СКЗИ для «Беспилотия» или как взлететь с СКЗИ на борту

Марина Сорокина

Руководитель продуктового направления

инфотекс ТЕХНОДЕСТ

Белый поток

План презентации

01

Правовое поле

Постановление №1701 как основа для защиты БАС.

02

Модель угроз и нарушителя

Кто и почему атакует каналы управления.

03

Требования к СКЗИ

Критерии выбора: от криптографии до габаритов.

04

Архитектура системы защиты

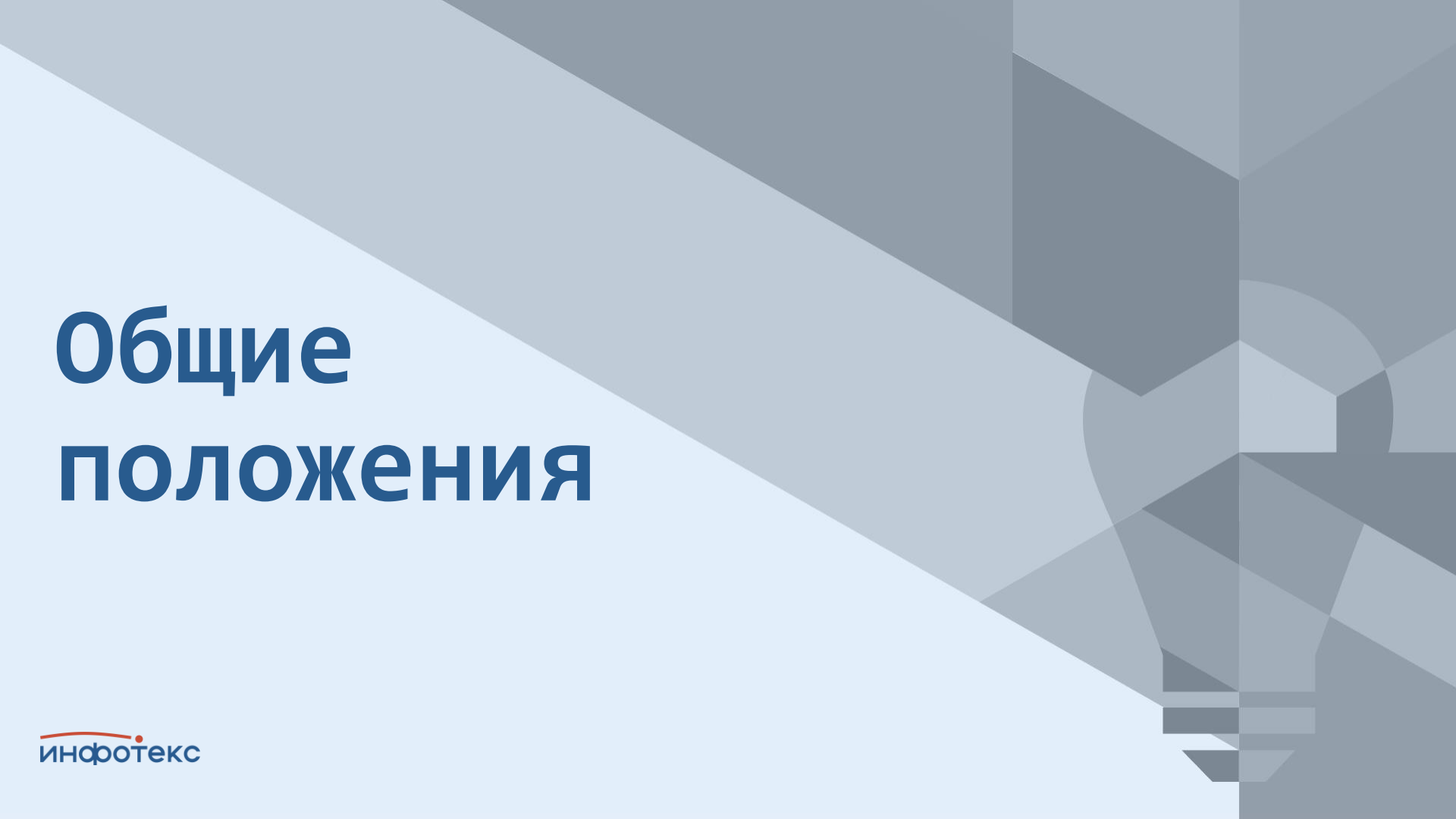
Возможные варианты реализации.

