Научная статья
Original article
УДК 656.9
doi: 10.55186/2413046X_2025_10_3_87

УЯЗВИМОСТЬ ПОДКЛЮЧЕННЫХ И АВТОНОМНЫХ ТРАНСПОРТНЫХ СРЕДСТВ И ЕЕ ВЛИЯНИЕ НА ГРУЗОВЫЕ ПЕРЕВОЗКИ АВТОНОМНЫМ ТРАНСПОРТОМ

VULNERABILITY OF CONNECTED AND AUTONOMOUS VEHICLES AND ITS IMPACT ON FREIGHT TRANSPORTATION BY AUTONOMOUS TRANSPORT

Слесарчук Алина Олеговна, аспирант кафедры предпринимательства и логистики, ФГБОУ ВО «Российский экономический университет им. Г.В. Плеханова», Москва, E-mail: ali-slesarchuk@yandex.ru

Slesarchuk Alina Olegovna, Postgraduate Student of the Department of Entrepreneurship and Logistics, Plekhanov Russian University of Economics, Moscow, E-mail: ali-slesarchuk@yandex.ru

Аннотация. В статье приведены результаты анализа систем автономных и подключенных транспортных средств и их уязвимости, которые могут иметь последствия для оказания транспортных услуг. Выявлено, что помимо физической безопасности человека, к которой стремятся производители всех транспортных средств, автономные транспортные средства должны еще обеспечивать защиту от взлома и других кибератак и конфиденциальность персональных данных. Для определения потенциальных угроз и коммерческих рисков, например для транспортной компании, был проведен анализ STRIDE. Данная методика включает в себя оценку рисков информационной безопасности по следующим категориям: спуфинг,

модификация, отказ от авторства, разглашение, отказ в обслуживании и повышение привилегий. Данная статья посвящена декомпозиции концепции системы управления автономным транспортным средством на основные элементы применению анализа STRIDE к этим компонентам. В рамках анализа выявлено, что высокий риск имеет угроза удалённого взлома бортового компьютера и/или нарушения алгоритмов одного из серверов автономного транспортного средства. Помимо анализа STRIDE была построена диаграмма потока данных (Data Flow Diagram) для подтверждения полученных результатов. В результате исследования автором сделан вывод о том, что работа над угрозами безопасности для автономных и подключенных транспортных средств позволит плавную модернизацию отрасли грузовых перевозок на автомобильном транспорте и выход на новый уровень клиентского сервиса.

Abstract. The article presents the results of an analysis of autonomous and connected vehicle systems and their vulnerabilities, which may have consequences for the provision of transport services. It has been revealed that in addition to human physical security, which manufacturers of all vehicles strive for, autonomous vehicles must also provide protection against hacking and other cyber attacks and confidentiality of personal data. A STRIDE analysis was conducted to identify potential threats and commercial risks, for example for a transportation company. This methodology includes an assessment of information security risks in the following categories: spoofing, modification, denial of authorship, disclosure, denial of service, and privilege escalation. This article is devoted to the decomposition of the concept of an autonomous vehicle control system into the main elements and the application of STRIDE analysis to these components. The analysis revealed that there is a high risk of remote hacking of the on-board computer and/or disruption of the algorithms of one of the servers of an autonomous vehicle. In addition to the STRIDE analysis, a Data Flow Diagram was constructed to confirm the results. As a result of the research, the author

concluded that working on security threats for autonomous and connected vehicles will allow a smooth modernization of the freight transportation industry in road transport and reaching a new level of customer service.
Ключевые слова: автономные и подключенные транспортные средства, парки транспортных средств, кибербезопасность, риски, требования безопасности, системные компоненты, своевременность доставки, клиентский сервис

Keywords: autonomous and connected vehicles, fleets of vehicles, cybersecurity, risks, security requirements, system components, on-time delivery, customer service

Тема развития подключенных и автономных транспортных средств с каждым годом становится актуальной для разработчиков и бизнеса с целью развивать новый сегмент экономики, но и для государства, которое считает такие транспортные средства инструментом для решения текущих экономических и социальных проблем.

