# Ligament

Ligament
TWO-FACTOR AUTHENTICATION

# Защита входа на вашей инфраструктуре

Windows и RDP · VPN и Wi-Fi · SSO · приложения · филиалы

Возможности, взаимодействия и сравнение · 10 октября 2026

# Какие задачи решает Ligament

## Сотрудники

Второй фактор для входа в Windows, VPN, Wi-Fi и корпоративные сервисы.

## Администраторы

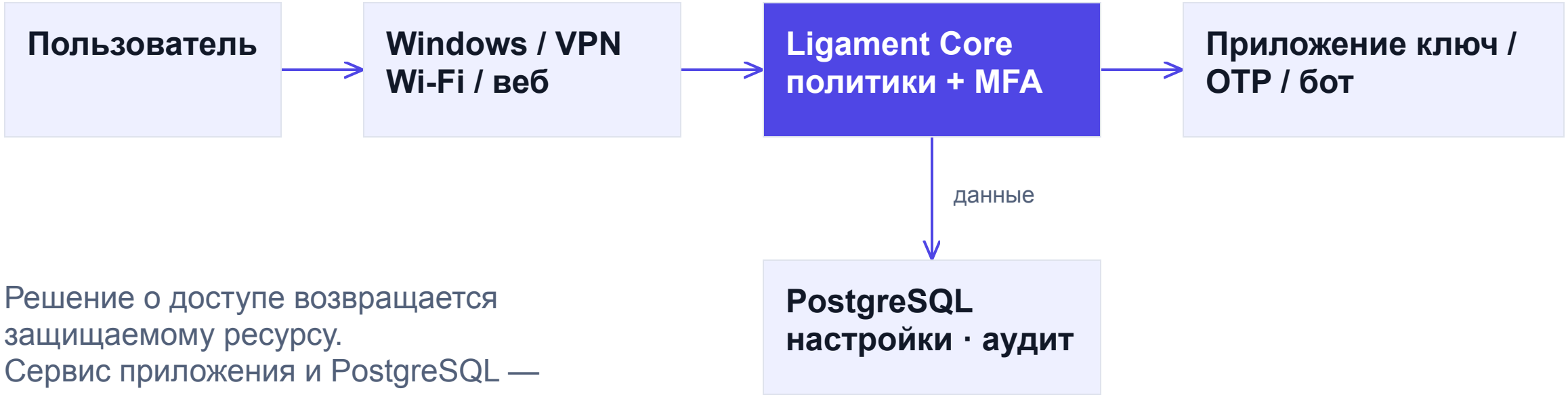
Единые политики доступа, управление устройствами и журнал событий.

## Распределённые команды

Relay для филиалов, временный гостевой доступ и встроенная помощь.

Состав функций зависит от редакции и разрешений в лицензии.

# Общая схема взаимодействия




Решение о доступе возвращается защищаемому ресурсу.
Сервис приложения и PostgreSQL — отдельные компоненты развёртывания.

Внешние каналы доставки и онлайн-сверка отдельных лицензий требуют сетевой связи.

# Факторы подтверждения

## Push и passkeys

Push с контрольным числом.
WebAuthn / FIDO2,
биометрия и аппаратные
ключи.

## Одноразовые коды

TOTP, HOTP
и резервные коды.
Доставка: email, SMS, голос.

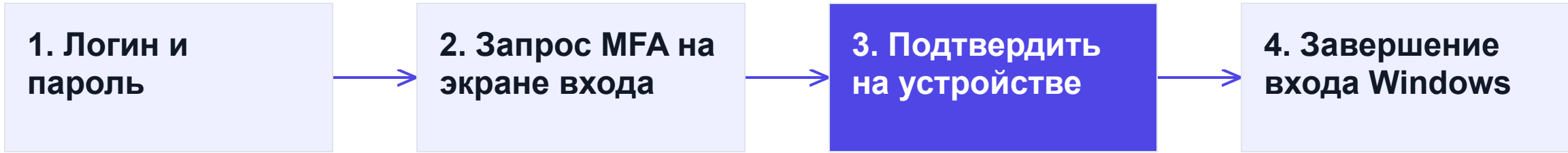
## Мессенджеры

Telegram, eXpress, MAX,
VK Teams, Slack, Mattermost,
Discord и VK.

Доступность канала зависит от его настройки; SMS, голос и боты требуют своего шлюза или сервиса.

СЦЕНАРИЙ 01

# Вход в Windows и RDP




Контрольное число связывает подтверждение с запросом входа.
Политики RDP и локальной консоли настраиваются отдельно.

