DOI10.58880/DKU.2026.01.02

МРНТИ 73.31.17

УДК 629.33

АКТУАЛЬНЫЕ УГРОЗЫ КИБЕРБЕЗОПАСНОСТИ ПОДКЛЮЧЁННЫХ АВТОМОБИЛЕЙ

Д. Н. Батырбеков

Казахстанско-Немецкий университет
Казахстан, г. Алматы

Аннотация

В статье рассматривается проблема кибербезопасности беспроводных интерфейсов современных автомобилей, которые становятся всё более уязвимыми для удаленных атак. Проводится обзор основных беспроводных технологий (Bluetooth, Wi-Fi, сотовая связь, NFC, GPS, UWB, цифровые ключи) и детальный анализ векторов атак на них, включая ретрансляцию сигналов, MITM-атаки и спуфинг. На основе реальных инцидентов, таких как взлом Jeep Cherokee, демонстрируются критические последствия компрометации: от нарушения приватности до угрозы жизни и здоровью. Предлагается обзор современных методов защиты, включая сегментацию сетей, криптографию, а также анализируются требования международных стандартов (ISO/SAE 21434) и регуляторов (UN R155/R156). Делается вывод о необходимости комплексного подхода к безопасности на всех этапах жизненного цикла автомобиля.

Ключевые слова: кибербезопасность автомобилей, беспроводные интерфейсы, CAN-шина, ISO/SAE 21434, UN R155, удаленный взлом, V2X, цифровые ключи.

Введение

Современные автомобили всё больше превращаются в «компьютеры на колёсах»: сотни электронных блоков управления ECU (Electronic Control Unit) обмениваются данными по множеству каналов, в том числе беспроводных [1, с. 1]. Это повышает удобство (мобильные приложения, удалённое управление, автопилот), но одновременно создаёт новые возможности для атаки. Исследование из «Коммерсантъ» говорит, что подавляющее большинство (более 80 %) кибератак на автомобили осуществляется дистанционно [2]. В 2015 г. два специалиста из международной компании в области кибербезопасности «IOActive» Чарли Миллер и Крис Валасек провели эксперимент по удалённому захвату Jeep Cherokee через уязвимость в модуле связи с внешним миром, сумев отключить в движении двигатель и тормоза автомобиля [3]. После данного эксперимента компании Jeep пришлось отозвать 1,4 млн автомобилей, но сама компания официально не подтвердила, что данная лазейка есть [4]. Подобные примеры подчёркивают актуальность темы: международный авто надзор ЕЭК ООН, ужесточают требования по безопасности автомобилей: R155 – это правило обязующее делать авто защищенной от хакеров и R156 – это правило об безопасном обновлении программного обеспечения. Также сама автомобильная индустрия внедряет стандарты ISO/SAE 21434 для противодействия растущим угрозам [5, с. 5].

Методы

В основе исследования лежит метод систематического обзора и анализа литературы. Источниковую базу составили публикации в профильных технических изданиях, отчёты исследовательских компаний (IOActive, VicOne), материалы конференций по кибербезопасности, а также нормативно-правовые документы (регламенты ЕЭК ООН, стандарты ISO/SAE). Всего было проанализировано более 30 источников, из которых 14 непосредственно процитированы в статье.

Анализ проводился в три этапа:

- Сбор данных - идентификация основных беспроводных интерфейсов, используемых в современных автомобилях, и поиск информации об известных уязвимостях.
- Классификация угроз - группировка атак по техническому принципу действия (физический уровень, протоколы связи, человеческий фактор) и по критичности последствий.
- Сравнительный анализ защитных мер - сопоставление рекомендуемых производителями практик с требованиями стандартов ISO/SAE 21434 и UN R155/R156, а также с реальными возможностями злоумышленников, описанными в кейсах (Jeep Cherokee, Nissan Leaf).

Применённый подход позволил не только обобщить разрозненные данные, но и выявить корреляцию между типами уязвимостей и предлагаемыми методами защиты, что отражено в структуре статьи.

Результаты

Обзор беспроводных технологий в современных автомобилях

Автопроизводители внедряют множество беспроводных интерфейсов для комфорта и связности. Основные из них:

- **Bluetooth:** используется для связи без использования рук, потокового аудио и соединения смартфонов, а также для некоторых функций «цифрового ключа». Многие автомобильные экраны управления интегрируют чипы Bluetooth (например, SDK BlueSDK), которые по оценке разработчиков встречаются примерно в 350 миллионах машин (включая Ford, Mercedes-Benz, Škoda, VW и др.) [6]. Bluetooth Low Energy (BLE) уязвим к ситуациям, когда злоумышленник перехватывает или подменяет сигнал между ключом и автомобилей названный «человек по середине», также может записать переданный сигнал между ключом и автомобилем названный replay, и небезопасной подключению к Bluetooth через смартфон [7]. Недавнее исследование выявило четыре слабости в Bluetooth-платформе автомобилей («PerfektBlue»), позволяющие злоумышленнику через подключение к развлекательной системе получить доступ к функциям управления [6, 7].

