КриптоПро NGate. Решение прикладных задач с помощью уникального TLS-шлюза удаленного доступа и VPN

Павел Луцик,
директор по продажам и развитию бизнеса
ООО «КРИПТО-ПРО»

Тренды

КРИПТОПРО

- Централизация всех видов доступа
- Увеличение количества используемых устройств
- Необходимость непрерывного доступа
- Постоянный рост числа сотрудников и партнеров, которым необходим удаленный доступ

Законодательство. ЕБС

КРИПТОПРО

- NGate входит в состав нескольких типовых и частных решений;
- Используется для **криптографической защиты** БПДн, передаваемых между банковскими отделениями (при сборе БПДн) и для **аутентификации** граждан (при получении услуг)
- **Только NGate** удовлетворяет 149-ФЗ (с изм. 482-ФЗ) и 4-МР в части удаленной идентификации в ЕБС:
  - ✓ Наличие необходимых **сертификатов ФСБ** России
  - ✓ Поддержка **ГОСТ и не ГОСТ**

Законодательство. ПДн/ГИС (21/17 приказ ФСТЭК)

КРИПТОПРО

- **Управление доступом (УПД)**
  - ✓ реализация защищенного удаленного доступа (УД) (УПД.13)
- **Защита ИС и передачи данных (ЗИС)**
  - ✓ обеспечение защиты ПДн при передаче (ЗИС.3)
- **Идентификация и аутентификация (ИАФ)**
  - ✓ Идентификация и аутентификация пользователей (работников) (ИАФ.1)
  - ✓ Защита обратной связи при вводе аутентификационной информации (ИАФ.5)
  - ✓ Идентификация и аутентификация внешних пользователей (ИАФ.6)

Законодательство. КИИ (239 приказ ФСТЭК)

- **Управление доступом (УПД)**
  - ✓ реализация защищенного УД (УПД.13)
  - ✓ контроль доступа из внешних ИС (УПД.14)
- **Защита ИС и ее компонентов (ЗИС)**
  - ✓ защита информации при ее передаче по каналам связи (ЗИС.19)
- **Идентификация и аутентификация (ИАФ)**
  - ✓ идентификация и аутентификация пользователей и процессов (ИАФ.1)
  - ✓ идентификация и аутентификация внешних пользователей (ИАФ.5)
  - ✓ двусторонняя аутентификация (ИАФ.6)
  - ✓ защита аутентификационной информации при передаче (ИАФ.7)
- **не допускается наличие УД напрямую к ЗОКИИ со стороны не работников (п.31)**
- **стойкость к санкциям (п.31)**
- **поддержка от производителя (п.31)**

Бизнес-потребности

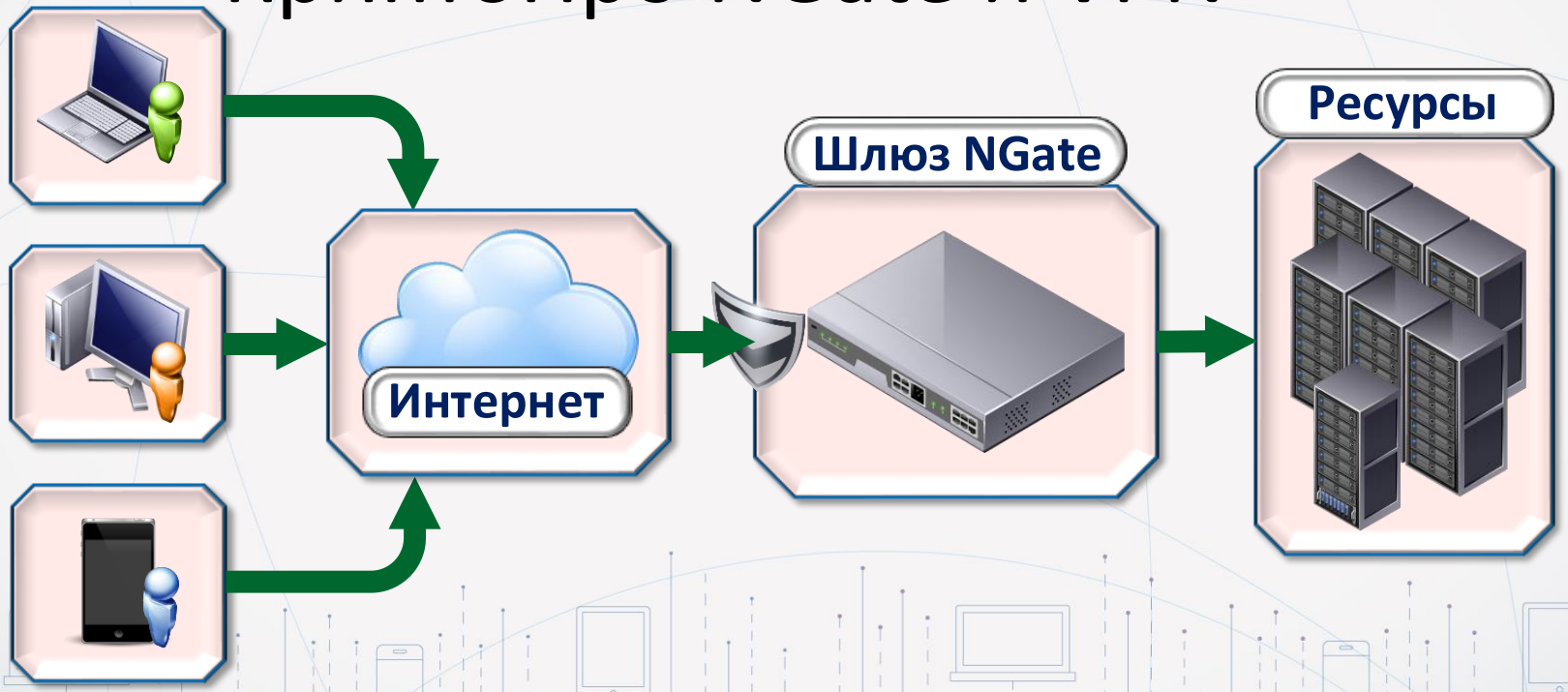
Удаленный доступ к корпоративным ресурсам с ПК и тонких клиентов

