

УДК 004.77+629.3.06+656.13

В.В. ДРОЗД

научный сотрудник отдела систем активной безопасности и управления НИЦ «Электромеханические и гибридные силовые установки мобильных машин»¹
E-mail: veronika.litarovich@gmail.com

В.В. САВЧЕНКО, канд. техн. наук, доц.

начальник отдела систем активной безопасности и управления НИЦ «Электромеханические и гибридные силовые установки мобильных машин»¹
E-mail: uus@tut.by

С.О. КОПЫТОК

ведущий инженер-программист²
E-mail: skb@ekran.by

В.В. ГОЗА

младший научный сотрудник отдела систем активной безопасности и управления НИЦ «Электромеханические и гибридные силовые установки мобильных машин»¹
E-mail: mechenistalker@gmail.com

¹Объединенный институт машиностроения НАН Беларуси, г. Минск, Республика Беларусь

²ОАО «Экран», г. Борисов, Республика Беларусь

Поступила в редакцию 04.04.2024.

ОБЛАЧНЫЕ ХРАНИЛИЩА И ТЕХНОЛОГИИ ПЕРЕПРОГРАММИРОВАНИЯ БОРТОВЫХ СИСТЕМ ВЫСОКОАВТОМАТИЗИРОВАННЫХ ТРАНСПОРТНЫХ СРЕДСТВ

Динамичное развитие технологий в высокоавтоматизированных транспортных средствах предполагает разработку новых методов передачи информации на борт транспортного средства своевременно и оперативно. В связи с этим активно развивается направление передачи данных «по воздуху». В статье рассмотрены облачные сервисы, которые могут применяться для обновлений «по воздуху» в высокоавтоматизированных транспортных средствах. Выделены основные (наиболее используемые) и дополнительные облачные сервисы. Представлена схема ответственности провайдера и клиента для облачных сервисов IaaS, PaaS, SaaS. Рассмотрены аспекты безопасности облачных сервисов как одна из наиболее значимых и приоритетных задач по предотвращению угроз и защиты персональных данных. Представлены и описаны конкретные категории обновлений «по воздуху», применяемые в высокоавтоматизированных транспортных средствах и прилегающей инфраструктуре. Рассмотрен процесс выпуска и установки обновлений прошивки и программного обеспечения «по воздуху» на высокоавтоматизированные транспортные средства, их составляющие и прилегающую инфраструктуру. Полученные результаты ориентированы на более глубокое понимание процесса обновления программного обеспечения «по воздуху».

Ключевые слова: безопасность облачных сервисов, высокоавтоматизированное транспортное средство, облачные сервисы, обновление «по воздуху», подключенный автомобиль

DOI: <https://doi.org/10.46864/1995-0470-2024-3-68-36-42>

Введение. Цифровая трансформация в автомобильной промышленности динамично развивается. Компания Movimento Group (Германия) является мировым лидером в области сферы услуг и технологий перепрошивки бортового оборудования. Компания провела анализ данных и представила отчет, в котором отображаются современные тенденции по «объему» программного обеспечения (метрика программного обеспечения — коли-

чество строк кода) в различных системах в сравнении, и как будет проходить изменение автомобиля в дальнейшем. Например, количество строк кода для различных объектов равняется следующим значениям: около 1,5 млн строк кода — истребитель F-22 Raptor Fighter Jet, около 13 млн строк кода — самолет Boeing 787, около 61 млн строк кода — компания Facebook, около 100 млн строк кода — современный беспилотный автомобиль.

