

Интернет-журнал «Отходы и ресурсы» <https://resources.today>  
Russian Journal of Resources, Conservation and Recycling

2023, Том 10, № 2 / 2023, Vol. 10, Iss. 2 <https://resources.today/issue-2-2023.html>

URL статьи: <https://resources.today/PDF/02INOR223.pdf>

DOI: 10.15862/02INOR223 (<https://doi.org/10.15862/02INOR223>)

**Ссылка для цитирования этой статьи:**

Массеров, Д. Д. Intelliot: умная среда IoT / Д. Д. Массеров, Д. А. Массеров // Отходы и ресурсы. — 2023. — Т. 10. — № 2. — URL: <https://resources.today/PDF/02INOR223.pdf> DOI: 10.15862/02INOR223

**For citation:**

Masserov D.D., Masserov D.A. Intelliot: a smart IoT environment. *Russian Journal of Resources, Conservation and Recycling*. 2023; 10(2): 02INOR223. Available at: <https://resources.today/PDF/02INOR223.pdf>. (In Russ., abstract in Eng.) DOI: 10.15862/02INOR223

УДК 004.896

### Массеров Даниил Дмитриевич

ФГБОУ ВО «Национальный исследовательский Мордовский государственный университет имени Н.П. Огарёва», Саранск, Россия

E-mail: [masserovggg@gmail.com](mailto:masserovggg@gmail.com)

ORCID: <https://orcid.org/0009-0000-0966-4100>

РИНЦ: [https://elibrary.ru/author\\_profile.asp?id=1161754](https://elibrary.ru/author_profile.asp?id=1161754)

### Массеров Дмитрий Александрович

ФГБОУ ВО «Национальный исследовательский Мордовский государственный университет имени Н.П. Огарёва», Саранск, Россия

Институт геоинформационных технологий и географии

Заместитель директора по научной, инновационной и международной деятельности

Кандидат экономических наук, доцент

E-mail: [masserow@yandex.ru](mailto:masserow@yandex.ru)

ORCID: <https://orcid.org/0000-0002-5076-2818>

РИНЦ: [https://elibrary.ru/author\\_profile.asp?id=675663](https://elibrary.ru/author_profile.asp?id=675663)

SCOPUS: <https://www.scopus.com/authid/detail.url?authorId=57225148227>

## Intelliot: умная среда IoT

**Аннотация.** В статье рассматриваются классические системы IoT, ориентированные на облако и обычно сосредоточенные на централизованной платформе IoT, куда загружаются данные для дальнейшей обработки. Показаны приложения IoT следующего поколения, включающие в себя такие технологии, как искусственный интеллект, дополненная реальность и распределенный реестр, чтобы реализовать полуавтономное поведение транспортных средств, руководство для пользователей и взаимодействие между машинами в доверенной манере. Подчеркивается, что такие приложения требуют более динамичных сред IoT, которые могут работать локально без необходимости связи с облаком. В данной статье описывается три варианта использования приложений IoT следующего поколения — в сельском хозяйстве (автономное управление парками сельскохозяйственных машин), здравоохранении (IoT для удаленного мониторинга пациентов) и промышленности (автономное взаимодействие производственных машин). Авторы выделили пять основных групп компонентов высокоуровневого вида логической архитектуры IntellIoT, которая включает в себя пять необходимых компонентов для решения выявленных проблем и позволяющая разрабатывать приложения следующего поколения IoT. В качестве опорных были приняты три ключевые концепции (Collaborative IoT, Human-in-the-loop и Trustworthiness), занимающие важное место в архитектуре IntellIoT. Авторами представлены текущие исследования по ключевым факторам для реализации концепции IoT нового поколения (подход IntellIoT) и выделены связанные с

ними исследовательские задачи для будущих исследований распределенных, самоуправляемых, полуавтономных приложений IoT в НИТЛ. В статье обозначены перспективы дальнейшей работы для повышения эффективности и надежности вычислительной и коммуникационной инфраструктуры.

**Ключевые слова:** интернет вещей; искусственный интеллект; технологии распределенного реестра; устройство; приложение; автономные системы; человеко-компьютерное взаимодействие

## Введение

В современных системах Интернета вещей (IoT) облачные платформы, как правило, являются центральными точками сбора и обработки данных. Однако эта модель IoT, ориентированная на облако, имеет свои ограничения [1–4]: ненадежное облачное соединение препятствует надежной работе сквозных приложений, ограниченная пропускная способность ограничивает объем обрабатываемых данных, большое время обхода препятствует работе в режиме реального времени, высокая стоимость транспортировки и приема данных, а также проблемы конфиденциальности и доверия. Более того, типичная иерархическая структура облачных платформ IoT препятствует использованию приложений с динамически меняющимся контекстом из-за недостаточной информированности отдельных подсистем и системы в целом насчет самих себя.

Для создания приложений IoT следующего поколения эти проблемы могут быть решены с помощью локализованных сред IoT, состоящих из гетерогенных устройств (например, периферийных устройств, а также девайсов с ограниченными ресурсами), которые могут совместно выполнять полуавтономные приложения IoT, включающие функции обнаружения, действия, рассуждения и управления. Однако, поскольку IoT-приложения не могут быть полностью автономными в своих решениях и действиях, им необходим человек для управления и оптимизации работы их искусственного интеллекта (ИИ).

