ТЕХНО 2019 infotecs ФЕСТ

ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ

12.09.2019

ViPNet TLS Gateway - универсальный TLS шлюз с дуальной криптографией

ViPNet TLS Gateway

ТЕХНО 2019 infotecs ФЕСТ

Шлюз безопасности, обеспечивающий защиту каналов по протоколу TLS с использованием алгоритмов ГОСТ и RSA

01

02

**ГОСТ Р 34.10-2001/2012,
ГОСТ Р 34.11-94/2012,
ГОСТ 28147-89**

Поддержка сертификатов, изданных разными УЦ, в т.ч. аккредитованными

03

04

Разные схемы аутентификации для защищаемых ресурсов

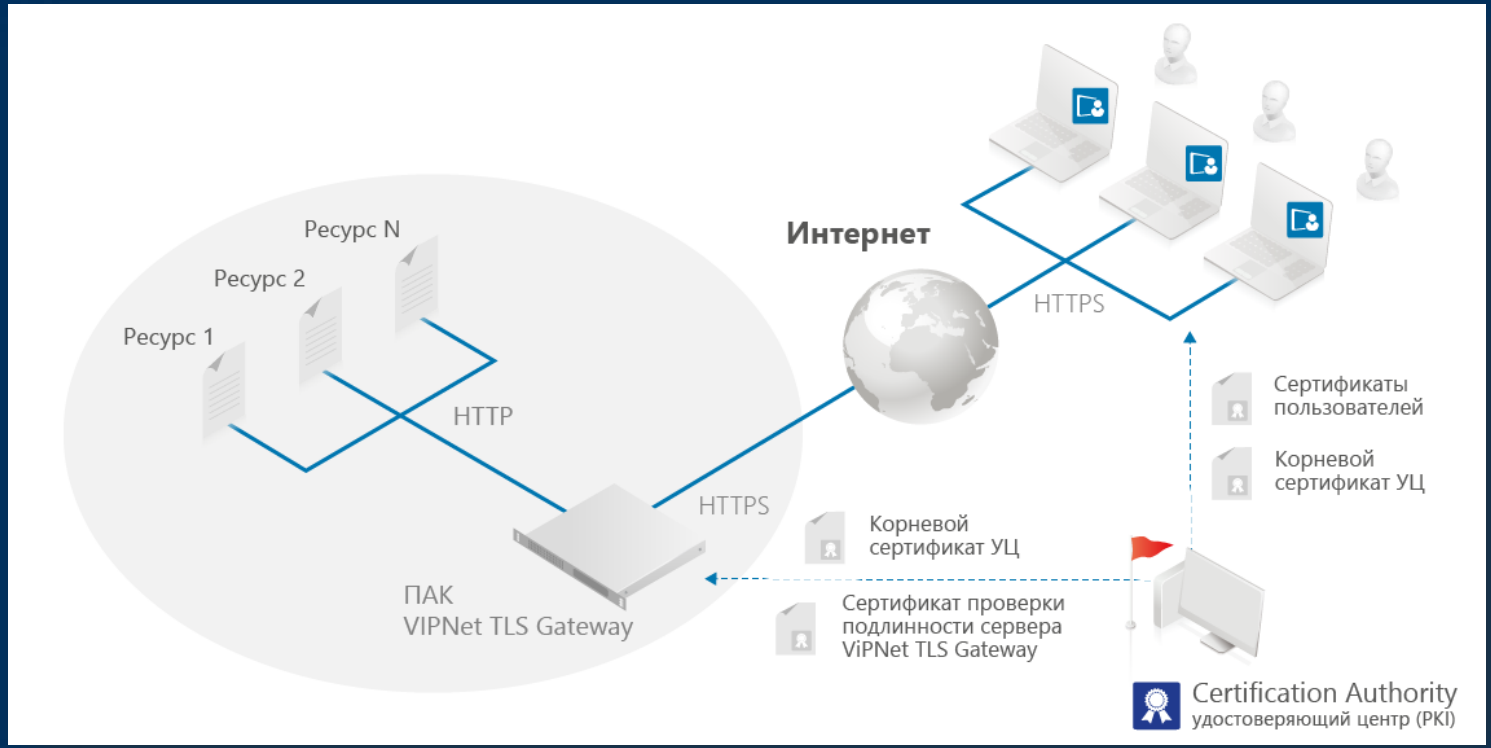
Поддержка политик разграничения доступа

05

06

Исполнения ПАК и ПК

ViPNet TLS Gateway



ViPNet TLS Gateway: исполнения

Название исполнения	TLS VA	TLS 500	TLS 1000	TLS 5000
Предельная пропускная способность в режиме обратного HTTPS-прокси (Мбит/с)	зависит от характеристик аппаратного обеспечения	до 300	до 750	до 3000