Обновление «по воздуху» (от английского Over-the-Air, сокращенно ОТА) в высокоавтоматизированном и беспилотном транспортном средстве впервые использовала компания Tesla. В ее электромобили встроен модуль передачи данных, которому нужна только SIM-карта местного оператора с доступом в интернет. Также можно подключить машину к домашней (или любой другой) Wi-Fi-сети или дать доступ к интернету со смартфона [1]. Удаленное обновление компания Tesla использует для постоянного совершенствования своих бортовых систем управления, причем таких обновлений может быть несколько в течение месяца. У автомобилей компании BMW для получения и установки обновлений используется специализированное мобильное приложение. Чтобы воспользоваться возможностями приложения необходимо соблюсти ряд условий: автомобиль должен быть не старше 2018 года выпуска, и на нем должна быть установлена операционная система BMW Operation System 7-й или 8-й версий. Автовладельцам останется только загрузить обновление на мобильное устройство и установить соединение с автомобилем по сети Wi-Fi. Система автоматически распознает файл и предложит установить обновление. Модели со встроенным модемом можно обновить по сотовой сети — на первые несколько лет доступ в интернет предоплачен производителем, а затем платить придется уже владельцу. Все производители автомобилей запрещают выполнять обновление во время движения, причем некоторые обновления могут устанавливаться от нескольких минут до нескольких часов. Как правило, владелец электромобиля выбирает, в какое время бортовые системы будут обновлять свое программное обеспечение [2].

Обновление программного обеспечения (ПО) может распространяться на все узлы с электронным управлением: пневмоподвеску, тормозную систему, силовую установку, электроусилитель руля, внешнее освещение и так далее. Еще в 2018 году Tesla одним дистанционным обновлением сократила тормозной путь Model 3 при торможении с 96 км/ч почти на 6 метров. Добиться этого удалось за счет изменения алгоритма работы антиблокировочной системы, который, естественно, пришел машинам «по воздуху».

На электромобилях можно увеличить мощность электрического мотора с помощью обновленного ПО без дополнительных технических изменений. Так, «перепрошитые» электрические моторы Model Y версии Long Range позволяют разогнаться до 100 км/ч за 4,3 секунды, хотя изначально на это уходило на полсекунды больше. Возможность купить такой чип-тюнинг появилась после обновления с индексом 2020.36 [2].

В 2021 году 30 моделей BMW (в общей сложности два миллиона автомобилей по всему миру) дистанционно получили обновление навигации,

а также улучшения функции удержания в полосе. В облачные сервисы обращается и комплекс BMW Connect. Он позволяет активировать дополнительные функции (даже платные) без посещения дилера. Например, адаптивное управление жесткостью подвески, автоматический дальний свет. Доступ к опциям зависит от технического оснащения конкретного автомобиля [2].

Проведенные исследования по теме работы и поиск информации в сети показали совпадение на русском и английском языках соответственно 2 результата и 32 млн. Можно считать, что продолжение работы по данному направлению является перспективным и требует развития.

Облачные сервисы. Современные высокоавтоматизированные ТС проводят обработку огромных массивов данных, для этих задач требуется наличие мощного бортового компьютера и больших ресурсов для хранения получаемой информации. В связи с этим в автомобильной промышленности с момента появления подключенных транспортных средств, беспилотных автомобилей и интеллектуальных автомобильных функций развиваются автомобильные облачные вычисления. Облачные вычисления — это технология распределенной обработки данных, в которой компьютерные ресурсы и мощности (различные аппаратные, программные средства, методологии и инструменты) предоставляются пользователю как интернет-сервисы для реализации своих целей, задач, проектов.

Основными и наиболее используемыми облачными сервисами являются:

- IaaS (Infrastructure-as-a-Service — инфраструктура как сервис): аренда виртуальных вычислительных ресурсов и хранилищ. Пользователь получает доступ к выделенным ресурсам — виртуальные серверы, вычислительные мощности, память, операционная система (возможно сменить на свою). Всем аппаратным обеспечением занимается провайдер [3];
- PaaS (Platform-as-a-Service — платформа как сервис): представляет собой готовую платформу для разработки, развертывания и тестирования программ и приложений, которую клиент может подстроить под свои потребности и нужды компании. Провайдер предоставляет доступ к системному ПО (операционные системы, виртуальные машины и т. д.), средствам разработки и тестирования, системам управления базами данных и дополнительным сервисам. Также провайдером предоставляется доступ к инструментам управления, администрирования и инфраструктуре (сервер, сеть, хранилище данных);
- SaaS (Software-as-a-Service — программное обеспечение как сервис): готовые к использованию приложения и сервисы, которые разрабатывает и обслуживает провайдер, не требующие со стороны пользователя никаких действий. ПО и прочие

сервисы разрабатывает и обслуживает провайдер. Пользователь получает доступ через браузер или приложение на персональных устройствах [3].

