ИНДИД

комплекс
решений
для защиты
айдентити

- PAM
- ITDR
- AM
- CM
- Octopus IdM
- BearPass

Цифровая идентичность — ценнейший актив вашего бизнеса. Позвольте нам гарантировать, что он будет принадлежать только вам

Защита айдентити давно перестала быть вопросом второстепенной важности. Реальность такова, что абсолютно любой бизнес — от стартапа до международной корпорации — рискует столкнуться с атаками злоумышленников, способными нанести ему весомый материальный ущерб и ударить по деловой репутации. Уберечь себя от таких рисков — стратегическая задача, и мы убеждены, что она требует осознанного и компетентного подхода. Мы доказали это, успешно защищая айдентити в финансовом секторе, на промышленных предприятиях и в крупнейших корпорациях страны — там, где кибербезопасность особенно важна для успеха и устойчивого развития.

Алексей Баранов

Основатель и генеральный директор Индид

Атаки на айдентити неизбежны. Настоящий успех — не в отсутствии угроз, а в способности предотвратить их без последствий

Нехитрые пароли, разблокированные устройства, забытые без присмотра, случайные ошибки пользователей в корпоративных системах — мы ежедневно наблюдаем, как эти, казалось бы, безобидные действия незаметно приводят к компрометации данных и влекут за собой катастрофические последствия для бизнеса. Сегодня не осталось никаких сомнений: защита цифровой идентичности — уже не опция, а критическая необходимость. Это основа доверия и безопасности для любой компании, которая ценит свои ресурсы и репутацию.

Если проанализировать резонансные случаи, связанные с кражей айдентити, становится очевидно: утечка идентификационных данных может произойти на любом уровне. Время, когда можно было закрыть глаза на защиту цифровой идентичности, безвозвратно прошло — сегодня эффективная стратегия обеспечения кибербезопасности требует продуманного подхода и использования новейших технологий, способных предотвратить кражу критически важной информации. Вы не можете гарантировать отсутствие атак на айдентити, но можете быть к ним полностью готовы.

Создаем будущее, где неприкосновенность айдентити оберегается с бескомпромиссной строгостью

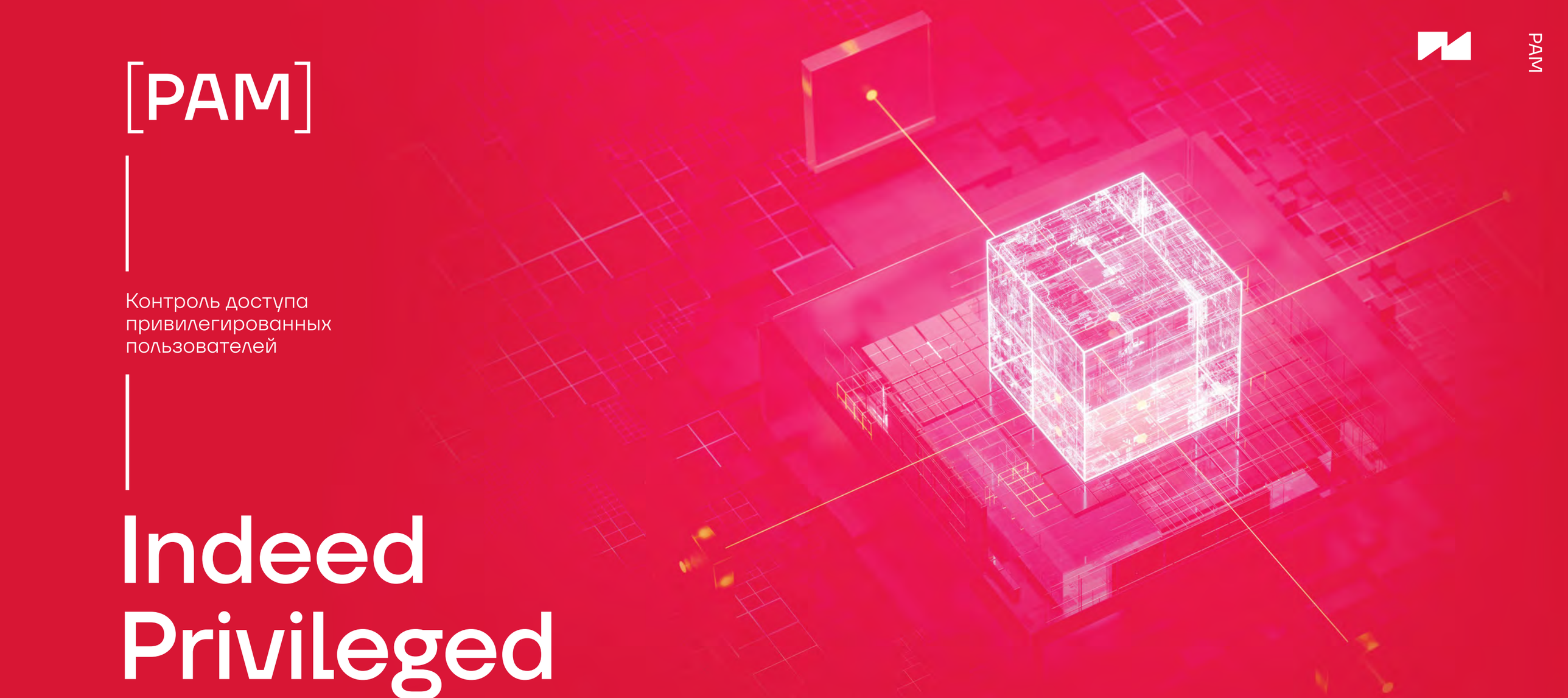
За годы работы мы накопили достаточно опыта и знаем, как дорого обходятся ошибки, связанные с кражей корпоративных айдентити. Мы понимаем: настоящая защита начинается задолго до атаки. Наши технологии позволяют гарантировать безопасность айдентити «на 360°», охватывая все уровни инфраструктуры. Мы разрабатываем системы, которые дают нашим клиентам твердую уверенность в надежной защите их цифровых активов.

