



# БЕЗОПАСНОСТЬ НАЧИНАЕТСЯ ЗДЕСЬ

**Павел Евенок**

**Руководитель отдела продаж**





## Наша миссия

Создание собственной экосистемы продуктов для безопасности ИТ-инфраструктуры заказчиков.



**120+** партнеров



**500+** успешных кейсов  
внедрения



**30+** интеграций с российскими  
разработками и платформами



**500 000 +**  
пользователей системы  
(по итогам 2023 г.)



## Команда

опытных  
профессионалов



**Кастомизация** решения  
под бизнес-цели заказчика



Реагирование на инциденты  
**24/7**



Соответствие стандарту  
**PCI DSS**

## Реестр отечественного ПО

Решение MULTIFACTOR находится в реестре российского ПО [№7046](#).

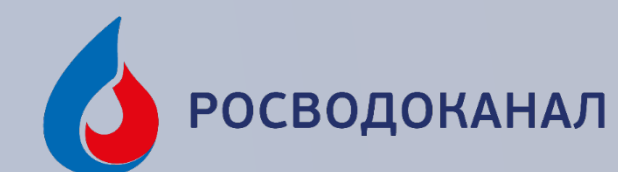
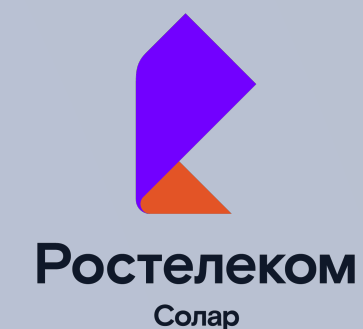
Решение доступно бесплатно до трех пользователей

[Подключить](#)



# Нам доверяют

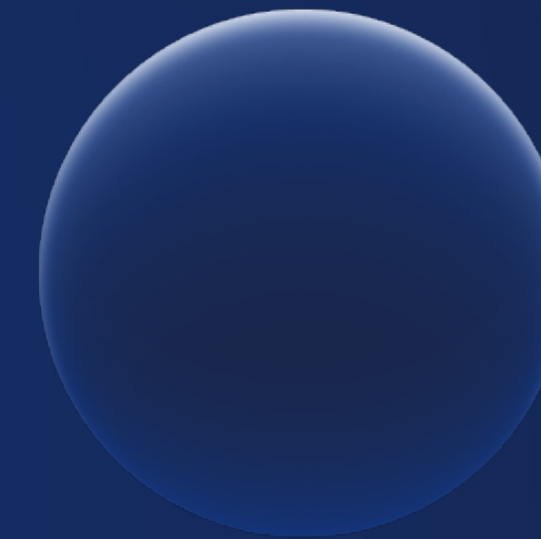
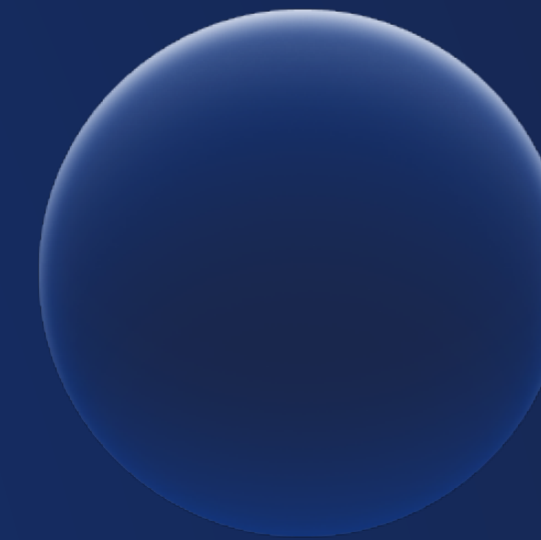
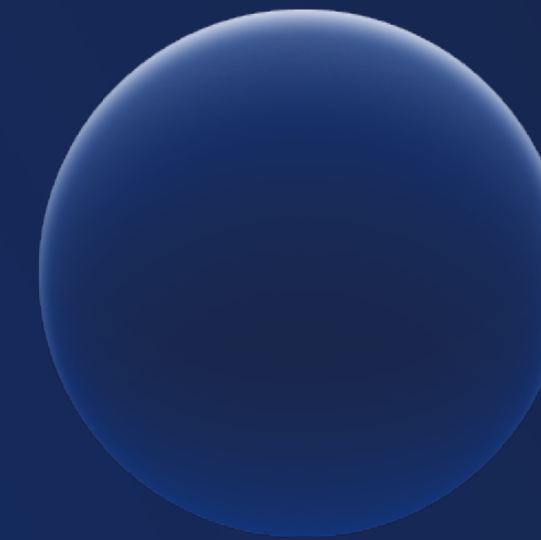
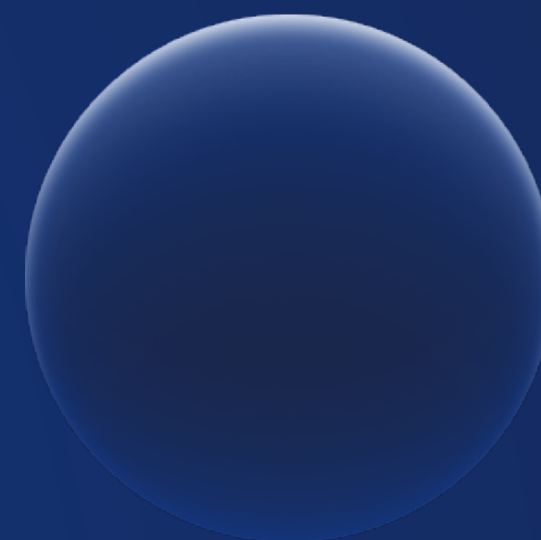
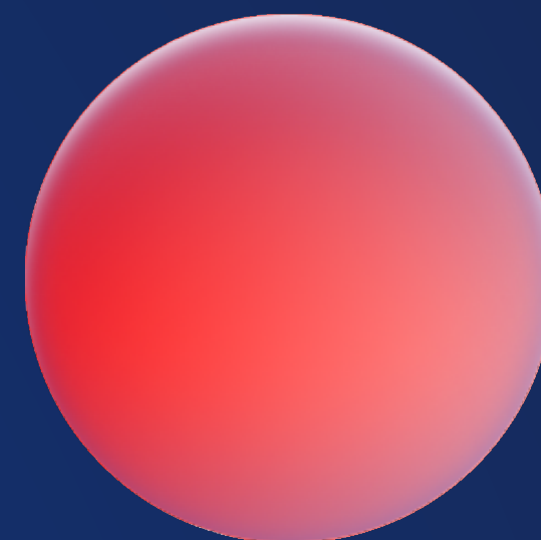
0 компании





