# 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»

# О нас

КРИПТОПРО

- Почти 20 лет на рынке
- Лидеры разработки СКЗИ
- Реализовано множество PKI-проектов
- Продукты интегрированы во многие ИС
- Участвуем в разработке стандартов RFC

# Тренды

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

# Драйверы и условия развития СЗИ

КРИПТОПРО

- Законодательство
- Бизнес-потребности
- Решение должно устраивать:
  - ✓ Пользователя
  - ✓ Администратора
  - ✓ Руководителя

# 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)**

# Законодательство. Другое

- **Удаленный мониторинг энергооборудования (1015 приказ Минэнерго от 06.11.2018):**
  - ✓ криптозащита удаленного соединения и обмена данными
  - ✓ применение сертифицированных средств защиты информации
- **Перевод госорганов на отечественную криптографию (Пр-1380, от 16.07.2016):**
  - ✓ Взаимодействие госорганов между собой
  - ✓ Взаимодействие граждан и организаций с госорганами
- **Импортозамещение (директива А.Силуанова от 06.12.2018)**
  - ✓ в 2021 году доля отечественного ПО в АО с госучастием и их «дочках» должна превысить 50%.

# Бизнес-потребности

**Удаленный доступ сотрудников к корпоративным ресурсам**

- 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

# Чего хочет пользователь?

- Надежный защищенный удаленный доступ
- Работа на всех устройствах и ОС
- Без управления со стороны пользователя
- Подключения через VPN клиента и без него

# Чего хочет администратор?

- Единое просто управляемое решение
- Отказоустойчивость и масштабирование
- Гибкая политика безопасности, без донастройки FW
- Аудит действий пользователя
- Поддержка со стороны производителя

# Чего хочет руководитель?

КРИПТОПРО

- Сертификация по необходимым классам
- Отсутствие ограничений на поставку (санкции)
- Отсутствие необходимости получения лицензий
- Приемлемая стоимость

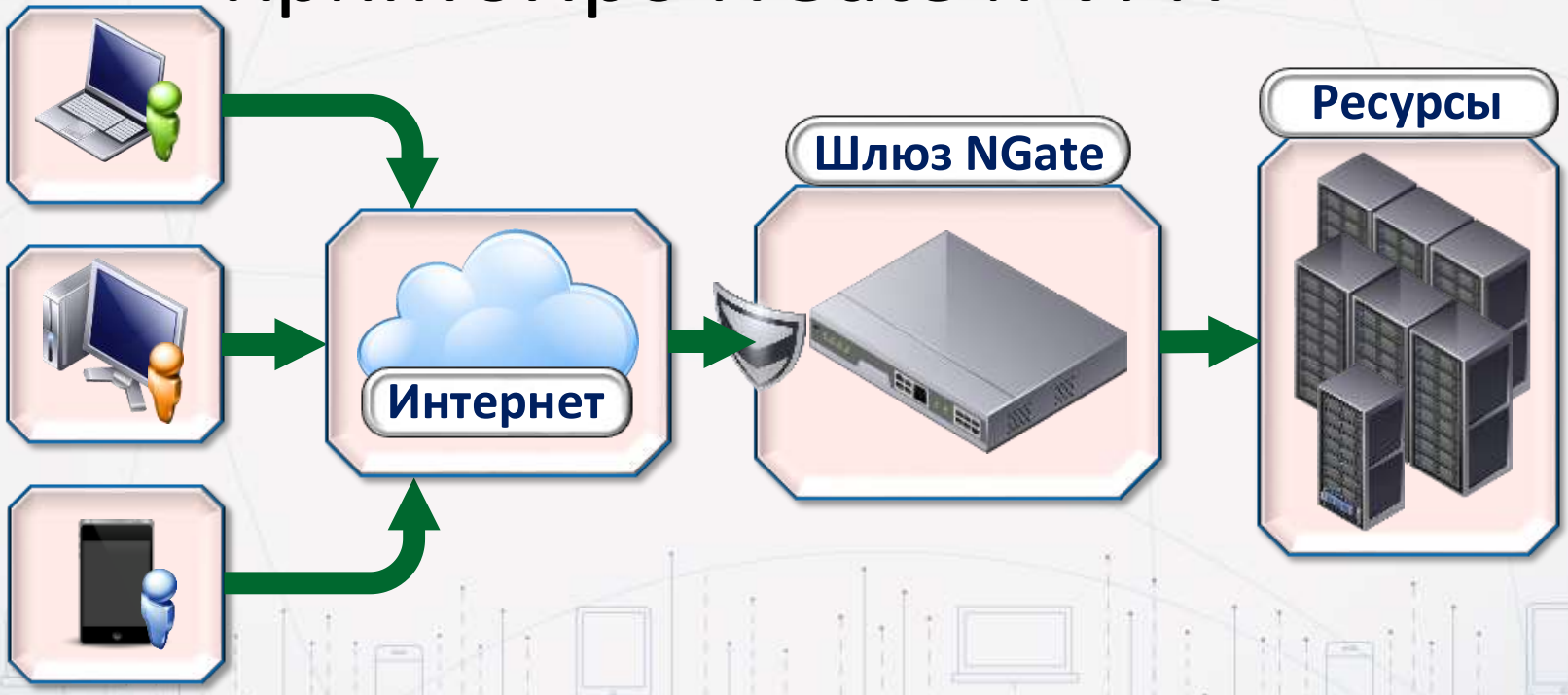
# Как в итоге должно быть?

