Суверенный фундамент

Доверенная ИТ-среда ФосАгро на российском стеке

АО «Апатит» / Номинация «Промышленность»

Операционная система
Astra Linux

Служба каталога
ALD Pro

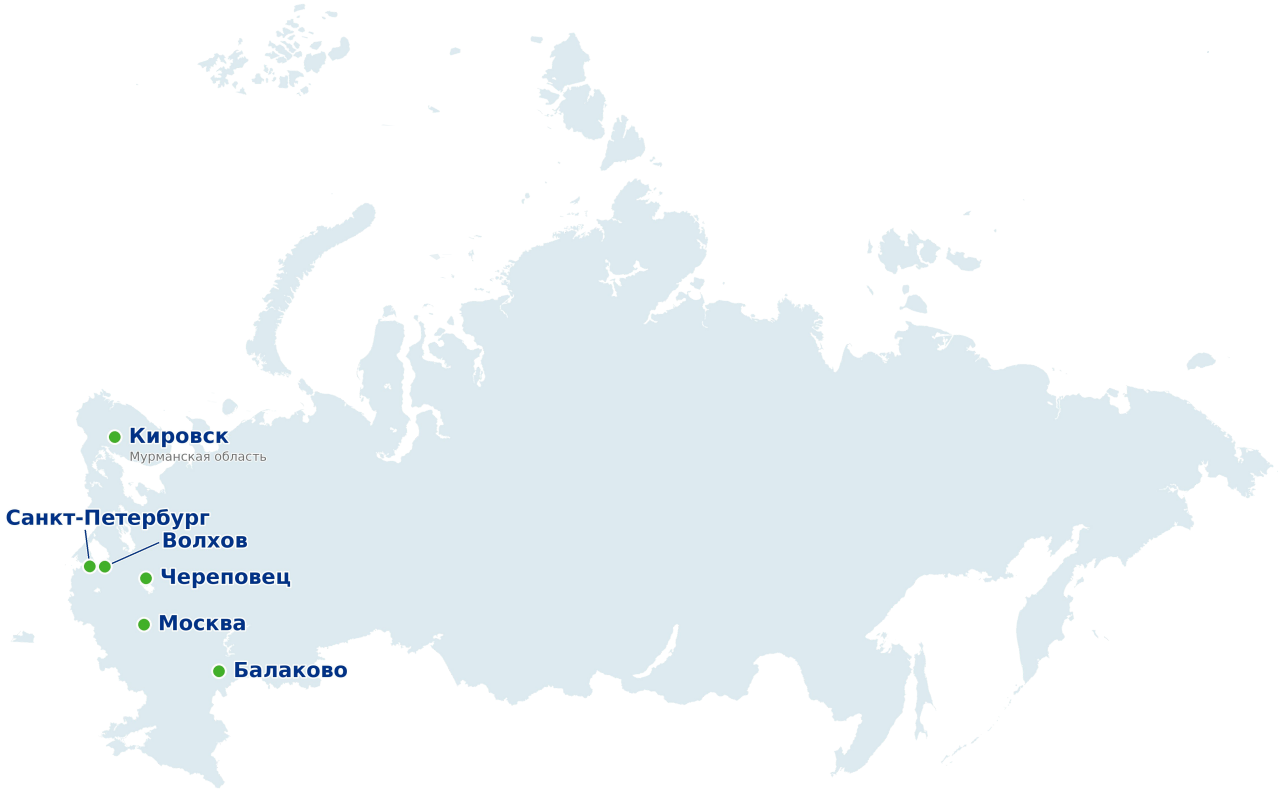
Единая аутентификация
Keycloak

МФА и удостоверяющий центр
Аладдин Р.Д.

