УДК 004.032.2:681.518.3 DOI: 10.26102/2310-6018/2020.30.3.010

Аспекты безопасного функционирования беспилотных транспортных средств в среде умного города

А.В. Абдулов, Е.А. Абдулова
Институт проблем управления им. В.А. Трапезникова РАН,
Москва, Российская Федерация

Резюме: В настоящее время беспилотные транспортные средства (БТС) для обеспечения автономной навигации в большей степени полагаются на GPS. Для реализации концепции умного города актуальным является поиск альтернативных методов локализации БТС, так как в реальных условиях сигнал GPS может либо отсутствовать, либо его точности бывает недостаточно для движения по маршруту или выполнения маневров. Следует отметить, что для внедрения технологий БТС существуют информационные проблемы: конфиденциальность и доверие, а также кибербезопасность. Поскольку в среде умного города все БТС должны быть подключены к сети, то вопросы кибербезопасности также требуют дополнительного внимания. Киберугрозы могут спровоцировать нарушения в работе как отдельных БТС, так и транспортной системы в целом. В статье выделены три категории программных систем БТС, обеспечивающих соответственно обработку данных, планирование и управление. Представлен подход к архитектуре функционирования БТС, основанной на сборе информации, принятии решений, сетевой и вычислительной многоуровневой аналитике. Для повышения уровня безопасности БТС предлагается использовать систему управления безопасностью, основанную на факторном анализе и методах расчета рисков. В части беспрепятственного движения, предлагается метод локализации БТС посредством их коммуникации на основе сетевых моделей локального позиционирования.

Ключевые слова: беспилотное транспортное средство, умный город, система управления безопасностью, архитектура функционирования, локальное позиционирование, сетевые модели

Для цитирования: Абдулов А.В., Абдулова Е.А. Аспекты безопасного функционирования беспилотных транспортных средств в среде умного города. *Моделирование, оптимизация и информационные технологии.* 2020;8(3). Доступно по: https://moit.vivt.ru/wp-content/uploads/2020/08/AbdulovAbdulova_3_20_1.pdf DOI: 10.26102/2310-6018/2020.30.3.010.

Aspects of the safe functioning of unmanned vehicles in a smart city environment

A.V. Abdulov, E.A. Abdulova
V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences,
Moscow, Russia

Abstarct: At present, unmanned vehicle (UV) to provide the accurate navigation under motion are in majority cases depended on GPS, what makes the access to the Network of importance for correct performance in the smart city environment. To implement the smart city conception, the search of alternative techniques of UV localization is vital, since in real conditions GPS signal may be either absent, or its accuracy may be found insufficient to move over a route or to implement maneuvers. One should note that there exist problems for putting in operation the UV technologies: ethical (confidentiality and trust) and cybersecurity. Since in the smart city environment all UVs are to be connected to the Network, then cybersecurity issues also require an additional attention. Cyber threats can provoke violations in both individual UVs and the transportation system as a whole. The paper emphasizes three main categories of UV program systems providing, correspondingly, sampling and processing data, planning, and control. An approach to the UV performance architecture is presented,

based on the sampling and processing data, decision making, network and computational multi-level analytics. To increase the UV security in a smart city, the paper proposes to utilize a safety management system based on the factor analysis and risks calculation techniques. To increase the UV security in the part of unobstructed motion, local positioning network models are proposed enabling to work out motion schemes.

Keywords: unmanned vehicle, smart city, functioning architecture, safety management system, local positioning, network models

For citation: Abdulov A.V., Abdulova E.A. Aspects of the safe functioning of unmanned vehicles in a smart city environment. *Modeling, Optimization and Information Technology*. 2020;8(3). Available from: https://moit.vivt.ru/wp-content/uploads/2020/08/AbdulovAbdulova_3_20_1.pdf DOI: 10.26102/2310-6018/2020.30.3.010.

Введение

В настоящее время в мире не существует единого понятия, что такое умный город. Для формирования единого понимания разрабатываются международные и национальные стандарты регулирующие базовые методы реализации концепции умного города. 13 августа 2020 года Росстандарт утвердил первые в России национальные стандарты в области создания и развития умных городов, которые начнут действовать с 2021 года.

Концепция создания умных городов предполагает эффективное управление городской инфраструктурой, в том числе в сфере транспортных услуг с применением беспилотных транспортных средств (БТС). В первую очередь это связано с мобильностью, которая имеет фундаментальное значение особенно в рамках этой концепции и позволяет не только перемещать товары, ресурсы, людей и т. д., но и способствует большему социальному взаимодействию. Использование БТС могло бы повысить безопасность дорожного движения за счет сокращения числа дорожно-транспортных происшествий, обусловленных человеческим фактором [1], а также уменьшить время пребывания в пути.

Перспективные системы автономной навигации, которые в настоящее время отсутствуют в обычных автомобилях, но являются неотъемлемой частью БТС включают сенсоры для восприятия окружающей среды, усовершенствованные алгоритмы обработки данных и принятия решений, а также срабатывания органов управления БТС с учетом внешних условий.

Все компоненты БТС в широком смысле можно разделить на модули, относящиеся к аппаратному и программному обеспечению. Компонентами аппаратного обеспечения являются сенсоры, исполнительные механизмы, а также технологии связи «транспортное средство-транспортное средство» (V2V) и «транспортное средство-инфраструктура» (V2I). Программное обеспечение включает модули, обеспечивающие интеграцию встраиваемых компонентов и необходимую обработку поступающей информации как в реальном времени, так и в фоновом режиме.

Аппаратная часть позволяет БТС видеть, общаться и двигаться. Сенсорное обеспечение БТС формирует поток данных о текущей обстановке – обнаружение светофоров и дорожных знаков, различного рода препятствий и ограждений, участков для движения других транспортных средств и пешеходов. Как правило, базовый набор датчиков БТС формируется из совокупности следующих компонентов: GPS-приемники, инерциальные измерительные модули (ИЗМ), видеокамеры, лидары, сонары и одометры. Для компенсации погрешностей показаний сенсоров для большинства БТС используется процесс «слияния», объединяющий данные от нескольких сенсоров, в том числе и разнородных. Стандартизация протоколов связи V2V и V2I позволит БТС общаться с другими участниками дорожного движения, передавать дополнительную полезную

информацию, а также управляющие команды. К исполнительным механизмам относятся приводы, отвечающие за управляемое перемещение БТС.

