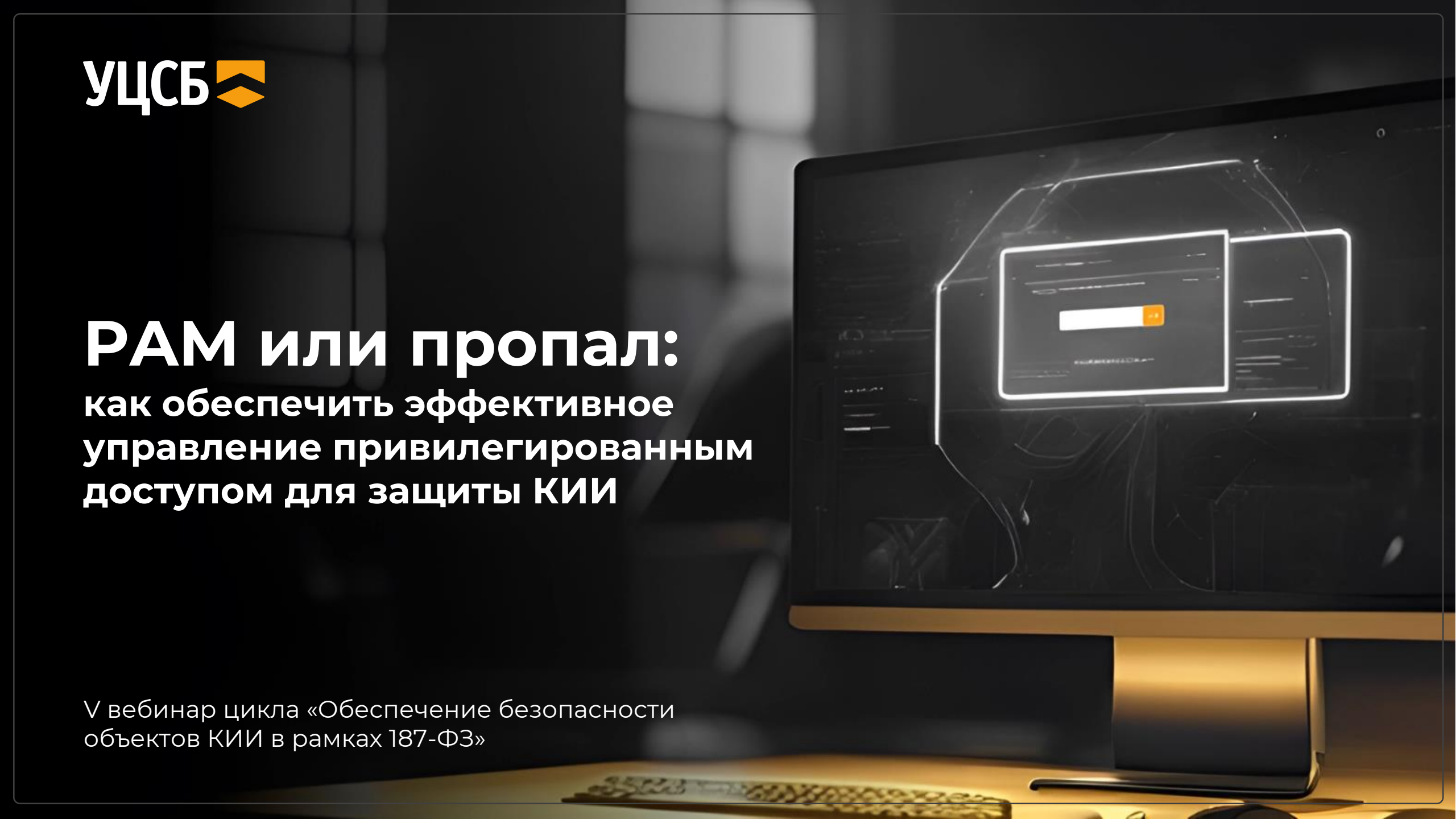
УЦСБ

PAM или пропал:

как обеспечить эффективное управление привилегированным доступом для защиты КИИ



V вебинар цикла «Обеспечение безопасности объектов КИИ в рамках 187-ФЗ»

СОДЕРЖАНИЕ

АТАКИ НА УЧЕТНЫЕ ЗАПИСИ

Типы атак:

- Password Spraying (распыление (частых) паролей)
- Sniffing (сканирование сети)
- Credential stuffing (подстановка украденных кредов)
- Brute-force (грубая атака, атаки на ДР, на хеши)
- Атаки на Active Directory (открытые пароли, DNSAdmins, Kerberos, и т.д.)
- Pass-to-Hash
- Подкуп
- Phishing/vishing
- Keylogger
- Поддельные точки доступа
- + 64 косвенного типа атак

20.04.2024

«Российский инженер смог при помощи личного ноутбука по нажатию кнопки лишить электричества жителей почти 40 населенных пунктов»

Подробнее на Cnews

РИСКИ ПРИВИЛЕГИРОВАННОГО ДОСТУПА В КИИ

ПРОНИКНОВЕНИЕ В ТЕХНОЛОГИЧЕСКУЮ СЕТЬ

- Простые пароли пользователей КИИ
- Незакрытые уязвимости и личные устройства с удаленным доступом
- Отсутствие средств контроля действий и вносимых изменений
- Ограниченность встроенных функций безопасности систем КИИ
- Невозможность установки специальных средств защиты
- Необходимость обмена данными с корпоративными системами управления

КРАЖА ИЛИ БЛОКИРОВКА КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ

- Базы персональных данных
- Схемы сетей, средств защиты
- Различные ноу-хау
- Описания технологического процесса
- Планы по выпуску продукции и развитию производства

НАРУШЕНИЕ ПРОЦЕССА ПРОИЗВОДСТВА

- Некорректные действия пользователей КИИ
- Распространение вирусов
- Отключение доступа к системе
- Очистка журналов событий

