

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 исказить, перехватывать и подменять



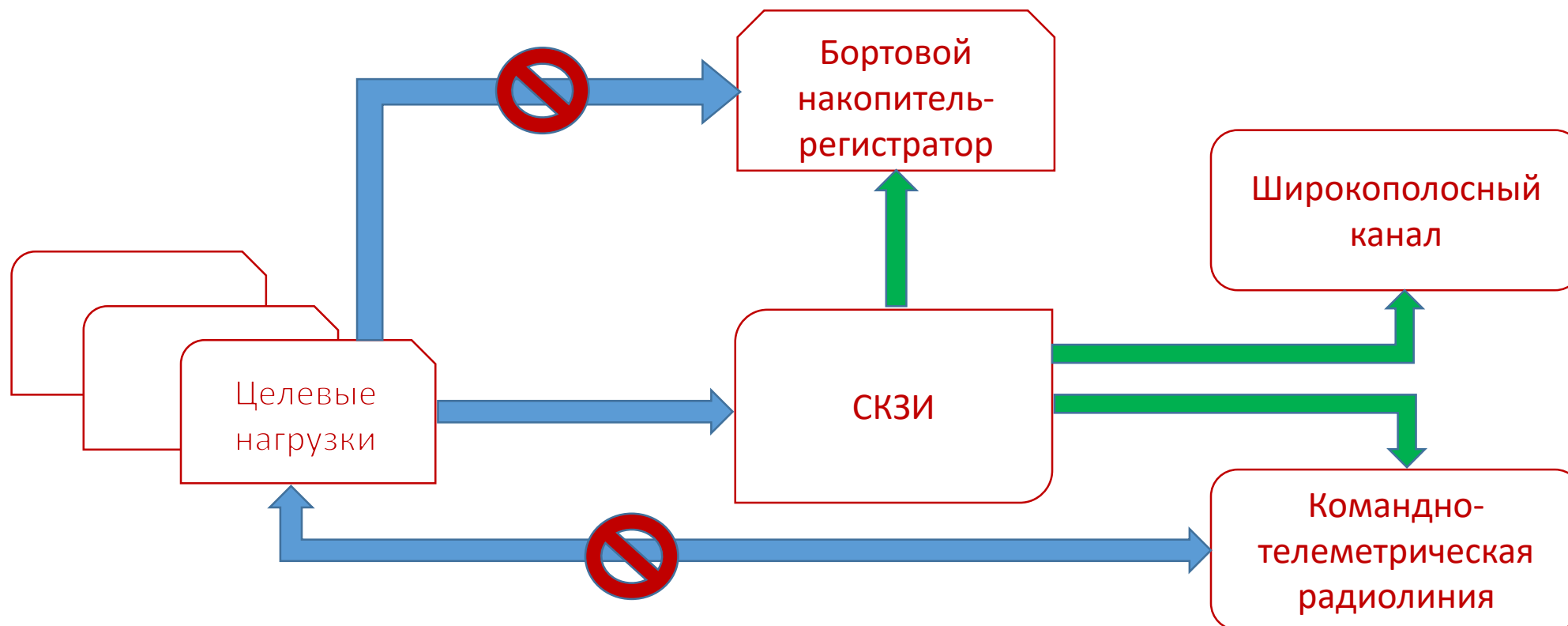
Инструкции для военного дрона похитили из-за дефолтного пароля для FTP

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

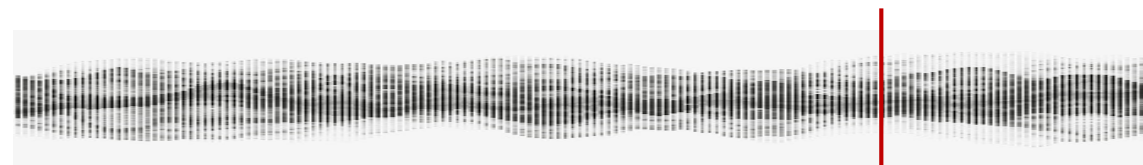
Р 1323565.1.034-2020: Протокол безопасности сетевого уровня, IPlir (транспортный режим)

Непрерывное использование широкополосного канала значительно ухудшает летные характеристики



БпЛА

Командно-телеметрическая радиолиния
(потокковая передача данных)