- **Wi-Fi:** позволяет организовать доступ в интернет в салоне, обновлять Программное Обеспечение по воздуху OTA (Over The Air), обмениваться данными с внешними сервисами. Как и в любой сети Wi-Fi, здесь возможны атаки типа «человек посередине», перехват трафика и внедрение вредоносных пакетов [1, с. 3]. Известно,

что модули Wi-Fi (например, в системе Uconnect) могут служить точкой входа для удалённого взлома – в эксперименте у Чарли Миллера и у Криса Валасека автомобиль в 2015 г. имел активную пользовательскую точку доступа Wi-Fi, через который показано заражение и последующее управление критическими системами [3].

- **Сотовая связь (GSM/4G/5G):** современные автомобили оснащаются модемами для телематики (вызова помощи при аварии, передавать ваше место положение, онлайн-навигация), V2X-коммуникаций это обмен данными автомобиля с окружающей средой, C-V2X также дает возможность работы через сотовые сети 4G/5G и удалённого мониторинга. Сотовый канал обеспечивает связь с серверами производителя и мобильным приложением владельца. Уязвимости в сотовом модуле или протоколах (например, подмена базовых станций, уязвимости в SIM-карте или встроенная электронная SIM-карта) могут позволить злоумышленнику получить доступ к сети автомобиля [8]. В частности, при атаке на Jeep Cherokee злоумышленники использовали соединение через сотовую сеть (кстати, не потребовалось даже знать точный IP – достаточно было «навестись» на GSM-интерфейс) [3; 8].

- **NFC (Near Field Communication):** применяется для бесконтактного доступа к автомобилю (цифровые ключи-смартфоны), запуска двигателя или оплаты внутри автомобиля. NFC имеет радиус действия в считанные сантиметры, но всё же подвержен классическим атакам «прокладки», когда сигнал от ключа перехватили и атакам повторного воспроизведения, при которых ранее перехваченный сигнал используют повторно. Спецификации цифровых ключей (например, Car Connectivity Consortium Digital Key) предусматривают NFC как резервный метод аутентификации при поднесении телефона к считывателю двери или при старте двигателя [9].

- **GPS:** обеспечивает навигацию и геолокацию. Однако GPS-сигнал можно подменить или заглушить: в результате автомобиль может получать ложные данные о своём местоположении и двигаться по неправильному маршруту, не замечая этого водитель [10]. В эксперименте учёных из Microsoft Research даже 38 из 40 водителей поверили поддельным подсказкам навигатора и сбились с маршрута [10]. Кроме того, подавление GPS (глушение сигнала) может временно дезориентировать автомобильные системы безопасности.

- **UWB (Ultra-Wideband):** новая радиотехнология для цифровых ключей и датчиков (например, скрытых в брелоках или смартфонах). UWB отличается высокой точностью измерения расстояния по времени полёта сигнала (до нескольких сантиметров), что делает его устойчивым к атакам «релэ» (когда злоумышленник ретранслирует сигнал брелока на авто на большом расстоянии) [11]. Устройства UWB устанавливаются в премиальных авто и смартфонах (например, Apple CarKey, некоторые модели BMW) для усиления безопасности бесконтактного доступа.

- **Цифровые ключи (смартфоны, умные часы):** объединяют указанные технологии (NFC/BLE/UWB) для открывания и запуска авто. Они позволяют дистанционно делиться доступом и управлять доступом онлайн. По задумке производителей, цифровой ключ должен быть более защищён, чем традиционный брелок: его доступ можно отозвать через приложение, а связь шифруется. Тем не менее, реализация таких систем находится в стадии активного развития, и потенциальные уязвимости пока выявляются исследователями.

Наряду с перечисленным, автомобили могут использовать радиоканалы 433 МГц (старые брелоки, TPMS, RFID-метки), DSRC или 5G-V2X для связи с инфраструктурой. Каждый такой беспроводной интерфейс – потенциальная входная точка для атаки, поэтому важно учитывать весь спектр технологий при анализе безопасности [1, с. 1; 8].