На рисунке 1 [4] представлена схема ответственности провайдера и клиента облачных сервисов IaaS, PaaS, SaaS.

Кроме основных представленных сервисов существует еще несколько дополнительных решений:

- BaaS (Backup-as-a-Service — резервное копирование как сервис): облачный сервис, предназначенный для создания и надежного хранения резервных копий данных клиентов. В случае сбоя работы пользовательского оборудования у клиента есть возможность восстановить все данные из облака [5];

- DRaaS (Disaster-Recovery-as-a-Service — аварийное восстановление как сервис): копирует и синхронизирует работу системы, реплицирует данные на облачный сервер. Как только со стороны клиентского оборудования или системы происходит аварийная ситуация, вся инфраструктура за считанные минуты перезапускается и начинает работу в запасной облачной системе;

- DBaaS (Database-as-a-Service — база данных как сервис): предоставляет возможность хранения и управления данными. Пользователь получает в аренду полностью настроенную и подготовленную базу данных у провайдера, который осуществляет управление и обслуживание [5];

- STaaS (Storage-as-a-Service — хранение как услуга): представляет собой аренду (бесплатно и платно с различным лимитом хранимых данных) у поставщика облачных услуг места для хранения информации в облаке, которое можно использовать для хранения любых видов данных, необходимых клиенту (мультимедиа, резервные копии и т. д.). К STaaS относятся сервисы Google Drive, Dropbox, Яндекс.Диск;

- SaaS (Security-as-a-Service — безопасность как услуга): предоставляет защиту системы провайдера. Клиенту, в свою очередь, необходимо просто оплатить подписку и осуществить интегра-

цию сервисов безопасности провайдера в свою систему.

Безопасность облачных сервисов. Все больше компаний обращаются к услугам облачных сервисов для обеспечения хранения, обработки и передачи данных, что в свою очередь позволяет сервисам развиваться и предоставлять большее количество облачных услуг. В связи с этим возникает вопрос об обеспечении безопасности использования и хранения данных в облаках, так как утечки и взломы могут нанести большие репутационные и финансовые потери.

Облачная безопасность, не зависящая от зоны ответственности, направлена на защиту таких компонентов, как:

- физические сети — локальные и глобальные, а также оборудование, связанное с обеспечением установки соединения по данным сетям;
- носители данных — любой объект, на который пользователь может записать данные и долгое время осуществлять их хранение;
- серверы данных — аппаратное и программное обеспечение опорной сети;
- сети виртуализации — все виды виртуальных машин и их ПО, хост-компьютеры;
- операционные системы;
- связующие программы — ПО для управления интерфейсами программирования приложений (API);
- среды выполнения — средства запуска и поддержания работы программ;
- данные — вся пользовательская информация, которую он хранит, предоставляет и изменяет;
- приложения — программные сервисы (электронная почта, офисные приложения, приложения для разработки кода);
- оборудование конечного пользователя — персональные компьютеры, мобильные устройства, устройства, относящиеся к интернету вещей [6].

В рамках стека облачных технологий для предоставления эффективной безопасности облака, необходимо обеспечить несколько уровней защиты [7]:

- превентивный контроль: представляет собой меры по предотвращению или снижению появления угроз. Например, средства контроля, позволяющие осуществлять блокировку неавторизованного доступа к конфиденциальным системам и данным;
- детективный контроль: внутренний контроль компании, который направлен на выявление ошибок в уже проведенных операциях посредством аудита, отчетности, мониторинга. В результате могут быть выявлены попытки несанкционированного доступа к системам и данным и их изменений;
- автоматический контроль: в общем понимании это средства, предназначенные для предотвращения, обнаружения и реагирования на обновления безопасности путем сравнения заданных контрольных параметров с имеющимися без участия пользователя;

