ФГБОУ ВО «МОСКОВСКИЙ АВТОМОБИЛЬНО-ДОРОЖНЫЙ
ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ (МАДИ)»

Общие подходы к модели рисков и угроз для высокоавтоматизированного и беспилотного движения

Жанказиев Султан Владимирович

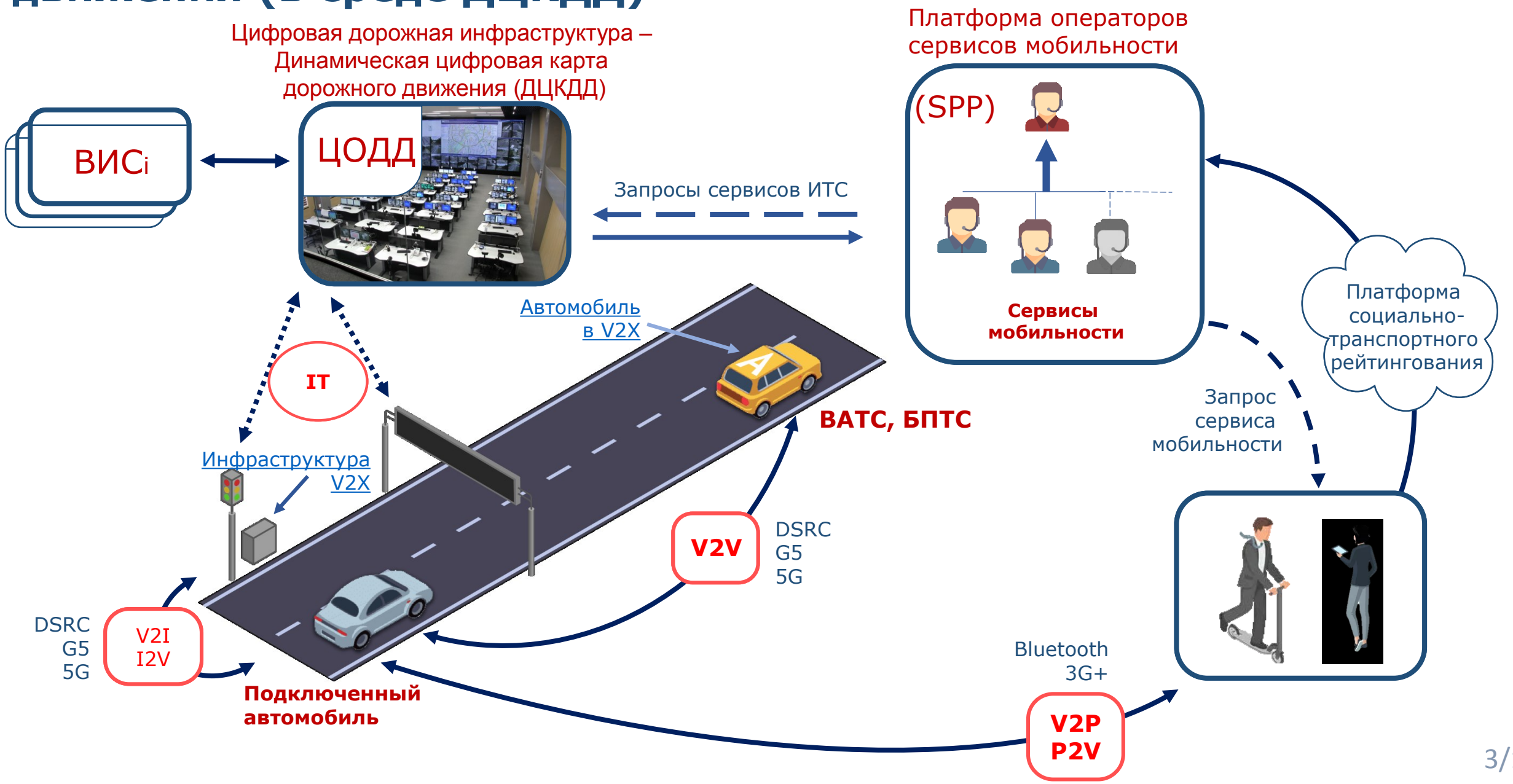
Д.т.н., профессор, заведующий кафедрой «Организация и безопасность движения, интеллектуальные транспортные системы» МАДИ

г.Москва, 20.06.2024г

Как будет выглядеть беспилотная мобильность?