Управление доступом
Solar inRights

Работу предприятия нельзя остановить ни на час

АО «Апатит» — субъект КИИ



7 000

Пользователей АРМ

6

Площадок

450+

Информационных систем

1

Вендор в основании исходной ИТ-среды

Переход требует миграции без «дня X»

ВИДИМЫЙ СЛОЙ



СКРЫТЫЕ ЗАВИСИМОСТИ

Замена ОС не устраняет зависимость приложений

Непрерывная работа

АСУ ТП, ERP, СЭД, DLP, КриптоПро и другие системы

Два стека одновременно

Две ОС, два каталога и два УЦ

Без массовой переделки ИС

Аутентификация встроена в приложения

Пять компонентов образуют единое доверенное ядро

ИСХОДНЫЙ СТЕК

Microsoft

Windows
Active Directory
Microsoft CA
NTLM

ПЕРЕХОДНЫЙ ПЕРИОД

Двустороннее доверие доменов



ЦЕЛЕВАЯ АРХИТЕКТУРА

Astra Linux SE	Операционная система
ALD Pro	Служба каталога
Keycloak	Единая аутентификация
Аладдин Р.Д.	МФА и удостоверяющий центр
Solar inRights	Управление доступом

ФСТЭК: Astra Linux SE — 1-й уровень доверия; ALD Pro — 2-й уровень доверия

7 000 пользователей переходят под централизованное управление

4 666

из 7 000 пользователей на Astra Linux



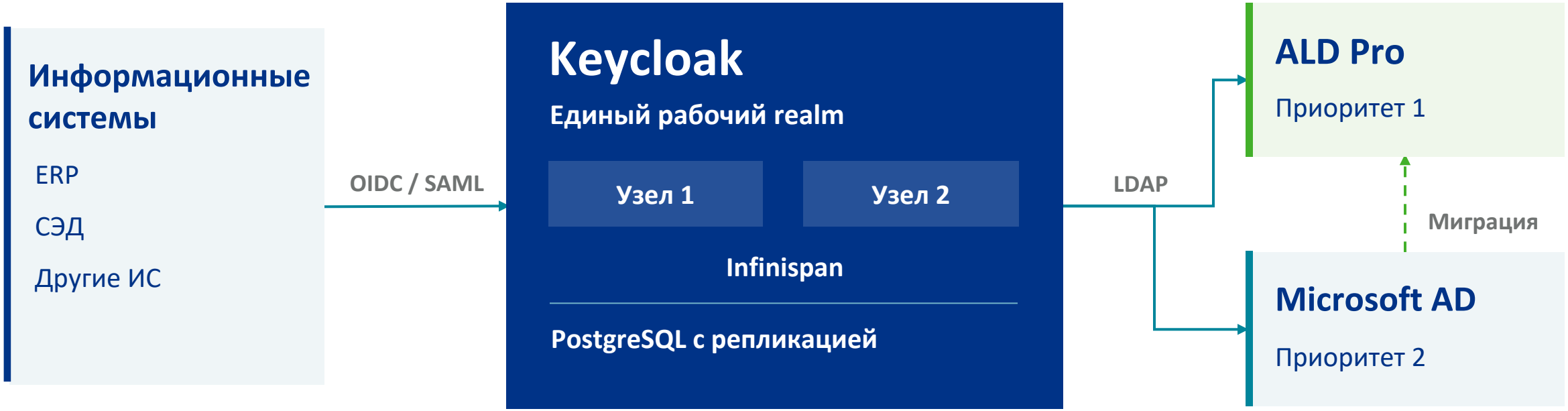
2024	2026	2027
Пилот	Текущий этап	Завершение