Таким образом, развитие подключенного и автономного транспорта в России стало задачей одного из национальных проектов. В мае 2024 года Президентом Российской Федерации был подписан Указ «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года».[1] В рамках национальной цели «Технологическое лидерство» стоит задача обеспечить «технологическую независимость и формирование новых рынков по таким направлениям, как биоэкономика, сбережение здоровья граждан, продовольственная безопасность, беспилотные авиационные системы, средства производства и автоматизации, транспортная мобильность (включая автономные транспортные средства)» и др.

[1] Указ Президента Российской Федерации от 07.05.2024 № 309 "О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года" // Официальное опубликование правовых актов 2024, 7 мая. URL: http://publication.pravo.gov.ru/document/0001202405070015

Автопроизводители автономных и подключенных транспортных средств при разработке системы безопасности должны учитывать, что транспортное средство должно обеспечивать физическую безопасность человека, защиту от взлома и других кибератак и конфиденциальность персональных данных.

В течение последних лет кибербезопасность стала одной из самых насущных проблем автономного транспорта. Хотя данный вопрос был достаточно обширно представлен в прессе, взлом автономных транспортных средств остается новым и мало изученным явлением. Среднее транспортное средство содержит 150 млн. строк кода, несколько компьютеров и большое количество проводных и беспроводных соединений с внутренними и внешними каналами связи. Чем больше функций и сетей имеет транспортное средство, тем выше вероятность его взлома или атаки на него.

Учитывая сложные встроенные системы и логистику, гигантский объем финансовых вложений необходимых для закрытия множества уязвимостей в системах защиты современных транспортных средств. Более того разовые взломы частных автомобилей всегда могут произойти, но для автономных и подключенных транспортных средств есть риск взлома миллионов машин, что можно риском для целых парков автомашин (например, роботов-такси, курьеров и тд.). Во многих отношениях взлом целых парков транспортных средств является более привлекательным с финансовой точки зрения, чем взлом отдельных автомобилей[2].

Существует методология моделирования угроз STRIDE. Ее разработала компания Microsoft. Данная методология позволяет систематически выявлять потенциальные угрозы безопасности на этапе проектирования и эксплуатации приложений, помогает разработчикам, архитекторам и специалистам по безопасности предугадывать уязвимости и разрабатывать

[2] Паре Д., Ребейн Х. Автономные и подключенные автомобили. Устройство, стандарты и перспективы развития / пер. с англ. В.С. Яценкова. – М.: ДМК Пресс, 2023. – 454 с.

стратегии защиты. STRIDE широко применяется для анализа архитектуры приложений, облачных решений, сетевой инфраструктуры и IoT-устройств[3].

Содержание метода:

– Spoofing (подмена),
– Tampering (несанкционированное изменение),
– Repudiation (отказ от действий),
– Information Disclosure (раскрытие информации),
– Denial of Service (отказ в обслуживании);
– Elevation of Privilege (повышение привилегий).

Этот метод помогает структурировать процесс анализа угроз и выявить потенциальные риски на ранних этапах разработки. В процессе анализа производится оценка рисков, просчитывается вероятность угрозы, потенциальный ущерб, предлагаются меры защиты при условии, что выбранные решения соответствуют требованиям безопасности и не нарушают функциональность системы.[4]

В связи с тем, что подключенный и автономный автомобиль представляет собой сложную систему, включающую программное обеспечение, аппаратное обеспечение, датчики, сети связи и взаимодействие с внешними системами (например, инфраструктурой дорожного движения), а чем больше функций и сетей имеет транспортное средство, тем выше вероятность его взлома или атаки на него, то выполним анализ STRIDE.