1 **Робот-водитель** → 2 **Робот-автомобиль** → 3 **Цифровая экосистема беспилотного движения**

Экосистема высокоавтоматизированного и беспилотного движения (в среде ДЦКДД)



Структура систем цифрового двойника ВАТС (в системе ДЦКДД)

* ИТС 3,4 – Интеллектуальные транспортные системы 3 или 4 уровня развития. Особенность: сервисы мобильности (в т.ч. ВАТС), реализуемые в сервисах ИТС

Примеры атак на высокоавтоматизированные автомобили (опыт МАДИ)

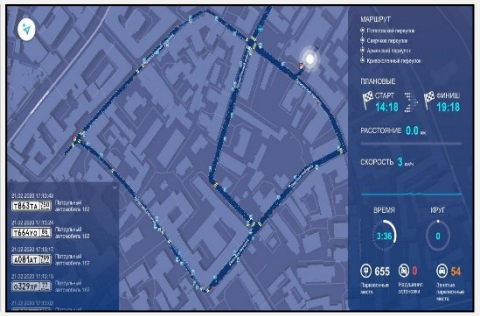
1

2019 г. - Технологический конкурс «Зимний город» - 4-5 цифровых «рельс» в полосе с политикой перестроения на основе данных ИТС

Реализовано <u>БЕЗОПАСНОЕ</u> движение ВАТС, БПТС

2

2020 – 2021г.г. - Запуск «беспилотного паркона» - движение по ДЦКДД в условиях максимальной конфликтности и высоких рисков ДТП



В процессе реализации выполнены следующие работы:

- Разработан условный «цифровой двойник участка дороги» г.Москвы;
- Разработан условный «цифровой двойник транспортного средства»;
- Выполнено оснащение «беспилотного паркона» техническими средствами для автономного движения;
- Разработана и апробирована технология ДЦКДД в условиях рисков ДТП.

Реализовано <u>СЕРВИСНОЕ</u> движение ВАТС, БПТС

<u>Выявлены два типа атак:</u>

- воздействие на территорию проведения конкурсных заездов.

  Результат – сбой высокоточной навигации.

