СТАНДАРТ БЕЗОПАСНОСТИ

СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА БАЗЕ ОБОРУДОВАНИЯ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ РОСТАБ®

ПРЕЗЕНТАЦИЯ АО «СТАНДАРТ БЕЗОПАСНОСТИ»

Предлагаемое АО «Стандарт безопасности» техническое решение позволит:

СТАНДАРТ БЕЗОПАСНОСТИ

- Создать единую и масштабируемую интегрированную систему безопасности на объектах предприятий
- Использовать программное обеспечение, включенное в Реестр российского ПО Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации (реестровая запись №24485)
- Применить контроллеры российского производства «РОСТАБ», выполняющие современные требования к интегрированным системам безопасности, в том числе в области кибербезопасности
- Унифицировать и стандартизировать внедряемые оборудование и ПО на объектах предприятий
- Интегрировать системы контроля доступом, видеонаблюдения и охранной сигнализации
- Внедрить на предприятии единый формат карт доступа российского производства с надежной защитой от клонирования

Ключевые особенности программного обеспечения РОСТАБ-А

СТАНДАРТ БЕЗОПАСНОСТИ

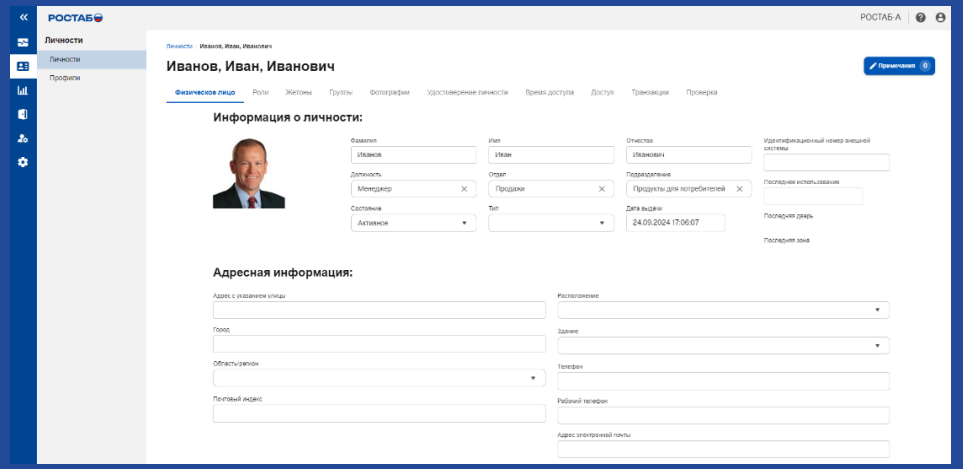
- Поддержка контроллеров СКУД российского производства РОСТАБ
- Поддержка контроллеров СКУД фирм Honeywell, LenelS2, Genetec, MAXXESS и HID Mercury Security для исключения необходимости замены уже установленного на объекте оборудования и минимизации затрат на обеспечение санкционной независимости
- ПО включено в Реестр Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации
- Поддерживаются российские дистрибутивы Linux
- ПО поставляется в составе сервера с ОС Linux или в виде виртуальной машины, СУБД – PostgreSQL/LDAP
- Работа операторов осуществляется через веб-интерфейс с использованием защищенного соединения SSL/TLS
- Использование веб-интерфейса позволяет обеспечить высочайший уровень кибербезопасности, удобство внедрения и обновления системы, а также независимость от используемой аппаратной платформы
- Поддерживается «горячее» резервирование серверов СКУД, в т.ч. с автоматическим переключением на резервный сервер
- Поддерживается шифрование каналов связи с контроллерами, модулями расширения и считывателями СКУД
- ПО РОСТАБ-А поддерживает работу с биометрическими терминалами распознавания лиц VisionPass

Программное обеспечение РОСТАБ-А

СТАНДАРТ БЕЗОПАСНОСТИ

«РОСТАБ-А» поддерживает:

- гибко настраиваемую ролевую модель управления
- разграничение областей видимости точек доступа, уровней доступа и владельцев карт СКУД между операторами
- гибкую настройку режимов аутентификации и алгоритмов доступа в СКУД
- многофакторную идентификацию в СКУД, проход в СКУД под принуждением, проход в СКУД с подтверждением, зональный и временной глобальный контроль повторного прохода (anti-passback), доступ в СКУД по правилу N-лиц
- централизованную выдачу идентификаторов пользователям СКУД и назначение прав доступа
- удаленное централизованное конфигурирование и управление оборудованием без необходимости непосредственного физического доступа к контроллерам, модулям СКУД и другому оборудованию