05

СКЗИ от ИнфоТеКС для БАС

Сценарии защиты информации

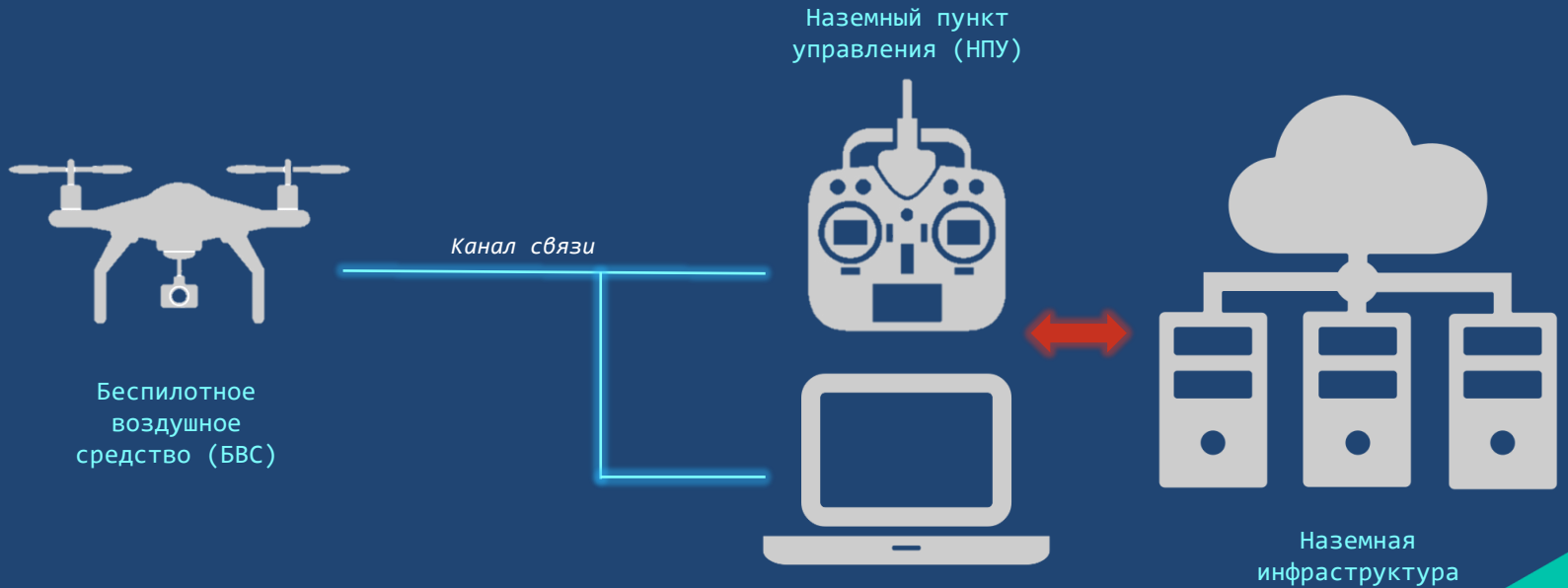
Общие положения



инфотекс

Что за зверь?

Беспилотная Авиационная Система (БАС) – это комплекс, включающий: наземный пункт управления, беспилотное воздушное средство, каналы связи, оператора и инфраструктуру.



Сферы применения БАС

Мониторинг и охрана

- Охрана границ, критических объектов,
- Мониторинг ЧС.

Промышленность и ТЭК

- Инспекция нефте- и газопроводов, ЛЭП,
- Картография и маркшейдерские работы.

Транспорт и логистика

- Доставка грузов (в т.ч. медицинских),
- Такси,
- Патрулирование дорожного движения.

Сельское хозяйство

- Мониторинг полей, точное земледелие,
- Агрохимическая обработка посевов.

Постановление Правительства РФ №1701 от 30.11.2024

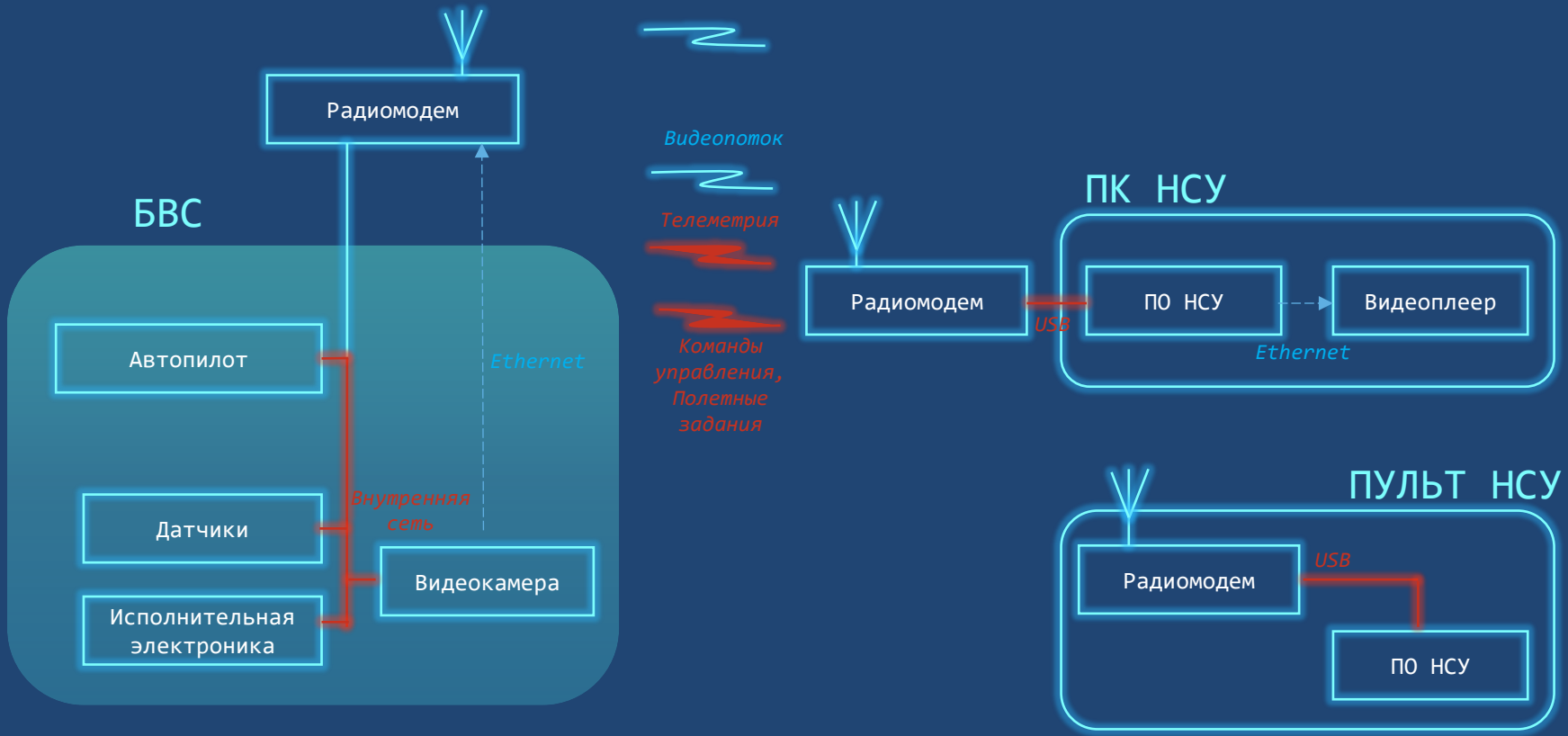
«Документ устанавливает требования к оснащению пилотируемых воздушных судов и беспилотных авиационных систем оборудованием связи, навигации, наблюдения, автоматического предотвращения столкновений, а также оборудованием удаленной идентификации, линиями контроля и СКЗИ».

СКЗИ для БАС в рамках ПП РФ 1701

- «все БАС, включающие БВС с максимальной взлетной массой от 0,25 до 30 кг должны быть оснащены средствами криптографической защиты информации, сертифицированными в установленном порядке»
- «требования применяются к беспилотным авиационным системам, произведенным в РФ или ввезённым на территорию РФ после марта 2027г.»