Максимальное число одновременных соединений в режиме обратного HTTPS-прокси и TCP-туннеля	зависит от характеристик аппаратного обеспечения	до 4700	до 8900	до 43500

Поддерживаемые виртуальные среды ViPNet TLS Gateway VA

- ✓ Oracle VM VirtualBox 5.0, 5.1, 5.2
- ✓ VMware vSphere ESXi 6.0, 6.5, 6.7;
- ✓ VMware Workstation 14, 15
- ✓ Платформы виртуализации, основанные на Kernel Virtual Machine (KVM)

ViPNet TLS Gateway: сертификация

- ✓ СКЗИ КС3 (три исполнения ПАК)
- ✓ СКЗИ КС1 (исполнение VA)

Зарегистрирован в Реестре российского ПО

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

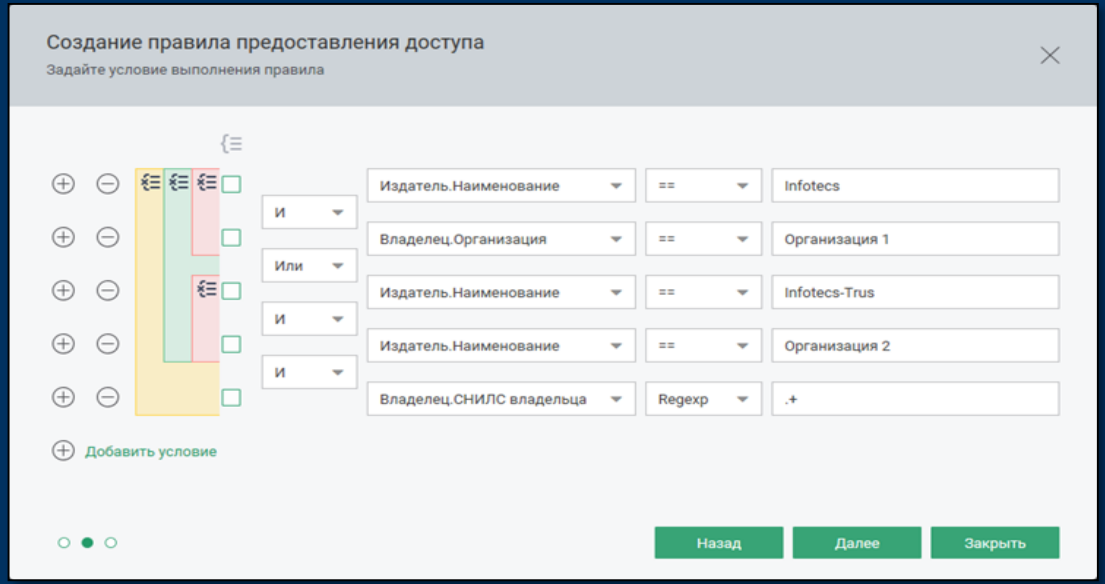
ViPNet TLS Gateway: функциональные возможности

Управление правами доступа к защищаемым ресурсам

- Ведение «белых» и «черных» списков сертификатов
- Обработка входящих запросов
- Создание правил предоставления доступа