- Веб-ресурсы
  - ✓ Почта (OWA), корпоративный портал, система обмена знаниями (Jive) и др.
  - ✓ Веб-консоли управления различных ИТ/ИБ систем
- Произвольные ресурсы
  - ✓ Удаленный рабочий стол, файловые ресурсы, офисное ПО, 1С и др.

Предоставление электронных услуг через защищенный канал:

- Порталы государственных услуг
- Сдача электронной отчетности
- Электронные торговые площадки
- Дистанционное банковское обслуживание
- Электронный документооборот

Шлюз удаленного доступа КриптоПро NGate и VPN



Основа NGate - КриптоПро CSP

- 18 лет развития продукта (КриптоПро CSP)
- Полностью самостоятельная реализация криптографии
- Рекордные скорости реализации российской криптографии
- Более 15 лет работы над «TLS с ГОСТ»

Зачем нужен NGate?

КРИПТОПРО

- Доступ к веб-приложениям по TLS с ГОСТ/не ГОСТ
- Доступ к произвольным ресурсам по VPN
- Контроль доступа к приложениям
- Снятие с приложений лишней нагрузки
- Исключение необходимости встраивания ГОСТа

Сертификация

КРИПТОПРО

- Сертификаты ФСБ по **КС1, КС2, КС3**
- Поддержка работы в **виртуальной** среде
- Поддержка в т.ч. **iOS, Android**
- Есть **экспортный** вариант

