## Устройство

Автономный грузовик состоит из множества физических модулей, которые обеспечивают его работу, автономное движение и безопасность. Ниже приведен список основных физических модулей автономного грузовика:

1. **Сенсорные системы**
   * **Лидары**: используют лазерные лучи для создания трехмерной карты окружающей среды.
   * **Радары**: используют радиоволны для определения расстояний до объектов и их скорости.
   * **Камеры**: обеспечивают визуальную информацию о дороге, дорожных знаках, светофорах и других объектах.
   * **Ультразвуковые датчики**: используются для обнаружения объектов на небольших расстояниях, особенно при парковке.
   * **Система датчиков состояния**: устройства определяющие состояния транспорта (спидометр, датчик открытия дверей, гироскоп, термометр и т.д.)
2. **Коммуникационные модули**
   * **Модули связи**: обеспечивают связь с другими транспортными средствами, инфраструктурой и облачными сервисами.
   * **GPS-модули**: обеспечивают точное определение местоположения грузовика.
3. **Вычислительные модули**
   * **Бортовой компьютер**: центральный процессор для обработки данных с сенсоров, принятия решений и управления системами грузовика.
   * **Графические процессоры (GPU)**: используются для обработки визуальной информации и выполнения сложных вычислений, связанных с машинным обучением.
4. **Системы управления**
   * **Электронная система управления двигателем**: контролирует работу двигателя, обеспечивая его оптимальную работу.
   * **Система управления тормозами**: включает в себя электронные модули для управления тормозной системой.
   * **Система управления рулевым управлением**: обеспечивает точное управление рулем для выполнения маневров.
   * **Система управления креплениями:** управляет задними воротами грузовика и креплениями груза внутри контейнера
5. **Энергетические модули**
   * **Батареи и системы управления батареями (BMS)**: обеспечивают питание электрических систем грузовика и управление зарядкой/разрядкой батарей.
   * **Системы управления энергопотреблением**: оптимизируют расход энергии для различных систем грузовика.
6. **Системы безопасности**
   * **Ядро безопасности:** обеспечивает киберимунный подход и защиту от недопустимых событий

Эти модули работают в тесной взаимосвязи, обеспечивая безопасное и эффективное движение автономного грузовика.

## Киберимунный подход

Киберимунный подход при проектировании автономного грузовика необходим для обеспечения его устойчивости к различным видам кибератак и угроз. В условиях увеличения сложности и взаимосвязанности электронных систем и программных компонентов, безопасность становится критически важным аспектом для нормального функционирования автономного транспортного средства. Вот несколько причин, почему киберимунный подход является важным:

**1. Защита от кибератак**

Автономные грузовики, оснащенные множеством сенсоров, камер и компьютеров, становятся мишенями для киберпреступников. Киберимунный подход позволяет выявлять и нейтрализовать попытки несанкционированного доступа, предотвращая потенциально катастрофические последствия, такие как захват управления транспортным средством.

**2. Обеспечение надежности систем**

Наличие устойчивой киберимунной системы обеспечивает непрерывную работу всех компонентов грузовика. Это особенно важно для автономного транспорта, где сбои в системах управления или сенсоров могут привести к серьезным авариям и повреждениям.

**3. Минимизация простоев и затрат на ремонт**

Киберимунный подход позволяет быстро обнаруживать и реагировать на инциденты, что минимизирует время простоя транспортного средства и затраты на ремонт. Системы самовосстановления и адаптации помогают транспортному средству быстро возвращаться в рабочее состояние после атак.

**4. Повышение доверия и принятия технологии**

Безопасность и надежность автономных грузовиков являются ключевыми факторами для их широкого принятия на рынке. Демонстрация способности защищать транспортное средство от киберугроз повышает доверие потребителей и регуляторов, способствуя более быстрому внедрению технологии.

**5. Соблюдение нормативных требований**

Многие страны и регуляторные органы начинают вводить строгие требования к безопасности автономных транспортных средств. Киберимунный подход помогает соответствовать этим требованиям, обеспечивая соответствие нормативам и стандартам безопасности.

**6. Адаптация к новым угрозам**

Киберугрозы постоянно эволюционируют, и методы атаки становятся все более изощренными. Киберимунные системы, использующие методы машинного обучения и искусственного интеллекта, могут адаптироваться к новым угрозам и обновлять свои защитные механизмы в реальном времени.

**7. Защита данных и конфиденциальности**

Автономные грузовики собирают и обрабатывают огромное количество данных, включая информацию о маршрутах, загрузках и окружающей среде. Киберимунные методы обеспечивают защиту этих данных от несанкционированного доступа и утечки, что является важным аспектом для защиты коммерческих интересов и конфиденциальности.

