No. 52. P. 710–728.

9. Dronemap Planner: A service-oriented cloud-based management system for the Internet-of-Drones / A. Koubâa, B. Qureshi, M.-F. Sriti [at al.] // Ad Hoc Netw. 2019. No. 86. P. 46–62.

10. Collaborative Data Acquisition for UAV-Aided IoT Based on Time-Balancing Scheduling / M. Ren, X. Fu, P. Pace [at al.] // IEEE Internet Things J. 2024. No. 11. P. 13660–13676.

11. Huang X., Fu X. Fresh Data Collection for UAV-Assisted IoT Based on Aerial Collaborative Relay // IEEE Sensors J. 2023. No. 23. P. 8810–8825.

12. Communication and networking technologies for UAVs: A survey / A. Sharma, P. Vanjani, N. Paliwal [at al.] // J. Netw. Comput. Appl. 2020. No. 168. P. 102739.

13. Security and Privacy for the Internet of Drones: Challenges and Solutions / C. Lin, D. He, N. Kumar [at al.] // IEEE Commun. Mag. 2018. No. 56. P. 64–69.

14. Dovgal V. A., Dovgal D. V. Analysis of vulnerabilities and security threats in a swarm of Wi-Fi-enabled drones that resist malicious attacks // The Bulletin of the Adyghe State University. Ser. : Natural-Mathematical and Technical Sciences. 2020. Iss. 3 (266). P. 67–73. URL: http://vestnik.adygnet.ru

15. Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations / N. Neshenko, E. Bou-Harb, J. Crichigno [at al.] // IEEE Commun. Surv. Tutorials. 2019. No. 21. P. 2702–2733.

16. Dovgal V. A., Dovgal D. V. Detecting and preventing the man in the middle attack in the foggy layer of a swarm of drones // The Bulletin of the Adyghe State University. Ser. : Natural-Mathematical and Technical Sciences. 2020. Iss. 2 (261). P. 53–59. URL: http://vestnik.adygnet.ru

Статья поступила в редакцию 10.09.2024; *одобрена после рецензирования 15.09.2024*; *принята к публикации 16.09.2024*.

The article was submitted 10.09.2024; *approved after reviewing 15.09.2024*; *accepted for publication 16.09.2024*.