Подробный анализ возможных угроз безопасности

Для каждой беспроводной функции автомобиля существуют специфические и универсальные виды атак. Общие методы включают перехват и воспроизведение (replay) сигналов, атаки «человек посередине» (MITM), энергетические атаки (глушение, джемминг), а также сложные аппаратные атаки на протоколы передачи. Рассмотрим ключевые категории угроз и реальные примеры:

- **Ретрансляция («Relay») и воспроизведение («Replay») сигналов электронного ключа:** наиболее известны случаи краж автомобилей с бесключевым доступом. Злоумышленники размещают передатчик у ключа владельца (например, на пороге дома), а приёмник у автомобиля – и «удлиняют» сигнал. Так они принудительно запирают транспортное средство и даже запускают двигатель, несмотря на то что ключ находится далеко. Ещё в 2011 г. исследователи продемонстрировали атаку на 10 автомобилей 8 марок, используя оборудование стоимостью ~$100; все машины можно было украсть без подбора кода [12]. Эта проблема частично решается применением UWB для привязки расстояния до брелока, но пока не полностью исключена (к примеру, при цифровых ключах по Bluetooth вырабатываются метки времени, хотя и они могут быть уязвимы) [11].

- **Атаки через Bluetooth-интерфейс:** Bluetooth используется в большинстве машин для подключения телефонов. Недавно обнаруженная уязвимость в Bluetooth-платформе «PerfektBlue» в реализации Bluetooth-интерфейса Infotainment-системы позволила удалённо влиять на управление автомобилем через простое подключение злоумышленника к развлекательной системе [6; 7]. По оценке, эта платформа установлена примерно в 350 млн машин (Ford, Mercedes, Skoda, VW и др.) [10]. Хотя заражение остаётся сложным в реальных условиях, сам факт указывает на серьёзность угроз. Эксперты предупреждают, что при наличии уязвимости в Bluetooth «медиасистеме» злоумышленник может затем воспользоваться «промахами в архитектуре» когда гостевой вход в роли Bluetooth системы имеет доступ к ECU (Electronic Control Unit) и проникнуть в критические ECU: открывать двери, включать свет, управлять рулём и другими функциями автомобиля [13].

- **Атаки через Wi-Fi:** Модули Wi-Fi могут использоваться для развлекательных функций и обновлений ПО. Злоумышленник, оказавшись в зоне досягаемости (например, подключившись к хот-споту автомобиля), теоретически способен захватить сессию или внедрить вредоносный трафик. В случае Jeep Cherokee уязвимый Wi-Fi модуль, позволил исследователям получить начальный доступ к системе Uconnect, которая может управлять всей мультимедией и связью в машине, после чего они перешли на шину CAN (внутренняя цифровая сеть) и взяли управление рулём и тормозами [3]. Аналогично, любые незащищённые Wi-Fi-соединения (в том числе в дилерских сервисах и зарядных станциях) могут стать трамплином для проникновения.

- **Атаки через сотовую связь:** Телематические модули, подключённые к мобильным сетям, дают удалённый доступ к автомобилю «из любой точки мира» при наличии интернет-соединения. Как показал эксперимент с Jeep, даже без физического доступа

злоумышленники могли «из ноутбука на другом континенте» отключать двигатель и блокировать тормоза [3]. В сотовых сетях возможны и чисто телекоммуникационные угрозы – подмена мачты (IMSI catcher), уязвимости SIM-карты/электронной SIM-карты, эксплойты в стеке LTE/5G [8]. Кроме того, инженеры описывали сценарии, когда при атаке на облачную инфраструктуру производителя можно получить контроль над OTA-обновлениями автомобилей, установив в них вредоносную прошивку.

- **Спуфинг и подавление GPS-сигнала:** Подделка GPS-данных может завести навигатор (или бортовую систему позиционирования ADAS) на ложный путь [10]. В лабораторных экспериментах алгоритмы GPS-спуфинга обманывают не только навигаторы в телефонах, но и любые встроенные автомобильные системы, в том числе автономные (умные) автомобили. Испытания на реальных дорогах показали, что около 95 % водителей следовали поддельным указаниям и могли выехать на опасные развязки. Глушение GPS, в свою очередь, может нарушить работу бортовых функций (навигатора, антипробуксовочных систем и др.), хотя современные ADAS обычно умеют «переключаться» на другие датчики.

