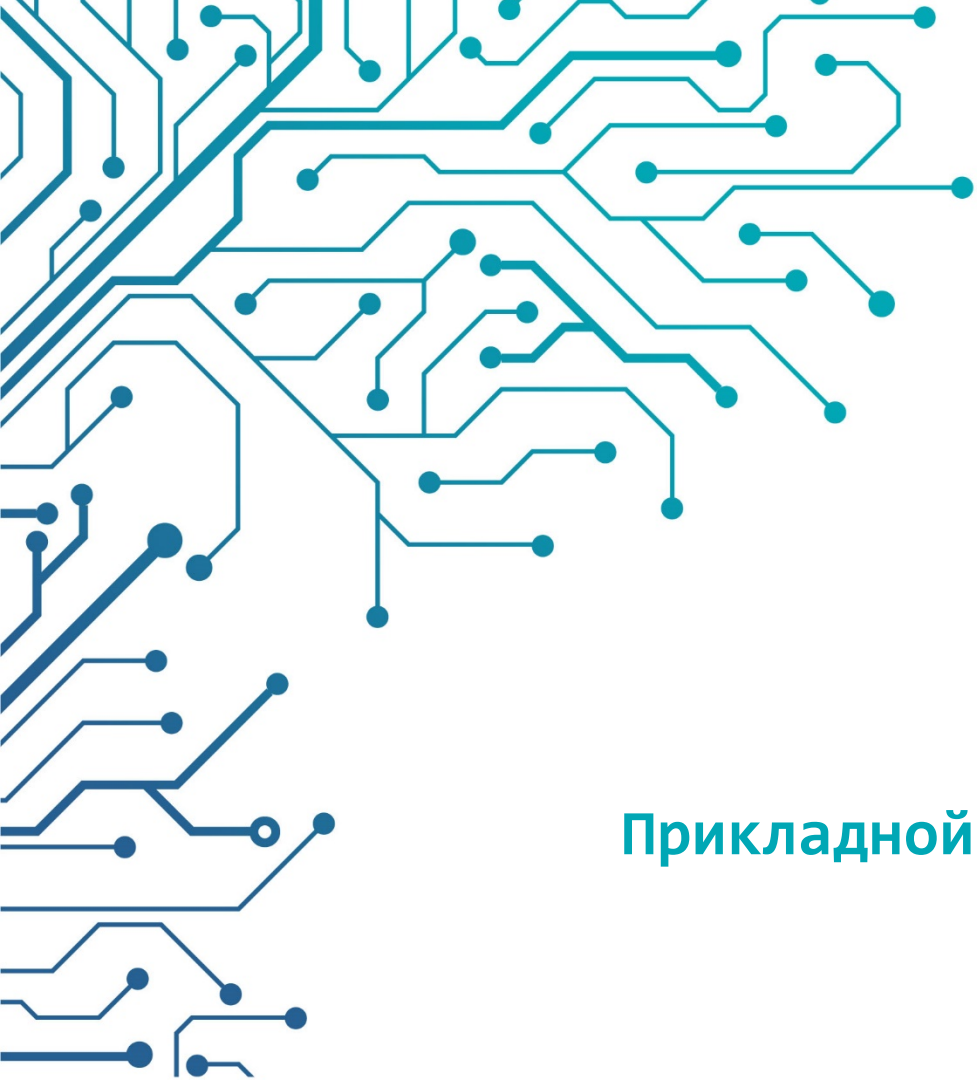


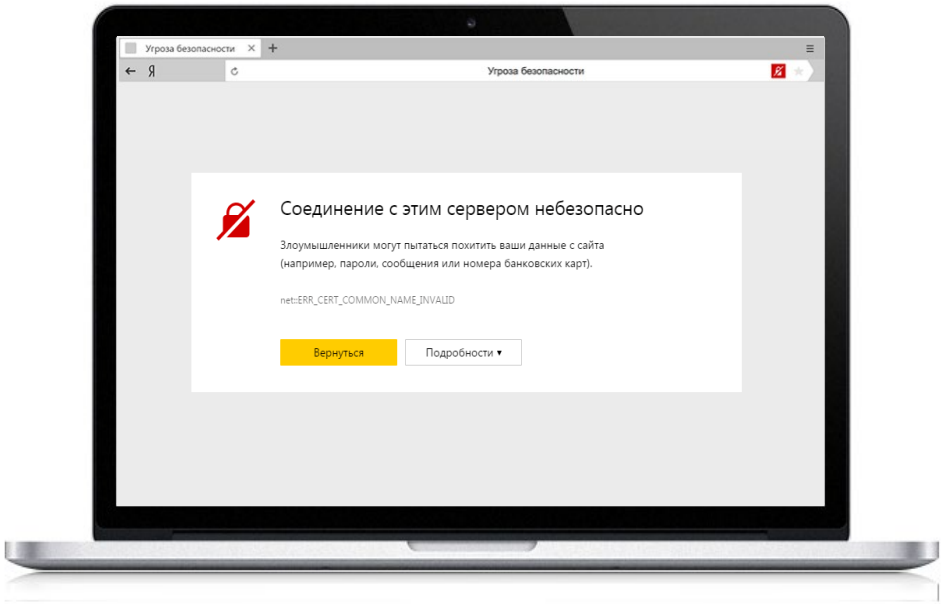
TLS ГОСТ

Прикладной. Мобильный. Серверный.

Еранов Сергей
АО «ИнфоТеКС»

Зачем нам ГОСТ TLS?