Анализ STRIDE для автономного автомобиля позволяет выявить потенциальные угрозы безопасности, связанные с его функционированием. Автономные автомобили представляют собой набор системных компонентов, отвечающих самостоятельное вождение автомобиля. Каждый из этих компонентов может быть подвержен различным типам атак.

[3] Рытов, М. Ю. Применение методологии stride для определения актуальных угроз безопасности программно-определяемых сетей / М. Ю. Рытов, Р. Ю. Калашников // Автоматизация и моделирование в проектировании и управлении. – 2019. – № 3(5). – С. 19-24. – DOI 10.30987/article_5d8d113d968333.98732766. – EDN NLSDLD.
[4] Методология STRIDE в моделировании угроз [Электронный ресурс] // ThreatScope 2025. URL: https://threatscope.ru/about-stride/

1. Определение компонентов системы:

a. Датчики и системы восприятия (камеры, лидары, радары).[5]

b. Система управления (двигатель, тормоза, рулевое управление).

c. Коммуникационные системы и сетевые интерфейсы (GPS, V2X, облачные сервисы).

d. Пользовательский интерфейс (приложение для смартфона, бортовой компьютер).

e. Участники (водитель/пассажиры, производитель автомобиля, заказчик грузоперевозки),

2. Применение модели STRIDE

Таблица 1. **STRIDE анализ уязвимости автономного транспорта**

Категории угроз	**Уязвимость**	**Мера защиты**	**Влияние на логистику**
Spoofing (Подмена)	**Угроза:** Злоумышленник может подделать сигналы GPS или Wi-Fi, чтобы ввести автомобиль в заблуждение относительно его местоположения. **Пример:** Поддельные GPS-сигналы могут заставить автомобиль свернуть не туда.	**Мера защиты:** Использование криптографической аутентификации для GPS-сигналов, проверка подлинности сетевых соединений.	Изменение траектории движения транспортного средства, что влияет на своевременность доставки.
	Угроза: Атака на идентификацию пользователя автомобиля. **Пример:** Злоумышленник может получить доступ к автомобилю, используя	**Мера защиты:** Многофакторная аутентификация для доступа к автомобилю.	Угон транспортного средства или кража груза из транспортного средства. Потеря товарно-материальных ценностей, значительное ухудшение

[5] What sensors are installed on autonomous driving cars? [Электронный ресурс] // SIC ELECTRONICS LIMITED 2024, 19 сентября. URL: https://www.sic-chip.com/info-detail/what-sensors-are-installed-on-autonomous-driving-cars

	поддельные ключи или учётные данные.		клиентского сервиса, нарушение цепи поставок в сети снабжения и распределения.
Tampering (Несанкци-онированное изменение)	**Угроза:** Изменение данных с датчиков (например, камеры или лидаров) для искажения восприятия окружающей среды. **Пример:** Наклейка на дорожном знаке может заставить автомобиль неверно интерпретировать ситуацию.	**Мера защиты:** Использование резервных датчиков и алгоритмов проверки целостности данных.	Изменение траектории движения транспортного средства, что влияет на своевременность доставки.
	Угроза: Взлом бортового компьютера для изменения алгоритмов управления. **Пример:** Установка вредоносного ПО, которое управляет автомобилем.	**Мера защиты:** Защита прошивки от несанкционированных изменений, использование TPM (Trusted Platform Module).	Влияние на соблюдение ПДД, увеличение вероятности аварийных ситуаций и/или аварий, из чего будет следовать утрата перевозимых товарно-материальных ценностей.
Repudiation (Отказ от действий)	**Угроза:** Злоумышленник может выполнить действие (например, отправить команду на изменение маршрута) и затем отрицать свою причастность. **Пример:** Отправка поддельной команды через удалённое управление.	**Мера защиты:** Логирование всех действий с цифровыми подписями для обеспечения постоянного отклика от серверов.	Ухудшение клиентского сервиса руками конкурентов за счет игнорирования договоренностей с грузоотправителем и грузополучателем, снижение показателя своевременности доставки.
	Угроза: Пассажир может отказаться от ответственности за действия, совершённые с помощью автомобиля.	**Мера защиты:** Привязка действий автомобиля к учётной записи владельца	Умышленное создание аварийной ситуации водителем/ пассажиром, что может способствовать потере или порче

