



# ЭВОЛЮЦИЯ РАМ-ТЕХНОЛОГИЙ И ВЕКТОРЫ РАЗВИТИЯ INDEED PRIVILEGED ACCESS MANAGER

Практика, тенденции, подходы

# О НАШЕЙ КОМПАНИИ

Компания Индид — российский вендор программного обеспечения для повышения информационной безопасности в компаниях разных отраслей экономики

**200+**

**АКТИВНЫХ  
ЗАКАЗЧИКОВ**

**14**

**ЛЕТ ОПЫТА**

Проектирование, разработка, тестирование и внедрение комплексных решений

**3**

**РАЗРАБОТАННЫХ  
ПРОДУКТА**

в Реестре отечественного ПО

**80+**

**СОТРУДНИКОВ**

Распределенная команда:  
4 региона, 3 страны

**3**

**ОФИСА В РОССИИ**

Москва, Санкт-Петербург,  
Великий Новгород

**5**

**СТРАН  
ПРИСУТСТВИЯ В СНГ**

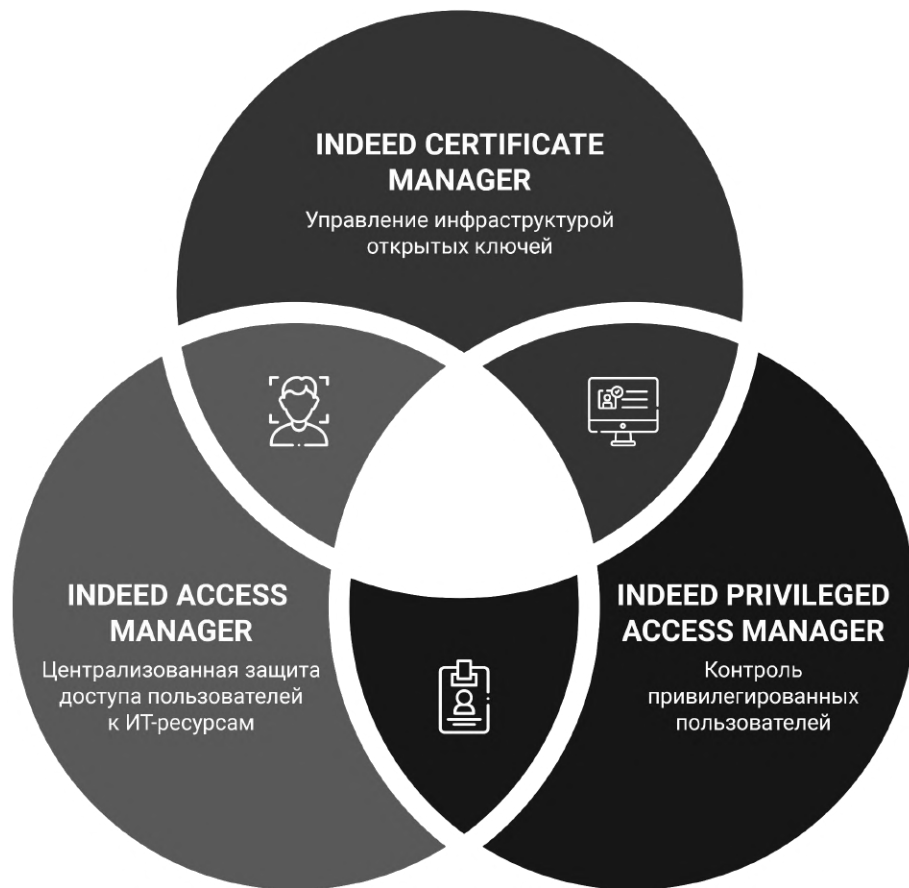
Россия, Казахстан, Беларусь,  
Узбекистан, Кыргызстан

**90+**

**РЕГИОНАЛЬНЫХ  
ПАРТНЕРОВ**

## НАШИ ПРОДУКТЫ

Все продукты находятся  
в Реестре отечественного  
программного обеспечения



# ПРОБЛЕМЫ КОНТРОЛЯ АДМИНИСТРАТОРОВ



## ОТСУТСТВИЕ ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ



### Кража данных, нарушение работы критичных компонентов

Слабо защищенный удаленный доступ администраторов и подрядчиков к критичным компонентам ИТ-инфраструктуры — источник повышенной опасности.



### Слабый контроль работы администраторов или подрядчиков

Контроль действий привилегированных пользователей не осуществляется, либо осуществляется частично через не предназначенные для этого инструменты.



### Лишние расходы на организацию работы

Затруднен учет реального объема работ и соблюдения требований SLA. Локальная работа с критичными компонентами требует затрат на логистику и снижает оперативность реагирования на сбои.



