ЛЕКЦИЯ 14
КИБЕРБЕЗОПАСНОСТЬ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ УПРАВЛЕНИЯ. УГРОЗЫ, УЯЗВИМОСТИ И МЕТОДЫ ЗАЩИТЫ ЭЛЕКТРОННЫХ БЛОКОВ И КАНАЛОВ ПЕРЕДАЧИ ДАННЫХ

Цель

Сформировать у обучающихся системное представление о кибербезопасности как о неотъемлемой составляющей современных интеллектуальных систем управления автомобилями. Рассмотреть классификацию угроз и уязвимостей, поверхность атаки современных автомобилей, методы защиты электронных блоков управления и каналов передачи данных, а также нормативно-правовую базу, регламентирующую требования к кибербезопасности в автомобильной отрасли.

Планируемые результаты

После изучения данной лекции обучающийся сможет:

- объяснять отличие автомобильной кибербезопасности от функциональной безопасности и информационной безопасности общего назначения;
- классифицировать активы, угрозы, уязвимости и поверхности атаки современных автомобилей;
- описывать требования стандартов ISO/SAE 21434 и нормативных актов UNECE к кибербезопасности;
- характеризовать основные методы защиты электронных блоков управления (безопасная загрузка, HSM, криптография);
- объяснять принципы работы систем обнаружения вторжений (IDS) в бортовых сетях;
- анализировать методы машинного обучения для обнаружения аномалий и кибератак.

Вопрос занятия. Современный автомобиль — это не просто транспортное средство, а сложная киберфизическая система, подключённая к интернету, облачным сервисам и другим автомобилям. Но чем больше связей, тем больше возможностей для атак. Может ли хакер удалённо захватить управление автомобилем? Как отличить кибератаку от случайной неисправности? И главное — можно ли спроектировать систему, которая будет защищена не только от известных угроз, но и от тех, которые появятся завтра?

1. Введение в кибербезопасность автомобиля

1.1. Почему кибербезопасность стала критической?

Современный автомобиль представляет собой распределённую киберфизическую систему, в которой механические агрегаты, электрические цепи, электронные блоки управления, программное обеспечение, бортовые сети и внешние каналы связи действуют в тесном единстве. Цифровая команда

способна изменить физическое состояние машины: разблокировать двери, включить силовую установку, изменить тяговый момент, активировать тормоза или вывести на экран указание водителю. Поэтому защита информации в автомобиле непосредственно связана с безопасностью движения.

По данным исследований, в 2025 году было зафиксировано 765 критических и высокоопасных автомобильных уязвимостей, что продолжает устойчивый рост с 2017 года. Цифровые поверхности атаки в автомобильном секторе стремительно расширяются. Среди недооценённых векторов атак эксперты выделяют уязвимости инфраструктуры OTA-обновлений, слабое управление ключами и компрометацию цепочек поставок.

Кибербезопасность автомобиля — это совокупность инженерных и организационных мер, обеспечивающих защиту электронных систем, программного обеспечения, данных и каналов связи от преднамеренного несанкционированного воздействия в течение всего жизненного цикла транспортного средства. Под жизненным циклом понимают этапы концепции, проектирования, производства, эксплуатации, обслуживания, обновления и вывода из эксплуатации.

Цель кибербезопасности состоит не в том, чтобы сделать атаку абсолютно невозможной. Для сложной подключённой системы такое обещание нереалистично. Цель заключается в **управлении риском**: необходимо затруднить проникновение, своевременно обнаружить подозрительное поведение, ограничить последствия, сохранить критичные функции и обеспечить восстановление.

1.2. Отличие от функциональной безопасности

Функциональная безопасность (ISO 26262) и кибербезопасность (ISO/SAE 21434) — это две взаимодополняющие, но различные области.

Область	Источник опасности	Пример	Главный вопрос
Функциональная безопасность	Случайная неисправность или систематическая ошибка	Отказ датчика скорости	Как предотвратить опасное поведение при отказе
Кибербезопасность	Преднамеренное воздействие нарушителя	Подмена сообщения скорости	Как предотвратить, обнаружить и ограничить атаку
Эксплуатационная безопасность	Условия использования и действия человека	Загрязнение камеры	Как безопасно применять функцию

Границы между областями пересекаются. Одинаковое внешнее проявление может иметь разные причины. Неверное значение датчика возникает из-за физического повреждения, программной ошибки или злонамеренной подмены. Поэтому диагностический алгоритм сначала фиксирует наблюдаемое

отклонение, а затем анализирует возможные причины. Защитное решение должно оставаться безопасным даже до окончательного определения источника.