**Боли рынка**

**01**







# ₽ 20 МЛН

Средний ущерб от кибератак хакеров для компаний в России <sup>1</sup>

## 14 млн

Россиян в 2023 г. работают удаленно <sup>2</sup>

## На 60%

Выросло количество утечек в мире за 2023 год <sup>3</sup>

## > 4 млн записей ПДн

Приходится в среднем на одну утечку информации.

В 2022 году в результате одной утечки в среднем было скомпрометировано 2,98 млн записей ПДн, то в 2023 году — 4,04 млн записей, то есть произошел рост на 35,6% <sup>3</sup>

**В результате компании сталкиваются с:**

- ▶ прямым и косвенным финансовым ущербом;
- ▶ ущербом репутации и потерей клиентов;
- ▶ кражей интеллектуальной собственности и коммерческой тайны;
- ▶ санкциями от регуляторов за несоблюдение нормативных требований.

<sup>1</sup> По данным [исследования «РТК-Солар» за 2023 г.](#)

<sup>2</sup> По данным онлайн-опроса ВЦИОМа на 2022 г.

<sup>3</sup> По данным аналитического отчета InfoWatch: [«Утечки информации в мире, 2022-2023 годы»](#)



# Проблемы

01 Боли рынка



## Небезопасность удалённых подключений

- ▶ Текущая геополитическая ситуация в стране, санкции, информационная война, хакинг, вирусы, фишинг и другие векторы атаки указывают на то, что пароли недостаточны для адекватной защиты.
- ▶ Подключения к ресурсам организации со скомпрометированных аккаунтов.
- ▶ Не отозванные доступы при увольнении сотрудника.



## Неэффективные процессы управления доступом

- ▶ Результат простоя бизнес-процессов из-за нерешённых проблем с доступом — значительные финансовые и временные издержки.
- ▶ Высокая нагрузка на команду IT-поддержки в связи с онбордингом и офбордингом пользователей, организацией удалённого доступа, обслуживанием учетных записей, сменой забытых паролей и паролей с истёкшим сроком действия.

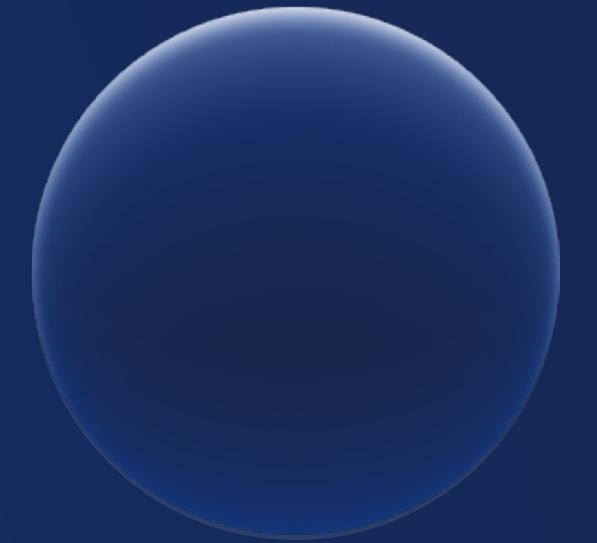
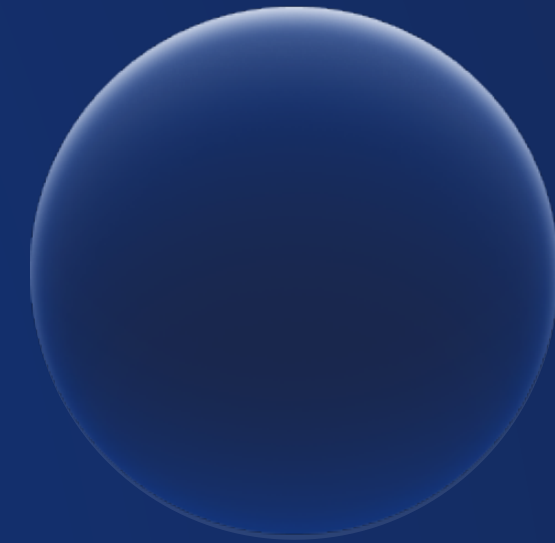


Реализация киберриска — вопрос времени, если превентивно не принять мер защиты подключения к корпоративным ресурсам.



**Решение**

**02**





# MULTIFACTOR

Сотрудники

Партнёры

Клиенты



## Провайдер учётных записей

- [MultiDirectory](#) – LDAP-каталог УЗ от МУЛЬТИФАКТОР
- Active Directory
- Linux Astra Directory
- NPS
- Samba 4
- Freeipa

✓ Защита входа

✓ Простая интеграция

✓ Покрытие всей инфраструктуры





### Отечественные и зарубежные VPN-шлюзы

- [UserGate](#)
- [С-Терра](#)
- [КриптоПро NGate](#)
- [Континент 4](#)
- [Ideco UTM](#)
- Рубикон
- [CheckPoint](#)
- [Cisco](#)
- [FortiGate](#)
- [Mikrotik](#)
- [OpenVPN](#)



### Облачные приложения, виртуализация, web

- [SAML](#)
- [OIDC](#)
- [OAuth-приложения](#)
- Мобильные приложения
- [Outlook Web Access \(OWA\)](#)
- [VMware](#)
- [Huawei Cloud](#)
- [Яндекс.Облако](#)
- [Веб-сайты](#)
- и др.



### Linux

- [SSH](#)
- [SUDO](#)
- [OpenVPN](#)
- PAM
- и др.



