КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ


# КОД ИБ | Новосибирск

25.09.2025

# Владимир Ковалев

- От администратора ИТ систем, до Java разработчика
- От 1С программиста до начальника отдела ИТ и руководителя проектов внедрения западных ERP систем
- От замдиректора завода по ИТ и… обратно к администрированию ИТ систем и руководству проектами

Резидент MVP Айдентити клуба

(www.identityclub.ru)

# Контроль привилегированных учетных записей

# Определение

PAM система - система, предназначенная для контроля и обеспечения безопасности учетных записей с повышенными правами доступа, таких как администраторские или системные учетные записи.

(с) Яндекс Алиса

# Кто в зоне риска

- ИТ-администраторы – сотрудники компании

Использование личных учетных записей для администрирования систем **недопустимо**!

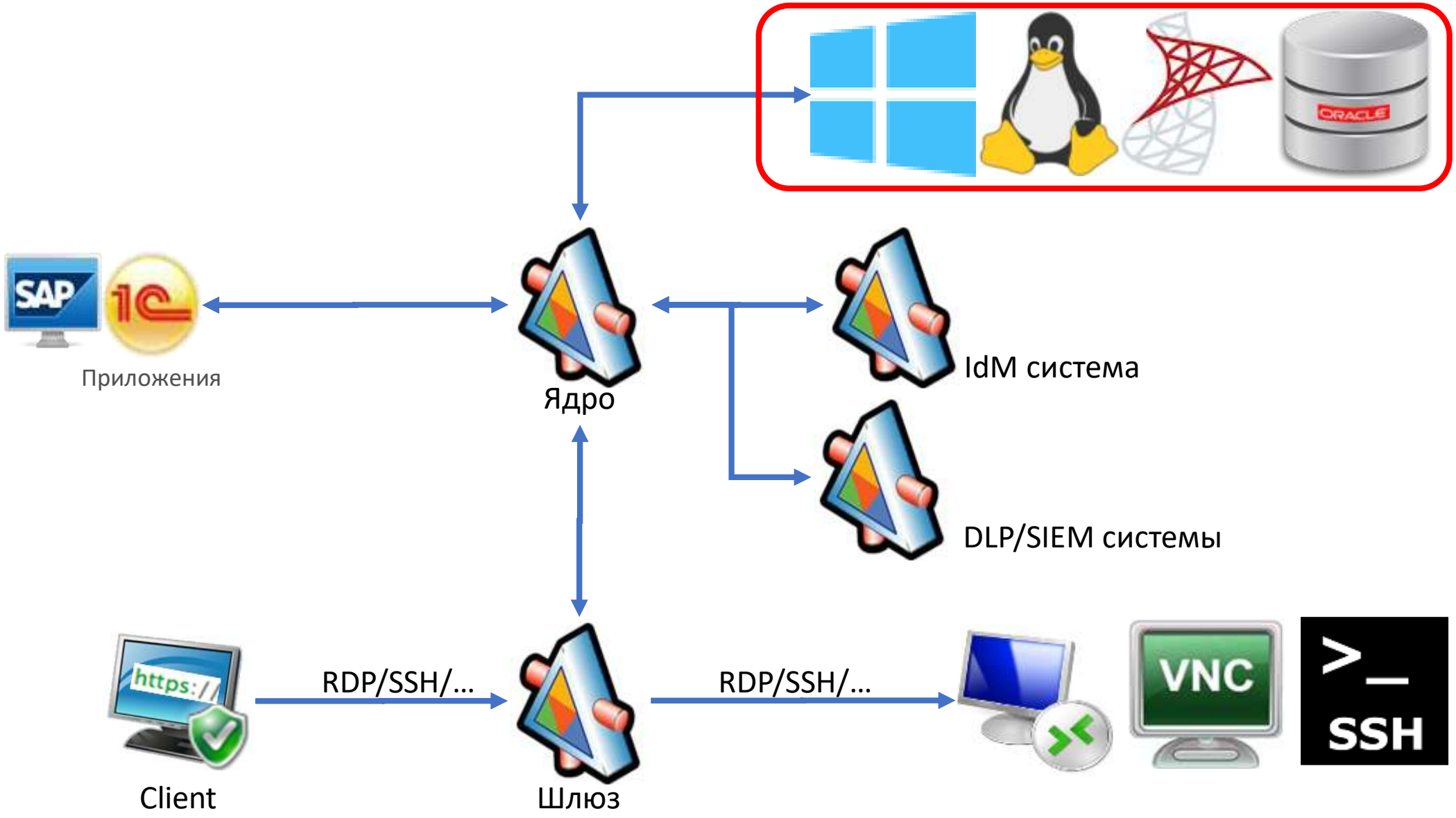
- Внешние подрядчики – в том числе администрирующие системы

Передача внешним подрядчикам учетных записей с административными правами доступа **недопустимо!**

