Ежегодная международная научно-практическая конференция
«РусКрипто’2020»

Вопросы криптографической защиты информации в интернете вещей и индустриальных системах

Д.В. Матюхин,
ФСБ России, заместитель председателя технического комитета по стандартизации ТК 26 «Криптографическая защита информации»

Особенности национальной ~~охоты~~ стандартизации интернета вещей

- Разработка стандартов осуществляется под эгидой *нескольких* технических комитетов (ТК 22, ТК 194, ТК 355, ТК 363, ПТК 706, …)
- Стандарты (проекты стандартов) предполагают использование криптографических механизмов, *не определяемых* документами (проектами документов) национальной системы стандартизации в области криптографической защиты информации (сфера компетенции ТК 26)
- Экспертиза проектов стандартов профильными ТК и ведомствами Росстандартом *не организована*, но осуществляется в инициативном порядке ТК 26 (нормативные документы ФСБ России предусматривают использование национальных стандартов в сертифицированных СКЗИ!)

Они попали в поле зрения ТК 26…

- ГОСТ Р 58603-2019 «Информационные технологии. Интернет вещей. Протокол организации очередей доставки телеметрических сообщений MQTT. Версия 3.1.1» на основе ISO/IEC 20922:2016 (ТК 22)
- Предварительный национальный стандарт ПНСТ 354-2019 «Информационные технологии. Интернет вещей. Протокол беспроводной передачи данных на основе узкополосной модуляции радиосигнала (NB-Fi)» (ТК 194)
- Проект ПНСТ «Информационные технологии. Интернет вещей. Протокол обмена для высокоемких сетей с большим радиусом действия и низким энергопотреблением» (LoRaWAN RU, ТК 194)
- Проект ПНСТ «Информационные технологии. Интернет вещей. Протокол беспроводной передачи данных для высокоёмких сетей на основе сверхузкополосной модуляции радиосигнала» (OpenUNB, ТК 194)

Они попали в поле зрения ТК 26…

- Проект ГОСТ Р ИСО/МЭК 27033–6 «Информационные технологии. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 6. Защищенный доступ к беспроводной IP-сети» (ТК 22)
- Проект ГОСТ Р «Требования к протоколам обмена информации между компонентами интеллектуальной системы учета и приборами учета» (ПТК 706)
- Проект ГОСТ Р «Информационные технологии. Стандарт информационных сервисов EPC (EPCIS)» (Electronic Product Code Information Services) на основе ISO/IEC 19987:2017 (ТК 355)
- Проект ГОСТ Р «Глобальная навигационная спутниковая система на транспорте. Технические средства контроля на транспорте. Единый расширяемый набор протоколов обмена данными технических средств контроля с информационными системами» (EGTS, ТК 363)

Криптография в некриптографических стандартах: позиция ТК 26

- Везде, где это возможно, использовать криптографические механизмы, определяемые документами (проектами документов) национальной системы стандартизации в области криптографической защиты информации или методическими документами ТК 26
- Опции в случае невозможности такого использования (отсутствует механизм с требуемыми функциональными или эксплуатационными свойствами):
  - Инициировать в ТК 26 разработку и стандартизацию соответствующего механизма
  - Согласовать с ТК 26 собственную разработку, представив её в соответствии с установленным в ТК 26 «Порядком оформления документов…» (включая обоснование!)
  - Исключить из проекта стандарта упоминание конкретных криптографических механизмов и обеспечиваемых ими свойств безопасности

Экспертиза ГОСТ Р 58603-2019 (MQTT v3.1.1)

- Дата введения в действие 01.01.2021
- Цитата из стандарта: «**Приложение А (рекомендуемое). Безопасность** … **А.2 Решения MQTT: безопасность и сертификация** … Реализация может потребовать соответствия определённым отраслевым стандартам безопасности, таким как NIST Cyber Security Framework, PCI-DSS, FIPS 140-2 и NSA Suite B. … **А.3 Упрощённая криптография и ограниченные устройства.** Широко применяется Улучшенный стандарт шифрования (AES) и Стандарт шифрования данных (DES).»
- Авторы искренне убеждены в полном отсутствии российских аналогов или они писали национальный стандарт другой страны?
- Считаем, что в принятом виде стандарт должен быть отменён

Экспертиза проекта ПНСТ 354-2019 (NB-Fi)

- Предложенный протокол предполагал использование блочного шифра XTEA-2, публикации о криптографических исследованиях которого отсутствуют
- Предложенный протокол не обеспечивает заявленных свойств безопасности, но использование в качестве блочного шифра ГОСТ Р 34.12-2015 «Магма» улучшает его криптографические и эксплуатационные свойства [Ноздрунов, CTCrypt 2018]
- В окончательной редакции проекта XTEA-2 заменён на ГОСТ Р 34.12-2015 «Магма» и исключено упоминание конкретных свойств безопасности протокола
- ПНСТ введён в действие 01.04.2019 на срок 3 года
- Подробнее о протоколе – на секции «Криптография в энергетическом секторе»