В данной статье мы рассматриваем исследовательские задачи на основе трех ключевых классов приложений IoT следующего поколения: (1) полуавтономное управление парком сельскохозяйственных машин (например, тракторов) в сочетании со вспомогательными устройствами (например, дронами), (2) пациенты, получающие полуавтономное руководство от искусственных «докторов» на основе данных, полученных от устройств IoT и (3) полуавтономное межмашинное взаимодействие на промышленных предприятиях (например, роботизированные руки и механизмы). Во всех трех областях применения человек-эксперт играет ключевую роль в управлении, мониторинге и обучении автономных систем с поддержкой ИИ.

Целью исследования является разработка и анализ моделей компонентов программного и информационного обеспечения для формирования и реализации архитектуры высокого уровня IntelliIoT.

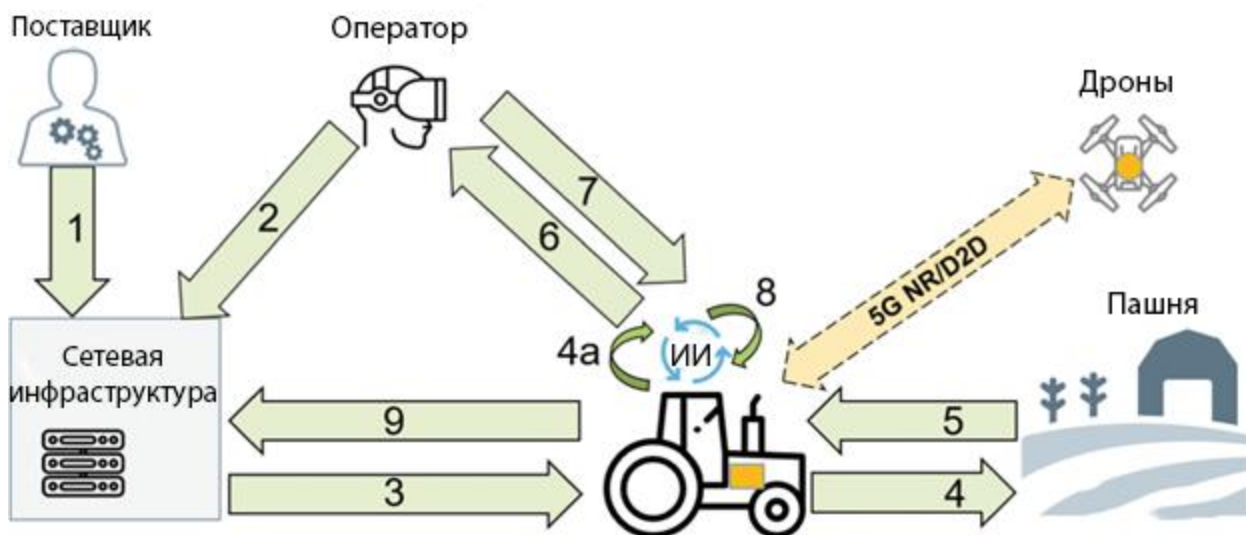
## Методология

Решение задачи осуществляется различными методами, в том числе, с использованием элементов системного и сравнительного анализа архитектур систем для создания приложений IoT следующего поколения, объектно-ориентированного моделирования информационных систем, а также проектирования баз данных (БД) с применением распределенного реестра.

## Результаты

В связи с многообразием вариантов использования IoT следующего поколения, мы выбрали три показательных случая.

*Автономное управление парками сельскохозяйственных машин.* На рисунке 1 описан пример использования полуавтономного парка сельскохозяйственных машин. Этот вариант использования подразумевает предоставление новых функциональных возможностей (например, реализации алгоритмов ИИ) для приложений IoT поставщиками (производителями тракторов) на этапе (1). Человек-оператор (фермер или руководство сельскохозяйственного парка) определяет цель для автономной деятельности (вспахивание или опрыскивание определенного сельскохозяйственного поля) трактора в сетевой инфраструктуре, как показано на шаге (2). На основе определенной цели составляется план внедрения приложения IoT и запускается развертывание необходимых функций на задействованных устройствах, например, тракторе или дронах, как показано на этапе (3). Далее развернутый ИИ управляет задействованными транспортными средствами, что включает в себя устранение заторов или других неблагоприятных событий с помощью датчиков транспортного средства (например, камер или LIDAR) на этапе (4). Этому может способствовать сканирование окружающей среды несколькими соседними автомашинами для федеративного обучения их моделей и более быстрой и надежной идентификации объектов. Полученные данные также могут служить в качестве обучающей базы данных для постоянного совершенствования базовых моделей ИИ.