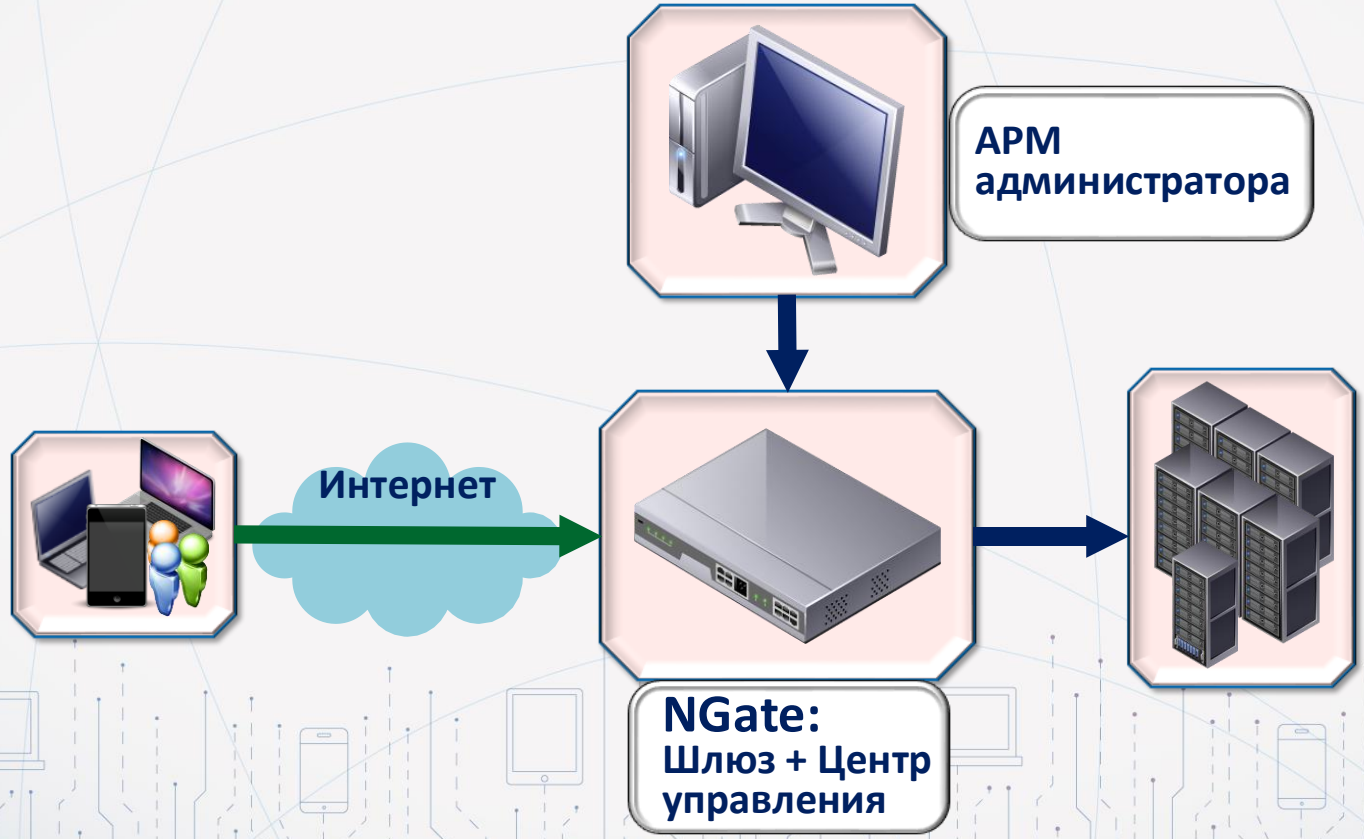
Компоненты

КРИПТОПРО

