Ежегодная международная научно-практическая конференция
«РусКрипто’2021»

Особенности внедрения СКЗИ в РТК с БпЛА МД

Поликарпов Александр,
Начальник отдела разработки СКЗИ, ООО «СТЦ»

Задачи, решаемые РТК с БпЛА МД

- Мониторинг природных и антропогенных объектов
- Наблюдение за объектами критически важной инфраструктуры
- Геологоразведочные работы
- Ретрансляция данных посредством БпЛА между удаленными абонентами
- Наблюдение за морскими экономическими зонами и территориальными водами

Комплексы малой дальности, предназначены для применения на расстоянии до 100 км, т.е. в пределах границ прямой радиовидимости с использованием дистанционно пилотируемого воздушного судна с взлетной массой менее 30 кг.

Уязвимость радиоканала РТК с БпЛА МД

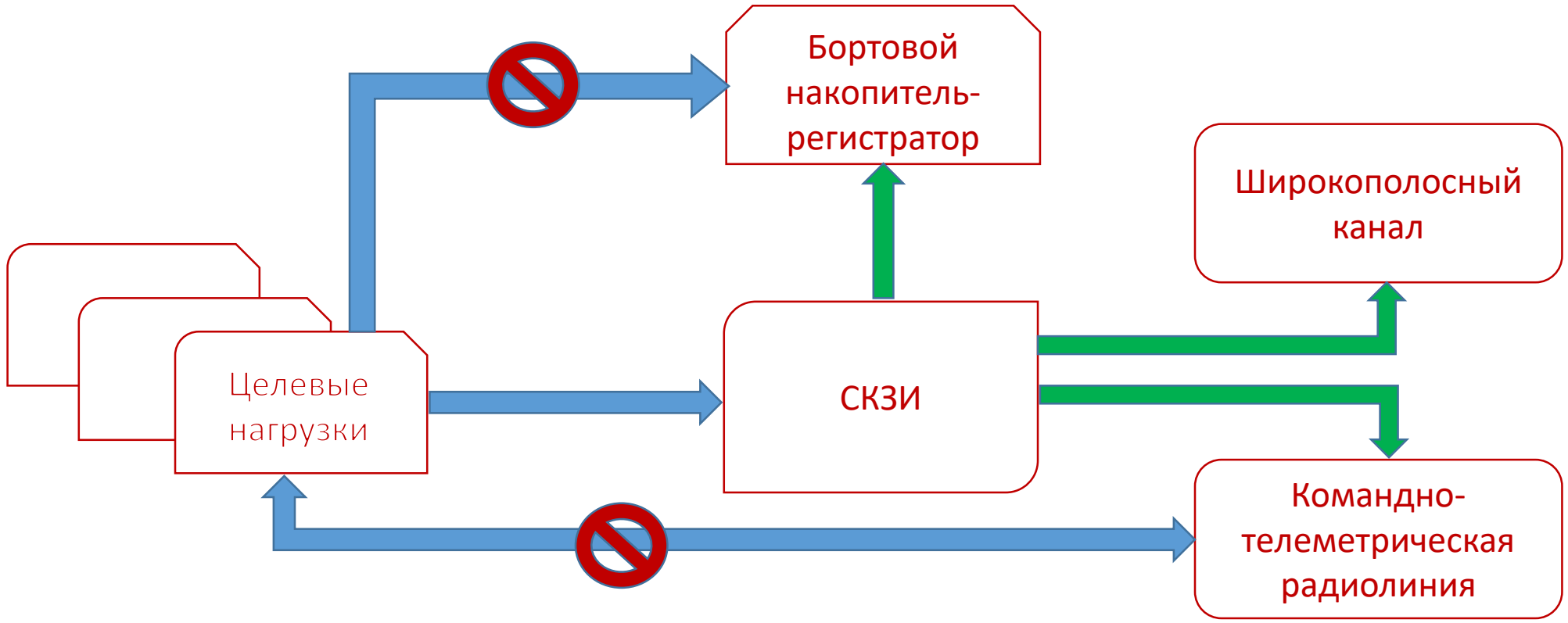
- Для управления БпЛА и доставки информации целевых нагрузок требуются каналы связи высокой пропускной способности с малой задержкой по времени доставки информации
- Помехи и искажения в радиоканале снижают скорость пересылки полезных данных вплоть до нуля
- Любые сигналы, принимаемые и отсылаемые БпЛА, можно искажать, перехватывать и подменять

