



Министерство науки и высшего образования Российской Федерации
Калужский филиал
федерального государственного автономного
образовательного учреждения высшего образования
«Московский государственный технический университет имени Н.Э. Баумана
**(национальный исследовательский университет)»
(КФ МГТУ им. Н.Э. Баумана)**

ФАКУЛЬТЕТ ИУК «Информатика и управление»

КАФЕДРА ИУК4 «Программное обеспечение ЭВМ, информационные технологии»

НАУЧНО-ИССЛЕДОВАТЕЛЬСКАЯ РАБОТА

«Исследование методов считывания и анализа данных CAN-шины автомобиля с использованием микроконтроллерных систем на базе MCP2515/TJA1050 и ESP32»

Студент гр. ИУК4-72Б _____ (Губин Е.В.)
(подпись) (Ф.И.О.)

Руководитель _____ (Алёхина Е.Д.)
(подпись) (Ф.И.О.)

Оценка руководителя _____ баллов _____
30-50 (дата)

Оценка защиты _____ баллов _____
30-50 (дата)

Оценка работы _____ баллов _____
(оценка по пятибалльной шкале)

Комиссия: _____ (Гагарин Ю.Е.)
(подпись) (Ф.И.О.)

_____ (Широкова Е.В.)
(подпись) (Ф.И.О.)

_____ (Алёхина Е.Д.)
(подпись) (Ф.И.О.)

*Калужский филиал федерального государственного автономного образовательного учреждения
высшего образования*
«Московский государственный технический университет имени Н.Э. Баумана
(национальный исследовательский университет)»
(КФ МГТУ им. Н.Э. Баумана)

УТВЕРЖДАЮ

Заведующий кафедрой ИУК4
(Гагарин Ю.Е.)
«02 » сентября 2025 г.

З А Д А Н И Е на НАУЧНО-ИССЛЕДОВАТЕЛЬСКУЮ РАБОТУ (НИР)

За время выполнения НИР студенту необходимо:

1. Выполните анализ полученной информации по заданной теме, осуществите обработку и систематизацию собранных материалов; сформулируйте выводы, адекватные полученным результатам; подготовьте отчет по выполненной работе.

в том числе:

- изучить принципы работы и историю развития автомобильной шины CAN;
- проанализировать стандарты и спецификации, регулирующие передачу данных в CAN-сетях;
- рассмотреть архитектуру и режимы работы контроллера MCP2515 и трансивера TJA1050;
- изучить методы подключения микроконтроллеров (на примере ESP32) к CAN-шине и способы безопасного считывания данных;
- исследовать вопросы информационной безопасности автомобильных сетей и определить меры предотвращения несанкционированного воздействия;
- выявить преимущества и ограничения применения CAN-шины для диагностических и исследовательских задач.

2. Подготовить реферативный отчет о проделанной работе и защитить результаты НИР.

Дата выдачи задания «02 » сентября 2025 г.

Руководитель	02.09.2025г. (подпись, дата)	E.Д. Алёхина (И.О. Фамилия)
Студент	02.09.2025г. (подпись, дата)	E.В. Губин (И.О. Фамилия)

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	4
1. АРХИТЕКТУРА И ПРИНЦИПЫ РАБОТЫ CAN-ШИНЫ АВТОМОБИЛЯ	6
1.1. Основные характеристики CAN-шины	6
1.2. Структура CAN-кадра и основные типы сообщений	7
1.3. Особенности автомобильных сетей и распределение функций	9
2. АППАРАТНЫЕ И ПРОГРАММНЫЕ СРЕДСТВА ДЛЯ ЧТЕНИЯ ДАННЫХ ИЗ CAN-ШИНЫ	11
2.1. Контроллер MCP2515 и трансивер TJA1050	11
2.2. Использование ESP32 для работы с CAN	12
2.3. Режимы работы MCP2515	13
3. БЕЗОПАСНОСТЬ РАБОТЫ С CAN-ШИНОЙ И МЕТОДЫ ЗАЩИТЫ	15
3.1. Уязвимости CAN-шины	15
3.2. Обеспечение безопасности при исследовании CAN-шины	16
3.3. Ограничения и предотвращение вреда автомобилю	17
ЗАКЛЮЧЕНИЕ	19
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	21

ВВЕДЕНИЕ

Современные автомобили представляют собой сложные киберфизические системы, в которых функции управления распределены между множеством электронных блоков. Координация их работы обеспечивается сетевыми протоколами, среди которых ключевую роль играет CAN-шина (Controller Area Network). Она используется практически во всех транспортных средствах — от легковых автомобилей до коммерческой техники — благодаря своей надежности, устойчивости к помехам и способности эффективно передавать данные в реальном времени.

