«РАЗРАБОТКА СИСТЕМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ УЗКОПОЛОСНЫХ БЕСПРОВОДНЫХ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ ТРАНСПОРТНОЙ ТЕЛЕМАТИКИ

Министерство транспорта Российской Федерации
ФГУП «ЗащитаИнфоТранс»

ЦЕЛИ И ЗАДАЧИ, РЕШАЕМЫЕ НА ПЕРВОМ ЭТАПЕ НИОКР

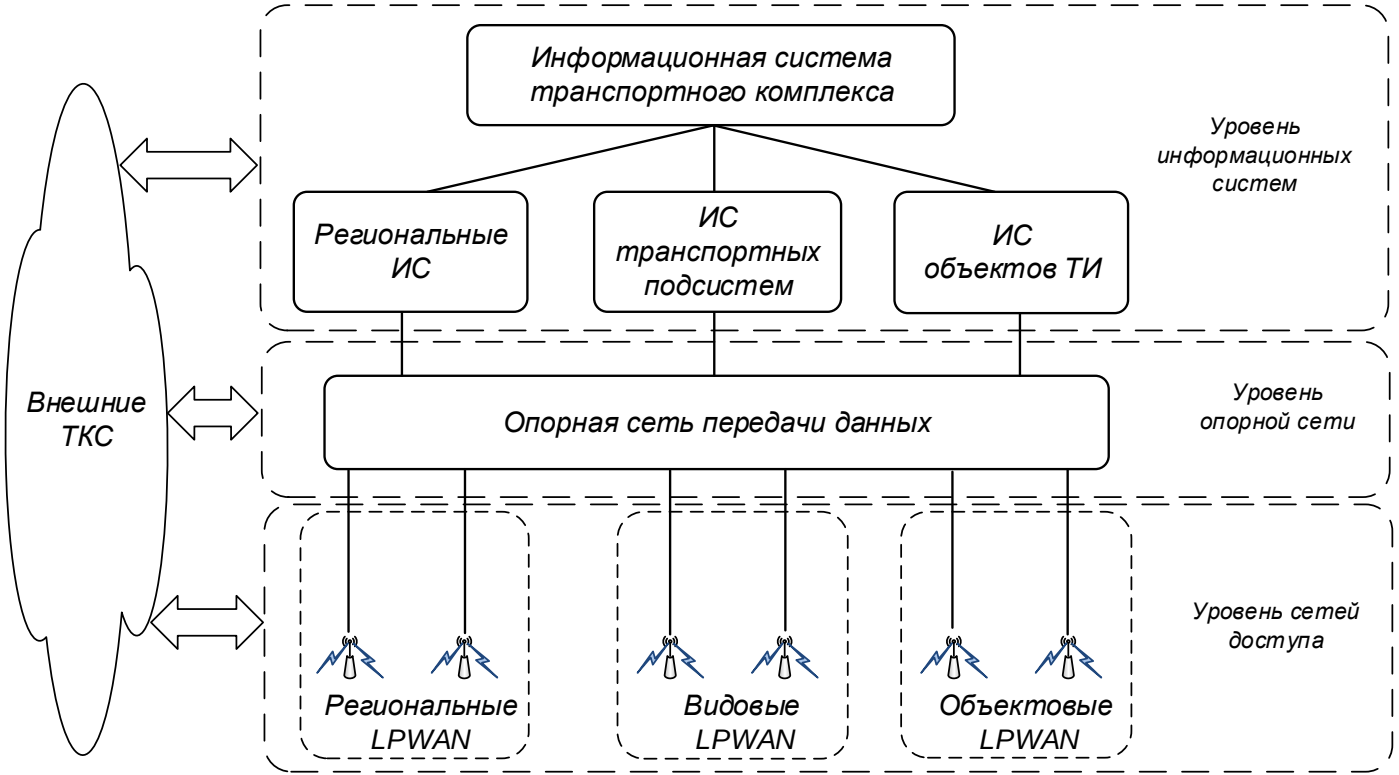
ЦЕЛЬЮ НИОКР ЯВЛЯЕТСЯ: РАЗРАБОТКА СИСТЕМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ УЗКОПОЛОСНЫХ БЕСПРОВОДНЫХ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ ТРАНСПОРТНОЙ ТЕЛЕМАТИКИ В ТРАНСПОРТНОМ КОМПЛЕКСЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