КРИПТОПРО

- Сертифицировано
- Не чувствительно к санкциям
- Поддерживаемо производителем
- Универсально, быстро, надёжно,
- Удобно, функционально, безопасно

# Шлюз удаленного доступа КриптоПро NGate и VPN

КРИПТОПРО



# 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»

# Актуальный TLS

КРИПТОПРО

- Методические рекомендации утверждены ТК 26 24.04.2014
- Основной протокол криптозащиты на ГОСТе в Интернете
- Криптографический стержень КриптоПро NGate

# Зачем нужен NGate?

КРИПТОПРО

- Доступ к веб-приложениям по TLS с ГОСТ/не ГОСТ
- Доступ к произвольным ресурсам по VPN
- Контроль доступа к приложениям
- 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

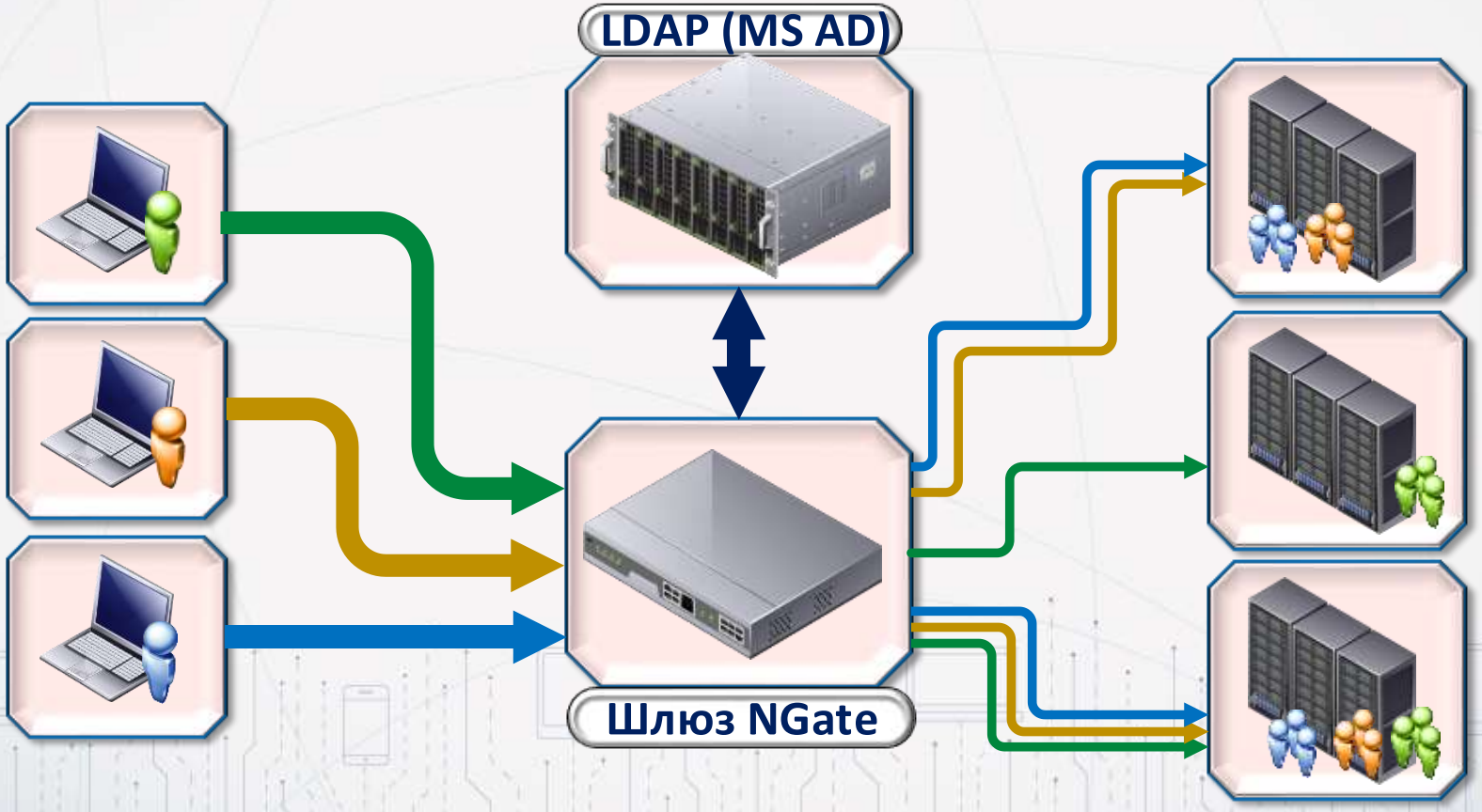
# Режимы работы

- TLS-терминатор
- Портальный доступ
- VPN доступ