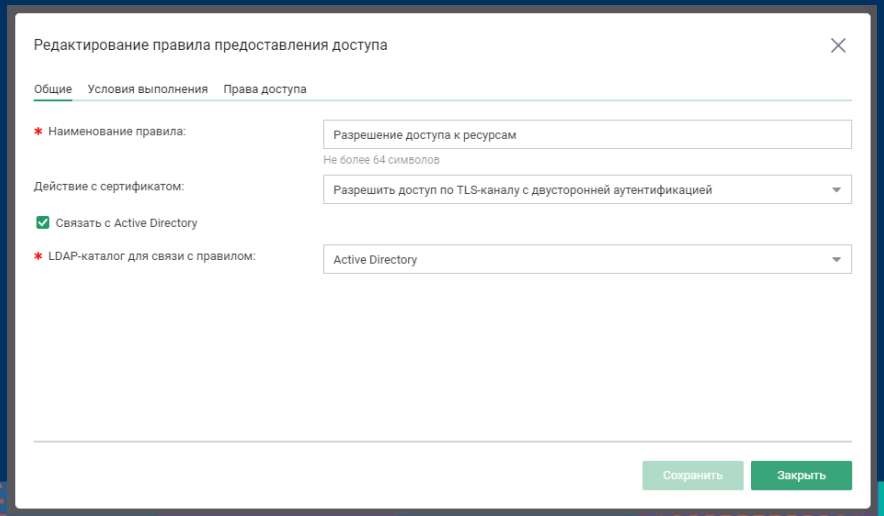
Расширенный конструктор правил доступа или блокировки

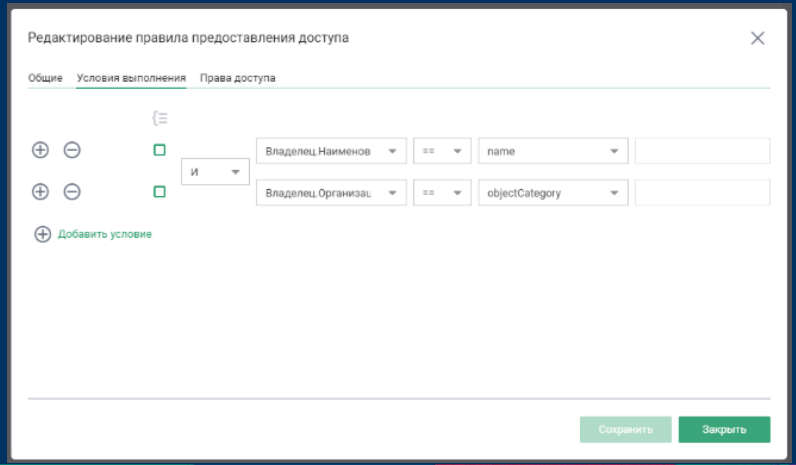
Конструктор составления правил по различным полям сертификатов



Интеграция с LDAP (Active Directory)

- ✓ Возможность подключения нескольких LDAP каталогов. Синхронизация автоматическая и принудительная
- ✓ Поля сертификата сопоставляются с атрибутами LDAP. Поля LDAP доступны в конструкторе





Поддержка различных УЦ

ТЕХНО 2019 infotecs ФЕСТ

Поддержка различных УЦ, в т.ч. всех аккредитованных (xml-список Минкомсвязи)

Автоматическое обновление CRL УЦ

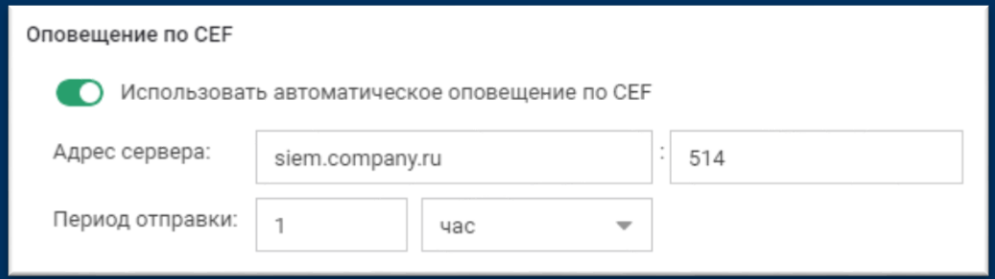
Одновременная поддержка сертификатов с ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012