ОТСУТСТВИЕ ЦЕНТРАЛИЗОВАННОГО КОНТРОЛЯ И УПРАВЛЕНИЯ

УЦСБ

ВАРИАНТЫ РЕШЕНИЙ

Оставить как есть

Работа с кадрами

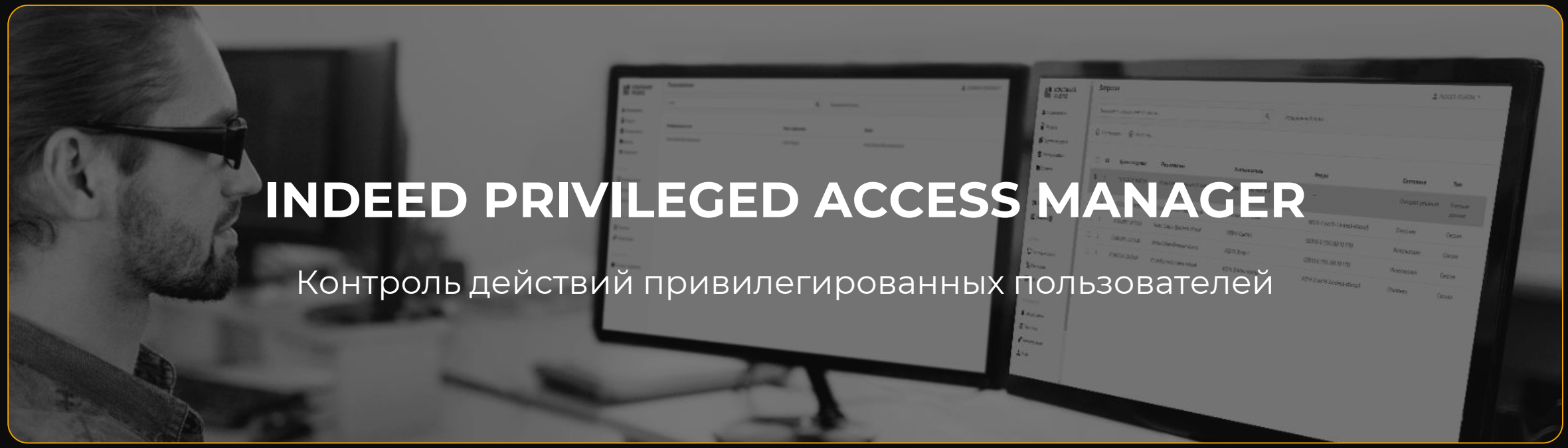
Организационные меры

Физический контроль

Использование встроенных функций контроля

Best practice: «Не вместо, а **вместе**», но и этого будет недостаточно

Класс средств	Ограничения
UAM/EMS	Реализуется на агенте Нет блокировок ввода Не все протоколы доступа
DLP	Частично на агенте Не все протоколы доступа Нет управления паролями
EPM	Пароли выдаются всем Нет аудита действий Нет защиты от ПП
IDM/IAG	Сложность внедрения Автовыдача прав Нет аудита действий
SIEM	Сложность правил Нет аудита действий Нет блокировок ввода
NGFW	Нет блокировок ввода Нет подтверждений Нет защиты от ПП
Terminal Server	Только журнал аудита Нет условий доступа Нет защиты от ПП



INDEED PRIVILEGED ACCESS MANAGER

Контроль действий привилегированных пользователей

Контроль административных учетных записей

Разные способы записи и анализа действий

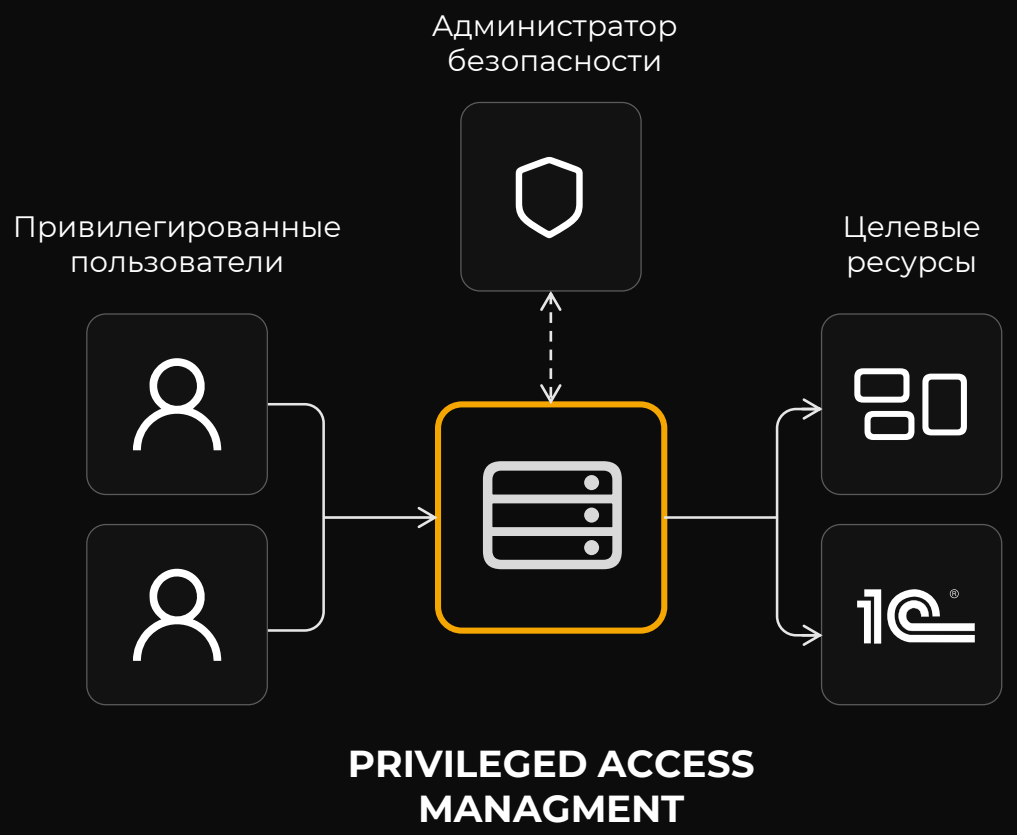
Управление привилегированным доступом

Гибкие политики управления

PAM – НЕОЖИДАННОЕ РЕШЕНИЕ СЛОЖНЫХ ЗАДАЧ

Системы контроля привилегированного доступа включают:

- Анализ сбоев систем
- Расследование причин, чтобы восстановить инфраструктуру обратно
- Препятствие краже/продаже паролей
- Выявление использования чужих учетных записей
- Контроль действий внешних подрядчиков
- Фиксация доступа скриптов и роботов (RPA)
- Повышение скорости расследований инцидентов ИБ
- Контроль действий увольняющихся сотрудников
- Снижение рисков при использовании личных устройств для администрирования
- Усиленная аутентификация (2FA)
- Поиск «забытых» УЗ администраторов