**Рисунок 1.** Вариант использования нового поколения IoT в сельском хозяйстве с поддержкой IntelliIoT (составлено авторами)

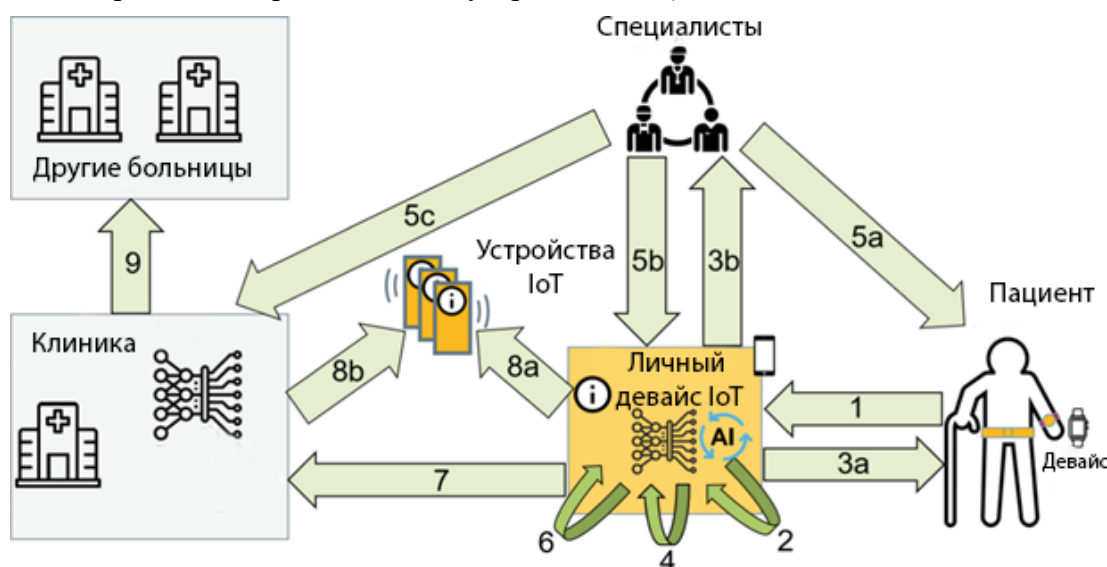
Если обнаружено препятствие и трактор не может определить, как его объехать (шаг 5), то управление трактором передается человеку-оператору (шаг 6). Данные с камер и датчиков передаются человеку-оператору, который может использовать технологию AR/VR, чтобы иметь объемное представление о ситуации. Для шага (7) необходимы как прямые, так и косвенные стратегии передачи дистанционного управления: Прямое взаимодействие с трактором (т. е. дистанционное управление транспортным средством) требует надежного и высокоскоростного соединения, обеспечивающего взаимодействие между оператором и трактором в режиме реального времени. Косвенное управление с помощью VR-инструментов направлено на определение целесообразной траектории вокруг трактора, и управление передается трактору, в то время как человек-оператор удаленно контролирует трактор, пока он правильно проходит по вновь определенной траектории. На основе данных, полученных от человека-оператора, транспортное средство может совершенствовать свои модели ИИ,

постоянно обучаясь (шаг 8) тому, как преодолевать такие препятствия в будущем, а также потенциально делиться полученной моделью с другими транспортными средствами.

В будущем поставщики услуг также будут предлагать такие полуавтономные автомобили (например, для оказания фермерских услуг). Затем необходимо заключить договорные соглашения с использованием технологии распределенного реестра (DLT). Эта информация будет являться цифровым доказательством того, что владелец поля санкционировал запрашиваемые услуги и территорию, на которой работает умное оборудование. Хранение выполненных сельскохозяйственных работ в DLT в качестве исторического свидетельства (шаг 9) может быть затем использовано в бизнес-моделях.

*IoT для удаленного мониторинга пациентов.* Достижения в области ИИ и систем с поддержкой IoT могут привести к значительным преимуществам в здравоохранении, позволяя врачам эффективно улучшать результаты, безопасность и комфорт пациентов, например, используя новые технологии для дистанционного руководства своими пациентами в процессе восстановления и реабилитации на дому. Это решение позволяет пациентам сосредоточиться на своем выздоровлении, давая им уверенность в том, что они в безопасности, что инструменты могут поддерживать и информировать их на протяжении всего пути, и что их врачи всегда в курсе событий, когда это необходимо.

На рисунке 2 описана система, которая использует входные данные устройств IoT для предоставления клиническим экспертам точной информации о состоянии здоровья их пациентов и предоставляет пациентам рекомендации и вмешательства с помощью ИИ под контролем клинических экспертов. Пациенты оснащены носимыми сенсорными устройствами, измеряющими соответствующие данные, которые передаются на персональное IoT-устройство (например, умные часы) (шаг 1). ИИ на борту этого IoT-устройства анализирует данные на этапе (2), чтобы определить необходимость вмешательства или рекомендаций в соответствии с исходной моделью ИИ и рабочими процессами вмешательства, ранее определенными в качестве целей врачами, отвечающими за пациента. Модель применяется к собранным данным, и когда обнаруживается необходимость вмешательства, пациенту отправляется либо рекомендация (шаг 3а), либо привлекается врач (шаг 3б). Таким образом, обмен данными, соответствующий требованиям конфиденциальности и безопасности, имеет решающее значение. Система может далее реализовать модель для мониторинга и диагностики технических проблем с ограниченными устройствами (шаг 4).