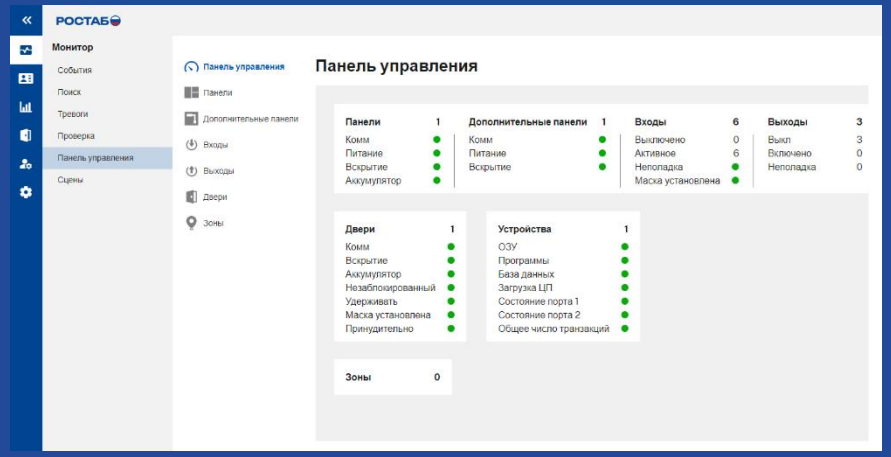


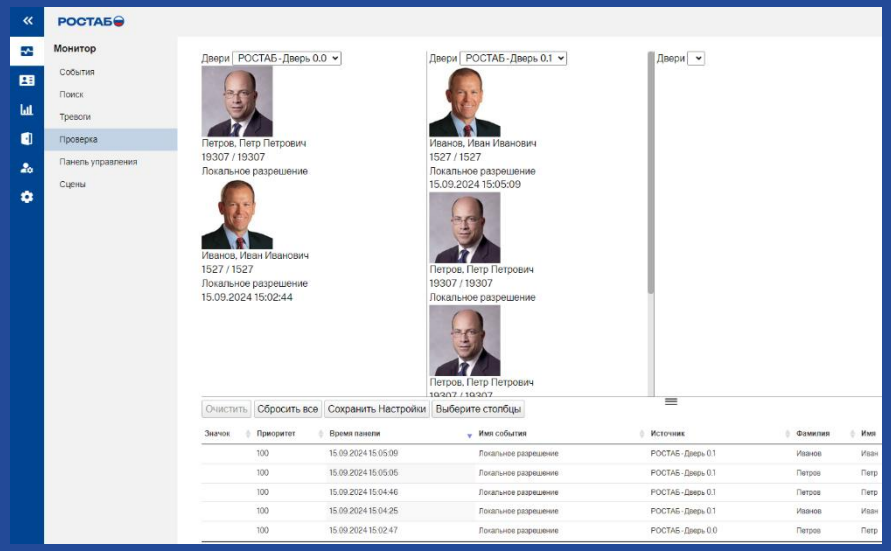
Программное обеспечение РОСТАБ-А

СТАНДАРТ БЕЗОПАСНОСТИ

«РОСТАБ-А» поддерживает:

- аппарат работы с записями посетителей и временными / разовыми идентификаторами – автоматизированная фиксация фактов выдачи и сдачи идентификаторов, управление картоприемниками СКУД различных типов, автоматическая блокировка идентификаторов СКУД при наступлении событий
- возможность добавлять дополнительные поля в записи пользователей (операторов), владельцев карт, посетителей
- формирование и экспорт отчетов, в т.ч. настраиваемых
- «горячее» резервирование серверов, в т.ч. с автоматическим переключением
- репликацию базы данных владельцев карт между несколькими серверами