- Бизнес-пользователи компании, работающие с чувствительными данными

- Специальные и сервисные учетные записи

# Архитектура – контроль жизненного цикла УЗ



# Контроль жизненного цикла учетных записей

**Создание УЗ**

- Создание УЗ
- Поиск УЗ

**Управление правами**

- Выдача и отзыв прав

**Использование УЗ**

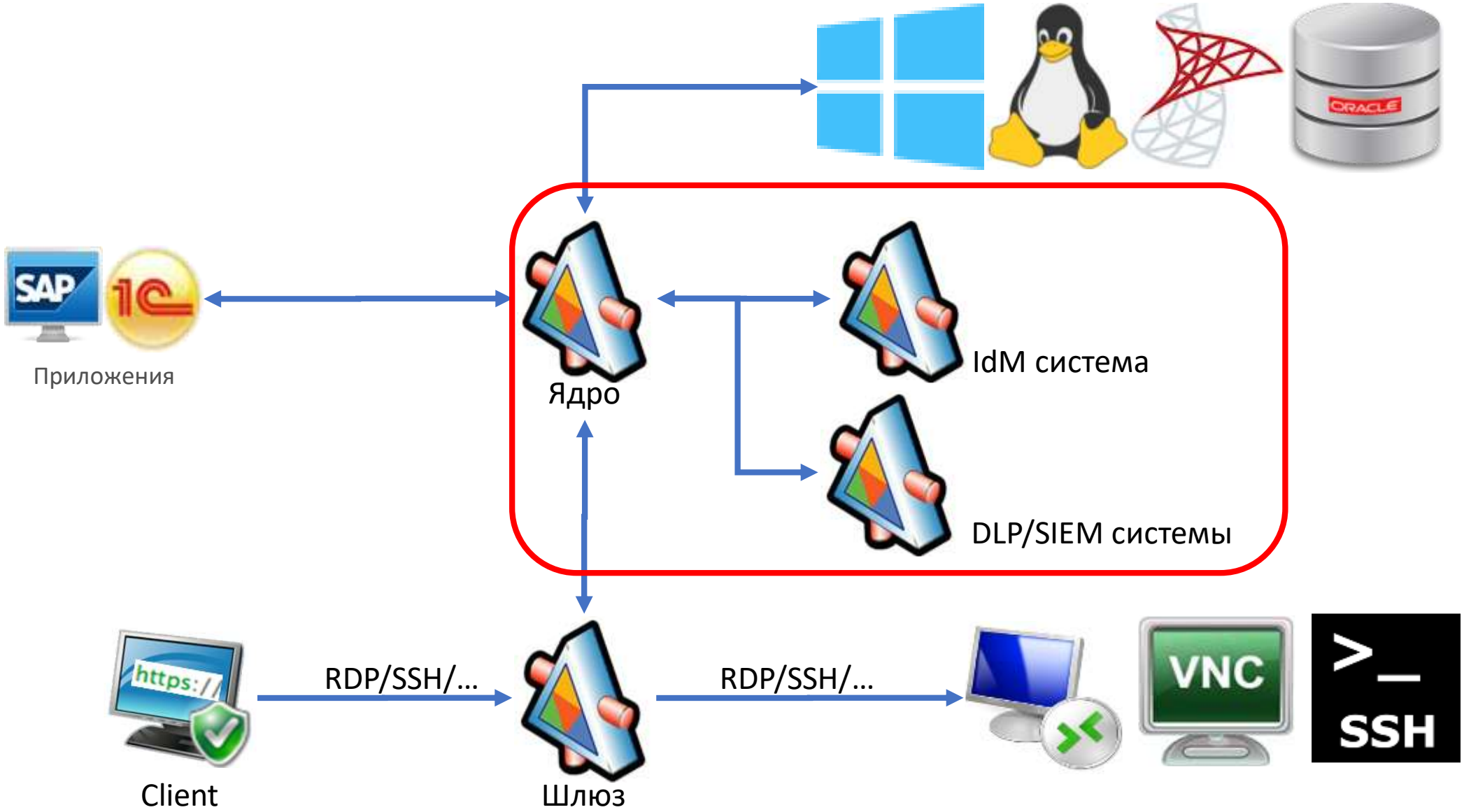
- Кто использует
- Ротация паролей
- Смена ответственного

**Вывод из эксплуатации**

- Отзыв прав
- Блокировка или удаление УЗ


...

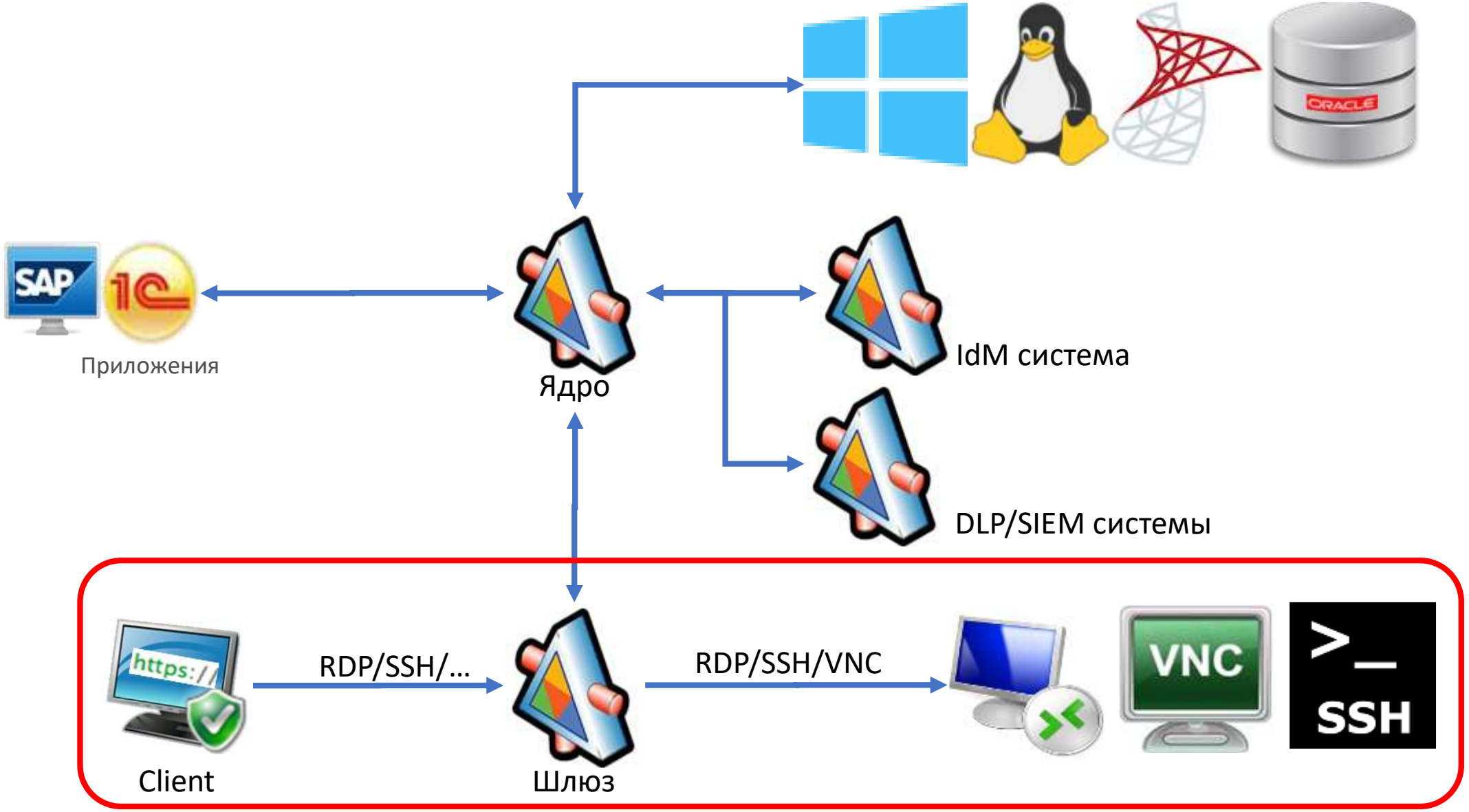
# Архитектура – интеграция с прочими системами