Выделяют три основные категории программных систем, обеспечивающих обработку данных, планирование и управление [2]. Эти категории определяют соответствующие блоки в архитектуре функционирования БТС, представленной на Рисунке 1. Система сбора и обработки данных обеспечивает способность БТС интерпретировать информацию, поступающую через сенсоры. Система планирования объединяет уже обработанные сенсорные данные с навигацией БТС и информацией из сети, полученной по каналам связи V2V/V2I, учитывая регламентированные правила и положения. И наконец, система управления преобразует цели, сформированные системой планирования, в доступные для БТС действия.

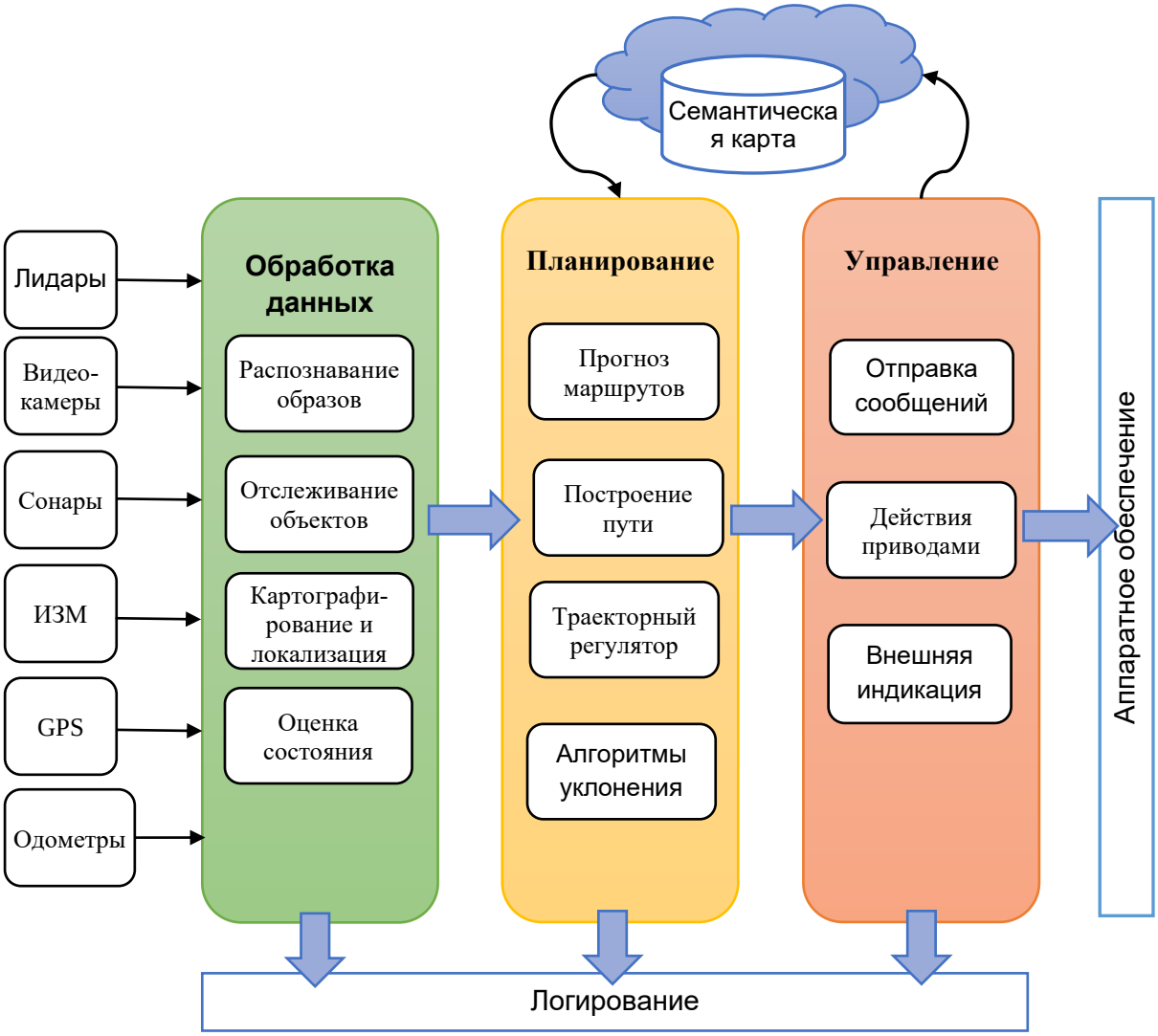

Рисунок 1 – Архитектура функционирования БТС
Figure 1 – Unmanned vehicle functioning architecture

БТС: обработка данных и планирование

Для повышения осведомленности и автономности БТС целесообразно выполнять обмен информацией не только между БТС и/или другими транспортными средствами, находящимися на дороге, но также между БТС и платформой обработки данных в

«облаке». Облачная платформа реализует два основных процесса: обработку показаний сенсоров и локализацию данных для планирования маршрута БТС. В «облаке» происходит непрерывное обновление семантической карты, которая также включает логические отношения между объектами и их свойствами в среде. В свою очередь, на основе облачных данных БТС могут корректировать текущие задачи планирования.

Блок обработки данных структурирует исходную сенсорную информацию и позволяет оценивать текущую ситуацию, создавать семантические карты и определять местоположение БТС.