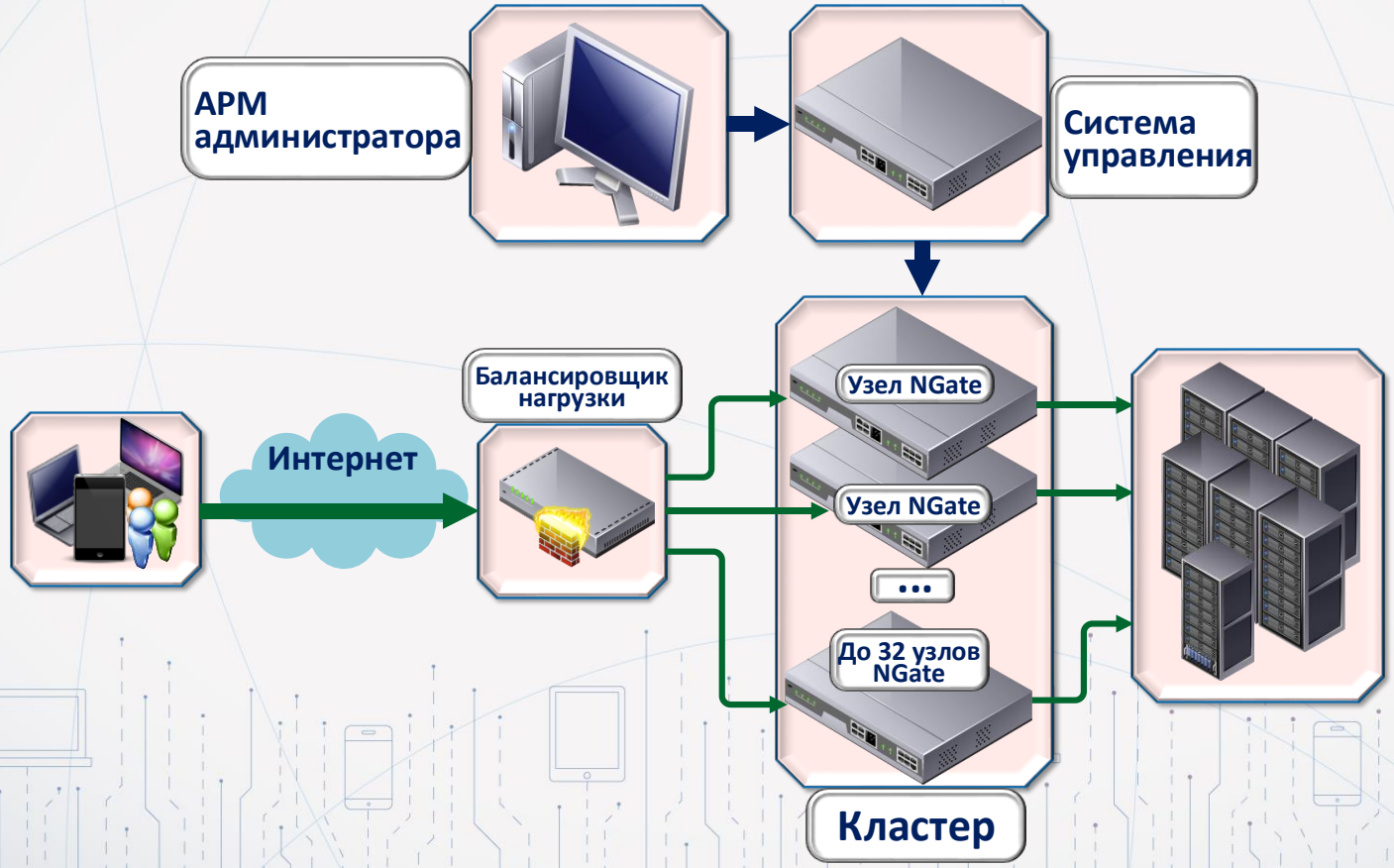
- Шлюз
- Система управления
- VPN-клиент