Применение сертифицированных СКЗИ в БАС – обязательное требование

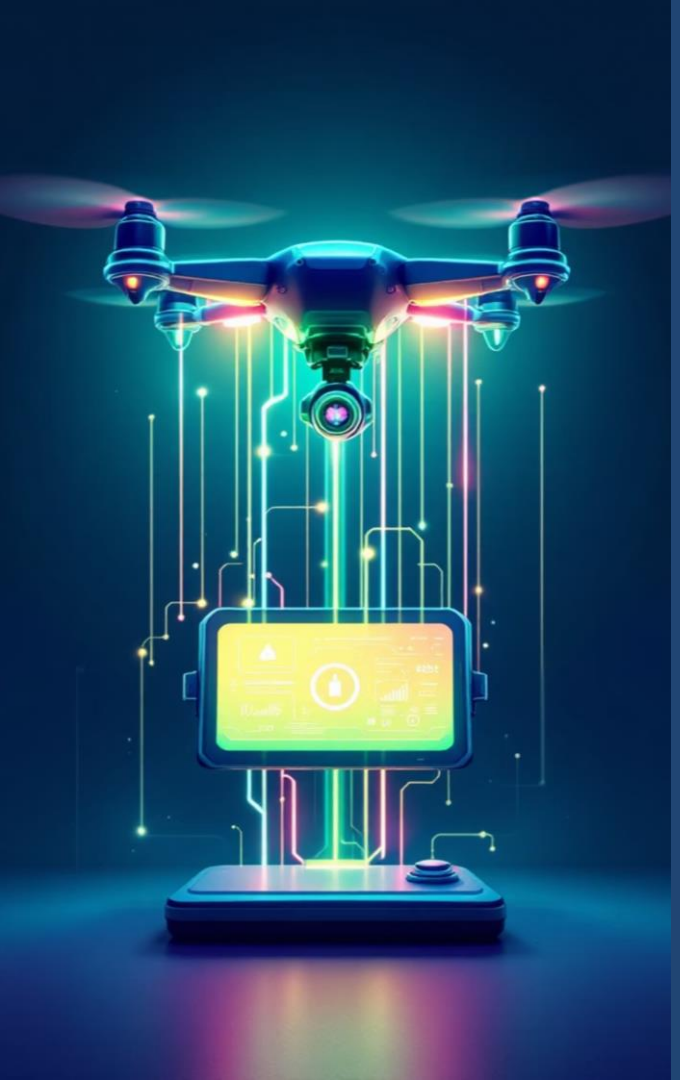
БАС под микроскопом: устройство



БАС под микроскопом: каналы связи

Взаимодействие пользователя с БВС осуществляется исключительно посредством основного и/или резервного радиоканала контроля и управления

- Специализированный радиоканал на основе проприетарных протоколов
- **GSM-канал (**использование мобильной связи)
- **Wi-Fi – канал (**беспроводное соединение)
- Специализированный спутниковый канал при дальней связи



БАС под микроскопом: движение информации

1

НСУ в БВС

Передача по Линии С2: полетное задание, параметры работы, команды управления (автоматический/ полуавтоматический режим), команды управления вспомогательными устройствами и полезной нагрузкой.

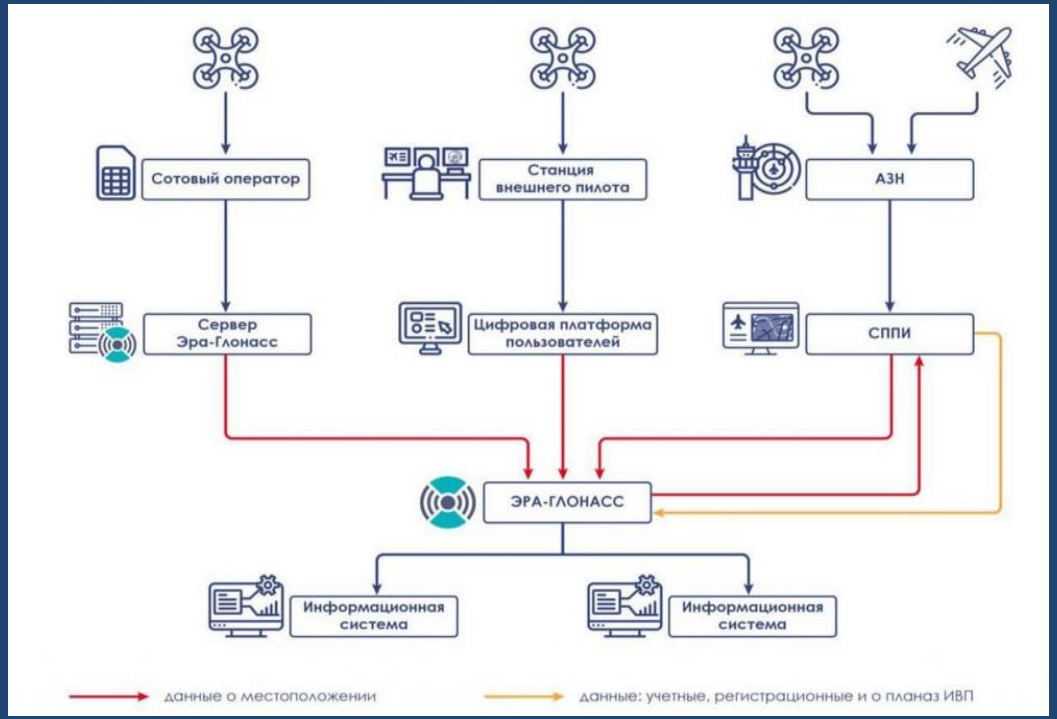
2

БВС на НСУ

Передача по Линии С2: показания датчиков, текущий режим, состояние бортовых устройств, телеметрия. По каналу полезной нагрузки: видеопоток с камеры.

Для сервисных сценариев: команды настройки автопилота, расширенный доступ к параметрам, сервисным командам и обновление ПО.

Бесшовное небо: единая система идентификации БАС



Автоматизацию процессов планирования, согласования и контроля полётов в единой цифровой среде с обменом актуальной оперативной информацией в режиме реального времени.