### VDI

- [VMware Horizon](#)
- [Citrix](#)
- [Remote Desktop](#)
- и др.



### Windows

- [Windows Logon](#)
- [VPN](#)
- [RD Gateway](#)
- [NPS](#)
- и др.



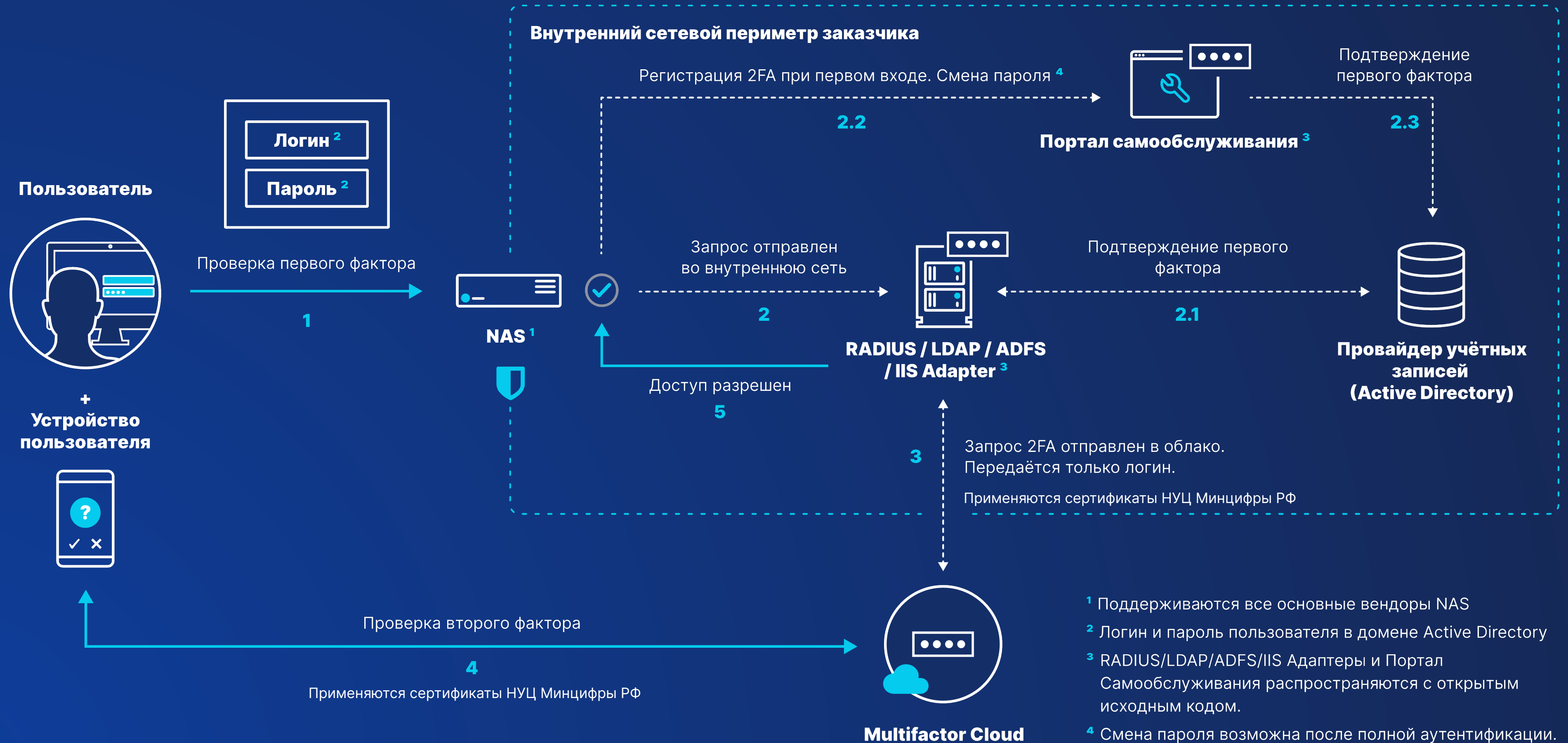
### Другое ПО

- [СКДПУ АйТи-Бастион](#)
- [1С-Bitrix24](#)
- [Точки доступа Wi-Fi](#)
- и др.



### SIEM-системы

- MULTIFACTOR совместим с SIEM-системами благодаря поддержке стандартных протоколов.