2. Основные свойства защищаемой информации

В контексте автомобильной кибербезопасности защите подлежат следующие свойства информации:

Конфиденциальность. Информация доступна только разрешённым субъектам. Для автомобиля это относится к персональным данным пользователя, истории поездок, координатам, идентификаторам ключей и учётным данным сервисов. Нарушение конфиденциальности может не изменять движение автомобиля, но создаёт риск слежения, мошенничества и неправомерного использования данных.

Целостность. Данные и команды не были несанкционированно изменены. Для управляющих систем целостность особенно важна. Подмена значения скорости, угла рулевого колеса, состояния двери или команды торможения способна привести к неправильному решению. Проверка целостности должна охватывать данные при передаче, хранении и выполнении программного кода.

Доступность. Функция и данные доступны в требуемый момент. Даже если сообщение не раскрыто и не изменено, его блокирование может быть опасным. Перегрузка сети, подавление радиосигнала или истощение вычислительных ресурсов способны задержать критичное сообщение. Для автомобиля доступность всегда оценивается с учётом временных ограничений.

Аутентичность. Сообщение, устройство, программа или пользователь действительно являются теми, за кого себя выдают. Подлинная команда должна поступать от разрешённого источника.

Неотказуемость и прослеживаемость. Позволяют установить, какое действие было выполнено, когда и каким субъектом. Эти свойства поддерживаются идентификацией, журналами событий и защищёнными процедурами обновления.

3. Активы, угрозы, уязвимости и риск

Проектирование защиты начинается не с выбора шифрования или межсетевого экрана, а с определения того, что необходимо защищать.

3.1. Активы

Активом называют объект, нарушение свойств которого способно причинить ущерб. Активами автомобиля являются:

- Управляющие функции (торможение, рулевое управление, ускорение).
- Электронные блоки управления (ECU).
- Программное обеспечение и прошивки.
- Ключи и сертификаты.

- Диагностические данные.
- Персональная информация пользователя.
- Журналы событий.
- Внешние сервисы и облачные интерфейсы.

3.2. Угрозы и уязвимости

Угроза — это потенциальная причина нежелательного события. **Уязвимость** — слабое место, которое может быть использовано угрозой. **Атака** — реализованная попытка воздействия. **Последствие** — физический, финансовый, операционный или репутационный ущерб. **Риск** связывает вероятность или осуществимость сценария атаки с тяжестью возможных последствий.

Типовые сценарии воздействия:

Сценарий	Механизм	Возможное последствие
Прослушивание	Пассивный перехват трафика	Утечка идентификаторов и данных
Подмена	Ввод ложного сообщения или команды	Неверное решение ЭБУ
Повтор	Повтор ранее допустимого сообщения	Несанкционированное действие
Отказ в обслуживании	Перегрузка сети или ресурса	Задержка или потеря функции
Повышение привилегий	Эксплуатация ошибки доступа	Управление защищённым компонентом
Несанкционированное обновление	Установка неподлинного ПО	Долговременный контроль системы

Для защиты от атаки повтором недостаточно проверить, что сообщение когда-то было подлинным. Система должна убедиться в его **свежести**. Применяются счётчики, временные метки, случайные запросы и криптографические коды аутентификации. Защита от отказа в обслуживании требует ограничения частоты запросов, приоритизации трафика и сохранения ресурсов для критичных задач.

3.3. Модель нарушителя

Нарушители различаются по целям, знаниям и ресурсам:

- **Случайный пользователь** может изменить настройки без понимания последствий.

- **Владелец** способен устанавливать неофициальное программное обеспечение.
- **Угонщик** стремится получить доступ или запустить двигатель.
- **Организованная группа** может атаковать парк автомобилей или серверную инфраструктуру.
- **Исследователь** ищет уязвимость для её ответственного раскрытия.

Следует учитывать физический и удалённый доступ. Физический доступ к диагностическому разъёму, блоку или проводке обычно даёт большие возможности, но требует приближения к автомобилю. Удалённая атака через мобильную связь, Wi-Fi, Bluetooth, приложение или облачный сервис потенциально масштабируется на большое число машин. Поэтому удалённые интерфейсы требуют особенно строгого разделения и контроля.

3.4. Поверхность атаки

Поверхностью атаки называют совокупность интерфейсов, через которые возможно взаимодействие с системой. К ней относятся:

- Беспроводной ключ (Smart Key).
- Радиоприёмники (RFID, NFC).
- Телематический модуль (сотовая связь).
- Bluetooth и Wi-Fi.
- USB-порты.
- Мультимедийная система.
- Мобильное приложение.
- Диагностический разъём (OBD-II).
- Зарядный интерфейс (для электромобилей).
- V2X-связь.
- Сервер производителя и облачные сервисы.
- Инструменты сервисной организации.

