Защита информационных ресурсов по протоколу TLS с использованием отечественных продуктов

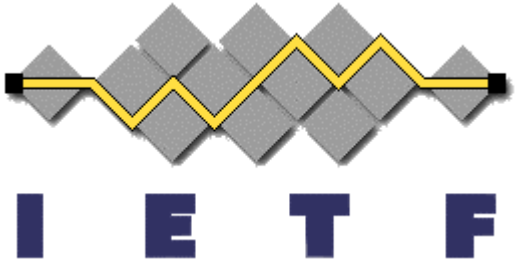
Еранов Сергей
Начальник отдела разработки компонентов инфраструктуры открытых ключей

infotecs

Зачем нам TLS ГОСТ

Стандартизация

- ГОСТ
- RFC
- Рекомендации ТК26
- Контрольные примеры



Результат: Мультивендорность для конечных потребителей

Активное продвижение со стороны государства

- Пр-1380 от 16 июля 2016 г. Поручение об обеспечении разработки и реализации комплекса мероприятий, необходимых для перехода органов власти на использование российских криптографических алгоритмов и средств шифрования

- Постановление Правительства от 30 июня 2020 г. № 963 «О реализации пилотного проекта по использованию российских криптографических алгоритмов и средств шифрования в государственных информационных системах»

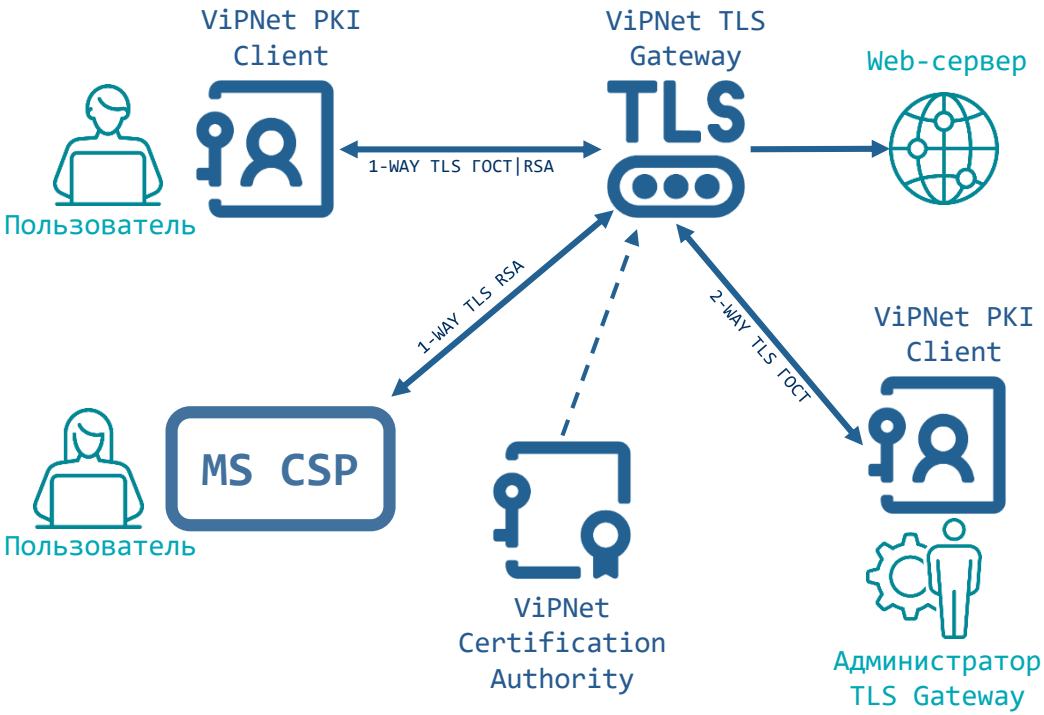
- Проект приказа Минкомсвязи «Об утверждении требований к технологиям взаимодействия средств информатизации, реализующих российские криптографические алгоритмы, с иными средствами информатизации»

- **Проекта Приказа ФСБ "Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием средств криптографической защиты информации"**