Индид — это ваш доверенный партнер и проводник в безопасную цифровую среду, где можно не опасаться рисков и не сомневаться в сохранности вашей информации. Вместе мы строим будущее, в котором цифровая идентичность становится наивысшей ценностью и оберегается бескомпромиссно строго.

[PAM]

Контроль доступа
привилегированных
пользователей

Indeed Privileged Access Manager



#ПривилегированныйДоступ
#КонтрольПодрядчиков
#ZeroTrust
#НулевоеДоверие
#РасследованиеКиберинцидентов
#УправлениеПривилегиями
#ГранулированныйДоступ

Indeed Privileged Access Manager [PAM]

Обеспечить безопасность привилегированных учетных записей жизненно необходимо любой компании, поскольку доступ к ним — заветная цель киберпреступников. Indeed Privileged Access Manager (PAM) — решение для централизованного управления действиями пользователей с расширенными правами доступа к критически важным цифровым активам и сервисам. Оно позволяет тщательно контролировать, кто и когда имеет доступ к особо значимым данным, а также отслеживать все операции в реальном времени. Это система, которая обеспечивает бесперебойную работу вашего бизнеса, предотвращая злоупотребление привилегиями и сводя к минимуму риск утечки конфиденциальной информации.

Кто?

Пользователь

Группа пользователей

Какие права?

Привилегированная УЗ

Пользовательская УЗ

Разрешение

Какие условия?

График доступа

Период доступа

Протокол доступа

Куда?

Серверы

Оборудование

Базы данных

Приложения

Ваша цифровая идентичность стоит того, чтобы как следует о ней позаботиться

Снизьте риски для ИБ, связанные с неконтролируемыми действиями привилегированных пользователей

Возьмите под контроль действия администраторов и других пользователей, работающих с чувствительной информацией

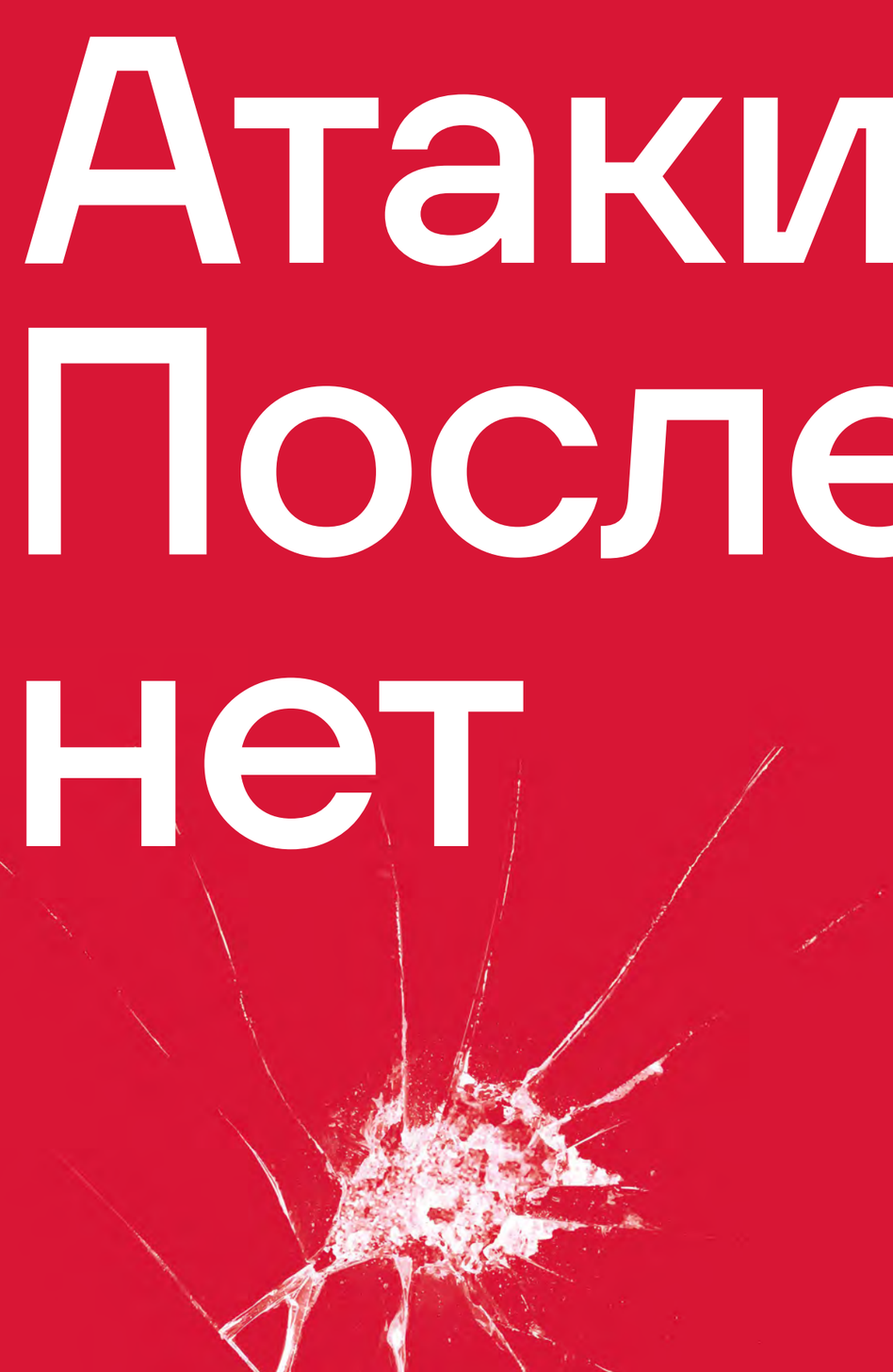
Управляйте доступом подрядчиков и других внешних пользователей

Записывайте действия и быстро расследуйте киберинциденты, связанные с действиями привилегированных пользователей

Выполняйте корпоративные требования безопасности легко и быстро

Обеспечивайте соответствие требованиям регуляторов к идентификации и аутентификации пользователей