Актуальность выбранной темы обусловлена растущим интересом к анализу данных транспортных систем, разработке интеллектуальных информационных устройств и систем диагностики автомобиля, а также развитию направления Internet of Things (IoT) и встраиваемых технологий. Считывание и обработка CAN-сообщений является базовой задачей при создании телематических терминалов, диагностических приборов, систем мониторинга и обеспечения безопасности. Кроме того, правильная работа с CAN-шиной требует понимания её архитектуры, особенностей формата сообщений, аппаратных средств и мер предосторожности — что делает изучаемую область важной как в теоретическом, так и в прикладном аспекте.

Практическая значимость исследования заключается в том, что результаты НИР позволяют разработать безопасный и корректный метод чтения данных с CAN-шины автомобиля с использованием модулей MCP2515 и TJA1050, а также микроконтроллера ESP32. Эти знания являются основой для последующей реализации системы чтения и анализа данных, которая будет использоваться в рамках выпускной квалификационной работы. Исследование затрагивает как аппаратные принципы взаимодействия с CAN-шиной, так и программные аспекты её обработки, включая обеспечение безопасности и предотвращение вмешательства в работу автомобиля.

Теоретическая ценность заключается в систематизации сведений о протоколах CAN, структуре данных, режимах работы контроллеров и специфике применения MCP2515 в связке с трансивером TJA1050. Особое внимание уделяется аспектам безопасности, поскольку любые разработки, связанные с автомобильными сетями, должны учитывать недопустимость вмешательства в критически важные функции транспортного средства.

Цель данного исследования — изучить архитектуру CAN-шины автомобиля и разработать обоснованный подход к безопасному считыванию данных с использованием модулей MCP2515/TJA1050 и микроконтроллера ESP32.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Проанализировать структуру и принципы работы CAN-шины, включая форматы кадров, типы сообщений и используемые скорости обмена.
2. Изучить аппаратные модули MCP2515 и TJA1050, определить особенности их взаимодействия с микроконтроллером ESP32.
3. Рассмотреть режимы работы контроллера MCP2515 и выбрать наиболее безопасный режим для исследования CAN-шины (например, listen-only).
4. Изучить аспекты безопасности CAN-шины, определить потенциальные угрозы и способы предотвращения влияния на работу автомобиля при чтении данных.
5. Сформировать рекомендации по практическому подключению и безопасной работе с автомобильной CAN-сетью.

Таким образом, данное введение формирует основу для выполнения исследования и обосновывает значимость изучаемой темы как для дальнейшей разработки системы чтения CAN-данных в рамках ВКР, так и для расширения знаний в области автомобильных информационных технологий.

1. АРХИТЕКТУРА И ПРИНЦИПЫ РАБОТЫ САН-ШИНЫ АВТОМОБИЛЯ

1.1. Основные характеристики CAN-шины

Controller Area Network (CAN) — серийный протокол обмена данными, изначально разработанный для автомобильных систем, но широко применяемый и в промышленности. Основные свойства CAN:

- Детерминированность и приоритеты. CAN использует механизм арбитража на уровне идентификаторов сообщений: при одновременной передаче нескольких узлов выигрыш получает кадр с меньшим (в смысле двоичного значения) идентификатором — это обеспечивает приоритет для критичных сообщений (например, управления двигателем или тормозами).
- Устойчивость к помехам. Физический уровень — дифференциальная передача по витой паре (CAN_H и CAN_L) — обеспечивает хорошую иммунизацию к электромагнитным помехам.
- Механизмы обнаружения и коррекции ошибок. CAN содержит многоуровневые средства выявления ошибок (бит-мониторинг, CRC, проверка формата кадра, контроль стэфлинга и т.д.) и алгоритмы «ограничения неисправных узлов» (error confinement).
- Гибкость в топологии. Наиболее распространена линейная шина с двухконцевой терминалторной нагрузкой (обычно $120\ \Omega$ на концах). Возможны ответвления, но они ограничены длиной и помехоёмкостью. Версии и стандарты. На практике встречаются несколько стандартов:
 - CAN 2.0A (Standard Frame) — 11-битный идентификатор (11-bit ID).
 - CAN 2.0B (Extended Frame) — расширенный формат с 29-битным идентификатором (11 + 18 бит), совместимый с прежними режимами.
 - CAN FD (Flexible Data-rate) — современное расширение протокола, позволяющее передавать до 64 байт данных в одном кадре и применять более высокую скорость передачи в фазе данных. CAN FD сохраняет базовый принцип арбитража по идентификатору, но меняет правила скорости и формата данных.