Сценарии применения

Сценарий 1

Публичный портал

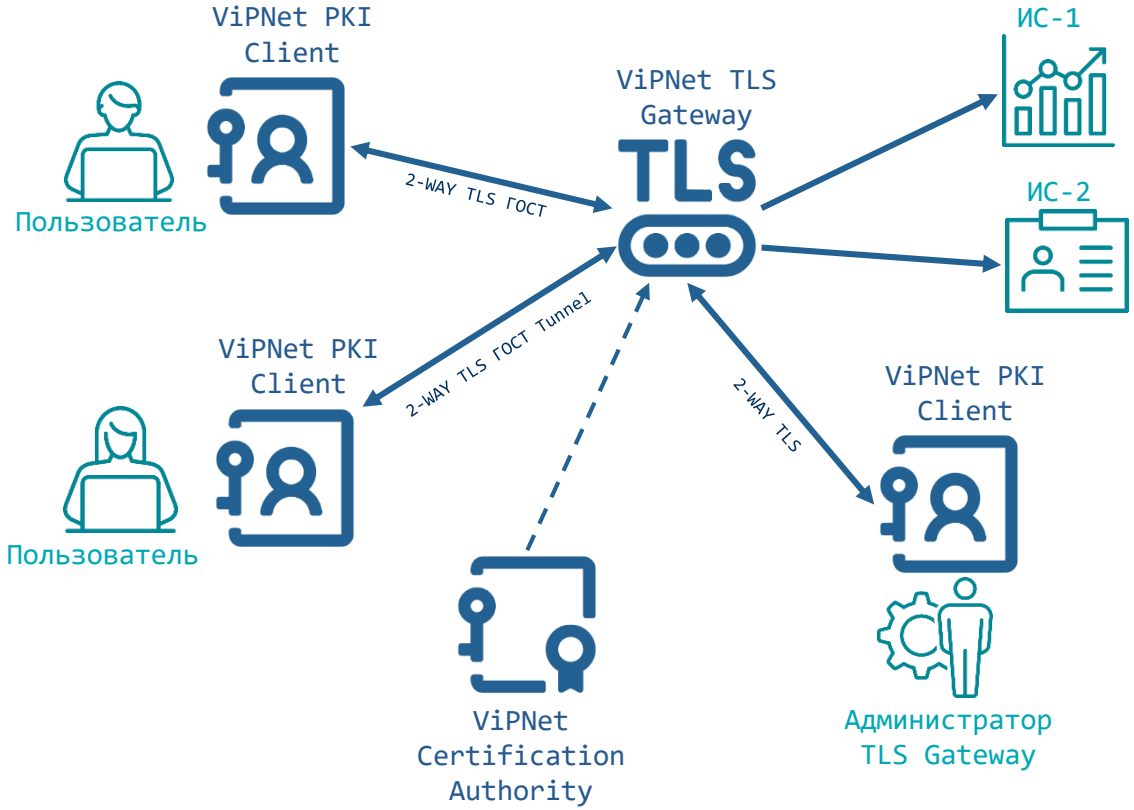


Для этого требуется:

- Единое пространство доверия – НУЦ
- Аутентификация сервера
- Общедоступность клиентского СКЗИ
- Дуальный режим

Сценарий 2

Доступ к корпоративным ресурсам



Для этого требуется:

- Аутентификация сервера
- Аутентификация клиента
- Разграничение доступа
- Защита TCP-трафика

Что для этого нужно

Для порталов

- ✓ Высокопроизводительные криптошлюзы
- ✓ Средства установления TLS соединений для веб-серверов

Для разработчиков

- ✓ Библиотеки и SDK для установки TLS соединений из приложений

Для пользователей

- ✓ Готовое СКЗИ для TLS

Готовые решения для использования TLS

ViPNet TLS Gateway

Высокопроизводительный TLS-криптошлюз

- Аутентификация клиента и сервера
- Управление доступом на основе сертификатов
- «Дуальный» режим работы
- Удаленное управление
- Кластеризация
- TLS 1.0 – 1.3
- IPv6

Модификации

Исполнение	TLS 550	TLS 1100	TLS 5500
Форм-фактор	ПАК 19” Rack 1U	ПАК 19” Rack 1U	ПАК 19” Rack 1U
Предельная пропускная способность (Мбит/с)	до 600	до 1800	до 7600
Число одновременных соединений	до 7000	до 14000	до 65000
Интерфейсы	6x Ethernet 10/100/1000	8x Ethernet 10/100/1000 4x 1G Ethernet Fiber SFP	4x Ethernet 10/100/1000 8x 10G Ethernet Fiber SFP+