При недоступности сервера поведение определяется fail-open / fail-close; аварийный доступ задаётся отдельно.

# UAC: подтверждение повышения прав

## Что поддерживается

Второй фактор для UAC с вводом учётных данных. При вводе данных администратора запрос адресуется ему.

## Что нужно настроить

Включить Elevation2FAEnabled и запрос учётных данных в политиках Windows. По умолчанию опция выключена.

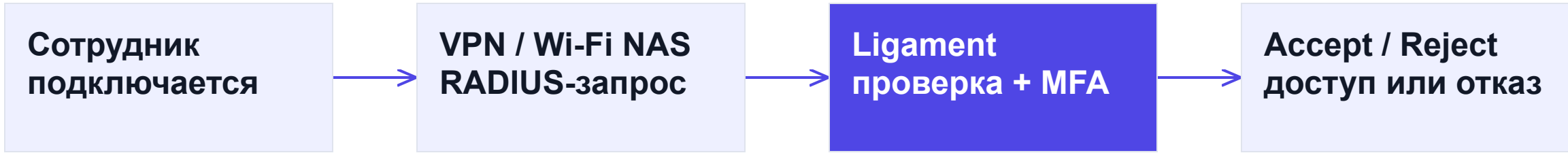
## Границы покрытия

Обычный диалог «Да / Нет» не вызывает этот сценарий. Службы и задачи планировщика не покрываются этим механизмом.

Пилот должен проверять конкретные политики Windows и реальные сценарии повышения прав.

СЦЕНАРИЙ 02

# VPN и Wi-Fi через RADIUS

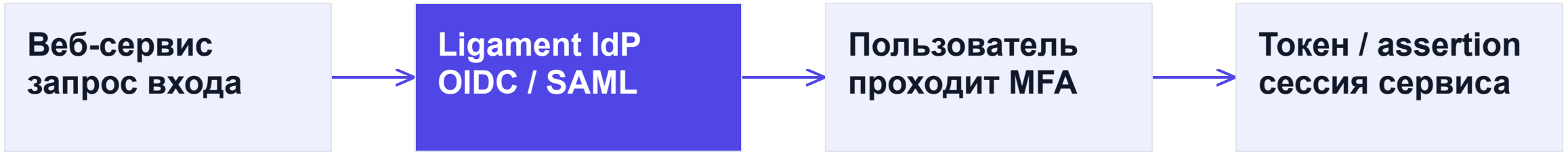



PAP · EAP-TTLS/PAP · PEAP/MS-CHAPv2 · Accounting
Окно доверия устройств — дополнительная лицензируемая функция.

Push требует согласованных таймаутов NAS. Совместимость проверяется для конкретной модели и протокола.

СЦЕНАРИЙ 03

# SSO: единый вход в веб-сервисы




OIDC и SAML реализованы в сервере.
AD / LDAP подключается для проверки учётных данных и синхронизации.

SSO и AD / LDAP требуют разрешённых функций лицензии. Forward-auth — отдельный способ защиты веб-приложений.

# Приложения и самообслуживание

## Одно подтверждение

Мобильные и настольные приложения: push, контрольное число, управление подключениями.

## Платформы

В проекте: Windows, macOS, Linux, Android и iOS.
PWA — доступ через браузер.
Клиент в исходниках: 1.1.24+50.

## Контроль пользователем

Просмотр своих устройств, сессий и истории входов.
Telegram-меню для доступных операций.

Наличие платформы в исходниках не означает наличие опубликованного установщика: проверяется при поставке.

# Филиалы и автономная работа Relay




## Связь доступна

Обновление локального снимка и передача событий в Core.

## Связь прервана

Работа с локально доступными данными. Доставка накопленного аудита после восстановления.

Автономность зависит от локальных факторов, актуальности снимка и лицензии; внешние каналы могут быть недоступны.

# Управление, аудит и эксплуатация

## Политики и роли

Настройки через веб-панель с хранением в PostgreSQL. Группы, устройства, блокировки и политики доступа.

## Наблюдаемость

Журнал событий, экспорт CSV,
Prometheus и health-проверки.
SIEM-коннектор — лицензируемый модуль.

## Сопровождение

Резервное копирование и восстановление.
Отзыв устройств и сессий, контроль событий доступа.

Для промышленного внедрения нужны резервирование, мониторинг и проверенный сценарий восстановления.

# Дополнительные сценарии

## Бастион и SOS

Web-SSH, RDP-проброс, ACL и запись сессий. SOS: обращение пользователя и удалённая помощь.