Размер поверхности атаки определяется не только количеством разъёмов. Важны доступные команды, привилегии компонента и его связь с критичными сетями. Развлекательная система может казаться некритичной, но при отсутствии сетевого разделения через неё открывается путь к управляющим блокам. Исследователи обнаружили, что жёстко заданные учётные данные (например, имена точек доступа) в прошивке информационно-развлекательной системы создают поверхность атаки межсетевого уровня, где локальная уязвимость может перерасти в удалённую компрометацию целых парков автомобилей.

3.5. Построение пути атаки

Сценарий атаки удобно представлять как последовательность шагов от внешнего интерфейса к активу. Первым шагом может быть получение доступа к беспроводному каналу или учётной записи. Затем нарушитель использует ошибку программного обеспечения, повышает привилегии, закрепляется в компоненте, исследует сеть и пытается перейти через шлюз. Последний шаг

направлен на изменение данных, выполнение команды или блокирование функции.

Для каждого шага определяются предварительные условия и существующие барьеры. Если хотя бы один обязательный переход надёжно закрыт, весь путь становится практически неосуществимым. Однако нельзя рассчитывать только на один барьер. Ошибка конфигурации, общая учётная запись или сервисный режим могут обойти предусмотренную защиту.

Особое внимание уделяется **масштабируемости**. Атака с физическим доступом к одному автомобилю и специальным оборудованием может иметь ограниченный ущерб для парка. Уязвимость облачного сервиса или беспроводного интерфейса способна применяться автоматически к тысячам автомобилей. Даже если единичное последствие умеренное, массовость повышает общий риск и срочность исправления.

4. Нормативно-правовая база

4.1. ISO/SAE 21434:2021 «Road vehicles — Cybersecurity engineering»

ISO/SAE 21434 является международным стандартом, определяющим инженерные требования к управлению рисками кибербезопасности на протяжении всего жизненного цикла электрических и электронных систем дорожных транспортных средств — от концепции и разработки до производства, эксплуатации, обслуживания и вывода из эксплуатации.

Стандарт определяет структуру для управления кибербезопасностью, включая:

- Управление рисками кибербезопасности на уровне концепции.
- Требования к разработке продуктов.
- Требования к производству, эксплуатации, обслуживанию и выводу из эксплуатации.
- Единый язык для общения и управления рисками кибербезопасности.

В отличие от ISO 26262, который фокусируется на случайных отказах, ISO/SAE 21434 адресует преднамеренные действия нарушителей. Стандарт требует от производителей внедрения **системы управления кибербезопасностью (Cybersecurity Management System, CSMS)** на протяжении всего жизненного цикла.

4.2. UN Regulation No. 155 — Cyber Security and Cyber Security Management System

UNECE Regulation No. 155 устанавливает единообразные положения concerning the approval of vehicles with regards to cyber security and cyber security management system. Регламент применяется к транспортным средствам категорий L, M, N и O, оснащённым по меньшей мере одним электронным блоком управления.

Ключевые требования R155:

- Производитель должен иметь действующий сертификат соответствия для системы управления кибербезопасностью (CSMS).
- CSMS должна охватывать весь жизненный цикл vehicle.
- Производитель должен проводить оценку рисков кибербезопасности и внедрять соответствующие меры защиты.
- Требуется мониторинг киберугроз и реагирование на инциденты.

R155 вступил в силу в качестве обязательного требования для новых типов транспортных средств с 1 июня 2026 года.

4.3. UN Regulation No. 156 — Software Update and Software Update Management System

UNECE Regulation No. 156 устанавливает требования к программным обновлениям и системам управления обновлениями. Регламент обязывает производителей внедрить **систему управления обновлениями программного обеспечения (Software Update Management System, SUMS)** для обеспечения операционной безопасности и кибербезопасности на протяжении всего жизненного цикла vehicle.

Ключевые требования R156:

- Производитель должен иметь сертифицированную SUMS.
- Обновления ПО должны быть безопасными (проверка подлинности и целостности).
- Обновления не должны нарушать функциональную безопасность.
- Водитель должен быть информирован об обновлениях.
- Должна быть возможность отката (rollback) в случае неудачного обновления.

4.4. Взаимосвязь стандартов

ISO/SAE 21434, UN R155 и UN R156 образуют взаимодополняющую нормативную базу:

- **ISO/SAE 21434** определяет **как** разрабатывать и внедрять защиту (инженерные требования).
- **UN R155** определяет **что** должно быть реализовано на уровне vehicle type approval (требования к CSMS и оценке рисков).
- **UN R156** определяет требования к **обновлениям ПО** как к критическому элементу жизненного цикла.