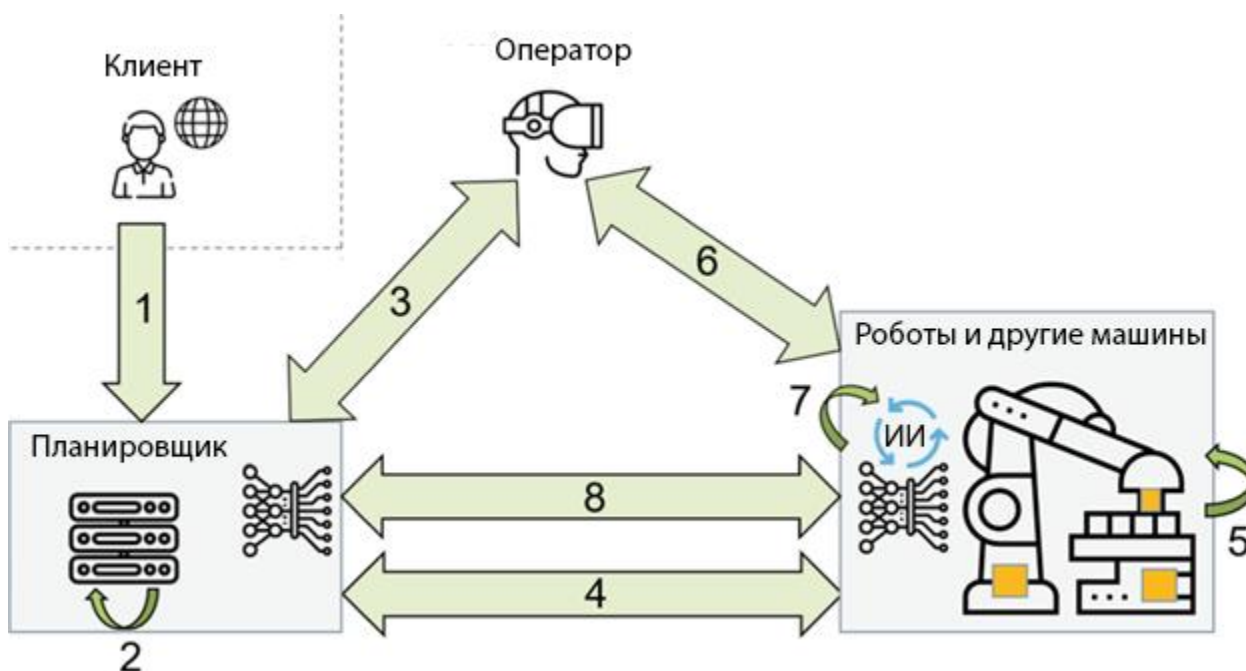


**Рисунок 2.** Вариант использования IoT в здравоохранении с поддержкой IntelliIoT (составлено авторами)



В решении IntelliIoT, когда происходит ухудшение состояния и оповещается медицинский специалист, врач может принять решение связаться с пациентом, как показано на рисунке (шаг 5a), ответить персональному устройству (шаг 5b) или поднять тревогу (шаг 5c). Врач предоставляет обратную связь, которая используется для проверки и повторного обучения модели ИИ локально на персональном IoT-устройстве (шаг 6). Затем обновления модели вносятся в агрегированную модель на пограничной инфраструктуре (например, в больнице) (шаг 7). Этот распределенный ИИ может быть реализован с помощью федеративного обучения, и обновление модели передается всем IoT-устройствам либо по принципу «устройство-устройство» (шаг 8a), либо через распространение агрегированной модели (шаг 8b). Кроме того, федеративное обучение может проводиться между больницами (шаг 9). Все эти коммуникации и взаимодействия должны быть обеспечены современными средствами безопасности и конфиденциальности, учитывающими все тонкости частных пользовательских данных.

*Автономное взаимодействие производственных машин.* Данный пример использования (рис. 3) описывает пример межмашинного взаимодействия. Клиент совместного производственного предприятия заказывает продукт, указывая цель производства (шаг 1). На шаге (2) определяется организация работы оборудования и соответствующий план процесса для производства желаемого продукта из заготовки. Планировщик процесса на основе событий отслеживает алгоритм производства и реагирует при изменении состояния «здоровья» машины. Если планировщик процесса не может самостоятельно найти решение производственной задачи (шаг 3), он может запросить поддержку у человека-оператора или заказчика. На этапе (4) роботу или автоматически управляемому транспортному средству (AGV) поручается транспортировка заготовки на следующий этап производства, а данные о производственном процессе отправляются на задействованные машины. Поскольку эти машины могут управляться владельцем завода или сторонним оператором, необходимо заключить договорные соглашения, для чего используется распределенный реестр. Кроме того, для обеспечения конфиденциальности и безопасности данных клиентов применяются комплексные механизмы безопасности.



