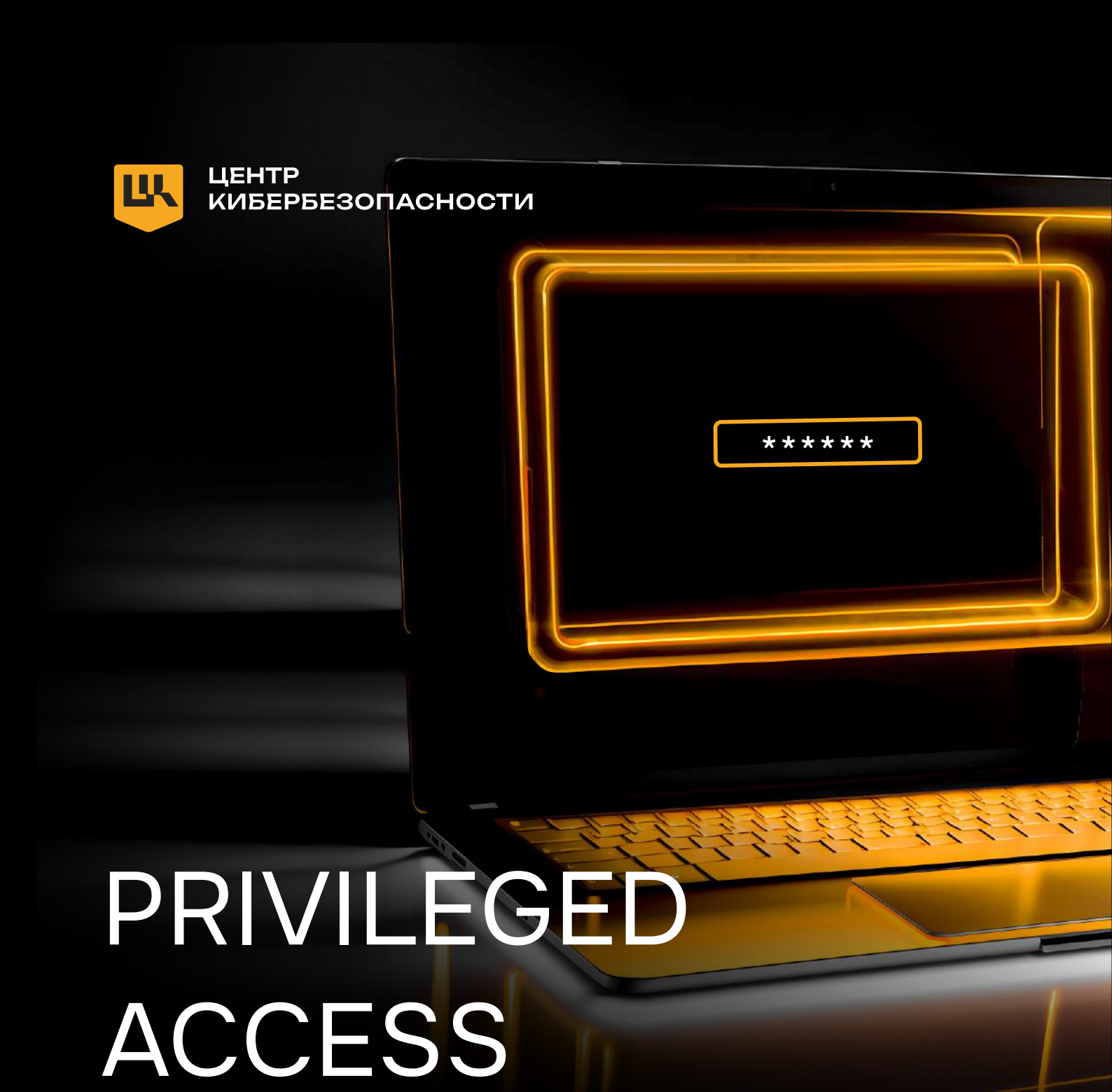
ЦЕНТР
КИБЕРБЕЗОПАСНОСТИ



PRIVILEGED ACCESS MANAGEMENT

Системы класса Privileged Access Management (PAM) позволяют существенно снизить риски, связанные с организацией привилегированного доступа сотрудников и контрагентов в информационные системы компании

РИСКИ БЕСКОНТРОЛЬНОГО ПРИВИЛЕГИРОВАННОГО ДОСТУПА

Угрозы безопасности информации

- ! Взлом паролей
- ! Распространение вредоносного ПО
- ! Кража конфиденциальных данных
- ! Вывод из строя информационных систем (ИС)
- ! Отключение доступа к ИС
- ! Несоответствие требованиям регуляторов