Производители, стремящиеся к сертификации по UN R155 и R156, должны внедрить процессы, соответствующие ISO/SAE 21434. NIST также участвует в развитии автомобильной кибербезопасности через Automotive Cybersecurity Community of Interest (COI), разрабатывая подходы к криптографии, целостности кода и безопасным обновлениям.

5. Методы защиты электронных блоков управления

5.1. Безопасная загрузка (Secure Boot)

Безопасная загрузка — это механизм, обеспечивающий выполнение только аутентичного и неповреждённого программного обеспечения при запуске ECU. Процесс основан на **аппаратном корне доверия (Hardware Root of Trust)** , реализованном через компоненты, такие как Hardware Security Modules (HSM), Trusted Platform Modules (TPM) или One-Time Programmable (OTP) память.

Процесс безопасной загрузки:

1. При включении питания первым запускается неизменяемый загрузчик (boot ROM), хранящийся в защищённой памяти.
2. Загрузчик проверяет цифровую подпись следующего этапа загрузки (например, загрузчика второго уровня) с использованием открытого ключа, жёстко заданного в boot ROM или хранящегося в HSM.
3. Если подпись верифицирована, управление передаётся на следующий этап.
4. Процесс повторяется для каждого последующего этапа (ядро ОС, приложения).
5. На каждом этапе проверяется целостность и подлинность кода.

Криптографические ключи или их хеши безопасно хранятся в HSM. В современных реализациях HSM может выполнять функции безопасного загрузчика на собственном ядре, обеспечивая защиту от компрометации даже в случае атаки на основное прикладное ядро. Безопасная загрузка предотвращает выполнение вредоносного кода, установленного через физический доступ, OTA-обновления или другие векторы атак.

5.2. Аппаратный модуль безопасности (Hardware Security Module, HSM)

HSM — это специализированный криптографический процессор, предназначенный для безопасного хранения ключей и выполнения криптографических операций в защищённой среде. В автомобильных ECU HSM обычно интегрируется в микроконтроллер.

Ключевые функции HSM:

- **Безопасное хранение ключей.** Ключи хранятся в защищённой памяти, недоступной для прикладного программного обеспечения.
- **Криптографические операции.** Выполнение шифрования, расшифрования, генерации и верификации цифровых подписей, вычисление кодов аутентификации сообщений (MAC).
- **Генерация случайных чисел.** Аппаратный генератор истинно случайных чисел для криптографических протоколов.
- **Ускорение криптографии.** Выполнение ресурсоёмких операций (например, RSA, ECC, AES) на аппаратном уровне.
- **Поддержка безопасной загрузки.** Хранение и управление ключами для верификации подписей загрузчика.

Анализ архитектуры автомобильных HSM показывает, что конструктивные решения HSM напрямую влияют на безопасность цепочки доверия при загрузке. HSM поддерживает такие механизмы, как безопасная загрузка, управление ключами, криптографические операции и доверенную связь между компонентами системы.

5.3. Защита от отката (Rollback Protection)

Защита от отката предотвращает установку более старой версии программного обеспечения с известными уязвимостями. Механизм основан на использовании счётчиков версий (version counters) или временных меток, которые хранятся в защищённой памяти (например, в OTP-памяти или HSM).

При установке обновления система проверяет, что номер версии нового ПО больше текущего. Если злоумышленник пытается установить старую версию, система отклоняет обновление. Счётчик версий защищён от записи — его можно только увеличивать, но нельзя уменьшать.

5.4. Сегментация сетей и межсетевые экраны

Сегментация разделяет информационно-развлекательный, телематический, диагностический и управляющий домены. **Шлюз** (gateway) пропускает только предусмотренные сообщения и направления обмена.

Принципы сегментации:

- Критичные сети управления (тормоза, руль, двигатель) отделены от некритичных (мультимедиа, телематика).
- Шлюз фильтрует трафик между доменами, пропуская только разрешённые сообщения.
- Диагностический доступ к критичным ECU ограничен и требует аутентификации.
- Отладочные интерфейсы (JTAG, SWD) в серийном изделии отключаются или требуют строгой аутентификации.

Межсетевые экраны (firewalls) на сетевых шлюзах реализуют:

- Фильтрацию по идентификаторам сообщений (CAN ID, Ethernet MAC/IP).
- Контроль частоты сообщений (rate limiting) для защиты от DoS-атак.
- Обнаружение аномальных паттернов трафика.

5.5. Криптографические механизмы

Шифрование защищает конфиденциальность, но не решает все задачи. Для управляющего сообщения часто важнее подтвердить источник и отсутствие изменения.