Атаки будут. Последствия — нет



01 **Обнаружьте все «слепые зоны»**
Наведите порядок в управлении правами доступа: выявите избыточные привилегии, неактивные учетные записи и ошибочные конфигурации

02 **Уменьшите поверхность атаки**
Предоставляйте гранулированный доступ и следуйте концепциям минимальных привилегий и нулевого доверия

03 **Реагируйте быстро и точно**
Атаки развиваются стремительно — будьте готовы молниеносно пресекать их

Гибко управляйте секретами

01 Сократите количество привилегированных учетных записей, необходимых для управления информационными системами компании

02 Гибко настраивайте политики, позволяющие регламентировать привилегированный доступ согласно корпоративным требованиям безопасности

03 Предотвратите риски, связанные с несанкционированным использованием паролей:

- Храните пароли в зашифрованном виде
- Меняйте пароли по расписанию
- Выдавайте разрешения на подключение, не раскрывая пароли привилегированных учетных записей

Расследуйте киберинциденты без проблем

01 Используйте многочисленные артефакты сессий (логи, видео, скриншоты, журнал событий) и интегрируйте данные с системами SIEM

02 Ограничивайте действия пользователей с помощью белых и черных списков команд

03 Просматривайте активные сессии и при необходимости прерывайте их в режиме реального времени

Обеспечьте абсолютный контроль над аутентификацией пользователей

01 Подключайтесь ко всем защищаемым объектам корпоративной инфраструктуры централизованно через единую точку доступа

02 Используйте многофакторную аутентификацию даже в тех сервисах, где ее технически невозможно реализовать с помощью классических систем управления доступом

03 Выдавайте разрешения с ограниченным сроком действия и предоставляйте пользователям доступ по расписанию

Zero Trust

Культура управления привилегиями начинается с нулевого доверия

01 Проверяйте и авторизуйте каждого пользователя и каждую техническую учетную запись перед предоставлением доступа к ресурсам

02 Используйте дополнительные факторы аутентификации при предоставлении доступа

03 Разделяйте сети на микросегменты для усиленного контроля доступа к ресурсам и приложениям

04 Исключите возможность открывать пользовательские сессии без подтверждения администратора

05 Используйте обширный набор логируемых артефактов сессий для упрощения киберрасследований. Просматривайте сессии в режиме онлайн и прерывайте их в случае подозрительных действий пользователя

Узнайте подробнее, как защитить привилегированные учетные записи

Клиенты говорят о продукте

Indeed PAM

PAM от Индид стал оптимальным решением, которое способно защитить доступ к критически важным корпоративным данным и отвечает современным стандартам информационной безопасности, а также всем нашим требованиям — надежность, зрелость и эффективность.

Особенно хочется выделить прозрачность в плане развития продукта. На этапе пилота у нас были специфические потребности, часть из которых не была реализована в текущей версии продукта. Однако эти функции были включены уже в план следующего релиза, и, что особенно важно, они действительно появились в новой версии в обозначенные сроки.

Татьяна Фомина
Директор по информационным технологиям и кибербезопасности HeadHunter

Результаты внедрения:

01
Автоматизация контроля и исполнения парольной политики

02
Строгий контроль и управление доступом привилегированных пользователей

03
Повышение уровня безопасности с помощью многофакторной аутентификации

04
Фиксация действий привилегированных сотрудников и внешних подрядчиков, а также аудит их действий

[ITDR]

Адаптивная
защита учетных данных
в корпоративной сети

Indeed Identity Threat Detection & Response

PAM

ITDR

#ОбнаружениеУгроз
#РеагированиеНаИнциденты
#БлокировкаАтак
#ЗащитаИзнутри
#ЗащитаАйдентити
#КомплекснаяЗащитаДанных
#Kerberos
#ЗащитаДомена

Мы серьезно переосмыслили подход к защите айдентити

Сегодня инфраструктура айдентити в силу своей уязвимости стала самой привлекательной мишенью для злоумышленников. Внедрение систем IAM, IGA и MFA — важный шаг к обеспечению безопасности, но они все же не способны полностью исключить риск компрометации учетных записей.

Концепция ITDR (Identity Threat Detection and Response) позволяет переосмыслить подход к защите айдентити, сосредоточив внимание на рисках организации в целом, а не на отдельных пользователях или приложениях. Indeed ITDR — единственное российское решение этого класса, централизованно интегрируемое в корпоративную сеть и позволяющее с высокой точностью выявлять и автоматически блокировать атаки непосредственно на уровне инфраструктуры айдентити.

В отличие от традиционных решений, продукт класса ITDR охватывает всю инфраструктуру айдентити в целом, включая разнородные среды со множеством доменов и протоколов, что значительно снижает риск утечки данных и выводит киберустойчивость компании на качественно новый уровень.

Отслеживайте и блокируйте любые атаки на корпоративные учетные данные

01 **Управляйте айдентити и минимизируйте риск компрометации данных**
События запроса доступа непрерывно собираются и отображаются в реальном времени, что позволяет выявлять и блокировать подозрительную активность до того, как она причинит ущерб

02 **Мгновенно реагируйте в случае атаки**
Обнаружив угрозу, система автоматически заблокирует пользователю доступ, чтобы молниеносно нейтрализовать финансовые и репутационные риски

03 **Создавайте многоуровневую стратегию кибербезопасности**
Интеграция ITDR с решениями классов SIEM, SOAR, XDR или IAM позволит эффективно обнаруживать попытки направленных атак и предотвращать проникновение злоумышленников в корпоративную инфраструктуру

Indeed ITDR не заменяет решения смежных классов, а дополняет их, обеспечивая полномасштабную защиту от угроз для айдентити

Перейдите на новый уровень защиты

[от направленных атак на айдентити]

01 Защищайте свою инфраструктуру айдентити от направленных атак, таких как Kerberoasting и Golden Ticket

02 Обнаруживайте слабые места в конфигурации вашей инфраструктуры и аномалии пользовательского поведения

03 Отсекайте любые нежелательные запросы доступа и реализуйте MFA для любых приложений, использующих доменную аутентификацию, без применения дополнительных решений