Инструкции для военного дрона похитили из-за дефолтного пароля для FTP

Проблемные вопросы внедрения СКЗИ в БпЛА МД

- Информационно-техническое взаимодействие БРЭО не позволяет обеспечить встраивание дополнительных элементов а так же вносить «избыточность» в передаваемую информацию
- Малые мощности вычислительных ресурсов, удовлетворяющих требованиям по массо-габаритным и энергетическим характеристикам, для размещения на БпЛА
- Повышенный риск потери БпЛА и компрометации СКЗИ
- Жесткие требования по устойчивости к внешним воздействующим факторам

«Модульный принцип» построения тракта передачи информации



Протоколы информационно-логического взаимодействия

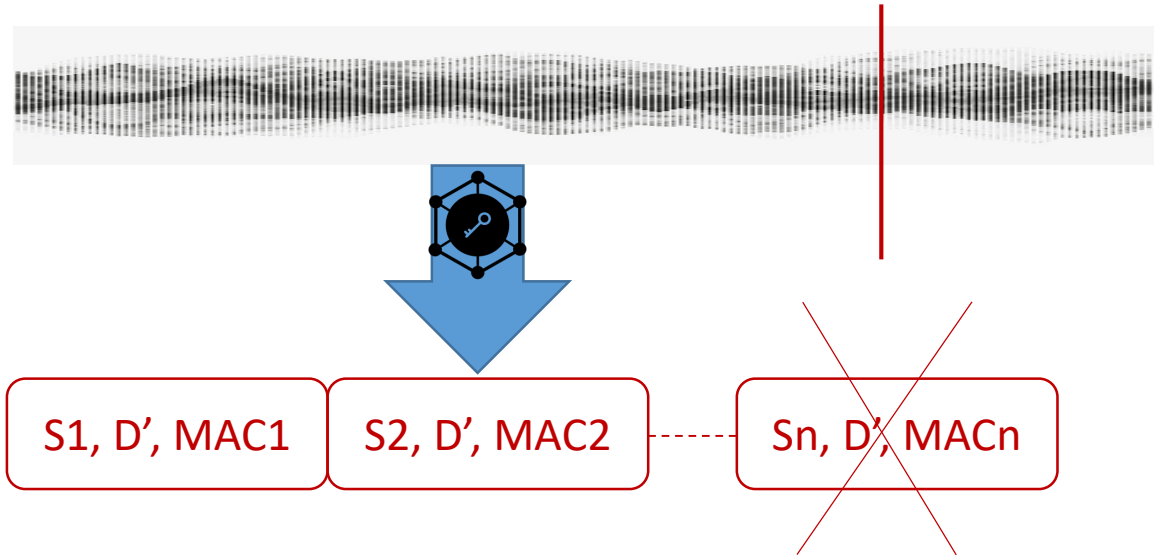
Широкополосный канал передачи данных целевых нагрузок (TCP, UDP)

Трансляция данных от целевых нагрузок как адресно, так и одновременно нескольким получателям

Р 1323565.1.025-2019: Форматы сообщений, защищенных криптографическими методами – CMS
Р 1323565.1.034-2020: Протокол безопасности сетевого уровня, IPlir (транспортный режим)

Непрерывное использование широкополосного канала значительно ухудшает летные характеристики БпЛА

Командно-телеметрическая радиолиния (потоковая передача данных)



Для обеспечения целостности и подлинности информации, необходимо динамическое изменение размера пакета формируемого СКЗИ, в зависимости от качества канала передачи

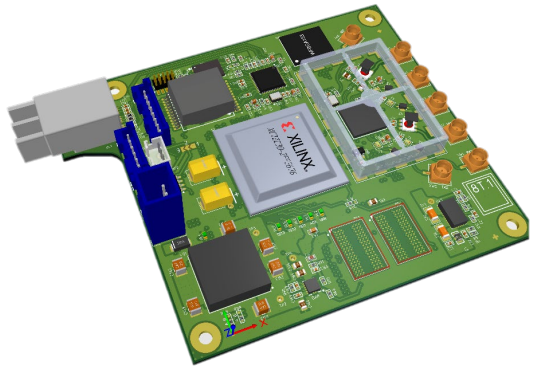
Управление ключами и ключевое распределение

- Необходимо учитывать обеспечение мер защиты ключевой информации, связанной с условиями повышенной компрометации и возможной потери БпЛА
- Применение мер защиты исключительно в рамках СКЗИ неизбежно ведет к росту его массо-габаритных характеристик
- Использование протоколов «открытого распределения» ключевой информации позволит упростить конструктивное встраивание СКЗИ в БпЛА МД

Физический интерфейс взаимодействия

- Требуется высокая пропускная способность и помехоустойчивость канала доставки информации
- Волоконная оптика обеспечивает необходимую скорость, устойчива к электромагнитным и радиочастотным помехам, что делает её идеальным решением для сопряжения СКЗИ с БРЭО