Независимость и безопасность



Какие возникают проблемы

SSL-сертификат, выданный иностранным УЦ, могут отозвать из-за санкций:

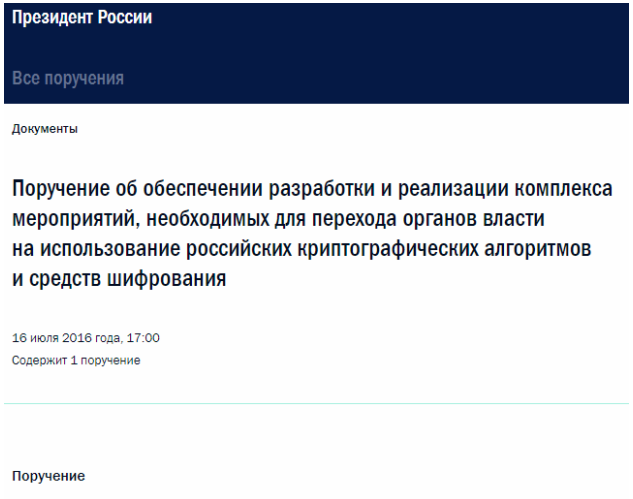
GeoTrust отозвала сертификат для сайта Общественной палаты из-за «аффилированности» с ДНР

Как решаются эти проблемы

Ведется запуск **Национального удостоверяющего центра**

Активное продвижение со стороны государства

- Поручение президента об использовании российских криптоалгоритмов и средств шифрования
- Директива об использовании отечественного ПО в компаниях с гос. участием



Стандартизация

Продукты ИнфоТеКС разрабатываются в соответствии со стандартами:

- RFC
- ГОСТ
- Рекомендации ТК26
- Контрольные примеры

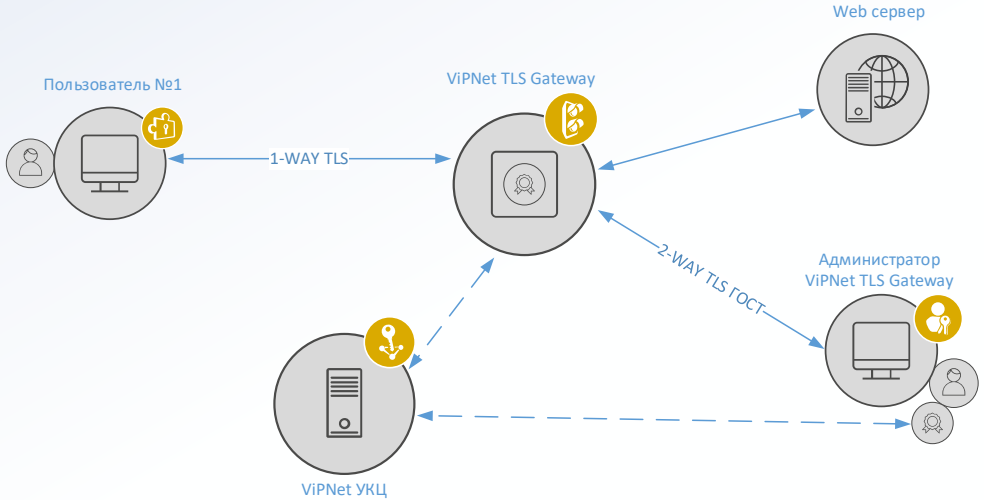
Результат:

Кроссвендорность
для конечных потребителей

Сценарии применения

Сценарий 1

Публичный портал



Задачи:

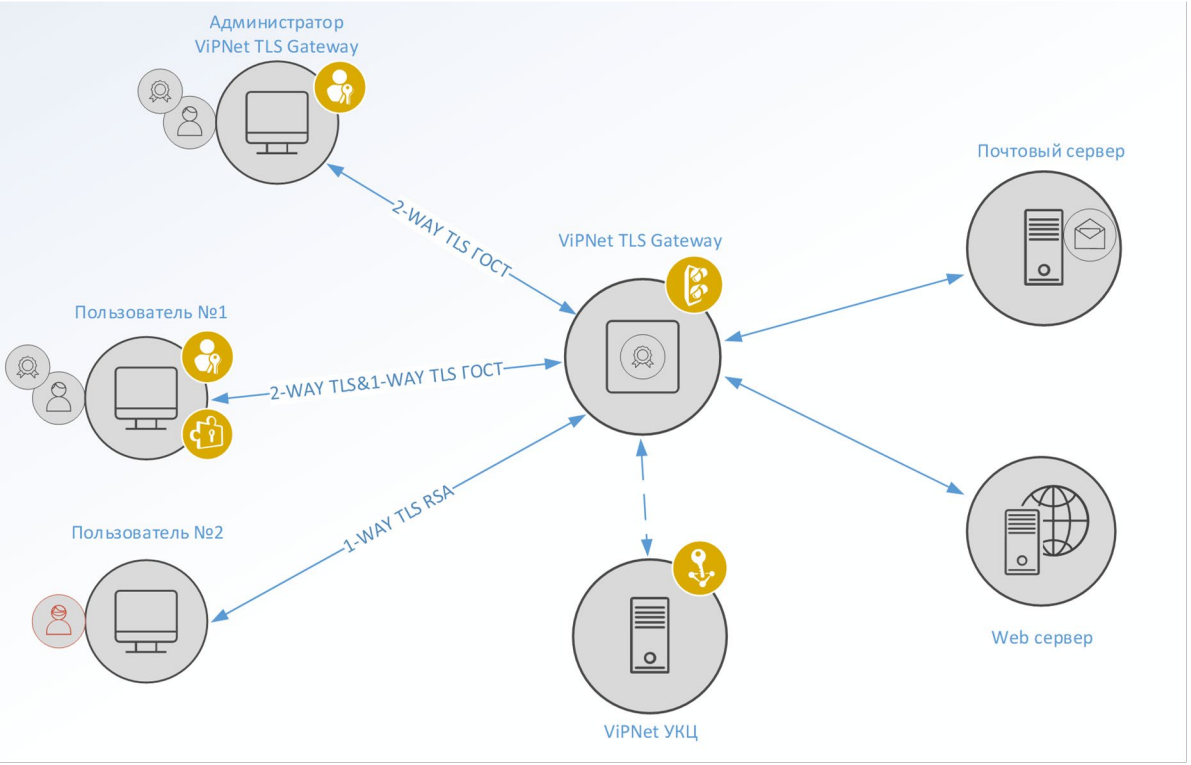
1. Подтверждение подлинности сервера
2. Защита передаваемых данных