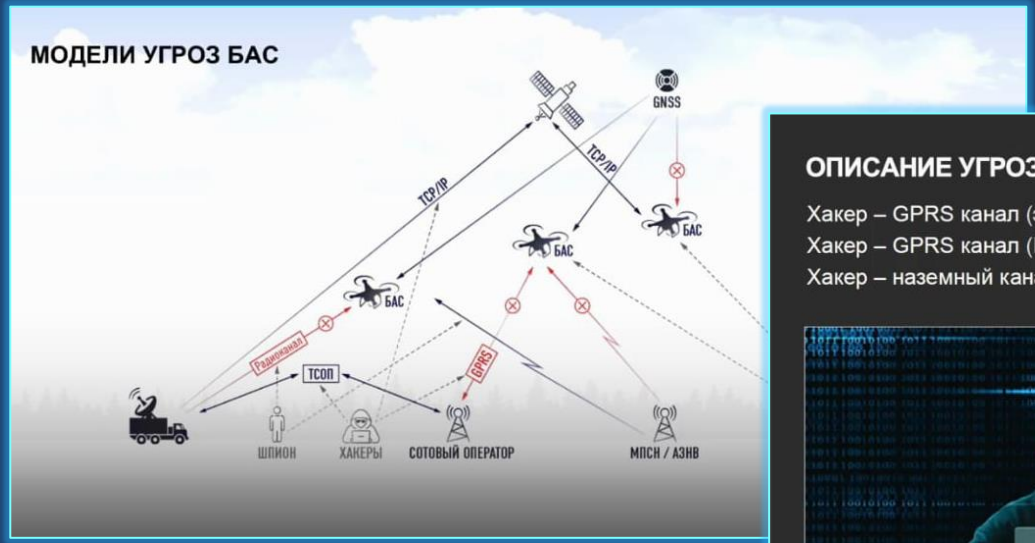
Модель угроз и нарушителя

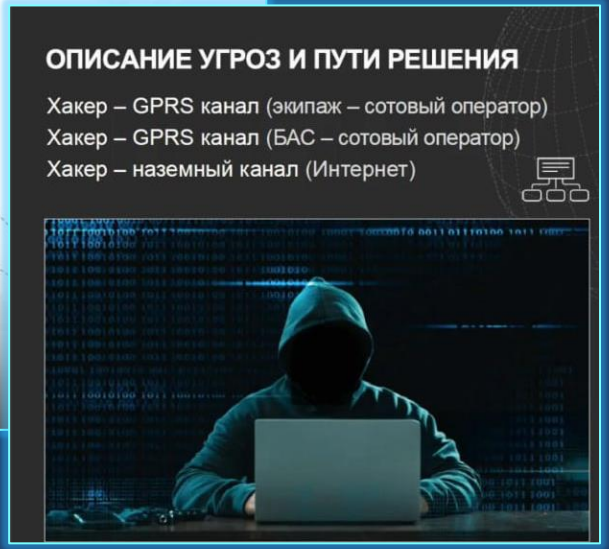
инфотекс

От чего должно защищать СКЗИ?

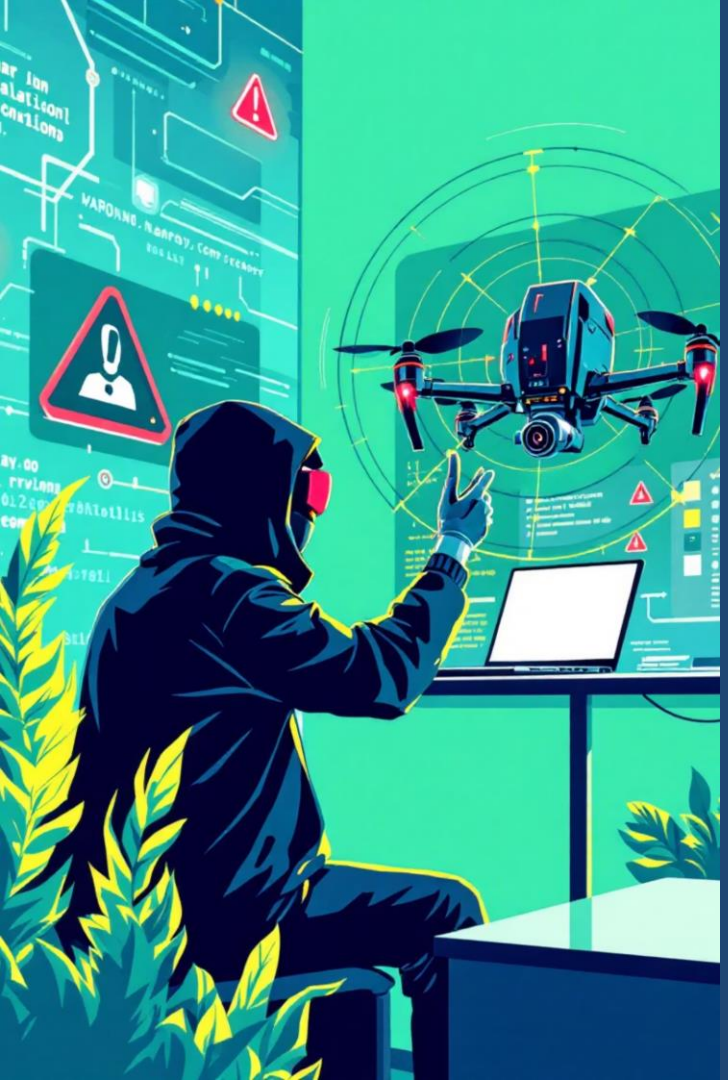
Типовая модель угроз и нарушителя информации для БАС не разработана.

Размышления на тему: МУИН от экспертов отрасли





Из презентации генерального директора ООО "БАС" А.Варятченко (Сессия "Цифровые системы контроля воздушного пространства: новые стандарты и решения" прошедшего форма «Беспилотные системы: технологии будущего»).