- **Атаки на цифровые ключи:** Цифровой ключ на смартфоне использует сложную логику: сочетание NFC/BLE/UWB, шифрование и биометрию. Тем не менее, возможны сценарии компрометации через уязвимости ОС телефона или Bluetooth-канала. Например, если злоумышленник получит физический доступ к потерянному смартфону с активным ключом (и обойдёт блокировку ОС), он сможет запускать авто. Также обсуждаются атаки на протоколы передачи ключей (MITM при первичной настройке ключа) или эксплойты в приложении производителя. Такие кейсы пока малочисленны, но требуют повышенного внимания: цифровые ключи ещё только входят в массовое использование.

- **Особые сценарии — V2X и автопилот:** С ростом автономных функций машины будут активно обмениваться информацией с инфраструктурой (V2I) и другими автомобилями (V2V) по стандартам DSRC или C-V2X (5G). Здесь возможны подмены сообщений о трафике или дорожных условиях, перехват команд. Например, зафиксирован риск MITM-атаки на DSRC-сообщения, когда «человек посередине» меняет данные о статусе светофоров или сообщениях аварийной ситуации [14]. В случае автомобилей с автопилотом такая подмена может принудительно заставить авто резко затормозить или изменить траекторию. Эти угрозы пока изучаются, но уже понятно, что V2X-коммуникации должны быть защищены криптографически (например, с подписями сообщений) и аутентифицированы.

В совокупности эти примеры демонстрируют, что компрометация беспроводных модулей даёт злоумышленнику широкий спектр возможностей: от кражи и угона машины до вмешательства в её управление и слежки за водителем.

Последствия компрометации беспроводных функций

Успешная атака на беспроводные интерфейсы автомобиля может привести к тяжёлым последствиям. В первую очередь, это **угроза безопасности водителя и пассажиров**. Так, при демонстрации взлома Jeep исследователи смогли не только отключать двигатель и тормоза, но и вызывать ложные сигналы на приборной панели – всё это в движущемся авто может закончиться аварией [3]. Аналогично, в атаке на Nissan Leaf дистанционно поворачивались колёса и блокировались двери [13]. Потенциально злоумышленник может спровоцировать ДТП или заблокировать машину в критической ситуации.

Во-вторых, **уязвляются вопросы приватности и конфиденциальности**. Успешный взлом позволяет следить за перемещениями автомобиля, записывать разговоры из салона и вытаскивать данные учётной записи водителя [13]. Учёные из PCAutomotive в своём отчёте показали, что после эксплойта исследователи могли не только управлять машиной, но и получить доступ к локации авто, текстовым сообщениям и аудиопотоку внутри салона. Это демонстрирует, что компрометация телематической или мультимедийной системы автоматически приводит к утечке личных данных владельца.

Ещё одним последствием является **кража и угоны**. Атаки на системы бесключевого доступа приводят к быстрому угону автомобилей без следов взлома замков [2]. Отдельные устройства, эмулирующие брелоки, уже продаются на чёрном рынке; несколько курьёзных случаев, когда мошенники угоняли десятки Tesla за короткое время при помощи уязвимостей в облачных сервисах, показали масштабность проблемы. В случае массового взлома каршерингов или общественного транспорта атаки могут парализовать транспортную сеть больших городов.

Наконец, компрометация беспроводных каналов ведёт к **значительным экономическим и репутационным потерям автопроизводителя**. После громких инцидентов (например, демонстрации Миллера и Валасека) компании вынуждены проводить масштабные сервисные кампании. Отзыв Jeep Cherokee затронул более миллиона машин [4]. При этом производители обычно подчеркивают, что исправляют не «дефект», а устраняют уязвимость, подтверждая тем не менее высокий уровень риска. Инвестиции в обеспечение безопасности и отзывы выливаются в значительные расходы, а доверие потребителей к бренду падает.

Обсуждение

Методы защиты, практики производителей и стандарты

Для противодействия перечисленным угрозам индустрия и регуляторы применяют комплексные меры:

- **Сегментация сетей и шлюзы:** Современная система управления всего автомобиля предполагает разделение критичных систем (движение, тормоза, рулевое) и развлекательной части (инфотейнмент) на отдельные шины данных (CAN, Ethernet) с изолированными контроллерами. Между ними устанавливаются безопасные шлюзы («брандмауэры»), которые фильтруют и проверяют сообщения [1, с. 4]. Это препятствует тому, чтобы компрометация Bluetooth/USB/Wi-Fi-входа в мультимедийную систему автоматически давала полный доступ к рабочим ECU. В дополнение, на CAN-шину можно ставить системы IDS/IPS (Intrusion Detection/Prevention), умеющие обнаруживать аномалии трафика и отключать подозрительные узлы (например, продукт Autovisor-IDS) [2].

