«Безопасный стиль вождения» безопасность компьютерной инфраструктуры автомобиля

Печёнкин Александр
руководитель проектов

Популярность автотранспорта

НЕОБИТ — Новые безопасные информационные технологии

- В России ~30 млн. автомобилей
- В мире > 1 млрд. автомобилей
- К 2020 ожидается ~1,7 млрд.
- ~30 тыс. смертей в год
- ~300 тыс. раненых в год

«Истина где-то рядом»

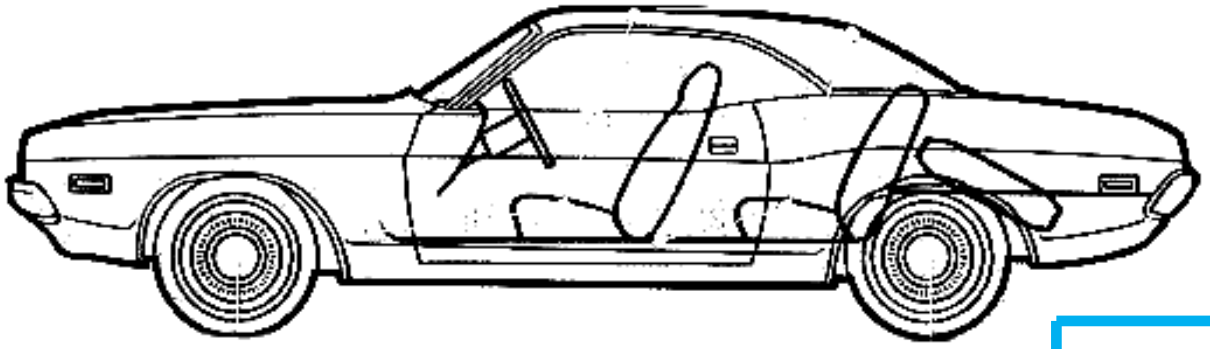
НЕОБИТ

Сериал «Секретные материалы»

«Хакер» угнал автомобиль с помощью особого CD-диска, вставленного в магнитолу

«Чего только не придумают киношники?»

Модули CAN-шины Dodge Challenger



Модуль управления радио

Управление рулевой колонкой

Дверь водителя

Пассажирские двери

Модуль управления двигателем

Антиблокировочная тормозная система

Hands Free Модуль

Вентиляция, кондиционер

...

CAN шина

Инциденты, связанные с автоэлектроникой

2009 г., Австралия, Ford Explorer	• Машина категорически не пожелала выходить из режима **cruise control** и упорно продолжала держать скорость 100 км/час, невзирая на все попытки водителя притормозить
2003 г., Таиланд, BMW	• **Министр финансов Таиланда** в правительственном BMW. В результате сбоя мотор заглох, двери оказались заперты, сервоприводы оконных стекол заблокированы, а воздушный кондиционер выключен
2005 г., США, Pontiac	• Проблема с **круиз-контролем**. В результате машина ехала со скоростью 130 км/час. Автомобиль сумели остановить только путем торможения об полицейскую машину
2009 г., США, Dodge Caravan	• Во время езды включил печку на полную мощность, не давая ее выключить

Использование автоугонщиками

Угон Porsche Cayenne в аэропорту Пулково Санкт-Петербурга

Центральный замок автомобиля был открыт при помощи подключения к CAN шине. Добрались до которой, проделав небольшое отверстие в задней правой двери.

Первые обвинения в целенаправленных воздействиях

Кто? Где? Когда?	• Скандальный журналист: Майкл Хастингс • США, Голливуд, 2013 г.
Что случилось?	• Машина на скорости ~160 км/ч проскочила 3 перекрестка на красный свет, а на абсолютно прямой дороге резко вылетела на разделительную полосу и ударилась в дерево с феноменально мощным взрывом
Из-за чего?	• Анализ видеозаписей показал, что было три взрыва. Два еще при движении автомобиля — в отсеке двигателя, а третий, с самым мощным воспламенением, охватил огнем кабину при столкновении с пальмой
Что говорят?	• *«В случае Майкла Хастингса те свидетельства, которые стали публично доступными, согласуются с признаками кибератаки»*

Стандартизация CAN

Стандартизующие организации	ISO 11898	ISO 11519-2
• Комитет ISO/TC22/SC3/WG1 • Американское Общество инженеров автомобилестроения (**S**ociety of **A**utomotive **E**ngineers) • Международная группа OSEK/VDX «Открытые системы и соответствующие интерфейсы для автомобильной электроники»	• Road vehicles Interchange of digital information digital information. Controller area network (CAN) for high-speed communication • Транспортные средства. Обмен цифровой информацией. Локальная сеть контроллеров CAN для быстрой связи	• Road vehicles. Low-speed serial data communication. Part 2. Low-speed controller area network (CAN) • Транспортные средства. Низкоскоростная последовательная связь данных. Часть 2. Низкоскоростная локальная сеть контроллеров CAN

