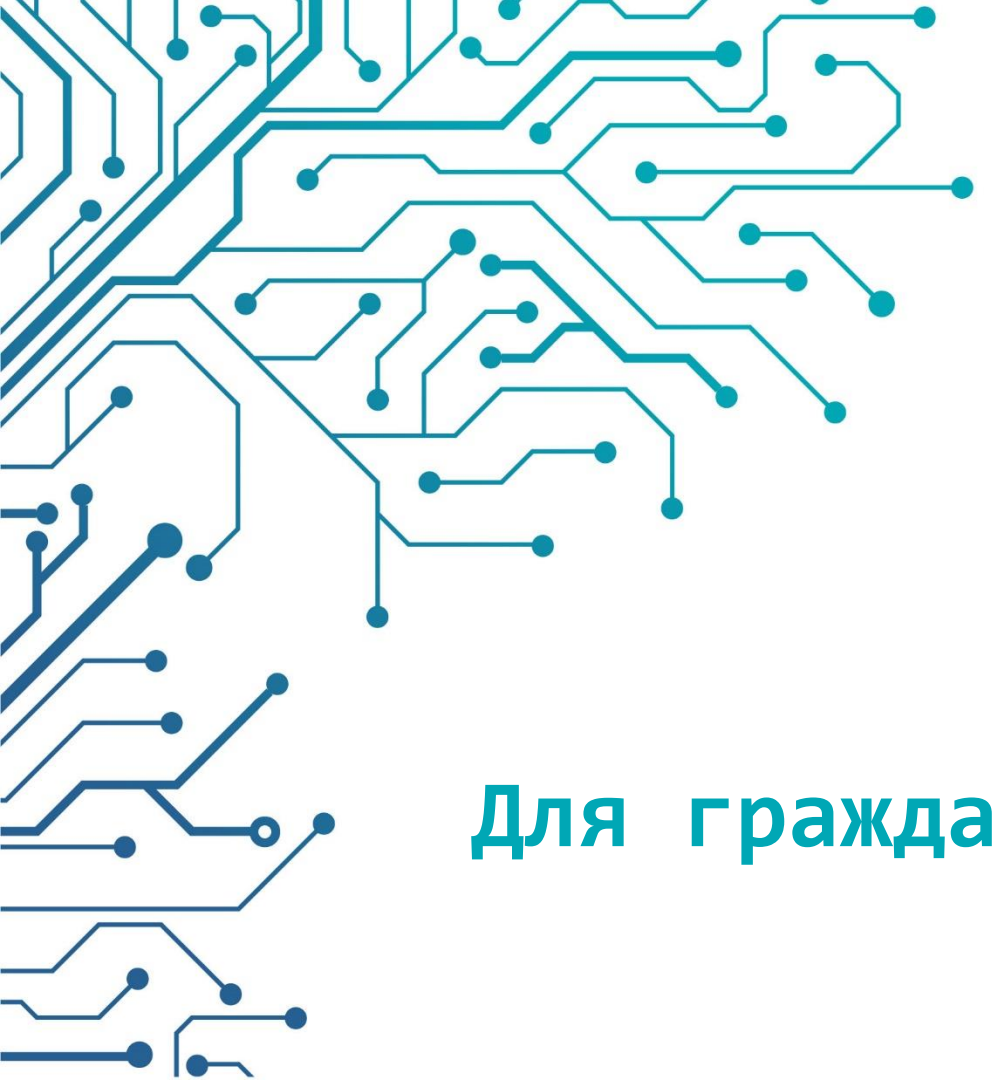
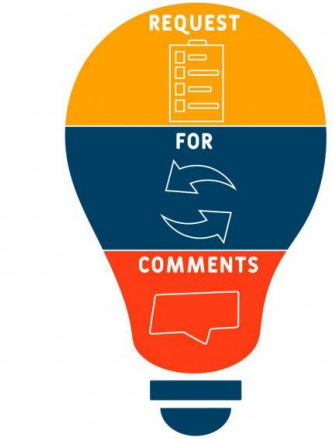


TLS ГОСТ
Для граждан и организаций

Еранов Сергей
АО «ИнфоТеКС»

Зачем нам ГОСТ TLS?