Платформы виртуализации

ViPNet TLS Gateway сертифицирован

- СКЗИ КС3 (исполнения ПАК)
- СКЗИ КС1 (исполнение VA)
- Зарегистрирован в Реестре российского ПО

Клиентское СКЗИ

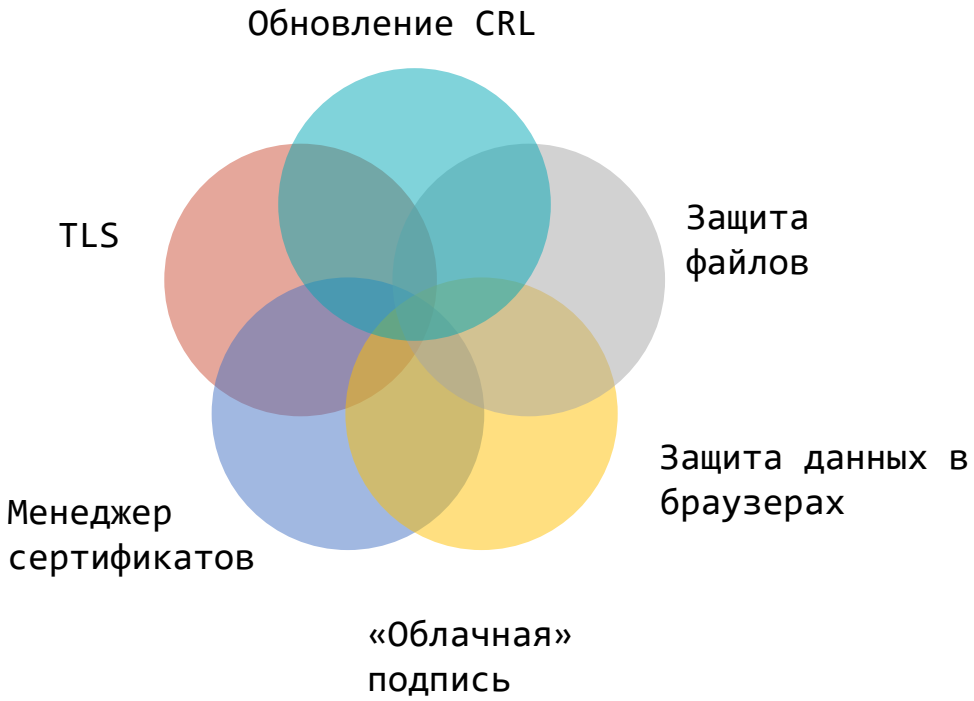
ViPNet CSP

ViPNet PKI Client

Любое сертифицированное СКЗИ

ViPNet PKI Client

Клиент для работы в инфраструктуре открытых ключей



- СКЗИ и средство ЭП
- Кроссплатформенный
- Кроссбраузерный
- Модульный
  - TLS Unit
  - File Unit
  - Web Unit
  - Certificate Unit
  - CRL Unit
  - Cloud Unit

ViPNet PKI Client. TLS Unit

Упрощает работу:

- Установка доверенных сертификатов УЦ
- Автоматическое обновление CRL

TLS соединение:

- локальный TLS-proxy
- TLS-туннель для TCP-трафика
- TLS 1.0 - 1.3

Преимущества:

- Кроссбраузерный

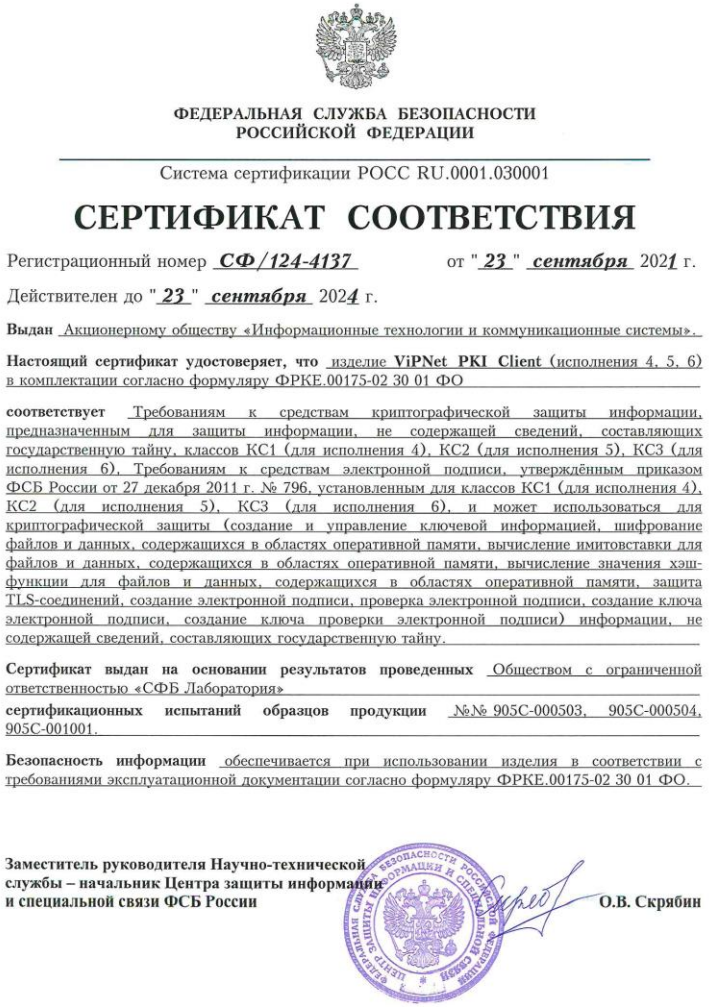
- Совместим с ViPNet TLS Gateway и TLS-шлюзами других производителей

Работа в мобильных браузерах

ViPNet PKI Client

Сертификация

- СКЗИ КС1-КС3
- Средство ЭП КС1-КС3
- Получена нотификация на вывоз



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/124-4137* от "*23*" *сентября* 2021 г.

Действителен до "*23*" *сентября* 2024 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что изделие **ViPNet PKI Client** (исполнения 4, 5, 6) в комплектации согласно формуляру ФРКЕ.00175-02 30 01 ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, классов КС1 (для исполнения 4), КС2 (для исполнения 5), КС3 (для исполнения 6), Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для классов КС1 (для исполнения 4), КС2 (для исполнения 5), КС3 (для исполнения 6), и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, защита TLS-соединений, создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «СФБ Лаборатория»

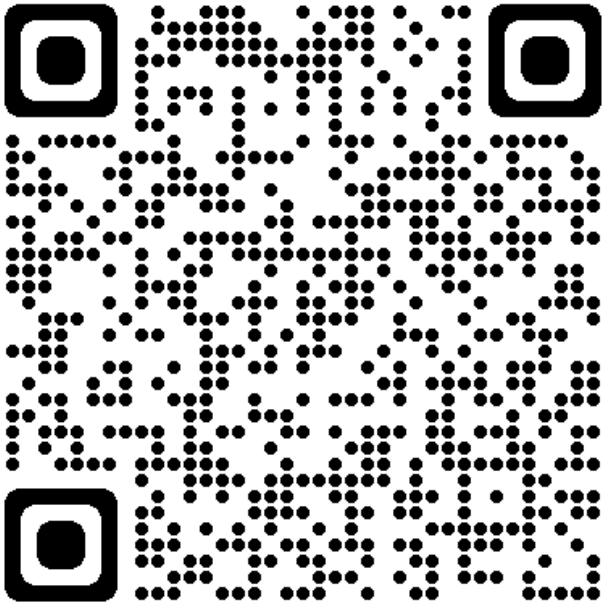
сертификационных испытаний образцов продукции №№ 905С-000503, 905С-000504, 905С-001001.

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями эксплуатационной документации согласно формуляру ФРКЕ.00175-02 30 01 ФО.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России **О.В. Скрябин**