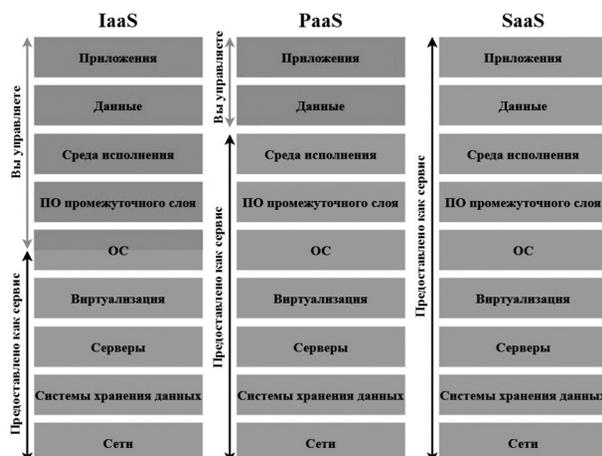


Рисунок 1 — Схема ответственности провайдера и клиента [5]
Figure 1 — Provider and client responsibility scheme [5]

- административный контроль: средства, разработанные для контроля за применением политики, стандартов, практик и процедур безопасности.

Безопасность данных — это аспект безопасности, связанный с технической стороной предотвращения угроз (несанкционированный доступ, кража данных) и возможностью сохранения конфиденциальности, доступности и целостности данных.

Для предотвращения несанкционированного доступа и сохранения конфиденциальности данных необходимо соблюдать следующие требования [8, 9]:

- шифрование: преобразование данных таким образом, чтобы прочитать и восстановить их мог только тот, у кого есть ключ шифрования. Зашифрованные данные даже в случае утечки невозможно восстановить и воспользоваться ими;

- защита сети: для защиты подключения локальной и облачной сети можно использовать Virtual Private Network (VPN — виртуальные частные сети), брандмауэр, отслеживание сетевого трафика. Все это поможет предотвратить несанкционированный доступ и атаки «человек посередине», а также предоставить защиту от DDos-атак;

- управление идентификацией и доступом (Identity and Access Management — IAM): осуществляется управление правами доступа к данным с использованием аутентификации и авторизации. Такой контроль позволяет ограничить пользователям доступ к закрытым данным. К IAM также относится многофакторная аутентификация, управление паролями;

- административный контроль: направлен на предотвращение, обнаружение и устранение угроз;

- планирование хранения данных: дублирование информации путем создания резервных копий, соблюдения действительности копий и инструкции для персонала в случае восстановления данных;

- нормативно-правовые требования: соответствие системы законодательным актам страны по защите данных и информации.

Обновление «по воздуху» в транспортных средствах. В автомобильное облако передается информация от датчиков, радаров и камер, которые контролируют и управляют транспортным средством автоматически без участия водителя. Облачные решения поддерживают непрерывный поток данных и обеспечивают бесперебойную работу сети. По этой причине облачные вычисления применяются в системах ADAS, в том числе и в системах мониторинга функционального состояния водителей.

В общем представлении OTA означает возможность загрузки приложений, услуг и конфигураций по мобильной или сотовой сети. OTA используется для автоматического обновления прошивки, программного обеспечения и даже ключей шифрования. Конкретные категории OTA включают в себя:

- Software over-the-air (SOTA) — обновление программного обеспечения: позволяет отправлять, загружать и устанавливать файлы на подключенные устройства. К ним относятся обновления программного обеспечения, патчи безопасности и новые функции [10]. Например, такие обновления могут принести пользу умному отоплению в подключенных домах или навигационным картам в подключенных транспортных средствах;

- Firmware-over-the-air (FOTA) — обновление прошивки: технология позволяет исправлять ошибки, улучшать функциональность системы и обновлять версии прошивки без вмешательства в устройство. Например, передовые системы помощи водителю (ADAS) внутри подключенных автомобилей нуждаются в этих загрузках для удаленного обновления электронных блоков управления (ECUs — Electronic Control Units) [10];

- Over-the-air service provisioning (OTASP) — предоставление беспроводных услуг: процесс обеспечения рабочих параметров мобильной станции «по воздуху»;

- Over-the-air provisioning (OTAP) — беспроводная конфигурация: представляет собой форму обновления OTA, посредством которой операторы сотовых сетей могут удаленно конфигурировать мобильный телефон (называемый клиентом или мобильной станцией в отраслевом представлении) и обновлять настройки сотовой сети, хранящиеся на его SIM-карте [11];

- Over-the-air parameter administration (OTAPA) — беспроводное управление параметрами: инициированный сетью процесс OTASP конфигурирования рабочих параметров мобильной станции «по воздуху».