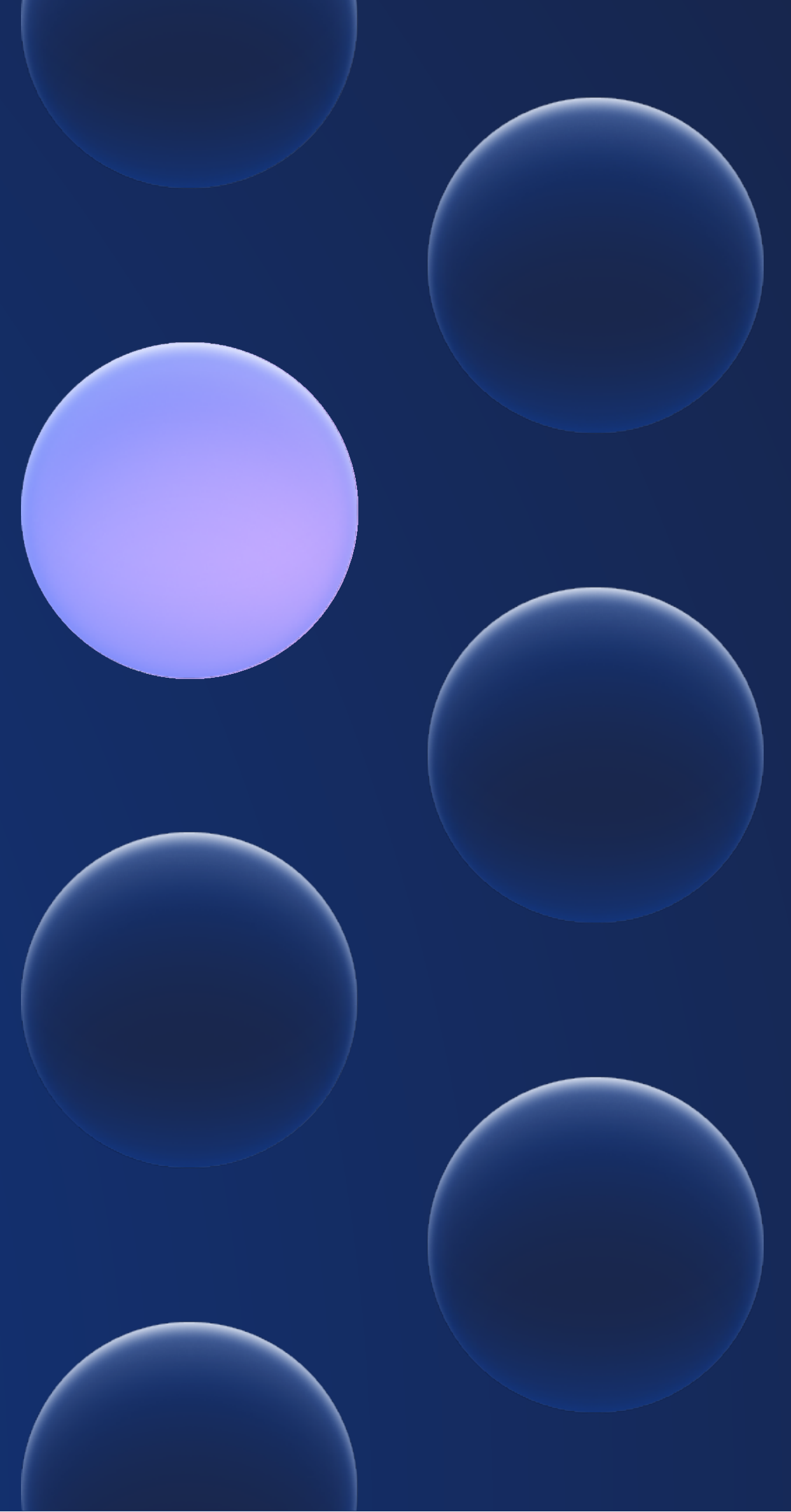


- <sup>1</sup> Поддерживаются все основные вендоры NAS
- <sup>2</sup> Логин и пароль пользователя в домене Active Directory
- <sup>3</sup> RADIUS/LDAP/ADFS/IIS Адаптеры и Портал Самообслуживания распространяются с открытым исходным кодом.
- <sup>4</sup> Смена пароля возможна после полной аутентификации.



# Обзор технологии MFA

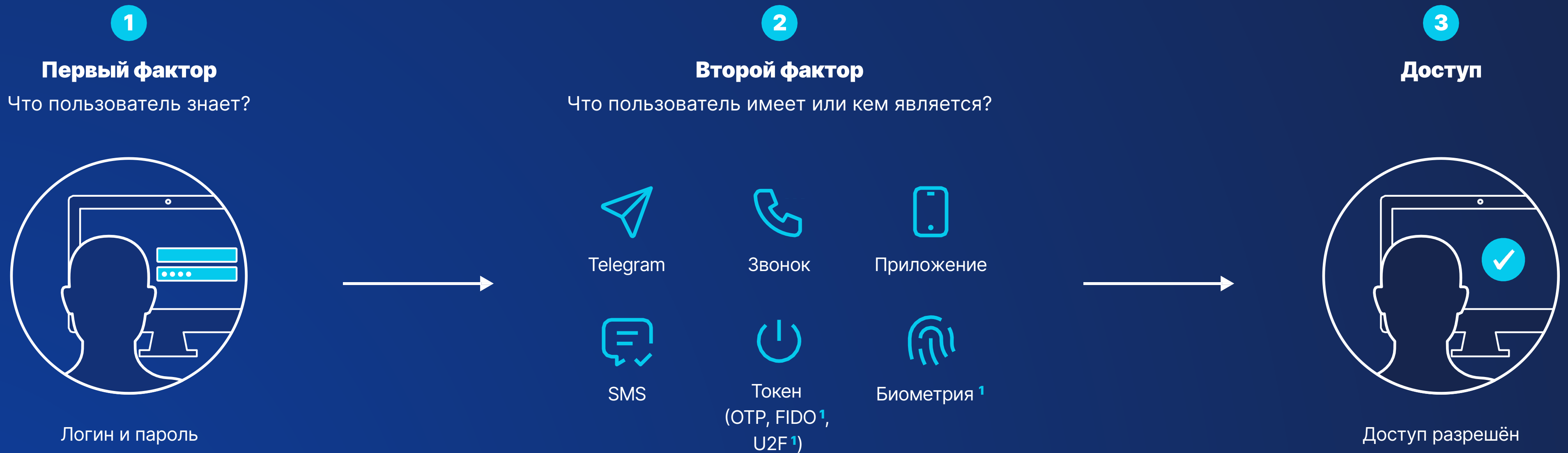
# 03





## Мультифакторная аутентификация

Пользователи могут подтвердить свою личность тем, что они знают (основной метод аутентификации, как правило, логин и пароль); тем, что у них есть (например, аппаратный или программный токен); тем, кем они являются (биометрия). Последние два — возможные способы проверки второго фактора.