1 ЗАДАЧА	Разработка концептуальных подходов к созданию системы криптографической защиты беспроводных узкополосных сетей «Интернета вещей» в транспортной отрасли российской федерации с учетом решений, приведенных в Концепции построения и развития узкополосных беспроводных сетей связи «Интернета вещей» на территории Российской Федерации
2 ЗАДАЧА	Разработка технических требований к системе криптографической защиты беспроводных узкополосных сетей «Интернета вещей» в транспортной отрасли

СОДЕРЖАНИЕ РАБОТЫ В РАМКАХ ПЕРВОГО ЭТАПА

1. **Провести анализ**
   существующих систем криптографической защиты и нормативно-технических требований, касающихся описания методов и алгоритмов криптографической защиты данных
2. **Разработать предложения**
   по модификации протоколов в сетях LPWAN на основе технологии DOA
3. **Разработать концептуальные подходы**
   к созданию системы криптографической защиты узкополосных беспроводных сетей передачи данных транспортной телематики в Транспортном комплексе Российской Федерации
4. **Разработать технические требования к Системе**

СТРУКТУРА СЕТИ СВЯЗИ



АНАЛИЗ СУЩЕСТВУЮЩИХ СИСТЕМ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ И НОРМАТИВНО-ТЕХНИЧЕСКИХ ТРЕБОВАНИЙ

АНАЛИЗ СУЩЕСТВУЮЩИХ СИСТЕМ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ НА СЕТЯХ LPWAN ВЫЯВИЛ СЛЕДУЮЩЕЕ:

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)

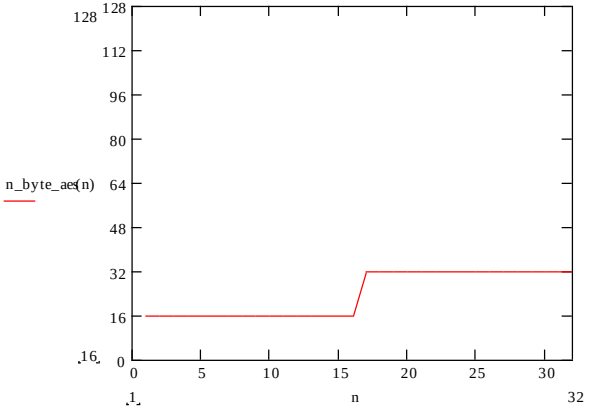
В протоколе LoraWAN допускается дополнительное кодирование протоколом Кузнечик на уровне приложений, при этом происходит дополнительное кодирование зашифрованного сообщения алгоритмом AES-128 (двойное шифрование на уровне приложений)

В качестве оптимального варианта защиты информации сетей LPWAN для критических приложений, целесообразно использовать «Протокол защищенного обмена для индустриальных систем» CRISP, разработанный компанией Инфотекс, который сейчас проходит согласование в качества стандарта

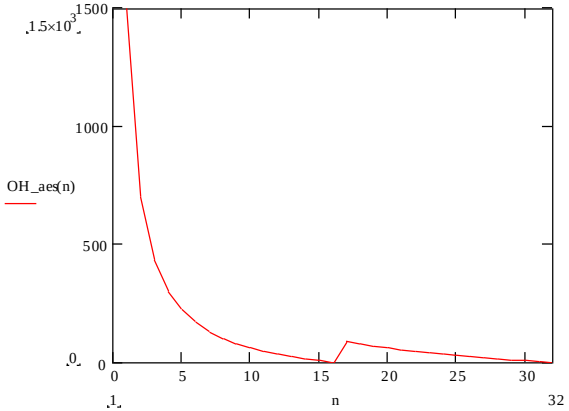
СРАВНИТЕЛЬНЫЙ АНАЛИЗ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ ПРИМЕНИТЕЛЬНО К СЕТЯМ LPWAN

Тип алгоритма шифрования	Размер блока шифрования	Длина ключа
«Кузнечик»	128 бит (16 байт)	256 бит
«Магма»	64 бит (8 байт)	256 бит
AES – 128	128 бит (16 байт)	256 бит