- **Криптографическая защита:** Все внешние соединения, будь то BLE-пара или OTA-обновление, должны надёжно аутентифицироваться и шифроваться. Протоколы ключей должны применяться с «поощрительными» для безопасности политиками (частая ротация сессий, временные метки, проверка расстояния). К примеру, в цифровых ключах применяются чипы с Secure Enclave и симметричные алгоритмы AES с длинными ключами [11]. Защита GPS и V2X-коммуникаций строится на подписях сообщений и PKI (как в IEEE 1609.2), чтобы исключить подмену дорожной информации [14].

- **Стандарты жизненного цикла (ISO/SAE 21434):** В 2021 г. принят международный стандарт по кибербезопасности автомобилестроения ISO/SAE 21434. Он задаёт процессный подход: анализ угроз и оценка рисков (TARA) на ранних этапах проектирования, разработка требований безопасности, проверка кода, а также управление уязвимостями и обновлениями в ходе всей эксплуатации [5, с. 5]. ISO/SAE 21434 конкретизирует верхнеуровневые требования, которые содержатся в регламентах UN R155/156. Компаниям рекомендуется интегрировать эти процессы «с нуля», а не внедрять их лишь формально перед сертификацией.

- **Регламенты UNECE (WP.29 R155/R156):** С июля 2022 г. в ЕС и других странах, подписавших Протокол 1958 г., новым легковым автомобилям предъявляются обязательные требования: внедрить систему управления кибербезопасностью (CSMS) и систему управления обновлениями ПО (SUMS) [5, с. 5]. Производитель обязан проводить анализ угроз, мониторинг инцидентов, управление уязвимостями и поставщиками, внедрить безопасное обновление ПО и оперативно информировать регулятора о киберсобытиях. Таким образом, появляются юридические рамки: безопасность становится не опцией, а требованием к выходу на рынок.

- **Практики производителей:** Многие автопроизводители создают системы «быстрого реагирования»: Bug Bounty-программы (например, у Tesla) и постоянный пентестинг. Активно внедряются OTA-обновления, чтобы исправлять уязвимости «по воздуху» в уже проданных авто [2]. Разрабатываются специализированные Security Operations Centers (SOC), анализирующие телеметрические данные сотен тысяч машин в реальном времени. Например, компания ТВТ («Автовизор») предлагает систему сбора инцидентов на базе SIEM, которая агрегирует данные обо всех авто и выявляет массовые атаки. Стандартизируются безопасные аппаратные модули (Hardware Security Modules) в микроконтроллерах, использование TrustZone и защищённых загрузчиков.

В целом, современные методы защиты опираются на принципы «security by design»: безопасность закладывается на всех этапах разработки и эксплуатации. Это должно сочетаться с гибкими механизмами реагирования (своевременные обновления, изоляция сегментов) и строгой операционной дисциплиной (контроль цепочек поставок). При грамотном применении таких мер шансы атак серьёзно снижаются.

Перспективы развития безопасности

С ростом связности и переходом к автономному вождению требования к безопасности будут только ужесточаться. В будущем машины будут ещё интенсивнее обмениваться данными (4G/5G, C-V2X, Wi-Fi 6E), появятся новые типы угроз (например, атаки на искусственный интеллект в автопилоте, квантовые атаки на криптографию). Решения могут базироваться на машинном обучении для детектирования аномалий в поведении автомобиля и блокчейне для аутентификации сообщений V2X.

В то же время законодательство продолжит развиваться: ожидаются обновления стандартов ISO/SAE 21434 (расширение области применения на мобильные устройства и инфраструктуру), введение европейских регламентов вроде RED и NIS2 в автомобильной сфере, а также совершенствование тестирования (например, киберрейтинги от TÜV). Сеть доверия на дорогах будет формироваться через международное сотрудничество (Auto-ISAC, обмен данными об инцидентах) и образование специалистов.

Кроме того, по мере роста рынка электромобилей и «умных» автомобилей будут развиваться и бизнес-модели – например, страховые тарифы будут учитывать уровень

киберзащищённости транспортного средства. Усилится внимание к защите инфраструктуры (станции зарядки, интеллектуальные светофоры) и к защите пользовательских устройств (телефонов с цифровыми ключами).

В целом, будущее безопасности беспроводных функций автомобилей видится в тесной интеграции отраслевых стандартов, проактивной защите на основе больших данных и постоянном «забеге» производителей с исследователями — каждый пытается опередить угрозы.

