



Презентация на тему:

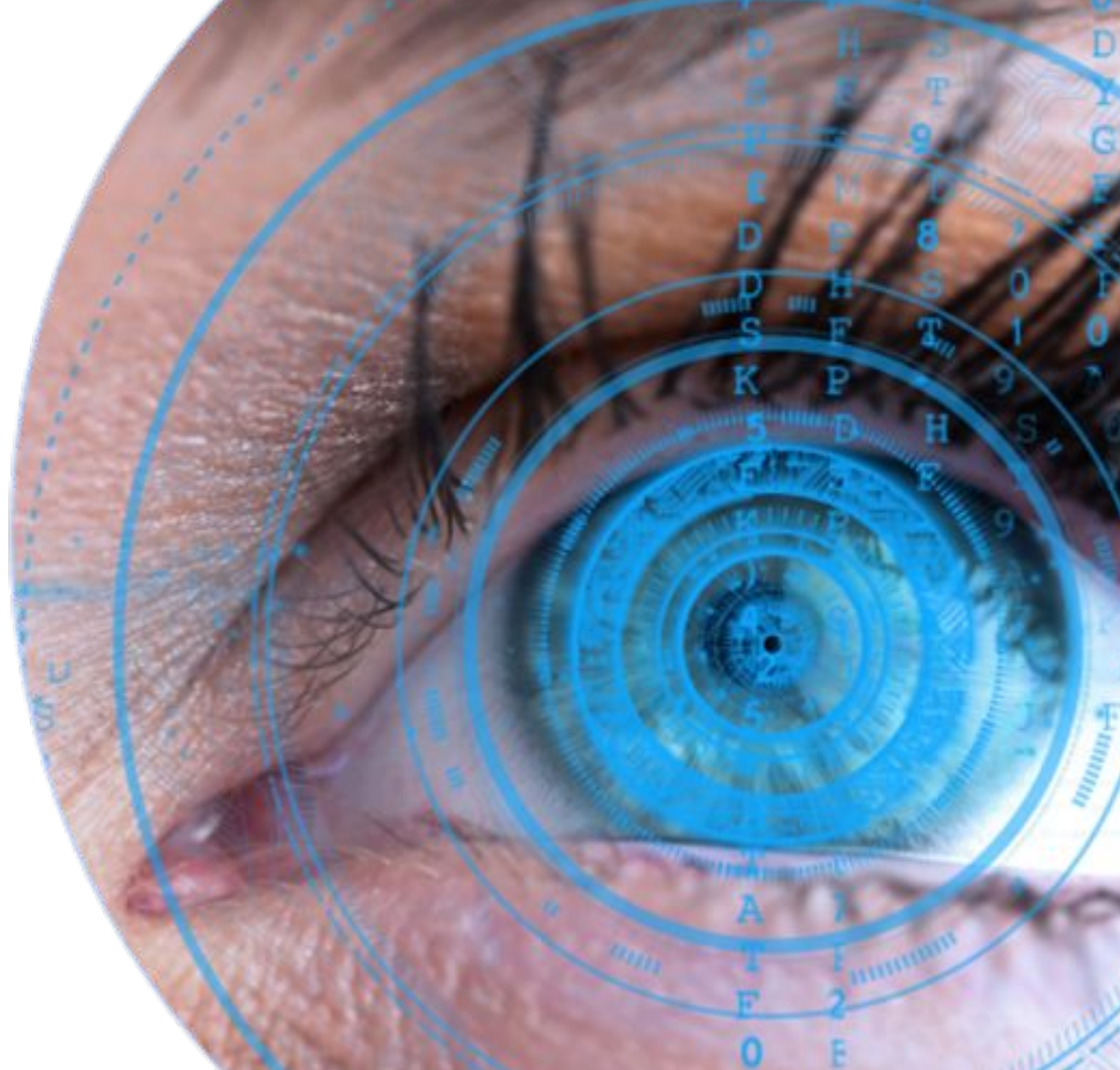
БИОМЕТРИЧЕСКИЕ СИСТЕМЫ КОНТРОЛЯ ДОСТУПА

Работу выполнил: Гурьянов
Игорь Олегович студент 1 курса

Что такое БСКД?

