Перспективные задачи в интеллектуальных транспортных системах

Науменко Антон Павлович
Зам. начальника отдела
ООО «СФБ Лаб»

Что такое ИТС?

Интеллектуальная транспортная система – комплекс систем, который помогает эффективно эксплуатировать транспортную сеть, используя информационные, коммуникационные и управленческие технологии, встроенные в транспортное средство или дорожную инфраструктуру.

Что такое ИТС?

Создание единой архитектуры ИТС позволяет контролировать **три** основных направления

- **Безопасность.** Снижение аварийности на дорогах
- **Мобильность.** Сбор информации о пробках от движущихся в потоке автомобилей и информирование участников движения
- **Защита окружающей среды.** Снижение ущерба окружающей среде от автотранспорта

Ключевые области цифровизации

Нормативная основа для создания ИТС

- Государственная программа «Развитие транспортной системы»
- Указ Президента РФ от 7 мая 2018 г. N 204 "О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года"
- Указ Президента РФ от 21 июля 2020 г. N 474 "О национальных целях развития Российской Федерации на период до 2030 года"
- Транспортная стратегия Российской Федерации до 2030 года с прогнозом на период до 2035 года
- О внесении изменений в государственную программу Российской Федерации «Развитие транспортной системы»
- Концепция создания и функционирования национальной сети интеллектуальных транспортных систем на автомобильных дорогах общего пользования
- Методика оценки и ранжирования локальных проектов в целях реализации мероприятия «Внедрение интеллектуальных транспортных систем, предусматривающих автоматизацию процессов...»

Сервисы, развиваемые в ИТС

Актуальное техническое состояние

Министерством транспорта определено **пять** уровней зрелости ИТС

0 (Нулевой)

1 (Начальный)

2 (Базовый)

3 (Зрелый)

4 (Продвинутый)

Актуальное техническое состояние

Уровни зрелости	Требования
0(Нулевой)	Отсутствие подсистем ИТС в агломерации или наличие отдельных типов периферийного оборудования, функционально, информационно и технически не связанного между собой
1(Начальный)	○ Наличие программы комплексного развития транспортной инфраструктуры, комплексной схемы организации дорожного движения ○ Наличие центра управления дорожным движением ○ Наличие центра управления общественным транспортом ○ Наличие подсистемы светофорного управления ○ Наличие подсистемы мониторинга параметров транспортных потоков ○ Наличие подсистемы метеомониторинга ○ Наличие интеграционной платформы
2(Базовый)	Дополнительно к первому уровню: ○ Наличие подсистемы диспетчеризации управления служб содержания дорог ○ Наличие подсистемы видеонаблюдения, детектирования ДТП и ЧС
3(Зрелый)	Требования не установлены
4(Продвинутый)	Требования не установлены

Актуальное техническое состояние

Уровни зрелости	Требования
0(Нулевой)	Отсутствие подсистем ИТС в агломерации или наличие отдельных типов периферийного оборудования, функционально, информационно и технически не связанного между собой
1(Начальный)	○ Наличие программы комплексного развития транспортной инфраструктуры, комплексной схемы организации дорожного движения ○ Наличие центра управления дорожным движением ○ Наличие центра управления общественным транспортом ○ Наличие подсистемы светофорного управления ○ Наличие подсистемы мониторинга параметров транспортных потоков ○ Наличие подсистемы метеомониторинга ○ Наличие интеграционной платформы
2(Базовый)	Дополнительно к первому уровню: ○ Наличие подсистемы диспетчеризации управления служб содержания дорог ○ Наличие подсистемы видеонаблюдения, детектирования ДТП и ЧС
3(Зрелый)	Требования не установлены
4(Продвинутый)	Требования не установлены

Необходимость обеспечения ИБ

ФЗ-187: субъект **КИИ** – государственный орган, государственное учреждение, российское юридическое лицо и (или) индивидуальный предприниматель, которому на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере: здравоохранения; науки; **транспорта;** связи…

Актуальное состояние ИБ. Проблемы и задачи

Только часть ИТС в стране на данный момент классифицирована как объект КИИ

Требуется создать базовую модель угроз ИТС (с учетом требования ФСБ и ФСТЭК)

Разработка с учетом актуальных угроз отечественных криптографических механизмов защиты с целью их последующей стандартизации