Размышления на тему: Опасные последствия

- Разрушение БВС (из хулиганских или аналогичных побуждений)
- Блокировка пролёта БВС в определённую зону (в том числе через потерю управления и/или разрушение)
- Кража Системы или её компонентов (БВС и/или Пульта)
- Завладение БВС для использования в противозаконных целях (в том числе террористических)

Размышления на тему: Выводы отрасли по МУИН

Для предотвращения актуальных угроз на уровне БАС наиболее действенными средствами защиты являются:

- Защита канала взаимодействия БВС-НСУ от постороннего вмешательства (агенты, спуфинг).
- Диверсификация каналов взаимодействия БВС-НСУ.

Требования к СКЗИ для защиты информации в БАС

инфотекс

Ключевые требования при выборе СКЗИ для БАС

Законодательные

Сертифицированные СКЗИ,ГОСТ-алгоритмы

Функциональные

Поддержка всех вариантов каналов связи, низкая задержка обработки команд.

Эксплуатационные

Компактность, низкое энергопотребление, прочность (вибрации, температуры).

Требования по временным характеристикам

Критическая задержка (Latency)

Время между отправкой команды с пульта и ее выполнением на борту не должно превышать **20-50 мс** для высокоманевренных аппаратов.

Проблема: Влияние криптографии

Процессы зашифрования/расшифрования и проверки ЭЦП вносят существенную временную задержку.

Решение: Оптимизация СКЗИ

Выбор СКЗИ, оптимизированных для работы в реальном времени, и использование криптографических протоколов без установления соединения.

Эксплуатационные сценарии БАС

Базовый режим

Полёт одного БВС в автоматическом или ручном режиме в зоне действия связи от одной НСУ.

Множественные БВС

Сопряжение одной НСУ с несколькими БВС (не менее пяти) и их параллельная работа.

Передача управления

Передача контроля над БВС от одного оператора к другому, с поддержкой работы нескольких НСУ.

Резервные каналы

Поддержка параллельной работы БВС с несколькими рабочими местами и резервными каналами связи (GSM, спутник).

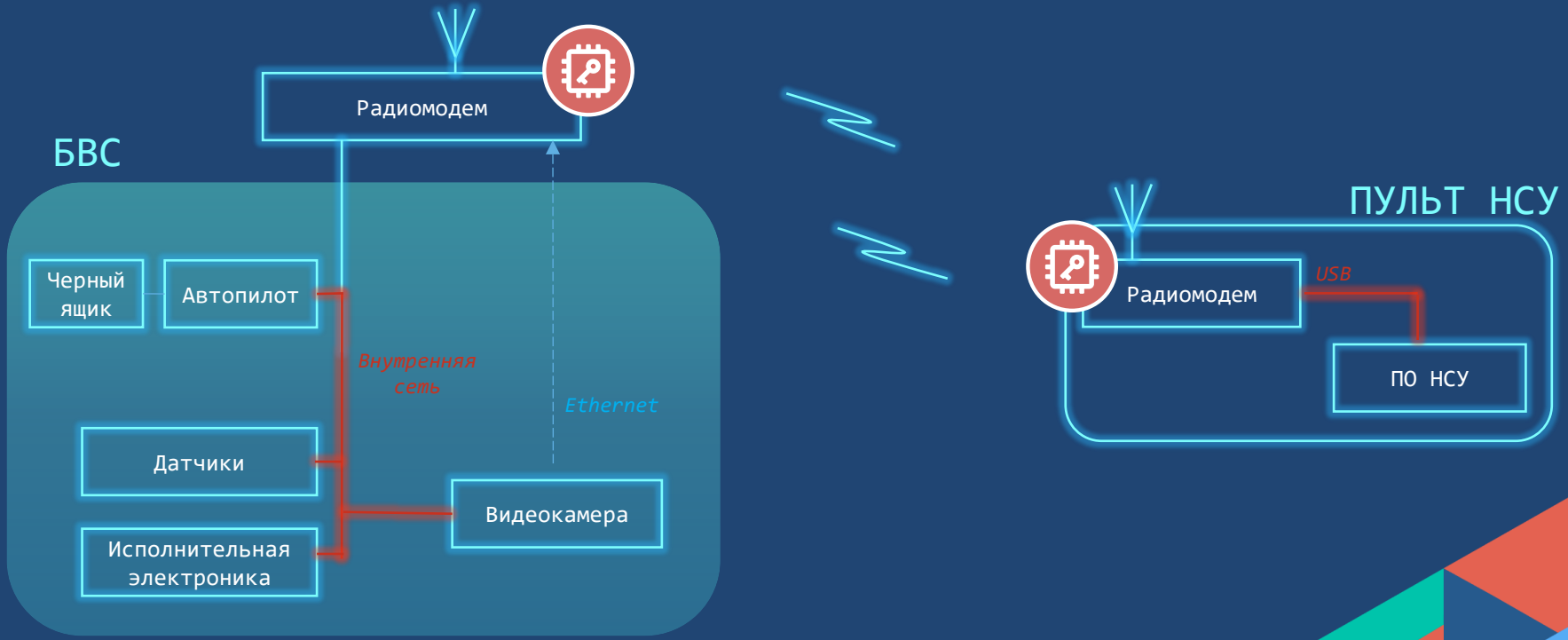
Требования к СКЗИ для БАС:

- СКЗИ должны быть встроенными в компоненты БАС, наложенные средства не целесообразно использовать из-за ограничений по весу, габаритам и потреблению
- В БАС используются разные каналы связи, в том числе радиоканал, беспроводные каналы и спутниковые каналы, СКЗИ должен позволять защищать информацию по любому из них (особенно если речь идет о системе «Бесшовное небо»
- Существенное влияние на выбор СКЗИ оказывает требование по латентности, СКЗИ должно вносить минимальные задержки и не иметь сессионный криптографический протокол