Код аутентификации сообщения (Message Authentication Code, MAC). Вычисляется на основе секретного ключа и содержания сообщения. Получатель выполняет собственный расчёт и сравнивает результат.

Цифровая подпись. Решает сходную задачу с использованием пары открытого и закрытого ключей и применяется, например, для проверки программного пакета.

Криптографический механизм надёжен только при правильном управлении ключами. Необходимо безопасно создавать, записывать, хранить, обновлять и отзывать ключи. Один общий ключ для большого парка упрощает производство, но компрометация одного устройства создаёт риск для всех. Индивидуальные ключи уменьшают масштаб последствия, однако усложняют инфраструктуру и восстановление.

Криптография требует вычислительного времени и увеличивает объём сообщений. В сети реального времени это учитывается при выборе алгоритма, длины кода и частоты проверки. Нельзя снижать безопасность произвольно, но и нельзя добавлять задержку, нарушающую управление. Поэтому защита проектируется одновременно с сетевой архитектурой и временным анализом.

6. Системы обнаружения вторжений (IDS)

Полностью предотвратить все воздействия невозможно, поэтому система должна **обнаруживать** отклонения. Бортовая система обнаружения вторжений (Intrusion Detection System, IDS) анализирует сообщения, состояния блоков, сетевую нагрузку и последовательности событий.

6.1. Классификация IDS для CAN-шины

IDS для CAN-шины классифицируются на три типа:

1. Rule-based IDS (на основе правил). Используют заранее заданные правила для обнаружения известных атак. Например, обнаружение сообщений с недопустимыми идентификаторами или частотой, превышающей порог. Преимущество — простота и низкая вычислительная сложность. Недостаток — неспособность обнаруживать новые, неизвестные атаки.

2. Traditional machine learning-based IDS (на основе традиционного машинного обучения). Используют методы, такие как Support Vector Machines (SVM), Random Forest, XGBoost, для классификации трафика как нормального или аномального. IDS-XGB на основе модели XGBoost демонстрирует точность, прецизионность и F1-меру, превышающие 99% на трёх реальных наборах данных, удовлетворяя ограничениям реального времени и встраиваемых систем.

3. Deep learning-based IDS (на основе глубокого обучения). Используют нейронные сети (CNN, LSTM, Transformer, GNN) для обнаружения сложных атак.

6.2. Методы обнаружения на основе машинного обучения

Гибридные подходы. Комбинация SVM и LSTM для обнаружения аномалий в CAN-сетях.

LSTM-автоэнкодеры. Используются для обнаружения атак нулевого дня (zero-day) в сетях CAN автономных транспортных средств в рамках эффективной вычислительной структуры few-shot learning.

Двухуровневая архитектура LSTM-CNN. Первый уровень (LSTM) выполняет бинарную классификацию (норма/атака), второй (CNN) —

многоклассовую идентификацию четырёх распространённых типов атак: отказ в обслуживании (DoS), Fuzzy, спуфинг RPM и спуфинг GEAR, достигая F1-меры 99,8%.

Графовые нейронные сети (GNN). Предлагаются для обнаружения вторжений в CAN-сети с учётом структурных взаимосвязей между сообщениями.

Модели на основе Transformer. Обнаруживают аномалии путём моделирования пространственных (полезная нагрузка, длина данных) и временных (интервалы между сообщениями) характеристик независимо и их слияния на этапе принятия решения.

Свёрточный Anomaly Transformer. Первый подход few-shot learning для многоклассового обнаружения вторжений в бортовых сетях.

6.3. Размещение средств обнаружения

Датчик обнаружения может работать внутри электронного блока, в сетевом шлюзе, телематическом модуле или облачной платформе:

- **Внутренний монитор** лучше знает состояние конкретной программы и способен заметить нарушение памяти или последовательности вызовов.
- **Шлюз** видит обмен между доменами и может блокировать переход.
- **Облачная система** имеет больше вычислительных ресурсов и сравнивает поведение большого количества автомобилей.

Централизованное наблюдение удобно для корреляции, но не должно быть единственной защитой. При потере связи автомобиль обязан локально обнаруживать наиболее опасные отклонения. С другой стороны, отдельный блок не видит полный путь атаки. Поэтому события передаются между уровнями с учётом приоритета, доступной полосы и требований приватности.

Эксперименты показывают, что стековая модель IDS, развёрнутая на CAN-шине и центральном шлюзе, способна обнаруживать как внутренние, так и внешние сетевые атаки со средней точностью обнаружения 99,99% для внутренних атак CAN и 99,81% для внешних сетевых атак.