Стандартизация



- ГОСТ
- RFC
- Рекомендации ТК26
- Контрольные примеры

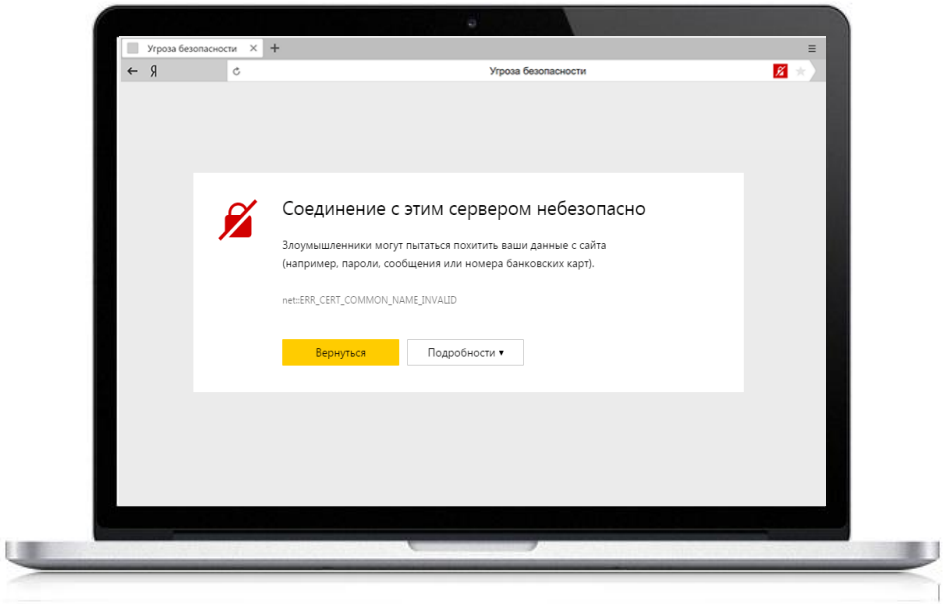
IETF

Результат: Мультивендорность для конечных потребителей

Распространенность

- ✓ Популярность систем с веб-интерфейсом, REST API и т.д.
- ✓ Наличие СКЗИ на рабочих местах для задач ЭП

Независимость и безопасность



Какие возникают проблемы

Отзыв сертификатов со стороны зарубежных УЦ

Как решаются эти проблемы

Используется УЦ Минкомсвязи на NIST-алгоритмах

Ведется запуск **Национального удостоверяющего центра**

Проблемы и вопросы

Где получить сертификат сервера

Где брать сертификат для ГОСТ TLS?

Минцифры выдает RSA-сертификаты для организаций

Корневой скачивается по https на сертификате Sectigo

Кому выдан:	*.gosuslugi.ru
Кем выдан:	Sectigo RSA Domain Validation Secure Server CA

Получение ГОСТ сертификата не встроено в инфраструктуру провайдеров хостинга

Если я – физлицо или ИП, где мне взять сертификат для своего сайта?

Как настроить TLS ГОСТ на сервере

Провайдеры хостинга сайтов – не предлагают такой услуги

VPS/VDS провайдеры – не предлагают готового решения

NGINX + APACHE HTTP SERVER PROJECT + OpenSSL Cryptography and SSL/TLS Toolkit

Требует квалификации

Только аутентификация и защита канала

Нет дуального режима «из коробки»

** Вопросы юридического характера не рассматриваем*

Где пользователю взять СКЗИ?

Что пользователю нужно?