### Снижение производительности труда офицеров безопасности

Чрезмерные трудозатраты на расследование сбоя или инцидента при использовании данных из “классических” систем мониторинга, т.к. они не показывают полную картину причин инцидента и виновных.

**УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ**

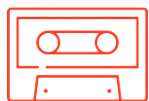
**НЕЭФФЕКТИВНЫЕ ЗАТРАТЫ РЕСУРСОВ**

# INDEED PRIVILEGED ACCESS MANAGER

Контроль действий привилегированных  
пользователей



Контроль  
административных  
учетных записей



Разные способы  
записи и анализа  
действий



Управление  
привилегированным  
доступом



Двухфакторная  
аутентификация

# РАСПРЕДЕЛЕННОЕ УПРАВЛЕНИЕ ДОСТУПОМ



## Поддержка протоколов:

- RDP
- SSH, Telnet
- HTTP(S)
- Иные проприетарные протоколы через публикацию приложений (RemoteApp)

## Поддержка управления паролями целевых ресурсов:

- Active Directory / OpenLDAP\* / FreeIPA\*
- MS Windows
- Linux/Unix
- СУБД (PostgreSQL, MS SQL, MySQL, Oracle DB)
- Web-Application
- Desktop Application

## Поддержка способов контроля действий:

- Видеозапись
- Текстовая запись
- Снимки экрана
- Теневое копирование файлов
- Блокировка ввода команд
- Разрыв удаленного подключения

## Поддержка интеграции:

- SIEM (syslog)
- Mail (SMTP)
- IdM
- API

\* Поддержка OpenLDAP / FreeIPA - в IV кв. 2022 г.

# РАЗВИТИЕ РАМ-ТЕХНОЛОГИЙ\*

Тренды развития рынка PAM:

Работа с учетными записями и аутентификаторами по модели «Нулевое доверие» (Zero Trust)

Предоставление доступа «Точно в срок» (Just-In-Time)

Улучшение пользовательского опыта

Поглощения и слияния для расширения функционала

\* Согласно циклу аналитических отчетов компании Gartner, 2019-2022



Поддержка усиленной аутентификации  
Поиск привилегированных учетных записей (Account Discovery)  
Управление машинными учетными записями (службы, скрипты, конфигурации, среды разработки и т.п.)



Запись действий, выявление команд и операций, с последующим анализом, включая выявление аномалий поведения  
Повышение привилегий и делегирование (Elevation & Delegation)



Автоматизация и оптимизация управления доступом  
Расширение возможностей интеграции с компонентами ИТ-инфраструктуры



Упрощение инсталляции и исчерпывающий набор материалов для эксплуатации  
Облачные инсталляции

## 01. ZERO TRUST - НУЛЕВОЕ ДОВЕРИЕ:

Пользователи не умеют обращаться с паролями

Администраторы могут забыть сменить пароль

Администраторы могут забыть поставить учетную запись под контроль

Подрядчики могут слить или скомпрометировать пароль

Пользователи могут обманывать о компрометации пароля



# УПРАВЛЕНИЕ ПАРОЛЯМИ УЧЕТНЫХ ЗАПИСЕЙ

Основные возможности:

Автоматический поиск и импорт учетных записей

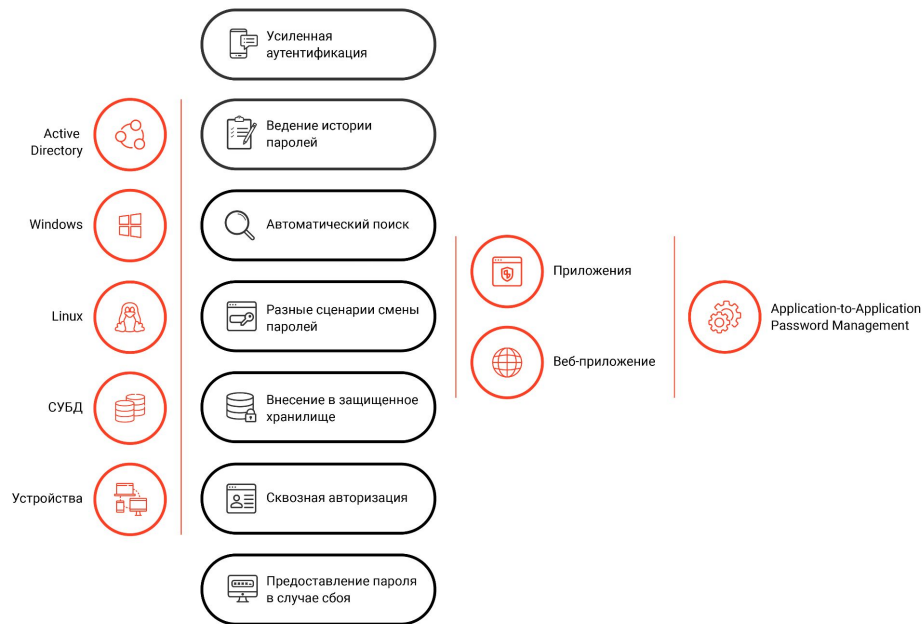
Управление паролями (обновление, выдача, сброс после подключения)