Заключение

По моему мнению, современные автомобили демонстрируют небывалый уровень связности, но эта же связность открывает перед злоумышленниками множество возможностей для взлома. В статье рассмотрены основные беспроводные интерфейсы (Bluetooth, Wi-Fi, GSM/5G, NFC, GPS, UWB и др.) и типичные методы атак через них – от ретрансляций сигналов ключей до спуфинга GPS и удалённого доступа через телематический модуль. Реальные кейсы (взлом Jeep Cherokee, Nissan Leaf, уязвимость Bluetooth-Infotainment) которые показали, что последствия атак могут быть катастрофическими: от кражи машины до вмешательства в управление на высокой скорости [3; 13].

Для противодействия этим рискам индустрия и регуляторы выстраивают многоуровневую защиту: разделяют сети, внедряют криптографию и мониторинг, стандартизируют процессы разработки (ISO/SAE 21434) и вводят обязательные требования (UNECE R155/R156). В перспективе важнейшими направлениями станут развитие систем обнаружения аномалий на базе ИИ и укрепление безопасности V2X-коммуникаций.

По моему мнению, вся безопасность современных автомобилей должна проектироваться «с нуля», а беспроводные интерфейсы – защищаться наравне с основными системами для безопасности людей. Я рекомендую концернам применять комплексный подход: анализ рисков (TARA) на этапе проектирования, внедрение сегментации и шифрования, обеспечение своевременных обновлений и обмен информацией об угрозах. Лишь такая архитектура позволит сохранить безопасность водителей и доверие к новым технологиям.

Список литературы

1. Connected Car Security: Automotive IoT Threats and Protection [Electronic resource] // Device Authority. — URL: https://deviceauthority.com/connected-car-security-automotive-iot-threats-and-protection/ (дата обращения: 20.01.2026).
2. Программное обеспечение безопасности [Электронный ресурс] // Коммерсантъ. — URL: https://www.kommersant.ru/doc/5293297 (дата обращения 20.01.2026).
3. Greenberg A. Hackers Remotely Kill a Jeep on the Highway—With Me in It [Electronic resource] / A. Greenberg // WIRED. — 2015. — 21 July. — URL: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (дата обращения: 20.01.2026).
4. West D. M. Jeep Cherokee hack offers important lessons on the "Security of Things" [Electronic resource] / D. M. West // Brookings. — 2015. — 3 August. — URL: https://www.brookings.edu/articles/jeep-cherokee-hack-offers-important-lessons-on-the-security-of-things/ (дата обращения: 20.01.2026).
5. Кибербезопасность в автомобильной промышленности: как обеспечить соответствие положениям ЕЭК ООН [Электронный ресурс] // Kaspersky ICS CERT. — 2024. — 7 февраля. — URL: https://ics-

cert.kaspersky.ru/publications/reports/2024/02/07/cybersecurity-in-the-automotive-industry-ensuring-compliance-with-unece-regulations/ (дата обращения: 20.01.2026).
6. Защищаем автомобиль от взлома через Bluetooth-уязвимость PerfektBlue [Электронный ресурс] // Блог Касперского. — URL: https://www.kaspersky.ru/blog/perfektblue-bluetooth-car-hack/40315/ (дата обращения: 20.01.2026).
7. PerfektBlue: исследователи нашли четыре уязвимости в Bluetooth-стеке для авто [Электронный ресурс] // Хакер. — URL: https://xakep.ru/2022/09/12/perfektblue/ (дата обращения: 20.01.2026).
8. Internet Crime Complaint Center (IC3). Motor Vehicles Increasingly Vulnerable to Remote Exploits [Electronic resource] // IC3. — 2016. — 17 March. — URL: https://www.ic3.gov/PSA/2016/PSA160317 (дата обращения: 20.01.2026).
9. From 433MHz to Digital Keys: The Security Evolution of Vehicle Access [Electronic resource] // EE Times Asia. — URL: https://www.eetasia.com/from-433-mhz-to-digital-keys-the-security-evolution-of-vehicle-access/ (дата обращения: 20.01.2026).
10. Исследователи предложили обманывать навигационные системы с помощью GPS-спуфинга [Электронный ресурс] // Хакер. — 2018. — 16 июля. — URL: https://xakep.ru/2018/07/16/new-gps-spoofing-attack/ (дата обращения: 20.01.2026).
11. From Key Fob to UWB: How Hackers Hijack Vehicle Entry Systems [Electronic resource] // VicOne. — URL: https://vicone.com/blog/from-key-fob-to-uwb-how-hackers-hijack-vehicle-entry-systems (дата обращения: 20.01.2026).
12. Электронные ключи автомобилей легко взломать [Электронный ресурс] // Хакер. — 2011. — 24 января. — URL: https://xakep.ru/2011/01/24/54599/ (дата обращения: 20.01.2026).
13. Электромобиль Nissan Leaf уязвим для кибератак. Хакерам удалось удаленно перехватить рулевое управление [Электронный ресурс] // Cnews. — 2025. — 13 мая. — URL: https://www.cnews.ru/news/top/2025-05-13_elektromobil_nissan_leaf_okazalsya (дата обращения: 20.01.2026).
14. Кибербезопасность автономных транспортных средств: угрозы, уязвимости и стратегии защиты [Электронный ресурс] // SecurityMedia. — URL: https://securitymedia.org/info/kiberbezopasnost-avtonomnykh-transportnykh-sredstv-ugrozy-uyazvimosti-i-strategii-zashchity.html (дата обращения: 20.01.2026).