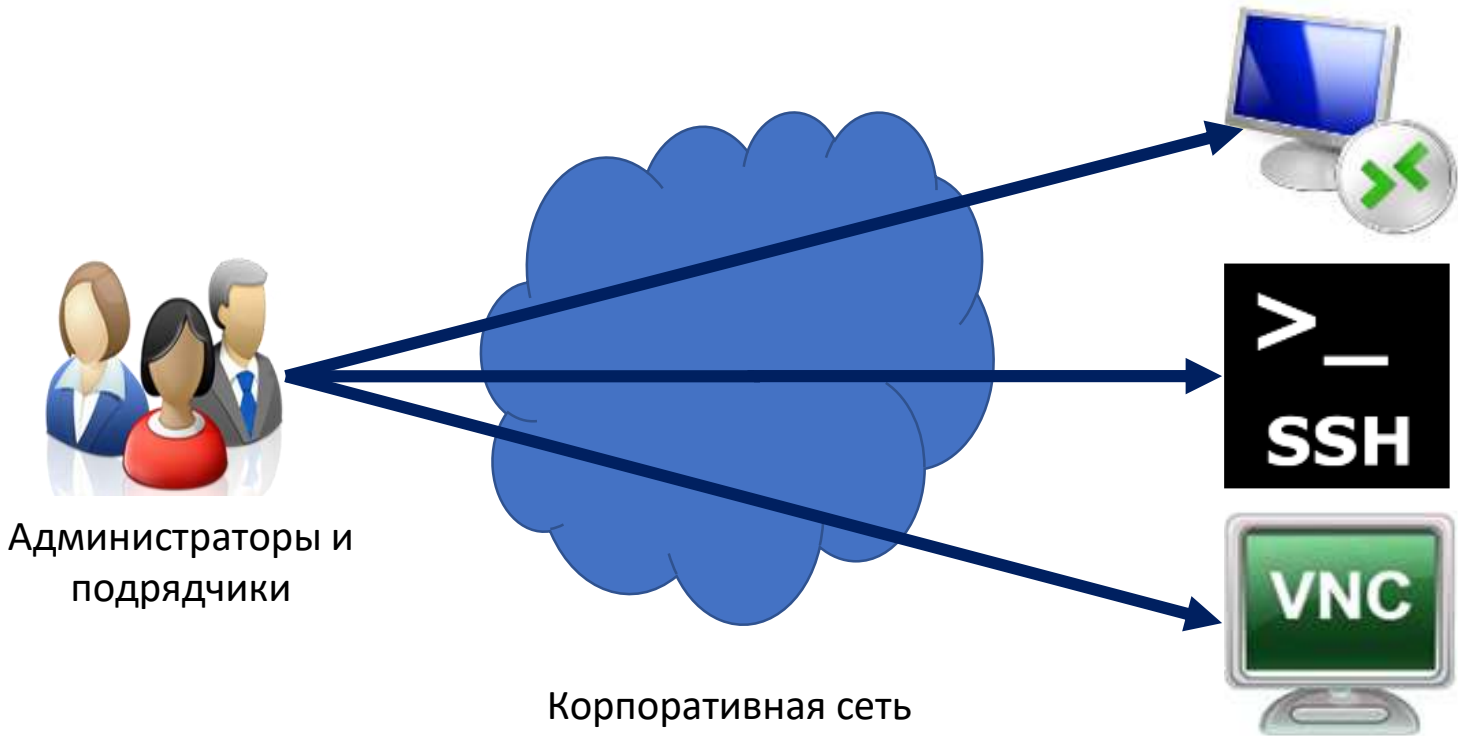
# Интеграция с IdM, DLP, SIEM, антивирусом

- Использование механизмов IdM для управления жизненным циклом привилегированных УЗ
- Передача данных сессий (файлов и буфера обмена) в DLP и антивирус
- Передача событий сессий в SIEM