**Рисунок 3.** Вариант использования IoT  
в производстве с поддержкой IntelliIoT (составлено авторами)

На этапе (5) локальный ИИ на борту робота решает, как робот выбирает заготовку и помещает ее в следующий станок. Если уровень уверенности локального ИИ низок, и он не может подобрать и разместить заготовку, он может снова запросить поддержку у человека-оператора или владельца станка (шаг 6). Используя технологию AR/VR, человек может виртуально захватить заготовку, чтобы поддержать робота. Для такого взаимодействия необходимо установить тактильную связь с учетом требований безопасности и конфиденциальности. Кроме того, 3D-камеры могут быть использованы для создания достаточно точной реконструкции окружающей обстановки и самого робота, что позволяет полностью контролировать и получать визуальную информацию о параметрах робота. Для захвата и тактильной обратной связи с пользователем необходимы специальные устройства ввода (например, стилус или перчатка). Если необходима поддержка удаленного оператора, тактильная связь может быть невозможна через интернет на большом расстоянии. Следовательно, оператор сможет управлять виртуальным роботом, визуализированным в локальном крае, с задержкой движения реального робота. После того как человек управляет заготовкой, локальный ИИ на роботе переобучается (шаг 7) и делегирует изученные параметры процесса другим роботам (шаг 8).

*Концепция IoT нового поколения: подход IntelliIoT.* Анализируя приведенные выше примеры использования, можно экстраполировать модель приложений следующего поколения IoT: приложения IoT обычно состоят из множества гетерогенных устройств, которые обладают свойством полуавтономного взаимодействия с помощью ИИ. Пользователи взаимодействуют с системой для предоставления знаний и тем самым могут (пере)обучать ИИ. Взаимодействие между устройствами и с пользователем может происходить тактильно, с низкой задержкой и высокой пропускной способностью.

Комплексное решение вышеперечисленных задач является движущей силой проекта IntelliIoT. Он направлен на разработку структуры для управления интеллектуальными средами IoT и их приложениями IoT, которая реализуется с помощью архитектуры, состоящей из трех строительных блоков (рис. 4): (а) распределенные, самосознательные и полуавтономные приложения IoT; (б) human-in-the-loop (HITL) для определения и поддержки автономности в (а) и (в) эффективная, надежная и заслуживающая доверия вычислительная и коммуникационная инфраструктура, обеспечивающая (а) и (б).



**Рисунок 4.** Концепция IntelliIoT для создания интеллектуальных сред IoT (составлено авторами)

Автономные программные агенты новой системы на основе гипермедиа (HyperMAS) [5] выполняют приложения IoT. Доступ к агентам и функциям предоставляется через стандартизированные интерфейсы, которые размещаются на IoT или краевых устройствах, например, на основе спецификаций W3C Web of Things [6]. Используя эти функции в качестве строительных блоков, программные агенты могут автономно создавать распределенные приложения IoT и выполнять эти приложения, гибко реагируя на динамику среды. Для дальнейшего упрощения разработки приложений IoT поддерживается совместимость с помощью компонентов, способных передавать данные между коммуникационными технологиями, протоколами и словарями. Программные агенты обладают самосознанием и наблюдают друг за другом для обнаружения и автономного устранения сбоев в работе.

Human-in-the-loop предоставляет информацию для среды IoT и поэтому имеет самое большое значение для системы: Во время проектирования человек определяет цели и требования. Затем механизм автоматически выводит и переводит рабочий процесс IoT-приложения во взаимодействие IoT/краевых устройств с соответствующими сетевыми ограничениями. Во время работы человек наблюдает за автономным поведением с поддержкой ИИ и предоставляет свои данные [7] для его улучшения. Для этого человеку необходимо использовать тактильное взаимодействие через AR/VR, чтобы уточнить модель и избежать блокировок, например, обучая промышленного робота, как обращаться с продуктом.

Умные IoT-среды должны работать на основе коммуникационной и вычислительной инфраструктуры, способной гибко поддерживать возможности, описанные выше, при этом необходимо эффективно управлять устройствами IoT с ограниченными ресурсами и более мощными пограничными ресурсами, интегрируя облачные сервисы, а также поддерживая сложные, затратные вычисления (например, выводы/обучение ИИ, а также AR-рендеринг). Пограничные ресурсы будут разнообразными [8], например, пограничные вычисления с множественным доступом (MEC), предлагаемые функциями 5G, или промышленные пограничные ресурсы, предлагаемые сетевыми вычислительными устройствами на производственных предприятиях. Вычисления и связь образуют замкнутую систему, с помощью которой инфраструктура будет оптимизирована интегрированным образом (т. е. развертывание прикладных функций на ресурсах IoT/edge должно быть оптимизировано с учетом ограничений сети, а сеть должна динамически управляться и реконфигурироваться для оптимального обслуживания приложений и устройств IoT/edge). Инфраструктура будет обеспечивать сверхнадежную связь с низкой задержкой благодаря динамическому управлению сетью, используя гетерогенные сетевые технологии (например, 5G NR, NB-IoT или D2D [9]). Беспроводной фронт-энд будет специально разработан для поддержки коммуникационных требований передовых технологий, таких как DLT и федеративное обучение.

Интегрируя вышеуказанные концепции, был получен высокоуровневый вид логической архитектуры IntellIoT. Три выделенные ключевые концепции (т. е. Collaborative IoT, Human-in-the-loop и Trustworthiness) занимают важное место в архитектуре.

Всего было выделено пять основных групп компонентов, а отдельные компоненты входят в одну из следующих групп:

- Совместные факторы IoT. Компоненты, сфокусированные на сотрудничестве различных полуавтономных субъектов для работы приложений IoT.
- Факторы human-in-the-loop. Компоненты, фокусирующиеся на вовлечении человека в процесс; например, для решения сложных ситуаций.
- Факторы доверия. Компоненты, которые фокусируются на конфиденциальности, безопасности и, в конечном итоге, на создании доверия в рамках IntellIoT.