Для этого требуется:

- Единое пространство доверия – НУЦ
- Односторонний TLS
- Дуальный режим
- Общедоступность клиентского СКЗИ

Сценарий 2

Доступ к корпоративным ресурсам



Задачи:

1. Защита соединений
2. Аутентификация клиентов

Для этого требуется:

Двусторонний TLS

TLS ГОСТ. Серверный

ViPNet TLS Gateway

ViPNet TLS Gateway

Высокопроизводительный TLS-криптошлюз

- Аутентификация клиента и сервера
- Дуальный режим
- Управление доступом на основе сертификатов
- Поддержка центров доверия
- Удаленное управление

Модификации

Исполнение	TLS 500	TLS 1000	TLS 5000	TLS VA
Форм-фактор	ПАК 19” Rack 1U	ПАК 19” Rack 1U	ПАК 19” Rack 1U	виртуальная машина
Предельная пропускная способность (Мбит/с)	до 300	до 750	до 3000	зависит от характеристик аппаратного обеспечения
Число одновременных соединений	до 4700	до 8900	до 44000	зависит от характеристик аппаратного обеспечения
Интерфейсы	4x Ethernet 10/100/1000	4x Ethernet 10/100/1000	4x Ethernet 10/100/1000 4x 10G Ethernet Fiber SFP+	зависят от характеристик аппаратного обеспечения