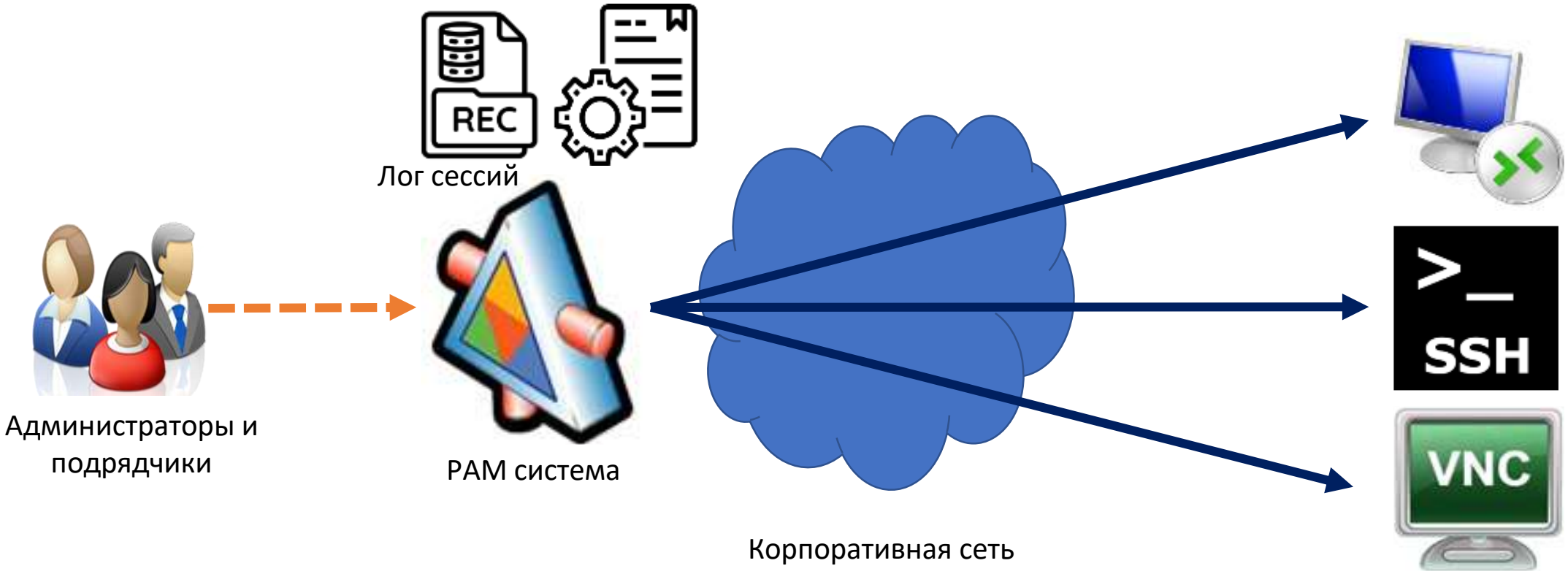
# Архитектура – менеджер сеансов



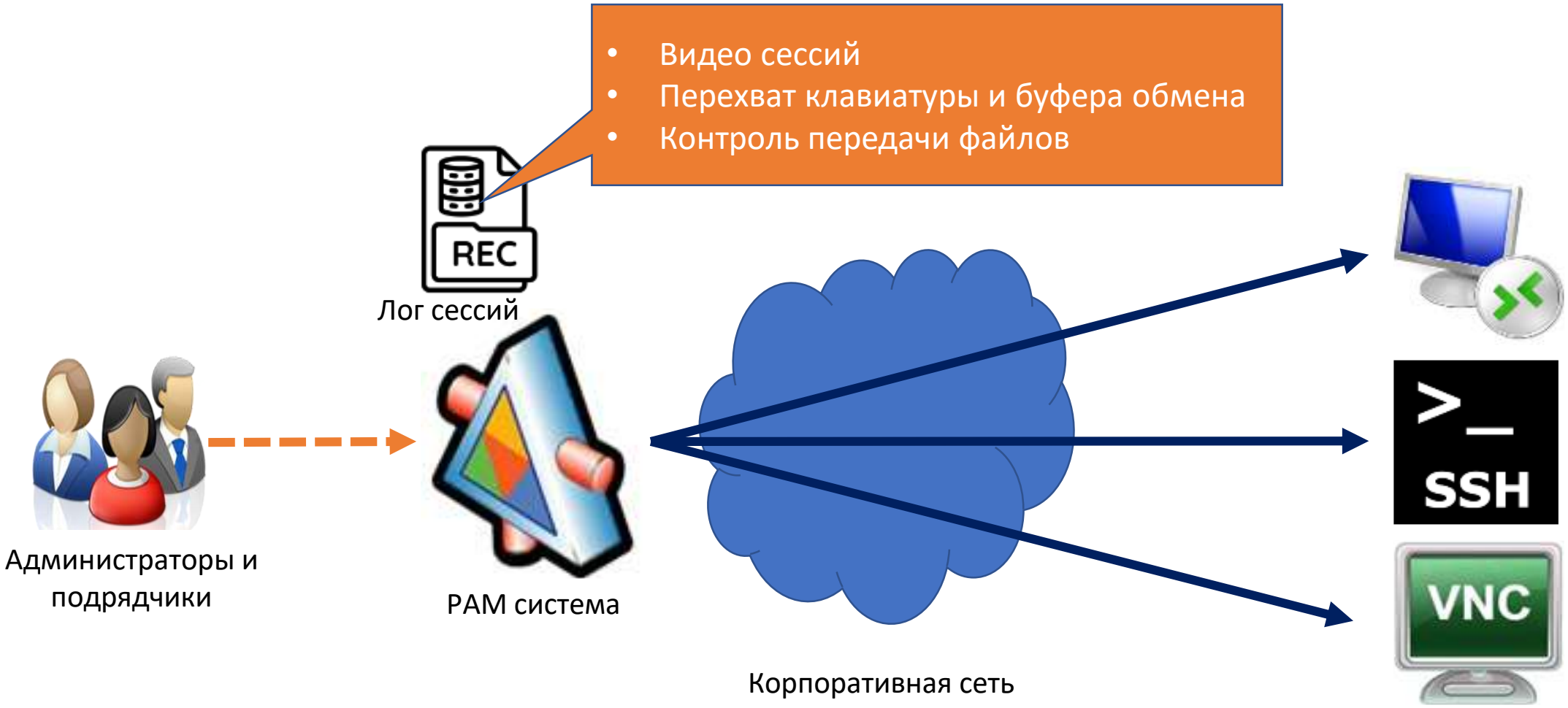