Основные положения стандарта CAN

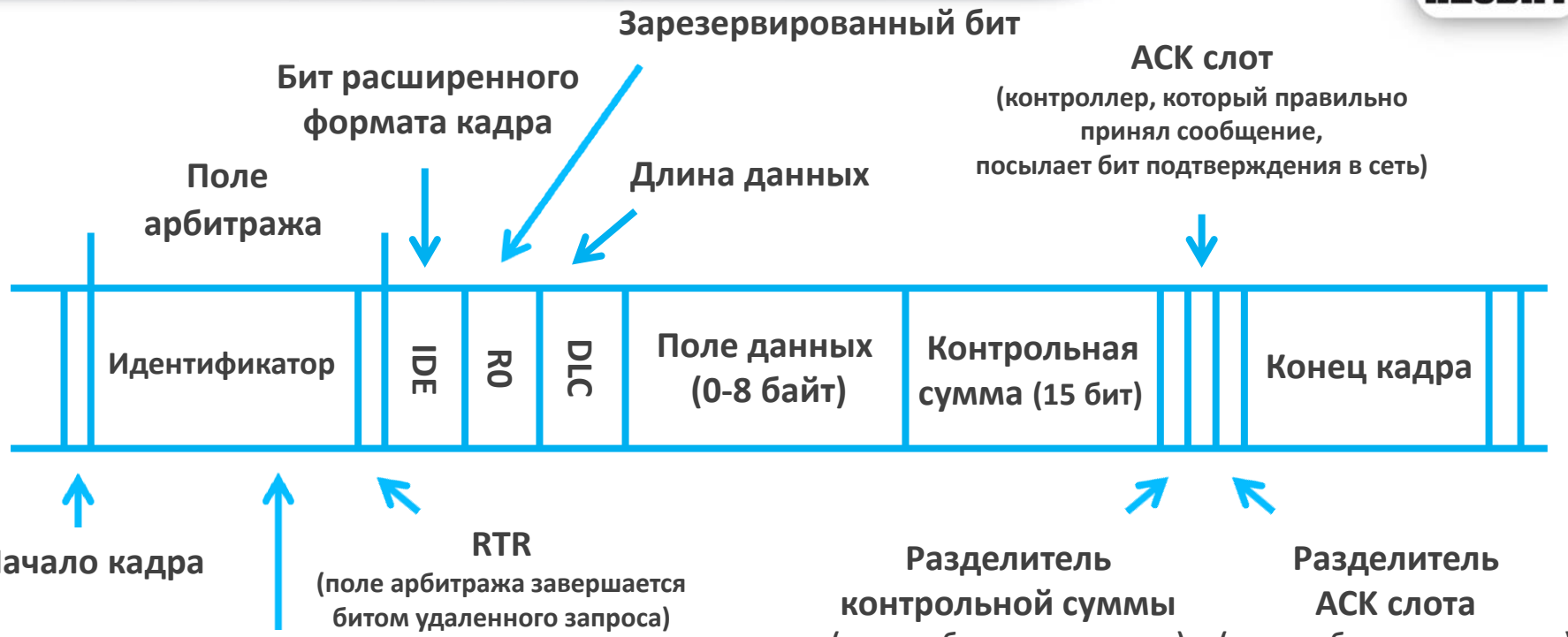
Режим передачи	• Последовательный, широковещательный, пакетный
Среда передачи	• Определяет передачу в отрыве от физического уровня • На практике под CAN-сетью понимают обычно подразумеваются сеть топологии «шина»
Недеструктивный арбитраж	• Гарантируется доступ к шине сообщений с максимальным приоритетом без задержек
Контроль ошибок	• Исчерпывающая схема контроля ошибок • Автоматическое устранение узла, являющегося источником ошибочных пакетов в сети
Применение	• Де-факто – стандарт для автомобильной автоматики

Области применения CAN

- **Различные виды транспорта**
- **Производственная промышленность**
- **Строительство**
- **Сельское хозяйство**
- **Медицинское оборудование**

CAN является идеальным решением
для любого оборудования,
где микроконтроллеры обмениваются
сообщениями друг с другом
и с удаленными периферийными
устройствами

Базовый формат кадра CAN



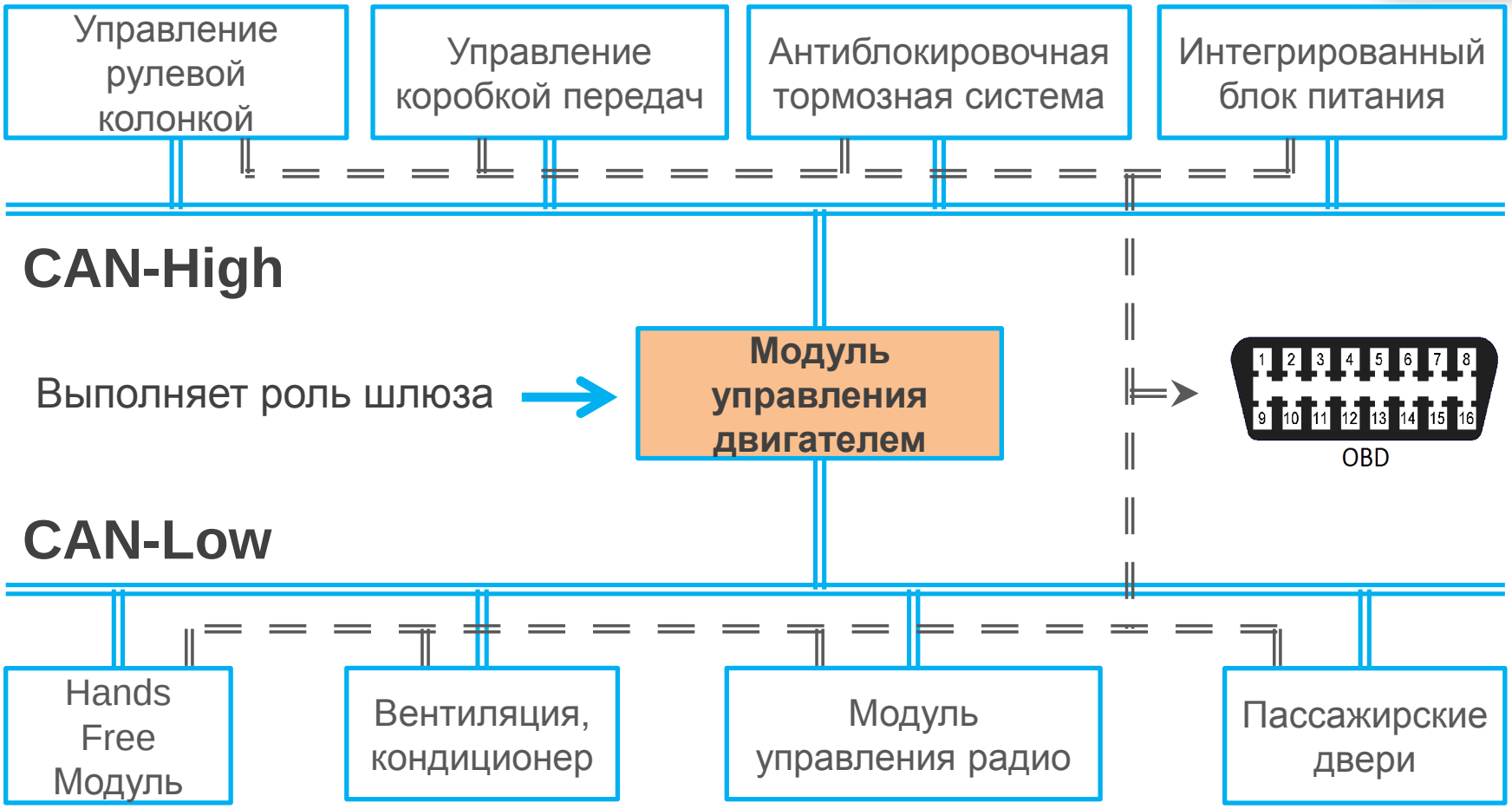
Уникальный Идентификатор
(идентификатор говорит о содержимом пакета и служит для определения приоритета при попытке одновременной передачи несколькими сетевыми узлами)

Логический ноль – доминантный бит
Логическая единица – рецессивный бит
При одновременной передаче в шину нуля и единицы, на шине будет зарегистрирован только логический ноль, а логическая единица будет подавлена.