S1, D', MAC1

S2, D', MAC2

~~Sn, D', MACn~~

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

Управление ключами и ключевое распределение

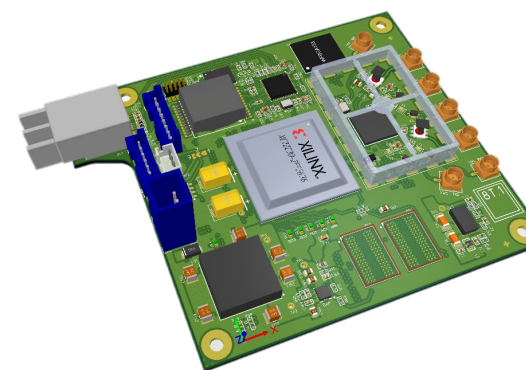
- Необходимо учитывать обеспечение мер защиты ключевой информации, связанной с условиями повышенной компрометации и возможной потери БпЛА
- Применение мер защиты исключительно в рамках СКЗИ неизбежно ведет к росту его массо-габаритных характеристик
- Использование протоколов «открытого распределения»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

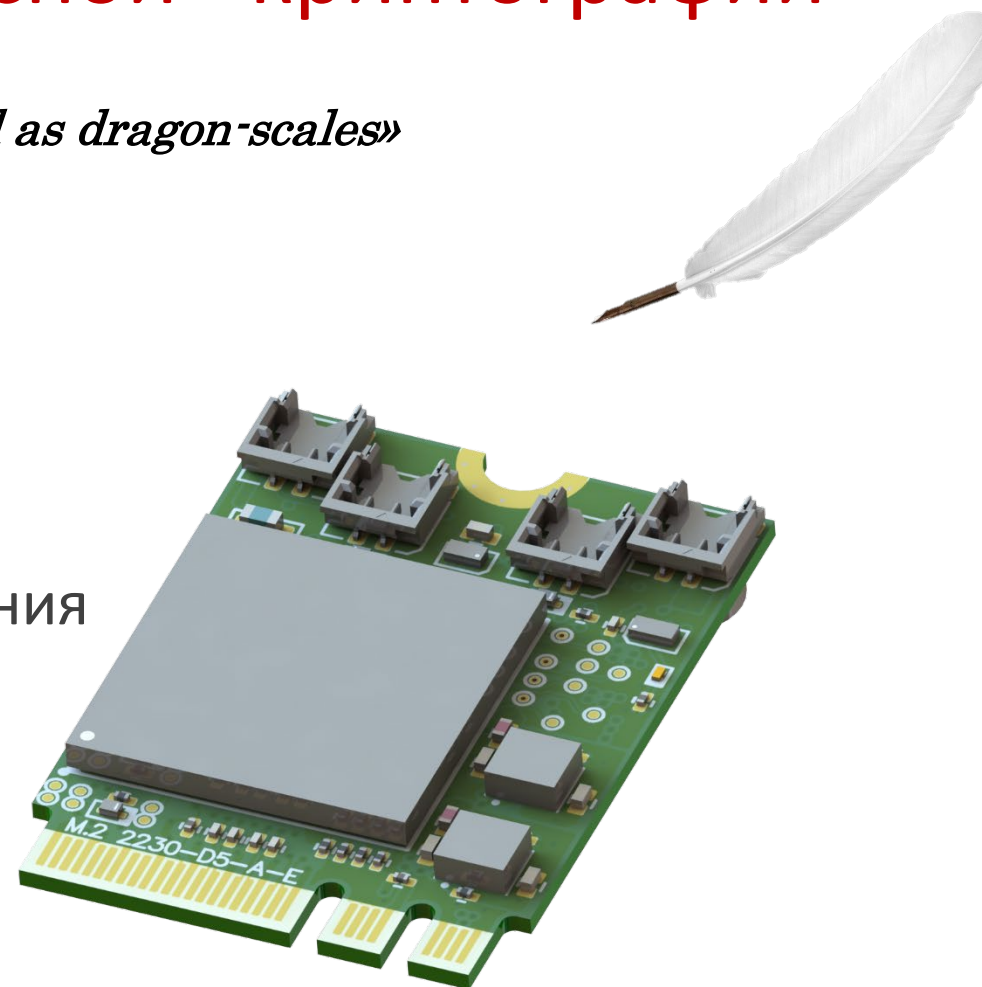
Современные решения для оптоволоконных линий имеют компактные размеры и соответствуют требованиям стойкости к внешним воздействующим факторам для применения на БЛА МД



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



The screenshot displays a simulation environment with a timing diagram at the top and source code at the bottom. The timing diagram shows signals like `dat_o[31:0]` and `key_r[95:0]` over time. The source code shows a Verilog module `trivium_top.v` with parameters and module instantiations.

