# НЕЙРОННЫЕ СЕТИ, ИНТЕРНЕТ ВЕЩЕЙ И БЛОКЧЕЙН В УПРАВЛЕНИИ БЕСПИЛОТНЫМ АВТОМОБИЛЕМ

*Селезнёв А.И., аспирант*

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Вишняков В.А. – д-р техн. наук, профессор*

В работе рассматривается применение Интернета вещей, нейронных сетей и блокчейн для управление беспилотным автомобилем. Анализируются особенности каждой из технологий и обсуждаются их недостатки.

**Введение.** Развитие беспилотных транспортных средств требует комплексного подхода к интеграции различных технологических решений. Беспилотный автомобиль (БА) в общем случае является наземным беспилотным транспортным средством, оснащенным рядом сенсоров(датчики), ИИ для обработки данных и навигационным модулем. Наиболее актуальными интеграционными решениями для БА являются нейронные сети, Интернет вещей (Internet of Things, IoT) и технология блокчейн.

Важным понятием в управлении БА являются интеллектуальные транспортные системы (ИТС) – это системы, использующие различные технологии автоматизации, компьютеры, системы управления и связи для повышения безопасности и эффективности транспорта, а также для повышения энергоэффективности и экологичности. Беспилотные автомобили в свою очередь включают в себя широкий спектр разнообразных технологий, касающихся электроники, динамики транспортных средств, связи, управления, датчиков и правильного понимания инстинктов поведения человека на дороге [1].

**Интернет вещей в БА.** Экосистема Интернета вещей для беспилотных систем, в которой вычислительные, коммуникационные и управляющие технологии тесно связаны, известна как киберфизическая система (КПС). Решения Интернета вещей, облегчающие связь между транспортными средствами, являются строительными блоками интеллектуальных транспортных систем. Система ИТС–Интернет вещей образует экосистему с сенсорными системами, системами мониторинга и системами отображения. Применительно к БА IoT платформа имеет следующие уровни:

1. Уровень восприятия. Он включает в себя все необходимое оборудование, включая датчики, исполнительные механизмы, процессоры и встроенное программное обеспечение, которые собирают разнообразные данные из физического мира.

2. Сетевой уровень. Включает в себя все беспроводные технологии, такие как Wi-Fi и сотовые технологии, включая 4G, 5G, 6G, а также протоколы связи, такие как MQTT, которые обеспечивают связь между уровнем устройства и облачным уровнем.

3. Уровень обработки. Выступает в качестве промежуточного программного обеспечения, этот уровень отвечает за обработку данных, полученных от предшествующих уровней.

4. Прикладной уровень, также называемый облачным уровнем IoT, это самый верхний уровень, содержащий важные серверы или облака для хранения и анализа данных. Кроме того, для связи и управления устройствами используется программное обеспечение для взаимодействия с людьми, системами и вещами, обеспечивая управление «подключенными устройствами». Он действует как централизованная система управления.

Экосистема Интернета вещей состоит из шести компонентов, взаимодействующих между собой: транспортное средство, человек, персональное устройство, сетевая инфраструктура, датчик и придорожное устройство. В такой обширной экосистеме IoT происходит многоуровневый обмен данными между всеми подключенными устройствами, которые являются ее частью. Шесть типов взаимодействий D2D (device-to-device) [2], включают взаимодействие между транспортными средствами (V2V), взаимодействие между транспортным средством и персональным устройством (V2P) (или взаимодействие между транспортным средством и человеческими устройствами, V2H), взаимодействие между транспортным средством и придорожным устройством (V2R), взаимодействие между транспортным средством и датчиком (V2S), взаимодействие между транспортным средством и инфраструктурой (V2I), взаимодействие между придорожным устройством и персональным устройством (R2P), взаимодействие между придорожными устройствами (R2R) и взаимодействие между датчиками и исполнительными механизмами (S2A).

Internet of Vehicles (IoV) и Internet of Autonomous Vehicles (IoAV) являются ответвлениями IoT для БА. Основные недостатки IoV:

1. Безопасность и конфиденциальность. IoAV предполагает обмен личной информацией пользователя, такой как местоположение и идентификационные данные, для получения точных результатов. Поскольку доступ к IoV осуществляется с множества устройств, он включает в себя различные технологии и сервисы, что делает его уязвимым для DDoS-атак и других вредоносных рисков. Различные части беспилотного автомобиля, такие как камеры, GPS, датчики, тормоза,

сигнализация, рулевое колесо и педаль акселератора, могут быть удаленно доступны, что ставит под угрозу конфиденциальность пользователей и может даже привести к летальному исходу.

2. Реагирование в реальном времени. Одним из важнейших условий бесперебойной работы сети IoAV является получение необходимой информации и принятие соответствующих решений с использованием максимально быстрой доступной связи, что по-прежнему отстает из-за существующих систем безопасности, которые вносят задержки в сеть из-за интенсивного процесса аутентификации.