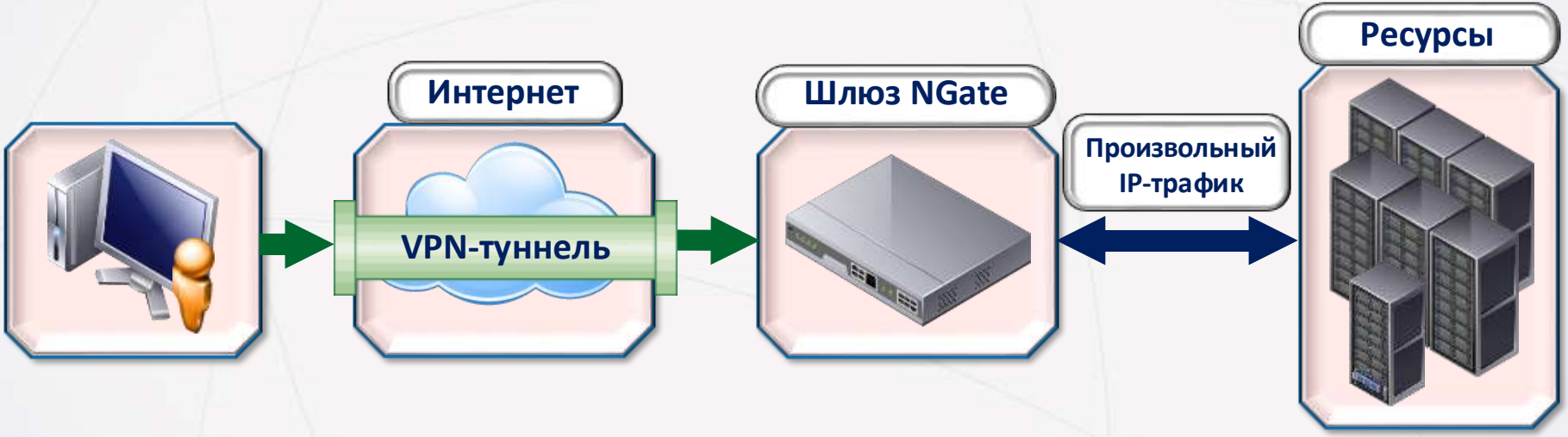
# TLS-терминатор

# Портальный доступ

КРИПТОПРО



# VPN доступ




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

# Методы аутентификации

КРИПТОПРО

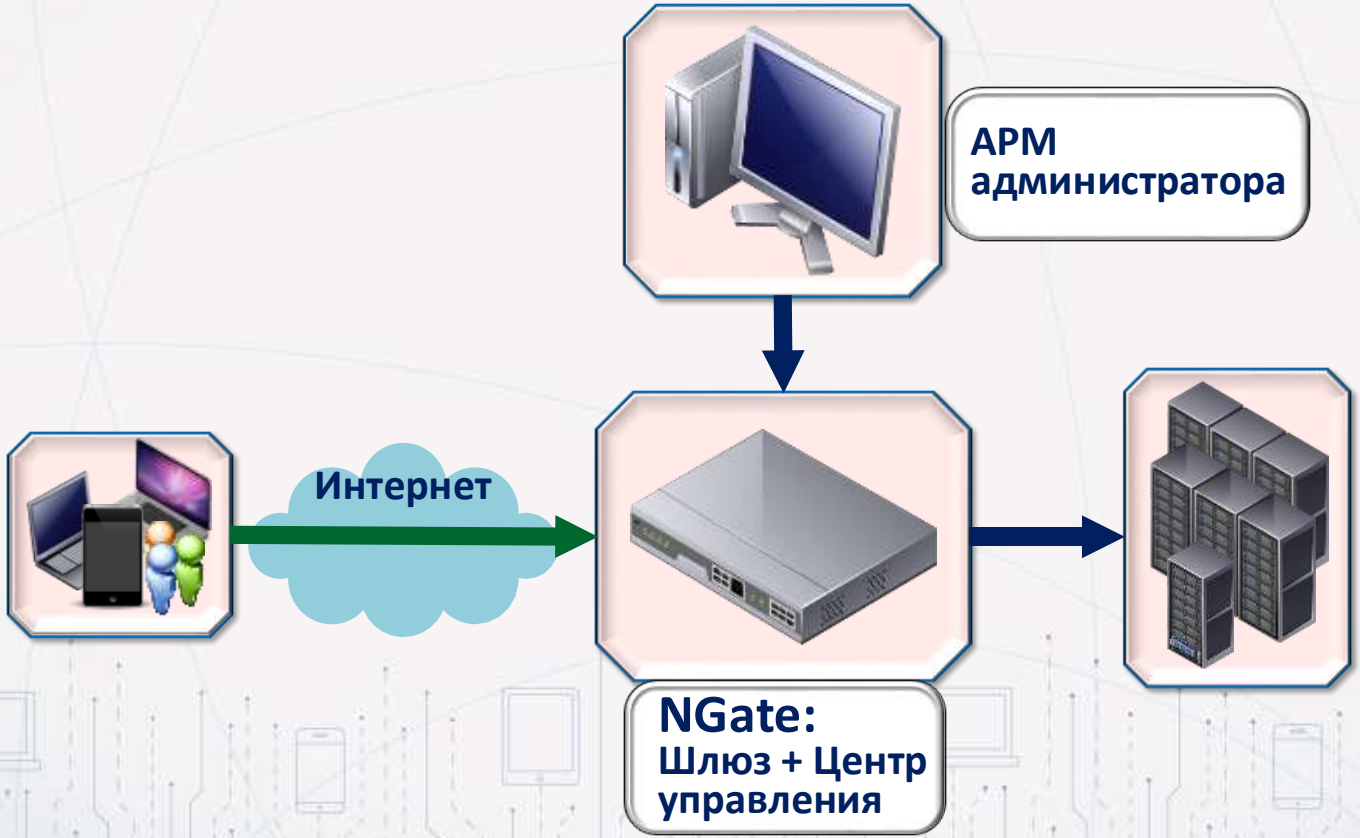
- Без аутентификации (прозрачно)
- Логин/пароль (MS AD/LDAP)
- Сертификат (валидность и/или поля)
- Сертификат в LDAP/MS AD
- UPN в MS AD
- OTP через Radius