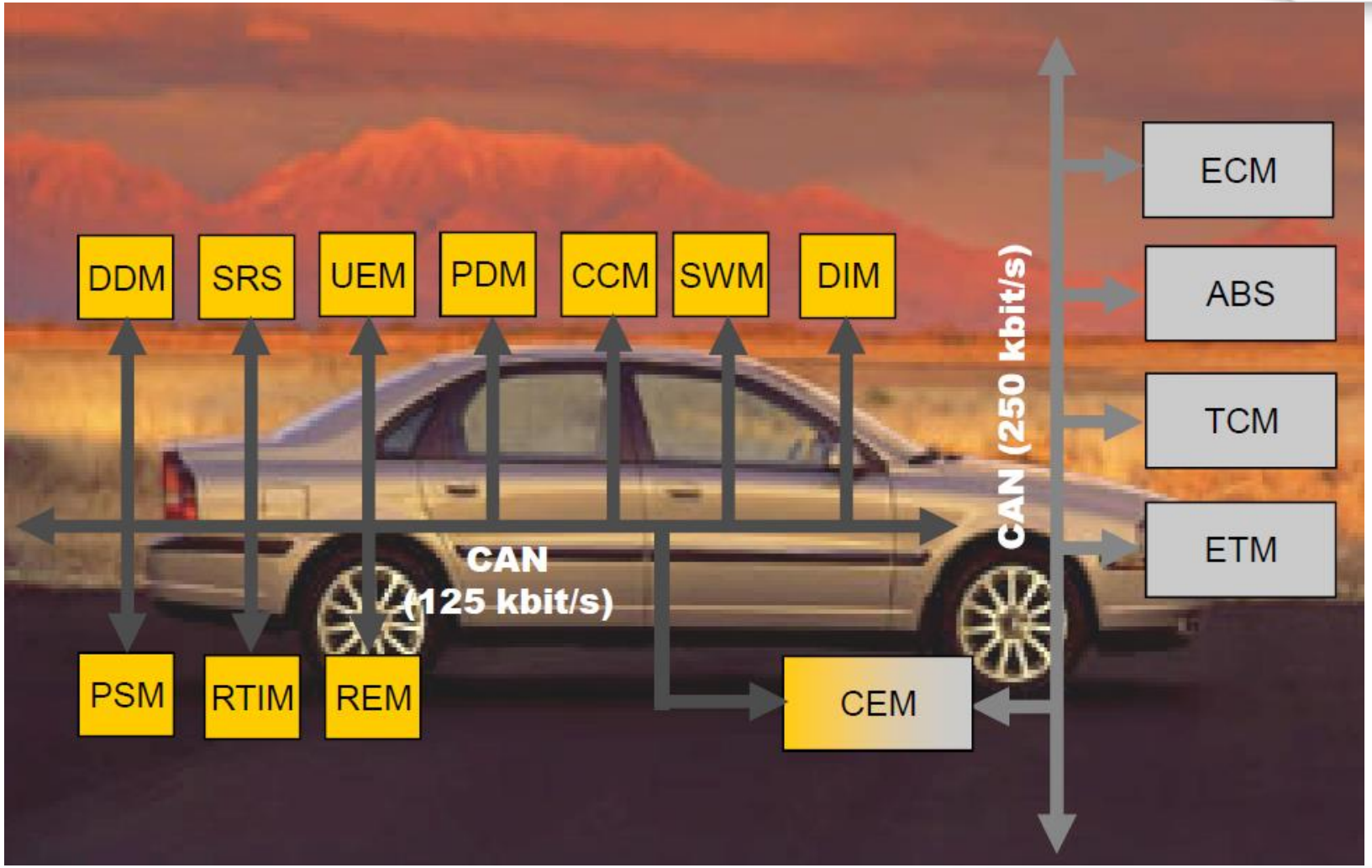
Скомпрометированный модуль CAN

Скомпрометировав один из модулей CAN, злоумышленник может отправлять в сеть произвольные сообщения. Искусственно созданные сообщения, могут быть получены другими модулями CAN сети, и восприняты ими как легитимные.