ЗАКОНОДАТЕЛЬНАЯ БАЗА ДЛЯ ВНЕДРЕНИЯ PAM

Федеральный закон № 149-ФЗ от 27.07.2006 г.
«Об информации, информационных технологиях и о защите информации»

Приказ ФСТЭК России № 31 от 14.03.2014 г.
«Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

Федеральный закон от № 187-ФЗ от 26.07.2017 г.
«О безопасности критической информационной инфраструктуры Российской Федерации»

Приказ ФСТЭК России № 235 от 21.12.2017 г.
«Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»

Приказ ФСТЭК России № 239 от 25.12.2017 г.
«Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

Кого касается

Оборонные и топливные комплексы | Наука и здравоохранение | Металлургическая отрасль | Атомная и другие виды энергетики | Транспорт

Сфера связи | Космическая, ракетостроительная и химическая промышленность | Банковская или иная финансовая сфера | Горнодобывающая отрасль

ПРИКАЗЫ ФСТЭК РОССИИ ОТ N 31/239

- I. Идентификация и аутентификация (ИАФ)
- II. Управление доступом (УПД)
- III. Ограничение программной среды (ОПС)
- IV. ~~Защита машинных носителей информации (ЗНИ)~~
- V. Аудит безопасности (АУД)
- VI. ~~Антивирусная защита (АВЗ)~~
- VII. ~~Предотвращение вторжений (компьютерных атак) (СОВ)~~
- VIII. Обеспечение целостности (ОЦЛ)
- IX. Обеспечение доступности (ОДТ)
- X. ~~Защита технических средств и систем (ЗТС)~~
- XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)
- XII. Реагирование на компьютерные инциденты (ИНЦ)
- XIII. ~~Управление конфигурацией (УКФ)~~
- XIV. ~~Управление обновлениями программного обеспечения (ОПО)~~
- XV. ~~Планирование мероприятий по обеспечению безопасности (ПЛН)~~
- XVI. Обеспечение действий в нештатных ситуациях (ДНС)
- XVII. Информирование и обучение персонала (ИПО)

ПРИКАЗЫ ФСТЭК 31/239 ПО ПУНКТАМ

СООТВЕТСТВИЕ	КОЛ-ВО ПУНКТОВ	ПЕРЕЧИСЛЕНИЕ ПУНКТОВ И ПРОЦЕССОВ
Полностью реализует	42	ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6, ИАФ.7 УПД.2, УПД.4, УПД.5, УПД.6, УПД.7, УПД.9, УПД.10, УПД.11, УПД.13 ОПС.3 АУД.3, АУД.4, АУД.6, АУД.7, АУД.8, АУД.9, АУД.10 ОЦЛ.1, ОЦЛ.2, ОЦЛ.5 ОДТ.1, ОДТ.2, ОДТ.3, ОДТ.4, ОДТ.5, ОДТ.6, ОДТ.7 ЗИС.1, ЗИС.30, ЗИС.1, ЗИС.2, ЗИС.3, ЗИС.6 ДНС.6
Реализует при определенных условиях	11	ИАФ.2 УПД.1, УПД.14 ОЦЛ.3, ОЦЛ.4 ЗИС.6 УКФ.1, УКФ.2, УКФ.3, УКФ.4 ИПО.1

АРХИТЕКТУРА И ВОЗМОЖНОСТИ

Поддержка протоколов:

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

Поддержка управления паролями целевых ресурсов:

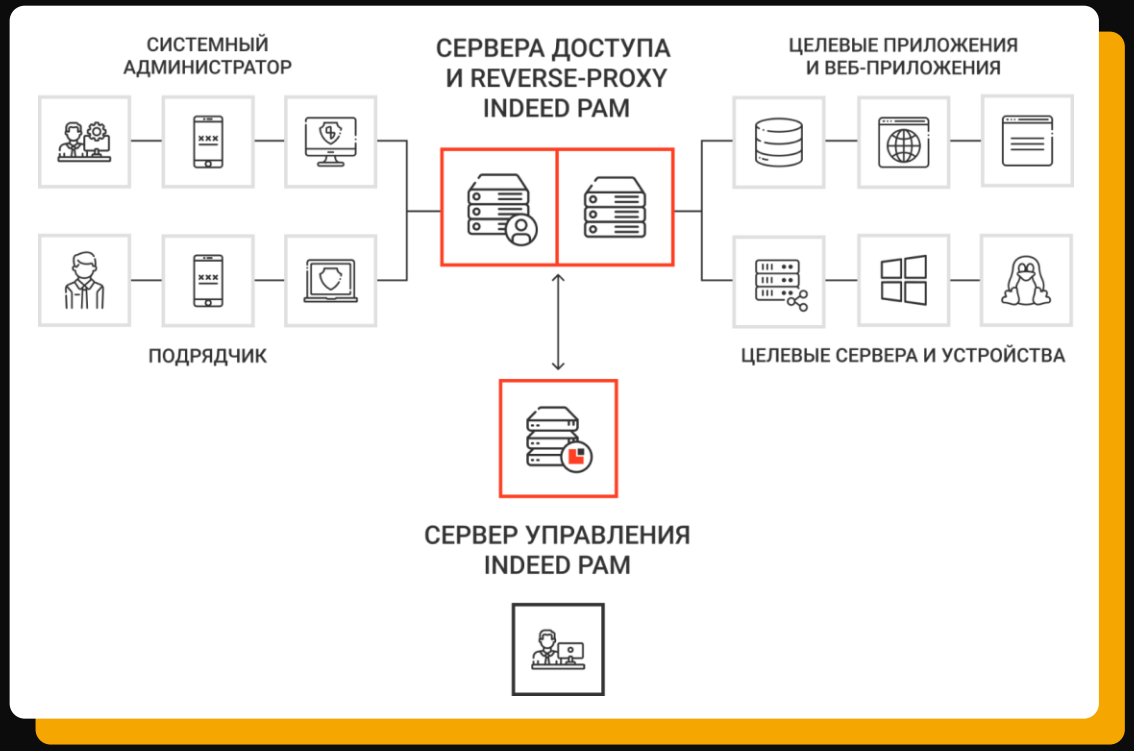
- Active Directory / FreeIPA/ ALD Pro/ OpenLDAP
- MS Windows
- Linux/Unix
- Cisco, Inspur BMC,
- СУБД (PostgreSQL, MS SQL, MySQL, Oracle DB)

Поддержка интеграций:

- RADIUS
- SIEM (syslog)
- Mail (SMTP)
- Mobile OTP (TOTP)
- ServiceDesk (CLI)
- IdM (API)

Поддержка способов контроля действий:

- Видеозапись, текстовая запись, снимки экрана
- Теневое копирование файлов
- Реакция на команды из черного и белого списка команд в SSH сессиях
- Контроль передачи файлов по протоколам SCP и SFTP
- Разрыв удаленного подключения



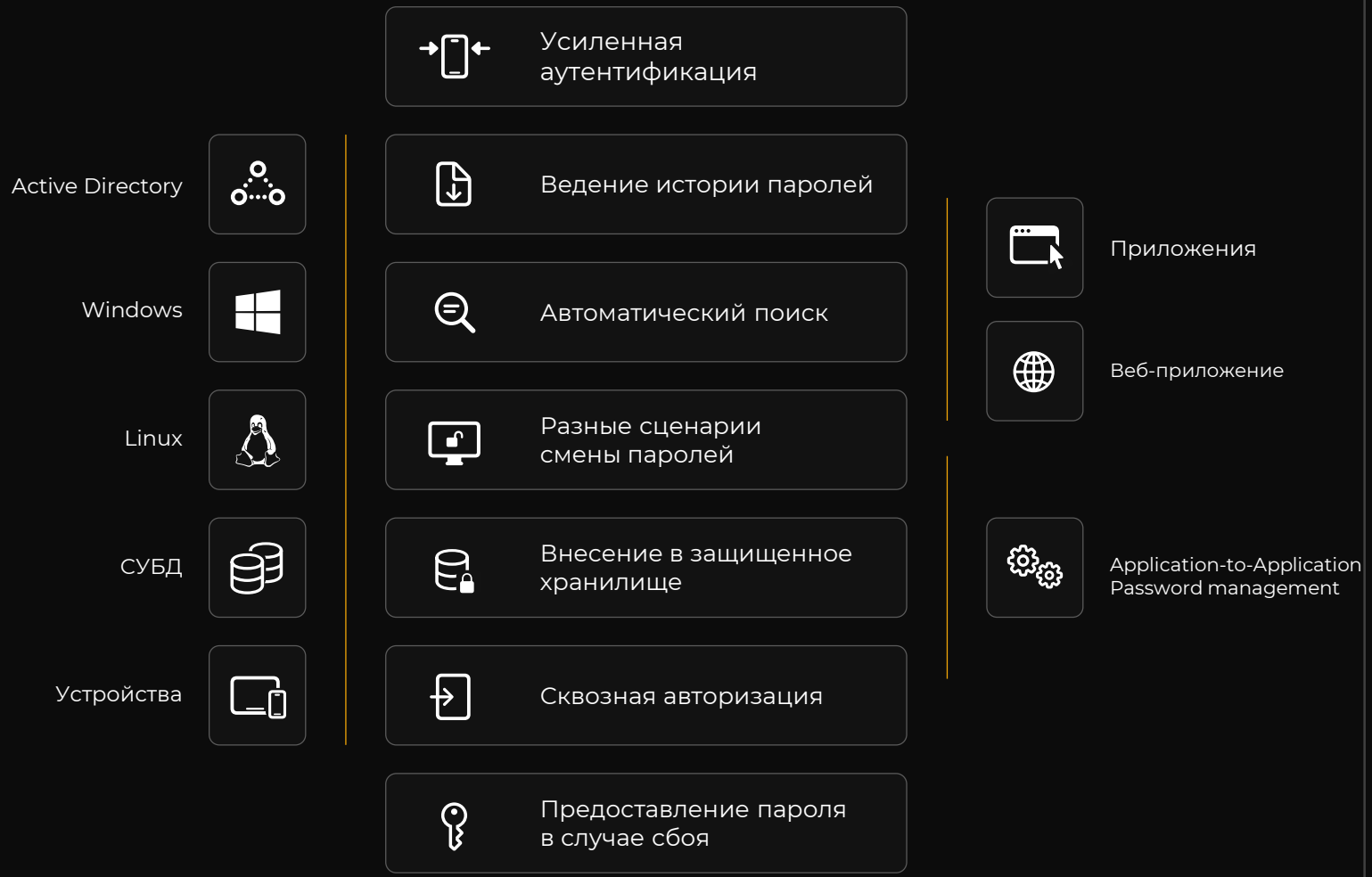
БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ ПРИВИЛЕГИРОВАННЫХ УЧЕТНЫХ ДАННЫХ

Недостатки парольной аутентификации:

- Подбор паролей
- Несанкционированная передача паролей
- Требование своевременной смены паролей при увольнении сотрудников

Решение позволяет:

- Сохранить пароли в секрете от сотрудников
- Проводить автоматический поиск и импорт привилегированных учетных записей
- Управлять паролями: обновление, выдача, сброс после подключения
- Осуществлять единый вход (Enterprise Single Sign-On) для целевых приложений
- Применять усиленную аутентификацию
- Вести историю паролей
- Application-to-Application Password Management



КОМПАНИЯ
ИНДИД

INDEED KEY:
МОБИЛЬНОЕ ПРИЛОЖЕНИЕ ДЛЯ АУТЕНТИФИКАЦИИ

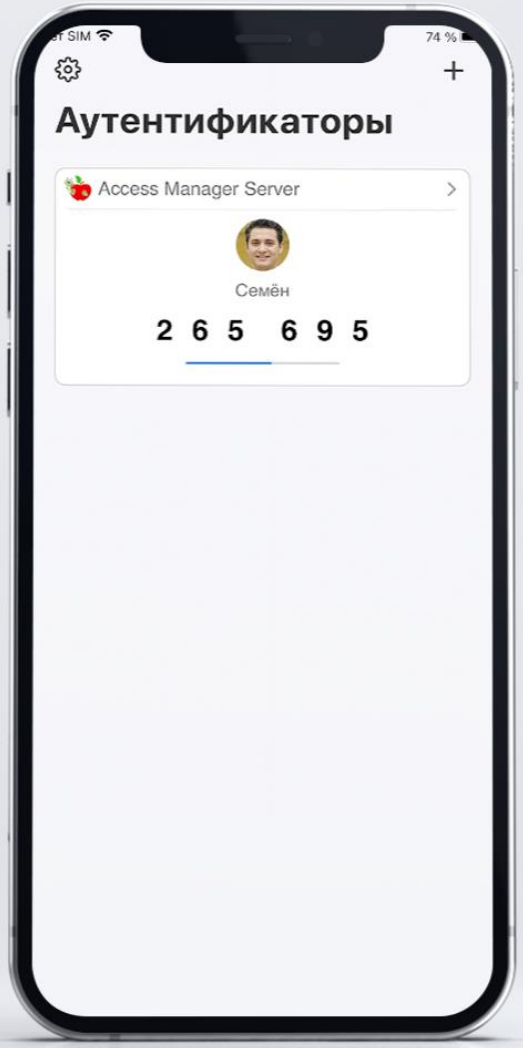
- Поддержка протокола аутентификации TOTP (одноразовые пароли)
- Поддержка аутентификации через push-уведомления
- Удобство применения для локального и удаленного доступа