## Гостевой доступ

Временные учётные записи, сотрудник-спонсор, ограничения по сроку и доступным ресурсам.

## Уведомления

Шлюз доставки с верификацией контактов. События и сообщения через настроенные каналы.

Доступность модулей определяется лицензией. Удалённая помощь и бастион требуют отдельной настройки доступа.

# Free и коммерческие редакции

| Возможности | Free | Demo / платные |
|---|---|---|
| **Лимит пользователей** | До 5 | По условиям лицензии |
| **MFA, RADIUS, аудит, доставка** | Доступны | Доступны |
| **SSO, LDAP, доверие устройств** | Недоступны | При разрешении в лицензии |
| **SIEM, SOS, бастион, гости, notify** | Недоступны | При разрешении в лицензии |
| **Relay и White-label** | Недоступны | Функции + лимит Relay |

Demo заявлен на 30 дней. Платная редакция не отменяет индивидуальный список разрешённых функций.

# Что означает работа без интернета

## Локальная обработка

Сервер, база и локальные факторы находятся у заказчика.
TOTP не требует доставки через внешний мессенджер.

## Бессрочная лицензия

Perpetual работает без онлайн-сверки.
Право на обновления ограничено maintenance-сроком.

## Подписка и Demo

Возможна лицензия с check_url.
При потере связи: grace 7 дней для подписки, 48 часов для Demo.

Обещание полностью изолированного контура допустимо только для подходящей лицензии и набора каналов.

# Сравнение моделей развёртывания

| Продукт / редакция | Развёртывание | Что учитывать |
|---|---|---|
| **Ligament** | Self-hosted: Core + PostgreSQL | Эксплуатация на стороне заказчика |
| **MULTIFACTOR** | SaaS + локальные адаптеры | ФСТЭК-версия — отдельная поставка |
| **MFASOFT SAS** | Локально / у сервис-провайдера | Модульная архитектура, кластеры |
| **Индид Облако.MFA** | SaaS | Не смешивать с Indeed AM |
| **Контур.ID** | Облако / On-premise | Выбирать конкретную редакцию |

On-premise доступен у нескольких вендоров. Оцениваются схема поставки, зависимости и условия сопровождения.

# Сравнение подтверждённых возможностей

| Продукт | Windows / RDP | VPN / RADIUS | Веб / SSO |
|---|---|---|---|
| **Ligament** | Credential Provider | Встроенный сервер | OIDC + SAML IdP |
| **MULTIFACTOR** | Заявлено вендором | RADIUS Adapter | SSO, SAML / OpenID |
| **MFASOFT SAS** | Вход в ОС / агенты | Агент FreeRADIUS | SAML / OIDC / ADFS |
| **Индид Облако.MFA** | Уточнить сценарий | Уточнить интеграцию | Web SSO: «скоро» |
| **Контур.ID** | WinLogon / RDG | RADIUS Adapter | Веб через ADFS |

«Уточнить» означает недостаток данных в проверенном источнике, а не отсутствие функции. Совместимость проверяется пилотом.