Поддержка пользовательских учетных записей

Enterprise Single Sign-On для целевых приложений

Усиленная аутентификация

Application-to-Application Password Management\*



\* Реализация AAPM - в версии 2.7 в III кв. 2022 г.

# КАТЕГОРИЗАЦИЯ ПРИВИЛЕГИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ



# КЕЙС – СТС МЕДИА

Обеспечена единая точка входа для привилегированных пользователей разных доменов с ресурсами, опубликованными через терминальные серверы на разных площадках

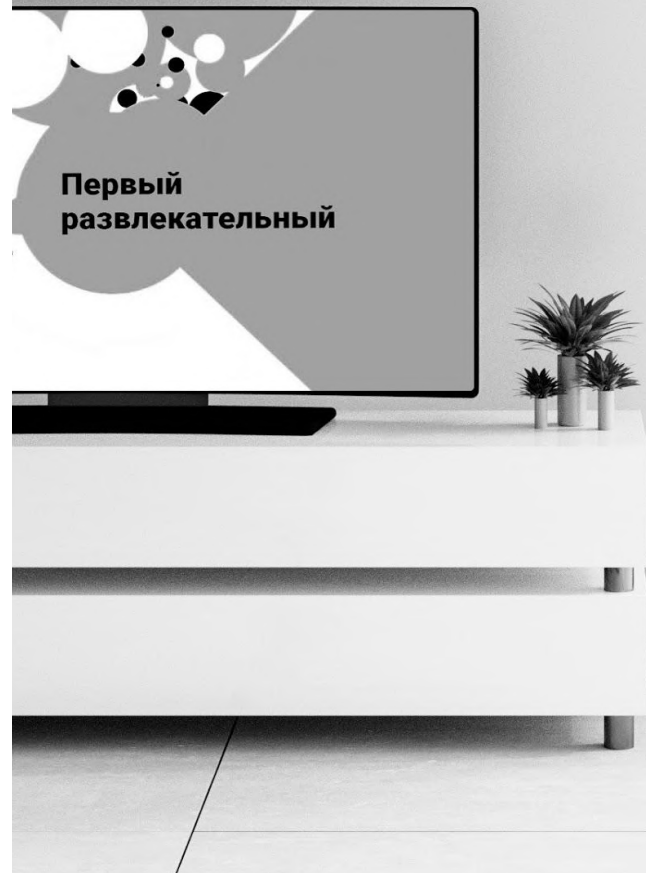
Используются механизмы многофакторной аутентификации привилегированных пользователей

Реализован контроль доступа к опубликованным на терминальных серверах корпоративным приложениям

[Интервью с начальником службы безопасности «СТС Медиа» о внедрении Indeed PAM](#)

**Охват пользователей:** более 100

Indeed Privileged Access Manager




# АКЦЕНТ РАЗВИТИЯ: КОНТРОЛЬ ПОЛЬЗОВАТЕЛЬСКИХ И МАШИННЫХ УЧЕТНЫХ ЗАПИСЕЙ

Реализовано
  Запланировано
  В перспективе


**КОМПАНИЯ  
ИНДИД**

		2018-2021				2022	2023	
Account Discovery	OS & User Catalog	Linux/Unix (SSH, Telnet)	Windows (RDP, WMI, RPC)	Active Directory (LDAP)			<b>Поддержка OpenLDAP, FreeIPA, ALD</b>	Другие
Сквозная аутентификация	App & Web-App	СУБД (via ESSO)	HTTP(S) (via ESSO)	App & Web-App (via ESSO)			Дополнительные приложения, исходя из запросов	СУБД (SQL)
Защищенное хранилище	Devices	*nix-based (SSH/Telnet)	Console (via ESSO)	Cisco (IOS)	Inspur BMC		Дополнительные устройства, исходя из запросов	Другие
Обновление и проверка паролей	Machine					<b>Application-to Application Password Manager</b>	Службы, Планировщик, Реестр и конфигурационные файлы	