- Чтобы работало
- Бесплатно
- Просто
- Разные платформы
- Разные браузеры

Проблемы пользователей

- Установка корневых
- Обновление CRL
- Поддержка различных ОС
- Возможность работы в любимом браузере

TLS ГОСТ. Серверный

ViPNet TLS Gateway

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

Отдаем на полгода бесплатно

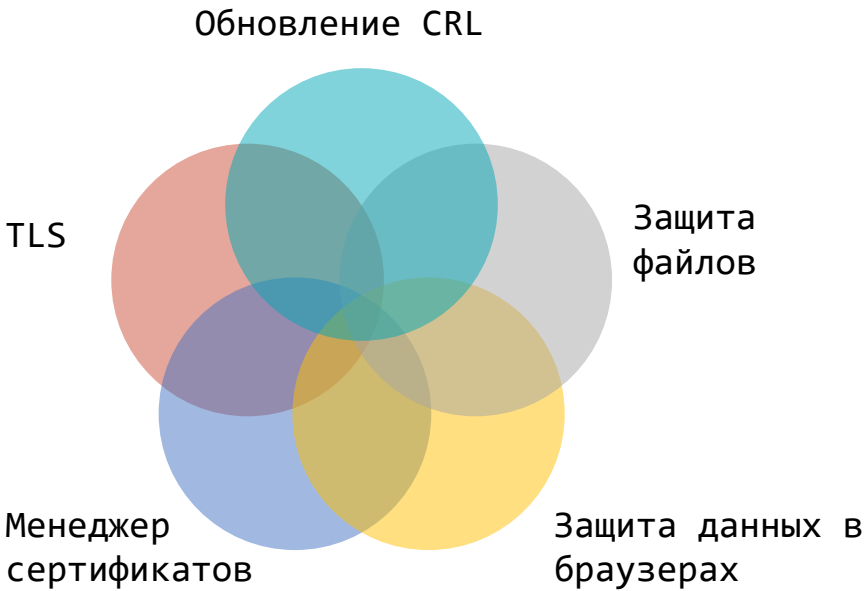
- TLS Gateway VA
- Бесплатная лицензия на полгода

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
  - Tunnel 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

Преимущества:

- Кроссбраузерный

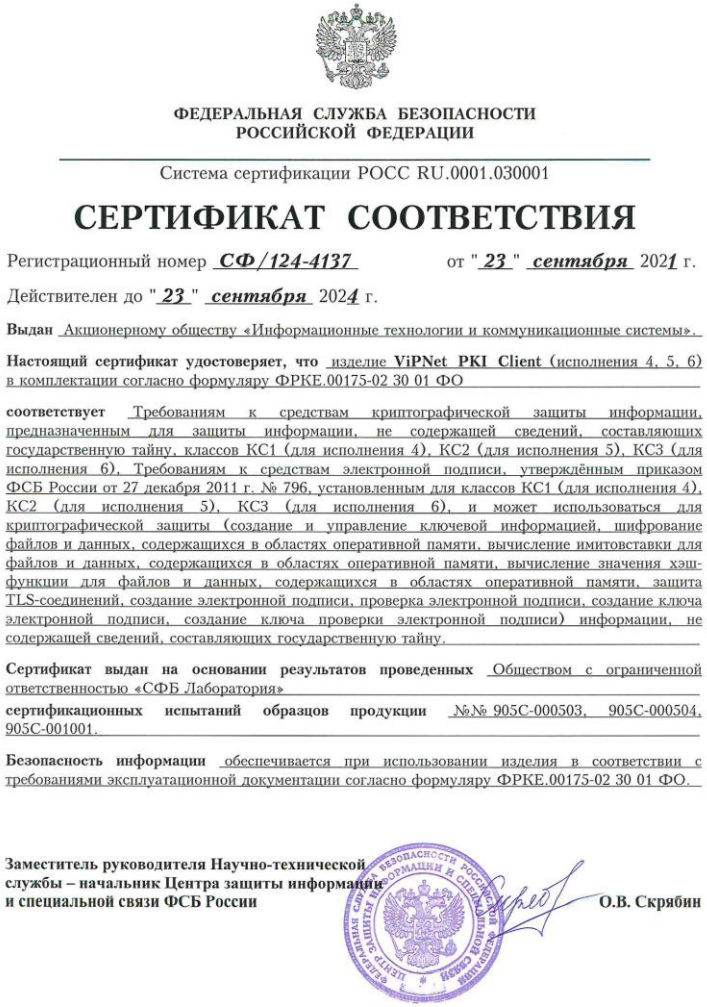
- Работа в мобильных браузерах

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

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»