Надежность работы навигационной системы напрямую зависит от достоверности данных модуля локализации. В городских условиях невозможно добиться необходимой точности локализации только с помощью инерциальных датчиков и GPS. Для создания карт окружающей среды с высоким разрешением система навигации БТС должна использовать всевозможные сенсорные данные: координаты GPS, показания ИЗМ, колесную одометрию, карты глубин с лидаров, сонаров и др. Локализация движущегося БТС на известной карте местности успешно выполняется с помощью метода фильтрации частиц [3]. Такой подход помогает повысить относительную точность определения местоположения более чем на порядок по сравнению с традиционными методами одометрии GPS-ИЗМ [4]. В системе целесообразно применять и другие методы динамического картирования городской среды, которые обеспечивают высокую точность, например, за счет одновременной локализации транспортного средства на формируемых ими картах [5, 6]. Благодаря наличию алгоритмов, позволяющих транспортному средству двигаться точно по заданной траектории, можно проводить автоматическую калибровку сенсоров [7]. Также на этом уровне функционирования БТС могут быть использованы методы обнаружения светофоров [8], пешеходов, ограждений, других транспортных средств и т. д. в реальном времени.

Блок планирования может быть представлен в виде следующих уровней: принятие решений, сетевой и вычислительная аналитика. Для корректной работы БТС на уровне принятия решений необходимы алгоритмы прогнозирования сложных динамических ситуаций, обеспечивающие безопасность и мобильность. Для построения маршрута движения БТС и его реализации необходимо: (а) определить пункт назначения, (б) использовать показания сенсоров, (в) обеспечить обмен данными с другими транспортными средствами, (г) обучать модели на исторических данных в области вождения транспортных средств, (д) обеспечить надежность и безопасность процесса принятия решения, и (е) управлять мобильностью на основе координации с другими транспортными средствами [9, 10].

На сетевом уровне используются технологии интернета вещей (IoT) для выполнения устройствами задач без вмешательства человека. БТС с интернетом вещей получает совокупность дополнительных интеллектуальных функций и опций, обеспечиваемых сервисами IoT. В основе этих функций лежит иерархия автономного вождения. При этом возможность принимать решение независимо от центра управления сохраняется. Подключенные к IoT БТС используют это соединение для обновления алгоритмов, обмена друг с другом информацией о дороге и т. п. Общая информация состоит из пути к пункту назначения, трафика и навигации. Вся эта информация распределяется между транспортными средствами, подключенными к IoT, и загружается в облачную систему по беспроводной сети для дальнейшего анализа и улучшения алгоритмов функционирования (см. Рисунок 2).

На уровне вычислительной аналитики выполняется переработка сенсорной информации БТС. Для сбора всех структурированных данных создается специальное облачное хранилище. Главным образом здесь сохраняются данные о вождении, что

позволяет в дальнейшем переобучать модели для улучшения качества управления БТС на основе методов искусственного интеллекта. Поскольку БТС находится в движении, а ему необходима актуальная информация о своем окружении, при этом время анализа сенсорных данных и скорость передачи данных ограничены, то обработка части данных может происходить в зоне граничных вычислений. Необходимость быстрого реагирования в процессе принятия решений усложняет задачу управления [11], что в свою очередь предъявляет высокие требования к серверам граничных вычислений.

Рисунок 2 – Информационные потоки: IoT – облако
Figure 2 – Information flows: IoT – cloud

Проблемы внедрения БТС

БТС могут улучшить качество городской жизни за счет повышения безопасности участников движения. Но существуют информационные проблемы, препятствующие внедрению соответствующих технологий, такие как конфиденциальность, доверие и кибербезопасность.

Конфиденциальность может стать серьезной проблемой, если в процессе принятия решений будет учтена информация, относящаяся непосредственно к людям. Например, получение визуальной информации от датчиков обнаружения препятствий может привести к вторжению в личную жизнь. Визуальные датчики могут записывать и сообщать данные о людях, которые были замечены перед транспортным средством, и таким образом, информация об этих людях может распространяться без их согласия. С точки зрения конфиденциальности необходимо учитывать следующие факторы: объем данных для сбора, доступ к собранным данным и момент времени, когда собранные данные больше не нужны и должны быть уничтожены.

Проблема доверия возникает как в аппаратных, так и в программных компонентах транспортных средств при сборке и имеет важное значение на этапе его использования. БТС должен принимать решение – как добраться до пункта назначения, соблюдая установленные правила. Для решения этой задачи необходимо обеспечить БТС модулем

верификации и валидации источников и самих данных. Например, этот модуль должен выявлять подмену GPS сигнала, искажение карт местности и т. п.

БТС связаны с собственными рисками и проблемами безопасности. Подключение к Интернету и другим технологиям открывает уязвимости системы и дает возможность «нарушителям» возможность изучить уязвимости и получить в дальнейшем доступ к компьютерной системе БТС и, следовательно, удаленно управлять им. В связи с этим, необходимо проводить всесторонний анализ безопасности и рассматривать возможные атаки на вычислительные ресурсы БТС [12].

Управление и устранение рисков конфиденциальности и кибербезопасности значительно влияет на успешность применения БТС. Проблемы конфиденциальности связаны с вероятностью передачи личных данных, которая может нарушать законы о конфиденциальности данных и создавать неопределенность в хранении, владении и передаче информации. Сетевое подключение БТС должно быть защищено от взлома для обеспечения безопасного функционирования БТС.

Безопасность и надежность функционирования БТС зависят от непрерывной беспроводной связи с внешней сетью, что увеличивает риск взлома. Подобные инциденты уже были описаны в литературе, например, подавление сигнала GPS, взлом сенсоров и карт местности для искажения восприятия, взлом беспроводной системы записи данных о событиях и направление атак типа отказа в обслуживании (DoS) для блокировки доставки критической информации [13-15].

Транспортная инфраструктура является объектом критической информационной инфраструктуры (КИИ), в свою очередь, БТС относятся к транспортной инфраструктуре и, следовательно, участвуют в формировании КИИ, а кибербезопасность БТС оказывает сильное влияние на общество. Открытость БТС для Интернета увеличивает киберугрозы для КИИ и такое воздействие может повлиять на благополучие общества в целом, поставив под угрозу целостность и доступность данных (например, может вызвать в будущем аварийные ситуации и нарушения движения) [16, 17].

Система управления безопасностью

Умные города являются удачной концепцией, основанной на создании сетей, связывающих между собой различные сущности (физические сущности, людей, управляющие сервера, сенсоры, датчики и т. д.) и относящихся к критической информационной инфраструктуре, и если в них внедрять технологии без учета безопасности, то возникающие проблемы безопасности могут быть более серьезными, чем те, которые связаны с кибербезопасностью других КИИ.