## 02. JUST IN TIME ACCESS - ДОСТУП ТОЧНО В СРОК:



Оптимальное использование вычислительных ресурсов и лицензий  
Предоставление доступа в заданное время по согласованию  
Динамическое создание правил доступа по заявке  
Временное предоставление доступа на период работ  
Динамическое изменение прав и полномочий учетных записей

# ЕДИНАЯ ТОЧКА УДАЛЕННОГО ДОСТУПА

Единый инструмент управления привилегированным доступом

Интеграция с ServiceDesk

Интеграция с Active Directory, OpenLDAP\*, FreeIPA\*

Импорт ресурсов из Active Directory, OpenLDAP\*, FreeIPA\* и CSV

Поддержка протоколов: RDP, SSH, Telnet, HTTP(S)

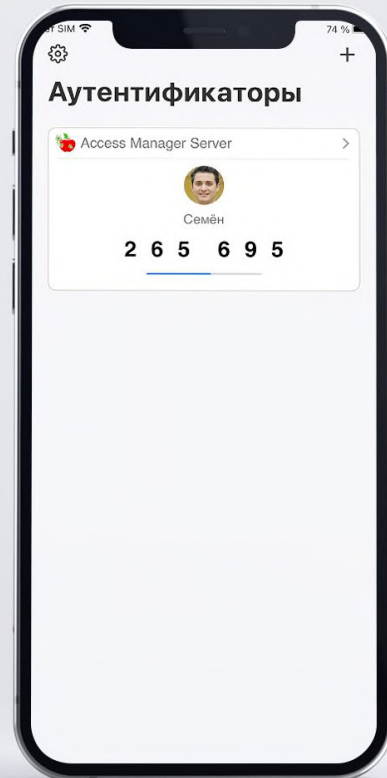
Поддержка публикации приложений (RemoteApp & Microsoft RDS)



# INDEED KEY: МОБИЛЬНОЕ ПРИЛОЖЕНИЕ ДЛЯ ЗАЩИТЫ ДОСТУПА

- | Поддержка протокола аутентификации TOTP (одноразовые пароли)
- | Поддержка аутентификации через push-уведомления\*
- | Удобство применения для локального и удаленного доступа

\* Поддержка аутентификации через push-уведомления будет осуществляться через интеграцию с Indeed Access Manager и появится в IV кв. 2022 г.



# КЕЙС – ГРУППА КОМПАНИЙ «ЕПК»

Защита доступа и контроль действий привилегированных пользователей при управлении технологическими процессами на промышленном предприятии

Реализованы инструменты удаленного контроля за действиями привилегированных пользователей со стороны сотрудников информационной безопасности

Интервью с руководителем отдела информационных систем ЕПК о внедрении Indeed PAM

**Охват пользователей:** 50

Indeed Privileged Access Manager





# АКЦЕНТ РАЗВИТИЯ: СОЗДАНИЕ СОБСТВЕННЫХ PROXY

Реализовано
  Запланировано
  В перспективе



	2018-2021				2022		2023	2024
Каталог пользователей			Active Directory				Поддержка OpenLDAP, FreeIPA, ALD	Каталог пользов.
Интеграция			Заявки через ServiceDesk				Аутентификация через RADIUS и OpenID Connect	Другие
Политики доступа		Сквозная аутентиф.	Группы ресурсов		Подразделения		Группы пользователей	Другие
Механизмы доступа	RemoteApp (MS RDS)	Windows SSH-Proxy	Windows Telnet-Proxy	Windows SSH-Proxy	Linux SSH-Proxy	Windows, Linux RDP-Proxy	Linux Telnet -Proxy	Windows, Linux SQL-Proxy
Управление паролями	История паролей	Выдача пароля	Выдача пароля по согласованию		Application-to Application Password Management		Подсистема плагинов для целевых систем	Другие
Предоставление доступа	Доступ по расписанию	Ограничение Длительности сессии	Временный доступ	Доступ по согласованию			Система заявок на доступ	Другие

### 03. УПРАВЛЕНИЕ ПРИВИЛЕГИЯМИ И КОНТРОЛЬ ДЕЙСТВИЙ:

Порождение концепций Zero Trust и Just In Time Access  
Пользователям могут быть выданы излишние полномочия  
Критичные действия требуют согласования и контроля  
Даже профессионал может ошибиться  
Никто не считается профессионалом, пока этого не докажет  
Пользователи могут попытаться скрыть инцидент

# ФИКСАЦИЯ И КОНТРОЛЬ ДЕЙСТВИЙ

Повышение эффективности реагирования:

Разные способы записи активности привилегированных пользователей

Фильтрация текстовых команд и разрыв соединения (SSH)

