Ежегодная международная научно-практическая конференция
«РусКрипто’2021»

Об уязвимостях протокола интернета вещей NB-Fi в новом проекте национального стандарта

Владислав Ноздрунов,
Эксперт, ТК 26

О протоколе NB-Fi

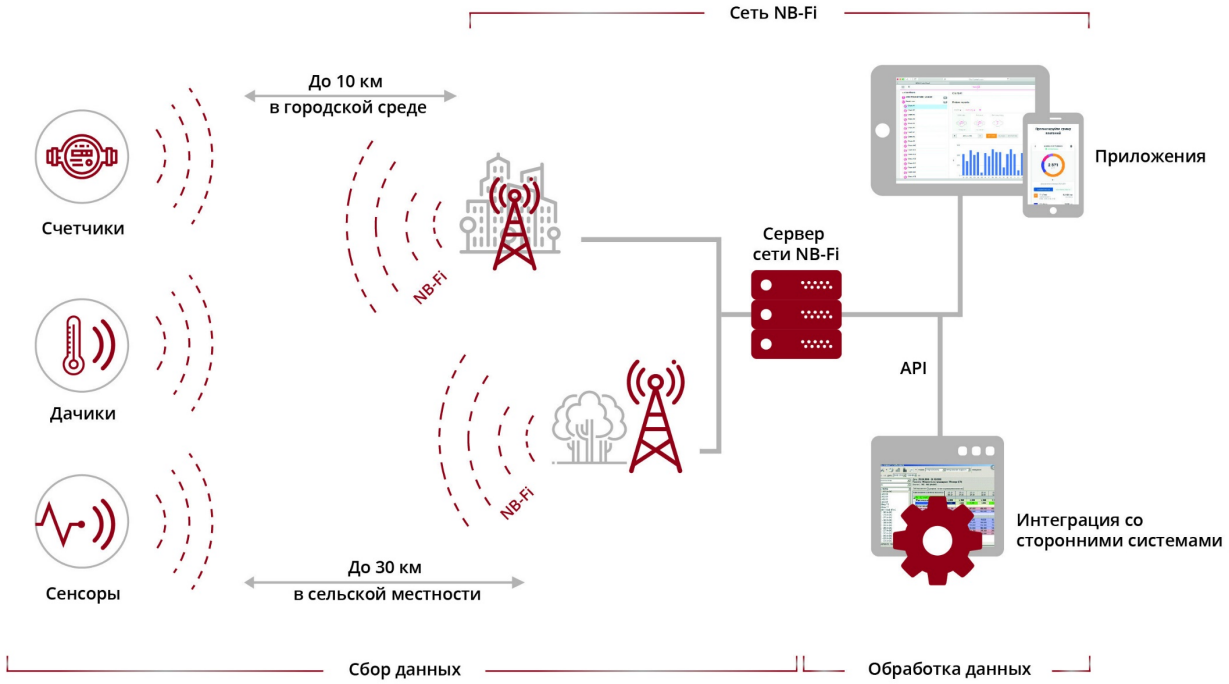
NB-Fi (Narrow Band Fidelity) – протокол беспроводной передачи данных на основе узкополосной модуляции.

Протокол разработан:

- компанией WAVIoT;
- АО «РВК»;
- Ассоциацией участников рынка интернета вещей.

О протоколе NB-Fi

Беспроводные решения для систем контроля и учета энергоресурсов



«Протокол беспроводной передачи данных NB-Fi для защищенного обмена данными между конечным устройством и сервером позволяет надежно обеспечить **конфиденциальность и целостность** передаваемой информации.»
©https://waviot.ru/

Немного истории

- Апрель 2018 г. – проект ПНСТ «Протокол беспроводной передачи данных на основе узкополосной модуляции радиосигнала (NB-Fi)».
- Май 2018 г. – атаки на протокол[1].
- Февраль 2019 г. – переработка и утверждение в качестве ПНСТ 354-2019.
- Март 2020 г. – криптоанализ[2] ПНСТ и рекомендации по модернизации.
- Декабрь 2020 г. – начало публичного обсуждения проекта ГОСТ для протокола NB-Fi.
- Март 2021 г. – «никогда такого не было и вот опять».