3. Проверка данных. Огромный объем данных, генерируемых сетью IoAV, необходимо эффективно собирать, обрабатывать и проверять для предотвращения ложных срабатываний.

4. Надежность. Для эффективной связи IoT с автономными транспортными средствами основным условием является стабильное соединение. Таким образом, сетевые узкие места, DoS-атаки и сбои в связи могут значительно затруднить работу инфраструктуры.

5. Глушение сигнала. Сеть IoAV уязвима для атак с использованием помех, таких как подавление данных, подавление сигнала и подавление GPS.

6. Огромные объемы информации для обработки. Подключенные к сети транспортные средства генерируют приблизительно 1 ГБ данных в секунду, и этот объем будет расти по мере того, как все больше инфраструктуры и устройств подключаются к сети и требуют возможности подключения.

**Нейронные сети в БА.** В беспилотных автомобилях нашли применения сверточные нейронные сети (CNN) для «восприятия» окружения – непрерывного сканирования и отслеживания окружающей среды с помощью различных типов доступных датчиков, включая радар, лидар или камеры. Существующие алгоритмы восприятия разделяются на:

1. Опосредованное восприятие использует сверточные нейронные сети для обнаружения одного или нескольких изображений и использования их для создания подробной карты окружающей среды беспилотного автомобиля путем анализа расстояний до других транспортных средств, деревьев, дорожных знаков и т. д. Например, беспилотные автомобили могут точно распознавать дорожные знаки с помощью глубоких нейронных сетей с высокой точностью. В других областях, таких как обнаружение полос движения и обнаружение светофоров, точность аналогична при использовании различных структур нейронных сетей. Например, YOLO Darknet v2 [3] может обнаруживать более 9000 объектов с помощью модели CNN с частотой 40–70 кадров в секунду (fps) в реальном времени. Точность обнаружения составляет 80% в реальном времени, чего почти достаточно для обнаружения большинства объектов в автономном вождении. В них реализованы такие методы, как обнаружение границ и анализ значимых элементов, для получения изображений высокого разрешения различных обнаруженных объектов.

2. Прямое восприятие обеспечивает интегрированное понимание сцены и принятие решений. БА создают фрагменты карт (включая расстояния до других транспортных средств и разметку полос) вместо подробной локальной карты или записи траектории. Таким образом, прямое восприятие сразу фокусируется на управлении рулевым колесом и скоростью транспортного средства, минуя начальную локализацию и построение карты.

Основные недостатки CNN для БА:

1. Чувствительность к изменениям условий окружающей среды. CNN могут демонстрировать снижение точности при работе в неблагоприятных погодных условиях (дождь, снег, туман, яркое солнце) или при резком изменении освещения.

2. Зависимость от качества и количества обучающих данных. Для эффективного обучения CNN требуется большой объём размеченных данных. Если набор данных недостаточно разнообразен (например, не включает редкие или экстремальные сценарии), сеть может плохо обобщать на новые ситуации.

3. Проблема переобучения. Глубокие CNN склонны к переобучению, когда модель становится слишком специализированной на обучающих данных и плохо работает с новыми, необученными данными. Это может привести к ошибкам в реальных условиях, когда ситуация отличается от тех, что были в обучающем наборе.

4. Высокие вычислительные требования. CNN, особенно глубокие архитектуры, требуют значительных вычислительных ресурсов для обучения и инференса (обработки данных в режиме реального времени). Это может ограничивать их применение в системах с ограниченными ресурсами или требовать использования мощных GPU/TPU, что увеличивает стоимость системы.

5. Уязвимость к атакам adversarial. CNN восприимчивы к adversarial-атакам – специально созданным возмущениям входных данных, которые незаметны для человека, но могут заставить модель ошибаться. Например, небольшие изменения в изображении дорожного знака могут привести к его неправильной классификации. Это создаёт серьёзные риски для безопасности, так как злоумышленники могут использовать такие атаки для нарушения работы беспилотного автомобиля.

6. Ограниченная способность к контекстному пониманию. Нейронные сверточные сети хорошо справляются с распознаванием статичных объектов, но могут испытывать трудности с пониманием контекста сцены.

7. Проблемы с измерением расстояний. CNN эффективны для обнаружения и классификации объектов, но они не всегда хорошо справляются с определением точных расстояний до них. Это критично для задач, требующих оценки дистанции до препятствий или других участников движения.

8. Длительное время обучения Обучение CNN, особенно на больших наборах данных, может занимать значительное время. Это замедляет процесс разработки и внедрения новых моделей, а также усложняет их адаптацию к быстро меняющимся условиям.