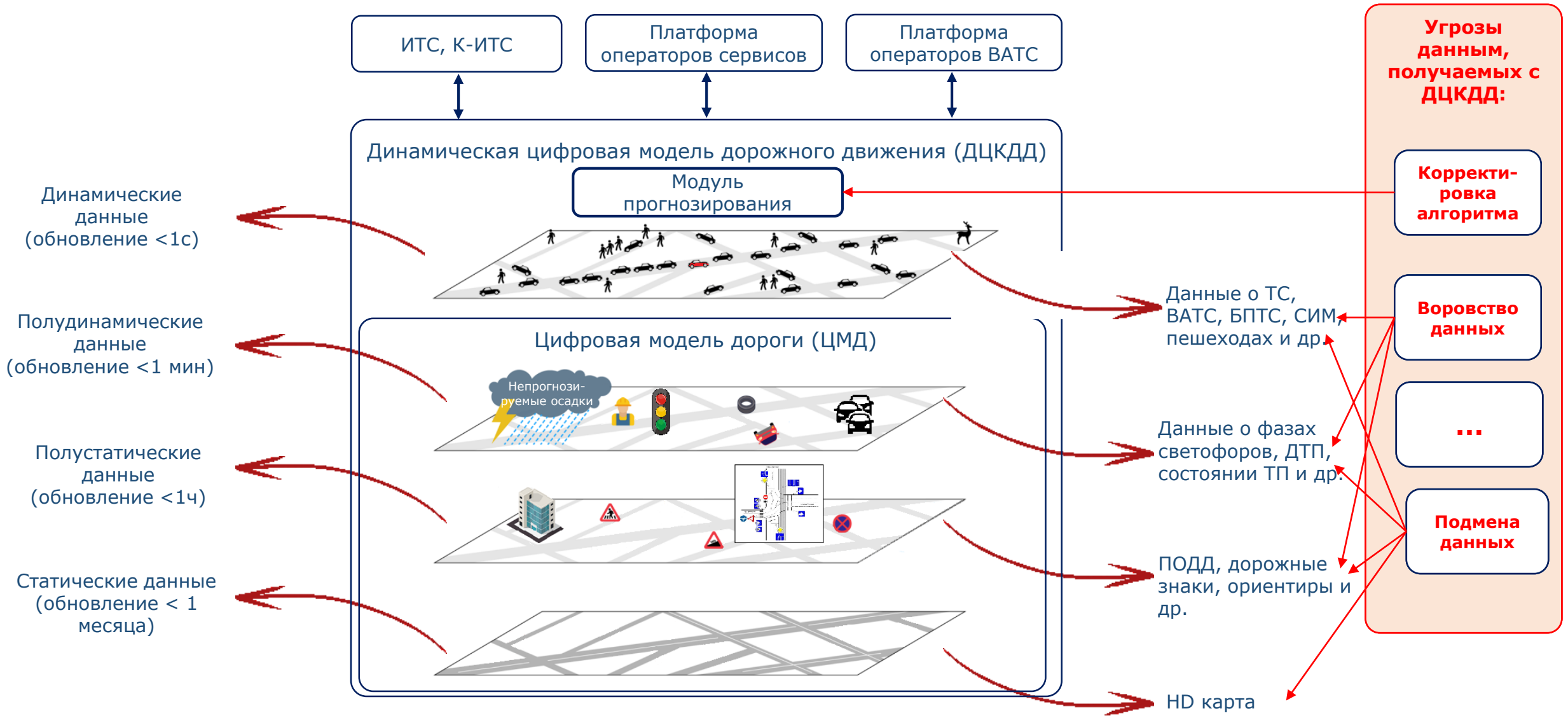
- вмешательство в работу систем технического зрения, анализа и управления (НВ).

  Результат – аварийный останов транспортного средства.

<u>Выявлены атаки</u> - вмешательство в работу систем технического зрения (НВ)

Результат – незначительное замедление движения.

Динамическая цифровая карта дорожного движения (ДЦКДД)



Уязвимости высокоавтоматизированного и автономного движения

Сервер производителя

Сервер поставщика / СТО

Сервер оператора ВАТС

Серверы операторов сервисов V2X

Телематика

R 155 ЕЭК ООН

32 уязвимости !!!