Экспертиза проекта ПНСТ LoRaWAN RU

- Первая редакция предполагала одновременное использование ГОСТ и AES, во второй редакции упоминание AES исключено
- И в первой, и во второй редакции заявлено, что протокол «предусматривает симметричное шифрование для обеспечения безопасной передачи данных», т.е. заведомо позиционируется авторами как криптографический, однако модель нарушителя, формулировки требуемых свойств безопасности и их обоснование в выбранной модели нарушителя не опубликованы
- Мнение экспертов ТК 26 о второй редакции проекта направлено в ТК 194 в конце января 2020 года, ждём согласительного совещания
- Подробнее о результатах экспертизы – в докладе эксперта ТК 26 на секции «Криптография в энергетическом секторе»

Экспертиза проекта ПНСТ OpenUNB

- В первой редакции заявлено: «Для обеспечения безопасности пользовательских данных протокол гармонизирован с отечественными алгоритмами шифрования – ГОСТ Р 34.12–2015» (т.е. протокол заведомо позиционируется авторами как криптографический), при этом
  - также допускается использование AES
  - отсутствует описание механизмов управления ключами или ссылка на такое описание
  - модель нарушителя, формулировки требуемых свойств безопасности протокола и их обоснование в выбранной модели нарушителя не опубликованы
- Отрицательный отзыв ТК 26 на первую редакцию проекта дан в октябре 2019 года, тогда же закончилось публичное обсуждение, сводка отзывов и окончательная редакция до сих пор не опубликованы

Экспертиза проекта ГОСТ Р ИСО/МЭК 27033–6

- Попытка принять международный стандарт с криптографией в качестве национального методом некачественного перевода с английского языка
- В проекте в качестве допустимых, рекомендуемых и даже обязательных к использованию упоминается большое число криптографических механизмов, не определяемых документами (проектами документов) национальной системы стандартизации в области криптографической защиты информации, хотя, как заявлено во Введении к проекту, в задачи стандарта входит лишь «определение конкретных рисков, методов проектирования и мер контроля для обеспечения безопасности беспроводных IP-сетей»
- Отрицательный отзыв ТК 26 на первую редакцию проекта дан в конце января 2020 года, сводка отзывов и окончательная редакция пока не опубликованы

Экспертиза проекта ГОСТ Р по СПОДЭС

- Проект разработан с учётом положений стандарта IEC 62056 (DLMS/COSEM)
- В соответствии с первой редакцией проекта требования к рассматриваемым протоколам в части криптографической защиты информации заключались в применении документов национальной системы стандартизации США (при наличии российских аналогов, включая методические рекомендации ТК 26 МР 26.4.003-2019 «Информационная технология. Криптографическая защита информации. Использование российских криптографических механизмов для реализации обмена данными по протоколу DLMS»)
- Отрицательное заключение ТК 26 на проект дано в декабре 2019 года
- В новой редакции требования по криптографической защите информации заменены ссылкой на МР 26.4.003-2019, заключение ТК 26 положительное
- Больше по теме – на секции «Криптография в энергетическом секторе»

Экспертиза проекта ГОСТ Р по EPC (EPCIS)

- Используется обмен данными по HTTP в соответствии с RFC 4130 («протокол AS2») или с использованием протокола TLS
- Модификация стандарта ISO, как и в рассмотренном выше случае с ГОСТ Р 58603-2019, не затронула криптографию, однако до принятия стандарта в таком виде дело, к счастью, не дошло
- Отрицательное заключение ТК 26 на проект дано в декабре 2019 года
- В течение января-марта 2020 года ТК 355 во взаимодействии с ТК 26 осуществлена доработка проекта, результатом которой стало появление в окончательной редакции требований соответствия криптографической защиты информации при применении протоколов AS2 и TLS документам национальной системы стандартизации Российской Федерации в области криптографической защиты информации.

Экспертиза проекта ГОСТ Р по EGTS

- Единственный из рассмотренных (проектов) стандартов, с первой редакции претендующий на использование исключительно отечественной стандартизированной криптографии (включая выведенный из действия ГОСТ 28147-89 ☺)
- Предварительный анализ проекта показывает, что
  - в ряде протоколов ключ симметричного шифрования передаётся в открытом виде
  - описание использования криптографических механизмов в рассматриваемых протоколах является неполным, в частности, не указаны конкретные режимы шифрования
- В настоящее время осуществляется подготовка заключения ТК 26

Благодарности

- Экспертам ТК 26 А.И. Бондаренко, Г.Б. Маршалко, А.Ю. Нестеренко, В.И. Ноздрунову, М.Б. Пискунову, А.М. Семёнову, С.В. Смышляеву, О.В. Шемякиной, работа которых отражена в данном докладе
- Участникам Рускрипто 2020 за внимание