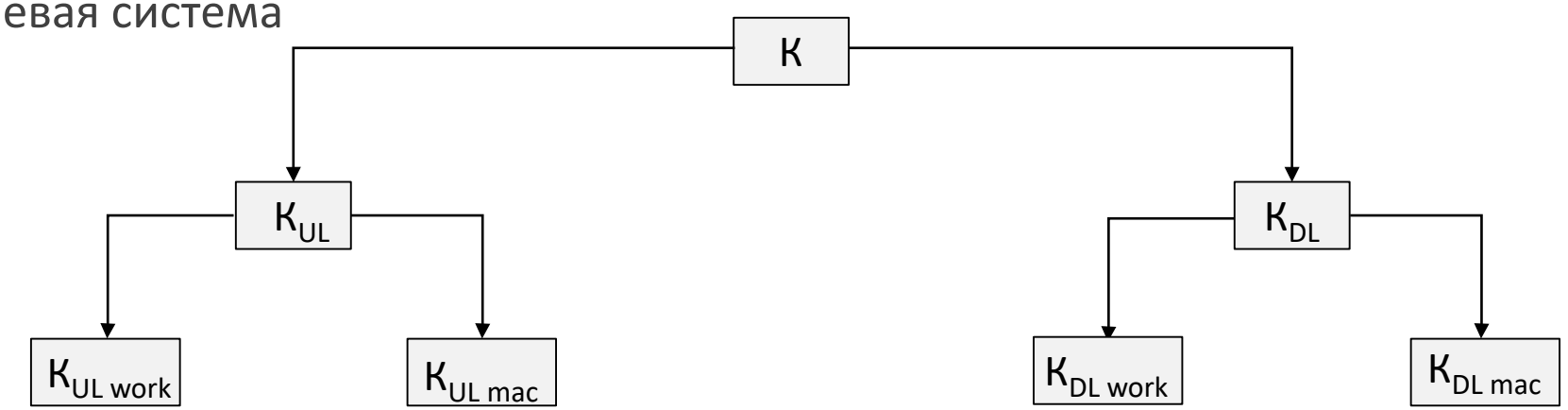
1. Nozdrunov V. About project of national standard "Protocol of IoT for the interchanging data in narrowband spectrum (NB-Fi)" (brief cryptanalysis). CTCrypt 2018.
2. Алексеев Е.К. Аспекты криптографической защиты протокола NB-Fi. Рускрипто 2020.

Стек протоколов NB-Fi

- физический уровень:
  - механизм приема-передачи произвольной информации по среде распространения;
  - требования к физ. характеристикам передаваемых пакетов;
- MAC-уровень:
  - формат полей пакетов;
  - способы адресации;
  - **методы защиты данных**;
  - **методы контроля целостности данных**;
- транспортный уровень
  - механизмы приема и передачи данных уровня приложения;
  - управляющие команды между устройством и сервером или устройством и устройством.