Одним из основных приоритетов развития БТС является повышение уровня безопасности, в том числе информационной и кибернетической. Но из-за увеличения различных угроз, связанных с совершенствованием информационных технологий, применения традиционных подходов для снижения риска до приемлемого уровня недостаточно. Системные причины многих инцидентов, связанных с несанкционированным доступом к системам управления, привели к значительному увеличению интереса к процедурам идентификации и управления рисками, а также к разработке и развитию систем управления безопасностью [18-20], которые характеризуются системностью, проактивностью и ясностью, а также на различных методах оценки риска [21, 22].

Функционирование системы управления безопасностью БТС должно представлять собой замкнутый цикл последовательно выполняемых операций: определение фактора риска, оценка степени опасности выявленных факторов риска, разработка вариантов локализации факторов риска, информирование органов

управления и поддержки принятия решений, а также анализ эффективности принятых мер. На Рисунке 3 представлена разработанная схема оценки безопасности на основе факторного анализа, в которой используется методика PDCA (цикл Шухарта-Деминга) для постоянного повышения безопасности.

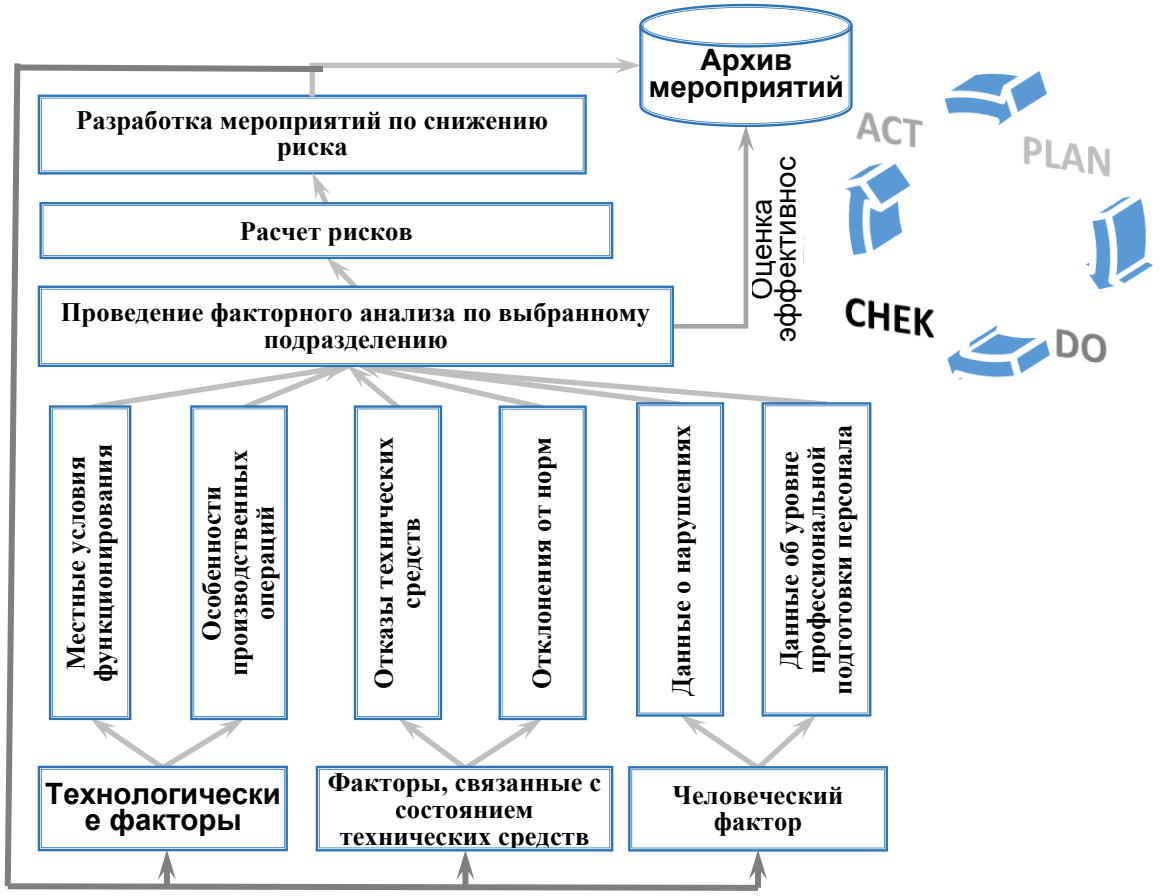

Рисунок 3 – Модель процесса управления рисками
Figure 3 – Risk management process model

Сетевые модели локального позиционирования

Для безопасного движения БТС должны отрабатывать схемы управления, способствующие избеганию столкновений. Для этого в условиях децентрализованной организации движения всем БТС целесообразно формировать модели наблюдаемых препятствий, учитывая динамические характеристики подвижных объектов (других транспортных средств, пешеходов и т. п.). Точность определения параметров модели напрямую связана с вероятностью столкновения.

Стоит отметить, что в реальном масштабе времени не всегда возможно точно определить местоположение и динамику других участников движения непосредственно с помощью бортовой вычислительной аппаратуры. Как правило, все участники движения заинтересованы в минимизации числа столкновений, поэтому при наличии каналов связи им следует обмениваться друг с другом полезной информацией. Таким образом, информационный обмен может стать одним из ключевых факторов в поиске безопасных траекторий движения.

Рассмотрим случай движения БТС в «толпе» с возможностью коммуникации друг с другом. Пусть БТС оснащены только дальномерами, позволяющими оценить расстояния до препятствий (например, многолучевой лидар), и модулями беспроводной

связи (например, Wi-Fi) для обмена сообщениями. Предполагается, что радиус действия модуля беспроводной связи сопоставим с габаритами БТС и его скоростными характеристиками, чтобы была возможность заблаговременно получать из сети полезную информацию от других участников.