Типичные скорости обмена. В автомобильной электронике часто используются следующие скорости (варианты зависят от конкретной подсети и производителя):

- 125 kbit/s — для низкоскоростных подсетей (комфорт, климат и др.);
- 250 kbit/s — широко применимый вариант (оборудование 2000-х);
- 500 kbit/s — часто для силовых и критичных подсетей (двигатель, трансмиссия);

Для CAN FD — физическая часть может работать значительно быстрее в фазе данных (зависит от реализации).

Факторы, влияющие на выбор скорости: длина и топология шины, требования по задержке и объёму данных, электромагнитная среда.

1.2. Структура CAN-кадра и основные типы сообщений

CAN-кадр — это структурированная единица обмена. Различают стандартный (11-бит ID) и расширенный (29-бит ID) форматы, а также несколько видов кадров по назначению.

Формат классического CAN-кадра (CAN 2.0 — упрощённо)

Основные поля стандартного data frame:

1. Start of Frame (SOF) — синхронизирующий бит.
2. Arbitration Field — содержит идентификатор (11 бит для стандартного кадра) и бит RTR (Remote Transmission Request).
3. Control Field — включает в себя IDE (индикатор расширенного идентификатора), r0 и DLC (Data Length Code — длина данных в байтах).
4. Data Field — 0–8 байт в классическом CAN (в CAN FD — до 64 байт).
5. CRC Field — контрольная сумма кадра.
6. ACK Field — поле подтверждения; принимающие узлы устанавливают доминантный бит в ACK, если кадр принят.
7. End of Frame (EOF) и интер-пакетный интервал.

Ключевые поля:

- Arbitration ID (идентификатор). Определяет приоритет и логическую «тему» сообщения (например, ID для скорости, ID для RPM). Низкое числовое значение — высокий приоритет.
- DLC (0–8). Количество байт данных (в классическом CAN).
- RTR (Remote Transmission Request). Позволяет запросить у другого узла передачу данных (remote frame).
- IDE. Определяет, используется ли стандартный или расширенный идентификатор.

Типы кадров

- Data frame — содержит полезные данные (основной тип).
- Remote frame — запрос на передачу данных (без data field).
- Error frame — формируется узлом при обнаружении ошибки; прерывает текущий кадр.
- Overload frame — сигнал для увеличения интервала между кадрами (редко применяется на практике).

Арбитраж выполняется «без потерянных битов»: при передаче каждого бита узлы мониторят шину. Битовое значение «доминант» (обычно лог.0) «перекрывает» рецессивный (лог.1). Узел, который попытался передать рецессивный, а видит доминантный — прекращает передачу и ждёт следующей возможности. Это эффективно даёт высший приоритет сообщениям с меньшими ID.

CAN включает несколько механизмов обнаружения ошибок:

- CRC-проверка данных;
- Bit stuffing — после пяти одинаковых битов вставляется противоположный бит; нарушение правила даёт форм-ошибку;
- Форматная проверка — неверный формат кадра;
- Bit monitoring — узел сравнивает отправляемые и наблюдаемые биты;
- ACK проверка — отправитель ждёт подтверждения от хотя бы одного приёмника.

При накоплении ошибок узел может перейти в Error Passive или Bus Off состояние — это защищает шину от неисправных узлов.

1.3. Особенности автомобильных сетей и распределение функций

Автомобильная архитектура использует CAN не как один общий канал для всего, а как набор подсетей, каждая из которых решает свои задачи.

Разделение подсетей (примерная модель)

- Powertrain CAN (двигатель/трансмиссия). Высокий приоритет, высокая скорость (часто 500 kbit/s). Передаются данные о оборотах, крутящем моменте, температуре, командах управления двигателем.
- Chassis CAN (тормоза, подвеска). Критические системы безопасности, также могут иметь высокую скорость.
- Body CAN (комфорт, двери, свет). Низкая и средняя скорость (125–250 kbit/s). Здесь идут сообщения о состоянии дверей, стеклоподъёмниках, климате.
- Diagnostic CAN / OBD-II. Интерфейс диагностики; стандартные PIDs и протоколы (см. ISO 15765-4 для CAN в OBD-II). Диагностический канал может использовать те же физические линии или отдельный диагностический адаптер.