Платформы виртуализации

Oracle VM VirtualBox
5.1, 5.2, 6.0

VMware vSphere ESXi
6.0, 6.5, 6.7

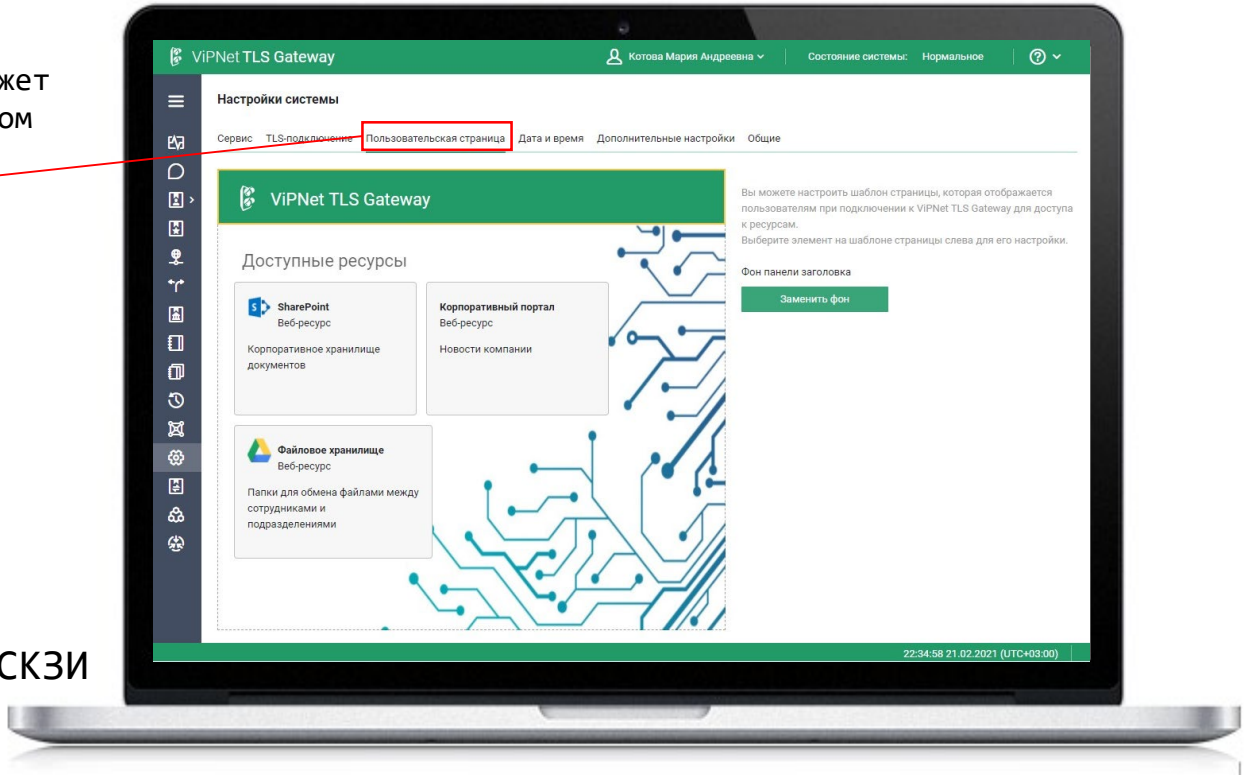
VMware Workstation
14, 15

Kernel
Virtual Machine

ViPNet TLS Gateway

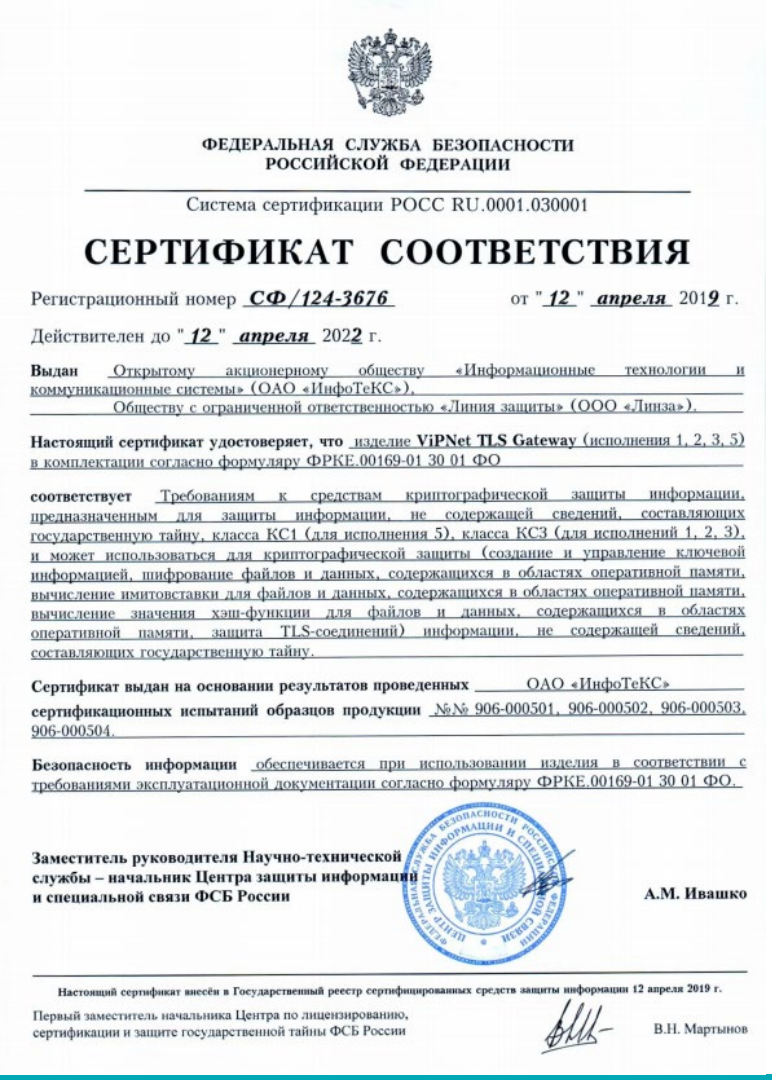
Пользовательская страница может быть модифицирована заказчиком

Пользовательская страница



Клиентское ПО – СКЗИ:

- ViPNet CSP
- ViPNet PKI Client
- Любое сертифицированное СКЗИ



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-3676 от "12" апреля 2019 г.

Действителен до "12" апреля 2022 г.

Выдан Открытому акционерному обществу «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»),
Обществу с ограниченной ответственностью «Линия защиты» (ООО «Линза»).

Настоящий сертификат удостоверяет, что изделие ViPNet TLS Gateway (исполнения 1, 2, 3, 5) в комплектации согласно формуляру ФРКЕ.00169-01 30 01 ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1 (для исполнения 5), класса КС3 (для исполнений 1, 2, 3), 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) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных ОАО «ИнфоТеКС» сертификационных испытаний образцов продукции №№ 906-000501, 906-000502, 906-000503, 906-000504.

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями эксплуатационной документации согласно формуляру ФРКЕ.00169-01 30 01 ФО.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России А.М. Ивашко

Настоящий сертификат внесён в Государственный реестр сертифицированных средств защиты информации 12 апреля 2019 г.

Первый заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России В.Н. Мартынов