REFERENCES

1. Connected Car Security: Automotive IoT Threats and Protection [Electronic resource] // Device Authority. — URL: https://deviceauthority.com/connected-car-security-automotive-iot-threats-and-protection/ (Accessed: 20.01.2026).

2. Programmnoe obespechenie bezopasnosti [Security Software] [Electronic resource] // Kommersant. — URL: https://www.kommersant.ru/doc/5293297 (Accessed: 20.01.2026). (In Russ.)

3. Greenberg A. Hackers Remotely Kill a Jeep on the Highway—With Me in It [Electronic resource] / A. Greenberg // WIRED. — 2015. — 21 July. — URL: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (Accessed: 20.01.2026).

4. West D. M. Jeep Cherokee hack offers important lessons on the "Security of Things" [Electronic resource] / D. M. West // Brookings. — 2015. — 3 August. —

URL: https://www.brookings.edu/articles/jeep-cherokee-hack-offers-important-lessons-on-the-security-of-things/ (Accessed: 20.01.2026).

5. Kiberbezopasnost' v avtomobil'noj promyshlennosti: kak obespechit' sootvetstvie polozheniyam EEK OON [Cybersecurity in the Automotive Industry: Ensuring Compliance with UNECE Regulations] [Electronic resource] // Kaspersky ICS CERT. — 2024. — 7 February. — URL: https://ics-cert.kaspersky.ru/publications/reports/2024/02/07/cybersecurity-in-the-automotive-industry-ensuring-compliance-with-unece-regulations/ (Accessed: 20.01.2026). (In Russ.)
6. Zashchishchaem avtomobil' ot vzloma cherez Bluetooth-uyazvimost' PerfektBlue [Protecting a car from hacking via the PerfektBlue Bluetooth vulnerability] [Electronic resource] // Kaspersky Blog. — URL: https://www.kaspersky.ru/blog/perfektblue-bluetooth-car-hack/40315/ (Accessed: 20.01.2026). (In Russ.)
7. PerfektBlue: issledovateli nashli chetyre uyazvimosti v Bluetooth-steke dlya avto [PerfektBlue: Researchers Find Four Vulnerabilities in Automotive Bluetooth Stack] [Electronic resource] // Xakep. — URL: https://xakep.ru/2022/09/12/perfektblue/ (Accessed: 20.01.2026). (In Russ.)
8. Internet Crime Complaint Center (IC3). Motor Vehicles Increasingly Vulnerable to Remote Exploits [Electronic resource] // IC3. — 2016. — 17 March. — URL: https://www.ic3.gov/PSA/2016/PSA160317 (Accessed: 20.01.2026).
9. From 433MHz to Digital Keys: The Security Evolution of Vehicle Access [Electronic resource] // EE Times Asia. — URL: https://www.eetasia.com/from-433-mhz-to-digital-keys-the-security-evolution-of-vehicle-access/ (Accessed: 20.01.2026).
10. Issledovateli predlozhili obmanyvat' navigatsionnye sistemy s pomoshch'yu GPS-spufinga [Researchers propose tricking navigation systems with GPS spoofing] [Electronic resource] // Xakep. — 2018. — 16 July. — URL: https://xakep.ru/2018/07/16/new-gps-spoofing-attack/ (Accessed: 20.01.2026). (In Russ.)
11. From Key Fob to UWB: How Hackers Hijack Vehicle Entry Systems [Electronic resource] // VicOne. — URL: https://vicone.com/blog/from-key-fob-to-uwb-how-hackers-hijack-vehicle-entry-systems (Accessed: 20.01.2026).
12. Elektronnye klyuchi avtomobilej legko vzlomat' [Car electronic keys are easy to hack] [Electronic resource] // Xakep. — 2011. — 24 January. — URL: https://xakep.ru/2011/01/24/54599/ (Accessed: 20.01.2026). (In Russ.)
13. Elektromobil' Nissan Leaf uyazvim dlya kiberatak. Khakeram udalos' udalenno perekhvatit' rulevoe upravlenie [Nissan Leaf electric car vulnerable to cyberattacks. Hackers managed to remotely intercept steering control] [Electronic resource] // Cnews. — 2025. — 13 May. — URL: https://www.cnews.ru/news/top/2025-05-13_elektromobil_nissan_leaf_okazalsya (Accessed: 20.01.2026). (In Russ.)
14. Kiberbezopasnost' avtonomnykh transportnykh sredstv: ugrozy, uyazvimosti i strategii zashchity [Cybersecurity of Autonomous Vehicles: Threats, Vulnerabilities and Protection Strategies] [Electronic resource] // SecurityMedia. — URL: https://securitymedia.org/info/kiberbezopasnost-avtonomnykh-transportnykh-sredstv-ugrozy-uyazvimosti-i-strategii-zashchity.html (Accessed: 20.01.2026). (In Russ.)