Все БТС имеют возможность строить свою локальную карту наблюдаемых объектов, передавать ее другим участникам сети и получать их карты препятствий. Для двумерного случая, локальная карта препятствий (см. Рисунок 4) состоит из списка пар {p, s}, где p = (d, a) – относительное положение наблюдаемого препятствия (удаленного на расстояние d и смещенного на угол a от курса наблюдателя) и s – вектор его состояния (габариты, планируемая траектория и др.). В общем случае для каждого БТС есть N наблюдаемых объектов и M полученных сообщений от участников сети.

Возникает проблема определения местоположения отправителя сообщения на локальной карте препятствий. Частично эту неопределенность можно сократить, решая для БТС задачу локального позиционирования с учетом следующего положения: расстояние между наблюдающими друг друга участниками движения одинаково.

Задача локального позиционирования заключается в определении относительного местоположения и параметров движения различных объектов. Особенностью задачи является отсутствие «маяков» общего назначения, относительно которых могли бы ориентироваться все участники движения. Когда несколько БТС объединены каналами связи для коммуникации можно разрабатывать и применять сетевые модели локального позиционирования [23] на основе известных подходов, таких как триангуляция, трилатерация и навигационное счисление [24].

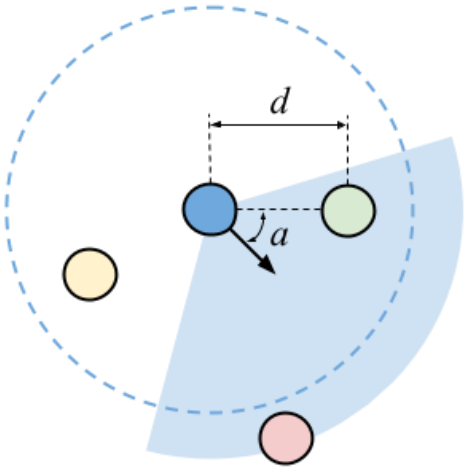

Рисунок 4 – Локальная карта препятствий
Figure 4 – Local map of obstacles

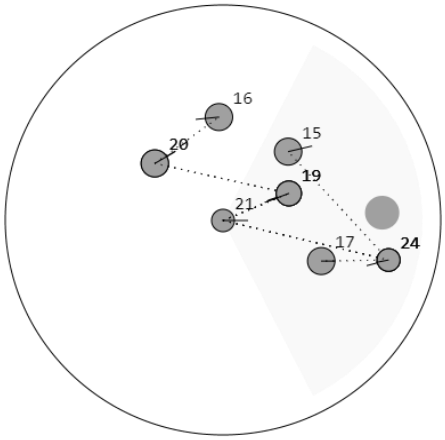

Рисунок 5 – Расширенная карта препятствий
Figure 5 – Extended map of obstacles

Если для БТС будет установлена связь сетевых адресов с их пространственными координатами путем сопоставления относительных взаимоположений, то по цепочке можно расширять исходную карту препятствий дополнительной информацией. Пример графа препятствий изображен на Рисунке 5. В случае успешного расширения своих локальных карт препятствий БТС смогут воспользоваться полученными из сети данными о векторах состояний других участников движения. Можно сказать, такая сетевая модель локального позиционирования позволяет повышать осведомленность участников движения без единого центра регулирования. Этот подход будет работать как в сетях с централизованными точками доступа, так и в распределенных самоорганизующихся mesh-сетях [25].

Для оценки эффективности фактора коммуникации и минимизации столкновений были проведены имитационные эксперименты на основе разработанного программного симулятора. На Рисунке 6 представлена сцена с движением по встречным потокам. Модель БТС с заданной частотой основного цикла строит свою локальную карту, отправляет свои данные в сеть, получает информацию о других из сети, анализирует обстановку и выбирает наиболее безопасное управление (см. Рисунок 7), приближающее к цели на основе расширенной карты препятствий. Результаты имитационного моделирования отображены на Рисунке 8. Полученные графики подтверждают эффективность предложенного подхода – разработанная модель позволяет существенно сократить число столкновений при движении по нерегулируемым встречным потокам.

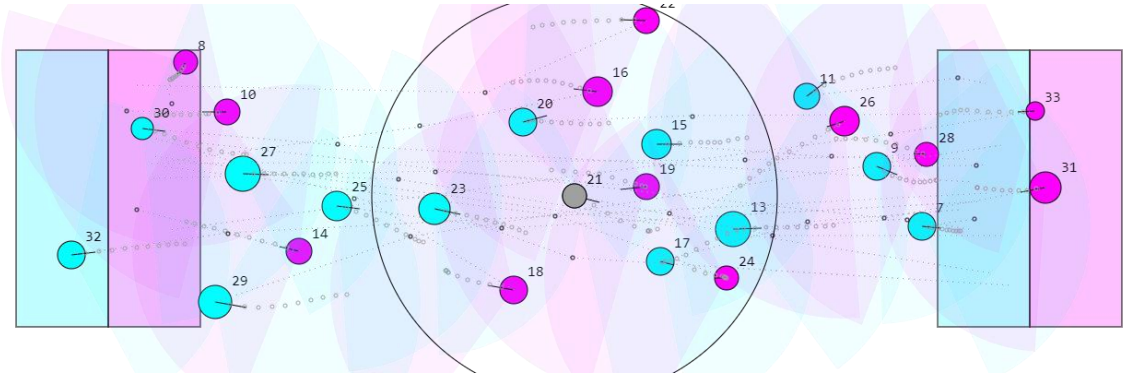

Рисунок 6 – Пример сцены из симулятора
Figure 6 – Example of a scene from the simulator

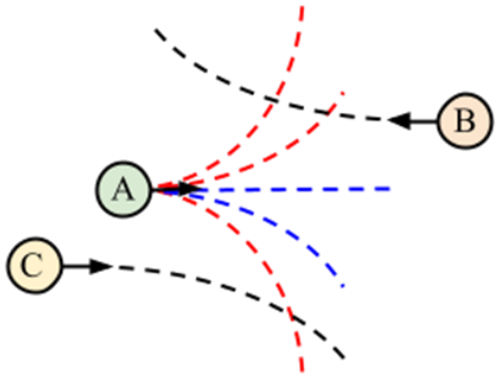

Рисунок 7 – Выбор безопасной траектории
Figure 7 – Choosing a safe path

Серия экспериментов T0 с минимальным числом средних столкновений на одного участника движения соответствует случаю полной осведомленности (как при централизованном подходе). Столкновения происходили лишь в редких случаях, когда динамика объектов не позволяла им уклоняться друг от друга. График T1 с худшими показателями построен на основе результатов серии экспериментов без коммуникации. Участники движения формировали свои траектории только на основе своих дальномеров, а все наблюдаемые препятствия считались неподвижными. Предложенный метод T2 приближает участников движения к условиям полной осведомленности.