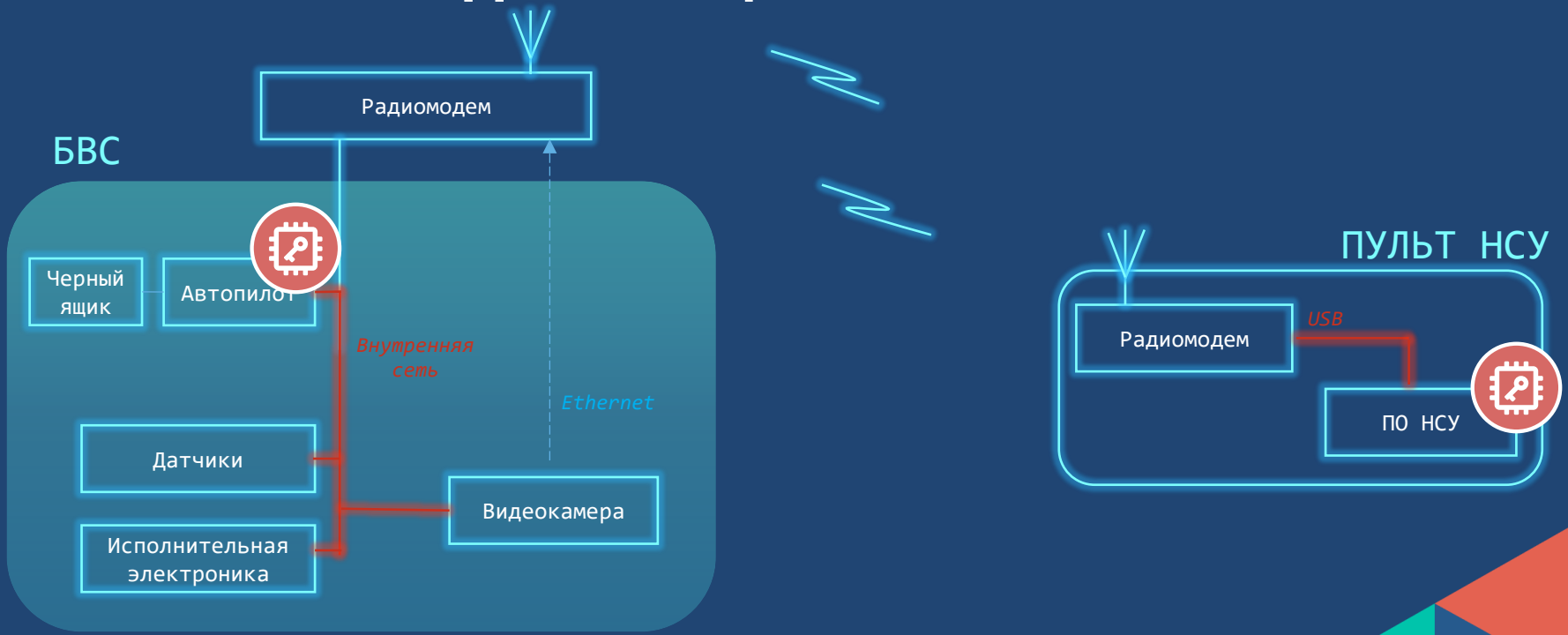
Архитектура системы защиты БАС

инфотекс

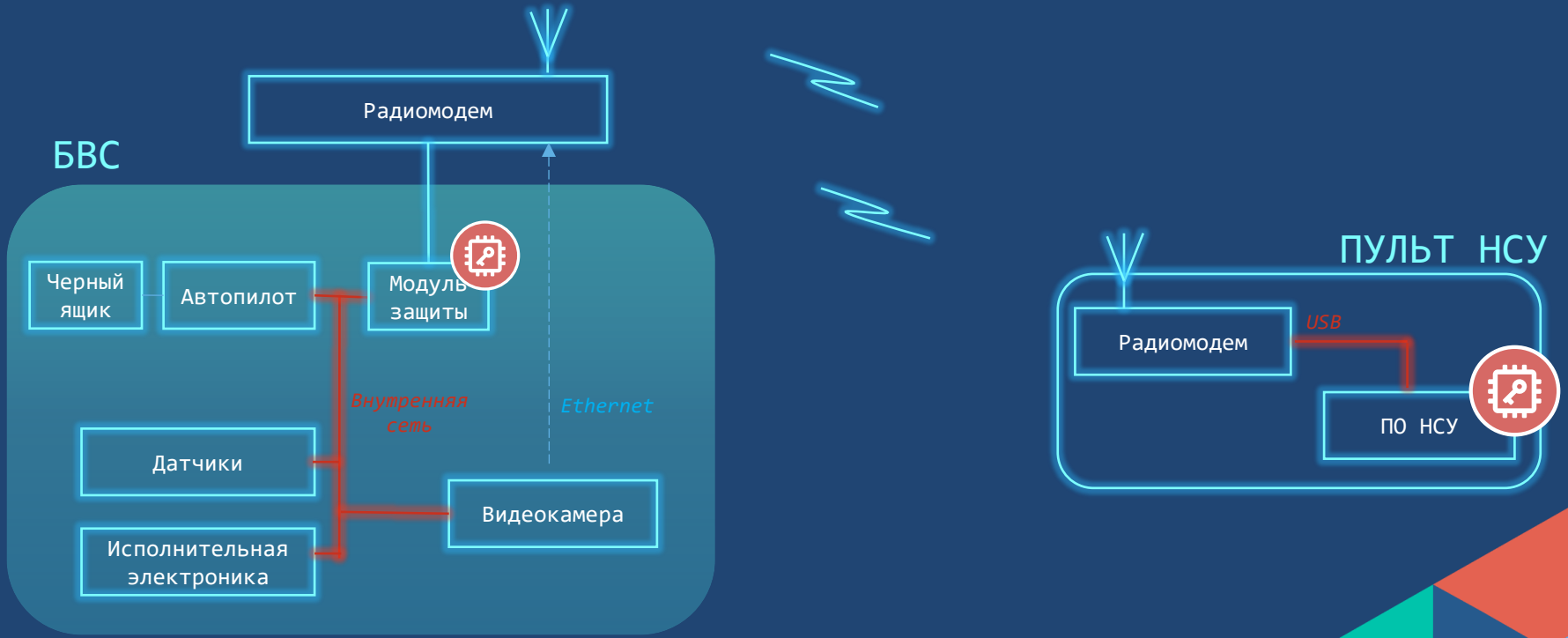
Вар. №1: СКЗИ в составе радиомодемов для защиты канала БВС-НСУ