Схемы внедрения. Всё в одном

КРИПТОПРО



Схемы внедрения. Кластер



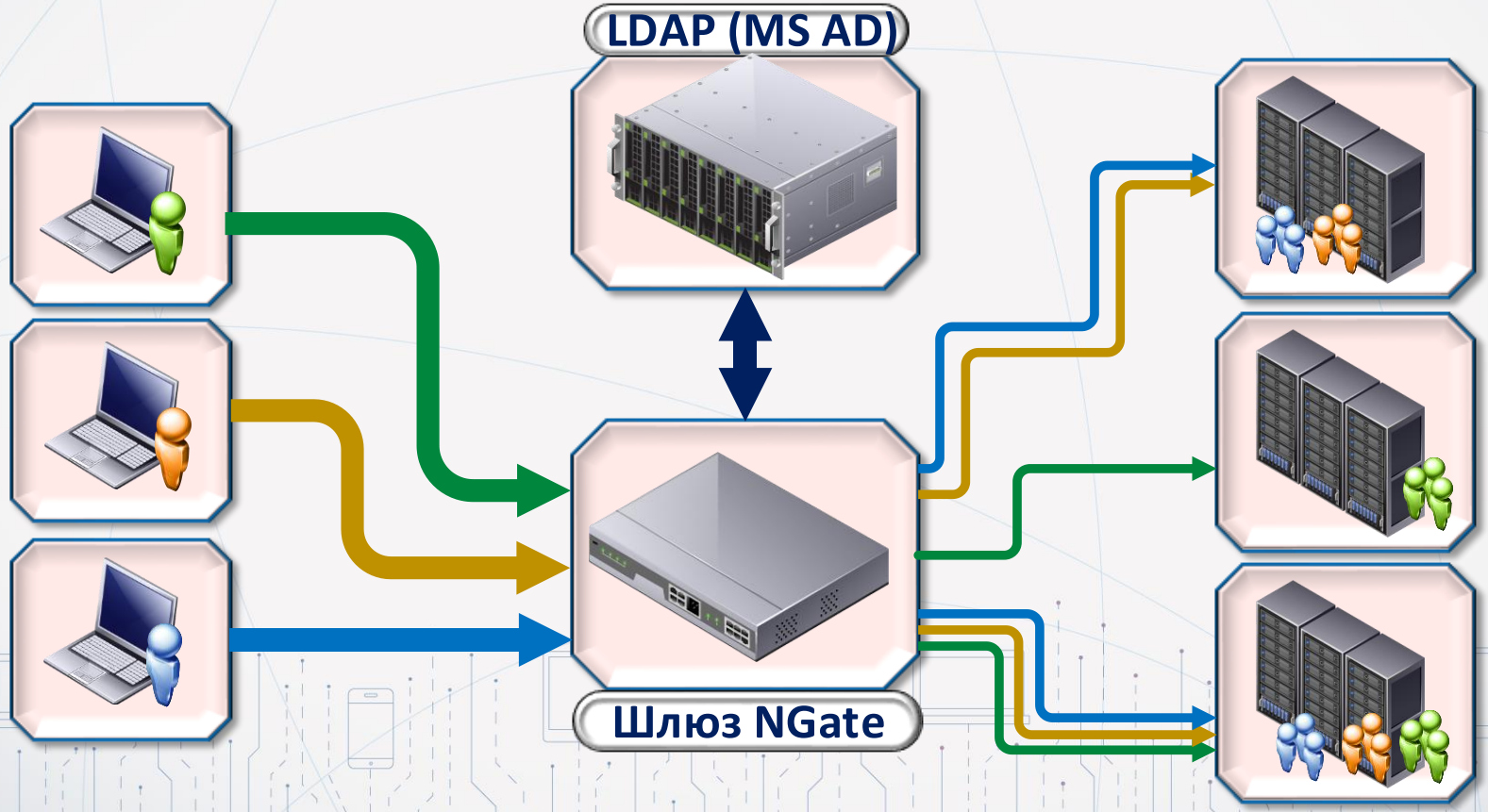
Режимы работы

- TLS-терминатор
- Портальный доступ
- VPN доступ

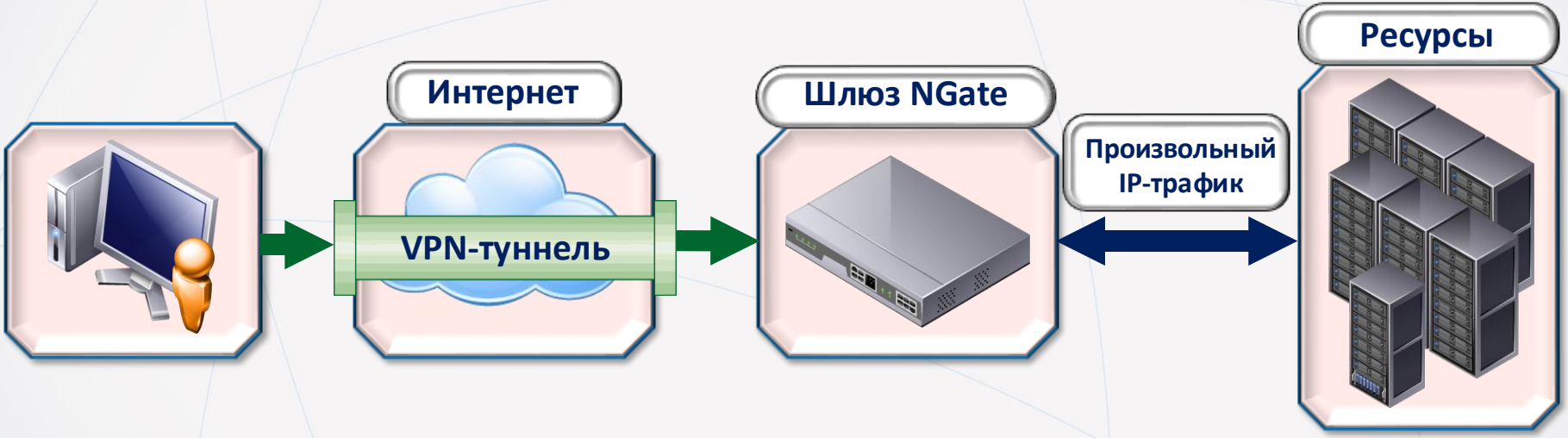
TLS-терминатор

Портальный доступ

КРИПТОПРО



VPN доступ



- Клиент под все платформы
- Поддержка VLAN
- Поддержка таблиц маршрутизации

Методы аутентификации

КРИПТОПРО

- Без аутентификации (прозрачно)
- Логин/пароль (MS AD/LDAP)
- Сертификат (валидность и/или поля)
- Сертификат в LDAP/MS AD
- UPN в MS AD
- OTP через Radius

Планы на будущее

КРИПТОПРО

- IPsec
- TLS с «Кузнечиком» и «Магмой»
- Доступ к ГосСОПКА и СМЭВ

Основные преимущества NGate

- Выполнение требований регуляторов
- Единственный на рынке полноценный сертифицированный TLS-VPN
- Поддержка ГОСТ и зарубежных алгоритмов
- Поддержка различных режимов работы и методов аутентификации
- Наличие клиентов под все популярные платформы
- Высокая скорость и масштабируемость
- Демократичная стоимость