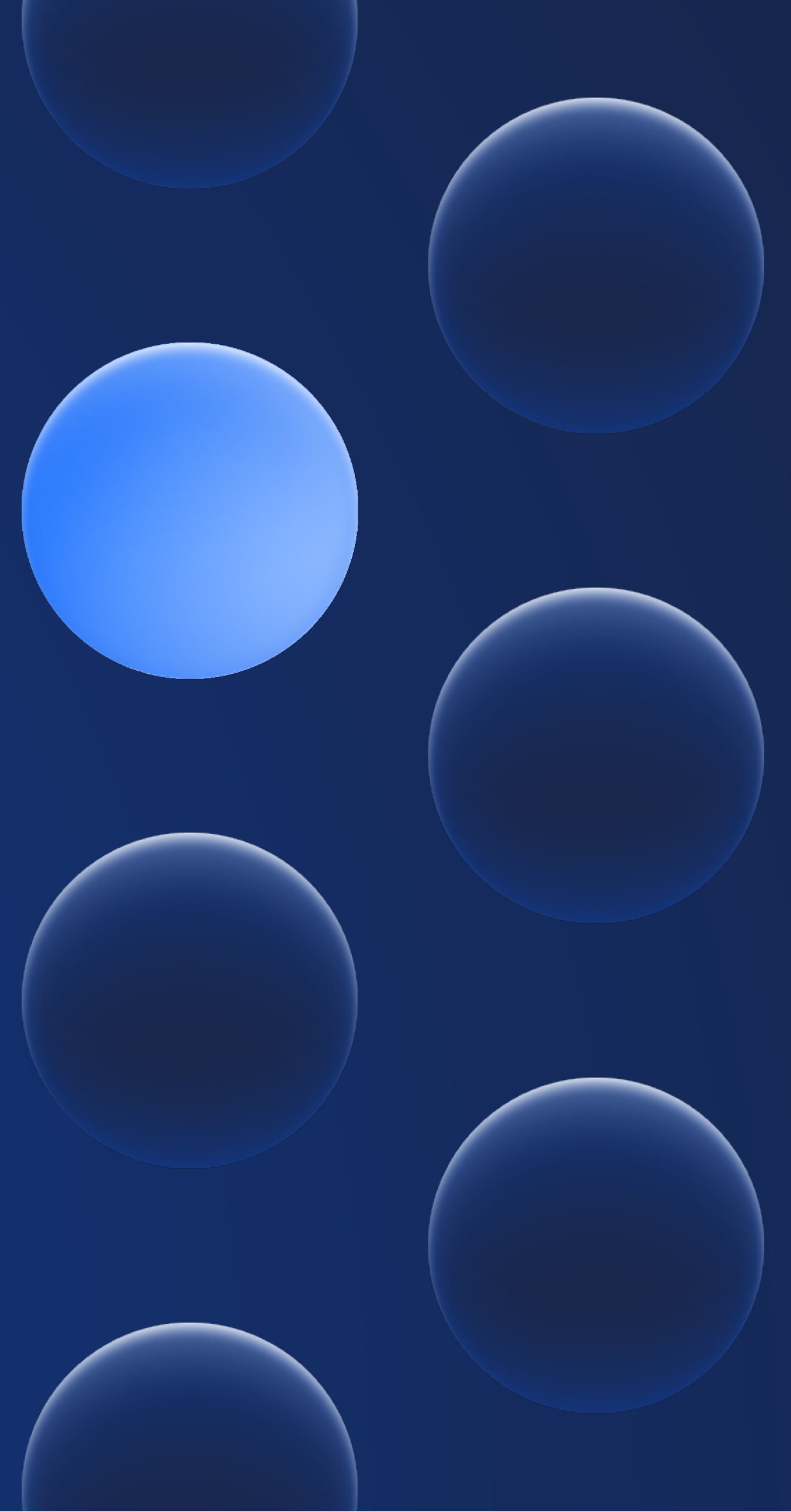
<sup>1</sup>FIDO, U2F токены и биометрия недоступны в конфигурации с межсетевыми экранами NAS (Checkpoint, Cisco, Mikrotik и др.) и VDI.





# Портал самообслуживания Self-Service Portal (SSP)

# 04





## Портал самообслуживания для пользователей Active Directory и других LDAP-каталогов

Позволяет пользователю самостоятельно настраивать и подтверждать владение вторым фактором доступа, менять текущий, истекший или забытый пароль после полной аутентификации. Управление устройствами Exchange ActiveSync. [Подробнее о портале на сайте](#)



Самостоятельный онбординг пользователей

### 2FA

Самостоятельная конфигурация 2FA



Возможность самостоятельного восстановления забытых паролей пользователями Active Directory (при условии прохождения предварительной аутентификации в мобильном приложении Multifactor)



Решение проблем с доступом без участия IT-поддержки

Компонент поставляется с открытым исходным кодом для Windows и Linux.