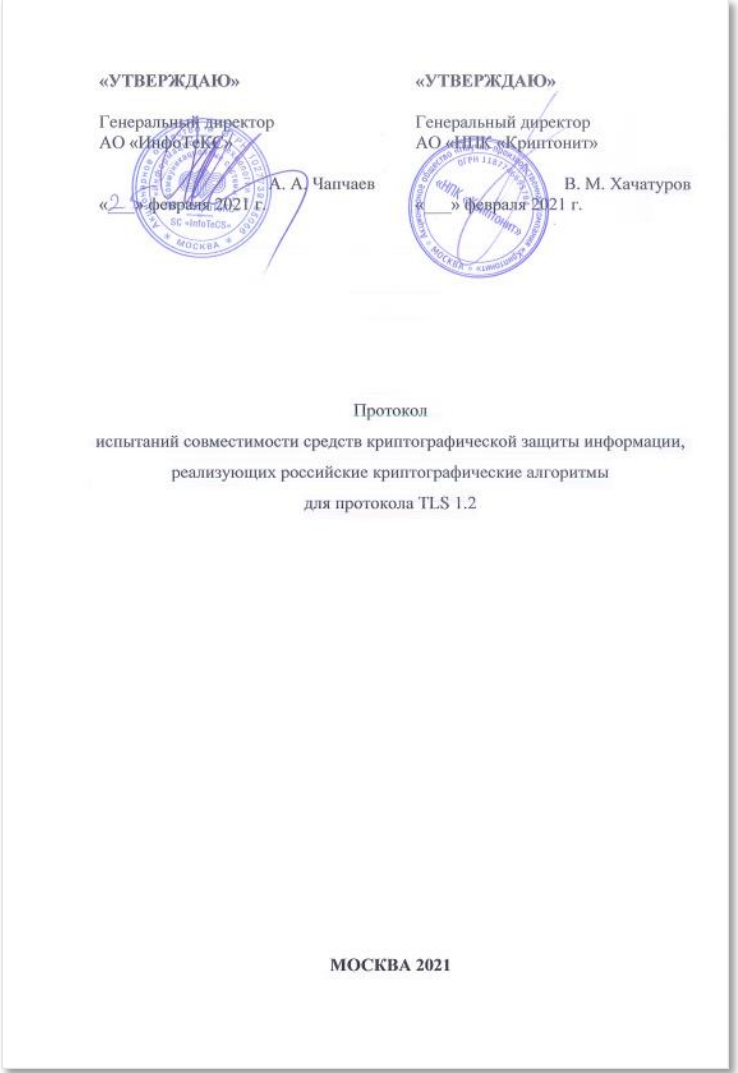
Демо-версия для Windows и Linux

- Доступна на сайте ИнфоТеКС
- Бесплатная лицензия на полгода
- Односторонний TLS бесплатно в любом браузере



Совместимость

- АО «НПК Криптонит» подтверждено соответствие TLS 1.2 эталонной реализации
- Успешно проведено встречное тестирование с реализацией TLS 1.2-1.3 других вендоров



«УТВЕРЖДАЮ»

Генеральный директор
АО «ИнфоТеКС»

А. А. Чапчаев

«2» февраля 2021 г.

«УТВЕРЖДАЮ»

Генеральный директор
АО «НПК «Криптонит»

В. М. Хачатуров

«___» февраля 2021 г.

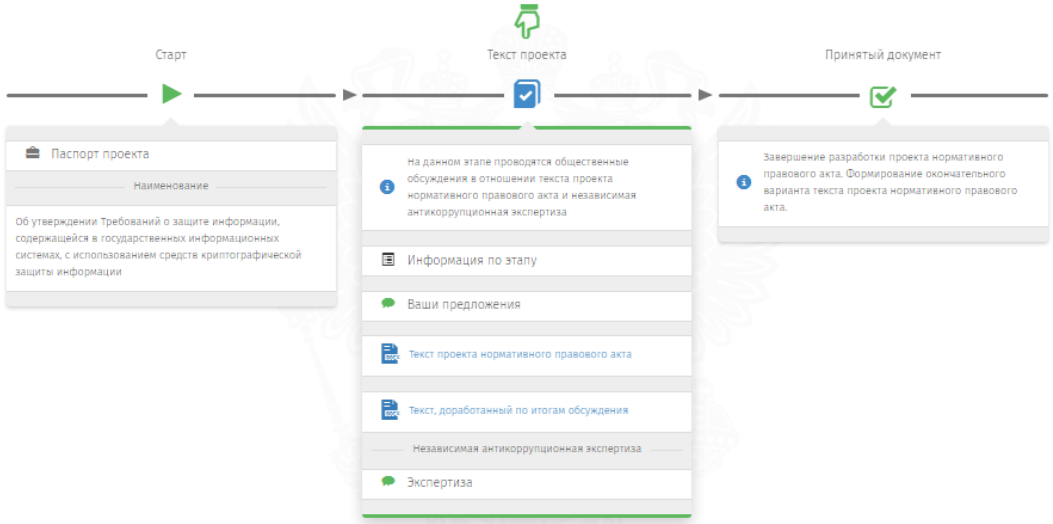
Протокол

испытаний совместимости средств криптографической защиты информации, реализующих российские криптографические алгоритмы для протокола TLS 1.2

МОСКВА 2021

Что нас ждет в ближайшем будущем

Проекта Приказа ФСБ "Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием средств криптографической защиты информации"



Требования к классу СКЗИ

> 6.Для обеспечения защиты информации, содержащейся в ГИС, должны использоваться только СКЗИ, сертифицированные ФСБ России.