Система управления устройством, координируемая производителем, выпускает новое программное обеспечение или обновление микропрограммы. Обновление загружается в облако, где оно ставится в очередь, загружается и проверяется целевым устройством через сотовое или мобильное соединение. После проверки устройство обычно выдает предупреждение, предлагающее владельцу утвердить или отклонить обновление [12]. После утверждения, вручную или автоматически, система устанавливает обновление и отправляет диагностическую информацию производителю. На рисунке 2 показан процесс OTA.

При обновлении OTA от периферии к облаку микроконтроллер получает образы встроенного ПО с удаленного сервера для обновления базового оборудования или приложения. Обновления OTA от шлюза к облаку используют подключенный к Интернету шлюз, который получает обновления с удаленного сервера для обновления самого программного приложения, хост-среды программного приложения или прошивки шлюза.

Крупные производители автомобилей регулярно выпускают обновления SOTA для инфор-



Рисунок 2 — Схема OTA
Figure 2 — Over-the-air update scheme

мационно-развлекательных и навигационных систем. SOTA также может обновлять программное обеспечение, управляющее физическими компонентами автомобиля или системами электронной обработки сигналов. В отличие от SOTA, апгрейды FOTA были реализованы в больших масштабах малым числом производителей автомобилей. Это связано с тем, что обновления FOTA обычно требуют большей вычислительной мощности, более быстрого мобильного подключения и более высокого уровня безопасности.

На основе представленного исследования и более ранних полученных данных об информационных потоках в коммуникационной платформе C-V2X (Cellular Vehicle-to-Everything) для высокоавтоматизированных транспортных средств, описанных в [13, 14], в дальнейшем планируется реализация с использованием макета системы, коммуникации высокоавтоматизированных транспортных средств между собой, интеллектуальными транспортными системами и облачными сервисами.

Заключение. Рассмотрены облачные сервисы, применяемые для обновлений «по воздуху» в высокоавтоматизированных транспортных средствах. Также приведены аспекты безопасности, которые помогут предотвратить возникновение

угроз со стороны третьих лиц и утечку персональных данных клиентов. Представлены технологии перепрограммирования различных бортовых систем и цифровых устройств, подключенных к шинам LIN и CAN автомобиля, «по воздуху». Представленные результаты позволяют конкретизировать структурную схему сервиса и приступить к ее прототипированию с использованием макета системы V2X.