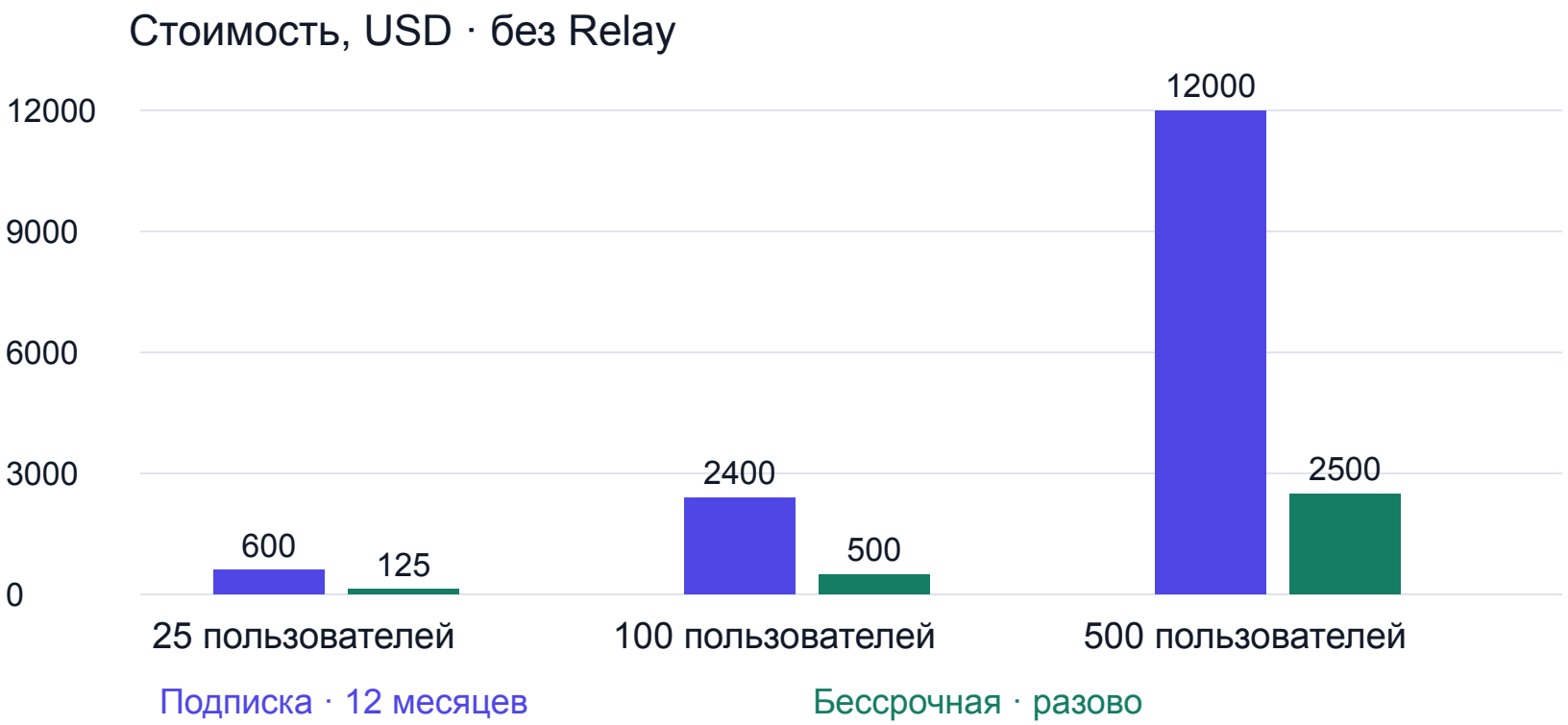
# Цены Ligament

| Редакция | Пользователи | Relay |
|---|---|---|
| **Free** | 0 · до 5 пользователей | Нет |
| **Demo** | 0 · заявлено 30 дней | По выданной лицензии |
| **Подписка** | 2 USD / пользователь / месяц | 400 USD / узел / срок |
| **Бессрочная** | 5 USD / пользователь разово | 1 000 USD / узел разово |

**Тарифы из описания проекта; оплата заявлена в USDT.**

Акция «12 + 1 месяц» описана неоднозначно: расчёты далее используют 12 оплаченных месяцев без бонуса. Условия фиксируются в КП.

