БЕЗОПАСНОСТЬ «ИНТЕРНЕТА ВЕЩЕЙ»

МИНИСТЕРСТВО ТРАНСПОРТА
РОССИЙСКОЙ ФЕДЕРАЦИИ

ЭКОСИСТЕМА ЦИФРОВЫХ ПЛАТФОРМ ЦИФРОВОГО ПРОСТРАНСТВА ТРАНСПОРТНОГО КОМПЛЕКСА

МУЛЬТИМОДАЛЬНЫЕ ГРУЗОВЫЕ ПЕРЕВОЗКИ

ПРЯМЫЕ СМЕШАННЫЕ ПАССАЖИРСКИЕ ПЕРЕВОЗКИ

УПРАВЛЕНИЕ ЦИФРОВОЙ ТРАНСПОРТНОЙ ИНФРАСТРУКТУРОЙ

ЕДИНАЯ ГОСУДАРСТВЕННАЯ ЦИФРОВАЯ ПЛАТФОРМА

Координация цифровых платформ, мониторинг состояния и управления развитием транспортного комплекса

ИНТЕГРАЦИЯ В МИРОВОЕ ТРАНСПОРТНОЕ ПРОСТРАНСТВО

ФУНКЦИОНАЛЬНАЯ И ТРАНСПОРТНАЯ БЕЗОПАСНОСТЬ

ЭКОЛОГИЧЕСКАЯ ПАРАДИГМА

БЕСПИЛОТНЫЙ ТРАНСПОРТ

■ ГОСУДАРСТВЕННЫЙ СЕГМЕНТ
■ БИЗНЕС-СЕГМЕНТ

ЦИФРОВАЯ ПЛАТФОРМА ТРАНСПОРТНОГО КОМПЛЕКСА

ТЕХНОЛОГИИ ИДЕНТИФИКАЦИИ

ПРОМЫШЛЕННЫЙ ИНТЕРНЕТ ВЕЩЕЙ

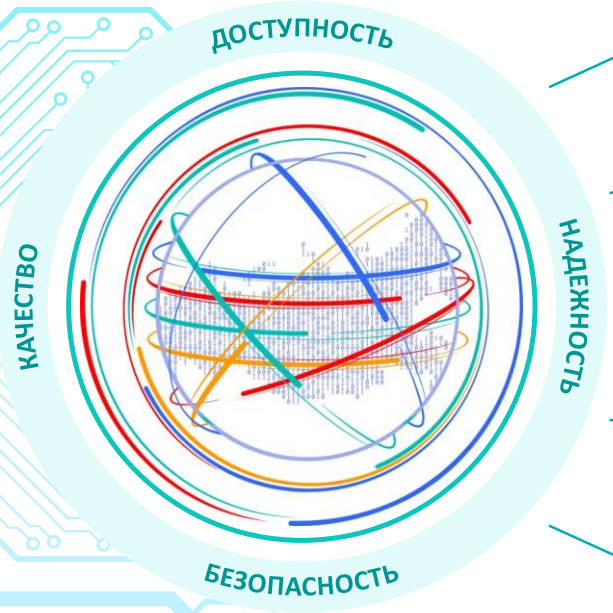
BIG DATA

БЛОКЧЕЙН

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ

МАШИННОЕ ОБУЧЕНИЕ

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ



ОТРАСЛЕВЫЕ СТАНДАРТЫ

ЕДИНОЕ ОКНО ЦИФРОВЫХ УСЛУГ

ЕДИНЫЙ РЕЕСТР ПРОСТРАНСТВЕННЫХ ДАННЫХ

КОНТРОЛЬ КАЧЕСТВА

СОЦИАЛЬНЫЕ СЕРВИСЫ

БЕЗОПАСНОСТЬ НА ТРАНСПОРТЕ

ЦИФРОВАЯ ПЛАТФОРМА МУЛЬТИМОДАЛЬНЫХ ПЕРЕВОЗОК
- ПРЕДВАРИТЕЛЬНОЕ ДЕКЛАРИРОВАНИЕ
- ВЕСОГАБАРИТНЫЙ КОНТРОЛЬ

МЕЖДУНАРОДНЫЙ ТРАНЗИТ
- БЕЗБУМАЖНЫЙ ДОКУМЕНТООБОРОТ
- ПРЕДВАРИТЕЛЬНОЕ ДЕКЛАРИРОВАНИЕ

ЦИФРОВАЯ ПЛАТФОРМА ТРАНСПОРТНОЙ БЕЗОПАСНОСТИ
- СЕРВИСЫ ТРАНСГРАНИЧНОЙ СЕТИ ДОВЕРИЯ
- ИНФОРМАЦИОННЫЕ СЕРВИСЫ

ТРАНСПОРТНАЯ ТЕЛЕМАТИКА
- УМНАЯ ДОРОГА
- МОНИТОРИНГ

ЦИФРОВАЯ ПЛАТФОРМА ПАССАЖИРСКИХ ПЕРЕВОЗОК
- УМНЫЙ МАРШРУТ
- ЭЛЕКТРОННОЕ БРОНИРОВАНИЕ

СУЩЕСТВУЮЩИЕ СИСТЕМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ НА СЕТЯХ LPWAN