Download on the App Store

GET IT ON Google Play

Explore It On App Gallery

* Indeed Key - бесплатное мобильное приложение



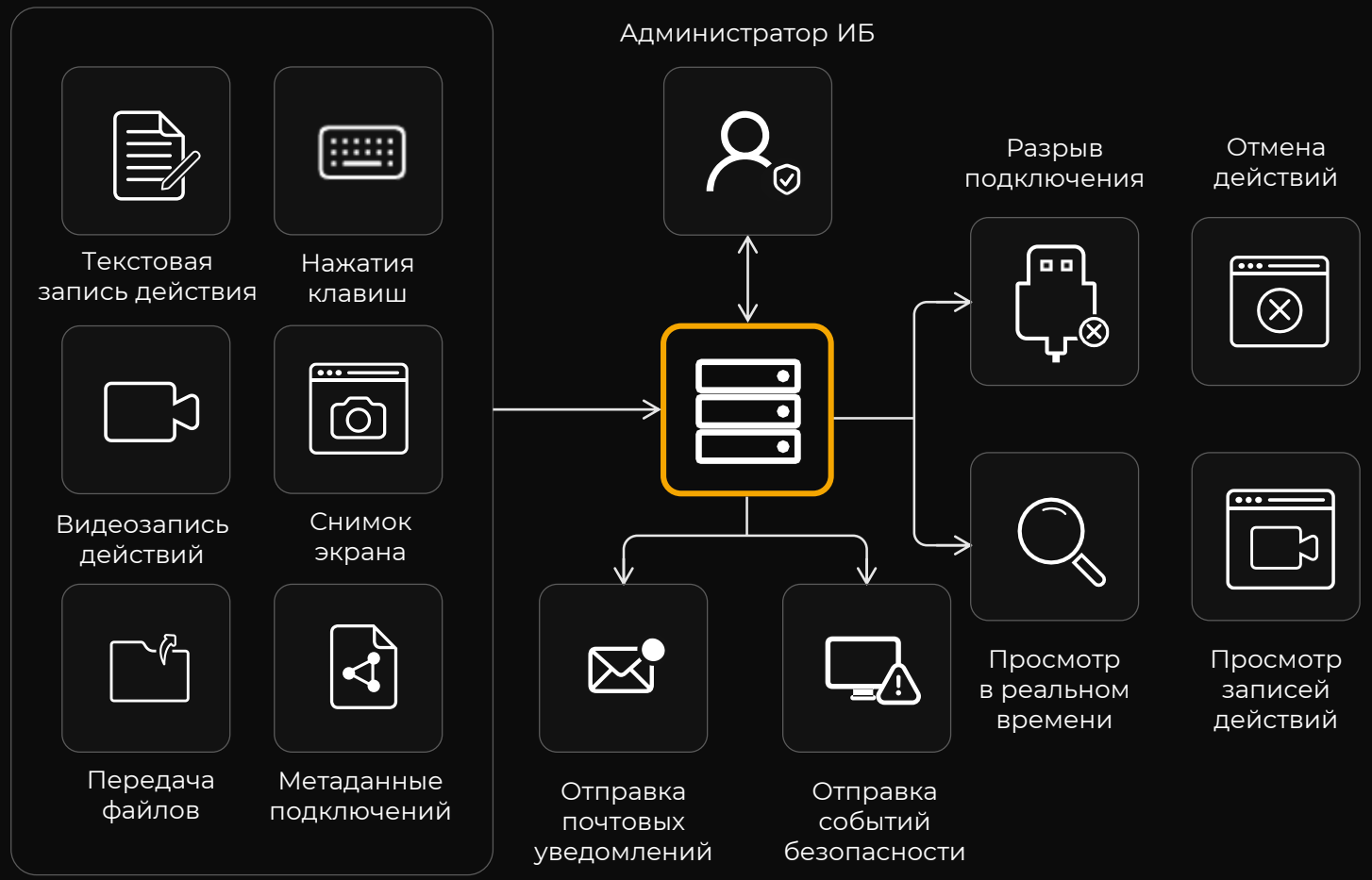
ФИКСАЦИЯ И КОНТРОЛЬ ДЕЙСТВИЙ

Иные решения ИБ имеют ряд ограничений:

- Необходимость установки агента мониторинга, что возможно далеко не на всех устройствах
- Доступность журналов для сервера мониторинга (если сервер недоступен нельзя получить с него журналы и проанализировать)
- Административные привилегии позволяют остановить агенты и удалить журналы

Использование PAM позволит:

- Зафиксировать действия в разном формате без установки агентов
- Осуществлять контроль вводимых команд и разрешать заранее определенные действия
- Воздействовать на административную сессию и на действия вручную или автоматически
- Контролировать передачу файлов, сохранить их теневые копии
- Повысить эффективность расследования