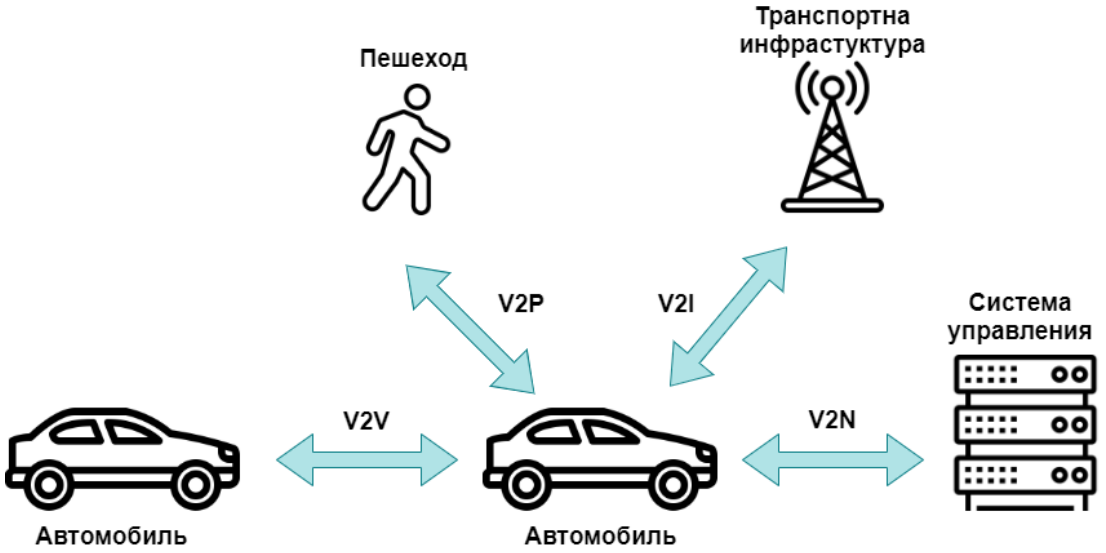
Внесение (при необходимости) изменений в существующую нормативную базу, регулирующую «Транспорт» в нашей стране

Криптографические задачи в ИТС

Организация защищенного взаимодействия для V2X

Для разработки и внедрения беспилотного транспорта, необходима организация взаимодействие **V2X** (*Vehicle-to-Everytning*)

V2X включает в себя: V2V, V2P, V2I, V2N



Криптографические задачи в ИТС

Организация защищенного взаимодействия для V2X

Особенности построения V2X

- Передача открытых данных (местоположение, скорость, направление следования и т.п.)
  ⇒ обеспечение целостности
- Большое количество участников движения ⇒ Большой объем передаваемых данных
- Быстрая смена положения участников движения
  ⇒ высокая пропускная способность сети

Криптографические задачи в ИТС

Организация защищенного взаимодействия для V2X

V2X передача открытых данных по каналу

Необходимость обеспечения целостность и/или конфиденциальность в многопользовательской сети

Использование криптографических алгоритмов

Криптографические задачи в ИТС

Организация защищенного взаимодействия для V2X

Согласно спецификациям ETSI ITS и IEEE 1609.2 разработана специальная PKI инфраструктура – **SCMS** (система управления безопасностью учетных данных)

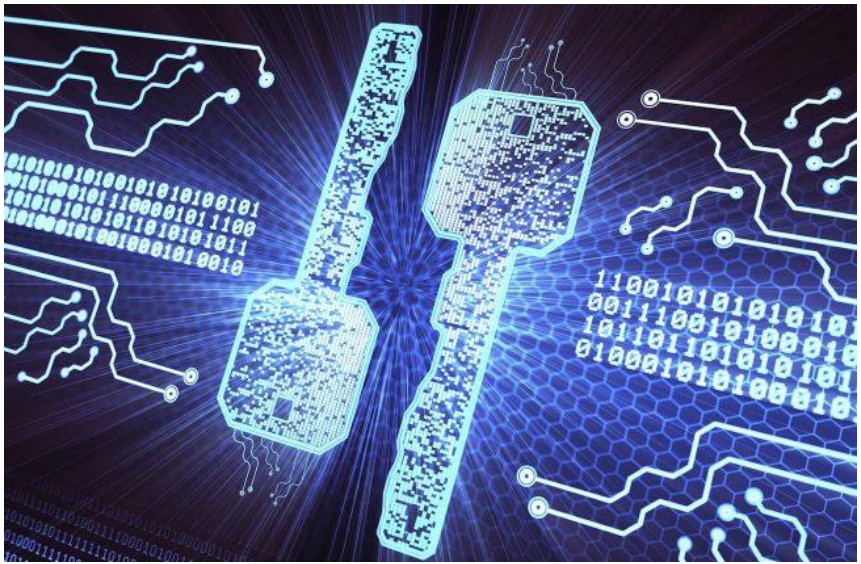
В состав SCMS включены:

- Схемы подписи ECDSA и ECQV
- Ассиметричная схема шифрования ECIES для защиты запросов между транспортной системой и УЦ
- Специальная схема подписи произвольного числа сертификатов за один запрос Butterfly Key Expansion

Криптографические задачи в ИТС

Организация защищенного взаимодействия для V2X

Еще одно направление для исследований и разработок: создание постквантовых схем подписи для V2X



Выводы

1. В ИТС как объект КИИ требуется внедрение отечественных криптографических механизмов (в частности, с целью обеспечения контроля целостности передаваемых данных и аутентификации участников системы)
2. Требуется разработка базовой модели угроз для ИТС с учетом требований ФСБ (и ФСТЭК) и с учетом необходимости применения криптографических методов
3. Требуется разработка соответствующих актуальным угрозам ИБ ИТС отечественных криптографических механизмов защита с целью их последующей стандартизации

ТЕХНО 2023 infotecs ФЕСТ

Спасибо за внимание!

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363