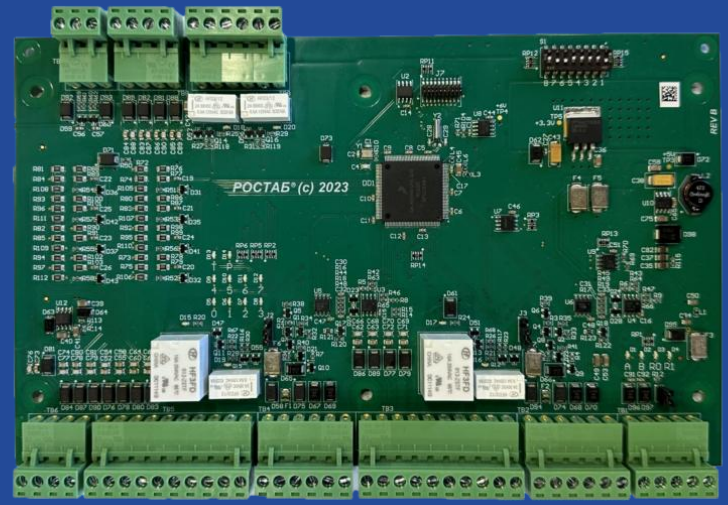
Контроллер РОСТАБ

Производителем оборудования и программного обеспечения «РОСТАБ» является АО «Стандарт безопасности». Производство находится в России

Интегрированная система безопасности «РОСТАБ» хорошо зарекомендовала себя на многочисленных объектах и доказала свою актуальность и надежность

Контроллер РОСТАБ обеспечивает высокое быстродействие и исключительно широкие возможности по программированию встроенной логики

Компания АО «Стандарт безопасности» организовала серийное производство и сервис-центр, а также имеет все необходимые свидетельства, сертификаты и лицензии. Это гарантирует не только оперативную реализацию новых функций, необходимых заказчикам и поддержку уже установленных систем, но и обеспечение информационной безопасности



Контроллер РОСТАБ

Сетевые контроллеры серии РОСТАБ позволяют создавать системы контроля и управления доступом и охранной сигнализации с распределенной архитектурой, где каждый контроллер хранит параметры конфигурации, локальную базу данных карт, временных зон и уровней доступа.

Программирование, мониторинг и управление контроллерами осуществляется с использованием ПО:

- «РОСТАБ» - версия под ОС Windows
  или
- «РОСТАБ-А» - версия под ОС Linux, включенная в Реестр российского ПО

Все изменения в конфигурации контроллеров, выполненные с использованием ПО, динамически загружаются в контроллеры, не требуя принудительной загрузки данных конфигурации по команде оператора.

СТАНДАРТ БЕЗОПАСНОСТИ

Варианты корпусов для контроллера

Структура контроллера РОСТАБ

СТАНДАРТ БЕЗОПАСНОСТИ

Основной
модуль контроллера

Шина RS-485 с шифрованием данных AES (128 или 256 бит)

Подключение
четырех считывателей,
8+2 шлейфов, 4 реле

Подключение
четырех считывателей,
8+2 шлейфов, 6 реле

Подключение до 31 модуля
расширения на один основной
модуль контроллера

Основной модуль контроллера
C-PW-IC

СТАНДАРТ БЕЗОПАСНОСТИ

Основной модуль контроллера C-PW-IC поддерживает подключение до 4 считывателей карт для управления двумя подключенными дверями. Возможно расширение до 64 дверей с помощью модулей. C-PW-IC поддерживает подключение любых считывателей с интерфейсами Виганда, OSDP и Clock/Data.

Сетевые контроллеры серии РОСТАБ позволяют создавать системы контроля и управления доступом и охранной сигнализации с распределенной архитектурой, где каждый контроллер хранит параметры конфигурации, локальную базу данных карт, временных зон и уровней доступа. Контроллер принимает решения о разрешении или запрещении доступа для карты без необходимости обращения к серверу с ПО СКУД.

Система контроля доступа может быть построена с использованием только модулей C-PW-IC без расширителей, подключаемых по интерфейсу RS-485.