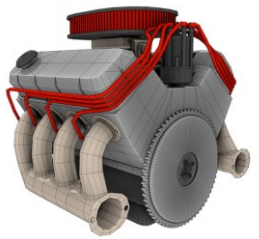
БИС

Тахограф

Устройство контроля состояния водителя

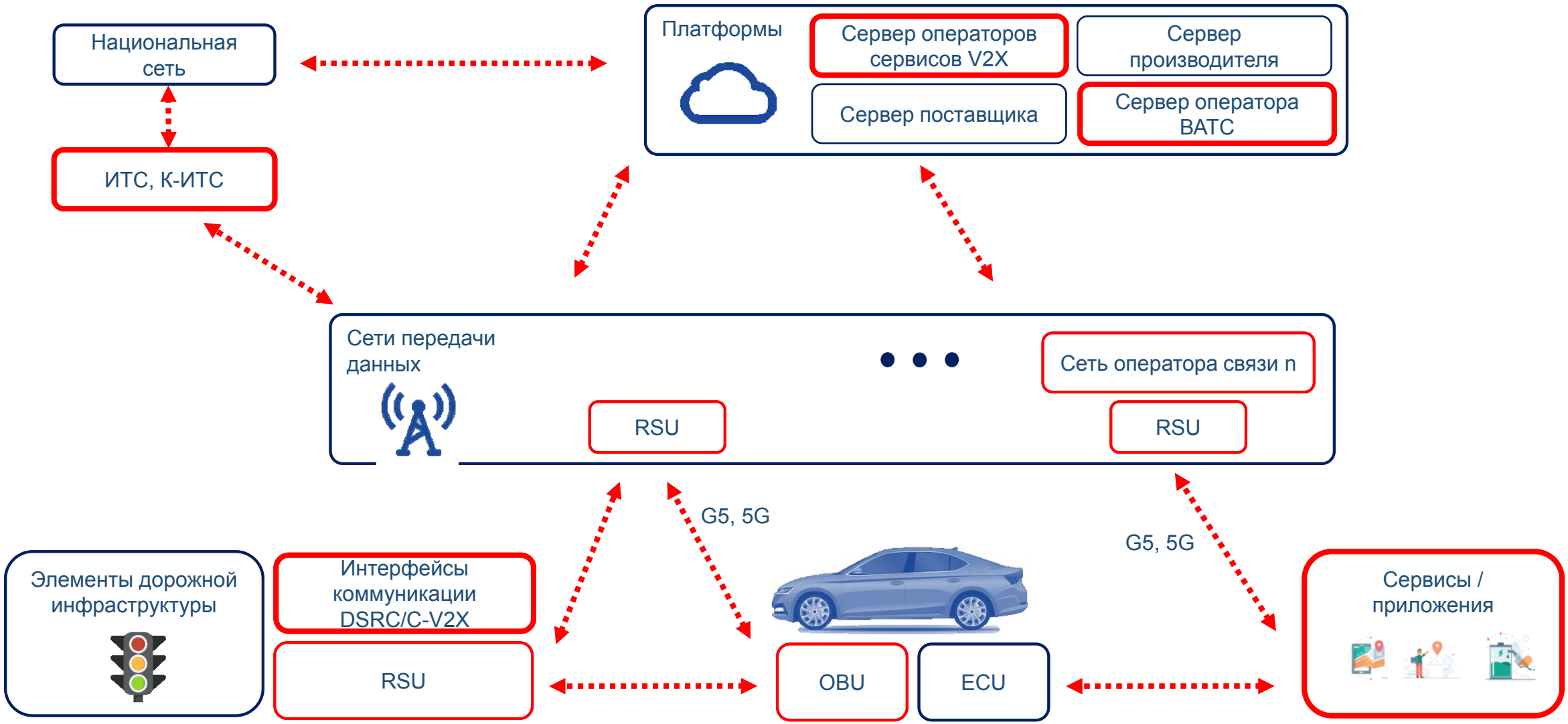
Контроллер СРС

АКПП



Двигатель

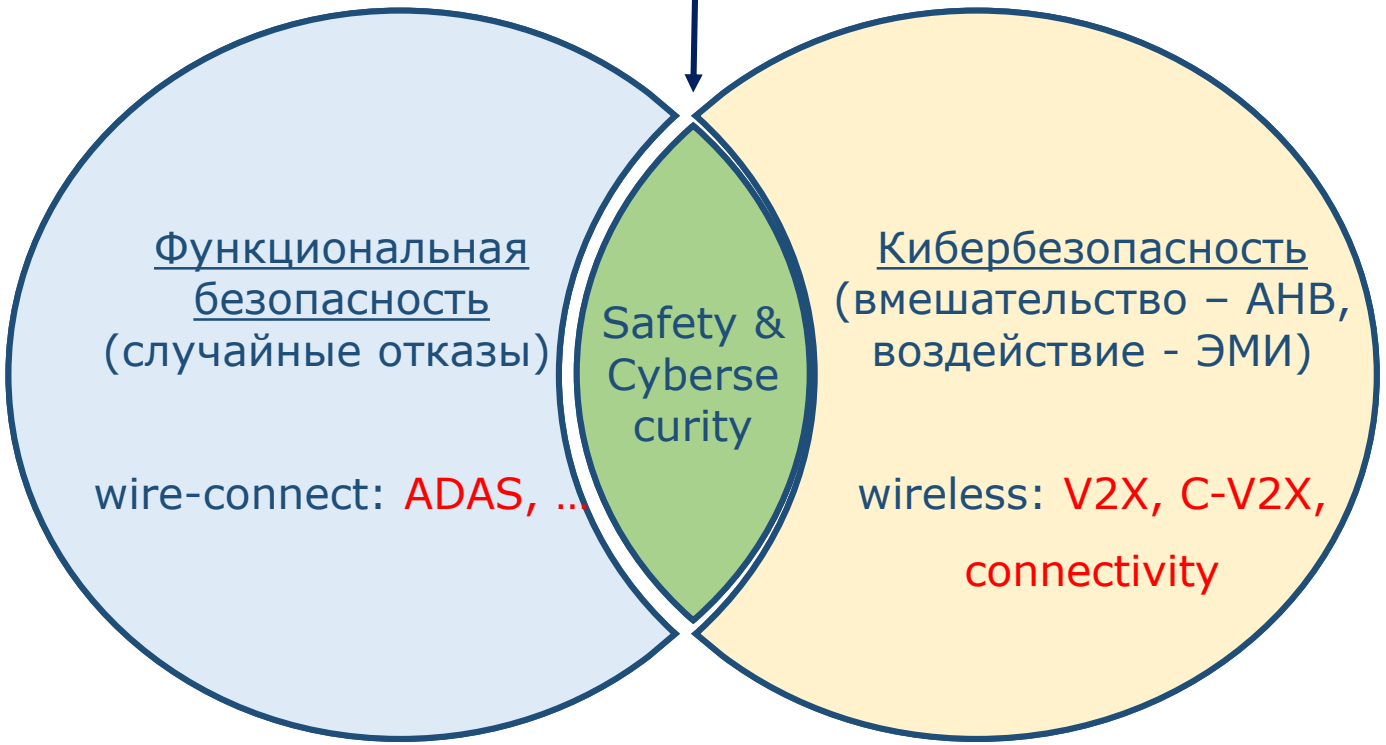
Обзор киберугроз экосистемы V2X



Взаимное влияние Safety & Cybersecurity

«В современных автомобилях функциональная безопасность и кибербезопасность – одно и то же» - *Дэн Амманн (**2018**, ex- President GM)*

2024 г (!)



! Существующая проблема: Отсутствие документов и требований технологического регулирования в части тестирования

! **Необходимо формировать требования к кибербезопасности на этапе проектирования системы с применением моделирования возможных угроз**

Статистика кибератак (2023 г)

- Одна кибератака может стоить втопроизводителю – до **1,1 млрд. долларов**
- Рост числа кибератак с 2018 по 2023 год – **225%**

Основные направления кибератак

- Серверная инфр-ра – **40%**
- Бесключевой доступ – **26%**
- Бортовая телематика– **12%**

Нормативное регулирование (международный опыт)

- UN Regulation R.155
- UN Regulation R.156
- ISO/SAE 21434

Нормативное регулирование (отечественный опыт)

Не регламентируется

Этапы возникновения и примеры угроз ВАТС

Этапы возникновения угроз ВАТС

- Примеры угроз ВАТС

Разработка

- Создание уязвимостей при проектировании системы и механизмов управления ВАТС, программном обеспечении ВАТС;

Производство

- Внедрение незащищенных коммуникаций при производстве элементов или сборке ВАТС;

Сборка и настройка

- Установка вредоносного ПО, изменение параметров системы управления ВАТС или характеристик элементов систем управления ВАТС при сборке и настройке;

Хранение

- Передача некорректных данных в систему управления ВАТС от серверов операторов сервисов V2X;

- Установка вредоносного ПО при прохождении технического обслуживания или обновления ПО системы управления ВАТС;
- Перехват управления у оператора ВАТС с целью совершения противоправных и/или преступных действий во время удаленного управления ВАТС и др.