	Пример: Использование автомобиля для незаконных целей.		перевозимых товарно-материальных ценностей.
Information Disclosure (Раскрытие информации)	**Угроза:** Утечка персональных данных пассажиров (маршруты, предпочтения, биометрические данные). **Пример:** Перехват данных через незащищённое соединение.	**Мера защиты:** Шифрование информации, которую генерирует автономный автомобиль.	Использование конкурентами персональных данных о рейсе и грузе, данных о ПО для достижения коммерческих целей.
	Угроза: Раскрытие данных о системах автомобиля (например, алгоритмы управления). **Пример:** Обратная разработка ПО для поиска уязвимостей.	**Мера защиты:** Зашифровка кода и данных в т.ч. с помощью DRM (Digital Rights Management).	
Denial of Service (Отказ в обслуживании)	**Угроза:** Злоумышленник может перегрузить систему автомобиля запросами, что приведёт к её зависанию или некорректной работе. **Пример:** DoS-атака на бортовой компьютер.	**Мера защиты:** Ограничение числа входящих запросов, использование защитных механизмов против DoS/DDoS.	Умышленное создание аварийной ситуации за счет перегрузки микросервисов автономного автомобиля, влияющих на его движение, что может способствовать потере или порче перевозимых товарно-материальных ценностей.
	Угроза: Блокировка работы датчиков или систем связи. **Пример:** Электромагнитное воздействие на датчики или GPS.	**Мера защиты:** Резервирование критических систем, защита от электромагнитных помех.	Умышленное создание аварийной ситуации за счет блокировки всех датчиков, что может способствовать потере или порче перевозимых товарно-материальных ценностей.

Elevation of Privilege (Повышение привилегий) через уязвимость в ПО.	**Угроза:** Злоумышленник может получить полный контроль над автомобилем, эксплуатируя уязвимости в системе. **Пример:** Удалённое управление автомобилем	**Мера защиты:** Строгая политика управления правами доступа, регулярное обновление ПО.	Умышленное создание аварийной ситуации водителем/ пассажиром, что может способствовать потере или порче перевозимых товарно-материальных ценностей. Использование конкурентами транспортного средства в своих коммерческих целях.
	Угроза: Получение доступа к системам автомобиля с ограниченными правами, но с возможностью эскалации. **Пример:** Взлом внутренней сети автомобиля через Bluetooth.	**Мера защиты:** Изоляция критических систем, мониторинг подозрительной активности.	

(Источник: составлено автором)

Все описанные выше угрозы можно сконсолидировать в три основные:

– взлом бортового компьютера и/или нарушение алгоритмов одного из серверов,

– подмена GPS-сигналов и/или изменение данных сенсорных датчиков (например, у автономного грузового автомобиля Яндекс их 31: 17 камер, 6 лидаров, 5 радаров, 2 инерциальных датчика, 1 спутниковый приемник.)[6],

– утечка данных через беспроводные сети (например, Bluetooth).

– Такие угрозы можно проранжировать согласно уровню риска:

– Высокий риск: Удалённый взлом бортового компьютера и/или нарушение алгоритмов одного из серверов.

– Средний риск: Подмена GPS-сигналов и/или изменение данных сенсорных датчиков.

[6] Блог компании Яндекс: Встречаем автономные грузовики Яндекса [Электронный ресурс] // Хабр 2024, 10 декабря. URL: https://habr.com/ru/companies/yandex/articles/864464/

– Низкий риск: Утечка данных через беспроводные сети.

Ранжирование помогает определить с какой угрозой необходимо работать в первую очередь.