# Компоненты

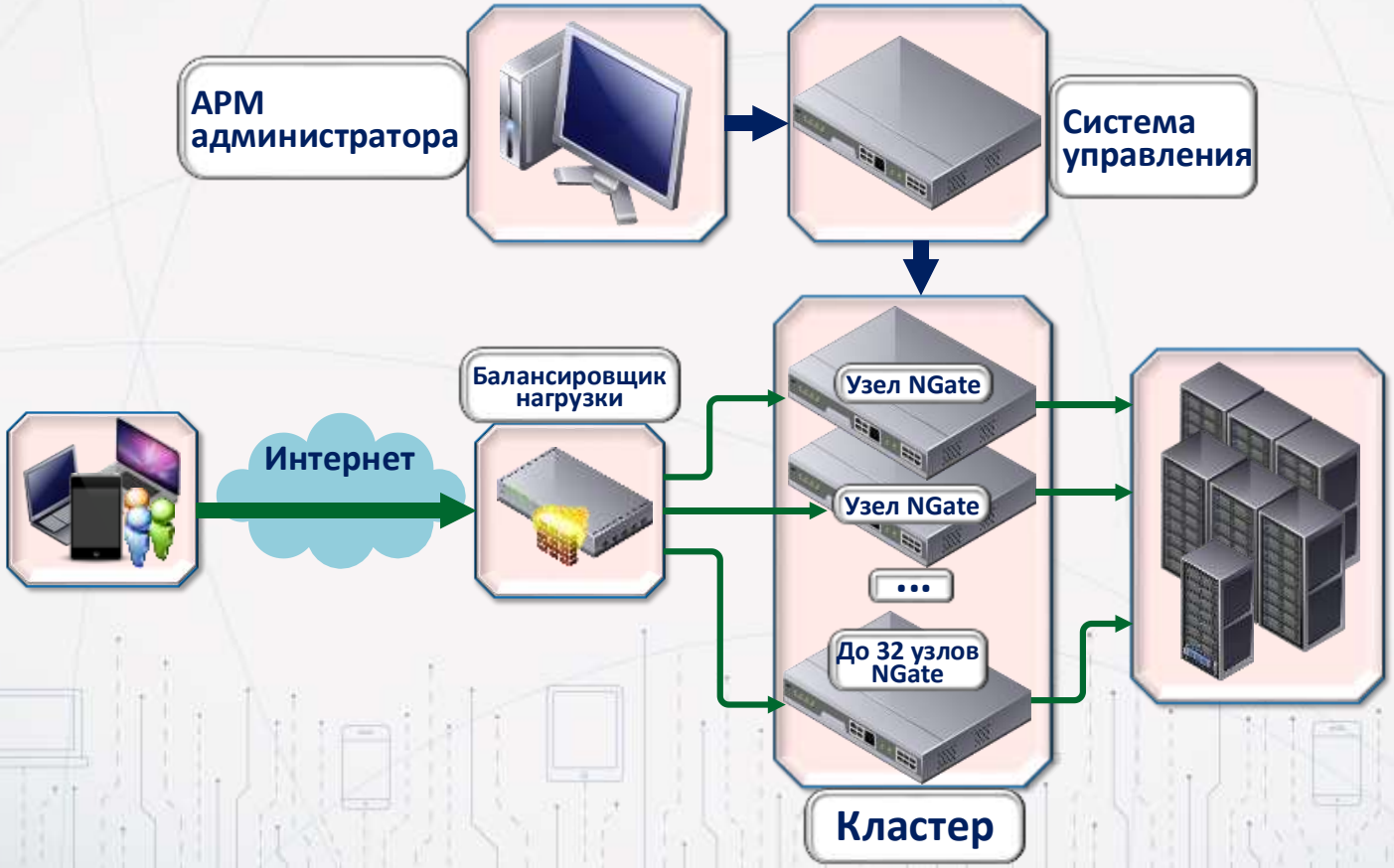
КРИПТОПРО

- Шлюз
- Система управления
- VPN-клиент

# Схемы внедрения. Всё в одном



# Схемы внедрения. Кластер



# Производительность

- до 700 Мбит/с на сессию
- до 40 000 одновременных сессий
- до 10 Гбит/с пропускная способность