- Управление инфраструктурой. Вычислительная и коммуникационная инфраструктура и ее возможности управления, позволяющие развертывать и управлять периферийными приложениями.
- Применение в конкретных случаях. Компоненты, специфичные для конкретного случая использования, такие как периферийные устройства и приложения IoT.

### Обсуждение

Для реализации своего видения IntellIoT улучшает уровень техники в смежных областях исследований. Приложения IoT следующего поколения требуют смены парадигмы от классического ML к распределенному, быстрому и надежному ML на периферии беспроводной сети [10]. Федеративное обучение (FL) — это децентрализованный метод обучения, при котором частные конфиденциальные сведения обучающие данные распределяются между субъектами обучения [11]. Далее, они обмениваются своими локальными моделями, а не обучающими данными, что позволяет сократить время ожидания связи во время машинного обучения. Однако влияние различных алгоритмов ML в реальных приложениях является открытой областью исследований.

IoT-приложения перемещаются из облака на периферию, чтобы вычисления происходили в непосредственной близости от производителей и потребителей данных [8]. Соответствующие решения включают такие концепции, как туманные вычисления или вычисления на границе с множественным доступом (MEC), где вычислительные ресурсы являются частью сети 5G. Это потенциально может решить проблемы, связанные с требованиями к времени отклика, ограничением срока службы батареи, экономией затрат на пропускную способность, безопасностью и конфиденциальностью (например, [4]). В приложениях NG IoT ключевой проблемой для вычислительной инфраструктуры является принятие решения о том, какой вычислительный ресурс использовать для выполнения конкретной рабочей нагрузки (например, для выполнения алгоритма искусственного интеллекта). Существует множество существующих стратегий распределения ресурсов, например, [12], которые оптимизируют различные показатели производительности, например, время отклика, пропускную способность, доступность или энергопотребление. Поэтому необходимы компоненты для расширенного, динамического управления ресурсами, которые могут гибко применяться в различных частных пограничных средах. IntellIoT разрабатывает механизм для оптимизированного распределения рабочих нагрузок между вычислительными ресурсами (т.е. сопоставление приложений IoT с устройствами). Он состоит из гибкой алгоритмической структуры, основанной на предыдущей работе [13] и настраиваемой на различные критерии оптимальности во время выполнения. Кроме того, она должна динамически адаптироваться к изменениям в сети на основе высокоуровневых требований приложений, т.е. обеспечивать управление инфраструктурой по замкнутому циклу.

В то время как устройства IoT/edge могут обеспечивать вычислительную часть инфраструктуры, коммуникационная часть должна управляться передовыми сетевыми технологиями, такими как 5G New Radio (NR) и его расширения для частных сетей и Industrial IoT. Кроме того, 5G eV2X, как полная переработка LTE V2X, может сыграть свою роль для совместной автоматизированной мобильности и «боковой связи» между устройствами (D2D) [9], например, между роботами и машинами. Для «тактильных» линий связи основной задачей является разработка коммуникационной структуры на основе управления для передачи в реальном времени тактильной информации (прикосновения, движения и т. д.) в дополнение к обычному аудиовизуальному и информационному трафику. Предлагаемые решения должны обеспечивать эффективное использование спектра [14] в нисходящем канале связи, с



массивной сенсорной обратной связью в восходящем канале связи, ориентируясь на 1 мс в нисходящем канале связи, 10 мс в восходящем канале связи с 99,99 % доступностью. Для поддержки сверхнадежной связи с низкой задержкой (URLL) в направлении TSN для 5G Industrial IoT исследуется 5G mmWave радио (с оптоволоконной скоростью передачи данных, реактивностью в реальном времени и большой сенсорной емкостью) [15], а также поддержка IEEE TSN. Что касается поддержки распределенных сетей, функции для планирования ad-hoc возможностей для улучшенной D2D связи не включают в себя конкретный планировщик, поэтому IntellIoT разрабатывает беспроводной планировщик D2D класса TSN, обеспечивающий детерминированное QoS для децентрализованных вычислений в контексте IoT.

Опираясь на вычислительную и коммуникационную инфраструктуру, артефакты IoT должны иметь возможность обнаруживать и взаимодействовать друг с другом. Первым крупным шагом на пути к этой цели стал Web of Things (WoT) [6], где взаимодействие между устройствами основано на архитектуре Web. Однако, что очень важно, взаимодействие на семантическом уровне является центральным требованием для будущего развития. На основе усилий W3C WoT изучаются новые способы использования гипермедиа для разработки эволюционирующих веб-интерфейсов и клиентов общего назначения. IntellIoT будет развивать эти разработки, интегрируя их с исследованиями в области многоагентных систем (MAS) для создания основанных на гипермедиа MAS (HyperMAS) [5], которые вертикально и горизонтально масштабируются в отношении количества агентов, устройств и взаимодействия между этими компонентами. Она будет поддерживать самосознающие агенты в среде IoT и полуавтономные системы IoT.