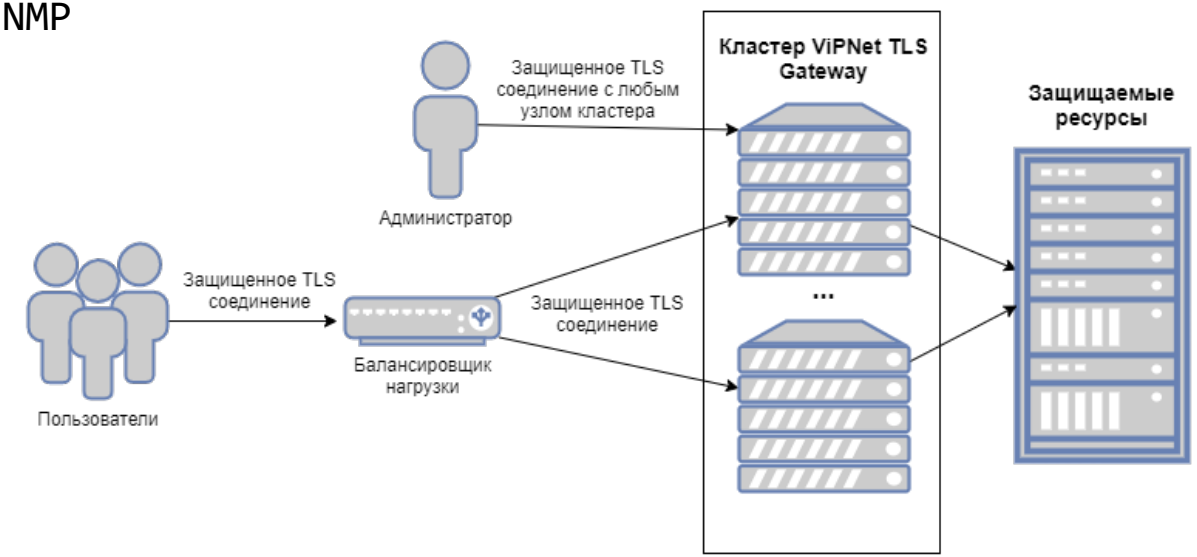
ViPNet TLS Gateway сертифицирован

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

ViPNet TLS Gateway 2

Новые возможности

- Кластер (2 - 64 узла)
- Проверка статусов сертификатов по OCSP
- Мониторинг шлюза по SNMP
- Настройка сети с IPv6

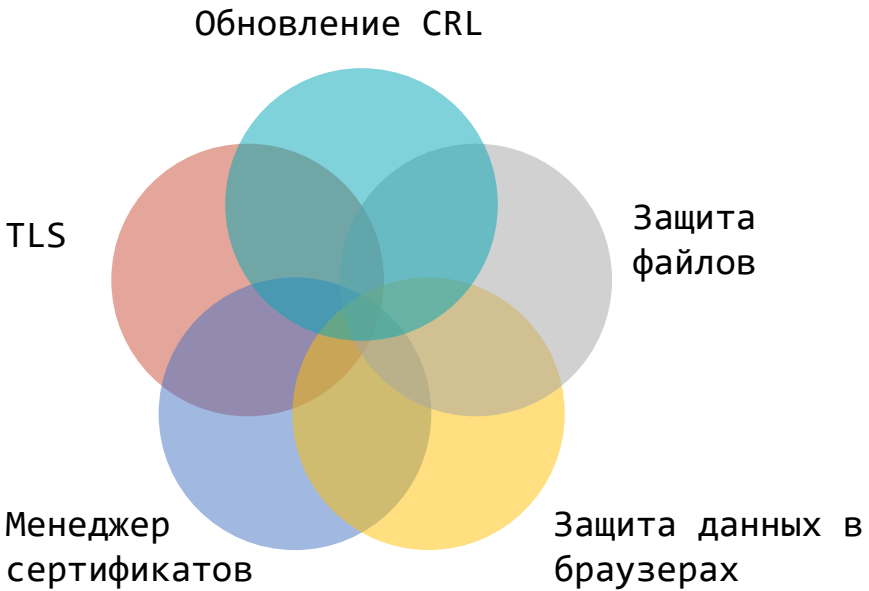


TLS ГОСТ. Клиентский. Мобильный

ViPNet PKI Client

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

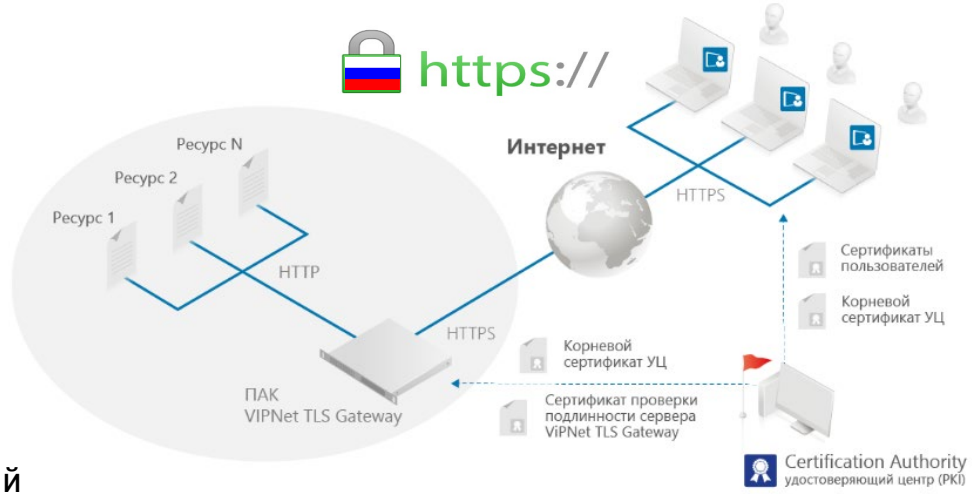
ViPNet PKI Client: TLS Unit

Функции:

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

Преимущества:

- Кроссбраузерный
- совместим с ViPNet TLS Gateway и TLS-шлюзами других производителей



ViPNet PKI Client

Сертификация

- СКЗИ КС1-КС3
- Средство ЭП КС1-КС3
- Может использоваться для реализации функций ЭП в соответствии с Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи»
- Получена нотификация на вывоз

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-3576 от "25" декабря 2018 г.

Действителен до "25" декабря 2021 г.

Выдан Открытому акционерному обществу «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»).

Настоящий сертификат удостоверяет, что изделие ViPNet PKI Client (исполнение 6) в комплектации согласно формуляру ФРКЕ.00175-01 30 01 ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС3, Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС3, 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 области оперативной памяти, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: 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 ОАО «ИнфоТеКС» сертификационных испытаний образца продукции № 905С-000502.