Мониторинг в режиме реального времени

Просмотр записей событий и сквозной текстовый поиск

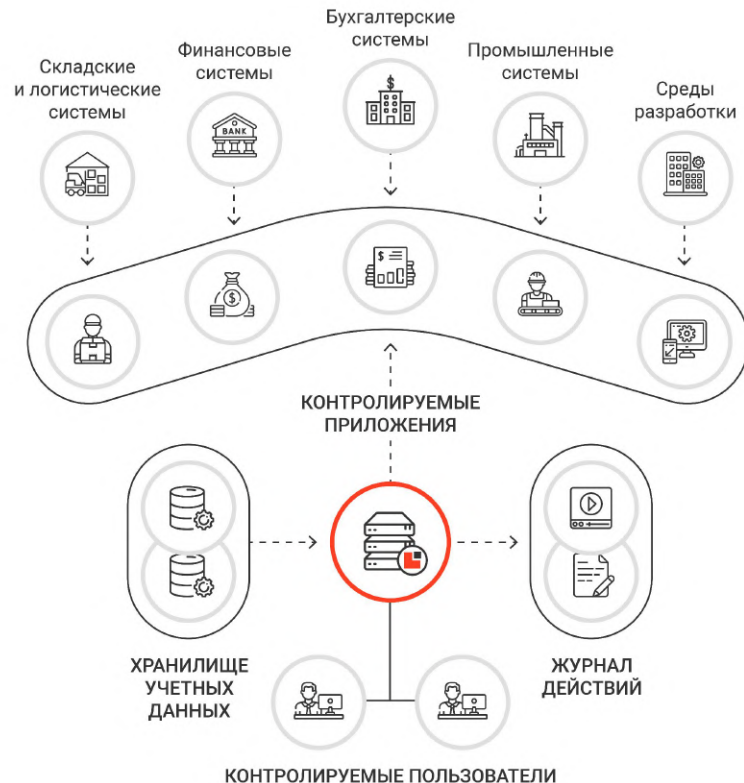
Перехват и теневое копирование передаваемых файлов (RDP, SFTP\*, SCP\*)



\* Поддержка SCP - в версии 2.7 в III кв. 2022 г.,  
SFTP - в версии 2.8 в IV кв. 2022 г.

# ЗАЩИЩЕННЫЙ ДОСТУП К КОРПОРАТИВНЫМ СЕРВИСАМ

- | Публикация любых приложений
- | Инструмент оперативной организации временного удаленного доступа к сервису
- | Дополнительные функции защиты и контроля для сервера приложений
- | Фиксация действий для анализа
- | Сохранение паролей целевых приложений в секрете от сотрудника



# КЕЙС – ФЕДЕРАЛЬНОЕ МИНИСТЕРСТВО

Большое количество целевых ресурсов и привилегированных пользователей разных категорий

Для подключений разной критичности настроены индивидуальные параметры записи действий

Заказные доработки для повышения эффективности контроля действий и реагирования на инциденты

**Охват пользователей:** более 200

Indeed Privileged Access Manager



# АКЦЕНТ РАЗВИТИЯ: **КОНТРОЛЬ** ВЫПОЛНЕНИЯ ОПЕРАЦИЙ

Реализовано
  Запланировано
  В перспективе



	2018-2021				2022	2023	2024
Инструменты отчетности	Интеграция с SIEM (syslog)	Выгрузка журналов (CSV, XLSX)	Уведомление по почте	Интеграция с SIEM (syslog: LEEF, CEF)	Интеграция с SIEM (текстовые действия)	Система отчетности	Другие
Реакция на операции	Фиксация сведений	Разрыв сессии	Отмена операции (SSH)	Повышение привилегий (SSH, sudo)		Дополнительные виды реакции на выявленные операции, исходя из запросов (в первую очередь - RDP, SSH, SQL)	
Выявление операций	Передача файлов (RDP)		Команды (SSH)		Копирование и файлы (SCP, SFTP)	Копирование и файлы (RDP)	
Инструменты анализа	Журнал событий	Журнал действий	Страницы польз., рес, УЗ.	Сквозной поиск		Синхронизация текстовых и видеозаписей действий	Теги для объектов
Методы записи действий	Видеофиксация и снимки экрана	Текстовая фиксация (SSH)	Текстовая фиксация (RDP)			Распознавание текста	Другие
Параметры доступа	Доступ по расписанию	Ограничение длительности	Временный доступ	Доступ по согласованию		Система заявок на доступ	Другие