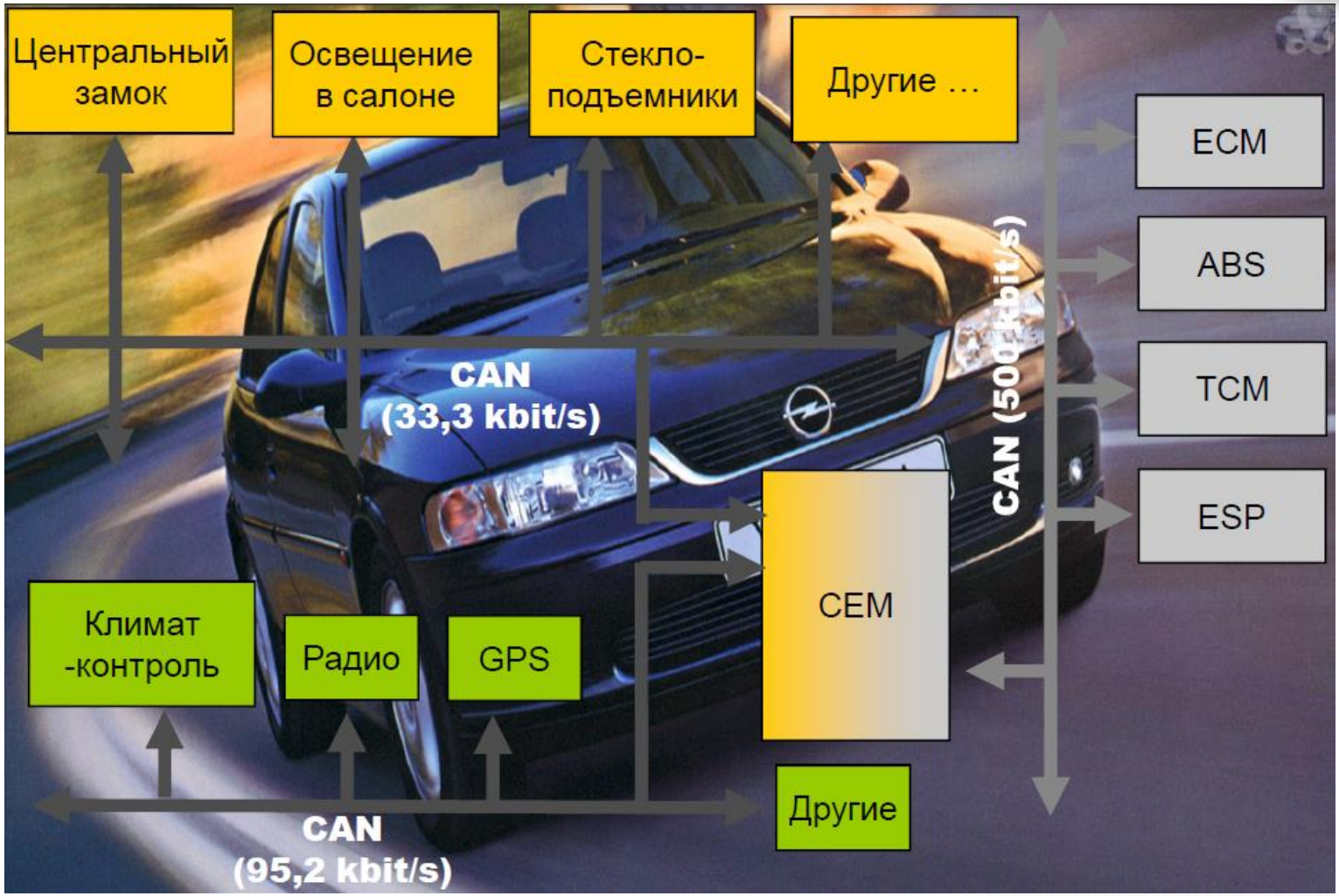
Уровни CAN шины



Volvo S80 (2000)



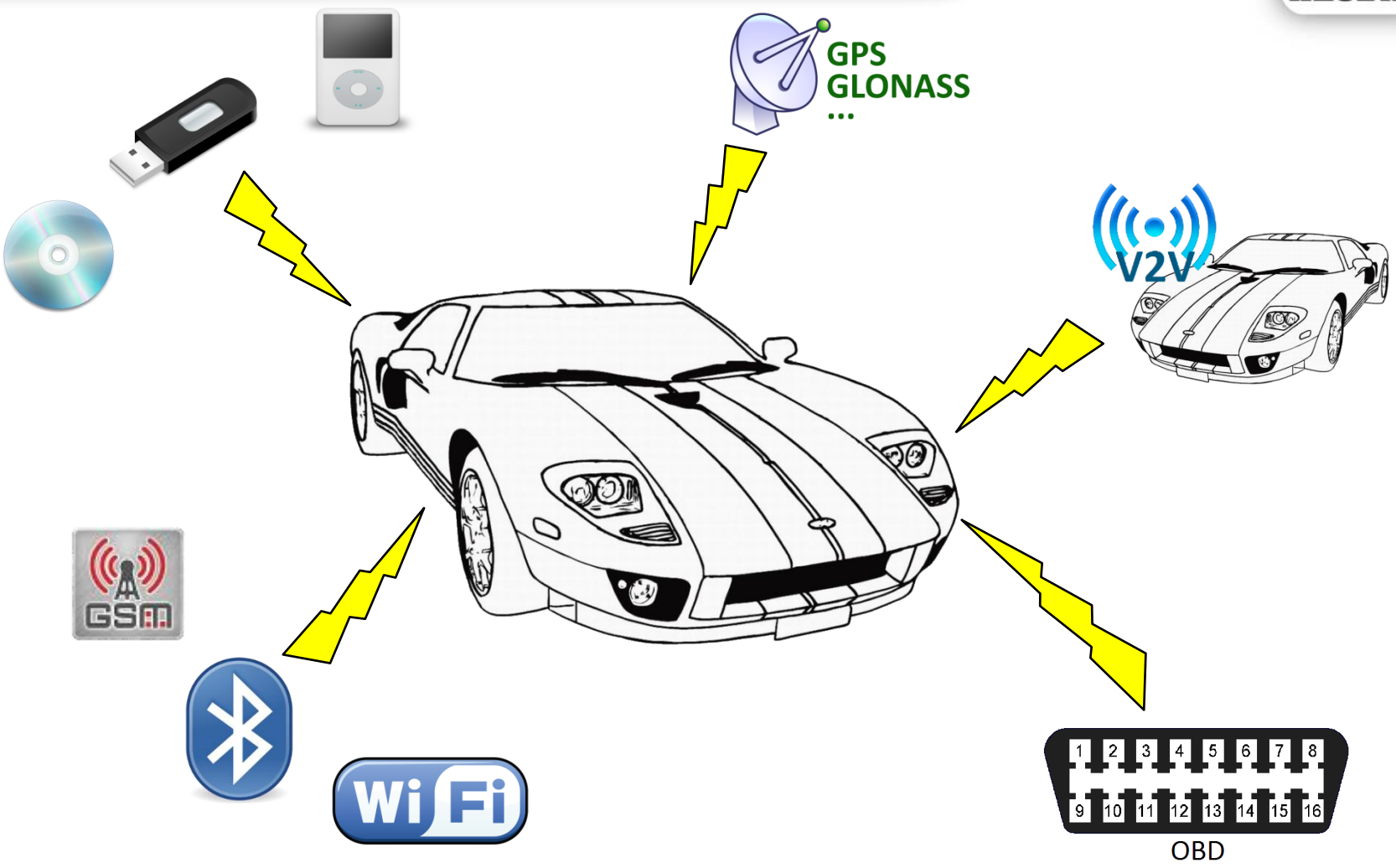
Opel Vectra (2005)



Модули CAN-шины Dodge Challenger

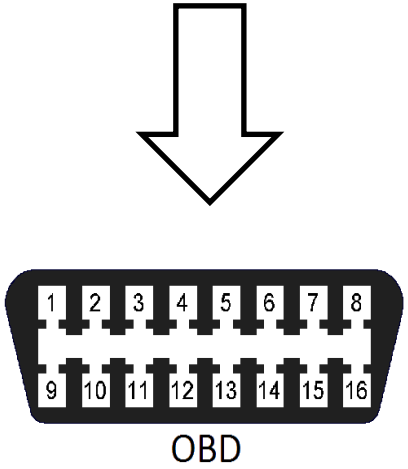
ORC Контроллер вторжения	**PCM** Модуль управления двигателем	**RCM** Модуль управления радио	**PDM** Пассажирские двери	**HFM** Hands Free модуль
TCM Управление коробкой передач	**TPM** Датчик давления шин	**EOM** Верхний электронный блок	**ESM** ЭБУ селектора	**HSM** Подогрев сиденья
ABS Антиблокировочная тормозная система	**SCM** Управление рулевой колонкой	**WIN** Беспроводной узел зажигания	**DDM** Дверь водителя	**PEM** Модуль беспроводного доступа
AMP ЭБУ усилителя	**TIPM** Интегрированный блок питания	**CCN** ЭБУ салонного оборудования	**SUNR** Управление люком	**HVAC** Вентиляция, кондиционер

Каналы входы в CAN-сеть



Диагностический порт

Злоумышленник подключается к диагностическому порту при помощи специального устройства



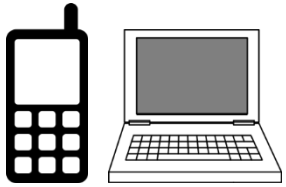
- Отправлять данные в CAN шину, возможно при помощи различных устройств, подключенных к диагностическому порту.