# Классическая схема подключения



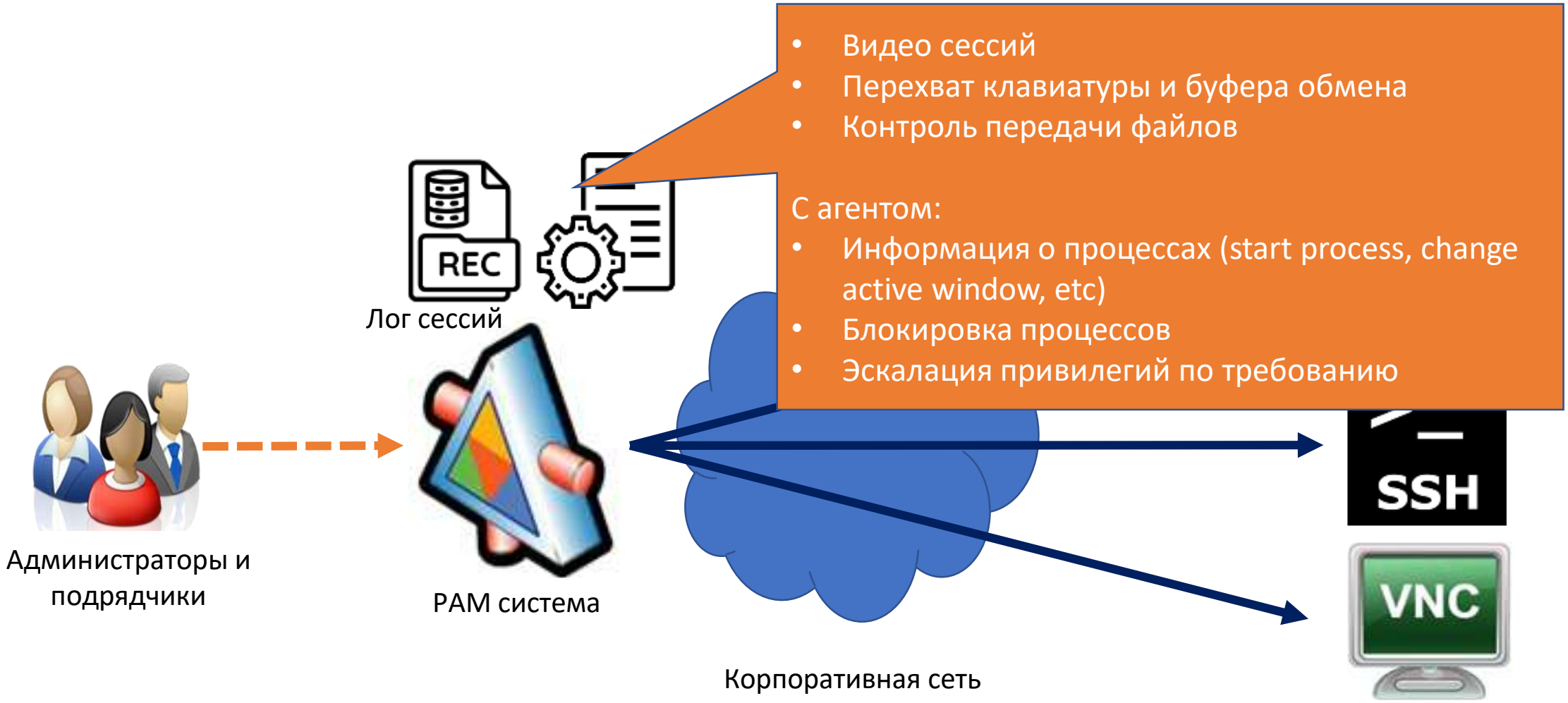
# После внедрения PAM системы



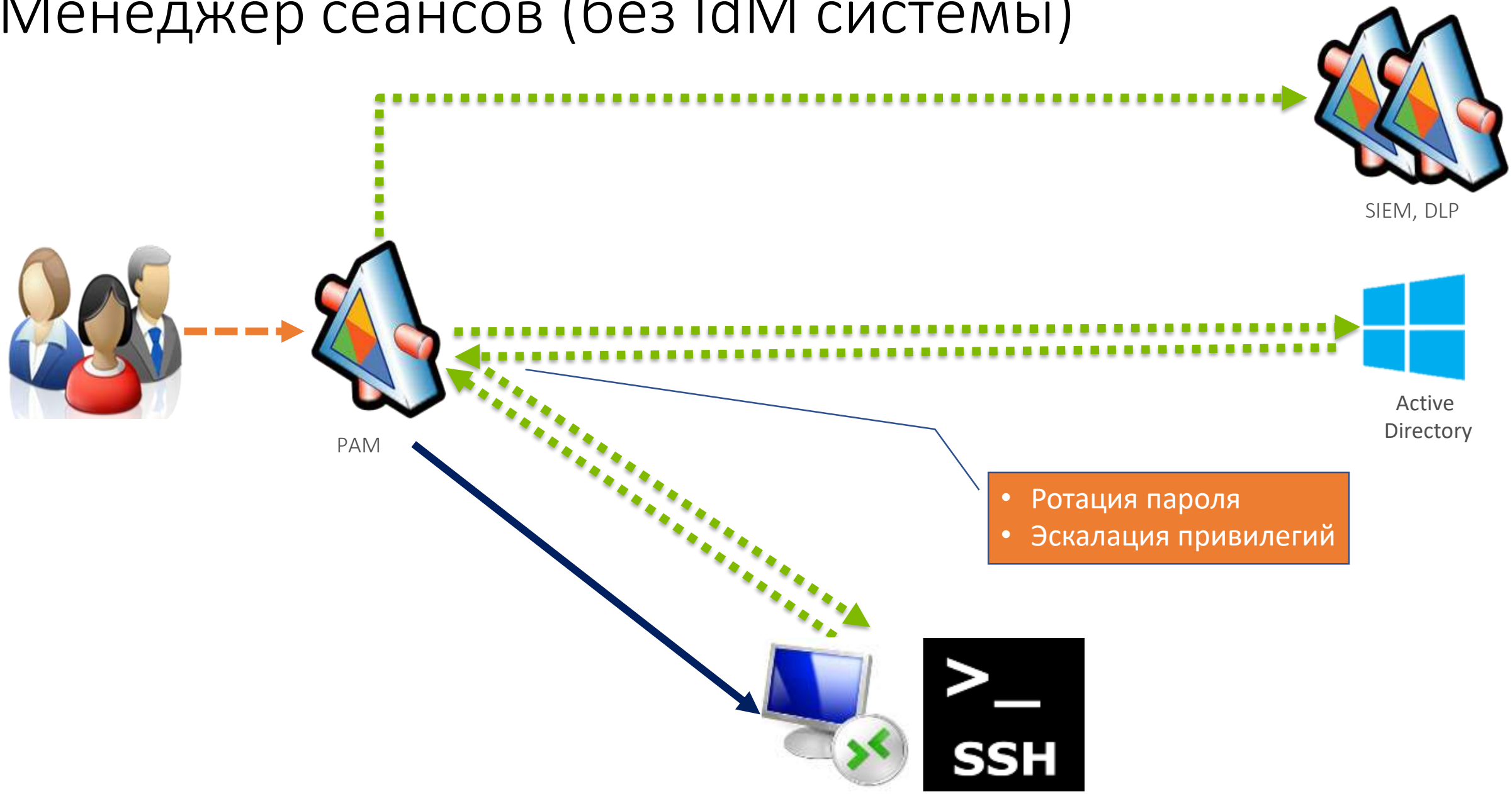