~30%

экономии времени ИТ-специалистов

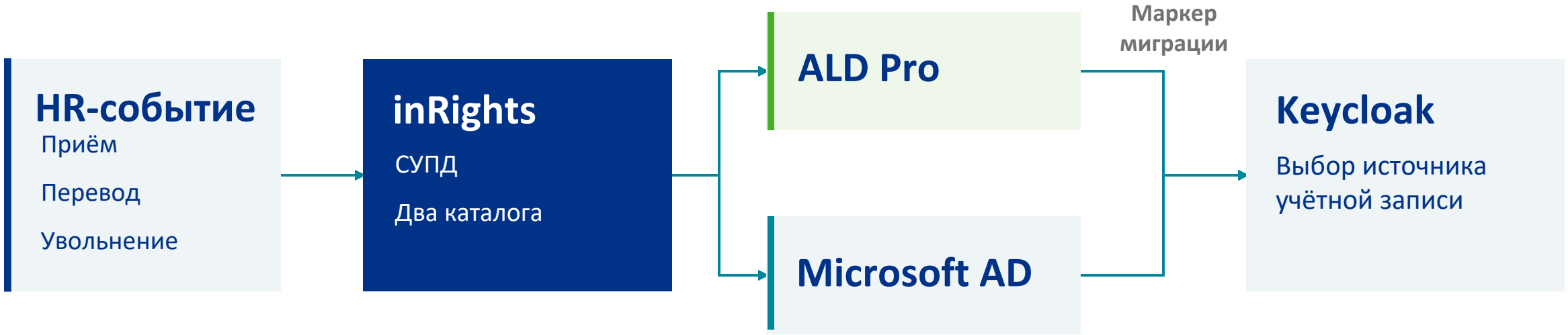
Единая консоль ALD Pro
Типовые образы
Внутренний репозиторий
Kerberos вместо NTLM

Авторизация в приложениях не зависит от домена



Миграция учётных записей стала штатной операцией IDM

Solar inRights управляет переходом между каталогами



SSO в IDM по OpenID Connect

Доставка паролей по СМС

МФА и PKI внедряются в закрытом корпоративном контуре

ВТОРОЙ ФАКТОР

JMS 4LX + JaCarta

Authentication Server

Keycloak
Интеграция через Authenticator SPI

Каналы
eXpress и корпоративное приложение

Методы
TOTP, push, токены и смарт-карты

УДОСТОВЕРЯЮЩИЙ ЦЕНТР

Aladdin Enterprise CA

Двухуровневая PKI

Криптография
КриптоПро CSP и HSM

Переход
Параллельная работа двух УЦ

Доверие
Перевыпуск сертификатов без разрыва

Общая консоль администрирования / События в SIEM / Поддержка в режиме единого окна

Пять инженерных задач потребовали собственных решений

01

Без окна переключения

Параллельный ввод с действующим стеком Microsoft

02

Два каталога в одном SSO

Собственная модель ролей Keycloak и корреляция записей

03

Двухсторонний траст

Трассировки winbind / NetBIOS и решение с поддержкой Астры

04

Миграция доверия PKI

Два УЦ и перевыпуск сертификатов с сохранением цепочек

05

Единый контур работ

Координация Астры, Аладдин, Солар и К2Тех

Миграция идёт без остановок производства

7 000
рабочих мест в периметре

6
площадок

0
остановок производства

4 666
АРМ на Astra Linux

~30%
экономии времени ИТ-специалистов

100%
Kerberos

1
точка аутентификации для ИС

100+
обученных специалистов

Методология применима к непрерывным производствам

Последовательность перехода сохраняет работу приложений

1. **Каталог с трастом**
2. **Брокер идентификации**
3. **IDM**
4. **Волны миграции ОС**
5. **МФА**
6. **PKI**
7. **Вывод Microsoft**

Металлургия **Энергетика** **Нефтехимия**

В 2027 году завершается переход базовой инфраструктуры

2027

Целевая технологическая независимость

Все 7 000 пользователей на Astra Linux

МФА в промышленной эксплуатации

Сертификаты на российском УЦ

Вывод Microsoft AD и Microsoft CA

Тиражирование на предприятия группы

2024	2025	2026	2027
Пилот	Начало этапа	Масштабирование	Завершение

Архитектуру и управление проектом ведёт команда АО «Апатит»

АО «Апатит»

Группа «ФосАгро»

Дирекция по информационным технологиям, Дирекция по экономической безопасности (Управление ИБ)

Заказчик, архитектура и управление проектом

Astra Linux и ALD Pro
Вендор и соисполнитель

МФА и удостоверяющий центр
Аладдин Р.Д.

Solar inRights
ГК «Солар»

Интегратор Keycloak
К2Тех