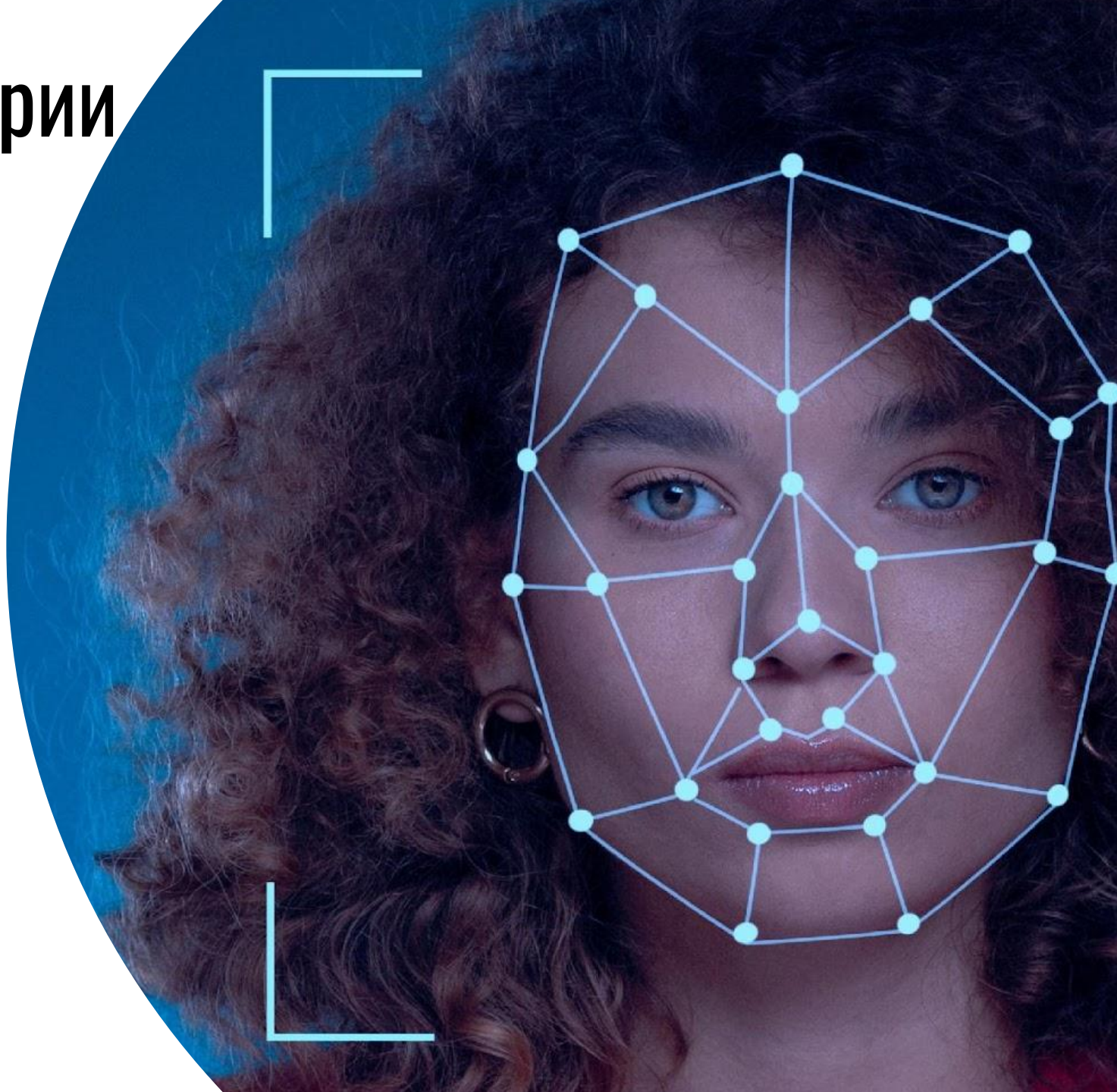
Биометрические системы контроля доступа (БСКД) представляют собой автоматизированные технологии, которые используют уникальные биологические характеристики человека (например, отпечатки пальцев, радужную оболочку глаза, голос, лицо) для проверки подлинности личности и авторизации доступа к защищенным объектам.

БСКД обеспечивают более высокий уровень безопасности, чем традиционные методы идентификации, такие как пароли или карты доступа. Люди не могут потерять или забыть свои биометрические характеристики, и они не могут передать их другому человеку.



Основные виды биометрии

- Распознавание отпечатков пальцев - сообщает информацию об уникальной линии и других особенностях строения и деталей пальца.
- Ирисовая биометрия - используется для распознавания уникального узора внутри глаза. Ирис - это окрашенная часть глаза
- Распознавание голоса - используется для сравнения озвучки с голосом
- Распознавание лица - используется для сравнения изображений лица в специальной базе данных.