Оверхед определяется тем обстоятельством, что для работы криптографического алгоритма необходимо равенство длины блока данных с длиной блока шифра, при их неравенстве алгоритм заполняет блок нулями

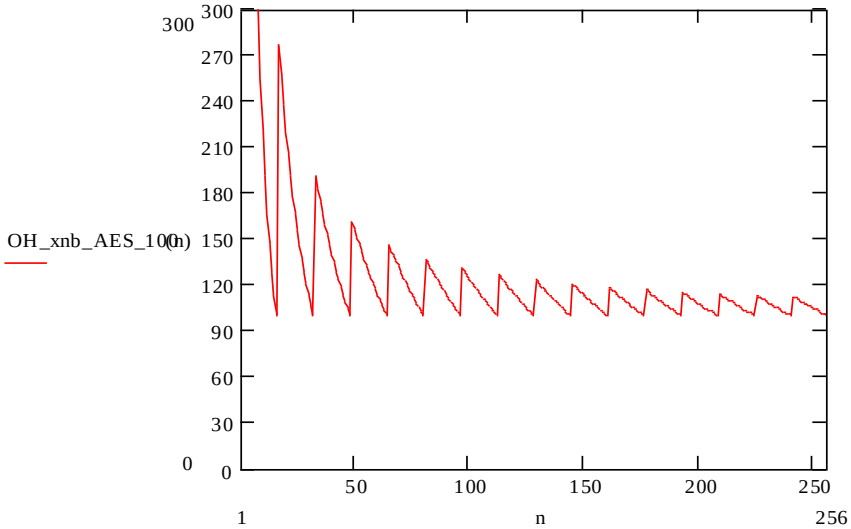


Число байт на выходе шифратора AES-128 в зависимости от числа байтов полезной нагрузки

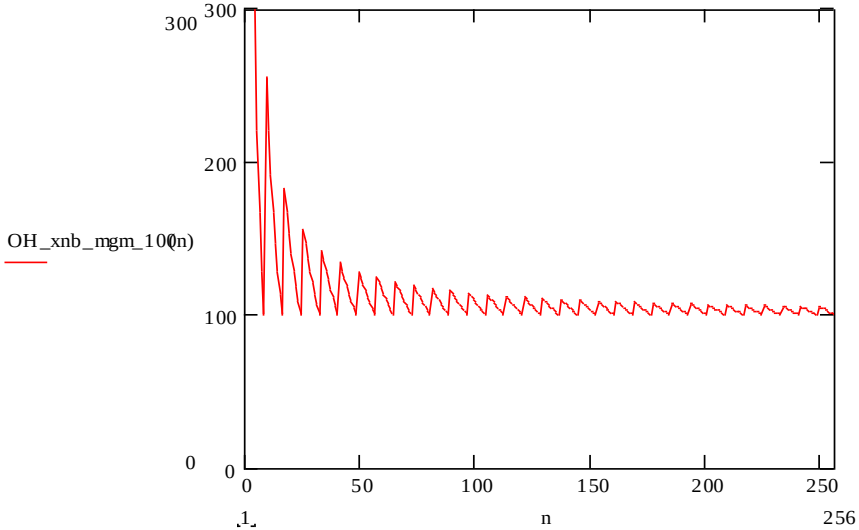


Оверхед (%) шифрования на выходе шифратора AES-128 в зависимости от числа байтов полезной нагрузки .

ОЦЕНКА СНИЖЕНИЯ ПРОПУСКНОЙ СПОСОБНОСТИ И УВЕЛИЧЕНИЯ ЗАДЕРЖЕК ПРИ ПЕРЕДАЧЕ ИНФОРМАЦИИ ПРИ ПРИМЕНЕНИИ СУЩЕСТВУЮЩИХ МЕТОДОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТЕХНОЛОГИИ XNB

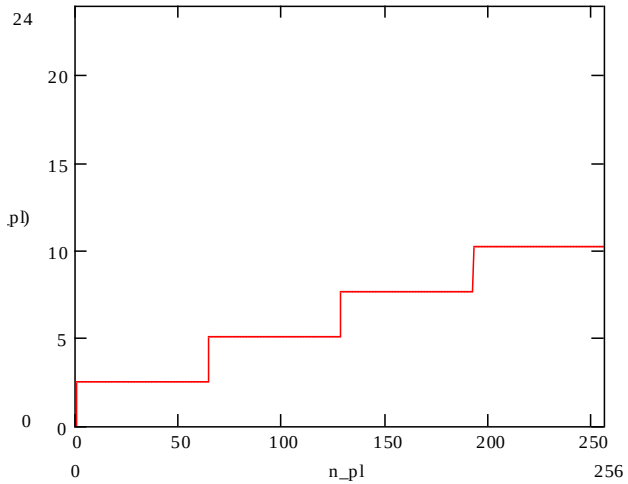


Суммарный оверхед MAC-уровня технологии XNB и шифрования выраженный в % при использовании алгоритмов AES-128 или «Кузнечик» в зависимости от длины передаваемого сообщения в байтах при полосе 100 Гц.

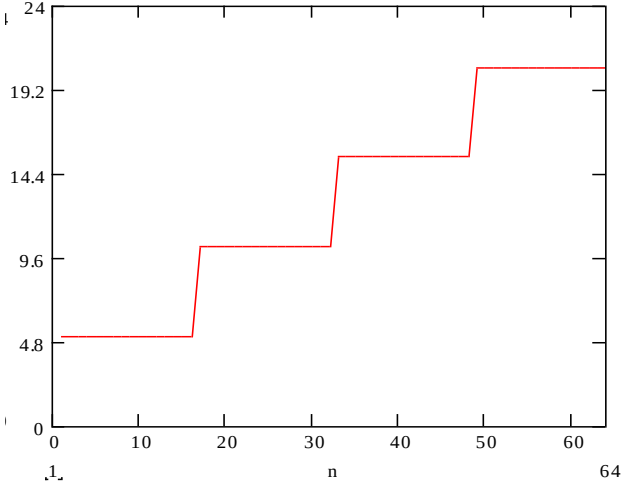


Суммарный оверхед MAC-уровня технологии XNB и шифрования выраженный в % при использовании алгоритма «Магма» в зависимости от длины передаваемого сообщения в байтах при полосе 100 Гц.

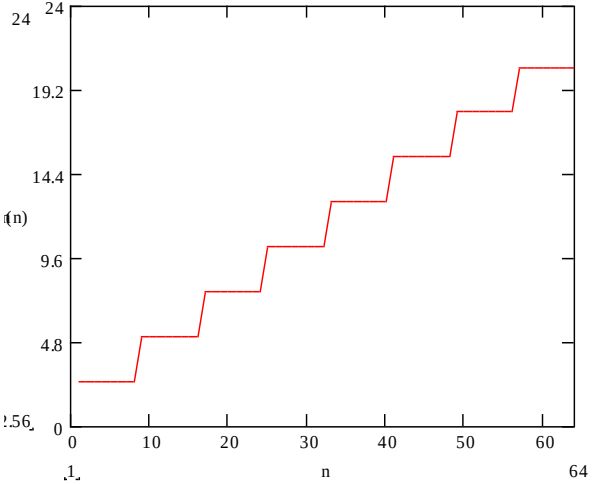
ОЦЕНКА СНИЖЕНИЯ ПРОПУСКНОЙ СПОСОБНОСТИ И УВЕЛИЧЕНИЯ ЗАДЕРЖЕК ПРИ ПЕРЕДАЧЕ ИНФОРМАЦИИ ПРИ ПРИМЕНЕНИИ СУЩЕСТВУЮЩИХ МЕТОДОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТЕХНОЛОГИИ XNB



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»

Криптографический протокол для M2M и IoT

Не всегда надежные каналы/ ограниченная пропускная способность

- без установления сессии -> предварительно распределенные ключи
- каждое сообщение несет всю необходимую информацию для обработки

Целостность и аутентичность важнее конфиденциальности

- обязательная имитозащита
- опциональное шифрование

Минимальный overhead

- адресация абонентов может быть неявная, через протоколы целевой системы
- все криптографические детали определяются номером криптографического набора
- в качестве синхропосылки используется номер сообщения