# После внедрения PAM системы – без агента



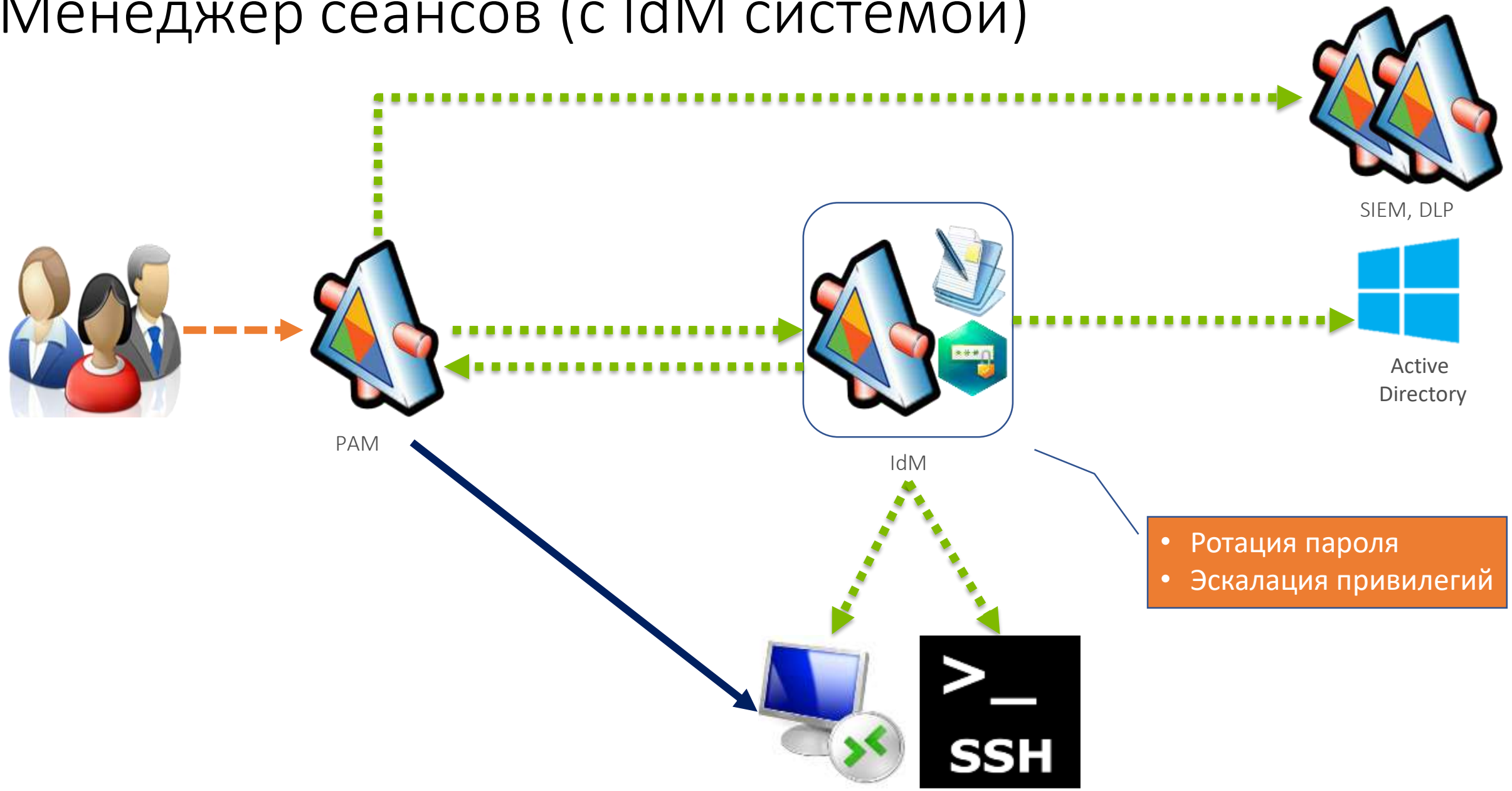
# После внедрения PAM системы – с агентом