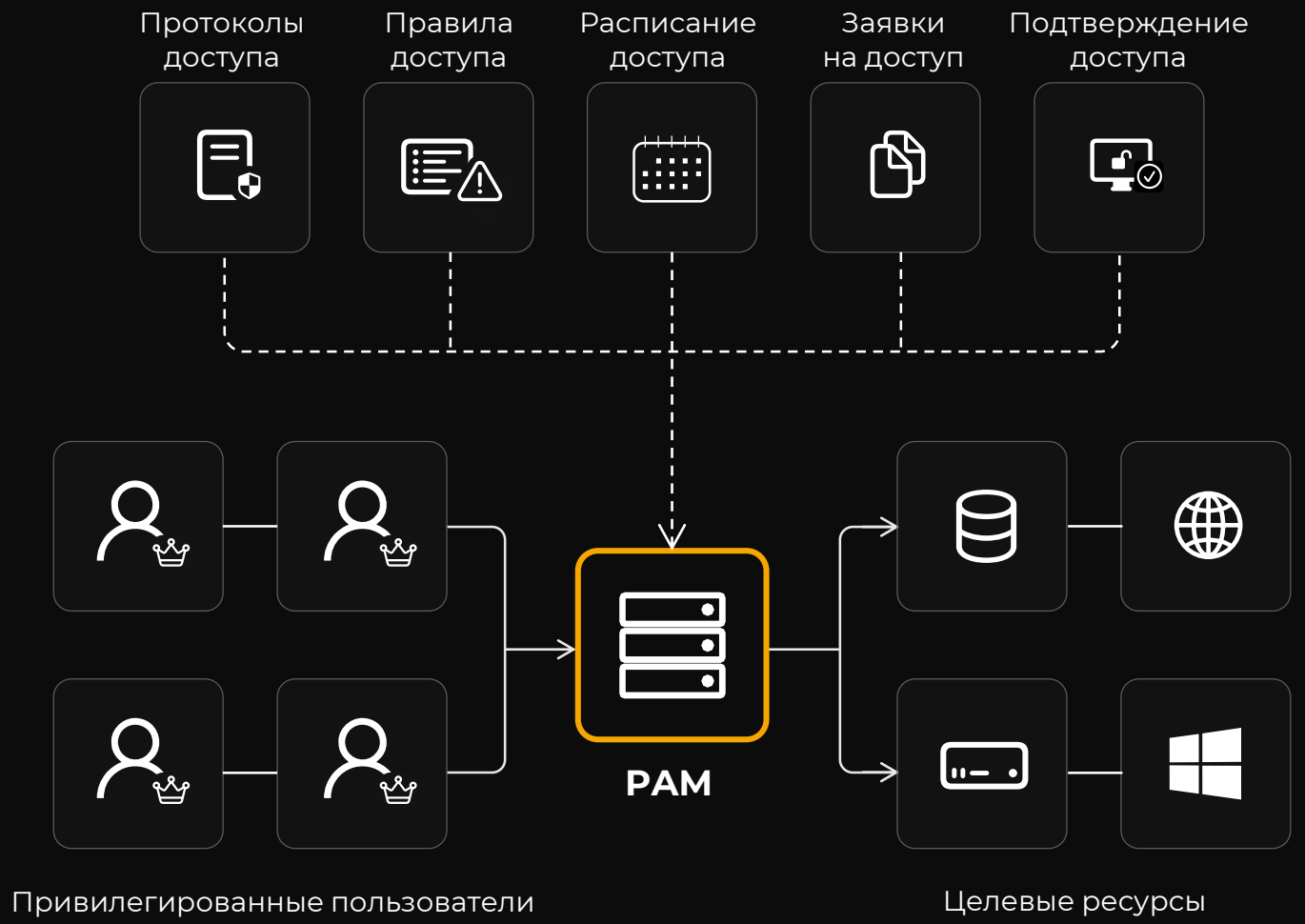
ЕДИНАЯ ТОЧКА УДАЛЕННОГО ДОСТУПА АДМИНИСТРАТОРОВ

Сложности и риски удаленного доступа:

- Низкий уровень защищенности личного рабочего устройства сотрудника и сети
- Открытие доступа извне к критичным ресурсам организации
- Чрезмерные полномочия, выдаваемые сотрудникам
- Необходимость изменения архитектуры сети для предоставления удаленного доступа

Использование PAM позволит избежать:

- Необходимости настройки сетевого взаимодействия на разных устройствах
- Установки дополнительного ПО на удаленные рабочие станции
- Корректировки выданных полномочий привилегированным пользователям и рядовым сотрудникам



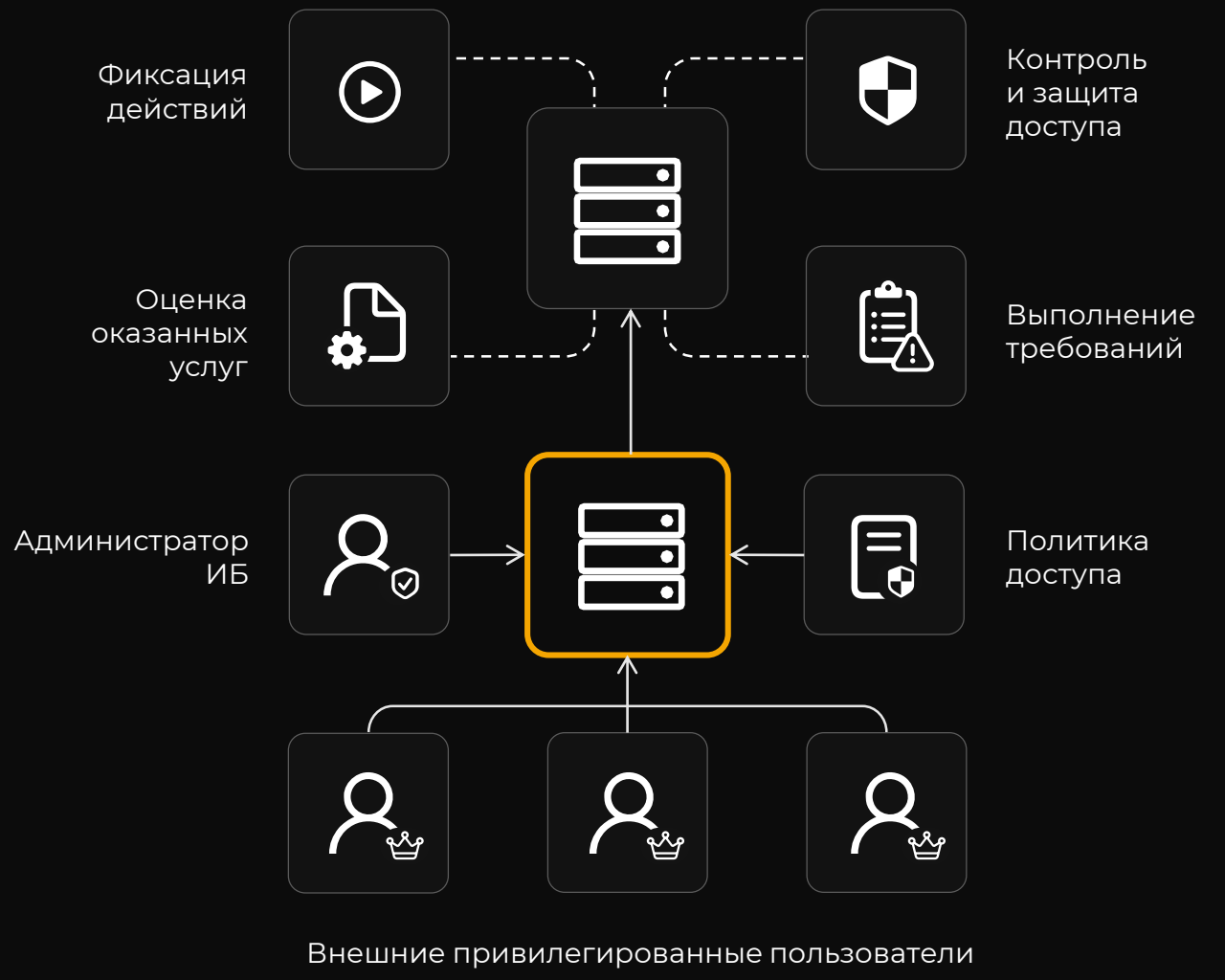
КОНТРОЛИРУЕМЫЙ ДОСТУП ПОДРЯДЧИКОВ

Сложности и риски привилегированного доступа:

- Локальная работа требует затрат на логистику и снижает оперативность реагирования
- Незащищенный удаленный доступ является источником повышенной опасности
- Затруднен учет реального времени работ и соблюдения требований SLA подрядчиков
- Невозможность объективной оценки выполненных работ
- Высокие трудозатраты на расследование сбоя или инцидента иными системами контроля

Решение позволяет:

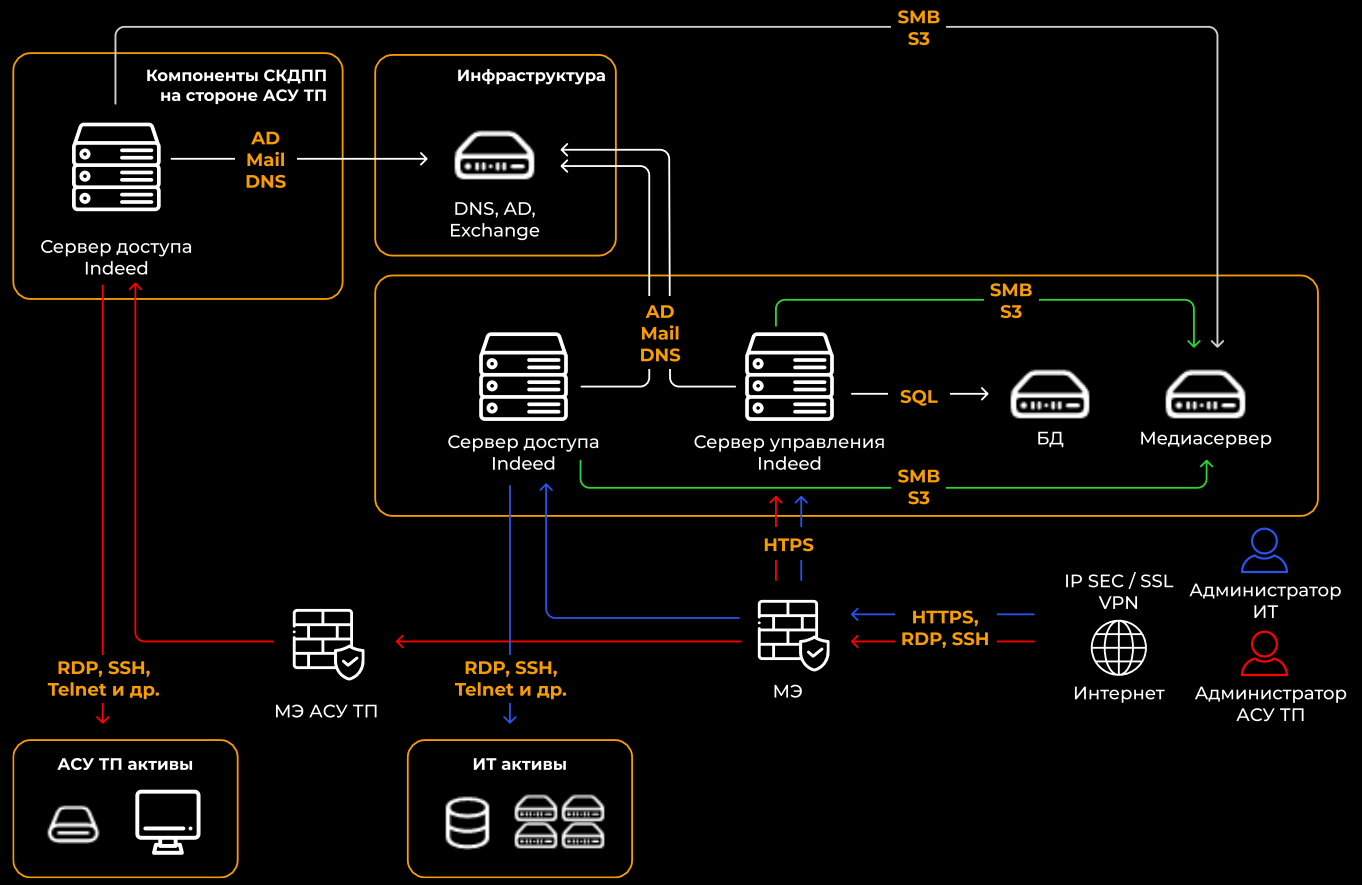
- Защитить и ограничить доступ (2FA, по расписанию и согласованием)
- Получить данные для оценки качества работы
- Записать активности подрядчиков при работе
- Экономить время и ресурсы при предоставлении привилегированного доступа



ЗАЩИТА ДОСТУПА В ПРОМЫШЛЕННОМ СЕГМЕНТЕ

Использование Indeed PAM позволит:

- Обеспечить однозначную идентификацию сотрудников, имеющих доступ к сегментам КИИ, включая подрядные организации на объектах
- Разграничить этот доступ в соответствии с политикой безопасности на предприятии
- Проанализировать поведение пользователей в процессе их работы и, таким образом, снизить риск инцидентов на предприятии
- Выявить прямое подключение в обход сервера доступа PAM и вовремя запустить меры реагирования



ИМПОРТОЗАМЕЩЕНИЕ

FUDO SECURITY

CYBERARK®

WALLIX CYBERSECURITY SIMPLIFIED

thycotic

BROADCOM®

IBM

BeyondTrust

ONE IDENTITY™

Замещаемые продукты:

- CyberArk PAM
- Fudo PAM
- Thycotic Secret Server
- One Identity Safeguard
- WALLIX Bastion PAM
- BeyondTrust PAM
- Broadcom-Symantec PAM
- Другие продукты класса PAM