Мониторинг и аудит

- Индикатор состояния
- Самотестирование (при запуске и 1 раз в сутки)
- Выгрузка служебных журналов и журнала событий через WEB-интерфейс
- Автоматическая передача данных в формате CEF в SIEM-системы

Автоматическая передача данных в формате CEF

- ✓ Передаются данные о:
  - ✓ состоянии TLS Gateway;
  - ✓ действующих лицензионных ограничениях.
- ✓ По запросу список событий можно расширить.

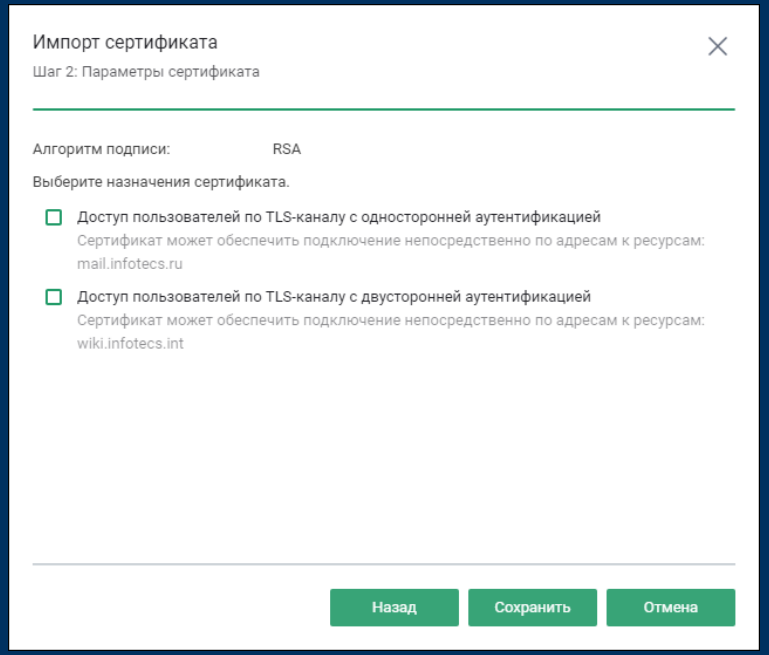


Организация TLS-туннеля для TCP-трафика

- ✓ Совместная работа с ViPNet PKI Client версии 1.3.
- ✓ Для протоколов RDP, SMTP, POP3, IMAP, WebDAV и др.

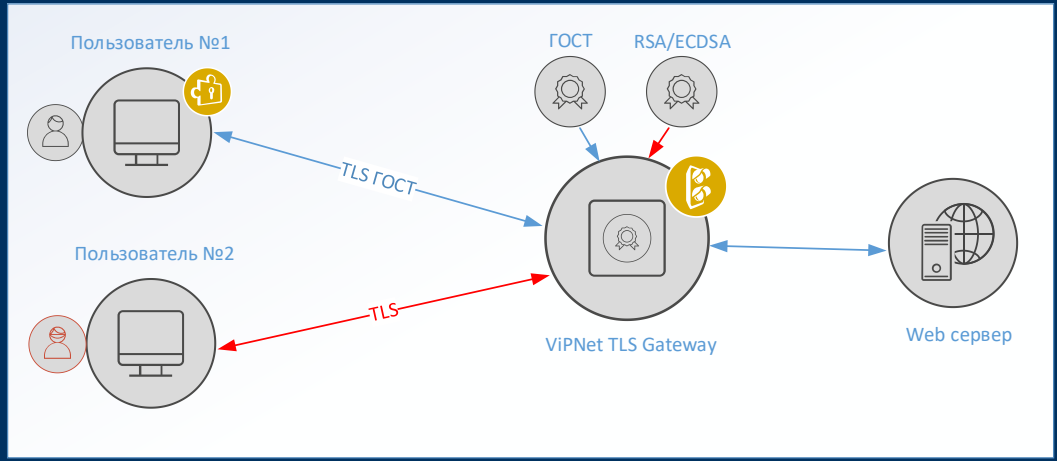
Поддержка RSA и ECDSA

- ✓ Начиная с версии 1.4, для подключения пользователей к ViPNet TLS Gateway могут использоваться сертификаты, сформированные по алгоритмам RSA и ECDSA.
- ✓ Импорт ключей в формате PFX.