## 04. УЛУЧШЕНИЕ ПОЛЬЗОВАТЕЛЬСКОГО ОПЫТА:

Удобство развертывания и масштабирования

Удобство управления и эксплуатации

Возможности интеграции и создание целостной экосистемы

Уровень оказываемого сервиса

Возможность заказной доработки функционала

Качество и доступность технической поддержки

Качество и доступность технических и иных материалов

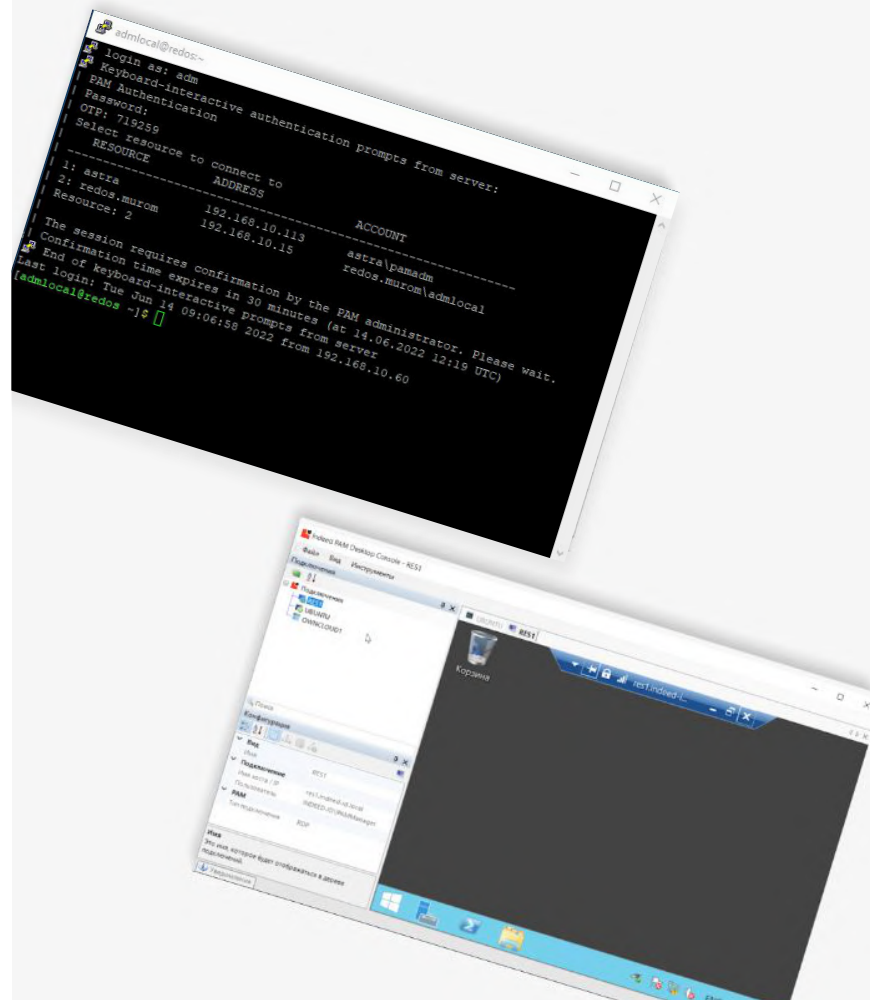
# ЧЕТЫРЕ СПОСОБА ПОДКЛЮЧЕНИЯ К РЕСУРСАМ

Скачиваемый RDP-файл с уже готовыми настройками подключения к конкретному ресурсу (для подрядчиков)

Строка подключения для клиентских приложений (для консольных подключений)

Прямое подключение на соответствующий сетевой порт на IP-адресе шлюза доступа с использованием стандартного ПО (Putty)

Программное обеспечение - менеджер удаленных подключений - содержит все доступные для пользователя подключения (для администраторов)

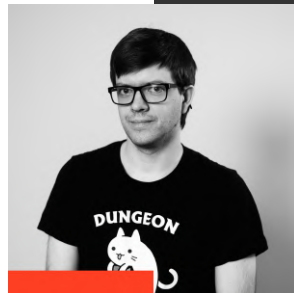




# ТЕХНИЧЕСКИЕ УСЛУГИ ДЛЯ ЗАКАЗЧИКОВ

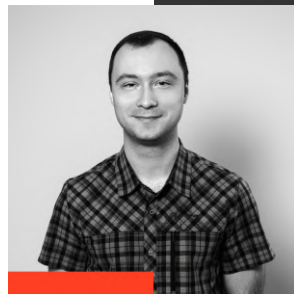
- Бесплатное тестирование продуктов
- Предоставление оборудования на период тестирования
- Русскоязычная техническая поддержка 24/7\*
- Удаленное подключение инженера
- Услуга брендирования продуктов под заказчиков
- Заказная доработка решений под задачи заказчика