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

Сертификат ФСТЭК России позволяет применять PAM:

- В государственных информационных системах до 1 класса защищенности
- В автоматизированных системах управления производственными и технологическими процессами до 1 класса защищенности
- В информационных системах персональных данных при необходимости обеспечения до 1 уровня защищенности
- В значимых объектах критической информационной инфраструктуры до 1 категории значимости

Выполнение требований:

- Федеральных законов № 149, 152, 187
- Приказов ФСТЭК России № 17, 21, 31, 239
- ГОСТ 57580.1-2017
- PCI DSS

ПРАКТИКА ЗАЩИТЫ КИИ С ПРИМЕНЕНИЕМ INDEED PAM

ЗАКАЗЧИК

ГК «РОСВОДОКАНАЛ»

ЗАДАЧИ

1. Обеспечить защиту от несанкционированного доступа злоумышленников с административными правами к корпоративным ИТ-ресурсам
2. Исключить рутинные операции из работы администраторов информационных систем

РЕЗУЛЬТАТ

1. Реализована группировка ресурсов: создано отдельное подразделение с ресурсами для каждого филиала и выданы права на управление подразделением соответствующему администратору PAM
2. Настроена дополнительная защита доступа администраторов с помощью механизма усиленной аутентификации на основе генератора одноразовых паролей (TOTP)

Подробнее: https://indeed-company.ru/blog/gk-rosvodokanal-vibiraet-indeed-pam/

ПРАКТИКА ЗАЩИТЫ КИИ С ПРИМЕНЕНИЕМ INDEED PAM

ЗАКАЗЧИК

АО «УК «КУЗБАССРАЗРЕЗУГОЛЬ»

ЗАДАЧИ

1. Усилить защиту доступа всех категорий пользователей (что особенно важно на фоне существующих сегодня в киберпространстве угроз)
2. Сформировать гибкие и удобные механизмы повышения эффективности контроля доступа к ИТ-системам Компании

РЕЗУЛЬТАТ

Внедрены продукты Indeed AM и Indeed PAM.

Их совместное применение обеспечивает:

1. эксплуатацию единой экосистемы усиленной аутентификации для доступа к корпоративным ИТ-ресурсам
2. централизованное управление доступом всех категорий пользователей
3. защиту удаленного доступа при подключении к внутренним корпоративным ресурсам через VPN
4. уменьшение риска утраты конфиденциальных данных и вероятности возникновения инцидентов
5. снижение трудозатрат специалистов по ИБ и повышение производительности труда сотрудников

Подробнее: https://indeed-company.ru/blog/indeed-pam-am-kuzbassrazrezugol/

ПРАКТИКА ЗАЩИТЫ КИИ С ПРИМЕНЕНИЕМ INDEED PAM

ЗАКАЗЧИК

ГРУППЫ КОМПАНИЙ ЕПК

ЗАДАЧИ

1. Обеспечить защиту от несанкционированного доступа
2. Реализовать дополнительную защиту в дополнение к инструментам парольной аутентификации

РЕЗУЛЬТАТЫ

1. Очевидные удобство и простота использования ПО класса PAM
2. Повышение дисциплинированности сотрудников за счет планирования и четкой проработки политики предоставления привилегированного доступа
3. Возможность самостоятельно расследовать любой инцидент, произошедший в информационной системе компании
4. Уменьшение поверхности атаки на информационные ресурсы компании

Подробнее: https://indeed-company.ru/blog/intervyu-epk-indeed-pam/

НЕСКОЛЬКО ПРОСТЫХ ШАГОВ — И ПРИВИЛЕГИИ ПОД ЗАЩИТОЙ

1. Анализируем требования и политику ИБ
2. Уточняем текущие решения, их функциональность и ваши сценарии использования
3. Подбираем решения по их функциональности и применимости для решения ваших задач
4. Обсуждаем с вами имеющиеся варианты, изучаем возможные ограничения решения и фиксируем обязательные требования
5. Составляем спецификацию и проводим бюджетирование
6. Пилотируем решение на вашем тестовом полигоне
7. Заключаем договор на создание системы и запускаем проект
8. Переводим решение в промышленную эксплуатацию
9. Обеспечиваем техническую поддержку, мониторинг USSC-SOC

УЦСБ

ПРОГРАММА ВЕБИНАРОВ

19.03	Как защитить КИИ от киберугроз? (Категорирование КИИ)
09.04	Как построить эффективную систему обеспечения ИБ объектов КИИ
25.04	Практические кейсы построения СОИБ
28.05	Мониторинг ЗОКИИ (SOC)
04.06	PAM или пропал: как обеспечить эффективное управление привилегированным доступом для защиты КИИ
04.07	Безопасная разработка ПО для значимых объектов КИИ
	Оценка защищенности для ЗОКИИ (с учетом Указа Президента РФ № 250)
	Подготовка к прохождению госконтроля

УЦСБ

ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

СПАСИБО ЗА ВНИМАНИЕ!
ВОПРОСЫ?

sec.ussc.ru

cybersec@ussc.ru

Илья Филичкин

Менеджер по развитию решений
УЦСБ

КОМПАНИЯ ИНДИД УЦСБ

ПАРТНЕР ВЕБИНАРА — КОМПАНИЯ ИНДИД

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

15+
ЛЕТ ОПЫТА

500+
ЗАЩИЩАЕМЫХ СИСТЕМ

120+
РЕГИОНАЛЬНЫХ ПАРТНЕРОВ

ПОЛНОСТЬЮ РОССИЙСКАЯ РАЗРАБОТКА

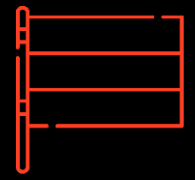
ЗАКАЗЧИКИ

Газпром нефть | Новатэк | Роснефть | Газпром | Россети
ГТЛК | Carcade | СТС | Магнит | О'КЕЙ
ВТБ | Альфа Банк | Банк Санкт-Петербург | МТС | epk

КОМПАНИЯ ИНДИД УЦСБ

ПРЕИМУЩЕСТВА РАМ ИНДИД

Русскоязычная техническая поддержка 24/7



Российский разработчик программного обеспечения

Бесплатное тестирование продуктов с возможностью предоставления оборудования (через партнеров)

Организация референсов и презентаций

КОМПАНИЯ ИНДИД

УЦСБ

ЛИНЕЙКА ПРОДУКТОВ

Все продукты находятся
в Реестре отечественного
программного обеспечения