04 Анализируйте сетевой трафик протоколов аутентификации

05 Интегрируйте решение в вашу инфраструктуру без модификации клиентов или серверов приложений

[Узнайте подробнее, как защитить вашу инфраструктуру айдентити изнутри]

PAM
ITDR
AM

[IAM]

Управление доступом
к цифровым активам компании
с возможностью многофакторной
аутентификации [MFA]

Indeed Access Manager

#MFA
#2ФА
#УправлениеДоступом
#УсиленнаяАутентификация
#ВторойФактор
#ПодтверждениеЛичности
#ЗащитаДоступа
#УправлениеУчетнымиЗаписями
#БезопасныйВходВСистемы
#SSO
#ЗащитаVPN

Indeed Access Manager [AM]

централизованно управляет идентификационной информацией сотрудников или подрядчиков — независимо от того, где они находятся, какими приложениями пользуются и на каких устройствах работают. Чтобы получить доступ к корпоративным системам, пользователь должен подтвердить свою личность с помощью усиленной многофакторной аутентификации (MFA). Внедрите Indeed AM, чтобы автоматически выполнять такую проверку и надежно защищать свои ресурсы.

Обеспечьте безопасность всех своих данных

01

Защитите учетные записи от компрометации

Используйте усиленную многофакторную аутентификацию вместо простых паролей и будьте уверены, что пользователи действительно являются теми, за кого себя выдают

02

Охватите все аспекты управления доступом

Управляйте всеми аспектами доступа — как внутри периметра, так и за его пределами, например при удаленном подключении пользователей

03

Подключайтесь откуда угодно

Применяйте технологию единого входа (SSO) для сквозной аутентификации: пользователям больше не понадобится запоминать множество паролей

04

Работайте в любых средах

Защитите данные на всех платформах, включая ОС Linux, благодаря гибким возможностям интеграции MFA в ИТ-инфраструктуру

Управляйте идентификационными данными — где бы вы ни были

Узнайте подробнее, как управлять доступом с помощью технологий усиленной аутентификации

PAM ITDR AM

01

Централизованно управляйте доступом из единой консоли

Работайте эффективнее: управляйте ролями и полномочиями пользователей через консоль администратора

02

Настраивайте многофакторную аутентификацию как вам удобно

Простая парольная защита — большой риск. Выбирайте оптимальные методы MFA из широкого ассортимента Indeed AM (OTP, push-уведомления, аппаратные смарт-карты и токены, удобное мобильное приложение Indeed Key)

03

Интегрируйте данные в системы мониторинга

Моментально передавайте данные в систему SIEM, чтобы полностью отслеживать все события доступа и оперативно реагировать на инциденты

04

Внедряйте различные сценарии усиленной аутентификации

Используйте широкий ассортимент модулей и агентов для интеграции с целевыми системами

Клиенты говорят о продукте

Indeed AM

В процессе масштабирования Indeed Access Manager мы расширили зоны покрытия инструментом двухфакторной аутентификации: 2FA стали использовать в большем количестве ИТ-систем и СЗИ.

Мы смогли этого достичь за счет широкого интеграционного функционала решения и оперативной поддержки со стороны команды компании «Индид». Это позволило нам повысить уровень защищенности корпоративной инфраструктуры и закрыть часть требований регуляторных органов (Банка России, ФСТЭК).

Сергей Крамаренко
Руководитель департамента кибербезопасности Альфа-Банка

Результаты внедрения:

01
Централизованная система беспарольной аутентификации мобильных (удаленных) сотрудников

02
Двухфакторная аутентификация при подключении по протоколу VPN

03
Аутентификация с помощью одноразовых паролей, генерируемых на смартфоне

PAM ITDR AM

КРОСС ТЕХНОЛОДЖИС
segezha group
CTC media
itprotect
АБСОЛЮТ БАНК
СДМБАНК
СТС
КИТФинанс Брокер
ГАЗПРОМ
ДРТ
K2 кибер безопасность
КУЗБАССРАЗРЕЗУГОЛЬ
СБЕР РЕШЕНИЯ
АВТОБАН
БСПБ
СДМБАНК
Сколково
СОГЛАСИЕ страхование