Классическая и «облачная» ЭП. Особенности

КРИПТОПРО

Классическая ЭП

- Носитель закрытого ключа персональный (токен, смарт карта, реестр)
- Криптопровайдер – на рабочем месте пользователя
- Средство ЭП – на рабочем месте пользователя

«Облачная» ЭП

- Носитель закрытого ключа – централизованное защищенное хранилище + двухфакторная аутентификация
- Криптопровайдер – централизованный (HSM)
- Средство ЭП – централизованное (поддержка основных форматов подписи, возможность интеграции)

Преимущества «облачной» ЭП

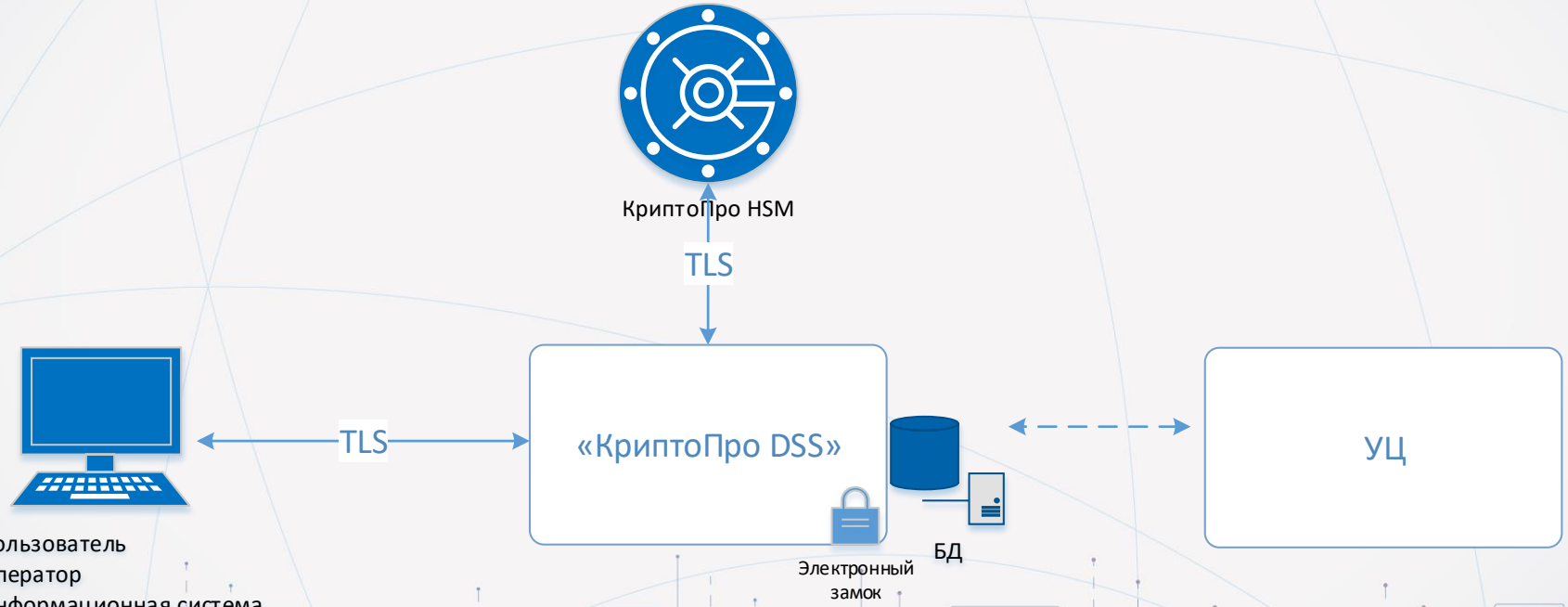
КРИПТОПРО

- Возможно использовать на любых мобильных телефонах, планшетах и др. устройствах, имеющих доступ в Интернет
- Снижение стоимости владения и развертывания инфраструктуры ЭП (экономия в разы)
- Доступность, как стоимостная, так и технологическая, т.к. не требует обучения для использования
- Простое встраивание функционала подписания и шифрования в существующие информационные системы
- Снижение риска компрометации ключей пользователей за счёт их централизованного защищённого хранения

Сервис «облачной» подписи ПАК «КриптоПро DSS»

- Централизованное защищенное хранение ключей
- Создание ЭП с использованием ПАКМ КриптоПро HSM

Схема взаимодействия с КриптоПро DSS



- Пользователь
- Оператор
- Информационная система

Соответствие уровням защищенности

Российская система требований к СКЗИ/СЭП

- Работа с ключами пользователей – уровень КВ/КВ2.
- Управление пользователями и их аутентификацией – уровень КС3.
- Средства аутентификации – уровни КС1, КС2, КС3.