Минимальные задержки обработки

- только симметричные механизмы
- минимальный набор механизмов

КРИПТОГРАФИЧЕСКИЙ ПРОТОКОЛ CRISP

ОБЕСПЕЧЕНИЕ ИМИТОЗАЩИТЫ

ЗАЩИТА ДАННЫХ – БЛОЧНЫЙ ШИФР, ИМИТОВСТАВКА

ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ

МАЛЫЙ РАЗМЕР ВСПОМОГАТЕЛЬНЫХ ДАННЫХ

ЗАЩИТА ОТ НАВЯЗЫВАНИЯ ПОВТОРНЫХ СООБЩЕНИЙ

ПОДДЕРЖКА АДРЕСНЫХ (ОДИН К ОДНОМУ) СООБЩЕНИЙ

ОКНО ПРИНЯТЫХ СООБЩЕНИЙ

ПОДДЕРЖКА МНОГОАДРЕСНЫХ (ОДИН КО МНОГИМ) СООБЩЕНИЙ

У АБОНЕНТОВ ОБЩИЙ СЕКРЕТНЫЙ КЛЮЧ
(МОЖЕТ БЫТЬ ПОЛУЧЕН С ПОМОЩЬЮ ПРОТОКОЛОВ, ОСНОВАННЫХ НА PKI)

ПОДДЕРЖКА ЯВНОЙ И НЕЯВНОЙ АДРЕСАЦИИ АБОНЕНТОВ

НЕ ПРЕДНАЗНАЧЕН ДЛЯ ВСТРАИВАНИЯ В КАКОЙ-ЛИБО ОПРЕДЕЛЁННЫЙ ПРОТОКОЛ ПЕРЕДАЧИ ДАННЫХ

ПРЕДСТАВЛЯЕТ СОБОЙ СОВОКУПНОСТЬ НАБОРА ПОЛЕЙ, ПРАВИЛ ИХ ФОРМИРОВАНИЯ И ОБРАБОТКИ

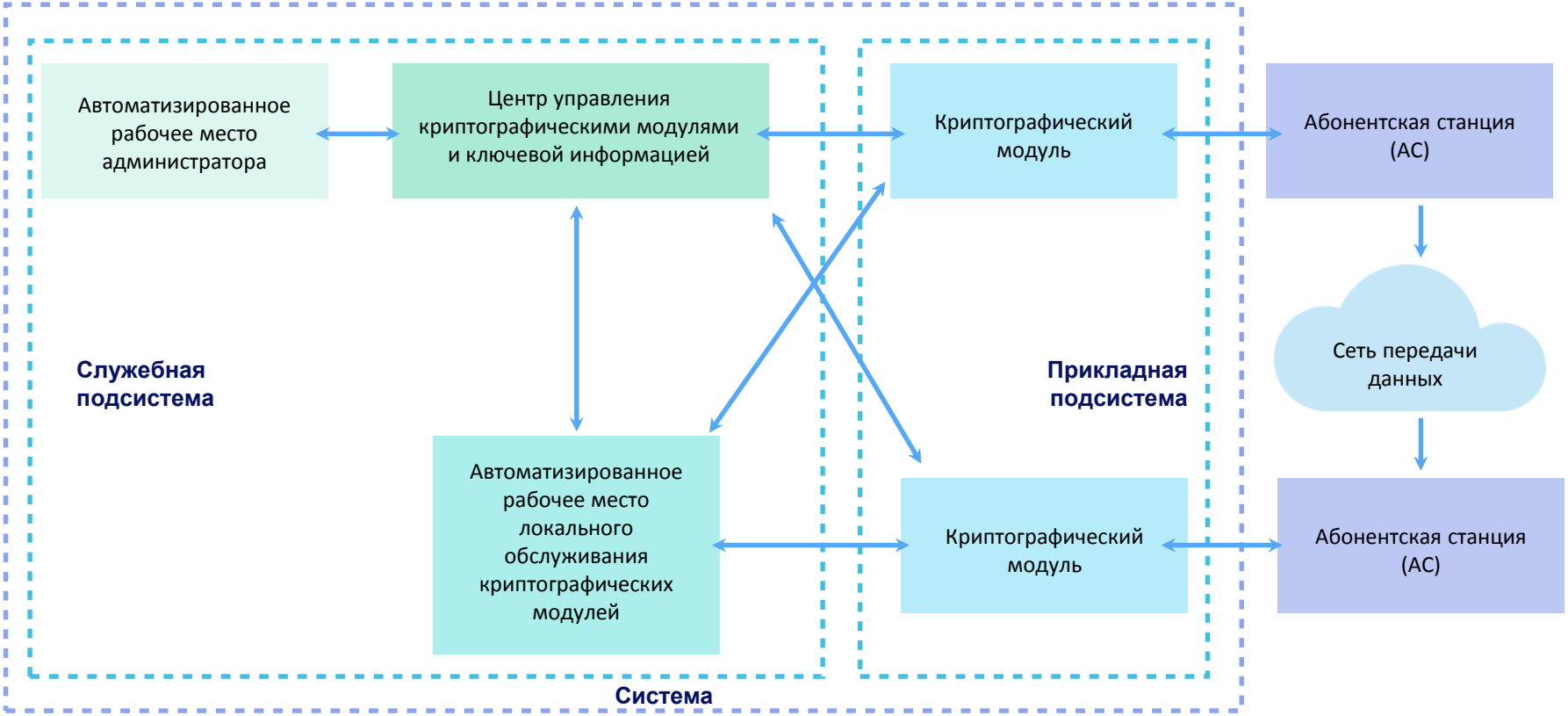
НА ЗАЩИЩАЕМУЮ СИСТЕМУ ВОЗЛАГАЕТСЯ ЗАДАЧА ДОСТАВКИ СФОРМИРОВАННЫХ ДАННЫХ ПОСРЕДСТВОМ ИСПОЛЬЗУЕМЫХ ПРОТОКОЛОВ. В ЧАСТНОСТИ, АДРЕСАЦИЯ И МАРШРУТИЗАЦИЯ ДАННЫХ ВОЗЛАГАЕТСЯ НА ЗАЩИЩАЕМУЮ СИСТЕМУ