Card Management

Централизованное управление жизненным циклом ключевых носителей и сертификатов

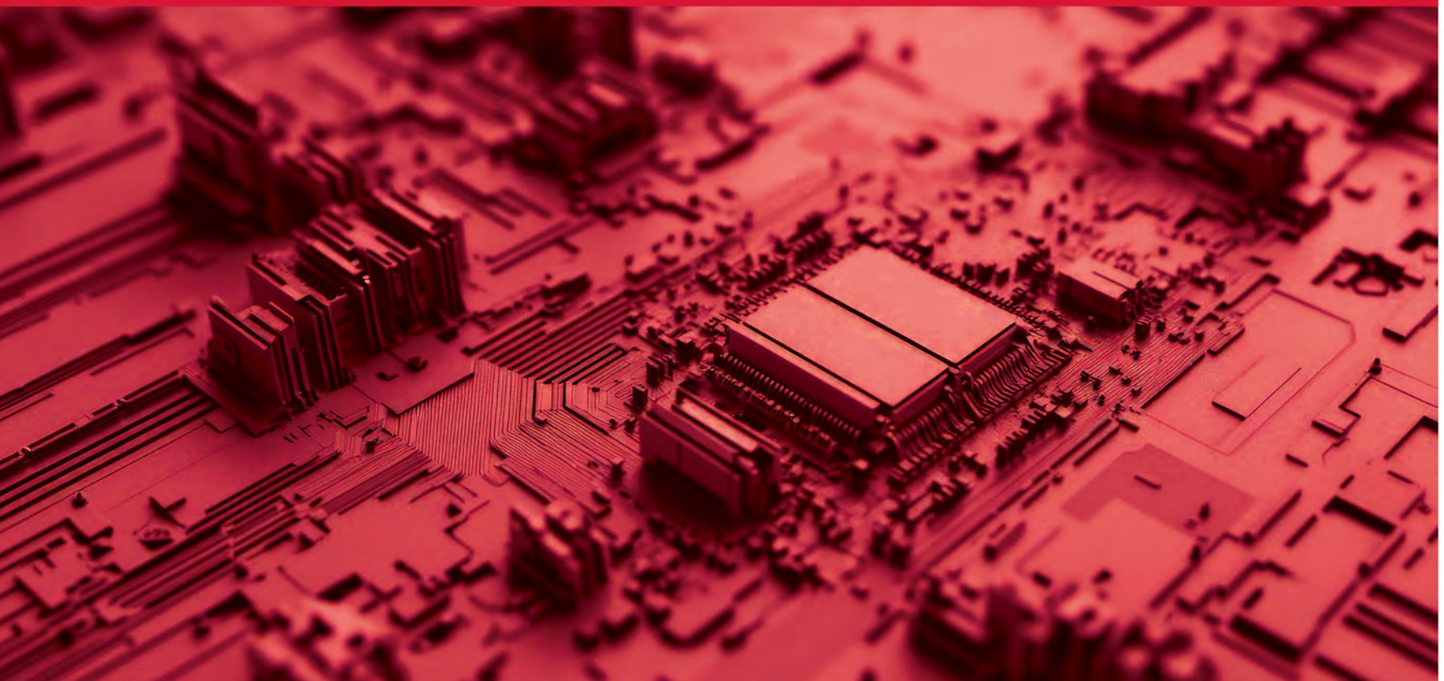
Indeed Certificate Manager

PAM
ITDR
AM
CM

#PKI
#СКЗИ
#ЭДО
#УЦ
#Криптография
#СКУД
#Шифрование
#ЭлектроннаяПодпись
#ФАПСИ№152
#63-ФЗ
#СМЭВ
#ЕСИА
#КлючевыеНосители
#ЦифровыеСертификаты

Indeed Certificate Manager [CM]

централизованно управляет цифровыми сертификатами и ключевыми носителями (токенами и смарт-картами) на всех этапах их жизненного цикла. Топ-менеджерам продукт помогает повысить производительность труда и сократить затраты на обеспечение ИБ и техподдержку, администраторам — освободиться от ежедневных рутинных операций, а пользователям — быстро выполнять необходимые действия без неудобств и лишних задержек. Автоматизируйте управление криптографической защитой информации: пусть служба ИБ сосредоточит внимание на стратегических задачах, пока Indeed CM исправно делает свою работу.



Базовые модули

- Консоль управления
- Сервис самообслуживания
- API
- Служба Card Monitor
- Журнал СКЗИ
- Журнал событий
- Настраиваемые журналы учета
- Сервис внутреннего электронного документооборота

Модули интеграции

- Коннекторы к удостоверяющим центрам
- Коннекторы к каталогам пользователей
- Коннектор к хранилищу данных
- Коннектор к ситемам аудита событий
- Коннектор к СМЭВ
- Коннекторы к Indeed Access Manager, Secret Net Studio и Рутокен Логон

Клиентские компоненты

- Клиентский агент для удаленного управления ключевыми носителями
- Middleware для работы с ключевыми носителями
- Client Tools для разблокировки ключевых носителей
- Модуль взаимодействия с принтером смарт-карт

Дополнительные модули

- «КриптоПро DSS»
- Indeed AirCard Enterprise

Забудьте о рутинном обслуживании

[PKI]

01 Сквозная автоматизация

Indeed CM возьмет на себя всю работу по выпуску и администрированию пользовательских сертификатов, разгрузит администраторов и обеспечит непрерывность бизнес-процессов

02 Учет средств криптографической защиты информации (СКЗИ)

Выполняйте требования регуляторов по учету СКЗИ без применения бумажных носителей и ручного ввода данных

03 Журналирование и аудит действий с ключевыми носителями

При подозрительном несоответствии действий система мгновенно отреагирует и поможет быстро расследовать инцидент

04 Интеграция с системами СКУД, Single Sign-On (SSO), IAM, IdM

Уволенный сотрудник не сможет получить доступ к корпоративным цифровым активам

05 Резервное копирование ключевой информации

Защищает важные данные от потери или повреждения

05 Самообслуживание через удобный портал из любой точки мира

Пользователям больше не придется разбираться в сложных интерфейсах и просить администратора обновить сертификат или разблокировать ключевой носитель

Ускоряйте бизнес-процессы с электронным документооборотом

01 **Устраните риски,** связанные с обменом документами по электронной почте, — храните и передавайте данные безопасно

02 **Легко и быстро подавайте документы** для получения ЭЦП через личный кабинет пользователя

03 **Храните, ищите и легко сортируйте** подписанные документы в электронном виде, ставьте отметки о получении оригиналов для бумажного архива

04 **Автоматически контролируйте** предоставление полного пакета документов при получении сертификата ЭЦП

Легко осуществляйте программу импортозамещения

01 Обеспечивайте интеграцию с российскими системами и средствами защиты информации

02 Администрируйте пользователей в среде Linux

03 Плавно мигрируйте с Active Directory

04 Выполняйте требования ФСТЭК, ГОСТ, PCI DSS

Клиенты говорят о продукте

Indeed CM

Кроме функциональных особенностей программного обеспечения, мы хотим отметить качественную работу специалистов технической поддержки, в частности оперативное предоставление информации и консультаций при настройке продукта и выполнении сложных технических задач по интеграции в нашу ИТ-инфраструктуру. Именно поэтому мы остановили свой выбор на Indeed Certificate Manager и рассчитываем на долгосрочное сотрудничество с компанией «Индид».