\* С привлечением партнеров, от Компании Индид — 8/5



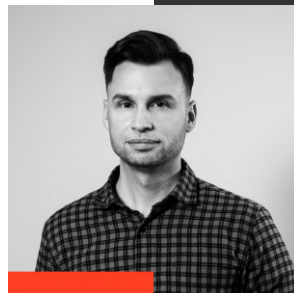
## НИКОЛАЙ ИЛЬИН

Эксперт по защите и управлению доступом



## МАКСИМ КУЗЬМОВ

Эксперт по контролю действий привилегированных пользователей

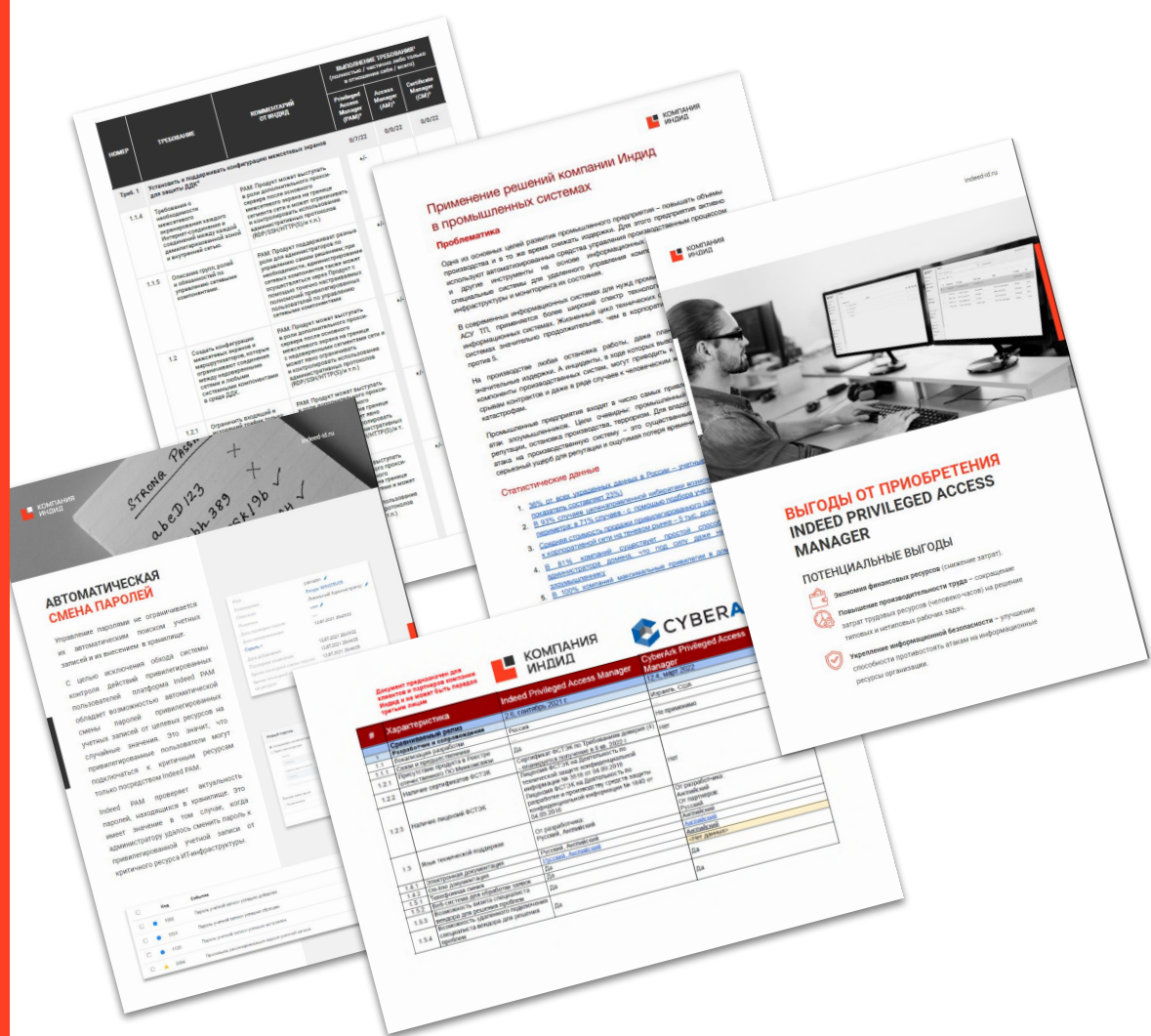


## МИХАИЛ ЯКОВЛЕВ

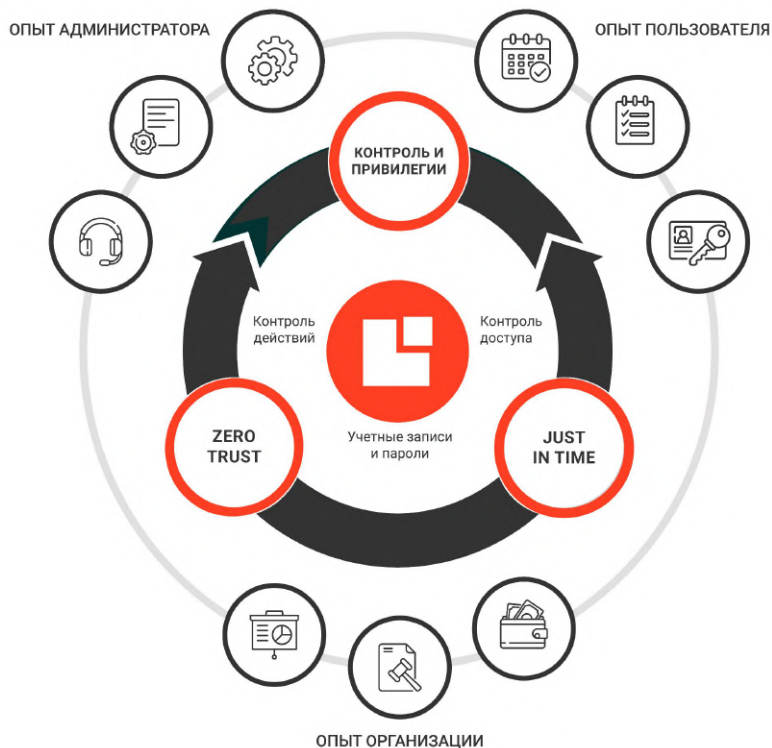
Эксперт по управлению инфраструктурой открытых ключей

# ТЕХНИЧЕСКИЕ И АНАЛИТИЧЕСКИЕ МАТЕРИАЛЫ

- Compliance - Оценки выполнения требований
- Comparisons - Сравнения продуктов с конкурентами
- Industry Use Cases - Отраслевые применения продуктов
- Solution Use Cases - Сценарии применения продуктов
- Benefits - Выгоды от применения продуктов
- И другие...



# НЕПРЕРЫВНОЕ СОВЕРШЕНСТВОВАНИЕ



## ОПЫТ АДМИНИСТРАТОРА

- | Удобство внедрения и интеграции
- | Качество документации
- | Уровень технической поддержки

## ОПЫТ ПОЛЬЗОВАТЕЛЯ

- | Доступ в заданное время
- | Контроль действий и полномочий
- | Управление учетками и паролями

## ОПЫТ ОРГАНИЗАЦИИ

- | Эффективность продукта
- | Выполнение требований
- | Ценовая политика



# КЕЙС — БАНК «САНКТ-ПЕТЕРБУРГ»

Долгая история партнерства и высокая оценка качества совместной работы

Реализована экосистема управления доступом от компании Индид

Проведена замена конкурирующего иностранного решения