В качестве эффективных и часто используемых мер защиты на такие угрозы выявляют такие как криптографическая аутентификация, шифрование данных и регулярное обновление ПО.

Помимо этого, в рамках анализа были сформулированы риски для транспортной компании, владеющей парком автономных грузовых автомобилей, из-за потенциальных угроз и кибератак:

– нарушение сроков доставки,

– потере или порче перевозимых товарно-материальных ценностей,

– потеря транспортного средства,

– использование конкурентами персональных данных о рейсе и грузе, данных о ПО в коммерческих интересах.

Согласно методологии STRIDE необходимо с определенной периодичностью обновлять анализ по мере изменения системы или появления новых угроз.

Кроме анализа STRIDE в моделировании потоков информации в системах автономного транспорта, которые могут быть подвержены угрозам безопасности, связанные с его функционированием, Data Flow Diagram может отобразить пути передачи информации между системами, базами данных и тд. для выявления мест потенциальных угроз.

В данной диаграмме выделяют 4 компонента[7]:

1) Процесс

– Процессы — это действия, которые изменяют или преобразуют данные. Эти действия могут включать вычисления, сортировку, проверку

[7] How to STRIDE [Электронный ресурс] // Threat-Modeling 2022, 11 сентября. URL: https://threat-modeling.com/how-to-stride-threat-model/ (дата обращения: 16.03.2025)

подлинности, перенаправление или любые другие преобразования, необходимые для продвижения данного сегмента потока данных.[8]

– В рамках описания потоков данных для работы автономного транспортного средства за основу взят процесс движения автономного автомобиля – т.е. преобразование данных от сенсорных датчиков с помощью зашитых алгоритмов реагирования на сигналы от них.

2) Внешняя сущность

– Это объекты, которые взаимодействуют с системой, отправляя или получая данные. Внешние сущности могут быть источниками или получателями информации.

– Внешним пользователем автономного транспортного средства является водитель, пассажир, заказчик грузоперевозки и др.

3) Хранилище данных

– Хранилища данных представляют собой места, где сохраняются исходные, промежуточные или конечные данные. Это могут быть базы данных, файлы или другие формы хранения информации.

– В данном примере базы данных будут аккумулировать информацию о маршрутах, о рейсах, об обменах сигналами с другими транспортными средствами.

4) Поток данных

– Потоки данных показывают направление перемещения информации между внешними сущностями, процессами и хранилищами данных. Они отображают, какие данные передаются и куда они направляются.

[8] What is a data flow diagram (DFD)? [Электронный ресурс] // IBM 2024, 22 ноября. URL: https://www.ibm.com/think/topics/data-flow-diagram (дата обращения: 19.03.2025)