### Мин. системные требования:

1 ядро CPU

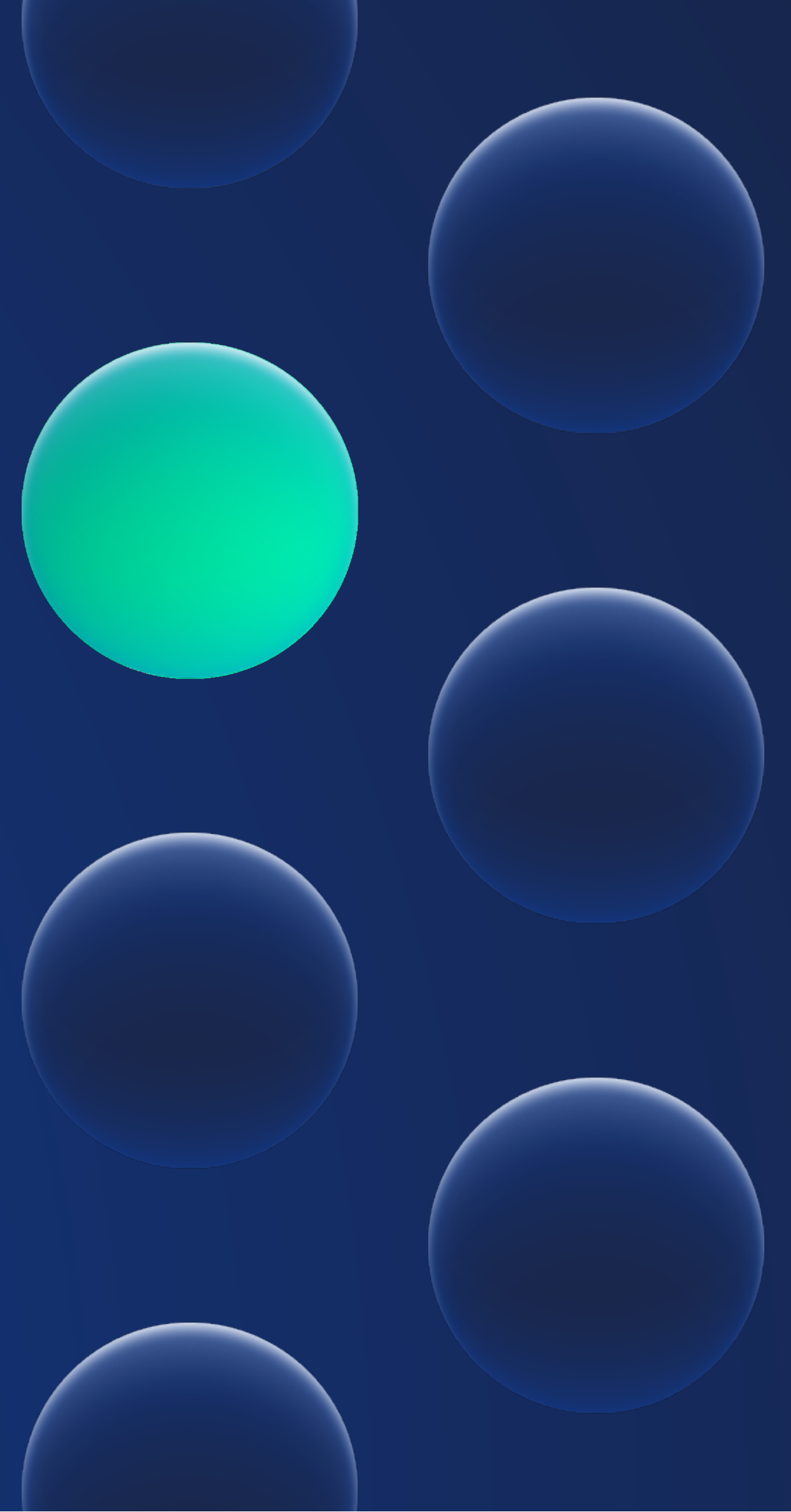
2Gb RAM

Windows Server 2012 и выше



# Обзор технологии Единый вход (SSO)

# 05





## SSO MULTIFACTOR — упрощение контроля доступа к корпоративным приложениям и второй фактор



### Уменьшение затрат

Единый провайдер учётных записей позволяет легко управлять всеми пользователями организации, выдавая доступы в зависимости от должности.



### Улучшенный пользовательский опыт

Отпадает необходимость запоминать множество паролей и учётных записей. Возможность изменения паролей во всех сервисах в пару кликов.



### Лучшее соответствие требованиям безопасности

Внедрение второго фактора во все системы, вне зависимости от их возможностей.



### Настраиваемые парольные политики

Парольные политики зависят от провайдера учётных записей, а не от сторонней системы.



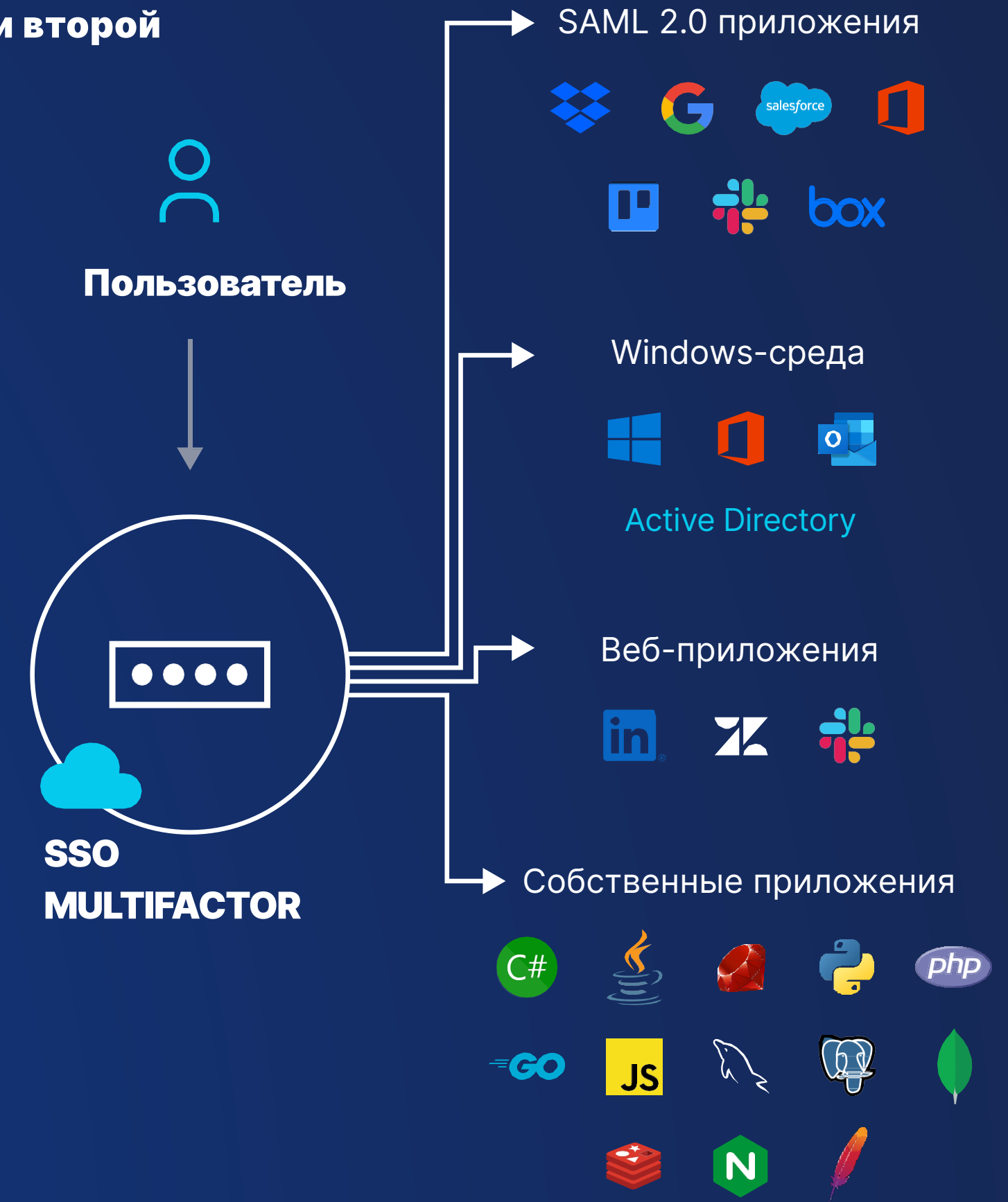
### Увеличенная продуктивность

Упрощенный контроль за доступами пользователей. Простое управление перемещением человеческих ресурсов организации.