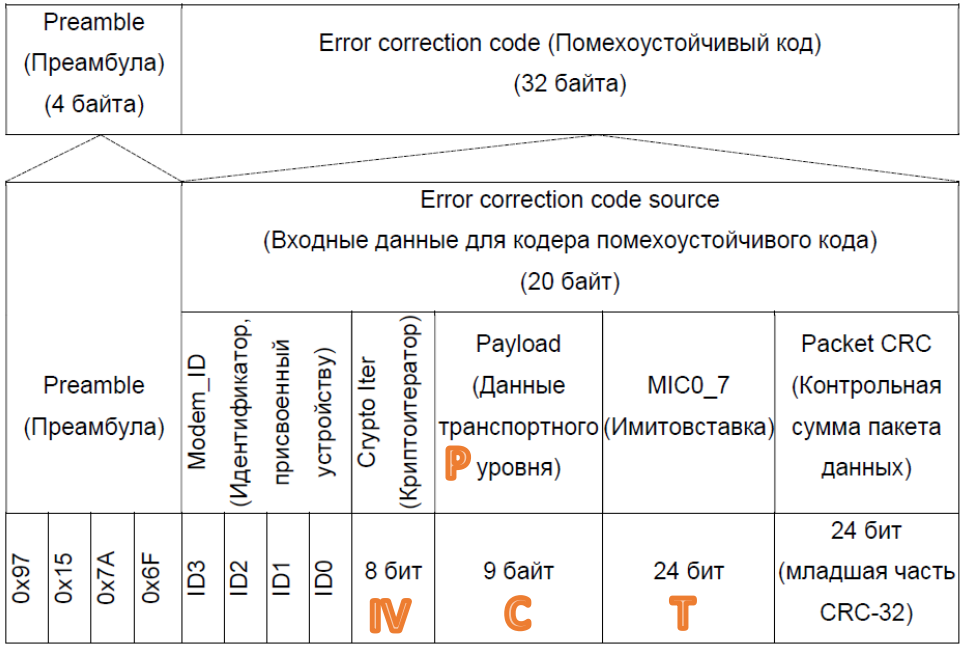
Криптография

- Примитив
  - «Магма» согласно ГОСТ Р. 34-12-2015.
- Режимы
  - шифрование CTR согласно ГОСТ Р. 34.13-2015;
  - выработка имитовставки согласно ГОСТ Р. 34.13-2015.
- Ключевая система



Структура пакетов MAC-уровня

UPLINK-пакет



- $C = CTR(K_{UL\,work}, IV, P)$,
  - где P – данные транспортного уровня.
- $T = OMAC(K_{UL\,mac}, C)$

DOWNLINK-пакет

Preamble (Преамбула)	Crypto Iter (Криптоитератор)	Payload (Данные транспортного уровня)	MIC0_7 (Имитовставка)	Определение ошибки и коррекция	
				Packet CRC (Контрольная сумма пакета данных)	Error correction code (Помехоустойчивый код)
32 бит	8 бит	9 байт	24 бит	24 бит (младшая часть CRC-32)	16 байт
	Error correction code source (Входные данные для кодера помехоустойчивого кода) (16 байт)				

- $C = CTR(K_{DL\,work}, IV, P)$,
  - где P – данные транспортного уровня.
- $T = OMAC(K_{\boldsymbol{DL}\,mac}, C)$

Нюансы

- CRC и помехоустройчивый код это не криптографические методы
  - Противник может корректно вычислять их значения для любых данных.
- Значение имитовставки зависит только от значения поля Payload
  - Противник может свободно изменять Преамбулу и Криптоитератор.
  - В новых пакетах противник может повторять предыдущую тройку (Криптоитератор, Payload, Имитовставка).
  - В новых пакетах противник может повторять пару (Payload, Имитовставка)[1].
- Некорретный алгоритм проверки имитовставки:
  - «в случае отрицательного результата проверки имитовставки на текущем комплекте ключей, необходимо циклически выполнять проверку имитовставки на последующих комплектах ключей до того момента, пока не будет достигнут положительный результат проверки имитовставки.»
  - Итог: случайное или намеренное искажение имитовставки ведет к бесконечному циклу и нарушению связи.

Навязывание

1. «За 50 долларов он вам вставляет проволочку. Электросчётчик крутится в совершенно противоположную сторону! Так что не вы платите электрокомпании, а ещё электрокомпания должна вам! Вот так!» © Х/ф «На Дерибасовской Хорошая Погода, или На Брайтон Бич Опять Идут Дожди»

Нюансы

В качестве размышления:

«Для работы в режиме «peer-to-peer» необходимо использовать конфигурационный флаг … При наличии данного флага, смену ключей при оборачивании криптоитератора выполнять не нужно. Таким образом, при работе в режиме «peer-to-peer», обеспечивается более низкий уровень криптозащиты данных, но упрощает реализацию механизма синхронизации значений криптоитераторов между узлами «peer-to-peer» соединения.»

- В режиме «peer-to-peer» возможно накопление объема материала для анализа.

«Присвоение корневых ключей устройствам должно выполняться при производстве оконечных устройств. Данные ключи должны быть «зашиты» в оконечные устройства и сохранены в базе данных сервера NB-Fi.»

- Каким образом оконечные устройства узнают ключи друг друга?

Вопросы

Контактная информация

Электронная почта:

Nozdrunov_vi@tc26.ru

Сайт:

www.tc26.ru