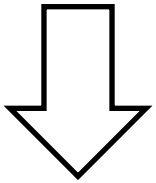
- При заражении интерфейсных компьютерных устройств, используемых на станциях автосервиса, оказываются скомпрометированными все подключавшиеся к ним машины.

Программная оболочка скомпрометирована и может быть использована для отправки команд в CAN сеть

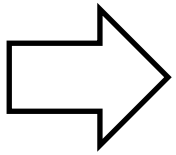
Беспроводные технологии

Злоумышленник при помощи беспроводных устройств формирует вредоносный пакет данных





Модуль CAN шины, предоставляющий беспроводной интерфейс

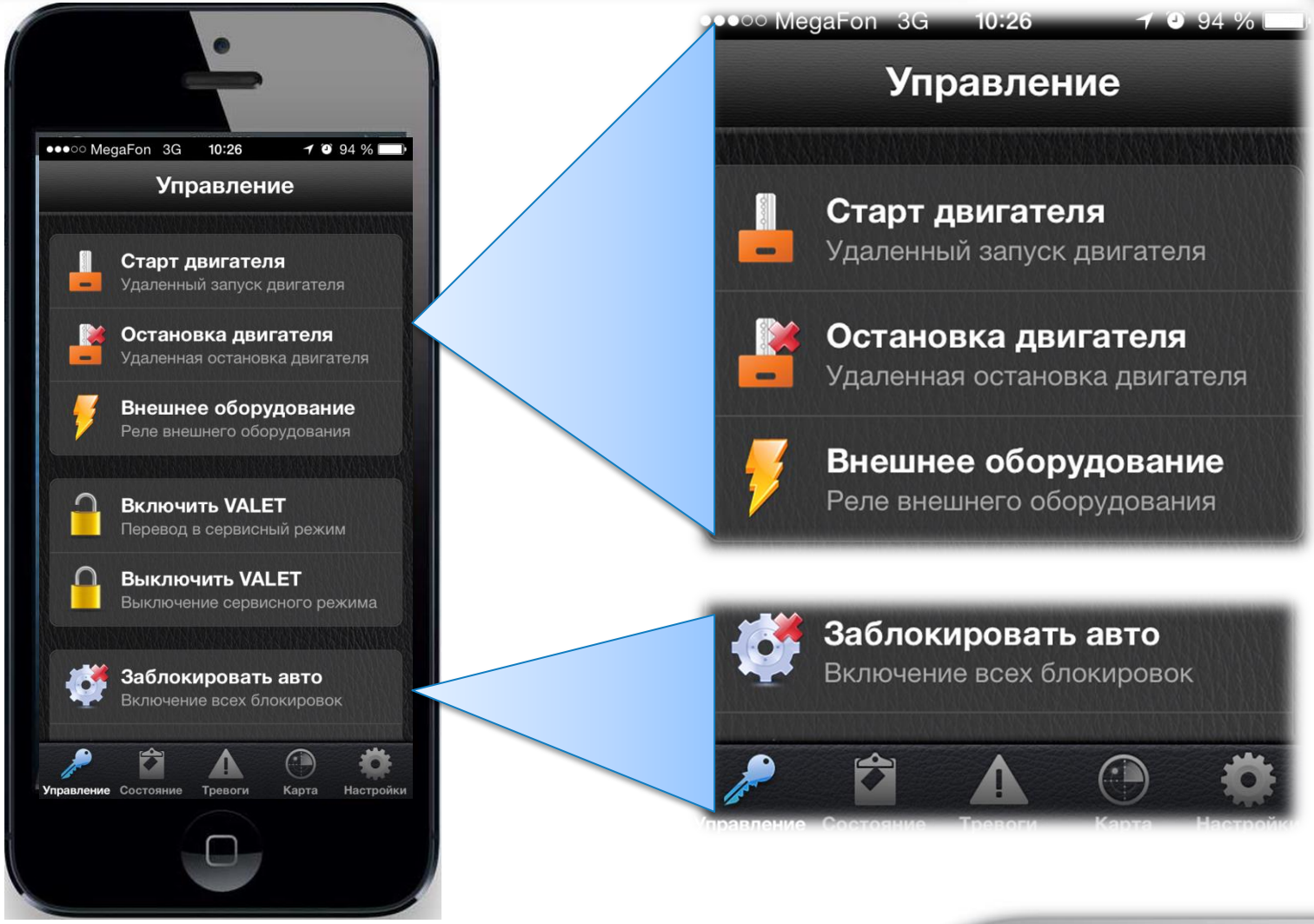


- Подавляющее число уязвимостей, по данным исследований CAESS (Center for Automotive Embedded Systems Security), возникают на границе взаимодействия интерфейсов модулей CAN шины.

Некорректная обработка данных приводит к выполнению внешнего кода

Программная оболочка беспроводного модуля скомпрометирована и может быть использована для отправки команд в CAN сеть

Управление сигнализациями



Автомобиль = большой смартфон

США

«Министерство транспорта США официально одобрило использование технологии «connected car», которая предполагает подключение автомобилей к беспроводному интернету для возможности управления и отслеживания автомобиля дистанционно

США

«Мы рассматриваем автомобиль как очередной цифровой девайс, как большой смартфон, – говорит президент отдела продвинутых устройств AT&T Гленн Лаури – наша цель – перевести автомобиль на другой уровень»

США

Как ожидается, министерство займется подготовкой новых норм, которые сделают технологию «vehicle-to-vehicle» обязательной