Преимущества биометрии

- Наивысший уровень безопасности, так как основан на биологических характеристиках, уникальных для каждого человека.
- Удобство использования без необходимости запоминать пароли или носить с собой ключи.
- Меньше возможности для мошенничества, так как биологические характеристики нельзя скопировать или передать другому человеку.

Недостатки биометрии

- Высокая стоимость оборудования и внедрения самой системы контроля доступа в заведения.
- Ограниченное количество биометрических характеристик, которые можно использовать для идентификации.
- Риск несанкционированного доступа к хранимым данным, если система не защищена от хакерских атак.

Некоторые случаи применения биометрии



Распознавание лиц для целей безопасности государства и правопорядка.



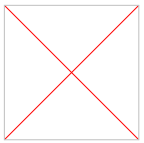
Контроль доступа на производстве, в банках и других финансовых учреждениях.



Идентификация и аутентификация пользователей в информационных системах.

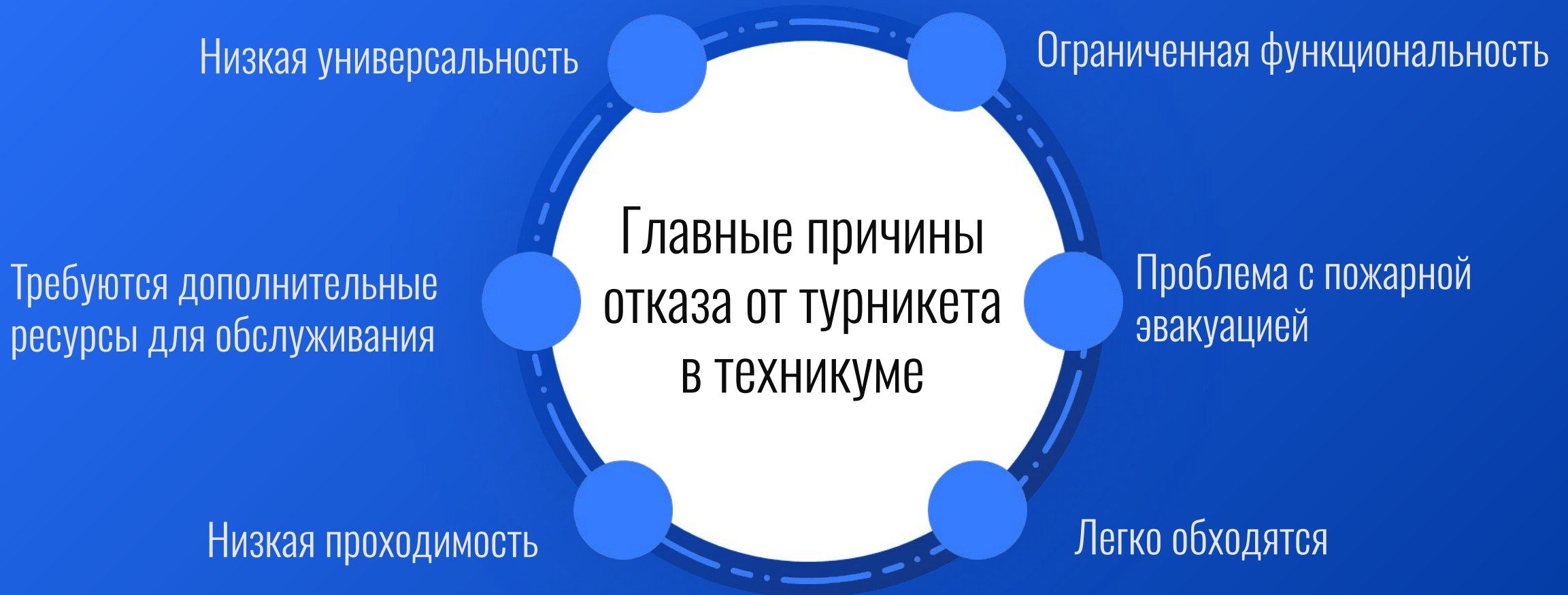


Идентификация пассажиров в аэропортах и на железнодорожных вокзалах.



Контроль доступа в зданиях, помещениях, к критической инфраструктуре.