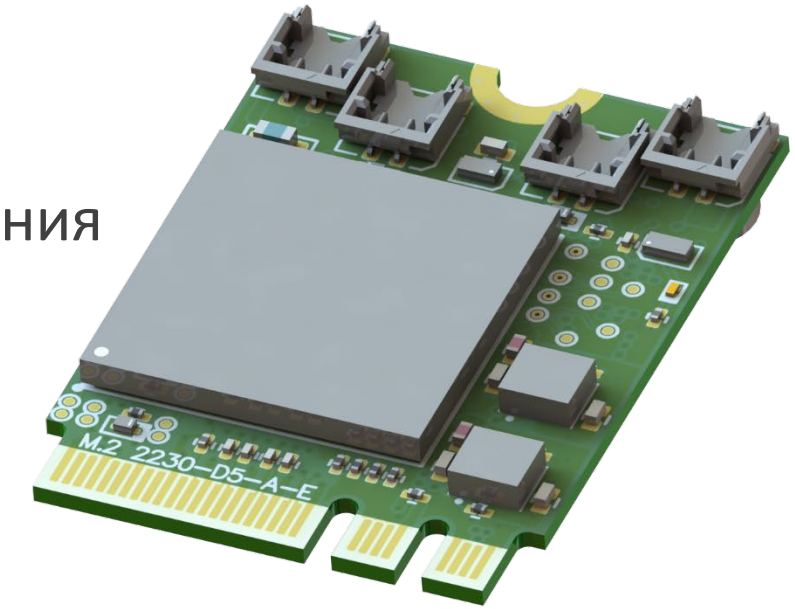
Современные решения для оптоволоконных линий имеют компактные размеры и соответствуют требованиям стойкости к внешним воздействующим факторам для применения на БпЛА МД



Использование «низкоресурсной» криптографии

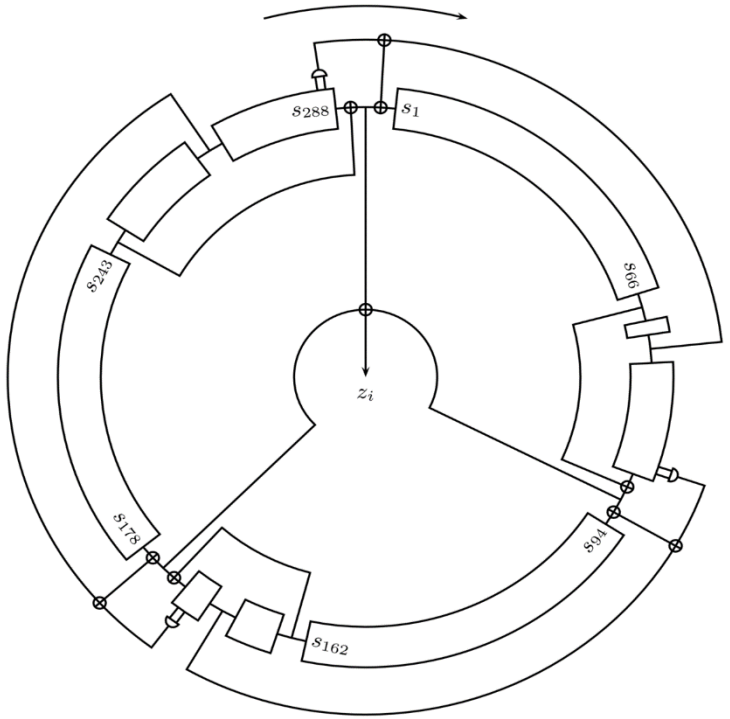
«As light as a feather, and as hard as dragon-scales»

- Меньшая вычислительная мощность
- Малый объем используемой памяти
- Необходимость снижения энергопотребления
- Жесткие требования по массе
- Снижение стоимости



TRIVIUM

- 2^{64} бит шифртекста, 80 бит К, 80 бит IV
- ISO/IEC 29192-3
- Стойкость к атаке перебором 2^{120}



- СКЗИ применяемые для защиты информации радиоканалов БЛА МД должны интегрироваться в БРЭО, приоритетом является снижение массы, габаритов и энергопотребления
- Унификация протоколов информационного взаимодействия и физических интерфейсов позволит применять единый тип СКЗИ на различных типах БпЛА
- Требуется разработка единой модели угроз для РТК с БпЛА

Вопросы

Контактная информация

Электронная почта:

apolikarpov@stc-spb.ru

Телефон:

+7 911 715-85-37