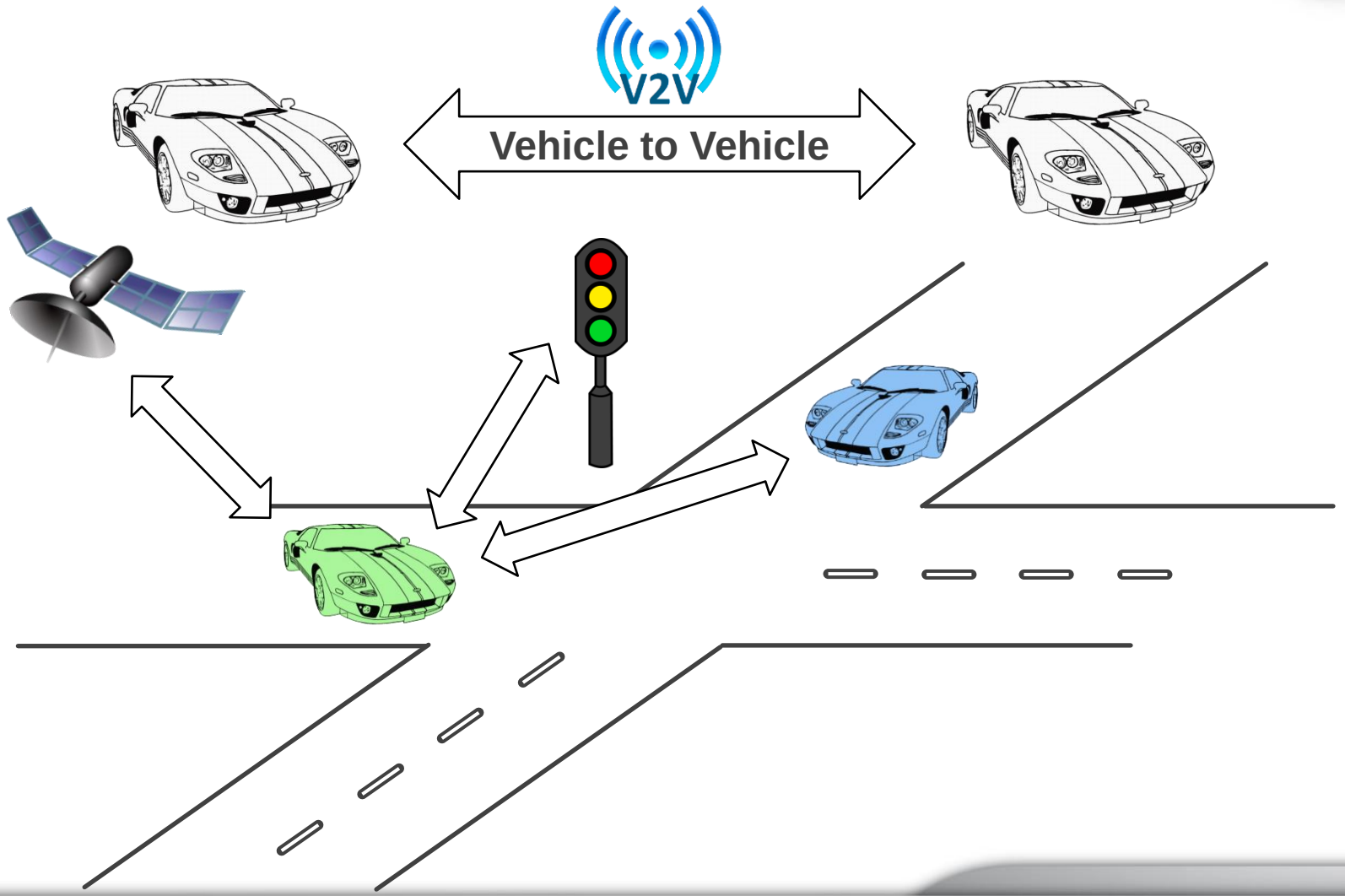
Европа

Европарламент вводит обязательную установку системы eCall на всех автомобилях с октября 2015 года

Россия

20 декабря Госдума приняла закон о работе системы экстренного реагирования при ДТП "ЭРА-ГЛОНАСС". Принятый закон вступает в силу 1 января 2014 года. А с 2015 года эта система станет обязательной к установке на автомобилях России, Белоруссии и Казахстана.

АвтоМобильная сеть - V2V



CD, USB, и другие устройства

Злоумышленник загружает вредоносный файл

RCM
Модуль управления радио

- По данным исследований CAESS (Center for Automotive Embedded Systems Security), некоторые модули CAN шины подвержены риску выполнения вредоносного кода, посредством специально сформированного медиа-файла.

Некорректная обработка файла приводит к выполнению внешнего кода

Программная оболочка модуля управления радио скомпрометирована и может быть использована для отправки команд в CAN сеть

Первые исследования

Официальный научно-технический орган США «Комитет Национальной академии наук по электронным системам управления автомобилей и их непреднамеренному ускорению»

Первые результаты

НОВЫЕ БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
НЕОБИТ

- Возможно без ведома автовладельца выключать двигатель, запирать двери, отключать тормоза, подменять показания спидометра и т.д.

Тотальный контроль

- Вредоносные программы могут затем бесследно и полностью самоуничтожаться, создавая видимость случайного отказа оборудования