Эксплуатация и техническое обслуживан

Пример сценария атаки

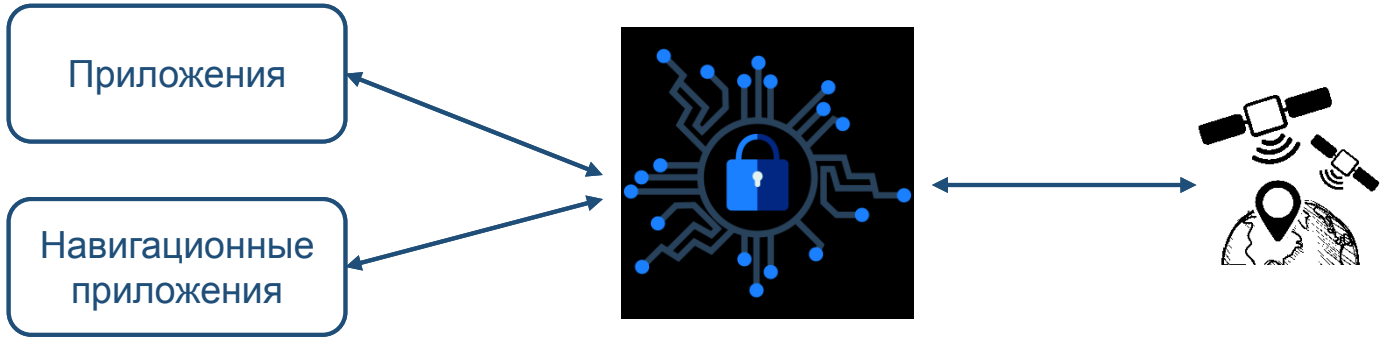
1. Программные сервисы, использующие данные о локации (LBS-сервисы) - сторонние приложения через интерфейс программирования приложения (API) навигатора предлагают рекламу по пути следования;
2. Навигатор передает данные стороннему приложению информацию о маршруте.

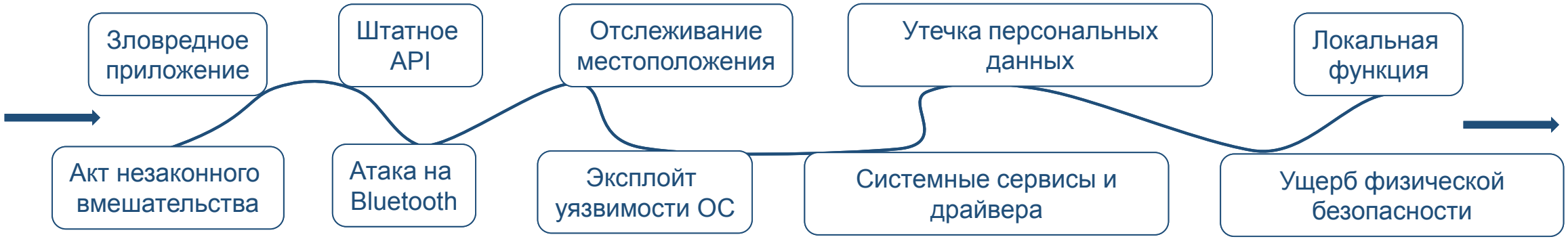
Активы вовлечённые в историю:

- Персональные данные (геолокация + время, маршрут и т.д.)

Ущерб, связанный с активами:

- Утечка персональных данных;
- Ущерб физической безопасности (*Злоумышленник может навязать пользователю маршрут*).





Решения

Необходимо:

- разработать модель нарушителя;
- разработать модель рисков и угроз;
- Разработать принципы (технические) и меры (нормативные) защиты.