Требования Европейского комитета по стандартизации (CEN) к серверной подписи

- CEN/TS 419241, выполнены все требования высшего уровня (QES, уровень 2).

Безопасные механизмы аутентификации в КриптоПро DSS

КРИПТОПРО

«Сертифицированные» ФСБ России методы аутентификации

1. SSL-ГОСТ с использованием сертификатов X.509
2. SSL-ГОСТ с использованием логина и пароля
3. Криптоапплет на SIM-карте
4. Приложение myDSS для смартфона

Квалифицированная ЭП

Иные методы аутентификации, реализованные в DSS

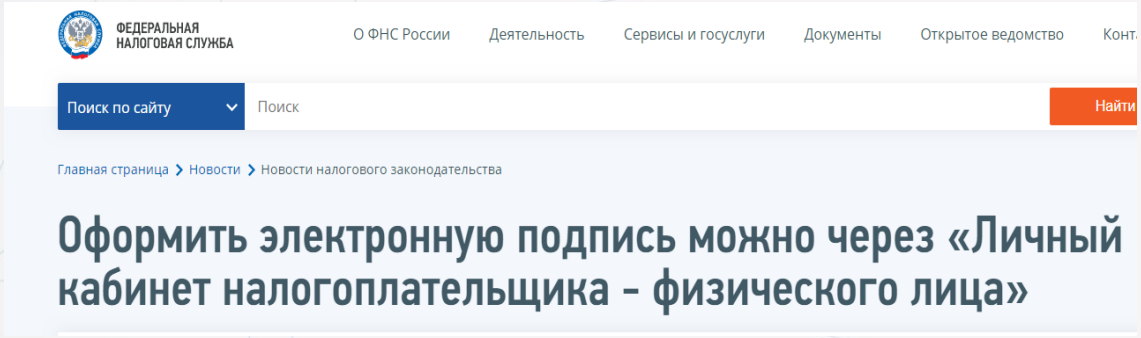
1. SSO
2. Генератор OTP (физический токен)
3. OTP-via-SMS
4. OTP-via-EMAIL

Неквалифицированная ЭП

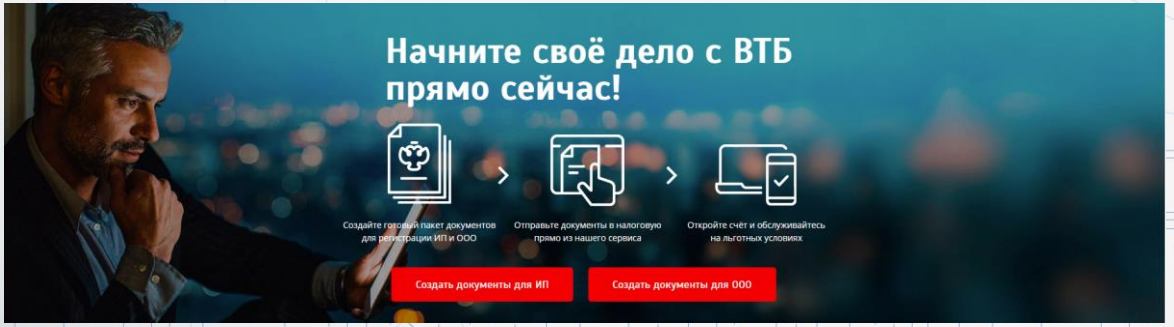
Опыт реализации интеграционных проектов

КРИПТОПРО

ФНС России



ВТБ



КриптоПро myDSS

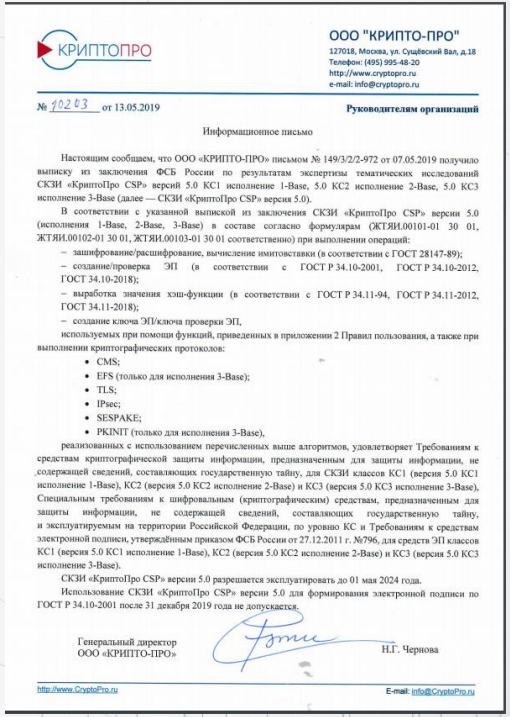
- ✓ Совместная разработка компаний КРИПТО-ПРО и SafeTech
- ✓ Технология PayControl
- ✓ Строгая аутентификация пользователей
- ✓ Безопасное online-взаимодействие
- ✓ Отображение документа
- ✓ Подтверждение операций с помощью функции HMAC_GOSTR3411_2012_256