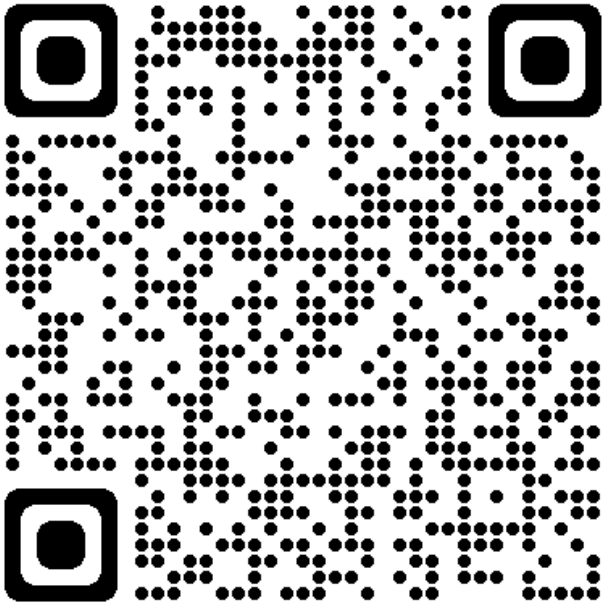
сертификационных испытаний образцов продукции №№ 905С-000503, 905С-000504, 905С-001001.

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
- Скоро! Односторонний TLS бесплатно



TLS ГОСТ. Клиентский

Криптопровайдер

ViPNet CSP

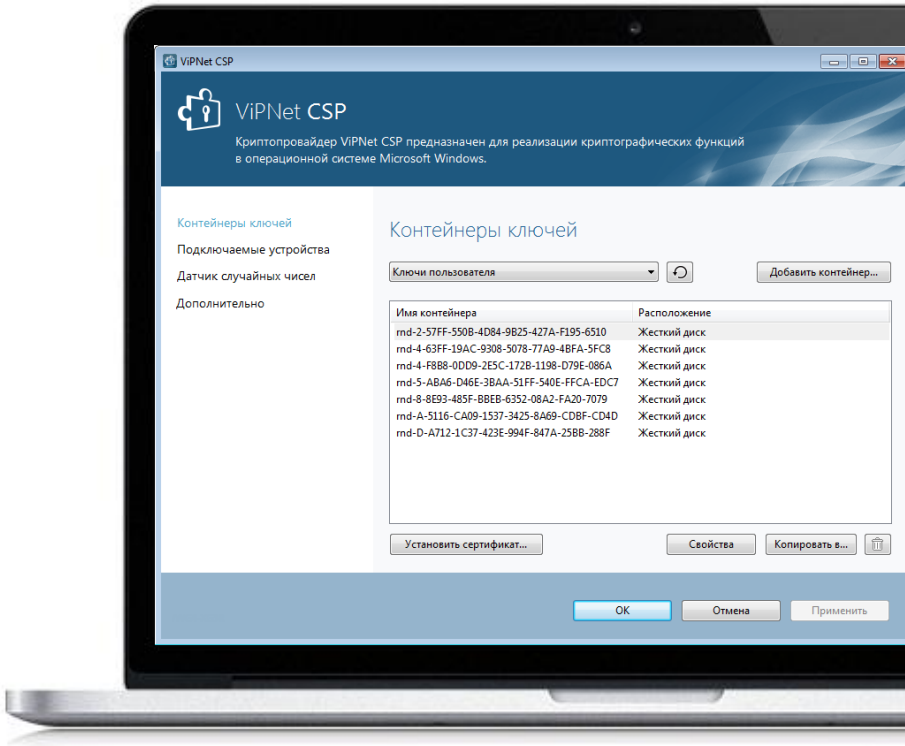
Сертифицированный криптопровайдер (КС1, КС2, КС3)