Разделение позволяет уменьшать нагрузку и повышать безопасность — критичные сообщения из powertrain не «засоряются» трафиком от мультимедиа.

Передача дифференциальная: логическое состояние определяется разницей между CAN_H и CAN_L.

Доминантное состояние обычно соответствует разности (CAN_H > CAN_L) примерно на ~2 В, рецессивное — близко к потенциалу питания.

На концах шины устанавливаются терминалы (типично 120 Ω между CAN_H и CAN_L), которые поглощают отражения при высоких скоростях и длинных линиях.

В CAN передаются самые разные параметры, приведём несколько типичных примеров (как практическая иллюстрация — часто используемые сведения в VAG/OBD и т.д.):

- Скорость автомобиля (Vehicle Speed). Часто публикуется с высокой периодичностью в соответствующем ID.
- Обороты двигателя (Engine RPM). Критичная информация для блока управления трансмиссией.
- Положение дроссельной заслонки / педали (Throttle Position).
- Состояния контроллеров (fault codes, статус ABS, переключения передач).
- Данные климат-контроля, датчиков дверей, состояния освещения — в отдельных подсетях.

Также в диагностическом интерфейсе OBD-II используются PID (Parameter IDs) — стандартизованные коды для запроса конкретных параметров (например, 0x0C — RPM, 0x0D — vehicle speed). Диагностические запросы, как правило, инициируются внешним тестером или диагностическим контроллером.

Автопроизводители часто вводят собственное распределение ID и форматов данных — одно и то же значение ID у разных производителей может означать разные вещи. Поэтому для анализа CAN-трафика важна карта идентификаторов (CAN-map) конкретного автомобиля, получаемая экспериментально или из сервисной документации.

2. АППАРАТНЫЕ И ПРОГРАММНЫЕ СРЕДСТВА ДЛЯ ЧТЕНИЯ ДАННЫХ ИЗ CAN-ШИНЫ

2.1. Контроллер MCP2515 и трансивер TJA1050

Модуль MCP2515 + TJA1050 является одним из наиболее распространённых решений для бюджетного и удобного подключения микроконтроллеров к CAN-шине. Он используется как в простых DIY-проектах, так и в профессиональных телематических устройствах.

MCP2515 — это автономный CAN-контроллер, полностью реализующий протокол CAN 2.0A/B. Он работает по интерфейсу SPI, благодаря чему легко интегрируется с любым микроконтроллером, поддерживающим этот интерфейс.

Ключевые возможности MCP2515:

- Поддержка CAN 2.0A (11-бит ID) и CAN 2.0B (29-бит ID)
- Скорость обмена до 1 Мбит/с
- Реализация всего стека CAN на аппаратном уровне
- Буферы передачи (TXB0–TXB2) и приема (RXB0–RXB1)
- Аппаратные маски и фильтры для отбора нужных ID
- Поддержка прерываний
- Возможность работы в разных режимах (Normal, Sleep, Loopback, Listen-Only)
- MCP2515 управляется через набор регистров, позволяющих конфигурировать скорость, фильтры, маски, состояние буферов, уровень ошибок и др. Для работы с ним существует большое количество библиотек под Arduino и ESP-IDF.

TJA1050 — это высокоскоростной CAN-трансивер, обеспечивающий физическое соединение между логикой микроконтроллера и дифференциальной линией CAN_H/CAN_L.

Основные функции TJA1050:

- Преобразование логических уровней MCP2515 в дифференциальные сигналы
- Обеспечение устойчивой передачи на высоких скоростях

- Защита шины и модулей от перенапряжений и помех
- Соответствие стандартам ISO 11898

TJA1050 не выполняет логику CAN — он лишь обеспечивает физический уровень, то есть *electrical interface*.

Таким образом, связка выглядит так:

`ESP32 \rightleftarrows SPI \rightleftarrows MCP2515 \rightleftarrows TJA1050 \rightleftarrows CAN-шина автомобиля`

Типовое подключение MCP2515 к ESP32:

MCP2515	ESP32
SCK	GPIO (SPI clock)
SI	MOSI
SO	MISO
CS	GPIO (chip select)
INT	GPIO (прерывание)

Питание модуля — 5 В, но SPI-интерфейс часто совместим с 3.3 В логикой (зависит от платы). TJA1050 работает на 5 В, но MCP2515 принимает 3.3 В как высокий сигнал на SPI.