КЛЮЧЕВЫЕ ОСОБЕННОСТИ

- Память на 240000 карт
- Буфер на 50000 событий
- До 250 уровней доступа для каждой карты
- Протокол OSDP с шифрованием связи со считывателями
- Поддержка IPv4/v6 и DHCP
- Шифрование связи с сервером TLS или AES-256/128
- Создание и загрузка сертификатов TLS для взаимной аутентификации с сервером СКУД
- Шифрование связи с модулями расширения (AES)
- Контроль доступа к сети по протоколу 802.1X
- Поддержка форматов карт до 200 бит
- Управление лифтами, турникетами и картоприемниками
- Поддержка Anti-passback по зоне, считывателю и времени
- Программируемые команды пользователя с клавиатуры
- Поддержка работы с беспроводными замками

Модуль расширения считывателей C-PW-R2

СТАНДАРТ БЕЗОПАСНОСТИ

Модули для подключения считывателей позволяют расширить систему на базе основного модуля контроллера C-PW-IC.

C-PW-R2 поддерживает подключение до 4 считывателей с интерфейсами Виганда, OSDP и Clock/Data для управления двумя точками доступа.

Модуль имеет 2 порта для считывателей с интерфейсом Виганда или 4 порта для считывателей OSDP, 8 входов шлейфов, 6 реле, 2 входа для контроля питания и открывания корпуса.

Шлейфы сигнализации, используемые для подключения элементов СКУД, а также извещателей охранной сигнализации, имеют возможность программирования электрической схемы с оконечными резисторами или без них. Номиналы оконечных резисторов и допуски на сопротивление шлейфа программируются.

КЛЮЧЕВЫЕ ОСОБЕННОСТИ

- При подключении к основному модулю контроллера C-PW-R2 может связывать события выбранных устройств с другими устройствами в системе, выполняя действия и позволяя им происходить независимо от сервера с ПО СКУД.
- C-PW-R2 может локально обрабатывать запросы на доступ на основе проверки кода объекта (site code), даже если модуль отключен от основного модуля контроллера.
- Питание 10-14 В постоянного тока, ток до 650 мА
- Входы для контроля источника питания и открывания корпуса

Модуль расширения охранных шлейфов C-PW-IN

СТАНДАРТ БЕЗОПАСНОСТИ

Модули для подключения охранных шлейфов позволяют расширить систему на базе основного модуля контроллера C-PW-IC.

C-PW-IN поддерживает подключение 16 входов шлейфов общего назначения, 2 выхода реле и 2 входа для контроля питания и открывания корпуса.

Шлейфы сигнализации имеют возможность программирования электрической схемы с оконечными резисторами или без них. Номиналы оконечных резисторов и допуски на сопротивление шлейфа программируются.

Выходы реле имеют НЗК и НРК и являются свободно программируемыми с функцией контроля питания.

КЛЮЧЕВЫЕ ОСОБЕННОСТИ

- Команды на постановку и снятие шлейфов сигнализации с охраны могут быть инициированы оператором, запрограммированной логикой или событиями от внешних устройств.
- Широкие возможности по программированию схемы шлейфа сигнализации и номиналов оконечных резисторов.
- Различение до 4 состояний по каждому шлейфу.
- Два программируемых релейных выхода поддерживают команды «Вкл.», «Выкл.», «Импульс» и «Повторяющийся импульс» по различным событиям.
- Питание 10-14 В постоянного тока, ток до 250 мА
- Входы для контроля источника питания и открывания корпуса

Модуль расширения выходов реле
C-PW-OUT

СТАНДАРТ БЕЗОПАСНОСТИ

Модули выходов реле позволяют расширить систему на базе основного модуля контроллера C-PW-IC.

C-PW-OUT имеет на плате 16 выходов реле и 2 входа для контроля питания и открывания корпуса.

Модуль может быть сконфигурирован для управления различными внешними устройствами на объекте, такими как устройства освещения, обогрева, кондиционирования, управление дверьми и лифтами. Устройства могут быть активированы по командам от выбранных системных устройств, локально и без вмешательства сервера СКУД.

Выходы реле имеют НЗК и НРК и являются свободно программируемыми с функцией контроля питания.