### Упрощённая связность

Интеграция нового приложения в инфраструктуру компании занимает меньше времени.

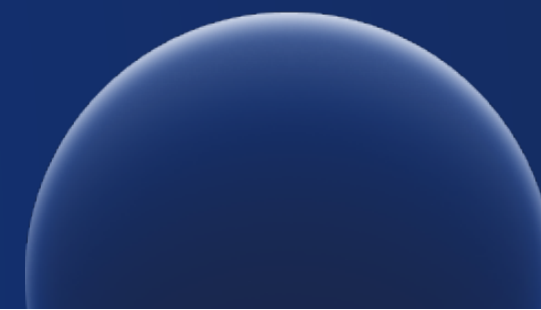
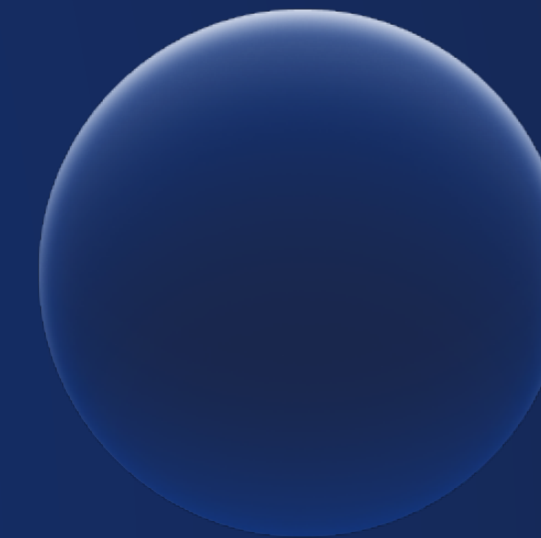
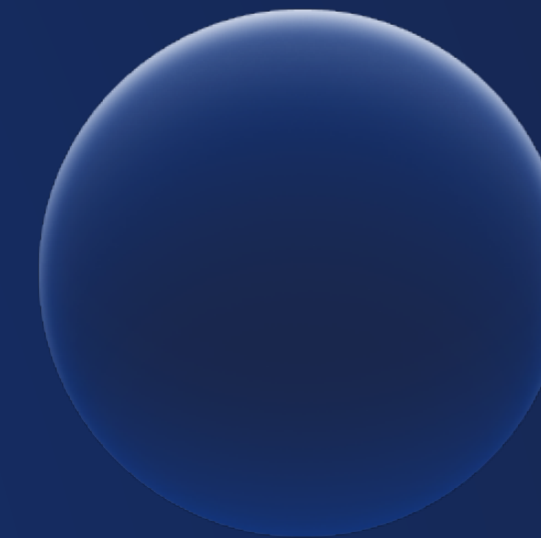
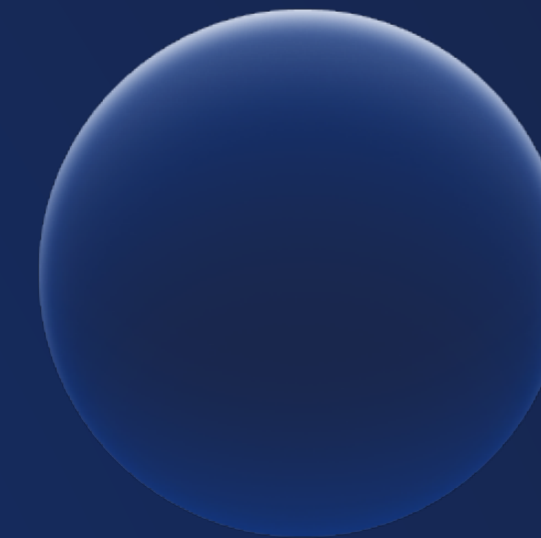
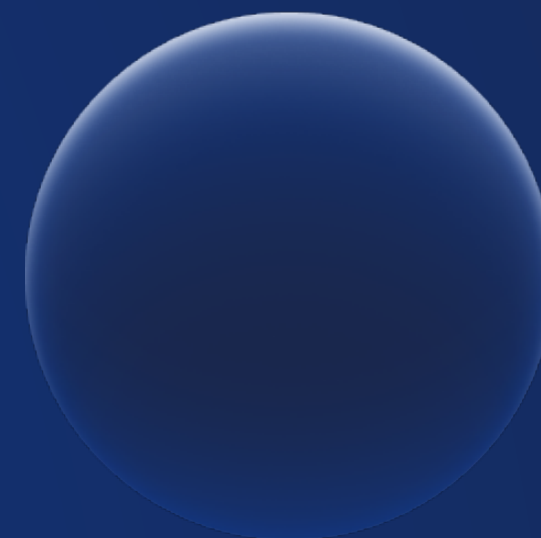






# Состав решения

06





## 1 Компоненты On-Premise

### 1. Портал самообслуживания

- Самостоятельная регистрация сотрудником второго фактора аутентификации в Multifactor Cloud;
- Смена пароля в корпоративном домене Active Directory с обязательной проверкой текущего пароля и подтверждением вторым фактором в Multifactor Cloud;
- Компонент поставляется [с открытым исходным кодом для Windows и для Linux](#)

#### Мин. системные требования для Windows:

1 ядро CPU

2Gb RAM

Windows Server 2012 и выше

#### Мин. системные требования для Linux:

1 Linux-сервер, протестирован на Debian 11

### 2. RADIUS, LDAP, ADFS, IIS Адаптеры

- Приём запросов на аутентификацию сотрудника в CheckPoint VPN, RDP и Citrix по протоколам;
- Проверка первого фактора аутентификации (логин и пароль) в домене;
- Проверка второго фактора аутентификации в Multifactor Cloud;
- Компоненты поставляются [с открытым исходным кодом для Windows и Linux](#).