# 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

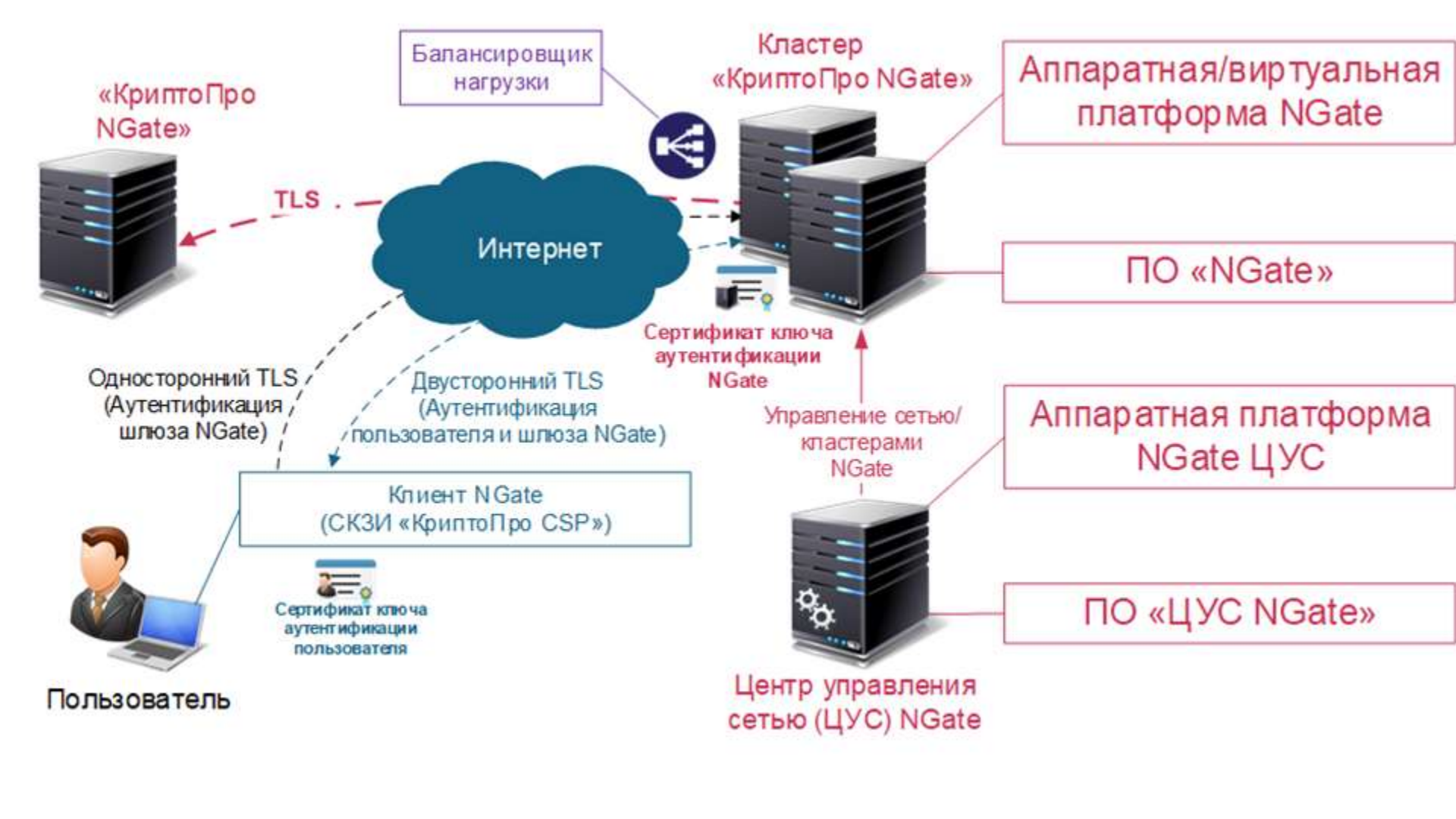
# Интеграции

- Системы аутентификации (AD, LDAP, Radius)
- Системы мониторинга (по SNMP)
- SIEM-системы (Syslog)
- Web Application Firewall

# Планы на будущее

КРИПТОПРО

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


Балансировщик нагрузки
Кластер «КриптоПро NGate»
Аппаратная/виртуальная платформа NGate
«КриптоПро NGate»
TLS
Интернет
ПО «NGate»
Сертификат ключа аутентификации NGate
Односторонний TLS (Аутентификация шлюза NGate)
Двусторонний TLS (Аутентификация пользователя и шлюза NGate)
Управление сетью/ кластерами NGate
Аппаратная платформа NGate ЦУС
Клиент NGate (СКЗИ «КриптоПро CSP»)
Сертификат ключа аутентификации пользователя
ПО «ЦУС NGate»
Пользователь
Центр управления сетью (ЦУС) NGate

# Лицензирование шлюзов

- ✓ Платформа NGate:
  - NGate 300 → до 500 одновременных подключений
  - NGate 600 → до 2 500 одновременных подключений
  - NGate 1000 → до 8 000 одновременных подключений
  - NGate 2000 → до 25 000 одновременных подключений
  - NGate 3000 → до 40 000 одновременных подключений
  - Кластер NGate → до 100 000 одновременных подключений
  - NGate на VM → до 1 000 одновременных подключений

- ✓ Лицензия на право использования СКЗИ «КриптоПро NGate» для 50 – 100 000 одновременных подключений

- ✓ Сертификат технической (расширенной технической) поддержки аппаратной платформы NGate сроком на 1 (2,3) года