Timing Diagram Data:

Name	Value
<code>n_rst_i</code>	1
<code>dat_i[31:0]</code>	22e93af1
<code>ld_dat_i[31:0]</code>	0000b3b
<code>ld_reg_a_i[2:0]</code>	0
<code>ld_reg_b_i[2:0]</code>	0
<code>init_i</code>	0
<code>proc_i</code>	1
<code>clk_i</code>	1
<code>dat_o[31:0]</code>	ba3a66eb
<code>busy_o</code>	0
<code>start_tests_s</code>	1
<code>key_r[95:0]</code>	00007d6dbeca598b193
<code>iv_r[95:0]</code>	00000b3bd8156cf69568

Source Code Snippets:

```

49 //////////////////////////////////////////////////
50 // Local parameter definitions
51 //////////////////////////////////////////////////
52 parameter
53     IDLE_e = 0,
54     WARMUP_e = 1,
55     WAIT_FROC_e = 2,
56     FROC_e = 3;
57 //////////////////////////////////////////////////
58 //////////////////////////////////////////////////
59 // Module instantiations
60 //////////////////////////////////////////////////
61 cipher_engine cphr(
62     .clk_i(clk_i),
63     .n_rst_i(n_rst_i),
64     .ce_i(cphr_en_r),
65     .ld_dat_i(ld_dat_i),

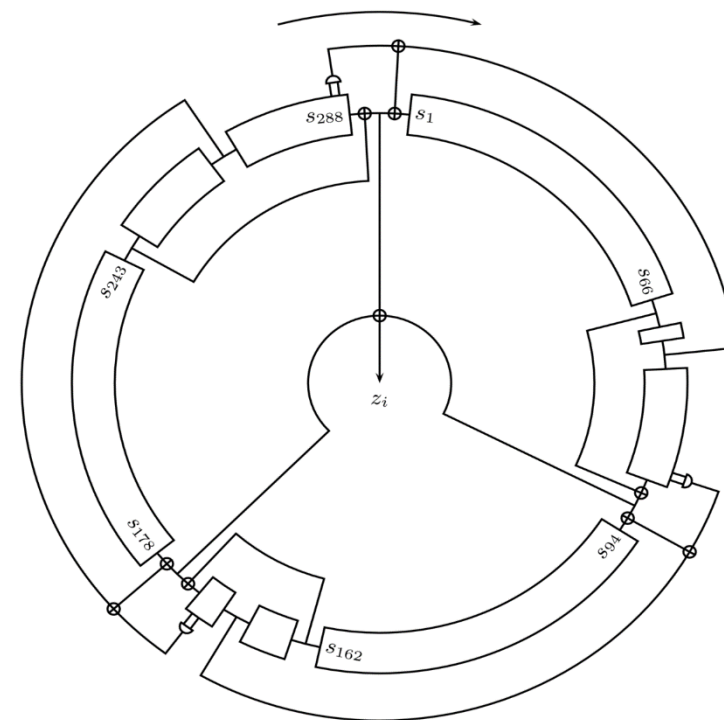
```

Design Runs Table:

Name	Constraints	Status	WNS	TNS	WHS	THS	TPWS	Total Power	Failed Routes	LUT	FF	BRAMs	URAM	DSP	Start	Elapsed	Run Strateg
synth_1	constrs_1	synth_design Complete!								223	368	0.00	0	0	3/13/21 12:40 PM	00:00:15	Vivado Synth
impl_1	constrs_1	route_design Complete!	NA	NA	NA	NA	NA	15.670	0	223	399	0.00	0	0	3/13/21 12:41 PM	00:00:41	Vivado Impl

TRIVIUM

- 2^{64} бит шифртекста, 80 бит K , 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