Дмитрий Никишов

Начальник службы информационной безопасности Группы «СМП Банк»

Результаты внедрения

Решены задачи по обслуживанию инфраструктуры открытых ключей, в частности вопросы по управлению и инвентаризации ключевых носителей, управлению жизненным циклом сертификатов аутентификации и электронной подписи, ведению журнала учета средств криптографической защиты информации (СКЗИ)

ПЭК

семья магазинов МАГНИТ

СМП БАНК ГРУППА ПСБ

ВТБ

СДМБАНК

БСПБ

PAM ITDR AM CM

Узнайте подробнее, как автоматизировать управление ключевыми носителями и цифровыми сертификатами

Индид Облако

Облачные сервисы
для управления доступом
и комплексной защиты бизнеса

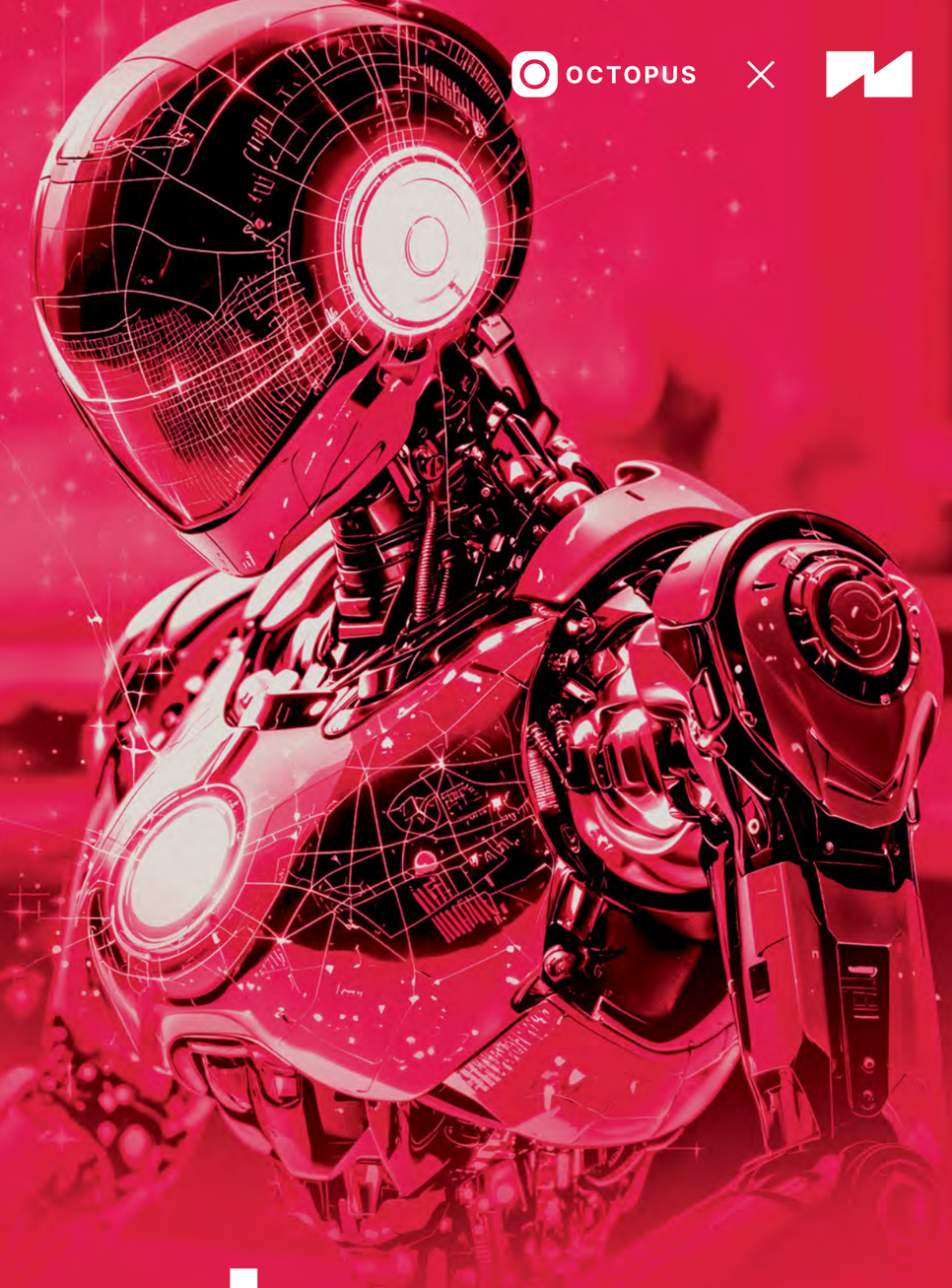
Помогаем малому и среднему бизнесу избегать финансовых и репутационных потерь, надежно защищая корпоративные учетные данные с помощью многофакторной аутентификации (MFA) и безопасного хранения паролей

Оставьте заявку для быстрого подключения к онлайн-сервису многофакторной аутентификации

[IdM]

Централизованное
управление привилегиями
и доступом к цифровым
активам компании

Octopus Identity Management



OCTOPUS × M

PAM ITDR AM CM

Octopus IdM

#УправлениеДоступом
#УправлениеПолномочиями
#ХранениеУчетныхДанных
#ВыдачаПравДоступа

Представьте, что в цифровом пространстве вашей компании наведен идеальный порядок: каждый сотрудник получает ровно столько полномочий, сколько ему действительно необходимо, клиенты и партнеры довольны быстрой и удобной процедурой входа в личный кабинет, а риск случайных ошибок и злонамеренных действий практически исключен. Такой порядок можно обеспечить при помощи Octopus IdM.

Эта система позволяет систематизировать разрозненные учетные записи и уровни допуска, чтобы легко назначать права и отслеживать действия пользователей на корпоративных ресурсах. Когда эти данные контролирует IdM, они доступны лишь тем, кому полагается, и не могут оказаться там, где их быть не должно. Держите полномочия пользователей под строгим контролем, чтобы ваше информационное пространство оставалось прозрачным и безопасным.