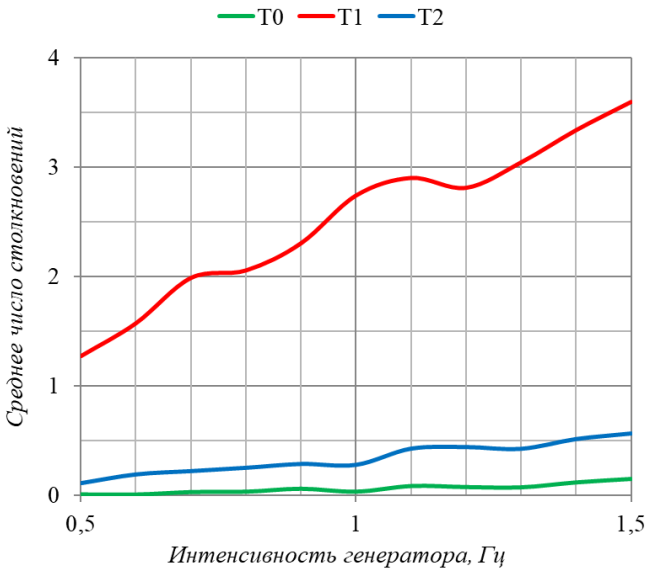

Рисунок 8 – Результаты экспериментов
Figure 8 – Simulation results

Заключение

Умный город стратегически подходит к развитию транспорта. Транспортная инфраструктура становится интеллектуальной. Тенденция к использованию динамической и мультимодальной информации заметна в управлении городской логистикой. Большие данные собираются с сенсоров БТС, камер безопасности, меток RFID и т. д. Особое место в транспортной инфраструктуре занимают БТС, которые требуют развития технологий: искусственный интеллект, телекоммуникационные системы, киберфизические интерфейсы, информационная и кибербезопасность [26]. Подход «умного города», ориентированный на безопасность, должен реагировать не только на существующие, но и на возникающие уязвимости, учитывать опасности,

возникающие при разработке новых технологий. В связи с этим системы управления безопасностью, основанные на определении рисков разного рода (кибербезопасность, эффективность и надежность программно-технических средств и т. д.), позволят выявить уязвимости, опасные факторы и разработать соответствующие компенсирующие меры, что в свою очередь повысит безопасность КИИ умного города.

Применение сетевых моделей локального позиционирования для организации движения БТС в умном городе позволит повысить безопасность движения БТС даже в случае отсутствия GPS. Кроме того, учитывая высокую сложность транспортной инфраструктуры умного города и повышенные риски целесообразно проводить испытания разрабатываемых моделей и алгоритмов в программных симуляторах [27] с виртуальными сценами, близкими к реальным.

Благодарности

Исследование выполнено при частичной финансовой поддержке РФФИ в рамках научных проектов № 19-29-06044 (раздел Сетевые модели локального позиционирования) и № 19-01-00767 (раздел Система управления безопасностью).

ЛИТЕРАТУРА

1. Thomopoulos, N., Givoni, M. The autonomous car – a blessing or a curse for the future of low carbon mobility? An exploration of likely vs. desirable outcomes. *European Journal of Futures Research*. 2015;3:14. Доступно по: https://link.springer.com/content/pdf/10.1007/s40309-015-0071-z.pdf. DOI: 10.1007/s40309-015-0071-z (дата обращения 15.08.2020).
2. Fagnant D.J., Kockelman K. Preparing a nation for autonomous vehicles: Opportunities, barriers and policy recommendations. *Transportation Research Part A: Policy and Practice*. 2015;77:167-181. DOI: 10.1016/j.tra.2015.04.003.
3. Carvalho G.P.S, Costa R.R. Localization of an Autonomous Rail-Guided Robot Using Particle Filter. *IFAC-PapersOnLine*. 2017;50(1):5642-5647. DOI: 10.1016/j.ifacol.2017.08.1112.
4. Cai G., Lin H., Kao S. Mobile Robot Localization using GPS, IMU and Visual Odometry. *Proceedings of the 2019 International Automatic Control Conference (CACS)*. 2019;1-6. DOI: 10.1109/CACS47674.2019.9024731.
5. Forster C., Zhang Z., Gassner M., Werlberger M., Scaramuzza D. SVO: semi direct visual odometry for monocular and multicamera systems. *IEEE Transactions on Robotics*. 2017;33(2):249-265. DOI: 10.1109/TRO.2016.2623335.
6. Engel J., Stckler J., Cremers D. Large-scale direct SLAM with stereo cameras. *Proceedings of the 2015 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*. 2015;1935–1942. DOI: 10.1109/IROS.2015.7353631.
7. Bar Hillel A., Lerner R., Levi D., Raz G. Recent progress in road and lane detection: a survey. *Machine Vision and Applications*. 2014;25:727-45. DOI: 10.1007/s00138-011-0404-2.
8. Russakovsky O., Deng J., Su H., Krause J., Satheesh S., Ma S., Huang Z., Karpathy A., Khosla A., Bernstein M., Berg A.C., Fei-Fei L. ImageNet large scale visual recognition challenge. *International Journal of Computer Vision*. 2015;115:211-252. DOI: 10.1007/s11263-015-0816-y.
9. Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles. Standards. J3016_201806, SAE International. 2018.