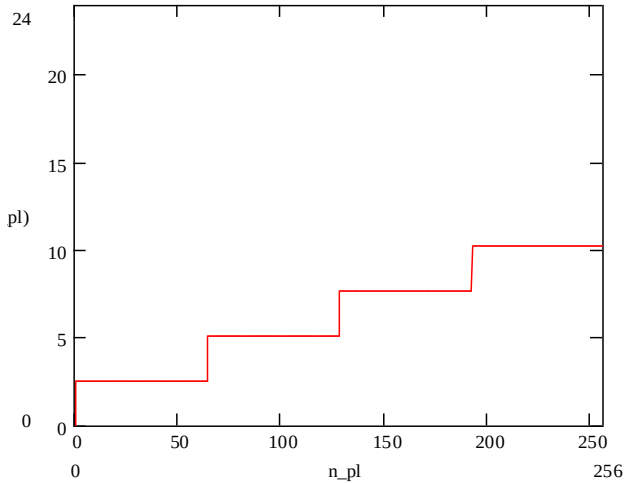
Стандартом де-факто в протоколах LPWAN (XNB, LoraWAN, NB-FI, SigFox, OpenUNB) является применение симметричного шифрования на основе протокола AES-128 на канальном уровне

В качестве альтернативы в протоколах, разрабатываемых в России, допускается использованием ГОСТ шифрования (Магма, Кузнечик)

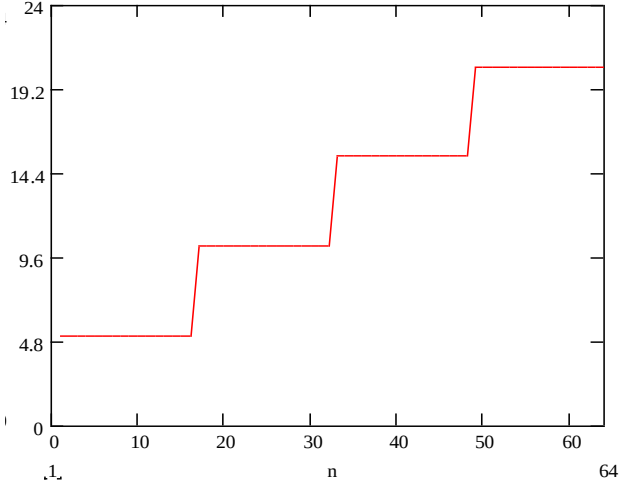
В протоколе LoraWAN допускается дополнительное кодирование протоколом Кузнечик на уровне приложений, при этом происходит дополнительное кодирование зашифрованного сообщения алгоритмом AES-128 (двойное шифрование на уровне приложений)

Оптимальный вариант защиты информации сетей LPWAN для критических приложений - «Протокол защищенного обмена для индустриальных систем» CRISP

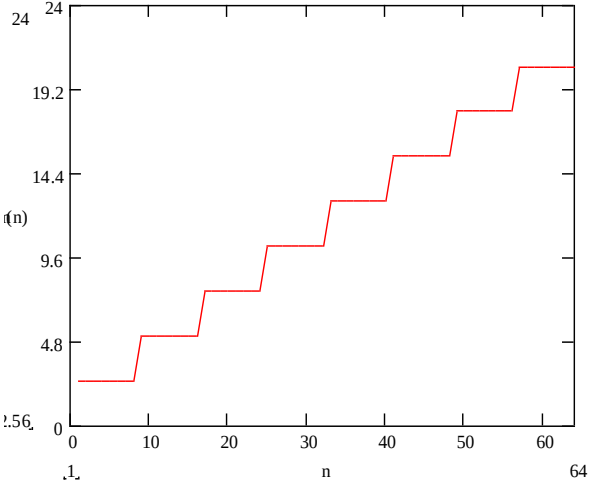
ЗАДЕРЖКИ ПРИ ПЕРЕДАЧЕ ИНФОРМАЦИИ НА СЕТЯХ LPWAN



Время передачи (сек) пакета полезной нагрузки длиной в битах при ширине канала 100 Гц без использования шифрования



Время передачи (сек) шифрованного пакета полезной нагрузки длиной в байтах при ширине канала 100 Гц с использованием криптоалгоритма AES-128 или «Кузнечик»



Время передачи (сек) шифрованного пакета полезной нагрузки длиной в байтах при ширине канала 100 Гц с использованием криптоалгоритма «Магма»

СИСТЕМА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ НА СЕТЯХ ПЕРЕДАЧИ ДАННЫХ ТРАНСПОРТНОЙ ТЕЛЕМАТИКИ В ТРАНСПОРТНОМ КОМПЛЕКСЕ РОССИИ

РЕЗУЛЬТАТЫ ВНЕДРЕНИЯ СИСТЕМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ

Уменьшение рисков нарушения функциональной безопасности систем, связанных с нарушением целостности данных

Сокращение времени разработки систем «Интернета вещей» на транспорте путём тиражирования типовых технических схем, решений и рекомендаций

Обеспечение однозначной аутентификация источников информации при использовании технологий LPWAN в транспортном комплексе Российской Федерации

Обеспечение устойчивости работы транспортного комплекса Российской Федерации при внедрении технологий «Интернета вещей»

СПАСИБО ЗА ВНИМАНИЕ!

МИНИСТЕРСТВО ТРАНСПОРТА
РОССИЙСКОЙ ФЕДЕРАЦИИ