Создайте безопасную цифровую среду на основе интеллектуального управления правами доступа

01

Контролируйте жизненный цикл доступа любых пользователей, включая сотрудников и подрядчиков, ко всем системам компании и на всех этапах — начиная с трудоустройства и заканчивая увольнением

02

Установите абсолютный контроль над привилегиями: управляйте ими централизованно и в любой момент инвентаризируйте права доступа

03

Ускорьте выдачу прав доступа сотрудникам — упорядочьте и унифицируйте процессы согласования прав и привилегий

04

Постройте образцовую модель управления доступом. Создавайте гибкие матрицы доступа с автоматической привязкой к ролям — по должностям, местам работы или отделам

05

Предотвращайте несанкционированное изменение настроек доступа: Octopus IdM динамически сверяет состояние прав доступа на управляемых им системах, отслеживает изменения и корректирует эти права по мере необходимости

06

Отслеживайте риски появления избыточных прав доступа: используйте матрицы разделения полномочий, позволяющие автоматически находить коллизии еще на этапе создания новой роли или предоставления пакетного доступа

07

Проводите быстрый аудит и создавайте отчеты — вам всегда доступна информация о том, кто к каким ресурсам имеет доступ, а также о том, как он был получен. Легко готовьте необходимые отчеты по сотрудникам, системам или ролям

08

Используйте портал самообслуживания с понятным настраиваемым интерфейсом, чтобы работать с заявками и согласовывать различные параметры. Организуйте общий каталог с разграничением видимости прав доступа для разных групп сотрудников

09

Обеспечьте доверие к данным о предоставлении доступа: регулярно актуализируйте права доступа в системах. Гарантируйте легитимность доступа, даже если он был получен не через систему IdM

10

Проводите ресертификацию — проверку соответствия параметров доступа ответственными сотрудниками. Вы можете создавать различные форматы регулярных проверок по своему усмотрению

Решайте нетривиальные задачи бизнеса

01

Снижайте затраты на лицензии — создавайте учетные записи в системах динамически: предоставляйте их, когда это действительно нужно, и отзывайте, когда они не используются

02

Предоставляйте доступ в зависимости от того, прошел ли пользователь необходимое обучение: внедрите эффективный механизм стимулирования к профессиональному росту

03

Управляйте жизненным циклом технических учетных записей, используя возможность привязывать их к кураторам, проектам или ролям

Управляйте привилегиями пользователей как посчитаете нужным

01

Применяйте все современные технологии — пользуйтесь преимуществами нативной поддержки Kubernetes, микросервисов и графовых баз данных, чтобы глубоко анализировать связи в области доступа и легко развертывать решение в ИТ-инфраструктуре

02

Развивайте решение самостоятельно — используйте возможность гибко настраивать конфигурации в его интерфейсе

03

Постройте целую экосистему защиты айдентити: Octopus IdM легко интегрируется со всеми решениями Индид, что обеспечивает всестороннюю защиту

Узнайте подробнее о том, как обеспечить абсолютный контроль над правами доступа пользователей

PAM ITDR AM CM **Octopus IdM**

BearPass × Octopus IdM

Password Management

Безопасное хранение
корпоративных паролей
и других секретов

BearPass

#ЗащитаПаролей
#МенеджерПаролей
#УправлениеСекретами
#ЗащищенноеХранилищеПаролей
#ГенерацияСложныхПаролей
#ЗащитаОтСкринкастаИБрутфорса
#ПроверкаПароля
#УтечкаПаролей

PAM
ITDR
AM
CM
Octopus IdM
BearPass

Корпоративные пароли —

ключ к самой ценной для вас информации. Их компрометация открывает злоумышленникам доступ к конфиденциальным данным вашей компании, к ее финансам и даже к контролю над ее бизнес-процессами. Ущерб может быть поистине колоссальным.
BearPass — удобный инструмент для управления корпоративными паролями и другими секретами. Система безопасно хранит всю секретную информацию и автоматически генерирует уникальные сложные пароли для каждого ресурса, избавляя сотрудников от необходимости помнить несколько сложных комбинаций. С BearPass вы обеспечите надежную защиту своих цифровых активов благодаря централизованному контролю и эффективному управлению доступом ко всей секретной информации.

Устраним хаос в работе с корпоративными секретами

Снизим риски утечки персональных данных

Обеспечим защиту даже в «закрытом контуре» корпоративной сети

Поможем в рамках программ импортозамещения и закупок по ФЗ 44 и 223

Ваши секреты принадлежат только вам. Мы позаботимся о том, чтобы никто не узнал их

Централизованное защищенное хранение
Пароли хранятся централизованно и защищены алгоритмами шифрования по стандарту AES-256. Без специальных прав доступ к паролям невозможен

Защита от сниффинга, кейлоггинга, скринкаста и брутфорса
Пароли защищены от любых уязвимостей, включая случайную демонстрацию на экране и взлом методом перебора паролей

Мониторинг Даркнета
Регулярный мониторинг паролей на компрометацию и присутствие в базе «слитых» паролей. Проверка осуществляется безопасно — без пересылки паролей по открытым каналам

Настраиваемые политики безопасности
Требования к сложности паролей можно настроить индивидуально не только для каждой папки, но и для каждой парольной записи

Двухфакторная аутентификация (2FA)
Можно подключить двухфакторную аутентификацию для приложений с поддержкой TOTP, биометрии (Face ID, Touch ID) и аппаратных токенов

Мгновенная генерация сложных паролей
Благодаря настраиваемому генератору паролей пользователям не придется придумывать пароли самостоятельно или использовать одни и те же пароли для разных служб

Хранить секреты просто как никогда

Использование откуда угодно
Оцените удобство адаптивного интерфейса BearPass — пользуйтесь им на стационарном ПК, на планшете и смартфоне

Создание персональных сейфов
Предоставьте пользователям возможность создавать персональные сейфы для личных паролей. Они защищены отдельным ключом и недоступны никому, включая BearPass

Автозаполнение парольных форм
Забудьте про ручной ввод паролей на сайтах. Установите расширение для Google Chrome, и парольные формы будут заполняться автоматически — одним кликом

Безопасная функция «Поделиться паролем»
Делитесь паролями без рисков, создавая временные или постоянные ссылки — прямо как в Google Drive

Папки и теги
Организуйте удобную древовидную систему хранения корпоративных секретов, чтобы все нужное всегда было под рукой

Настраиваемые поля
Не хватает стандартных описательных полей? Не беда! Настройте интерфейс по своему вкусу, добавив дополнительные поля, которые нужны именно вашей организации