7. Уровень реагирования и восстановления

После обнаружения необходимо выбрать реакцию, пропорциональную риску. Система может:

- Отклонить сообщение.
- Ограничить интерфейс.
- Закрыть сессию.
- Временно заблокировать источник.
- Изолировать сетевой сегмент.
- Перевести функцию в безопасное состояние.
- Предупредить водителя.
- Отправить событие в центр мониторинга.

Слишком слабая реакция не остановит атаку, а чрезмерная сама создаст опасность. **Главный принцип автомобильной реакции** — не превращать защиту в новую опасность. Нельзя безусловно выключать критичный блок во время движения только потому, что обнаружено подозрительное сообщение. Сначала блокируется источник или конкретная команда, сохраняются локальные базовые функции, водитель получает понятное сообщение, а переход в более жёсткое состояние выполняется при безопасных условиях.

Восстановление включает возврат к доверенному состоянию, установку исправления, замену компрометированных ключей, проверку конфигурации и анализ журналов. После инцидента обновляют правила обнаружения и модель риска.

8. Интеграция функциональной безопасности и кибербезопасности

Современные исследования показывают необходимость **объединённого подхода** к функциональной безопасности и кибербезопасности. Кибербезопасность в соответствии с ISO/SAE 21434 фокусируется на защите ECU от атак и поддержании целостности системы. Стандарт идентифицирует **атаки с внедрением неисправностей (fault injection attacks)** как растущий риск.

Интеграция подходов позволяет:

- Обнаруживать как случайные неисправности, так и преднамеренные атаки.
- Использовать общие механизмы диагностирования для обоих типов событий.
- Обеспечивать единую стратегию перехода в безопасный режим.

В зональных архитектурах ECU механизмы функциональной безопасности ISO 26262 и механизмы кибербезопасности ISO/SAE 21434 могут быть интегрированы в единую архитектуру.

9. Комплексный пример: подозрительная дистанционная команда

Рассмотрим ситуацию: облачный сервис передаёт автомобилю команду дистанционного запуска. Криптографическая подпись формально верна, но команда поступает из нового региона, после серии неудачных входов в учётную запись и в необычное время. Отдельный признак не доказывает атаку. Однако корреляция повышает риск.

1. **Получение:** зарегистрировать входы, параметры устройства, источник команды, время, координаты и состояние автомобиля.
2. **Проверка:** подтвердить подпись, актуальность токена, права пользователя и свежесть команды.
3. **Корреляция:** связать новый регион, серию отказов, смену устройства и команду запуска.

4. **Оценка:** определить уверенность, возможное последствие и допустимость запуска в текущем состоянии.

5. **Решение:** отклонить команду, временно ограничить дистанционные операции и запросить дополнительное подтверждение.

6. **Реакция:** уведомить владельца, сохранить защищённый журнал и передать событие в мониторинг.

Пример показывает, что правильная криптографическая подпись не всегда означает безопасное действие. Учётные данные могли быть похищены. Поэтому Smart-система учитывает контекст и поведение. Одновременно она не должна навсегда блокировать законного владельца: предусматриваются восстановление доступа и проверяемая процедура отмены ограничения.

10. Вызовы и перспективы развития

10.1. Основные вызовы

Растущая поверхность атаки. Подключённые, автономные такси вводят риск физического вмешательства со стороны пассажиров. Сложность цепочки поставок ПО означает, что уязвимости могут скрываться на любом уровне. Уязвимости в инфраструктуре OTA, слабое управление ключами и компрометация цепочек поставок остаются критическими слепыми зонами.

Новые способы атак. Атаки на компоненты ИИ и сенсоры vehicle через манипулятивные входные данные создают новые риски.

Интеграция ИИ в защиту. Использование ИИ для обнаружения атак создаёт новые проблемы, связанные с объяснимостью, предвзятостью данных и дрейфом моделей.

Квантово-устойчивая криптография. Необходимость перехода на алгоритмы, устойчивые к квантовым вычислениям.

Баланс безопасности и производительности. Криптографические операции и IDS требуют вычислительных ресурсов, что может влиять на производительность систем реального времени.

10.2. Перспективы развития

Обнаружение атак на основе ИИ. Развитие методов few-shot learning для обнаружения атак нулевого дня.

Цифровые двойники для безопасности. Создание виртуальных моделей для тестирования сценариев атак и оценки уязвимостей.

Квантово-устойчивая криптография. Разработка и внедрение алгоритмов, устойчивых к квантовым вычислениям.

Федеративное обучение. Обучение моделей обнаружения на распределённых данных без их централизации для повышения приватности.

Интеграция с автономным вождением. Разработка комплексных подходов к безопасности, учитывающих как кибербезопасность, так и функциональную безопасность систем автономного вождения.