#### Мин. системные требования для Windows:

4 ядра CPU

4Gb RAM

Windows Server 2012 и выше

#### Мин. системные требования для Linux:

1 CPU

2 GB RAM

8 GB HDD

## 2 Облако Multifactor

### [multifactor.ru](https://multifactor.ru)

Безопасное размещение в ДЦ DataLine, Selectel и Yandex Cloud

- Подтверждение и подпись запросов на аутентификацию пользователей вторым фактором;
- Личный кабинет IT-службы вашей организации для управления и контроля доступа сотрудников к ресурсам с 2FA;
- Журнал событий;
- API и инструменты разработчика.

#### SLA

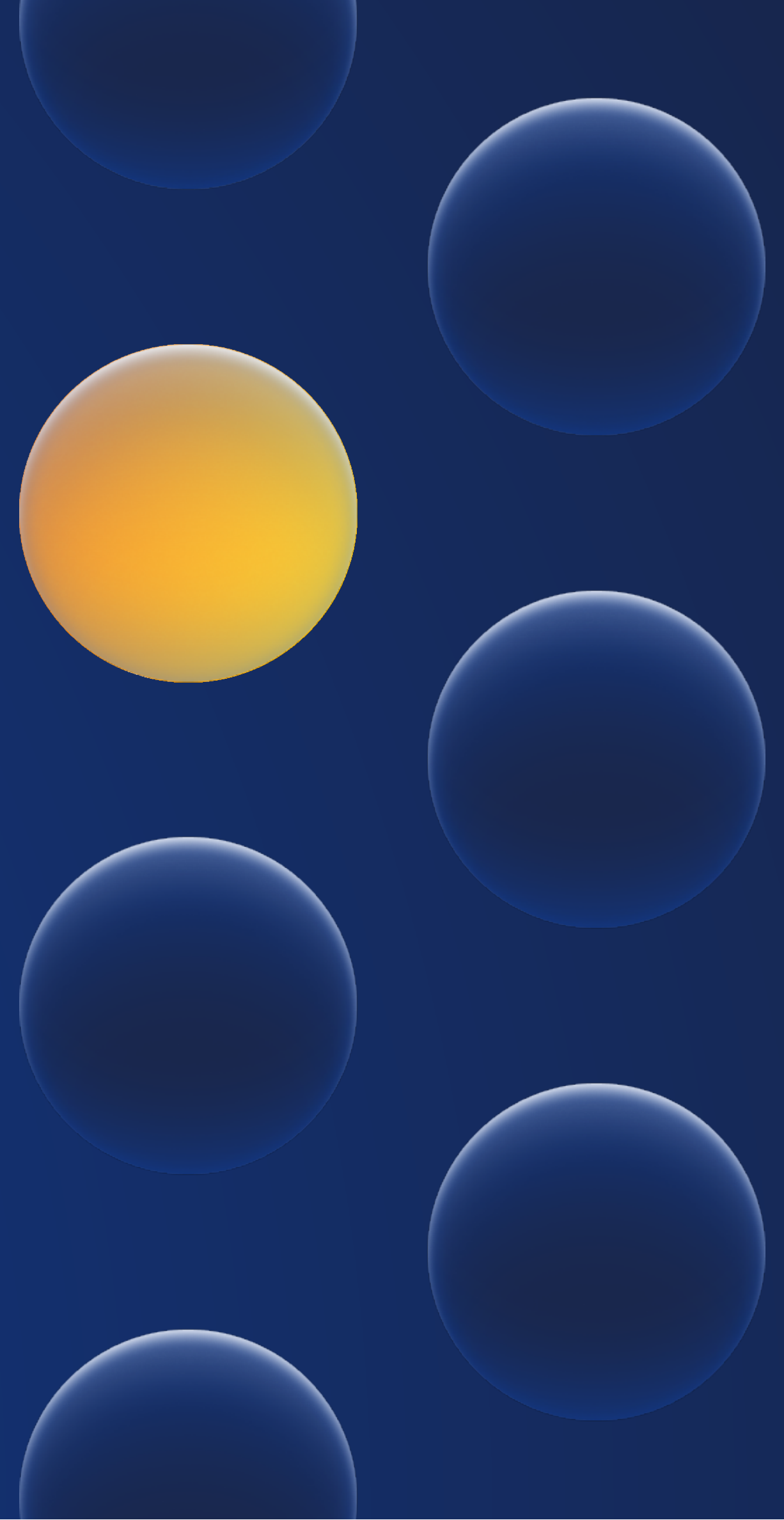
● Аптайм **99.99%**

● Тех. поддержка



# Почему MULTIFACTOR?

# 07





### Высокая доступность

Аптайм 99.98% времени. Решение, проверенное реальными интеграциями с клиентами.



### Отказоустойчивость

Отказ облака Multifactor не скажется на вашем бизнесе. В худшем случае инфраструктура возвращается на предыдущий уровень доступа, без использования второго фактора.



### Производительность

Облако Multifactor — 1800 tps; RADIUS Adapter - 120 tps <sup>1</sup>



### Безопасность инфраструктуры

Облако Multifactor располагается в дата-центрах DataLine, Selectel, Yandex Cloud в Москве с многоуровневой физической защитой, резервными интернет-каналами и источниками питания.



### Масштабируемость

Без ограничений по количеству пользователей и ресурсов.



### Нулевой CAPEX

SaaS решение для любого бизнеса.



### Простая адаптация пользователей

Интуитивный и простой процесс подключения пользователей к многофакторной аутентификации. Возможность автоматического подключения.



### Упрощение работы пользователей

MULTIFACTOR позволяет упростить парольные политики. Комбинируется с возможностями SSO.



### Настройка любых процессов

Возможность добавить любую необходимую бизнес-логику.



### Режим Bypass

Позволяет группам или отдельным пользователям входить без второго фактора

**SLA**

● Аптайм **99.99%**

● Реагирование на инциденты **7x24x1H**

<sup>1</sup>Горизонтальное масштабирование при необходимости





**Остались вопросы?**

**[p.evenok@multifactor.ru](mailto:p.evenok@multifactor.ru)**

**Павел Евенок**

Руководитель отдела продаж

+7 921 427 78 70