ViPNet TLS Gateway: принцип работы в дуальном режиме

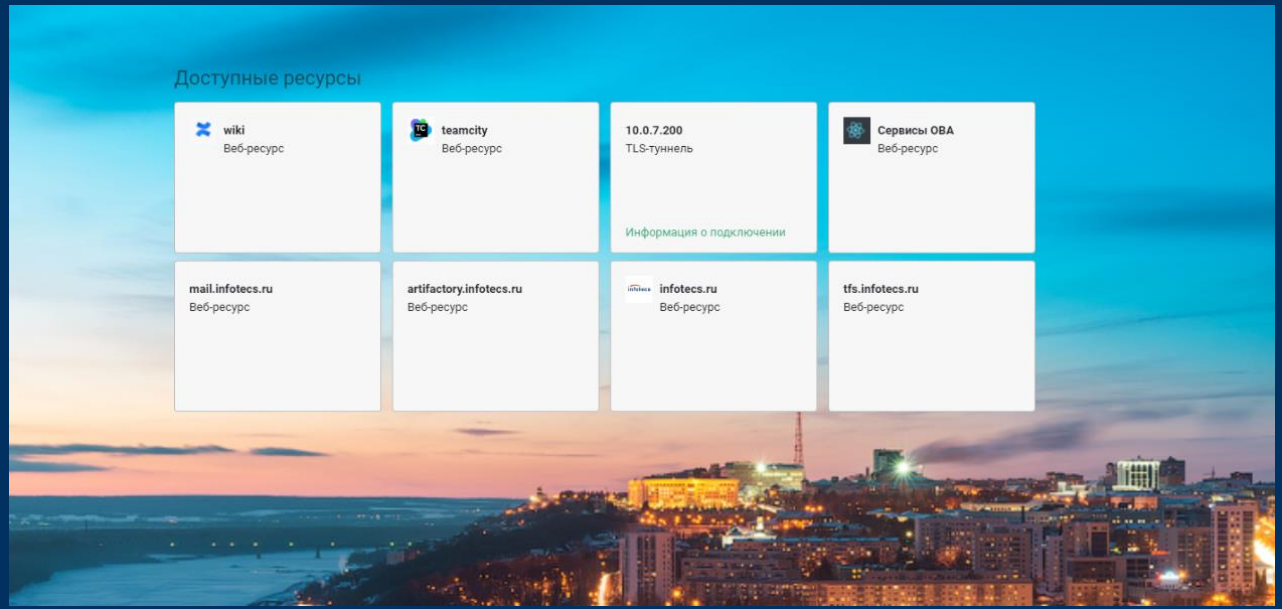
- ✓ Приоритет в работе у ГОСТ-криптоалгоритмов.
- ✓ В случае невозможности организации TLS ГОСТ (например, отсутствует необходимый ГОСТ-криптопровайдер), будет организовано соединение с использованием установленного сертификата RSA/ECDSA.



Подключение клиентов

Вариант I: через пользовательскую страницу (необходимо ввести адрес шлюза).