Приказом от 20.10.2023 г №944 о.д. на базе ФГБОУ ВО МАДИ под эгидой Минцифры РФ создана рабочая группа (РГ) «Кибербезопасности в экосистеме высокоавтоматизированного и беспилотного движения» (КЭВБД)

Руководитель РГ - ***С.В. Жанказиев***

ЭТАПЫ работ РГ КЭВБД

2024 г.	2025 г.	2026 г. → ...
РГ КЭВБД	Центр компетенций КЭВБД	+ Орган по сертификации в области КЭВБД

ВЗАИМОДЕЙСТВИЕ

Министерство цифрового развития и массовых коммуникаций РФ	Министерство промышленности и торговли РФ	Министерство транспорта РФ
Доверенная платформа «СейфНет» НТИ	Институты развития	Министерство образования и науки РФ

kaspersky · positive technologies · ATOM · Ростех

РОСАТОМ · ГРИНАТОМ РОСАТОМ · КРИТИЧЕСКИЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ РОСАТОМ · НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

Модель нарушителя

Предложения по защите ВАТС от АНВ

Сервер производителя

Сервер поставщика / СТО

Сервер оператора ВАТС

Серверы операторов сервисов V2X

Телематика

БИС

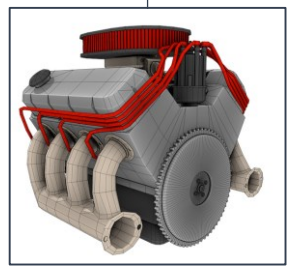
Центральный шлюз

Тахограф

Устройство контроля состояния водителя

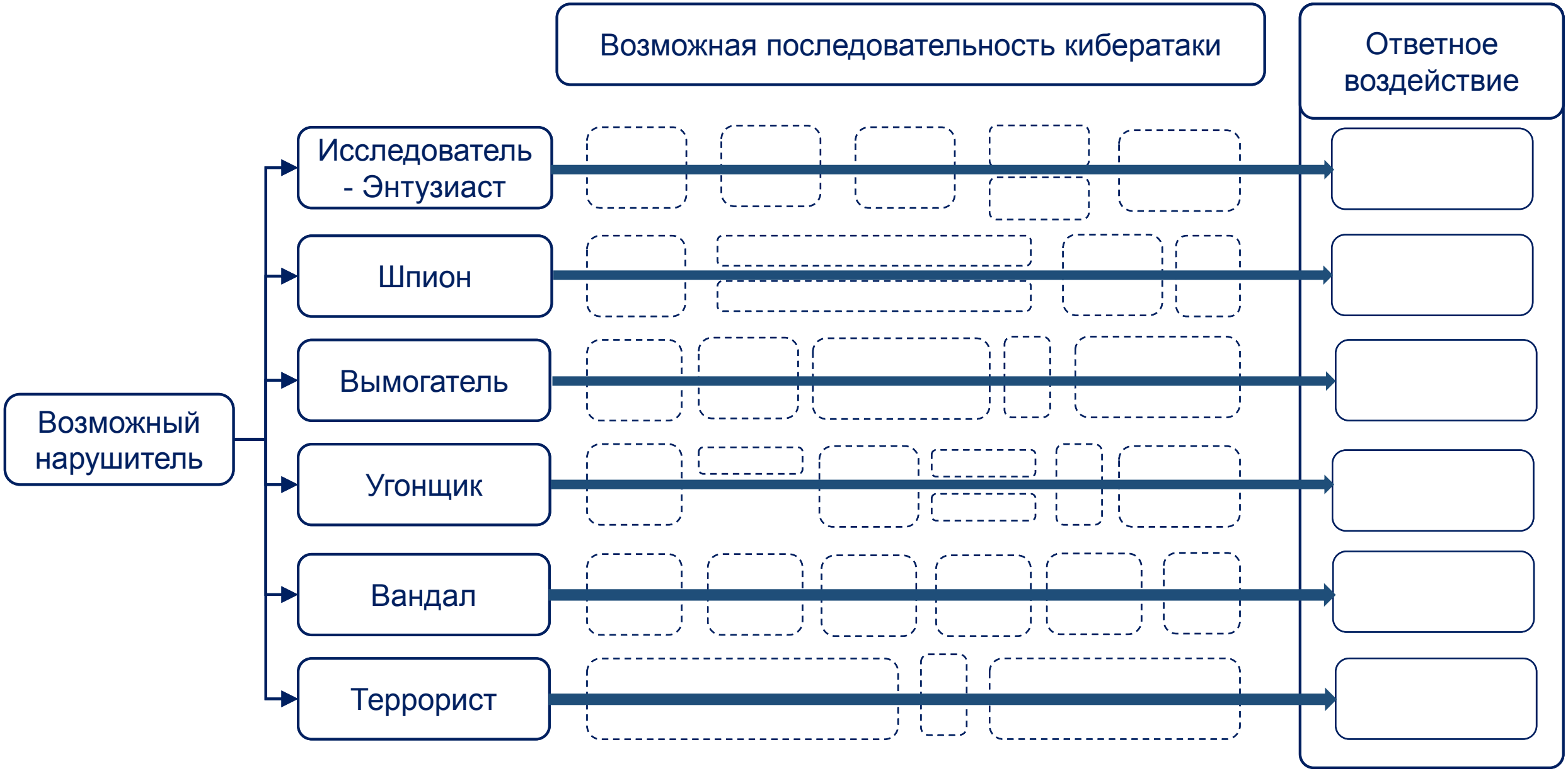
Контроллер CPC

АКПП



Двигатель

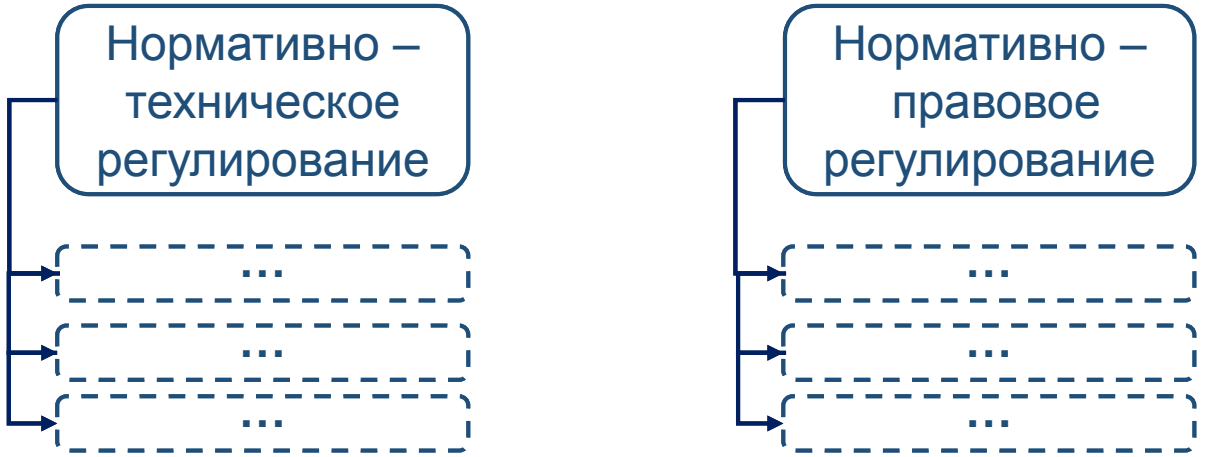
Моделирование угроз



Регуляторное воздействие

Задача 1:

Определить требования к кибербезопасности на уровне Экосистемы и зарегулировать соответствующими документами:



Задача 2:

На первоначальном этапе предложить производителям проходить испытания устойчивости к кибератакам, исходя из перечня самых распространенных уязвимостей.

Задача 3:

Целесообразно создание органов по сертификации технологий, обеспечивающих кибербезопасность Экосистемы, а так же аттестации специалистов.

Спасибо за внимание!