# Как стоимость зависит от числа пользователей




**24 × N**

Подписка за 12 месяцев

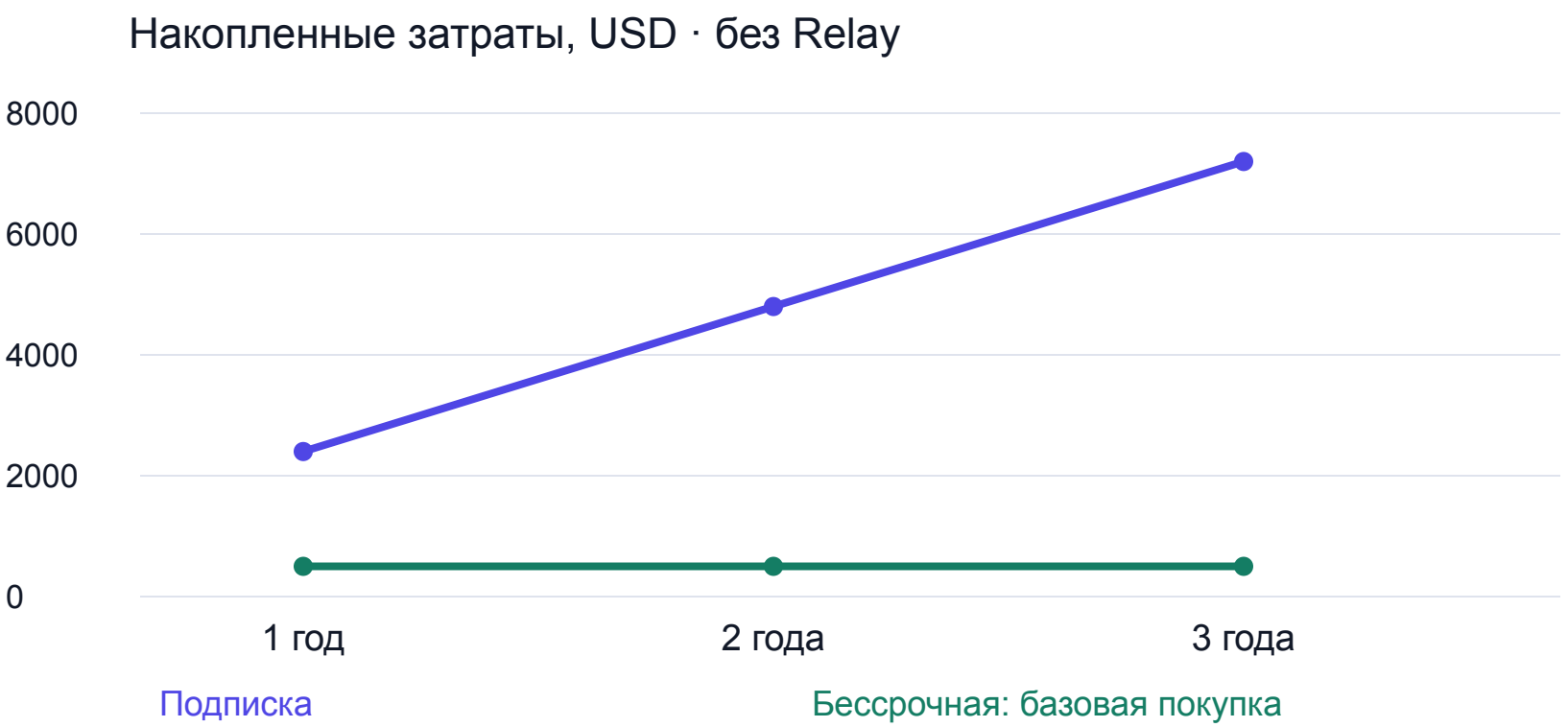
**5 × N**

Бессрочная лицензия

N — число лицензируемых пользователей. Только лицензии: без инфраструктуры, внедрения, SMS и стоимости обновлений.

ПРИМЕР: 100 ПОЛЬЗОВАТЕЛЕЙ

# Затраты на лицензии за 1–3 года




## Подписка

2 × 100 × 12 × годы

## Бессрочная

5 × 100 = 500 USD
Обновления — отдельно

Это не полный TCO: продление maintenance и поддержки не оценено. Бонусный месяц и скидки в расчёт не включены.

# Публичные ценовые ориентиры аналогов

| Продукт | Публичный ориентир | Основание / ограничение |
|---|---|---|
| **MULTIFACTOR** | От 344 ₽ / лицензия / месяц | Стандартный; SSO — от 420 ₽ |
| **MFASOFT SAS** | От 661 000 ₽ | Локальное внедрение: от 250 лицензий |
| **Индид Облако.MFA** | Прайс по запросу | Цена зависит от тарифа и договора |
| **Контур.ID** | КП по запросу | Единый сопоставимый прайс не найден |

Разные комплектации и валюты: это ориентиры, не рейтинг дешевизны. Итоговые цены, налоги и поддержка уточняются в КП.

# Плюсы, ограничения и выбор решения

## + Сильные стороны

Контроль своей инфраструктуры.
Free для небольшой команды.
MFA, SSO и Relay в одном продукте.
Несколько способов подтверждения.

## – Ограничения

Сопровождение сервера и БД.
Часть модулей требует лицензии.
UAC зависит от политики Windows.
Внешним каналам нужна связь.

## Критерии выбора

Проверить реальные интеграции,
работу при отказах и поддержку.
Сертификаты и реестр — по документам нужной поставки.

Ligament подходит для контроля локального контура; требования к сертификации, SLA и масштабу проверяются отдельно.

СЛЕДУЮЩИЙ ШАГ

# Пилот и источники

## 1. Выбрать ресурс → 2. Настроить факторы → 3. Проверить отказы

Начать с небольшой группы. Проверить вход, отказ, потерю устройства, недоступность сервера и восстановление из резервной копии.

## ligam.org · admin@ligam.org

Источники: исходники 2fa и ligament-apps; описание Ligament;
multifactor.ru · mfasoft.ru · indeed-cloud.ru · support.kontur.ru
Подробные ссылки и условия расчётов — в заметках слайдов и файле SOURCES.md.