SUMMARY

WIRELESS TECHNOLOGIES IN MODERN VEHICLES: ANALYSIS OF CYBERSECURITY THREATS AND PROTECTION METHODS

D.N. Batyrbekov[1]

1. Kazakh-German University
Kazakhstan, Almaty

The article addresses the cybersecurity challenges of wireless interfaces in modern vehicles, which are becoming increasingly vulnerable to remote attacks. It provides an overview of key wireless technologies (Bluetooth, Wi-Fi, cellular, NFC, GPS, UWB, digital keys) and a detailed analysis of attack vectors, including signal relaying, MITM attacks, and spoofing. Based on real-world incidents, such as the Jeep Cherokee hack, the critical consequences of compromise are demonstrated, ranging from privacy violations to threats to life and health. An overview of modern protection methods, including network segmentation and cryptography, is offered, and the requirements of international standards (ISO/SAE 21434) and regulators (UN R155/R156) are analyzed. The conclusion emphasizes the need for a comprehensive approach to security throughout the entire vehicle lifecycle.

Keywords: automotive cybersecurity, wireless interfaces, CAN bus, ISO/SAE 21434, UN R155, remote hack, V2X, digital keys.

ТҮЙІНДЕМЕ

ҚАЗІРГІ АВТОМОБИЛЬДЕРДЕГІ СЫМСЫЗ ТЕХНОЛОГИЯЛАР: КИБЕРҚАУІПСІЗДІК ҚАТЕРЛЕРІН ТАЛДАУ ЖӘНЕ ҚОРҒАУ ӘДІСТЕРІ

Д.Н. Батырбеков[1]

1. Қазақстан-Неміс Университеті

Қазақстан, Алматы

Мақалада қашықтан шабуылдарға осал болып отырған заманауи автомобильдердің сымсыз интерфейстерінің киберқауіпсіздік мәселесі қарастырылады. Негізгі сымсыз технологияларға (Bluetooth, Wi-Fi, ұялы байланыс, NFC, GPS, UWB, сандық кілттер) шолу жасалып, оларға жасалатын шабуыл векторларына, соның ішінде сигналдарды релелендіруге, MITM-шабуылдарына және спуфингке егжей-тегжейлі талдау жүргізіледі. Jeep Cherokee автомобилін бұзу сияқты нақты оқиғалар негізінде бұзылудың ауыр зардаптары көрсетіледі: жеке өмірге қол сұғушылықтан өмір мен денсаулыққа төнетін қатерге дейін. Қазіргі заманғы қорғау әдістеріне, соның ішінде желілерді сегменттеуге және криптографияға шолу жасалып, халықаралық стандарттардың (ISO/SAE 21434) және реттеушілердің (UN R155/R156) талаптары талданады. Автомобильдің барлық өмірлік циклі кезеңінде қауіпсіздікке кешенді көзқарас қажеттігі туралы қорытынды жасалады.

Түйінді сөздер: автомобильдер киберқауіпсіздігі, сымсыз интерфейстер, CAN шинасы, ISO/SAE 21434, UN R155, қашықтан бұзу, V2X, сандық кілттер.

Автор: Батырбеков Диас Нурланулы - студент Казахстанско-Немецкий университета, факультет информационного инжиниринга в экономике student.batyrbekov@dku.kz