Список литературы

1. Software updates [Electronic resource] // Tesla. — Mode of access: <https://www.tesla.com/support/software-updates>. — Date of access: 04.03.2024.
2. Сумцов, Р. Что и как в современных машинах можно обновить «по воздуху» (и сколько это стоит) [Электронный ресурс] / Р. Сумцов // Auto.ru. — Режим доступа: <https://auto.ru/mag/article/chto-i-kak-mozhno-obnovit-v-mashine-po-vozduhu/>. — Дата доступа: 04.03.2024.
3. Облачная пирамида: IAAS, PAAS и SAAS [Электронный ресурс] // GIGACLOUD. — Режим доступа: <https://gigacloud.ua/ru/blog/navchannja/hmarna-piramida-iaas-paas-ia-saas>. — Дата доступа: 08.03.2024.
4. Облачные сервисы: история появления, виды, динамика рынка. Подробный обзор [Электронный ресурс] // CNewsMarket. — Режим доступа: https://market.cnews.ru/news/top/2019-10-30_oblachnye_servisy_istoriya. — Дата доступа: 08.03.2024.
5. Обзор облачных сервисов [Электронный ресурс] // REG.PY. — Режим доступа: <https://www.reg.ru/blog/obzor-oblachnyh-servisov/>. — Дата доступа: 11.08.2023.
6. Что такое безопасность облака? [Электронный ресурс] // kaspersky. — Режим доступа: <https://www.kaspersky.ru/resource-center/definitions/what-is-cloud-security>. — Дата доступа: 14.03.2024.
7. Что такое облачная безопасность? [Электронный ресурс] // ORACLE. — Режим доступа: <https://www.oracle.com/cis/security/cloud-security/what-is-cloud-security/>. — Дата доступа: 14.03.2024.
8. What is data privacy – and why is it important? [Electronic resource] // Integrate. — Mode of access: <https://www.integrate.io/blog/what-is-data-privacy-why-is-it-important/>. — Date of access: 15.03.2024.
9. What is data protection and privacy? [Electronic resource] // CLOUDIAN. — Mode of access: <https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/>. — Date of access: 15.03.2024.
10. How OTA technology helps update connected cars on the fly [Electronic resource] // SOFTEQ. — Mode of access: <https://www.softeq.com/blog/ota-technology-updating-connected-cars-on-the-go>. — Date of access: 16.03.2024.
11. Sandoval, N. What is Over-the-Air? OTA provisioning explained [Electronic resource] / N. Sandoval // Emnify. — Mode of access: <https://www.emnify.com/iot-glossary/over-the-air>. — Date of access: 18.03.2024.
12. Mixon, E. OTA update (over-the-air update) [Electronic resource] / E. Mixon, C. Steele // TechTarget. — Mode of access: <https://www.techtarget.com/searchmobilecomputing/definition/OTA-update-over-the-air-update>. — Date of access: 18.03.2024.
13. Анализ информационных потоков в коммуникационной платформе C-V2X / В.В. Литарович [и др.] // Актуальные вопросы машиноведения: сб. науч. тр. / Объедин. ин-т машиностроения НАН Беларуси; редкол.: С.Н. Поддубко [и др.]. — Минск, 2019. — Вып. 8. — С. 145–147.
14. Савченко, В.В. Консолидация данных в коммуникационной платформе для высокоавтоматизированных транспортных средств / В.В. Савченко, В.В. Литарович // Тр. НГТУ им. П.Е. Алексеева. — 2022. — № 2(137). — С. 105–114. — DOI: https://doi.org/10.46960/1816-210X_2022_2_105.

DROZD Veranika V.

Researcher of the Department of Active Security and Control Systems of the R&D Center “Electromechanical and Hybrid Power Units of Mobile Machines”¹

E-mail: veronika.litarovich@gmail.com

SAVCHENKO Vladimir V., Ph. D. in Eng., Assoc. Prof.

Head of the Department of Active Security and Control Systems of the R&D Center “Electromechanical and Hybrid Power Units of Mobile Machines”¹

E-mail: uus@tut.by

KOPYTOK Sergei O.

Lead Software Engineer²

E-mail: skb@ekran.by

HOZA Vital V.

Junior Researcher of the Department of Active Security and Control Systems of the R&D Center “Electromechanical and Hybrid Power Units of Mobile Machines”¹

E-mail: mechenistalker@gmail.com

¹Joint Institute of Mechanical Engineering of the NAS of Belarus, Minsk, Republic of Belarus

²OJSC “Ekran”, Borisov, Republic of Belarus

Received 04 April 2024.

CLLOUD STORAGE AND ON-BOARD SYSTEMS REPROGRAMMING TECHNOLOGY FOR HIGHLY AUTOMATED VEHICLES

The dynamic development of technologies in highly automated vehicles requires the development of new methods for transmitting information on board a vehicle in a timely and efficient manner. In this regard, the direction of data transmission over the air is actively developing. The article considers cloud services that can be used for over-the-air updates in highly automated vehicles. The main, most used and additional cloud services are highlighted. The provider and client responsibility scheme for cloud services IaaS, PaaS, SaaS is presented. The aspects of security of cloud services are considered as one of the most important and priority tasks to prevent threats and protect personal data. Specific categories of over-the-air updates used in highly automated vehicles and adjacent infrastructure are presented and described. The process of releasing and installing firmware and software updates over-the-air on highly automated vehicles, their components and adjacent infrastructure is considered. The results obtained are oriented towards a deeper understanding of the over-the-air software upgrade process.