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

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России А.М. Ивашк

Настоящий сертификат внесён в Государственный реестр сертифицированных средств защиты информации 25 декабря 2018 г.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России А.В. Парфено

TLS ГОСТ. Прикладной

Криптографические компоненты

ViPNet CSP

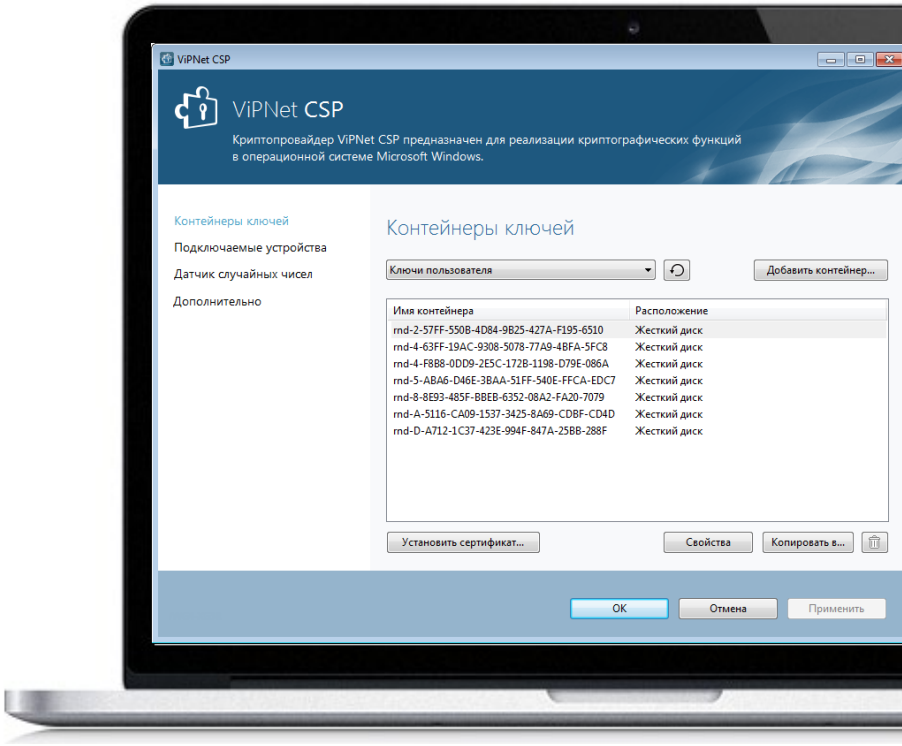
Сертифицированный криптопровайдер (КС1, КС2, КС3)

Работа с ЭП
- ГОСТ Р 34.10-2001*
- ГОСТ Р 34.10-2012

Хэширование
- ГОСТ Р 34.11-94*
- ГОСТ Р 34.11-2012

Шифрование
- ГОСТ 28147-89
- ГОСТ Р 34.12-2015
- ГОСТ Р 34.13-2015

Интерфейсы
- MS CryptoAPI
- MS CNG (BCrypt)
- PKCS#11



Работа с ключами
на внешних устройствах

Бесплатный TLS в браузерах

* В режиме совместимости

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/124-4027* от "*01*" *марта* 2021 г.

Действителен до "*31*" *декабря* 2021 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы» (АО «ИнфоТеКС»).

Настоящий сертификат удостоверяет, что средство криптографической защиты информации (СКЗИ) **ViPNet CSP 4.4** (исполнения 1, 2, 3, 4, 5) в комплектации согласно формуляру ФРКЕ.00106-06 30 01 ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1 (для исполнений 1, 4), класса КС2 (для исполнений 2, 5), класса КС3 (для исполнения 3). Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1 (для исполнений 1, 4), класса КС2 (для исполнений 2, 5), класса КС3 (для исполнения 3) 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, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: 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 №№ 637Д-000501, 637Д-000502.

Безопасность информации обеспечивается при использовании СКЗИ в соответствии с требованиями эксплуатационной документации согласно формуляру ФРКЕ.00106-06 30 01 ФО.

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

infotecs

ViPNet CSP 4.4 сертифицирован ФСБ

ViPNet CSP 4.4 for Windows
КС1, КС2, КС3

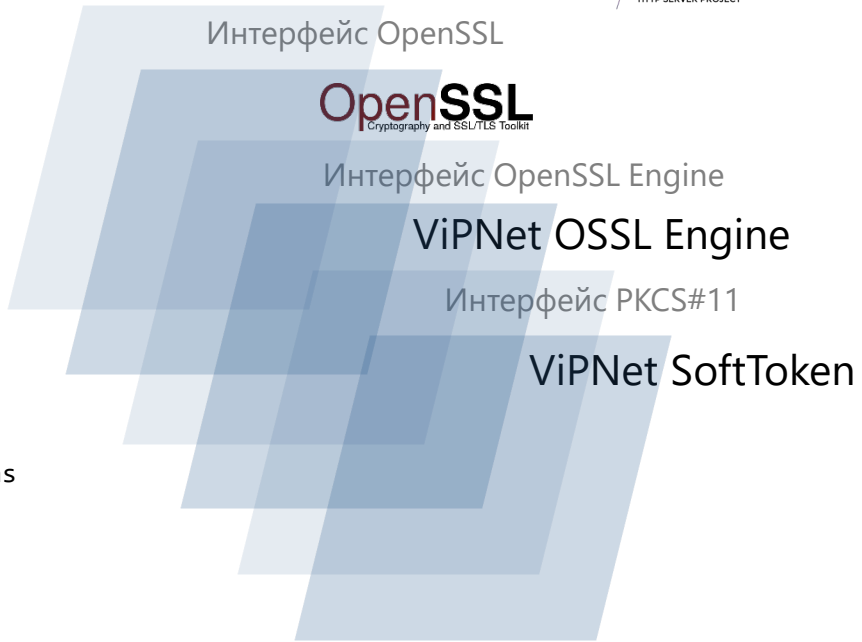
ViPNet CSP 4.4 for Linux
КС1, КС2

ViPNet CSP 4.4 for Linux
КС3 – в процессе сертификации

ViPNet OSSL

Криптобиблиотека на базе OpenSSL (КС1, КС2, КС3)