Непродуктивное расходование ресурсов отдела ИТ

- ! Сложная процедура выдачи учетных записей
- ! Ручной учет аутентификаторов

Снижение производительности труда пользователей

- ! Несколько учетных записей на пользователя
- ! Сложная процедура получения доступа к ресурсам

ОТСУТСТВИЕ ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ

PAM – ЭФФЕКТИВНОЕ УПРАВЛЕНИЕ ПРИВИЛЕГИРОВАННЫМ ДОСТУПОМ

- Централизованное управление привилегированным доступом сотрудников к целевым ресурсам
- Обнаружение и контроль использования привилегированных учетных записей
- Сокращение количества привилегированных учетных записей и поверхности атаки
- Обеспечение многофакторной аутентификации сотрудников при доступе к привилегированным учетным записям
- Аудит действий пользователей и реализация механизмов расследования инцидентов
- Управление паролями, а также изоляция пользователей от целевых систем
- Реализация сложных политик безопасности, а также интеграция со смежными средствами ИБ
- Выполнение требований регуляторов по ИБ

Сценарий применения

Управление паролями
Ключевая цель — исключение несанкционированного административного доступа к ИТ-системам компании

Единая точка удаленного доступа
Ключевая цель — внедрение управляемого удаленного привилегированного доступа к корпоративным ресурсам

Защита доступа сегмента АСУ ТП и КИИ (опционально)
Ключевая цель — обеспечение защищенного и контролируемого доступа к критичной инфраструктуре

Мониторинг и расследование
Ключевая цель — повышение эффективности реагирования благодаря фиксации действий привилегированных пользователей для расследования инцидентов

Контролируемый доступ подрядчиков
Ключевая цель — создание временного и безопасного доступа для внештатных пользователей в ИТ системы компании, получение данных для оценки качества работы

Выявление аномалий для SOC и ЦОД (опционально)
Ключевая цель — обеспечение качественной обработки поступающих событий и повышение скорости реагирования

Преимущества внедрения PAM

- Все привилегированные учетные записи известны и находятся под контролем
- Единая точка доступа к ключевым элементам инфраструктуры
- Предотвращение потенциально опасных действий
- Архив записей сессий доступа к ключевым элементам инфраструктуры
- Уменьшение поверхности атаки
- Строгие парольные политики учетных записей даже для систем, которые сами не могут их поддерживать

КОМПЕТЕНЦИИ

Опыт работы с 2007 года на рынке информационной безопасности

- Собственный Сервисный центр, обеспечивающий круглосуточный прием заявок
- Первая линия технической поддержки по решениям информационной безопасности
- Собственные демо-стенды с решениями класса PAM (Indeed PAM, СКДПУ НТ)

Эксперты УЦСБ имеют многолетний опыт реализации проектов по созданию систем защиты и непрерывно развивают свои профессиональные компетенции, подтверждая их сертификатами ведущих производителей.

Компания Индид: «Установка и настройка системы Indeed PAM в базовой конфигурации»

АйТи Бастион: «Комплекс СКДПУ НТ: обеспечение безопасного и эффективного доступа к информационным системам организаций, в том числе объектам КИИ»

One Identity: «Privileged Access Management & Identity Governance Presales Accreditation»

О ЦЕНТРЕ КИБЕРБЕЗОПАСНОСТИ УЦСБ

Центр кибербезопасности — объединение профильных компетенций УЦСБ для защиты критически важных систем от кибератак.

Помогаем выбрать и настроить инструменты информационной безопасности для ИТ-инфраструктур различного уровня зрелости

Предоставляем комплексные услуги по обеспечению кибербезопасности бизнеса и государственных организаций

Преимущества

Соответствие стандартам и требованиям

- Внедрена система менеджмента качества в соответствии со стандартами ISO 9001
- Имеются лицензии ФСБ России (№454 от 05.08.2013) и ФСТЭК России (№0348 от 07.12.2015, №0607 от 08.10.2007)
- Применяются методики на основе международных стандартов и рекомендаций (NIST, OWASP, PCI DSS)

Ценные для рынка компетенции

- Опыт разработки нетиповых интеграций с самописными или нишевыми системами российского и зарубежного производства
- Компетенции по внедрению решений ИБ в сложной ИТ-инфраструктуре

Команда с подтвержденной экспертизой

- Дипломы и сертификаты в области кибербезопасности
- Выявленные и зарегистрированные уязвимости
- Публикации в СМИ
- Опыт создания собственных продуктов и сервисов

620100, г. Екатеринбург, ул. Ткачей, д. 6

+7 (343) 379-98-34

cybersec@ussc.ru

sec.ussc.ru

Telegram

Хабр