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

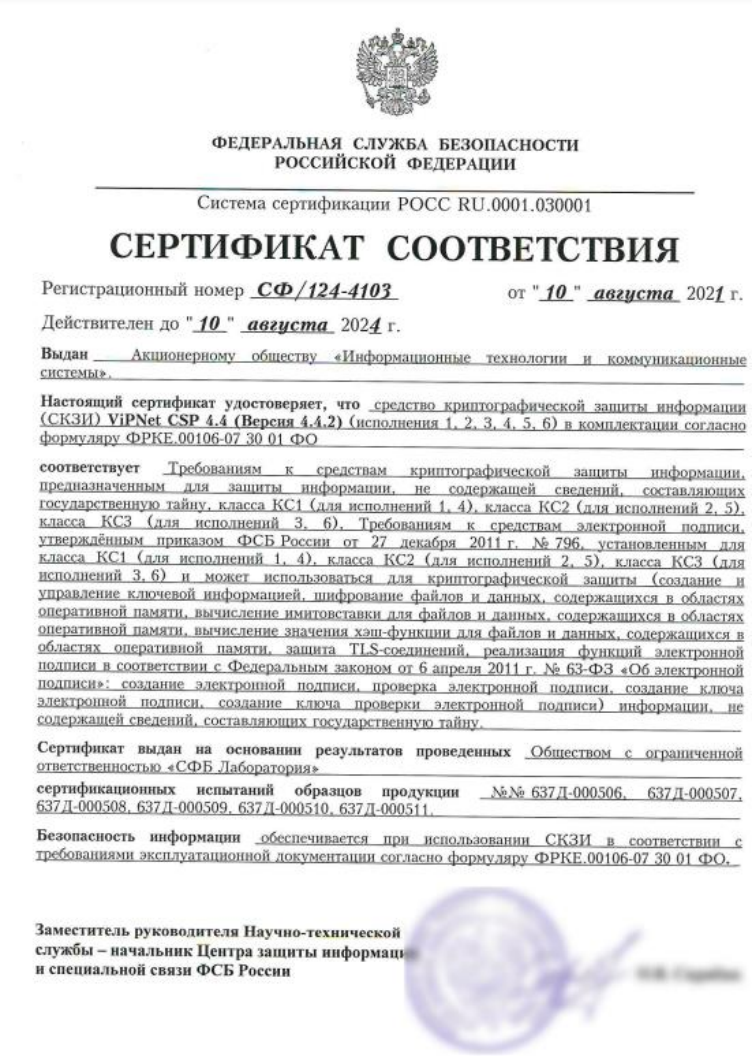
Интерфейсы
- MS CryptoAPI
- MS CNG (BCrypt)
- PKCS#11



Работа с ключами
на внешних устройствах

Бесплатный TLS в браузере

* В режиме совместимости



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/124-4103* от "*10*" *августа* 2021 г.

Действителен до "*10*" *августа* 2024 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что средство криптографической защиты информации (СКЗИ) **ViPNet CSP 4.4 (Версия 4.4.2)** (исполнения 1, 2, 3, 4, 5, 6) в комплектации согласно формуляру ФРКЕ.00106-07 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 исполнений 3, 6), 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 исполнений 3, 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, 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-000506, 637Д-000507, 637Д-000508, 637Д-000509, 637Д-000510, 637Д-000511.

Безопасность информации обеспечивается при использовании СКЗИ в соответствии с требованиями эксплуатационной документации согласно формуляру ФРКЕ.00106-07 30 01 ФО.

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

ViPNet CSP 4.4 сертифицирован ФСБ

Спасибо за внимание!

Еранов Сергей

e-mail: sergey.eranov@infotecs.ru

Подписывайтесь на наши соцсети

https://t.me/infotecs_news

https://vk.com/infotecs_news