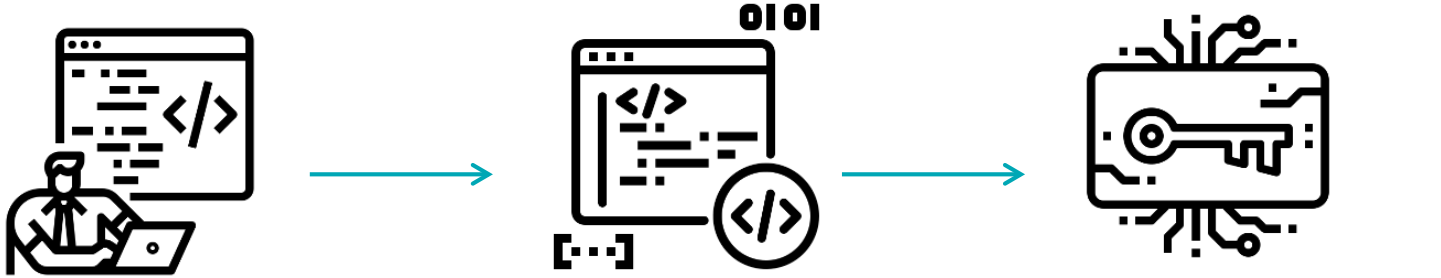
Работа с ЭП	• ГОСТ Р 34.10-2001* • ГОСТ Р 34.10-2012
Хэширование	• ГОСТ Р 34.11-94* • ГОСТ Р 34.11-2012
Шифрование	• ГОСТ 28147-89 • ГОСТ Р 34.12-2015 • ГОСТ Р 34.13-2015
Организация TLS	• TLS 1.2 • TLS 1.3
Интерфейсы	• OpenSSL • PKCS#11 • ViPNet OpenSSL Extensions
Работа с ключами на внешних устройствах	