- ✓ Сертификат технической (расширенной технической) поддержки СКЗИ «КриптоПро NGate» сроком на 1 (2,3) года

# Лицензирование ЦУС

- ✓ Для управления всеми кластерами NGate достаточно одного ЦУС (аппаратная платформа NGate ЦУС 100 или VM)
- ✓ ПО NGate ЦУС лицензируется по количеству управляемых кластеров NGate
- ✓ Лицензия на право использования ПО ЦУС СКЗИ "КриптоПро NGate" для необходимого количества кластеров СКЗИ "КриптоПро NGate"
- ✓ Сертификат технической (расширенной технической) поддержки аппаратной платформы NGate ЦУС 100 на 1 (2,3) года
- ✓ Сертификат технической (расширенной технической) поддержки ПО ЦУС СКЗИ «КриптоПро NGate» на 1 (2,3) года

# Лицензирование клиентской части

- ✓ Подключение с односторонней TLS-аутентификацией (только шлюза NGate):
  - Клиентская лицензия на ПО и сертификат аутентификации клиента не требуется

- ✓ Подключение с двусторонней TLS-аутентификацией (взаимная аутентификация):

  - Сертификат аутентификации пользователя и шлюза NGate (сервера) – создает:
    - ❑ Сервис ЦУС-VPN ООО «КРИПТО-ПРО»
    - ❑ Любой УЦ на основе ПАК «КриптоПро УЦ»

  - Лицензия на право использования СКЗИ «КриптоПро CSP»
    - ❑ Постоянная лицензия на рабочее место (для ЭП)
    - ❑ Ограниченная лицензия, встроенная в сертификат аутентификации
      - ○ Сервис ЦУС-VPN ООО «КРИПТО-ПРО»
      - ○ Коммерческие УЦ - партнеры ООО «КРИПТО-ПРО»
      - ○ Лицензионный договор на КриптоПро УЦ с отчислениями

# 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)