# Менеджер сеансов (без IdM системы)

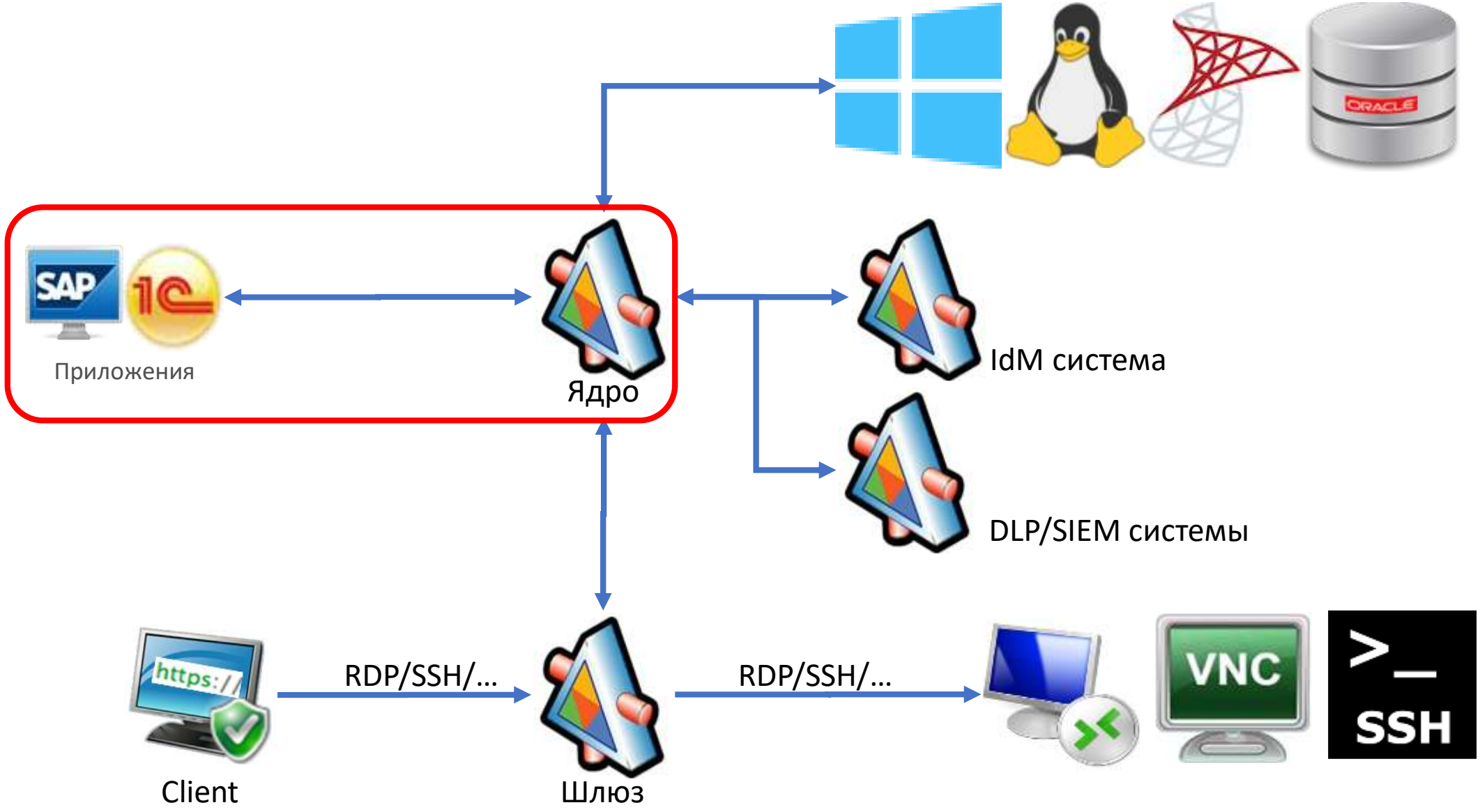


# Менеджер сеансов (с IdM системой)

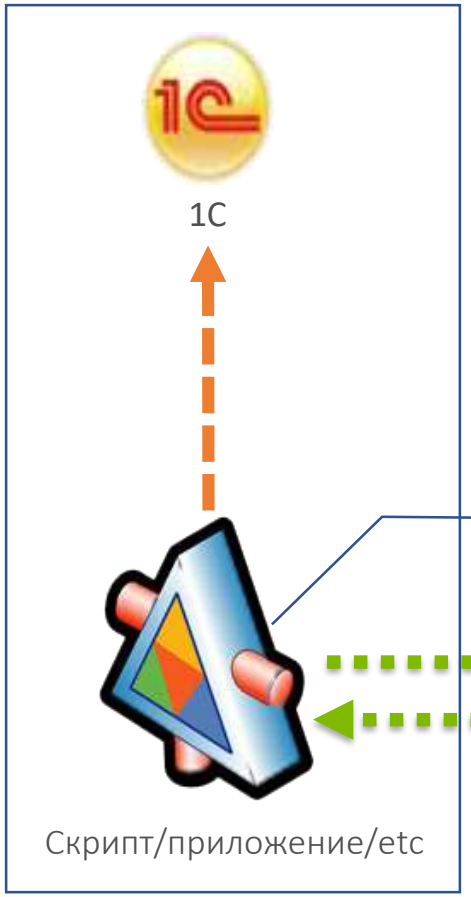



- Ротация пароля
- Эскалация привилегий

# Архитектура – App2App password management



# App2App password management




```
…
$user = "учетная запись"
$pass = "aGjSAv23jh%agj!^%@"
# использование учетки
…
```

# App2App password management

**Пример скрипта на PowerShell**

**Было**

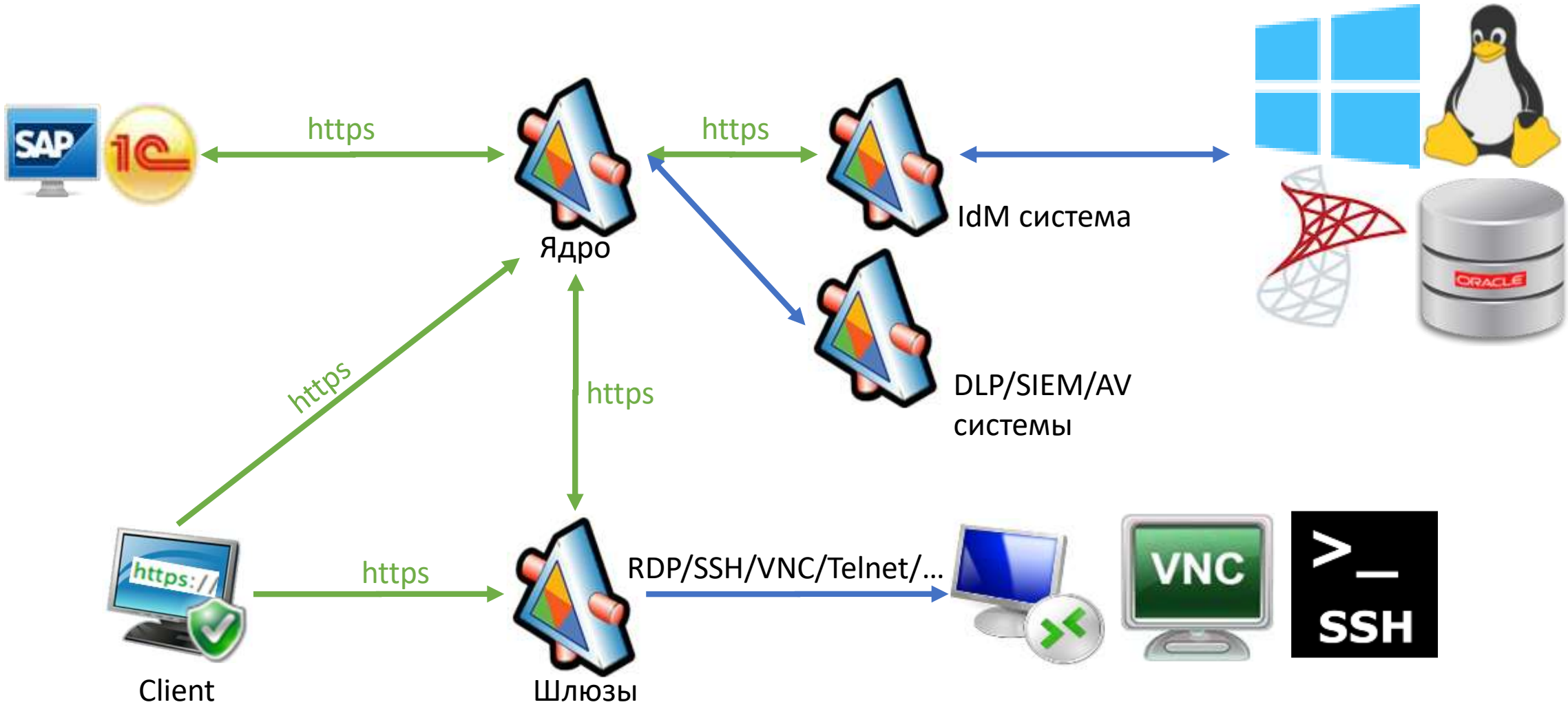
```
…
$user = 'учетная запись'
$pass = 'kajsghdjhsagj!^%@^"
# использование учетки
…
```

**Стало:**

```
…
# получение учетных данных в память по токену
$apiURI = https://IdM.domain.local/API/App2App/getCredential
$cred = Invoke-RestMethod -Method POST -Uri $apiURI -Body "5cb38847-1bb4-4669-af99-bebbe75f832b"
# использование учетки
…
```

# Наш опыт

# Архитектура



# Текущий функционал

- Поддержка протоколов
  - RDP (+Remote App)
  - SSH
  - VNC
  - Telnet
  - Kubernetes
  - Hyper-V
- Интеграция с IdM, DLP системами и антивирусом
- Централизованное управление географически распределенной системой
- Кластеризация шлюзов active-active.
- Поддержка 2FA
- **Очень** компактная запись сессий

# Текущий статус

- 47 шлюзов
- 2200+ пользователей системы
- Более 90.000 сессий, длительностью более 180.000+ часов

# Вопросы?