2.2. Использование ESP32 для работы с CAN

ESP32 — мощный микроконтроллер с Wi-Fi, Bluetooth и большим количеством периферии. Важное преимущество ESP32 — высокая производительность и возможность параллельной обработки данных благодаря двум ядрам.

Совместимость CAN и ESP32:

- Высокая тактовая частота — позволяет быстро обрабатывать входящие кадры
- SPI интерфейс — обеспечивает надёжную работу с MCP2515
- Возможность подключения по Wi-Fi/Bluetooth — удобно для телематики
- Большой выбор библиотек и примеров

Для работы с MCP2515 на ESP32 распространены:

- Arduino MCP_CAN — готовая библиотека с удобными функциями

- ESP-IDF CAN driver (TWAI) + внешняя MCP2515 библиотека
- ESP32CAN — альтернативная реализация

Пример типовых функций:

- CAN.begin(CAN_500KBPS, MCP_8MHZ) — запуск контроллера
- CAN.readMsgBuf(&len, buf) — чтение данных
- CAN.getId() — получение ID кадра
- CAN.filter() — настройка фильтров

При запуске MCP2515 необходимо указать:

- частоту кварца модуля (часто 8 МГц или 16 МГц)
- желаемую скорость CAN (125/250/500/1000 kbit/s)
- режим работы (normal/listen-only и др.)

Фильтры и маски позволяют принимать только нужные кадры по ID, что снижает нагрузку на ESP32.

2.3. Режимы работы MCP2515

MCP2515 поддерживает несколько режимов работы. Это особенно важно при исследовании CAN-шины автомобиля, поскольку неправильная конфигурация может привести к передаче данных в сеть — а это недопустимо в рамках безопасного анализа.

Основные режимы

1. Normal Mode

- Стандартный режим: модуль может передавать и принимать данные.
- Не рекомендуется при пассивном анализе CAN-шины!

2. Listen-Only Mode (режим только чтение)

- Модуль только принимает данные и никогда не передаёт.
- Идеален для безопасного анализа автомобильной сети.
- Исключает участие в арбитраже и вмешательство в работу автомобиля.

3. Loopback Mode

- Используется для тестирования.

- Переданные данные проходят внутреннюю петлю и принимаются обратно.
- CAN-шина физически не используется.

4. Sleep Mode

- Сниженное энергопотребление.
- Используется в автономных системах с редким опросом данных.

В реальном автомобиле любое неконтролируемое вмешательство в CAN может привести к:

- ошибкам в блоках управления
- нарушению работы некоторых подсистем
- конфликтам сообщений
- диагностическим ошибкам

Поэтому все исследования должны проводиться в режиме, исключающем отправку кадров, то есть в Listen-Only.

3. БЕЗОПАСНОСТЬ РАБОТЫ С CAN-ШИНОЙ И МЕТОДЫ ЗАЩИТЫ

3.1. Уязвимости CAN-шины

CAN не предусматривает встроенной криптографической защиты или аутентификации. Это приводит к ряду уязвимостей, связанных как с безопасностью, так и с надёжностью.

Основные уязвимости:

1. Отсутствие аутентификации сообщений

Каждый узел, способный передать кадр, может выдать себя за любой другой — достаточно знать идентификатор. Это позволяет:

- подделывать сообщения (spoofing)
- имитировать данные датчиков
- отправлять управляющие команды

2. Уязвимость к перегрузке (DoS / bus flooding)

CAN использует общий канал. Если узел начнёт передавать кадры с высоким приоритетом (малым ID) очень часто, другие узлы окажутся вытеснены арбитражом.

В результате:

- задержки в управлении
- ошибки шинных модулей
- отказ критичных систем

3. Возможность «немого захвата» сообщений

Закладка или некорректная конфигурация узла может перехватывать или занижать приоритет сообщений, затрудняя работу других ECU.

4. Диагностические команды (UDS) в уязвимых ECU

Некоторые ECU допускают выполнение сервисных команд программирования или калибровки через CAN, если не предусмотрена защита (seed-key, защита по скорости бота и т.д.).