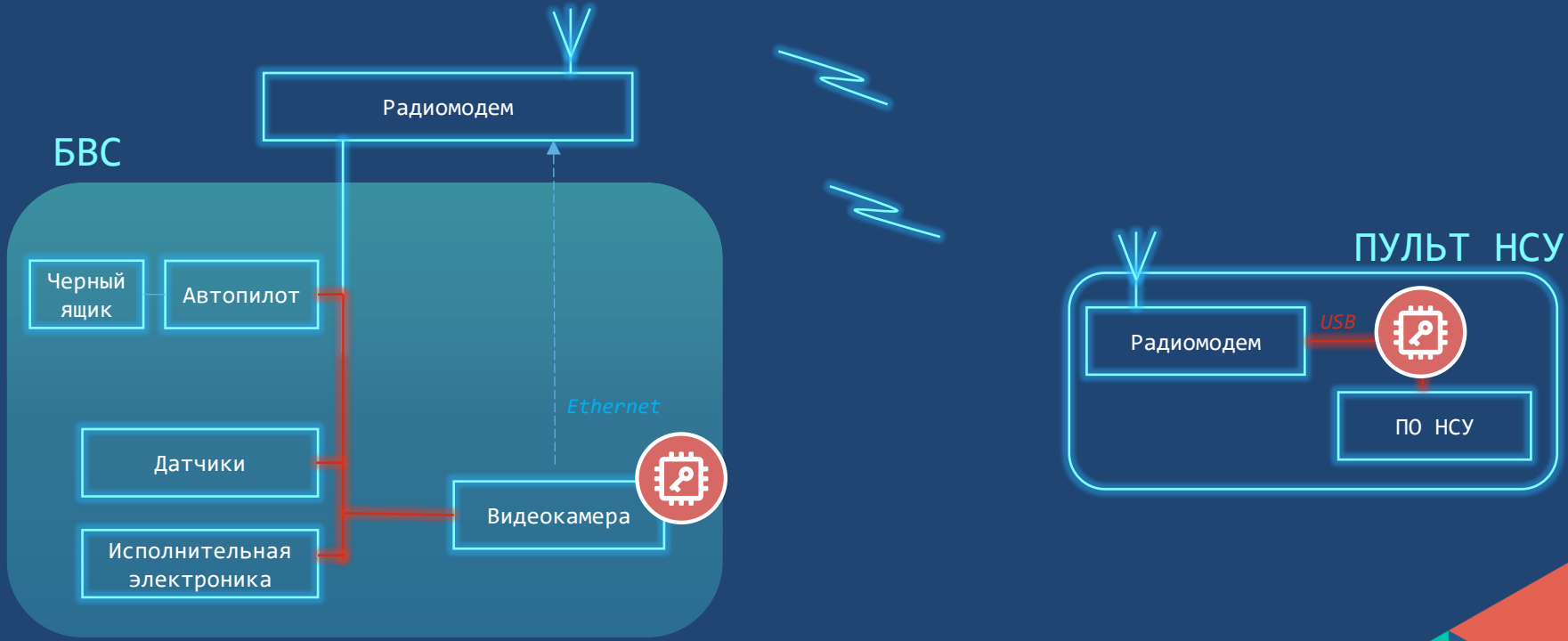
Вариант №2: СКЗИ в составе автопилота для защиты канала БВС-НСУ



Вариант №3: СКЗИ в составе отдельного модуля защиты



Защита видеоканала



СКЗИ от ИнфоТеКС для БАС

инфотекс

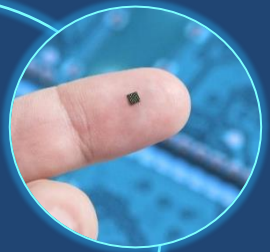
Решение ViPNet SIES

Встраиваемые СКЗИ
ViPNet SIES

CRISP: ГОСТ 71252-2024

Криптомодуль
ПАК ViPNet
SIES Core

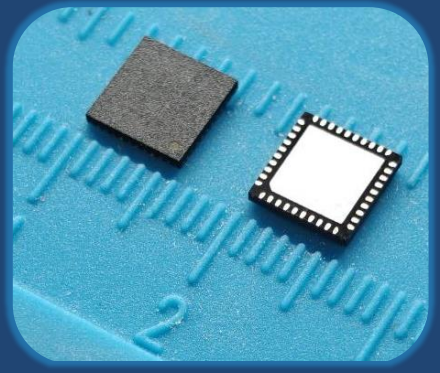
Крипточип
ПАК ViPNet SIES



Программный клиент
ПО ViPNet SIES

Система управления СКЗИ
ViPNet SIES MC

Продукты для встраивания в БАС



ПАК ViPNet SIES Core Nano – крипточип для встраивания в датчики и другие IIoT-устройства:

- Встраивание по SPI
- Хранение ключей до 16 лет
- Рабочий диапазон температур -40…+85^{0}C
- Форм-фактор – BGA36/QFN40
- СКЗИ класса КС3, защита от атак инженерного проникновения (СКЗИ-НР)

ПАК ViPNet SIES Core – криптомодуль для встраивания в концентраторы данных, IIoT-шлюзы:

- Встраивание по UART, USB, SPI
- Возможность использования вне КЗ
- Рабочий диапазон температур -40…+70^{0}C
- Форм-фактор – плата PCI Express® Full-Mini Card (51 x 30 x 11,2 мм)
- СКЗИ класса КС3

ПО ViPNet SIES Unit – ПО для интеграции с серверами и рабочими станциями:

- ПО работает как сервис ОС
- Интеграция – RESTfull API (HTTP/1.1), gRPC API (HTTP/2) или SDK
- Поддерживаемые ОС – Windows, Linux (Debian 9.8, 10/ Ubuntu 16, 18/ Astra Linux 1.6, 1.7)
- Установка на защищаемое устройство или выделенную платформу
- СКЗИ класса КС1, КС3

Использование криптографического протокола CRISP для защиты данных

инфотекс

CRISP

ГОСТ Р 71252-2024.