Объяснимый ИИ (XAI). Разработка методов, позволяющих интерпретировать решения, принимаемые ИИ-моделями обнаружения.

Автоматизированное реагирование. Разработка систем, способных автоматически изолировать скомпрометированные компоненты и перестраивать сетевую топологию.

11. Закрепление и завершение

11.1. Мини-тест

1. Чем автомобильная кибербезопасность отличается от функциональной безопасности?
2. Какие основные свойства информации подлежат защите в автомобильных системах?
3. Что такое поверхность атаки и какие элементы её формируют?
4. Как работает безопасная загрузка (Secure Boot) в ECU?
5. Какие методы машинного обучения применяются для обнаружения вторжений в CAN-сетях?

11.2. Эталонные краткие ответы

1. **Функциональная безопасность** (ISO 26262) адресует случайные неисправности и систематические ошибки. **Кибербезопасность** (ISO/SAE 21434) адресует преднамеренные действия нарушителей. Одинаковое внешнее проявление (например, неверное значение датчика) может иметь разные причины, и система должна корректно реагировать в обоих случаях.
2. Защите подлежат **конфиденциальность** (доступ только разрешённым субъектам), **целостность** (отсутствие несанкционированных изменений), **доступность** (функция доступна в требуемый момент), **аутентичность** (подтверждение источника), **неотказуемость и прослеживаемость** (возможность установить, кто и когда выполнил действие).
3. **Поверхность атаки** — совокупность интерфейсов, через которые возможно взаимодействие с системой: беспроводной ключ, телематический модуль, Bluetooth, Wi-Fi, USB, мультимедиа, мобильное приложение, диагностический разъём, зарядный интерфейс, V2X, облачные сервисы.
4. **Безопасная загрузка** основана на аппаратном корне доверия (HSM). При включении первый загрузчик проверяет цифровую подпись следующего этапа. Процесс повторяется для каждого уровня. Если подпись не верифицируется, выполнение блокируется. Ключи хранятся в защищённой памяти HSM.
5. Применяются **гибридные подходы** (SVM + LSTM), **LSTM-автоэнкодеры** для обнаружения атак нулевого дня, **двухуровневые LSTM-CNN** архитектуры, **графовые нейронные сети (GNN)** , **модели на основе Transformer**, **свёрточные Anomaly Transformer** для few-shot обучения.

11.3. Итоговые положения

Кибербезопасность автомобиля — это управление риском преднамеренного цифрового воздействия на протяжении жизненного цикла. Цель — затруднить проникновение, своевременно обнаружить аномалии, ограничить последствия и обеспечить восстановление.

Основные свойства защиты: конфиденциальность, целостность, доступность, аутентичность, неотказуемость и прослеживаемость.

Активы, угрозы, уязвимости и риск являются основой для проектирования защиты. Поверхность атаки современных автомобилей стремительно расширяется.

Нормативная база включает ISO/SAE 21434 (инженерные требования), UN R155 (CSMS и type approval) и UN R156 (SUMS и безопасные обновления).

Методы защиты ECU включают безопасную загрузку (Secure Boot), аппаратные модули безопасности (HSM), защиту от отката, сегментацию сетей и криптографические механизмы.

Системы обнаружения вторжений (IDS) классифицируются на rule-based, традиционные ML-based и deep learning-based. Достигают точности обнаружения >99%.

Реагирование и восстановление должны быть пропорциональны риску и не создавать новой опасности.

Интеграция функциональной безопасности и кибербезопасности позволяет обнаруживать как случайные неисправности, так и преднамеренные атаки.

Перспективы развития связаны с ИИ-обнаружением, квантово-устойчивой криптографией, федеративным обучением и объяснимым ИИ.

Задание после лекции

Выберите один из аспектов кибербезопасности интеллектуальных систем управления (безопасная загрузка, HSM, IDS на основе машинного обучения, нормативные требования UN R155/R156) и подготовьте аналитический обзор (2–3 страницы), в котором:

1. Опишите выбранный аспект и его роль в обеспечении кибербезопасности автомобиля.
2. Объясните принципы работы и технические решения.
3. Проанализируйте преимущества и ограничения.
4. Приведите примеры из научных исследований или промышленности.
5. Оцените перспективы развития выбранного аспекта.