Пользовательская страница может быть выполнена в корпоративном стиле заказчика

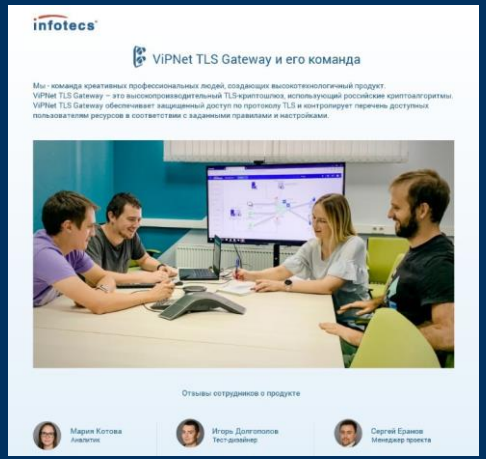


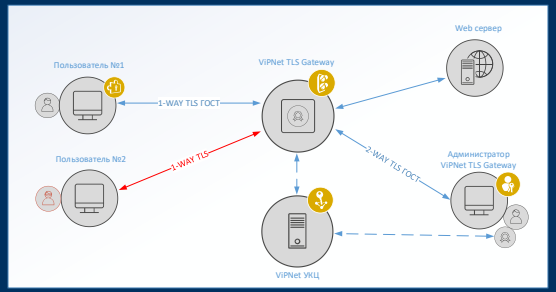
Подключение клиентов

Вариант II: прозрачный (бесшовный) режим (непосредственно по адресам защищаемых ресурсов).

Возможно подключение:

- ✓ только с использованием ГОСТ-криптоалгоритмов
- ✓ комбинация ГОСТ и RSA/ECDSA

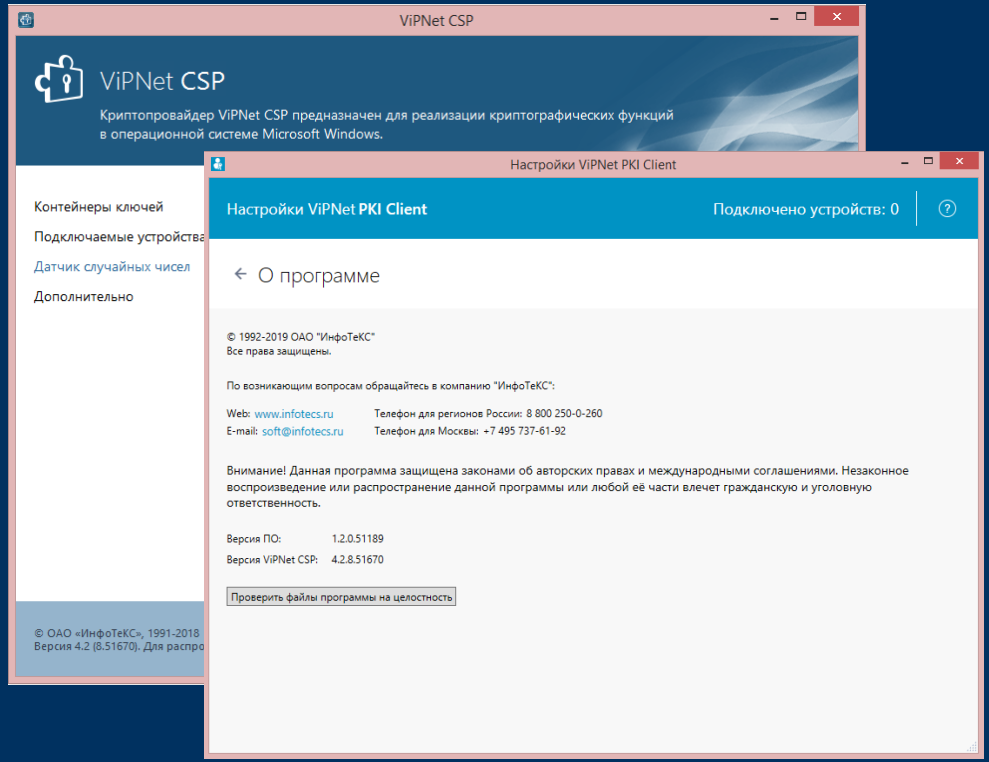




Подключение клиентов

Клиентское ПО:

- ✓ ViPNet CSP;
- ✓ ViPNet PKI Client;
- ✓ любое СКЗИ (например, КриптоПРО CSP, Спутник и т.п.).



ТЕХНО 2019 infotecs Фест

Спасибо
за внимание!