10. Russell H.E.B., Harbott L.K., Nisky I., Pan S., Okamura A.M., Gerdes J.C. Motor learning affects car-to-driver handover in automated vehicles. *Science Robotics*. 2016:1(1). DOI: 10.1126/scirobotics.aah5682.
11. Anagnostopoulos C. Edge-centric inferential modeling & analytics. *Journal of Network and Computer Applications*. 2020;164:102696. DOI: 10.1016/j.jnca.2020.102696.
12. Petit J., Shladover S.E. Potential cyberattacks on automated vehicles. *IEEE Transactions on Intelligent Transportation Systems*. 2015;16(2):546–556. DOI: 10.1109/TITS.2014.2342271.
13. Lim H.S.M., Taeihagh A., Autonomous Vehicles for Smart and Sustainable Cities: An In-Depth Exploration of Privacy and Cybersecurity Implications. *Energies*. 2018;11(5):1062. DOI: 10.3390/en11051062.
14. Kohler W.J., Colbert-Taylor A. Current law and potential legal issues ertaining to automated, autonomous and connected vehicles. Santa Clara High Technology Law Journal. 2014;31(1), 99.
15. Parkinson S., Ward P., Wilson K., Miller J. Cyber threats facing autonomous and connected vehicles: future challenges. *IEEE Transactions on Intelligent Transportation Systems*. 2017:18(11): 2898–2915. DOI: 10.1109/TITS.2017.2665968.
16. Von Solms R., Van Niekerk J. From information security to cybersecurity. *Computers & Security*. 2013;38:97-102. DOI: 10.1016/j.cose.2013.04.004
17. Fagnant D.J., Kockelman K. Preparing a nation for autonomous vehicles: Opportunities, barriers and policy recommendations. *Transportation Research Part A: Policy and Practice*. 2015;77:167–181. DOI: 10.1016/j.tra.2015.04.003.
18. Li C.-Y., Wang J.-H., Zhi Y.-R., Wang Z.-R., Gong J.-H. Simulation of the Chlorination Process Safety Management System Based on System Dynamics Approach. *Procedia Engineering*. 2018;211:332-342. DOI: 10.1016/j.proeng.2017.12.020.
19. Kalashnikov A., Sakrutina E. Safety management system and Significant Plants of Critical Information Infrastructure. *IFAC-PapersOnLine*. 2019;52(13):1391-1396. DOI: 10.1016/j.ifacol.2019.11.393.
20. Iskhakov A., Meshcheryakov R. Intelligent system of environment monitoring on the basis of a set of IoT-sensors. *Proceedings of the 2019 International Siberian Conference on Control and Communications (SIBCON 2019)*. 2019;1-5. DOI: 10.1109/SIBCON.2019.8729628.
21. Чопоров О.Н., Нежельский Е.Р., Белоножкин В.И., Паринова Л.В. Разработка системы управления рисками организации, подключенной к сети интернет. *Информация и безопасность*. 2018;21(3):290-295.
22. Калашников А.О., Сакрутина Е.А. Модель прогнозирования рискового потенциала значимых объектов критической информационной инфраструктуры. *Информация и безопасность*. 2018;21(4):465-470.
23. Abdulov A.V., Abramenkov A.N. Collision Avoidance by Communication for Autonomous Mobile Robots in Crowd. *Proceedings of the 11th International Conference "Management of Large-Scale System Development" (MLSD)*. 2018;1-5. DOI: 10.1109/MLSD.2018.8551804.
24. Sand S., Dammann A., Mensing Ch. Position Estimation. *Positioning in Wireless Communications Systems*, Wiley Telecom, 2014. DOI: 10.1002/9781118694114.ch4.
25. Гусс С.В. Самоорганизующиеся mesh-сети для частного использования. *Математические структуры и моделирование*. 2016;4(40):102-115.
26. Promyslov V.G, Sakrutina E., Meshcheryakov R. Coherence Criterion for Security Architecture of Digital Control System. *Proceedings 2019 International Russian*

Automation Conference (RusAutoCon). 2019;1-5. DOI: 10.1109/RUSAUTOCON.2019.8867615.
27. Abdulov A.V., Abramenkov A.N., Shevlyakov A.A. Visual Odometry Approaches to Autonomous Navigation for Multicopter Model in Virtual Indoor Environment. *Advances in Systems Science and Applications*. 2018;18(3):17-28. DOI: 10.25728/assa.2018.18.3.583.

REFERENCES

1. Thomopoulos, N., Givoni, M. The autonomous car – a blessing or a curse for the future of low carbon mobility? An exploration of likely vs. desirable outcomes. *European Journal of Futures Research*. 2015;3:14. Доступно по: https://link.springer.com/content/pdf/10.1007/s40309-015-0071-z.pdf. DOI: 10.1007/s40309-015-0071-z (дата обращения 15.08.2020).
2. Fagnant D.J., Kockelman K. Preparing a nation for autonomous vehicles: Opportunities, barriers and policy recommendations. *Transportation Research Part A: Policy and Practice*. 2015;77:167-181. DOI: 10.1016/j.tra.2015.04.003.
3. Carvalho G.P.S, Costa R.R. Localization of an Autonomous Rail-Guided Robot Using Particle Filter. *IFAC-PapersOnLine*. 2017;50(1):5642-5647. DOI: 10.1016/j.ifacol.2017.08.1112.
4. Cai G., Lin H., Kao S. Mobile Robot Localization using GPS, IMU and Visual Odometry. *Proceedings of the 2019 International Automatic Control Conference (CACS)*. 2019;1-6. DOI: 10.1109/CACS47674.2019.9024731.
5. Forster C., Zhang Z., Gassner M., Werlberger M., Scaramuzza D. SVO: semi direct visual odometry for monocular and multicamera systems. *IEEE Transactions on Robotics*. 2017;33(2):249-265. DOI: 10.1109/TRO.2016.2623335.
6. Engel J., Stckler J., Cremers D. Large-scale direct SLAM with stereo cameras. *Proceedings of the 2015 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*. 2015;1935–1942. DOI: 10.1109/IROS.2015.7353631.
7. Bar Hillel A., Lerner R., Levi D., Raz G. Recent progress in road and lane detection: a survey. *Machine Vision and Applications*. 2014;25:727-45. DOI: 10.1007/s00138-011-0404-2.
8. Russakovsky O., Deng J., Su H., Krause J., Satheesh S., Ma S., Huang Z., Karpathy A., Khosla A., Bernstein M., Berg A.C., Fei-Fei L. ImageNet large scale visual recognition challenge. *International Journal of Computer Vision*. 2015;115:211-252. DOI: 10.1007/s11263-015-0816-y.
9. Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles. Standards. J3016_201806, SAE International. 2018.
10. Russell H.E.B., Harbott L.K., Nisky I., Pan S., Okamura A.M., Gerdes J.C. Motor learning affects car-to-driver handover in automated vehicles. *Science Robotics*. 2016:1(1). DOI: 10.1126/scirobotics.aah5682.
11. Anagnostopoulos C. Edge-centric inferential modeling & analytics. *Journal of Network and Computer Applications*. 2020;164:102696. DOI: 10.1016/j.jnca.2020.102696.
12. Petit J., Shladover S.E. Potential cyberattacks on automated vehicles. *IEEE Transactions on Intelligent Transportation Systems*. 2015;16(2):546–556. DOI: 10.1109/TITS.2014.2342271.
13. Lim H.S.M., Taeihagh A., Autonomous Vehicles for Smart and Sustainable Cities: An In-Depth Exploration of Privacy and Cybersecurity Implications. *Energies*. 2018;11(5):1062. DOI: 10.3390/en11051062.