Контрольные вопросы

1. Что понимается под кибербезопасностью автомобиля?
2. Какие свойства информации подлежат защите?
3. Чем кибербезопасность отличается от функциональной безопасности?
4. Что является активом Smart-системы?
5. Как связаны угроза, уязвимость, атака и последствие?
6. Что включает модель нарушителя?
7. Что называют поверхностью атаки?
8. Почему удалённый интерфейс может иметь повышенный риск?
9. Какие типовые сценарии воздействия применимы к автомобилю?
10. Каковы требования стандарта ISO/SAE 21434?
11. Что такое CSMS и какие требования к нему предъявляет UN R155?
12. Каковы требования UN R156 к обновлениям ПО?
13. Что обеспечивает безопасная загрузка (Secure Boot)?
14. Для чего выполняется сегментация бортовой сети?
15. Что такое HSM и какие функции он выполняет?
16. Какие криптографические механизмы применяются в автомобилях?
17. Как классифицируются IDS для CAN-шины?
18. Какие методы машинного обучения применяются для обнаружения вторжений?
19. Каковы преимущества и ограничения rule-based IDS?
20. Каковы преимущества и ограничения ML-based IDS?
21. Что такое атака нулевого дня (zero-day) и как она обнаруживается?
22. Какие требования предъявляются к журналу событий безопасности?
23. Как оценивается киберриск?
24. Почему реакция должна быть пропорциональна риску?
25. Что означает принцип многоуровневой защиты (defence in depth)?
26. Почему подлинная команда может оказаться опасной?
27. Какие этапы включает восстановление после инцидента?
28. Как интегрируются функциональная безопасность и кибербезопасность?
29. Каковы основные вызовы автомобильной кибербезопасности?
30. Каковы перспективы развития автомобильной кибербезопасности?

Список рекомендуемой литературы

Основная литература

1. Robert Bosch GmbH. Automotive Handbook. 11th ed. — Chichester: Wiley, 2022. — 2047 p. — ISBN 978-1-119-91190-6.
2. ISO/SAE 21434:2021. Road vehicles — Cybersecurity engineering. — Geneva: International Organization for Standardization, 2021. — DOI: 10.4271/ISO/SAE21434.
3. UN Regulation No. 155 — Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system [2025/5].
4. UN Regulation No. 156 — Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system.

Дополнительная литература

5. Matheus K., Königseder T. Automotive Ethernet. 3rd ed. — Cambridge: Cambridge University Press, 2021. — ISBN 978-1-108-84195-5.
6. Kim S., Shrestha R. Automotive Cyber Security: Introduction, Challenges, and Standardization. — Springer, 2020.
7. Chowdhury N., Mackenzie L. Vehicular Communications for Smart Cars: Protocols, Applications and Security Concerns. — CRC Press, 2021.
8. Intrusion Detection Systems for In-Vehicle Networks: Protocols, Applications, and Challenges // IEEE Xplore, 2025.
9. Lightweight temporal and spatial fusion for intrusion detection in automotive controller area network // ScienceDirect, 2026.
10. GNN-Based in-Vehicle Network Intrusion Detection System // IEEE Xplore, 2025.
11. EF-IDS: An efficient intrusion detection system with enriched features for CAN bus in modern vehicles // ScienceDirect, 2025.
12. IDS_XGB: Next-Generation Intrusion Detection for Automotive Embedded Systems // Springer Professional, 2026.
13. Zero-Day Threat Detection in Autonomous Vehicles Using Few-Shot LSTM Autoencoders on CAN Bus Data // IEEE Xplore, 2025.
14. Multi-class intrusion detection system for in-vehicle networks using few-shot learning and convolutional anomaly transformer network // ScienceDirect, 2025.
15. A dual layer LSTM-CNN framework for real time and precise per-message intrusion detection in In-vehicle networks // ScienceDirect, 2025.
16. Anomaly Detection in Automotive CAN Networks Using a Hybrid Approach // IEEE/ACS AICCSA, 2025.
17. Automotive HSMs — Architectural Challenges and Security Implications // arXiv, 2026.

18. ISO 26262:2018. Road Vehicles — Functional Safety. Parts 1–10. — Geneva: International Organization for Standardization, 2018.
19. ISO 24089:2023. Road Vehicles — Software Update Engineering. — Geneva: International Organization for Standardization, 2023.

Электронные ресурсы

20. SAE International. SAE Technical Papers Database. — Режим доступа: https://www.sae.org/publications/technical-papers.
21. IEEE Xplore. Scientific and Technical Publications Database. — Режим доступа: https://ieeexplore.ieee.org.
22. ScienceDirect. Scientific and Technical Publications Database. — Режим доступа: https://www.sciencedirect.com.
23. UNECE. UN Regulations on Cybersecurity and Software Updates. — Режим доступа: https://unece.org/transport/vehicle-regulations.
24. ISO. International Standards Catalogue. — Режим доступа: https://www.iso.org.
25. NIST. Automotive Cybersecurity Community of Interest (COI). — Режим доступа: https://csrc.nist.gov[reference:51].