Протокол защищенного обмена для индустриальных систем

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 71252–2024

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Протокол защищенного обмена для индустриальных систем

Издание официальное

Москва
Российский институт стандартизации
2024

- Обеспечение целостности, конфиденциальность опциональна
- Защита от навязывания повторных сообщений
- Бессесионность
- Минимальный размер добавляемых данных (18 байт «точка-точка» и 19 байт групповые коммуникации)
- Минимальные задержки на обработку
- Работа на любых каналах связи с малой пропускной способностью (в том числе non-IP)
- Высокая энергоэффективность

Возможные сценарии обеспечения ИБ для БАС

Защита коммуникаций БВС – НСУ:

- Обеспечение целостности по протоколу CRISP (ГОСТ 71525-2024)
- Шифрование по протоколу CRISP (ГОСТ 71525-2024)

Защита информации самого БВС :

- Криптографическая идентификация
- Доверенное удаленное и локальное обновление ПО
- Доверенное конфигурирование (в том числе через конфигуратор)
- Черный ящик для хранения журнала устройства

Эксплуатационные сценарии БАС

Базовый режим

Полёт одного БВС в автоматическом или ручном режиме в зоне действия связи от одной НСУ.

Множественные БВС

Сопряжение одной НСУ с несколькими БВС (не менее пяти) и их параллельная работа.

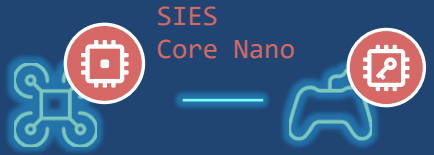
Передача управления

Передача контроля над БВС от одного оператора к другому, с поддержкой работы нескольких НСУ.

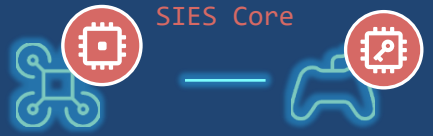
Резервные каналы

Поддержка параллельной работы БВС с несколькими рабочими местами и резервными каналами связи (GSM, спутник).

Эксплуатационные сценарии: Базовый режим

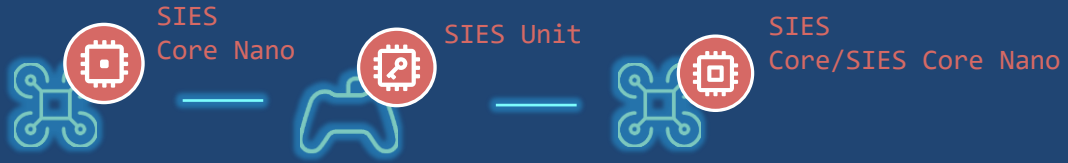


- Ключевая информация в БВС (SIES Core Nano) загружается при производстве БВС
- Сопряжение БВС и НСУ должно происходить через личный кабинет или специальную утилиту, которая взаимодействует с SIES MC Mapper и SIES MC. После сопряжения ключевая информация для парной связи загружается в НПУ (нужен канал связи)
- Такой вариант подходит для долгосрочной эксплуатации



- Инициализация БВС(SIES Core) - на производстве
- Ключевая информация в БВС (SIES Core) и НПУ загружается при сопряжении, если нет канала до БВС, то конверт с ключами может пробрасывать НСУ
- Сопряжение БВС и НСУ должно происходить через личный кабинет или утилиту, которая взаимодействует с SIES MC Mapper и SIES MC. Такой вариант подходит для долгосрочной эксплуатации

Эксплуатационные сценарии: Множественные БВС



- Инициализация БВС(SIES Core/ Core Nano) происходит на производстве
- Для взаимодействия используется мультивещательный ключ
- Загрузка ключевой информация в БВС (SIES Core/ Core Nano) и НПУ загружается при сопряжении, если нет канала до БВС, то конверт с ключами может пробрасывать НСУ
- Сопряжение БВС и НСУ должно происходить через личный кабинет или утилиту, которая взаимодействует с SIES MC Mapper и SIES MC. Такой вариант подходит для долгосрочной эксплуатации

Эксплуатационные сценарии: Передача управления

- Инициализация БВС(SIES Core/ Core Nano) происходит на производстве
- Для взаимодействия использоваться мультивещательный ключ
- Загрузка ключевой информация в БВС (SIES Core/ Core Nano) и НПУ загружается при сопряжении, если нет канала до БВС, то конверт с ключами может пробрасывать НСУ
- Сопряжение БВС и НСУ должно происходить через личный кабинет или утилиту, которая взаимодействует с SIES MC Mapper и SIES MC. Такой вариант подходит для долгосрочной эксплуатации

Эксплуатационные сценарии: Резервные каналы управления

- Инициализация БВС(SIES Core/ Core Nano) происходит на производстве
- Для взаимодействия БВС может использоваться парные связи (в случае выполнения разных задач) – для основного взаимодействия и для резервного взаимодействия
- Для взаимодействия БВС может использоваться резервированная парная связь (в случае дублирования задач)
- Загрузка ключевой информация в БВС (SIES Core/ Core Nano) и НПУ загружается при сопряжении, если нет канала до БВС, то конверт с ключами может пробрасывать НСУ Сопряжение БВС и НСУ должно происходить через личный кабинет или утилиту, которая взаимодействует с SIES MC Mapper и SIES MC. Такой вариант подходит для долгосрочной эксплуатации

Временные характеристики при использовании ViPNet SIES

- Рекомендуется выбирать интерфейс SPI для интеграции с SIES Core и SIES Core Nano
- Есть подходы по нормализации трафика для увеличения производительности
- Требуются натурные испытания

Выводы

- Применение СКЗИ в БАС является обязательным согласно ПП1701.
- Отсутствие единой утвержденной модели угроз и нарушителя требует разработки МУИН каждым производителем. Подходы при разработке МУИН могут сильно отличаться от вендора к вендору.
- На данный момент производители не рассматривают в МУИН угрозы, связанные с эксплуатацией системы «Бесшовное небо», так как нет утвержденной технического решения по данной теме.
- К СКЗИ в БАС предъявляются серьезные требования с точки зрения габаритов, латентности и ограничений по питанию.
- СКЗИ в БАС должны поддерживать все сценарии эксплуатации БАС.

САНКТ ПЕТЕРБУРГ

инфотекс
ТЕХНОДЕСТ

Марина Сорокина
Marina.Sorokina@infotecs.ru

Академия инфотекс · Учебный центр инфотекс · AMPIRE · TELEOFIS · КОМФОРТЕЛ оператор связи бизнес-класса · РУТОКЕН компания АКТИВ · TS Solution · AXOFT

Подписывайтесь
на наши соцсети