**Технология блокчейн в БА.** Блокчейн [4] может использоваться в беспилотных автомобилях в следующих сценариях:

1. Технология автономного вождения: данные, полученные от датчиков транспортного средства, хранятся в блокчейне, что позволяет всем сторонам отслеживать и обмениваться информацией о безопасности транспортного средства и способах его использования владельцем более строгим образом, повышая прозрачность информации и снижая риск кражи данных.

2. Телематика – использует технологию блокчейна для обеспечения безопасного и надежного распределения данных и взаимодействия между множеством автономных транспортных средств и другими организациями, такими как региональные власти и общественные учреждения.

При применении технологии блокчейна в БА следует учитывать следующие особенности:

1. Безопасность транспортных средств. Датчики на транспортных средствах используются для обнаружения превышения скорости, оповещения или даже управления транспортным средством, а также для обнаружения постоянного отклонения транспортного средства от курса, чтобы предотвратить неосторожное вождение и снизить количество аварий.

2. Управление авариями. Автоматическое позиционирование и оказание экстренной помощи при аварии являются наиболее важными функциями управления авариями. Благодаря бортовому компьютеру, технологиям беспроводной связи и глобальной спутниковой системе позиционирования, можно в первую очередь отправить сигнал о помощи спасательным организациям при возникновении аварии. Блокчейн может предоставить необходимую информацию и помочь определить точное местоположение транспортного средства и тяжесть аварии, что значительно облегчает спасательные работы в условиях жесткой конкуренции.

3. Мониторинг транспортных средств включает в себя глобальную спутниковую систему позиционирования и технологии беспроводной связи. Он объединяет различные дополнительные услуги, такие как диспетчеризация команд, отслеживание целей, аварийная сигнализация и передача информации, в одном блокчейне. Благодаря целостности данных в системе блокчейна, можно отслеживать маршрут, усталость водителя, перегрузку и аварийную сигнализацию, эффективно повышая достоверность информации.

Проблемы применения блокчейна в БА:

1. Из-за анонимности невозможно подтвердить точность источников данных.

2. Невозможно достичь ситуации, в которой одновременно удовлетворяются требования безопасности, масштабируемости и эффективности выполнения.

Данные блокчейна анонимны и нет способа определить, какому транспортному средству принадлежат данные. Отсутствует технологическая основа блокчейна для мобильной среды сетей беспилотных автомобилей [5], спецификация смарт-контрактов не получила широкого распространения. Данные с датчиков в беспилотных автомобилях или в системах автомобильных сетей V2I (система «автомобиль-инфраструктура», «автомобиль-дорога»), V2N (система «автомобиль-сеть»), V2V (система «автомобиль-автомобиль»), V2P (система «автомобиль-пешеход») и V2D (система «автомобиль-устройство») должны регулироваться в виде смарт-контрактов для защиты соответствующих прав, прежде чем они будут добавлены в систему блокчейн. Огромный объем данных, генерируемых различными приложениями, и то, как технология блокчейн работает в инфраструктуре с высокими вычислительными требованиями, также представляют собой проблемы.

**Заключение.** Таким образом применение каждой из технологий для беспилотного автомобиля позволяет существенно расширить его функционал. Интернет вещей является центральной частью БА, связывая все его сенсоры, бортовые компьютеры и внешнюю среду в единую интеллектуальную сеть. Нейронные сети необходимы для «восприятия» окружения и «осмысления» поступающих данных с сенсоров, так как традиционные алгоритмы обработки не способны справиться с многообразием реальных дорожных ситуаций. Блокчейн нужен для обеспечения надежности и безопасности в беспилотном управлении и взаимодействии с внешней средой.

***Список использованных источников:***

*1. Autonomous Vehicles Enabled by the Integration of IoT, Edge Intelligence, 5G, and Blockchain. Sensors. 2023;23(4):1963.*

*2. Vermesan, O. Automated driving progressed by internet of things. European Union's Horizon 2020 Research and Innovation Programme (2014–2020). 2018.*

*3. Reddy, P.P. Driverless Car-Design of a Parallel and Self-Organizing System; EasyChair Preprint no. 1248; EasyChair: Manchester, UK, 2019.*

*4. Bhutta, M.N.M.; Khwaja, A.A.; Nadeem, A.; Ahmad, H.F.; Khan, M.K.; Hanif, M.A.; Song, H.; Alshamari, M.; Cao, Y. A Survey on Blockchain Technology: Evolution, Architecture and Security. IEEE Access 2021, 9, 61048–61073.*

*5. Jain, S.; Ahuja, N.J.; Srikanth, P.; Bhadane, K.V.; Nagaiah, B.; Kumar, A.; Konstantinou, C. Blockchain and Autonomous Vehicles: Recent Advances and Future Directions. IEEE Access 2021, 9, 130264–130328.*