Администрируйте доступ как вам удобно

01

Поддержка SSO и LDAP
Авторизация с помощью SAML SSO и маппинг ролей со службами, поддерживающими протокол LDAP (например, Microsoft Active Directory)

02

Роли и группы пользователей
Возможность управлять правами пользователей с помощью ролей и групп

03

Импорт и экспорт данных
Возможность импортировать и экспортировать данные в форматах CSV и JSON

04

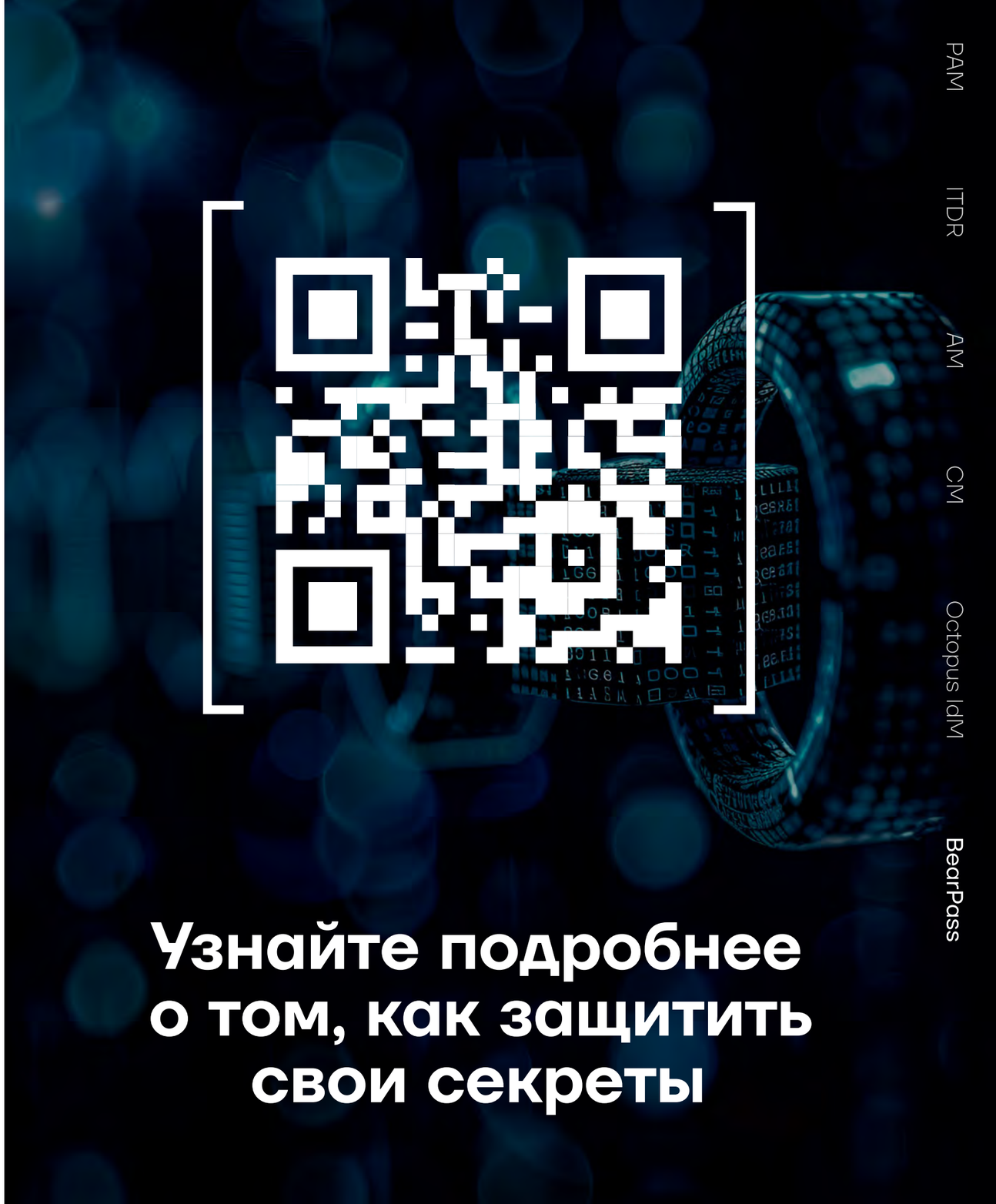
Подробное журналирование
Детальное журналирование всех событий, включая историю изменения паролей и «снятие маски» с пароля

05

Контроль действий каждого пользователя
В любой момент можно получить отчет о том, к каким секретам у сотрудника есть доступ, и увидеть подробную историю его действий. Лишить пользователя доступа к паролям можно буквально одним кликом

06

Аудит безопасности
Автоматически формируемый отчет регулярно предоставляет сводную информацию о том, соответствуют ли пароли установленным политикам, как давно они менялись и насколько высок риск их компрометации



PAM ITDR AM CM Octopus IdM BearPass

Узнайте подробнее о том, как защитить свои секреты

Техническая экспертиза, поддержка
и наставничество, инвестиции
и партнерства — всё для ускорения
роста перспективных проектов

PAM
ITDR
AM
CM
Octopus IdM
BearPass

Помогаем стартапам в сфере кибербезопасности расти и становиться лидерами рынка

Всего один осознанный шаг для повышения киберустойчивости вашего бизнеса

→ indeed-company.ru

sales@indeed-company.ru

8 800 333-09-06

123112, Москва, комплекс «Федерация» (башня «Восток»), Пресненская набережная, 12, офис 7709

Все продукты успешно прошли экспертизу и внесены в реестр отечественного программного обеспечения Минцифры

Победитель премии «РУССОФТ 2023»
Самые высокие темпы развития в категории «Лидеры роста — средний бизнес»

Победитель премии «Время инноваций» 2024
Лучший проект года в категории «Импортозамещение»
За проект по внедрению Indeed AM в в Альфа-Банке

Лауреат премии Digital Leaders Award 2025
Лучший проект года в категории «Безопасность»
За проект по внедрению Indeed PAM в международном аэропорту Шереметьево

Технологии разработаны на территории РФ и сертифицированы ФСТЭК