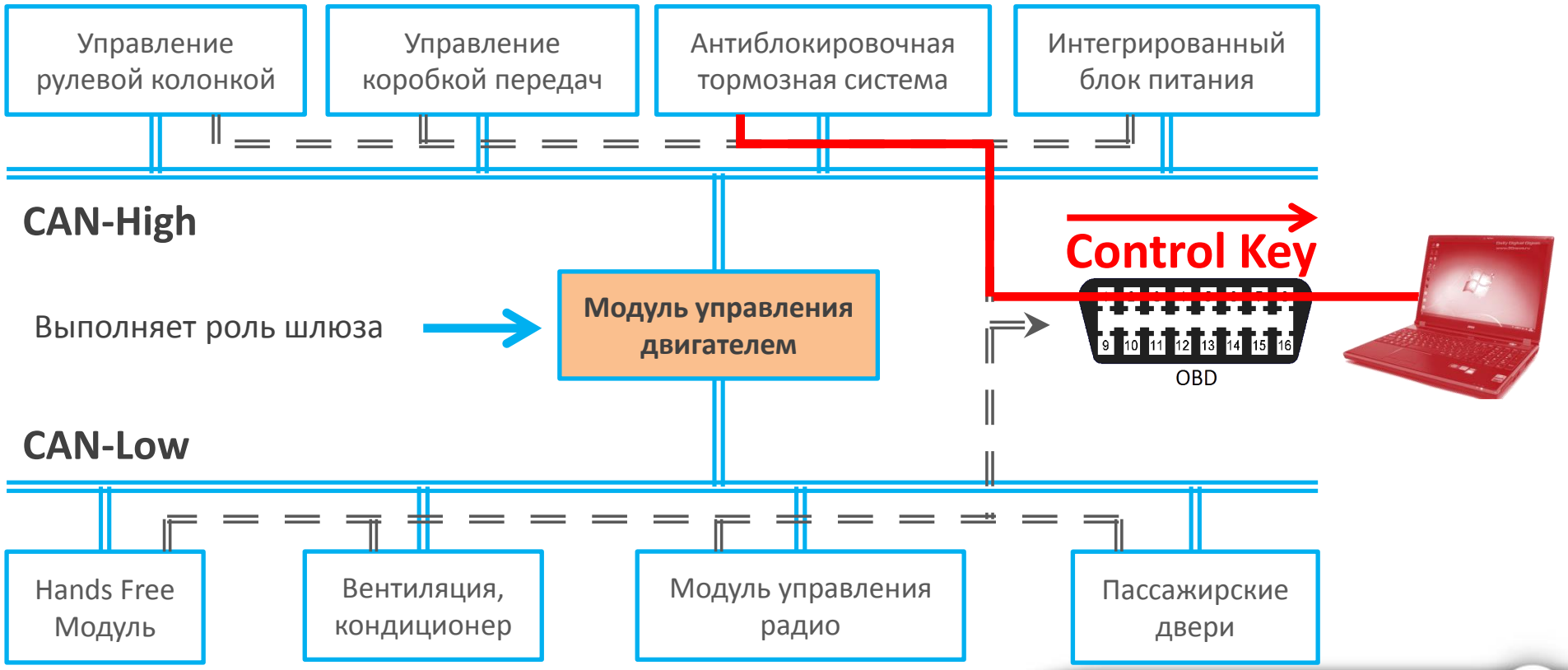
Безуликовость

- Превратили песню на CD и iPod в троянского коня. Когда она воспроизводится магнитолой ее прошивка перепрограмми-руется, что дает точку входа в систему CAN

Внедрение

Безопасность и CAN-шина

Для некоторых критически важных команд чаще всего необходима разблокировка с помощью Device Control Key.
Без данного ключа контроллер может проигнорировать команду.



Разблокировка критически важных команд

Модуль	Действие	Возможен ручной сброс	На скорости	Необходима разблокировка
PCM	Открытие багажника	Нет	Да	Нет
PCM	Разблокировка всех дверей	Да	Да	Нет
PCM	Увеличение оборотов	Нет	Да	Да
PCM	Отключение цилиндров	Да	Да	Да
PCM	Отключение усилителя руля	Да	Да	Да
PCM	Отключение тормозов	Да	Да	Да
RCM	Изменения на дисплее радио	Нет	Да	Нет
PCM	Блокировка машины	Да	Да	Да
PCM	Разблокировка машины	Да	Да	Да
PCM	Удаленный запуск	Нет	Нет	Да

Брутфорс Device Control Key

JAMES	Flash	TAMER	DRIFT	PANDA
MAZDA	COLIN	Bosch	HAZEL	Janis
MazdA	MHeqy	a_bad	12345	Rowan
mAZDa	BradW	conti	ARIAN	Jesus

Работа Charlie Miller & Chris Valasek, результаты представлены на DEF Con

Средства анализа CAN через OBD-II

EcomCat

- Реализовано на C
- Чтение данных из CAN шины
- Запись данных в CAN шину

EcomCat API

- Получение CAN пакетов
- Отправка CAN пакетов
- Отправка диагностических пакетов