Основные проблемы турникета стандартного типа



РЕКОМЕНДАЦИИ ПО ВЫБОРУ ТИПА БИОМЕТРИИ

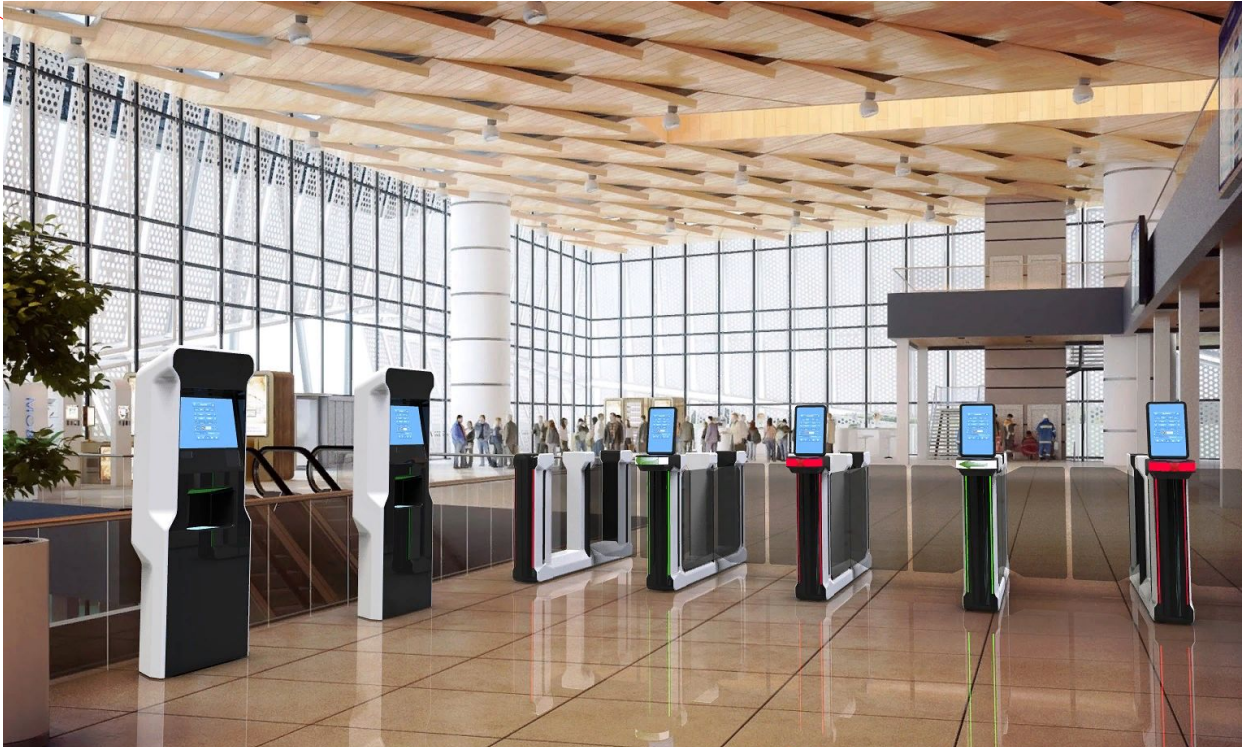
1. Размер учебного заведения.
2. Частота доступа пользователей в различные зоны техникума
3. Уровень безопасности
4. Бюджет



Этапы внедрения биометрической системы контроля доступа

Разработка индивидуальной биометрической системы защиты может включать следующие этапы:

1. Определение и анализ требований
2. Выбор типа биометрической системы.
3. Анализ требований и сбор данных
4. Разработка алгоритмов распознавания
5. Разработка программного обеспечения
6. Тестирование и настройка
7. Внедрение и поддержка
8. Учеба и обучение пользователей.





Будущее биометрии

Биометрические системы идентификации обладают высоким уровнем безопасности и точности, кроме того, они являются удобными и простыми в использовании. Эти технологии находят широкое применение в различных отраслях, включая финансы, здравоохранение, государственное управление, авиацию, транспорт, производство, образование и науку.

В общем и целом, биометрические системы имеют большой потенциал в обеспечении безопасности и предоставлении новых возможностей для идентификации личности. Они могут использоваться в сочетании с другими технологиями и методами, чтобы создать более безопасную среду для всех. Однако необходимо учитывать проблемы, связанные с конфиденциальностью и защитой личных данных, чтобы обеспечить максимальную безопасность и комфорт для пользователей.