5. Физический доступ — низкий порог атаки

Любой, кто подключился в OBD-II, может:

- слушать CAN
- отправлять кадры
- активировать диагностические режимы

Это не значит, что автомобиль легко «взломать», но делает CAN одним из слабозащищённых каналов.

3.2. Обеспечение безопасности при исследовании CAN-шины

В исследовательских работах и экспериментальной диагностике важно обеспечить максимальную безопасность автомобиля. Неправильная конфигурация оборудования может привести к ошибкам ECU или, в худшем случае, нарушению работы отдельных подсистем.

Ниже перечислены основные методы безопасной работы.

1. Использование режима Listen-Only

В режиме Listen-Only MCP2515:

- не участвует в арбитраже
- не подтверждает кадры (ACK suppressed)
- не передаёт никаких данных

Таким образом:

- невозможно случайно отправить кадр
- минимальное влияние на шину
- автомобиль работает полностью автономно
- безопасно даже при движении автомобиля

2. Аппаратное ограничение передачи

Если оборудование позволяет, отключают линию TX:

- разрывают TX выход MCP2515
- оставляют только приём (RX)

Это создаёт жёсткое подтверждение, что устройство физически не может вмешиваться в сеть.

3. Использование фильтров и масок

Использование только тех ID, которые нужны для исследований:

- уменьшает нагрузку на микроконтроллер

- предотвращает ошибки из-за переполнения буферов
- помогает анализировать только необходимые данные

Фильтрация никак не влияет на безопасность автомобиля, но повышает безопасность анализа.

4. Изоляция от силовых подсетей

Если возможно, рекомендуется работать через диагностическую шину (OBD-II), а не напрямую с линией High-Speed CAN, используемой в силовых системах.

Причины:

- диагностическая шина ограничена по набору команд
- многие ECU игнорируют небезопасные действия, если они идут с диагностического адреса
- OBD-II предусматривает стандартные безопасные PIDs

3.3. Ограничения и предотвращение вреда автомобилю

Существует распространённое заблуждение, что через OBD-II порт можно легко заглушить автомобиль.

На практике срабатывают следующие ограничения:

1. Ограничения OBD-II (ISO 15765-4)

Диагностические запросы:

- обрабатываются только теми ECU, которые предназначены для диагностики
- не влияют на управление двигателем
- не участвуют в реальном арбитраже CAN-сети

Пример: команда чтения оборотов двигателя (PID 0x0C) лишь запрашивает информацию, но не вмешивается в работу мотора.

2. ECU игнорируют некорректные сообщения

Большинство современных блоков управления:

- игнорируют кадры, не соответствующие ожидаемому формату
- проверяют CRC и длину данных

- используют внутренние алгоритмы защиты

Это делает случайное вмешательство крайне маловероятным.

3. Защита от критичных команд

Управляющие команды (например: управление топливной рампой, тормозной системой, калибровки датчиков) выполняются только:

- на заглушенном двигателе
- после перехода в сервисный режим
- после успешной аутентификации (seed-key)
- с ограничением по скорости шины

Поэтому заглушить двигатель в движении через диагностический порт невозможно, если нет уязвимости в конкретном ECU.

4. Практические рекомендации по безопасному подключению

При анализе CAN-шины на автомобиле рекомендуется:

- использовать Listen-Only
- подключаться к диагностическому порту
- не включать питание автомобиля во время переподключений
- избегать работы в силовых подсетях без необходимости
- использовать отдельный изолированный адаптер

Эти меры позволяют получить данные не вмешиваясь в работу автомобиля.

ЗАКЛЮЧЕНИЕ

В ходе выполнения данной научно-исследовательской работы была проведена комплексная оценка архитектуры, принципов работы и особенностей взаимодействия с автомобильной CAN-шиной, а также рассмотрены аппаратные и программные решения, позволяющие безопасно осуществлять её анализ. В работе раскрыты ключевые характеристики протокола CAN, его структура, механизмы арбитража, обработки ошибок и организация сетей внутри современного автомобиля. Это позволило сформировать целостное понимание того, как электронные блоки управления взаимодействуют друг с другом и каким образом происходит передача данных между различными подсистемами транспортного средства.