ПРЕДЛОЖЕНИЯ ПО МОДИФИКАЦИИ ПРОТОКОЛОВ В СЕТЯХ LPWAN НА ОСНОВЕ ТЕХНОЛОГИИ DOA

В СООТВЕТСТВИИ С АРХИТЕКТУРОЙ ЕИТС, СИСТЕМА ИДЕНТИФИКАЦИИ ЦИФРОВЫХ ОБЪЕКТОВ НАХОДИТСЯ ВЫШЕ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

МОДИФИКАЦИИ ПРОТОКОЛОВ LPWAN НЕ ТРЕБУЕТСЯ

КОНЦЕПТУАЛЬНЫЕ ПОДХОДЫ К СОЗДАНИЮ СИСТЕМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ



ФУНКЦИОНАЛЬНАЯ СТРУКТУРА СИСТЕМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ УЗКОПОЛОСНЫХ БЕСПРОВОДНЫХ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ ТРАНСПОРТНОЙ ТЕЛЕМАТИКИ В ТРАНСПОРТНОМ КОМПЛЕКСЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Разработка технические требования к Системе

В рамках первого этапа НИОКР, в соответствии с техническим заданием, были разработаны технические требования к системе в составе:

- Назначение Системы
- Состав Системы
- Назначение, технические характеристики и основные функции Криптографического модуля, интегрированного с АС
- Назначение, технические характеристики и основные функции Криптографического модуля, интегрированного с СБД
- Назначение, технические характеристики и основные функции ключевого центра
- Назначение, технические характеристики и основные функции АРМ локального обслуживания