Уровень значимости информации	Масштаб ГИС (сегмента ГИС)		
	Федеральный	Региональный	Объектовый
Высокий	КВ	КС3	КС2
Средний	КС3	КС3	КС1
Низкий	КС2	КС1	КС1

Требования к классу СКЗИ

> 16.Класс СКЗИ, подлежащих использованию для защиты информации в ГИС (сегменте ГИС), при ее взаимодействии с другими ГИС и (или) сегментами других ГИС определяется по более высокому классу СКЗИ…

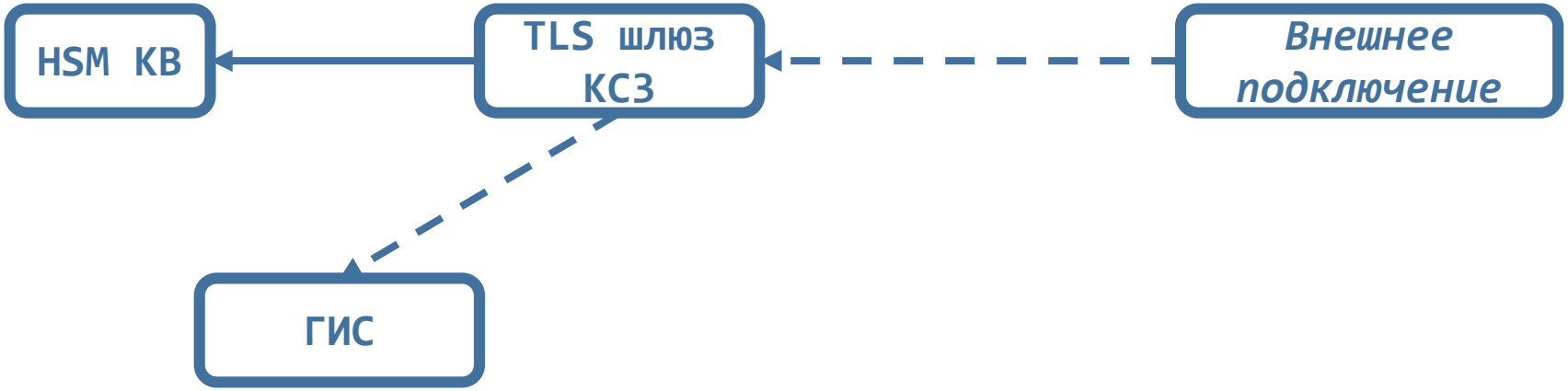
Требования к классу СКЗИ

> 20.В случае если в модели угроз безопасности информации в качестве актуальной угрозы определена возможность источника атак привлекать специалистов, имеющих опыт разработки и анализа СКЗИ…, то для защиты информации в ГИС (сегменте ГИС) необходимо использовать СКЗИ класса КВ.

Есть место для TLS класса КВ

Но есть ли он на рынке?

TLS КС3+



Общие моменты:

1. Есть готовые решения
2. Необходимость приобретения и эксплуатации 2 ПАК

Варианты реализации TLS КС3+

Все криптографические операции в HSM

- Снижение нефункциональных характеристик TLS-шлюза
- СКЗИ класса КВ

HSM – хранилище ключа

- Отсутствие негативного влияния на производительность
- TLS строится СКЗИ класса КС3

Что мы можем предложить

ПАК

ViPNet HSM

+

СПО

ViPNet TLS Gateway

=

ПАК ViPNet TLS КВ

ViPNet TLS KB

- Один ПАК
- СКЗИ класса КВ
- Меры защиты ViPNet HSM
- **Все привычные функции TLS Gateway**

Продукт находится в разработке, будет доступен для тестирования в начале 2023

Спасибо за внимание!

Еранов Сергей

e-mail: sergey.eranov@infotecs.ru

Подписывайтесь на наши соцсети

vk.com/infotecs_news

t.me/infotecs_news

rutube.ru/channel/24686363