* В режиме совместимости

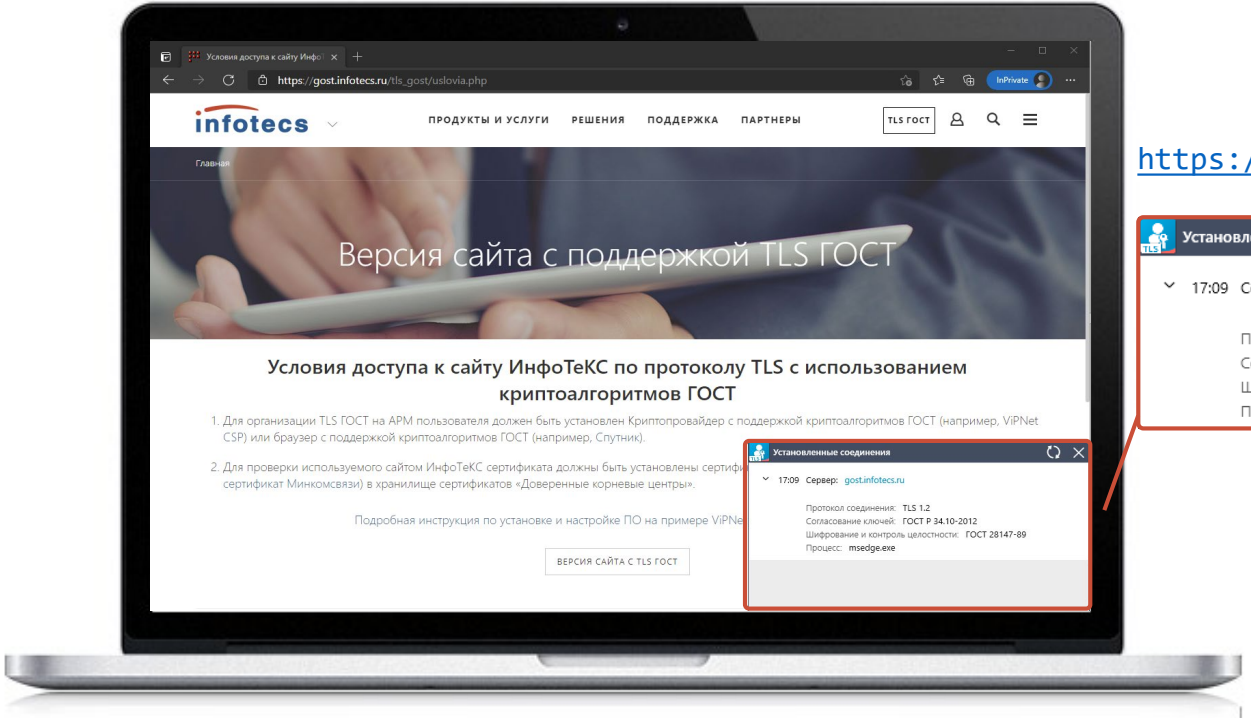
ViPNet OSSL легко встроить

и вызывать криптографические функции

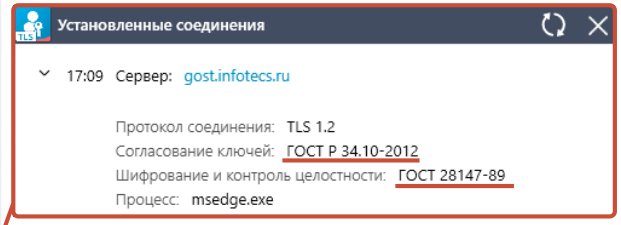


Соблюдение стандартов и встречное тестирование

Подключиться к сайту ИнфоТеКС
по ГОСТ TLS



https://gost.infotecs.ru/

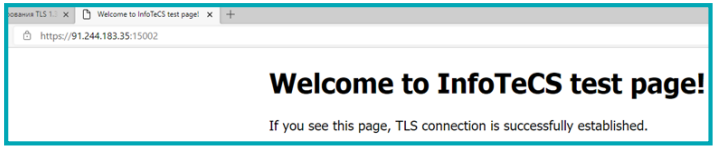


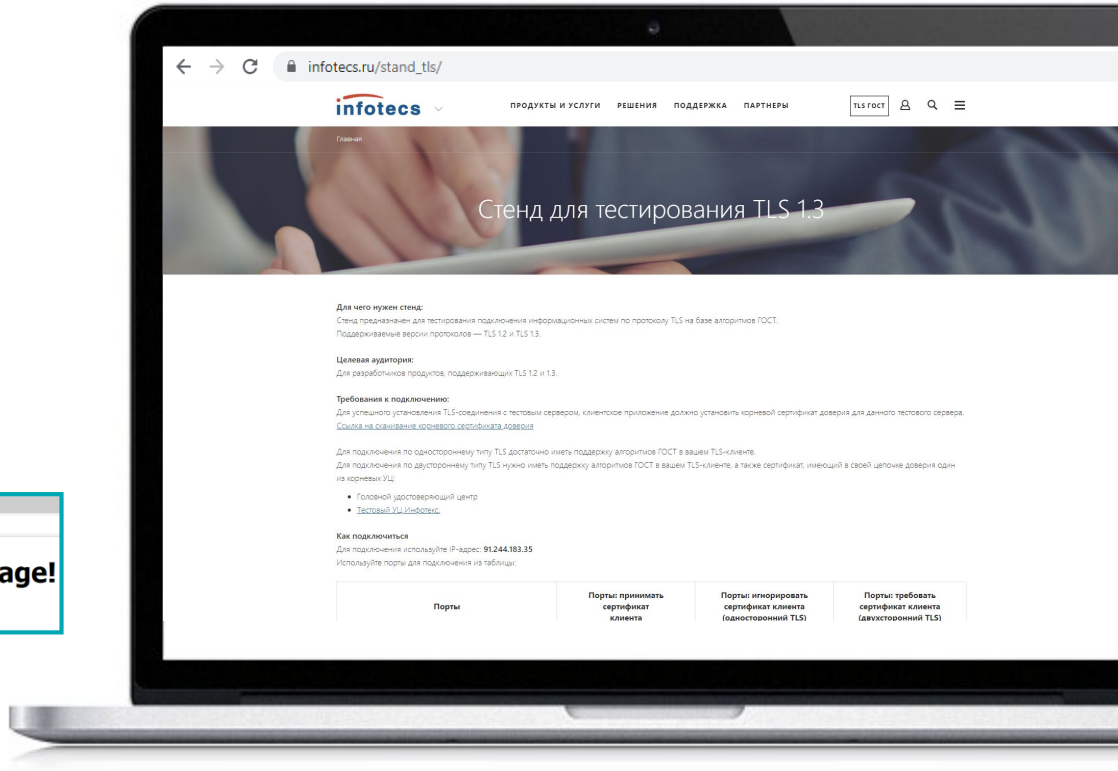
Протестировать TLS 1.2 и 1.3

на нашем стенде

https://infotecs.ru/stand_tls/

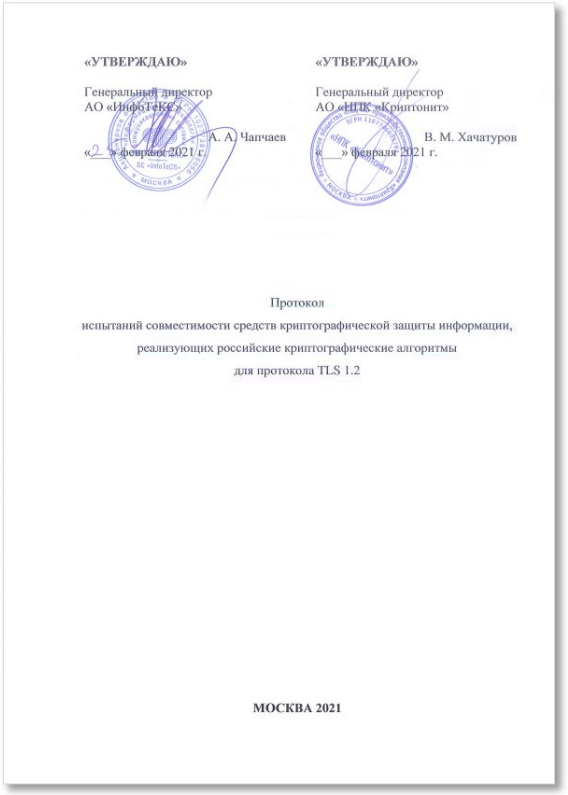
1. Подключиться по IP
2. Выбрать необходимый режим: односторонний/двусторонний
3. Получить сообщение об успешном подключении:





Испытания совместимости в Криптонит

с эталонной реализацией протокола TLS 1.2



«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

TLS Gateway

PKI Client
для Windows

PKI Client
для Linux

Спасибо за внимание!

Еранов Сергей

e-mail: sergey.eranov@infotecs.ru

Подписывайтесь на наши соцсети

@infotecs.ru

@vpninfotecs

@InfoTeCS_Moscow