Загрузите в App Store

ДОСТУПНО В Google Play

КриптоПро CSP 5.0: Облачный провайдер

- Подписано заключение ФСБ России
- Добавлена поддержка платформы Android
- Работа с неизвлекаемыми ключами (ФКН)
- «Облачный» токен – технология Cloud CSP



КРИПТОПРО

ООО "КРИПТО-ПРО"
127018, Москва, ул. Сущёвский Вал, д.18
Телефон: (495) 995-48-20
http://www.cryptopro.ru
e-mail: info@cryptopro.ru

№ 92 03 от 13.05.2019

Руководителям организаций

Информационное письмо

Настоящим сообщаем, что ООО «КРИПТО-ПРО» письмом № 149/3/2/2-972 от 07.05.2019 получило выписку из заключения ФСБ России по результатам экспертизы тематических исследований СКЗИ «КриптоПро CSP» версий 5.0 КС1 исполнение 1-Base, 5.0 КС2 исполнение 2-Base, 5.0 КС3 исполнение 3-Base (далее — СКЗИ «КриптоПро CSP» версии 5.0).

В соответствии с указанной выпиской из заключения СКЗИ «КриптоПро CSP» версии 5.0 (исполнения 1-Base, 2-Base, 3-Base) в составе согласно формулярам (ЖТЯИ.00101-01 30 01, ЖТЯИ.00102-01 30 01, ЖТЯИ.00103-01 30 01 соответственно) при выполнении операций:

– зашифрование/расшифрование, вычисление имитовставки (в соответствии с ГОСТ 28147-89);
– создание/проверка ЭП (в соответствии с ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ 34.10-2018);
– выработка значения хэш-функции (в соответствии с ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012, ГОСТ 34.11-2018);
– создание ключа ЭП/ключа проверки ЭП,

используемых при помощи функций, приведенных в приложении 2 Правил пользования, а также при выполнении криптографических протоколов:

- CMS;
- EFS (только для исполнения 3-Base);
- TLS;
- IPsec;
- SESPAKE;
- PKINIT (только для исполнения 3-Base),

реализованных с использованием перечисленных выше алгоритмов, удовлетворяет Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, для СКЗИ классов КС1 (версия 5.0 КС1 исполнение 1-Base), КС2 (версия 5.0 КС2 исполнение 2-Base) и КС3 (версия 5.0 КС3 исполнение 3-Base), Специальным требованиям к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, и эксплуатируемым на территории Российской Федерации, по уровню КС и Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27.12.2011 г. №796, для средств ЭП классов КС1 (версия 5.0 КС1 исполнение 1-Base), КС2 (версия 5.0 КС2 исполнение 2-Base) и КС3 (версия 5.0 КС3 исполнение 3-Base).

СКЗИ «КриптоПро CSP» версии 5.0 разрешается эксплуатировать до 01 мая 2024 года.

Использование СКЗИ «КриптоПро CSP» версии 5.0 для формирования электронной подписи по ГОСТ Р 34.10-2001 после 31 декабря 2019 года не допускается.

Генеральный директор
ООО «КРИПТО-ПРО» Н.Г. Чернова

http://www.CryptoPro.ru E-mail: info@CryptoPro.ru

https://cryptopro.ru/products/csp_5_0

Материалы по NGate

КРИПТОПРО

- https://www.cryptopro.ru/products/ngate - общее описание
- https://www.cryptopro.ru/products/ngate/presentations - презентации, брошюры, схемы
- https://www.cryptopro.ru/products/ngate/downloads - загрузка виртуальных образов для тестирования (90 дней)
- https://plutsik.blogspot.com/2019/03/ebsid.html - статья про особенности выбора средств удаленной идентификации в ЕБС
- https://ng-test.cryptopro.ru - доступ к тестовому стенду (test/test)
- ngate@cryptopro.ru - ящик для вопросов по NGate

КРИПТОПРО

Спасибо за внимание!

plutsik@cryptopro.ru
+7 (495) 995-48-20 (доб. 150)