Внедрение киберимунного подхода в проектирование автономных грузовиков является необходимым для обеспечения их безопасности, надежности и долгосрочной эксплуатационной готовности. Это помогает не только защитить транспортное средство от текущих угроз, но и готовить его к будущим вызовам, обеспечивая устойчивое развитие технологий автономного транспорта.

## Следствия недостаточной безопасности

Взломанный автономный грузовик может представлять серьезную опасность, так как злоумышленники могут получить контроль над различными системами транспортного средства. Вот перечень критических действий, которые может выполнить взломанный автономный грузовик:

**1. Потеря управления и манипуляция движением**

* **Ускорение или торможение**: Злоумышленник может заставить грузовик резко ускориться или затормозить, что может привести к авариям.
* **Изменение направления**: Перехват управления рулевым управлением может привести к внезапным изменениям направления движения, включая выезд на встречную полосу или съезд с дороги.

**2. Деактивация систем безопасности**

* **Отключение тормозов**: Отключение или манипуляция тормозной системой может привести к неспособности остановить грузовик.
* **Отключение систем предотвращения столкновений**: Выключение этих систем увеличивает риск аварий.

**3. Сбои в работе сенсоров и систем навигации**

* **Искажение данных сенсоров**: Злоумышленник может изменять или подменять данные, поступающие с лидаров, камер, радаров, что приведет к неправильной оценке окружающей обстановки и возможным авариям.
* **Манипуляция GPS-сигналами**: Нарушение работы навигационной системы может привести к отклонению от маршрута или запутыванию грузовика в незнакомой местности.

**4. Использование грузовика в качестве оружия**

* **Направление на толпу или здания**: Злоумышленник может использовать грузовик для намеренного наезда на пешеходов или врезания в здания и другие объекты.
* **Создание дорожных происшествий**: Грузовик может быть направлен на столкновение с другими транспортными средствами для создания массовых аварий.

**5. Саботаж и вандализм**

* **Повреждение инфраструктуры**: Злоумышленник может направить грузовик на критически важные объекты инфраструктуры, такие как мосты, туннели, заправочные станции.
* **Блокировка дорог**: Остановка грузовика на стратегически важных участках дороги может привести к значительным заторам и нарушению транспортного потока.

**6. Нарушение логистических операций**

* **Кража груза**: Злоумышленник может использовать взлом грузовика для кражи или повреждения перевозимого груза.
* **Изменение маршрута**: Перенаправление грузовика в другое место может привести к задержкам в доставке и финансовым потерям.

**7. Нарушение работы энергетических систем**

* **Разрядка батареи**: Принудительная разрядка батареи может оставить грузовик без энергии, что приведет к его остановке в неподходящем месте.
* **Перегрев или повреждение батареи**: Нарушение работы систем управления батареей может вызвать перегрев или даже возгорание.

**8. Нарушение систем связи**

* **Отключение связи с центром управления**: Злоумышленник может разорвать связь грузовика с диспетчерским центром, что затруднит или сделает невозможным вмешательство операторов для восстановления контроля.
* **Манипуляция данными V2X**: Искажение или подделка данных, передаваемых между транспортными средствами и инфраструктурой, может создать ложное ощущение безопасности или вызвать аварии.

Эти критические действия показывают, насколько важно обеспечить надежную защиту автономных грузовиков от кибератак. Киберимунные системы и комплексные меры безопасности являются необходимыми для предотвращения таких сценариев и обеспечения безопасной эксплуатации автономных транспортных средств.

## Цели безопасности

* Выполняются только аутентичные задания управляющего центра
* Все операции выполняются согласно заданию управляющего центра (маршрут, зоны погрузки/выгрузки, зоны трассы)
* В случае критического отказа ТС не причинит критического ущерба людям и зданиям

## Предположения безопасности

* Управляющий центр надежный и сотрудники работающие там обладают достаточной квалификацией
* ТС движется по специально подготовленной дороге (исключаются неровности поверхности и другие внедорожные препятствия на всём протяжении маршрута)
* Маршрут составлен корректно (корректно разделен на зоны и корректно составлена траектория)

## Зоны маршрута

Маршрут может быть разделен на зоны:

* **Начало/конец маршрута:** из этих зон ТС начинает и заканчивает движение
* **Зона погрузки/выгрузки:** в данных зонах возможно открытие кузова и креплений груза, в других участках маршрута данное действие запрещено
* **Городская зона:** на данных участках маршрут проходит вблизи зданий и людей
* **Свободная зона:** на данном участке в непосредственной близости от маршрута не находится критичных объектов

## Архитектура