Особое внимание было уделено связке MCP2515 и TJA1050 как наиболее распространённому и доступному варианту подключения микроконтроллеров к CAN-шине. Анализ показал, что данная комбинация обеспечивает аппаратную реализацию протокола CAN и надёжную работу на физическом уровне, а микроконтроллер ESP32 предоставляет широкие возможности для обработки данных, их анализа и дальнейшей интеграции в телематические системы. Были рассмотрены режимы работы MCP2515, среди которых ключевое значение имеет режим Listen-Only, гарантирующий безопасное подключение к автомобильной сети без риска вмешательства в её функционирование.

Важным результатом исследования стало изучение вопросов безопасности CAN-шины. Показано, что отсутствие встроенных механизмов аутентификации и криптографической защиты делает сеть уязвимой к подделке сообщений, перегрузке и другим воздействиям. Однако при соблюдении методологии безопасного анализа — использовании режима «только чтение», применении фильтров, аппаратном ограничении передачи, а также подключении через диагностическую шину — риск негативного влияния на работу автомобиля практически исключается.

Результаты данной НИР обладают как теоретической, так и практической ценностью. Они создают основу для дальнейшего выполнения выпускной квалификационной работы, в рамках которой будет реализована система чтения данных CAN-шины автомобиля с использованием ESP32. Полученные знания помогут корректно и безопасно настроить оборудование, провести анализ данных и интерпретировать результаты без угрозы для автомобиля и его систем.

Таким образом, поставленная цель исследования достигнута: определены принципы работы CAN-шины, изучены технические средства для её анализа и разработан подход к безопасному считыванию данных. Итоги работы создают фундамент для дальнейших практических экспериментов и разработки полнофункционального решения в сфере автомобильной телематики.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Аверченков, В.И. Основы научного творчества [Электронный ресурс]: учеб. пособие/ В.И. Аверченков, Ю.А. Малахов. — Брянск: Брянский государственный технический университет, 2012. — 156 с.— Режим доступа: <http://www.iprbookshop.ru/7004>.
2. Астанина, С.Ю. Научно-исследовательская работа студентов (современные требования, проблемы и их решения) [Электронный ресурс]: монография/ С.Ю. Астанина, Н.В. Шестак, Е.В. Чмыхова. — М.: Современная гуманитарная академия, 2012.— 156 с.— Режим доступа: <http://www.iprbookshop.ru/16934>.
3. Губарев, В.В. Квалификационные исследовательские работы [Электронный ресурс]: учеб. пособие/ В.В. Губарев, О.В. Казанская. — Новосибирск: Новосибирский государственный технический университет, 2014. — 80 с.— Режим доступа: <http://www.iprbookshop.ru/47691>.
4. Жданов А.В., Лукьянов М.В., Михайлов П.Е. Анализ параметров обмена данными в автомобильной сети CAN // Автомобильная промышленность. – 2020. – № 5. – С. 34–38.
5. Куевда Е.Е., Селиванов А.А. Особенности применения контроллеров MCP2515 в транспортных CAN-сетях // Электронные средства и системы управления. – 2019. – № 2. – С. 12–17.
6. Курочкин, А. В. Локальные сети автомобилей и их диагностика: учебное пособие. – М.: Академия, 2018. – 256 с.
7. Новиков, Ю.Н. Подготовка и защита бакалаврской работы, магистерской диссертации, дипломного проекта [Электронный ресурс] : учебное пособие / Ю.Н. Новиков. — 4-е изд., стер. — Санкт-Петербург : Лань, 2019. — 34 с. — URL: <https://e.lanbook.com/book/122187>.
8. Половинкин, А.И. Основы инженерного творчества. [Электронный ресурс]: учебное пособие / А.И. Половинкин.— СПб : Лань, 2019. — 364 с.— Режим доступа: <https://e.lanbook.com/book/123469>.

9. Рекомендации по написанию и оформлению курсовой работы, выпускной квалификационной работы и магистерской диссертации [Электронный ресурс]: учебно-методическое пособие/ Е.В. Зудина [и др.]. — Волгоград: Волгоградский государственный социально-педагогический университет, 2016. — 57 с.— Режим доступа: <http://www.iprbookshop.ru/57785>.

10. Рыжков, И.Б. Основы научных исследований и изобретательства. [Электронный ресурс]: учеб. пособие / И.Б. Рыжков. — СПб.: Лань, 2013. — 224 с.— Режим доступа: <http://e.lanbook.com/book/30202>.

11. Тарасов М.Ю., Глухов И.С., Алексеев Д.Г. и др. Исследование уязвимостей автомобильных сетей передачи данных CAN // Инженерный вестник. – 2021. – № 8. – С. 21–27.