14. Kohler W.J., Colbert-Taylor A. Current law and potential legal issues ertaining to automated, autonomous and connected vehicles. Santa Clara High Technology Law Journal. 2014;31(1), 99.
15. Parkinson S., Ward P., Wilson K., Miller J. Cyber threats facing autonomous and connected vehicles: future challenges. *IEEE Transactions on Intelligent Transportation Systems*. 2017:18(11): 2898–2915. DOI: 10.1109/TITS.2017.2665968.
16. Von Solms R., Van Niekerk J. From information security to cybersecurity. *Computers & Security*. 2013;38:97-102. DOI: 10.1016/j.cose.2013.04.004
17. Fagnant D.J., Kockelman K. Preparing a nation for autonomous vehicles: Opportunities, barriers and policy recommendations. *Transportation Research Part A: Policy and Practice*. 2015;77:167–181. DOI: 10.1016/j.tra.2015.04.003.
18. Li C.-Y., Wang J.-H., Zhi Y.-R., Wang Z.-R., Gong J.-H. Simulation of the Chlorination Process Safety Management System Based on System Dynamics Approach. *Procedia Engineering*. 2018;211:332-342. DOI: 10.1016/j.proeng.2017.12.020.
19. Kalashnikov A., Sakrutina E. Safety managemnt system and Significant Plants of Critical Information Infrastructure. *IFAC-PapersOnLine*. 2019;52(13):1391-1396. DOI: 10.1016/j.ifacol.2019.11.393.
20. Iskhakov A., Meshcheryakov R. Intelligent system of environment monitoring on the basis of a set of IoT-sensors. *Proceedings of the 2019 International Siberian Conference on Control and Communications (SIBCON 2019)*. 2019;1-5. DOI: 10.1109/SIBCON.2019.8729628.
21. Choporov O.N., Nezhelsky E.R., Belonozhkin V.I., Parinova L.V. Development of the control system information risk of the organization. *Informatsiya i bezopasnost'*. 2018;21(3):290-295.
22. Kalashnikov A.O., Sakrutina E.A. A model of predicting risk potential of significant plants of critical information infrastructure. *Informatsiya i bezopasnost'*. 2018;21(4):465-470.
23. Abdulov A.V., Abramenkov A.N. Collision Avoidance by Communication for Autonomous Mobile Robots in Crowd. *Proceedings of the 11th International Conference "Management of Large-Scale System Development" (MLSD)*. 2018;1-5. DOI: 10.1109/MLSD.2018.8551804.
24. Sand S., Dammann A., Mensing Ch. Position Estimation. *Positioning in Wireless Communications Systems*, Wiley Telecom, 2014. DOI: 10.1002/9781118694114.ch4.
25. Guss S.V. Private wireless mesh networks. *Mathematical Structures and Modeling*. 2016;4(40):102-115.
26. Promyslov V.G, Sakrutina E., Meshcheryakov R. Coherence Criterion for Security Architecture of Digital Control System. *Proceedings 2019 International Russian Automation Conference (RusAutoCon)*. 2019;1-5. DOI: 10.1109/RUSAUTOCON.2019.8867615.
27. Abdulov A.V., Abramenkov A.N., Shevlyakov A.A. Visual Odometry Approaches to Autonomous Navigation for Multicopter Model in Virtual Indoor Environment. *Advances in Systems Science and Applications*. 2018;18(3):17-28. DOI: 10.25728/assa.2018.18.3.583.

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Абдулов Александр Викторович, научный сотрудник, лаборатория Автоматизированных систем массового обслуживания,

Alexander V. Abdulov, Researcher, Laboratory Of Automated Systems Of Mass Service, V.A. Trapeznikov Institute Of Control Sciences Of The

Федеральное государственное бюджетное учреждение науки Институт проблем управления им. В. А. Трапезникова Российской академии наук, Москва, Российская Федерация
e-mail: aabdulov@asmon.ru
ORCID: 0000-0003-4015-4699

Абдулова (Сакрутина) Екатерина Алексеевна, научный сотрудник, лаборатория Сложных сетей, Федеральное государственное бюджетное учреждение науки Институт проблем управления им. В. А. Трапезникова Российской академии наук, Москва, Российская Федерация
e-mail: consoft@ipu.ru
ORCID: 0000-0002-7843-5202

Russian Academy Of Sciences, Moscow, Russian Federation

Ekaterina A. Abdulova (Sakrutina), Researcher, Laboratory Of Complex Networks, V.A. Trapeznikov Institute Of Control Sciences Of The Russian Academy Of Sciences, Moscow, Russian Federation