Keywords: security of cloud services, highly automated vehicle, cloud services, over-the-air update, connected car

DOI: <https://doi.org/10.46864/1995-0470-2024-3-68-36-42>

References

1. *Software updates*. Available at: <https://www.tesla.com/support/software-updates> (accessed 04 March 2024).
2. Sumtsov R. *Chto i kak v sovremennykh mashinakh mozno obnovit "po vozdukh" (i skolko eto stoit)* [What and how modern cars can be updated “over the air” (and how much it costs)]. 2022. Available at: <https://auto.ru/mag/article/chto-i-kak-mozhno-obnovit-v-mashine-po-vozduhu/> (accessed 04 March 2024) (in Russ.).
3. *Oblachnaya piramida: IAAS, PAAS i SAAS* [Cloud pyramid: IAAS, PAAS and SAAS]. 2021. Available at: <https://gigacloud.ua/ru/blog/navchannja/hmarna-piramida-iaas-paas-i-saas> (accessed 08 March 2024) (in Russ.).
4. *Oblachnye servisy: istoriya poyavleniya, vidy, dinamika rynka. Podrobnyy obzor* [Cloud services: history of appearance, types, market dynamics. Detailed review]. 2019. Available at: https://market.cnews.ru/news/top/2019-10-30_oblachnye_servisy_istoriya (accessed 08 March 2024) (in Russ.).
5. *Obzor oblachnykh servisov* [Overview of cloud services]. 2022. Available at: <https://www.reg.ru/blog/obzor-oblachnykh-servisov/> (accessed 11 March 2024) (in Russ.).
6. *Chto takoe bezopasnost oblaka?* [What is cloud security?]. Available at: <https://www.kaspersky.ru/resource-center/definitions/what-is-cloud-security> (accessed 14 March 2024) (in Russ.).
7. *Chto takoe oblachnaya bezopasnost?* [What is cloud security?]. Available at: <https://www.oracle.com/cis/security/cloud-security/what-is-cloud-security/> (accessed 14 March 2024) (in Russ.).
8. Tobin D. *What is data privacy – and why is it important?* 2024. Available at: <https://www.integrate.io/blog/what-is-data-privacy-why-is-it-important/> (accessed 15 March 2024).
9. *What is data protection and privacy?* Available at: <https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/> (accessed 15 March 2024).

10. Tsiukhai T. *How OTA technology helps update connected cars on the fly*. 2021. Available at: <https://www.softq.com/blog/ota-technology-updating-connected-cars-on-the-go> (accessed 16 March 2024).
11. Sandoval N. *What is over-the-air? OTA provisioning explained*. 2020. Available at: <https://www.emnify.com/iot-glossary/over-the-air> (accessed 18 March 2024).
12. Mixon E., Steele C. *OTA update (over-the-air update)*. 2022. Available at: <https://www.techtarget.com/searchmobilecomputing/definition/OTA-update-over-the-air-update> (accessed 18 March 2024).
13. Litarovich V.V., Mylnikov V.V., Savchenko V.V., Chernin M.A. Analiz informatsionnykh potokov v kommunikatsionnoy platforme C-V2X [Analysis of information flows in the C-V2X communication platform]. *Aktualnye voprosy mashinovedeniya*, 2019, iss. 8, pp. 145–147 (in Russ.).
14. Savchenko V.V., Litarovich V.V. Konsolidatsiya dannykh v kommunikatsionnoy platforme dlya vysokoavtomatizirovaniykh transportnykh sredstv [Consolidation of data in communication platform for highly automated vehicles]. *Transactions of NNSTU n.a. R.E. Alekseev*, 2022, no. 2(137), pp. 105–114. DOI: https://doi.org/10.46960/1816-210X_2022_2_105 (in Russ.).