Широкое внедрение технологий IoT во множестве областей требует рассмотрения требований безопасности, конфиденциальности и доверия на ранней стадии проектирования [16]. Даже безопасно инициализированные устройства могут быть скомпрометированы, что позволяет злоумышленникам влиять на подключенные устройства, сеть или совместные приложения. Для защиты от таких атак можно использовать механизмы, основанные на доверии, путем мониторинга поведения каждого участника. Развертывание IoT также должно обладать интеллектом для проактивной защиты, например, с помощью методов защиты движущихся целей (MTD) [17], когда управляемые искусственным интеллектом агенты периодически изменяют топологию и/или конфигурацию сети для противодействия атакам. Таким образом, оценки обеспечения безопасности для систем IoT все еще находятся в зачаточном состоянии (например, [18]). Поэтому IntellIoT обеспечивает безопасность и надежность за счет сочетания: (а) непрерывного обеспечения безопасности на основе фактических данных, включающего гибридные оценки, которые учитывают различные поверхности атак и уязвимости; (б) вычислительных механизмов на основе доверия, которые будут действовать как распределенная система обнаружения вторжений, и (в) стратегии MTD с процессами, учитывающими контекст безопасности.

Поддерживая эти механизмы безопасности и доверия, IntellIoT использует технологию распределенного реестра (DLT) для кодирования логики транзакций и политик, которые включают требования и обязательства стороны, запрашивающей доступ к ресурсу IoT, а также его поставщика [19]. Это может привести к появлению целой волны новых приложений, обеспечивающих доверенный доступ к ресурсам IoT. Таким образом, современная технология развивается в трех аспектах (на основе работы [20]): (1) обход ресурсных ограничений устройств; (2) продвижение проектов сетей IoT с преобладанием восходящего канала; (3) обеспечение совместимости с устройствами сторонних производителей. В IoT периферийный шлюз с DLT-решениями оснащен необходимым вычислительным интеллектом. Тем не менее, устройства в блокчейне должны хранить копию записи DLT, которая может быть большой и увеличиваться со временем, что ограничивает масштабируемость системы. Более

того, транзакции, связанные с умными контрактами, требуют двухстороннего коммуникационного трафика, что нарушает распространенное предположение о том, что в системах IoT преобладает восходящий трафик. IoT/устройство в сети блокчейна должно быть способно проверять информацию в блокчейне, что связано с нисходящим трафиком. Таким образом, система IntellIoT предоставляет архитектуру, которая нацелена на компромисс между сложностью устройства, достигнутым доверием и возможностями сети, а также на поддержание доверия, когда устройство принадлежит третьей стороне.

### Заключение

Основным вкладом данной статьи является анализ трех классов использования IoT следующего поколения, экстраполяция общего шаблона, представление структуры IntellIoT и постановка ключевых исследовательских задач, связанных с ней. Все три варианта использования основаны на полуавтономном поведении системы IoT. Несколько разнородных устройств взаимодействуют между собой, а автономное управление их совместной работой обеспечивается с помощью искусственного интеллекта, который может быть обучен или переобучен при вмешательстве человека. Такая схема может быть принята для многих приложений IoT.

Описанная схема охватывает три ключевых области: обеспечение распределенного искусственного интеллекта для автономного поведения, обеспечение эффективной и надежной связи вычислительных ресурсов, и включение человека (путем обеспечения доверия к системе) и обучение на основе его вклада. Описанная структура IntellIoT затрагивает все три области. Представленная высокоуровневая архитектура объединяет программные компоненты для реализации функциональных возможностей, необходимых для этих областей. Полная реализация этой архитектуры в настоящее время находится в процессе. Таким образом, обозначены ключевые исследовательские задачи, с которыми приходится сталкиваться, и описан дальнейший путь исследований для этого проекта и последующих.

### ЛИТЕРАТУРА

1. Горбунова М.В., Омётов А.Я., Комаров М.М., Беззатеев С.В. Обзор проблем внедрения технологии распределенного реестра // Информационно-управляющие системы. 2020. № 2(105). С. 10–19.
2. Жумашева С.Т., Муханова А., Смагулова Ж.Б. Цифровизация как основа инновационного потенциала аграрного производства Казахстана // Проблемы агрорынка. 2020. № 2. С. 45–52.
3. Родина А.А. Применение туманных вычислений и распределенного реестра в системах экологического мониторинга на основе IOT // Известия Тульского государственного университета. Технические науки. 2021. № 2. С. 56–61.
4. Yi, S., Hao, Z., Qin, Z., Li, Q.: Fog computing: platform and applications. In: 2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb), 2015, pp. 73–78.
5. Ciortea, A., Mayer, S., Gandon, F., Boissier, O., Ricci, A., Zimmermann, A.: A decade in Hindsight: the missing bridge between multi-agent systems and the world wide web. In: Proceedings of the 18th International Conference on Autonomous Agents and Multi Agent Systems, 2019, pp. 1659–1663.