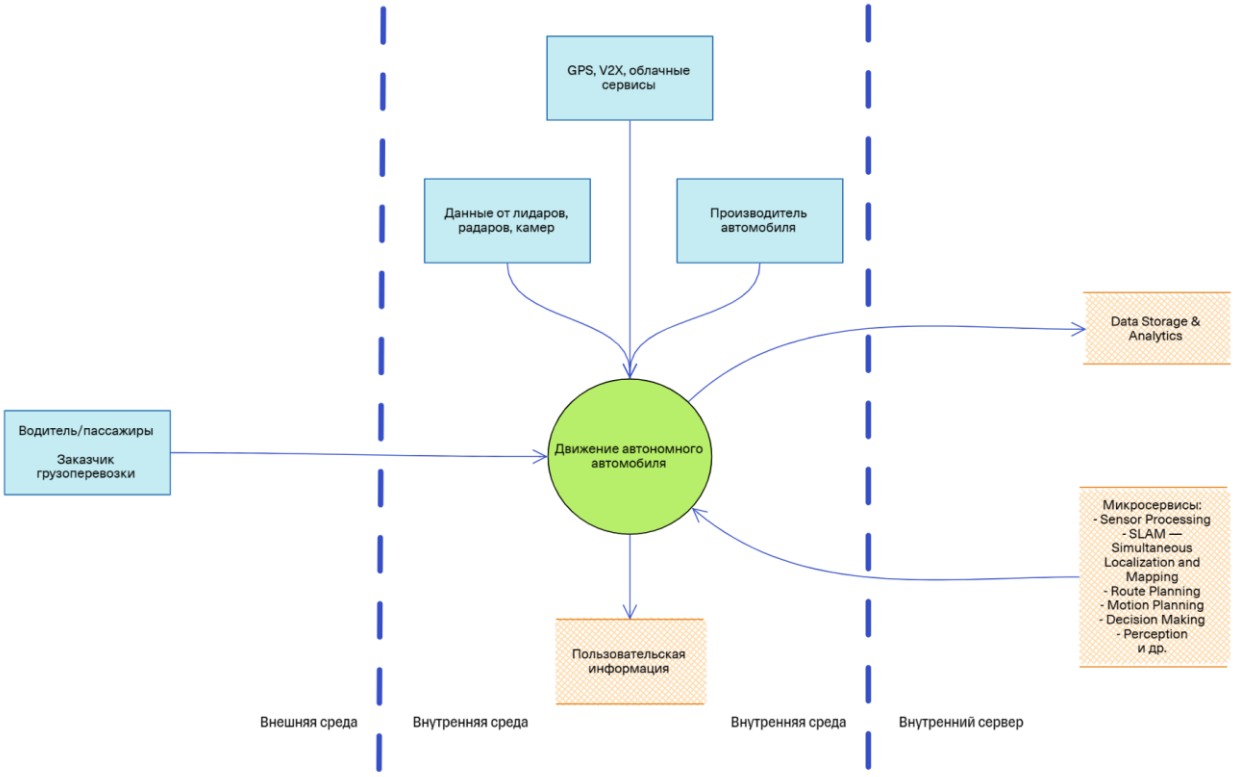

Рисунок 1. **Data Flow Diagram (DFD) – Верхнеуровневая диаграмма потока информации, необходимой для движения автономного автомобиля**

Диаграмма показала, что самым уязвимым участком к атакам и взломам будет передача информации из внешней среды во внутреннюю, а значит каналы обмена информации на этом участке должны быть надежно защищены, предположительно средствами криптозащиты.

Автопроизводители осознают опасность взлома автопарка и встраивают в транспортные средства эшелонированную защиту, в том числе на уровне глобальной архитектуры безопасности, с защитой путем шифрования коммуникаций и сетей как внутри, так и снаружи транспортных средств. Кроме того, они работают рука об руку с сетевыми операторами, которые обеспечивают подключение транспортных средств, создавая информационные узлы безопасности автомобиля, в которых аналитики могут выявлять угрозы безопасности для парка автомобилей.

Метод STRIDE позволяет систематически анализировать угрозы кибербезопасности для автономных автомобилей и разрабатывать эффективные меры защиты, а диаграмма потока данных показала, что самым уязвимым участком к атакам и взломам будет передача информации из внешней среды во внутреннюю. Такие анализы особенно важны для таких сложных систем, где уязвимости могут привести к серьезным последствиям, включая аварии и утечку конфиденциальных данных. Потенциально автономные грузовые транспортные средства будут захватывать долю рынка грузовых перевозок, который исчисляется 6 491 т в год.[9] Для успешного функционирования отрасли необходимо соблюдение требований безопасности, которые были раскрыты в статье, что подтверждает актуальность выбранной темы.

Список источников

1. Указ Президента Российской Федерации от 07.05.2024 № 309 "О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года" // Официальное опубликование правовых актов 2024, 7 мая. URL: http://publication.pravo.gov.ru/document/0001202405070015

2. Паре Д., Ребейн Х. Автономные и подключенные автомобили. Устройство, стандарты и перспективы развития / пер. с англ. В.С. Яценкова. – М.: ДМК Пресс, 2023. – 454 с.

