Михаил Хмелевский

Владелец продукта «СКУД»

Безопасный СКУД

по стандартам ФинТеха

СКУД2025 ТЕХНОЛОГИИ И КОММУНИКАЦИЯ

СБЕР

СКУД СБЕРа

Самая большая система контроля доступа в России и восточной Европе

Количество считывателей

50+ тыс.

Количество контроллеров

15+ тыс.

Количество пользователей

300+ тыс.

Интегрировано в СКУД

>1млн.

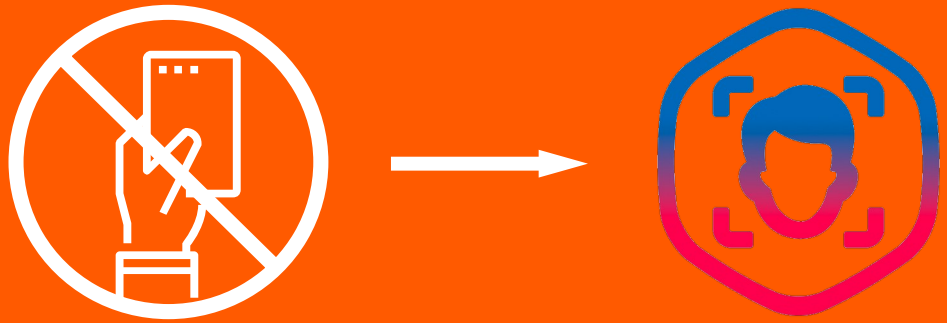
СБЕР

Безопасный СКУД — это набор организационно — технических мер, которые позволяют обеспечивать комплексный подход

СБЕР

СКУД для пользователя — начинается с карты-пропуска, или сданной биометрии - с разрешением использовать её для проходов в СКУД.

Отказ от пластика



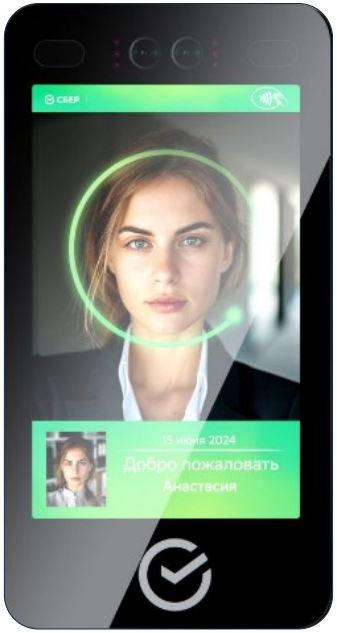
Внедрение биометрии

Что такое безопасная карта ?
Это карта, которую невозможно взломать или скопировать.

Em-Marine, HID,
UID, MIFARE Classic..

AES128/256, ECC
Длинные ключи
Временные метки

Биотерминалы СБЕРа



Биометрия в Банке: — полностью соответствует 572-ФЗ

1 **2 размера:**

Экраны
6` и 8`
дюймов

2 **Крепление:**

Стена,
Турникет,
Стойка

3 **Всепогодное исполнение:**

Работают
От -30 С°
до +60 С°

СБЕР

Внедрение биометрии

Первый биотерминал

Старт пилотного проекта полностью «белых» биотерминалов для Банка

Q4 2024

Штаб-квартира Кутузовский, 32

800+ биотерминалов на объектах Банка, для сотрудников

Q3 2025

Биометрия для гостей

Организация доступа по биометрии для посетителей Банка

Q4 2025

Подрядчики и КИИ

Возможность использования биометрии на объектах КИИ

Q1 2026

СБЕР

Мониторинг и диагностика

1

Пользователи:

Расширенное логгирование, аналитика действий администраторов и операторов в СКУД

Выявление внеплановых изменений настроек и конфигураций оборудования СКУД

Интеграция принципа «Второй руки» для подтверждения критичных активностей

2

Оборудование:

Блокировка и разблокировка точек доступа за рамками существующих сценариев СКУД

Выявление удержания в положении «открыто» и принудительного открытия удерживающих устройств

Анализ и выявление характерных признаков повторного прохода

3

Серверы и ПО:

Отслеживание CPU и Memory нагрузки/загрузки серверных компонентов СКУД

Резервное копирование баз данных и журналов событий

Контроль параметров электропитания

Двухфакторная или OTP авторизация администраторов серверной части СКУД

СБЕР

Регламенты и контроль

1

1. Регламент установки и ввода в эксплуатацию компонентов СКУД

Регулируем процесс монтажа и настройки оборудования СКУД.
Включаем требования к порядку тестирования и приемки системы, инструкции по запуску и проверке функциональности всех устройств.

2

2. Регламент технического обслуживания СКУД

Определяем перечень мероприятий по поддержанию исправности и готовности системы. Содержит рекомендации по регулярному осмотру оборудования, замене комплектующих, диагностике состояния отдельных узлов и проведению профилактических работ.

3

3. Регламент регистрации происшествий и инцидентов в СКУД

Определяем действия операторов и инженеров при обнаружении проблем в функционировании СКУД. Включает протоколирование ошибок, формирование уведомлений ответственным лицам и принятие экстренных мер для устранения неисправностей.

4

4. Регламент взаимодействия пользователей со СКУД

Задаём правила обращения пользователей с оборудованием СКУД, уточняем процедуры выдачи карт доступа, идентификации личности, обучения правильному использованию СКУД.

5

5. Регламент информационной безопасности в СКУД

Направлен на защиту конфиденциальных сведений, хранящихся в базе данных СКУД. Включаем меры предосторожности против утечек персональных данных, описываем способы шифрования информации и принципы/методологию ограничения доступа к критически важной информации.

Ролевая модель: RBAC

1

Лучше = меньше:

Роли формируются исходя из организационной структуры и специфики бизнес-процессов компании.

Формирование происходит по принципу «соблюдение минимальной достаточности прав для реализации функционала».

Дробление ролей по объектам/подразделениям: минимизируем глобальные инциденты.

2

Аудит ролей:

Регулярные ревизии текущих ролей, выявление избыточных или устаревших прав,
устранение несоответствий между фактическим положением дел и существующими правилами.

Новые роли создаются:
- при появлении новых типов задач,
- вводе в эксплуатацию нового функционала,
- изменении структуры организации.

3

Единое управление:

Любые операции по изменению состава ролей, назначению и отзыву прав - централизованно управляются единой службой администрирования:

- обеспечиваем гибкость и масштабируемость моделей

- упрощаем поддержку большого числа пользователей.

RBAC: Должность + Роль + Функционал = Набор прав доступа

СБЕР

Спасибо !

СКУД2025 ТЕХНОЛОГИИ И КОММУНИКАЦИЯ