PyEcom

- Обертка для Python

Ford Focus 2

Volkswagen Passat B6


BCM


Блок управления двигателем

Блок управления электроусилителем


Датчики ABS

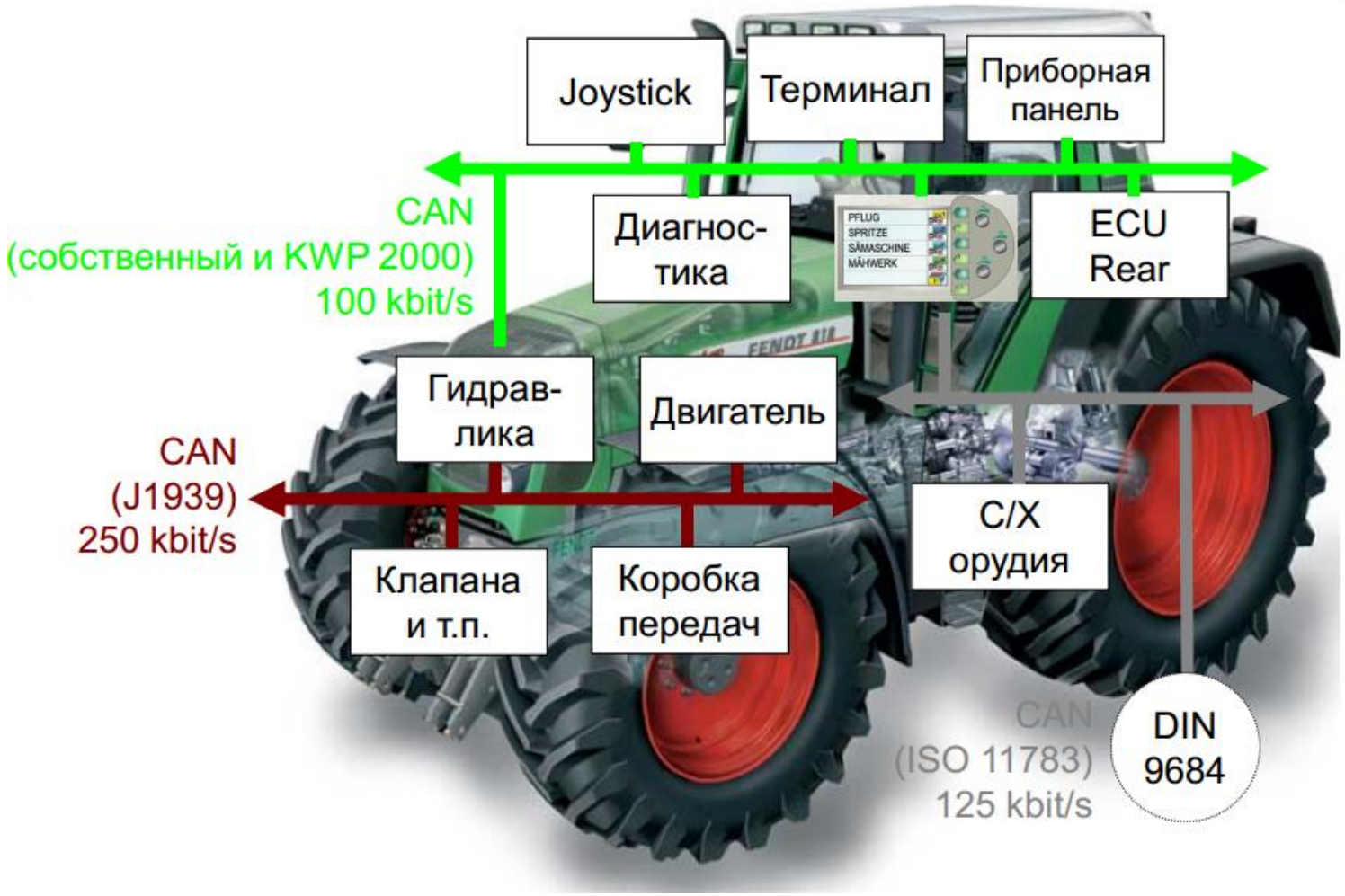
CAN


Иммобилайзер

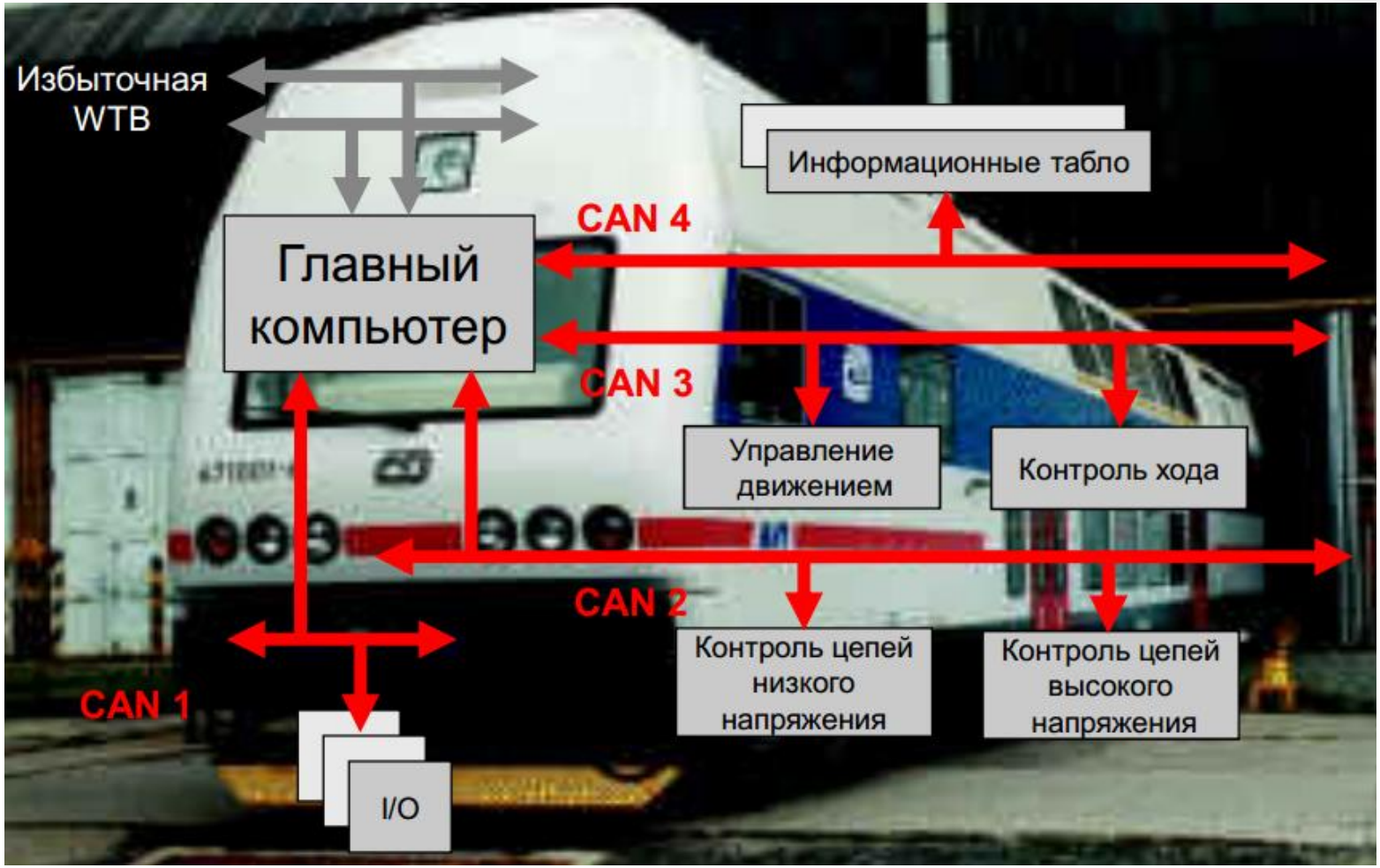

Ключ


Педали

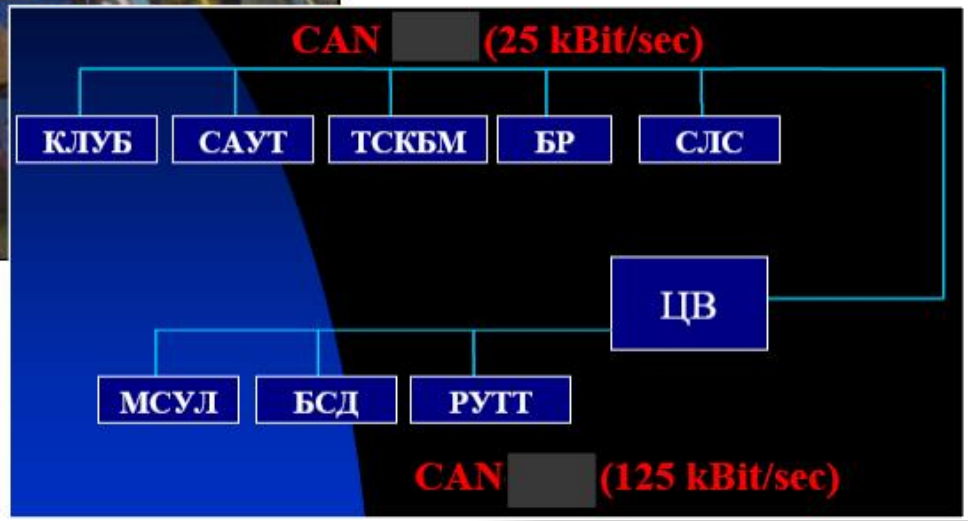
Сельскохозяйственная техника



Пригородный поезд ЕМ471



Унифицированная кабина машиниста




НОВЫЕ БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
НЕОБИТ