3. Рытов, М. Ю. Применение методологии stride для определения актуальных угроз безопасности программно-определяемых сетей / М. Ю. Рытов, Р. Ю. Калашников // Автоматизация и моделирование в проектировании и управлении. – 2019. – № 3(5). – С. 19-24. – DOI 10.30987/article_5d8d113d968333.98732766. – EDN NLSDLD.

[9] Росстат: Транспорт в России 2024 [Электронный ресурс]. — URL: https://rosstat.gov.ru/storage/mediabank/Transport_2024.pdf

4. Методология STRIDE в моделировании угроз [Электронный ресурс] // ThreatScope 2025. URL: https://threatscope.ru/about-stride/ (дата обращения: 10.03.2025)

5. What sensors are installed on autonomous driving cars? [Электронный ресурс] // SIC ELECTRONICS LIMITED 2024, 19 сентбря. URL: https://www.sic-chip.com/info-detail/what-sensors-are-installed-on-autonomous-driving-cars (дата обращения: 10.03.2025)

6. Блог компании Яндекс: Встречаем автономные грузовики Яндекса [Электронный ресурс] // Хабр 2024, 10 декабря. URL: https://habr.com/ru/companies/yandex/articles/864464/ (дата обращения: 19.03.2025)

7. How to STRIDE [Электронный ресурс] // Threat-Modeling 2022, 11 сентября. URL: https://threat-modeling.com/how-to-stride-threat-model/ (дата обращения: 16.03.2025)

8. What is a data flow diagram (DFD)? [Электронный ресурс] // IBM 2024, 22 ноября. URL: https://www.ibm.com/think/topics/data-flow-diagram (дата обращения: 19.03.2025)

9. Росстат: Транспорт в России 2024 [Электронный ресурс]. — URL: https://rosstat.gov.ru/storage/mediabank/Transport_2024.pdf

References

1. Decree of the President of the Russian Federation dated 05/07/2024 No. 309 "On the National Development Goals of the Russian Federation for the period up to 2030 and for the future up to 2036" // Official publication of Legal acts 2024, May 7. URL: http://publication.pravo.gov.ru/document/0001202405070015

2. Pare D., Rebein H. Autonomous and connected cars. Device, standards and development prospects / translated from English by V.S. Yatsenkov, Moscow: DMK Press, 2023, 454 p.

3. Rytov, M. Y. Application of stride methodology to identify current security threats to software-defined networks / M. Y. Rytov, R. Y. Kalashnikov //

Automation and modeling in design and management. – 2019. – № 3(5). – Pp. 19-24. – DOI 10.30987/article_5d8d113d968333.98732766. – EDN NLSDLD.

4. STRIDE methodology in threat modeling [Electronic resource] // ThreatScope 2025. URL: https://threatscope.ru/about-stride / (date of request: 10.03.2025)

5. What sensors are installed on autonomous driving cars? [Electronic resource] // SIC ELECTRONICS LIMITED 2024, September 19. URL: https://www.sic-chip.com/info-detail/what-sensors-are-installed-on-autonomous-driving-cars (date of request: 10.03.2025)

6. Yandex company blog: Meet the autonomous trucks of Yandex [Electronic resource] // Habr 2024, December 10. URL: https://habr.com/ru/companies/yandex/articles/864464 / (date of request: 19.03.2025)

7. How to STRIDE [Electronic resource] // Threat-Modeling 2022, September 11. URL: https://threat-modeling.com/how-to-stride-threat-model / (date of request: 16.03.2025)

8. What is a data flow diagram (DFD)? [Electronic resource] // IBM 2024, November 22. URL: https://www.ibm.com/think/topics/data-flow-diagram (date of request: 19.03.2025)

9. Rosstat: Transport in Russia 2024 [Electronic resource]. — URL: https://rosstat.gov.ru/storage/mediabank/Transport_2024.pdf