6. Kovatsch, M., Matsukura, R., Lagally, M., Kawaguchi, T., Toumura, K., Kajimoto, K.: Web of Things (WoT) Architecture (2020). <https://www.w3.org/TR/wot-architecture/>. W3C Recommendation.
7. Holzinger, A., et al.: Interactive machine learning: experimental evidence for the human in the algorithmic loop. *App. Intell.* 49(7), 2019, pp. 2401–2414.
8. Yousefpour, A., et al.: All one needs to know about fog computing and related edge computing paradigms: a complete survey. *J. Syst. Architect.* 98, 2019, pp. 289–330.
9. Хаджиева Л.К., Хаджиев М.Р., Хашумов И.У. Перспективы внедрения технологии 5G и взаимодействие с системой "Умный дом" // Вестник ГГНТУ. Технические науки. 2021. Т. 17. № 4(26). С. 21–32.
10. Park, J., Samarakoon, S., Bennis, M., Debbah, M.: Wireless network intelligence at the edge. *Proc. IEEE* 107(11), 2019, pp. 2204–2239.
11. Konecny J., McMahan, B.H., Ramage, D., Richtarik, P. (2016) Federated optimization: Distributed machine learning for on-device intelligence. arXiv preprint arXiv: 1610.02527 <https://arxiv.org/abs/1610.02527>.
12. Cardellini, V., Grassi, V., Presti, F.L., Nardelli, M.: Optimal operator placement for distributed stream processing applications. In: *Proceedings of the 10th ACM International Conference on Distributed and Event-based Systems*, 2016, pp. 69–80.
13. Seeger, J., Broring, A., Carle, G.: Optimally self-healing IoT choreographies. *ACM Trans. Internet Technol. (TOIT)* 20(3), 2020, pp. 1–20.
14. Bennis, M., Debbah, M., Poor, H.V.: Ultrareliable and low-latency wireless communication: tail, risk, and scale. *Proc. IEEE* 106(10), 2018, pp. 1834–1853.
15. Giordani, M., Polese, M., Roy, A., Castor, D., Zorzi, M.: Initial access frameworks for 3GPP NR at mmWave frequencies. In: *2018 17th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net)*, 2018, pp. 1–8.
16. Сорокин Д.В., Бондарчук А.П., Сторчак К.П. Инфраструктура промышленных сетей ИОТ, а также киберугрозы в доступе ИОТ решениях // Телекоммуникационные и информационные технологии. 2019. № 4(65). С. 120–127.
17. Xiong, X.-L., Yang, L., Zhao, G.-S.: Effectiveness evaluation model of moving target defense based on system attack surface. *IEEE Access* 7, 2019, pp. 9998–10014.
18. Массеров, Д.А. Применение искусственного интеллекта в концепции Интернета вещей / Д.А. Массеров, Д.Д. Массеров. DOI: 10.15862/05ITOR222 // Отходы и ресурсы. 2022 № 2. URL: <https://resources.today/PDF/05ITOR222.pdf> (дата обращения: 29.01.2023).
19. Khan, M.A., Salah, K.: IoT security: review, blockchain solutions, and open challenges. *Futur. Gener. Comput. Syst.* 82, 2018, pp. 395–411.
20. Danzi, P., et al.: Communication aspects of the integration of wireless IoT devices with distributed ledger technology. *IEEE Netw.* 34(1), 2020, pp. 47–53.

### **Masserov Daniil Dmtrevch**

Ogarev Mordovia State University, Saransk, Russia  
E-mail: masserovggg@gmail.com

ORCID: <https://orcid.org/0009-0000-0966-4100>

RSCI: [https://elibrary.ru/author\\_profile.asp?id=1161754](https://elibrary.ru/author_profile.asp?id=1161754)

### **Masserov Dmitriy Alexandrovich**

Ogarev Mordovia State University, Saransk, Russia  
E-mail: masserow@yandex.ru

ORCID: <https://orcid.org/0000-0002-5076-2818>

RSCI: [https://elibrary.ru/author\\_profile.asp?id=675663](https://elibrary.ru/author_profile.asp?id=675663)

SCOPUS: <https://www.scopus.com/authid/detail.url?authorId=57225148227>

## **Intelliot: a smart IoT environment**

**Abstract.** This paper examines classic cloud-based IoT systems, typically centered on a centralized IoT platform where data is uploaded for further processing. Next-generation IoT applications are shown, incorporating technologies such as artificial intelligence, augmented reality and distributed registry to implement semi-autonomous vehicle behavior, user management and machine-to-machine interaction in a trusted manner. It is emphasized that such applications require more dynamic IoT environments that can run locally without the need to connect to the cloud. The article describes three use cases for next-generation IoT applications — in agriculture (autonomous management of fleets of agricultural machines), healthcare (IoT for remote patient monitoring) and industry (autonomous interaction between production machines). The authors identified five key component groups of a high-level representation of the IntelliIoT logic architecture, which includes the five necessary components to address the identified challenges and enable the development of next-generation IoT applications. Three key concepts (Collaborative IoT, Human-in-the-loop, and Trustworthiness) that occupy an important place in the IntelliIoT architecture were taken as benchmarks. The authors present current research on key factors for implementing the next generation IoT concept (the IntelliIoT approach) and highlight relevant research challenges for future research on distributed, self-managed, semi-autonomous IoT applications in HITL. The paper outlines prospects for future work to improve the efficiency and reliability of computing and communication infrastructure.

**Keywords:** internet of things; artificial intelligence; distributed registry technologies; device; application; autonomous systems; human-computer interaction