Уменьшена общая стоимость владения системой контроля действий привилегированных пользователей

**Масштаб:** 200 пользователей



# ТЕХНОЛОГИЧЕСКИЕ ПРЕИМУЩЕСТВА ПРОДУКТОВ КОМПАНИИ ИНДИД



## Централизованное управление и мониторинг

Единая система централизованного управления аутентификацией, инфраструктурой открытых ключей, удаленным и привилегированным доступом с едиными журналами мониторинга соответствующих событий ИБ



## Экономия ресурсов и повышение производительности труда

Автоматизация и оптимизация рутинных операций по управлению PKI, по контролю и защите доступа и по управлению привилегированным доступом с помощью специализированных инструментов



## Усиленная аутентификация и контроль использования паролей

Поддержка разнообразных сценариев усиленной аутентификации для различных сценариев работы, защищенное хранение и управление паролями и ключами, исключаящее их небезопасное использование



## Интеграция с целевыми системами и компонентами ИТ-инфраструктуры

Поддержка интеграция со всеми корпоративными сервисами и системами, а также с иными техническими средствами защиты информации



**ПРОЗРАЧНОСТЬ** – ОДИН  
ИЗ КЛЮЧЕВЫХ ФАКТОРОВ  
СОТРУДНИЧЕСТВА





# НАШИ ЗАКАЗЧИКИ



## КОНТАКТЫ

 [indeed-company.ru](https://indeed-company.ru)

 [sales@indeed-company.ru](mailto:sales@indeed-company.ru)

 8 800 333-09-06