ЭФФЕКТ ОТ ВНЕДРЕНИЯ СИСТЕМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ

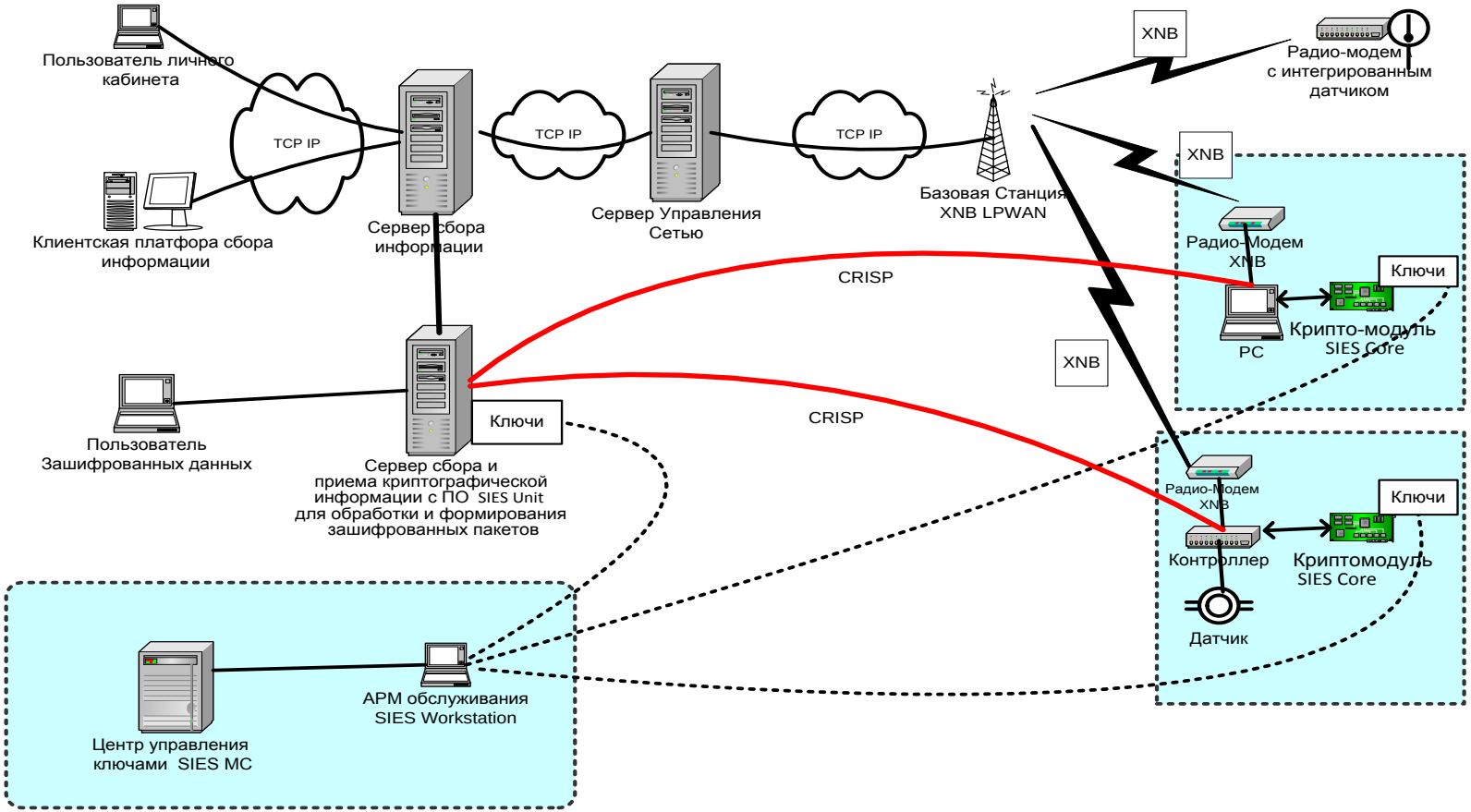
Уменьшение рисков нарушения функциональной безопасности систем, связанных с нарушением целостности данных

Сокращение времени разработки систем «Интернета вещей» на транспорте путём тиражирования типовых технических схем, решений и рекомендаций, разработанных в рамках данной работы

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

Применение результатов НИОКР позволит повысить устойчивость Транспортного комплекса Российской Федерации при внедрении технологий «Интернета вещей» при сборе, обработке и передаче телеметрической информации с транспортной инфраструктуры

ОПЫТНЫЙ ОБРАЗЕЦ СИСТЕМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ



БЛАГОДАРЮ ЗА ВНИМАНИЕ!

Министерство транспорта Российской Федерации
ФГУП «ЗащитаИнфоТранс»