КЛЮЧЕВЫЕ ОСОБЕННОСТИ

- Команды по управлению реле могут быть инициированы оператором, запрограммированной логикой или событиями от внешних устройств.
- Широкие возможности логики для управления различными устройствами.
- Релейные выходы поддерживают команды «Вкл.», «Выкл.», «Импульс» и «Повторяющийся импульс» по различным событиям.
- Каждое реле может коммутировать 2 А при 30 В пост. тока.
- Питание 10-14 В постоянного тока, ток до 390 мА
- Входы для контроля источника питания и открывания корпуса

Кибербезопасная инфраструктура

СЧИТЫВАТЕЛИ РОСТАБ ST-ID

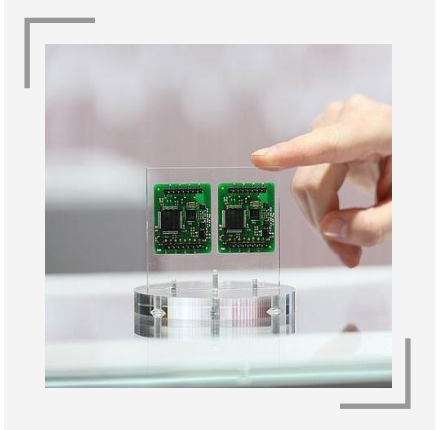
КИБЕРБЕЗОПАСНАЯ ЭКОСИСТЕМА

СТАНДАРТ БЕЗОПАСНОСТИ

ЗАЩИЩЕННЫЕ СЧИТЫВАТЕЛИ И ИДЕНТИФИКАТОРЫ

Считыватели карт MIFARE Plus EV1/EV2 и мобильных идентификаторов NFC и Bluetooth®

Считыватели для контроля автотранспорта и идентификаторы дальнего радиуса действия

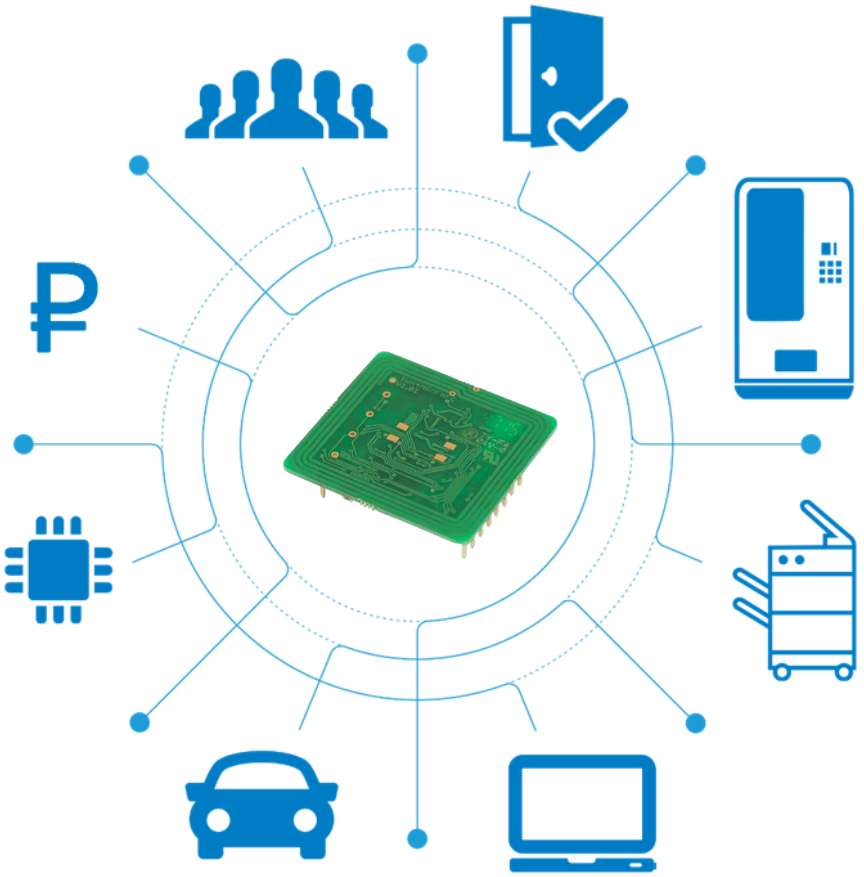


Встраиваемые модули считывателей для любых типов устройств

Решение для автоматизации процесса кодирования карт MIFARE

СЧИТЫВАТЕЛИ ДЛЯ РАЗЛИЧНЫХ ОБЛАСТЕЙ ПРИМЕНЕНИЯ

СТАНДАРТ БЕЗОПАСНОСТИ



- Физический контроль доступа
- Контроль рабочего времени
- Индивидуальный доступ к печати на принтере
- Контроль доступа к оборудованию в офисе и торговым терминалам
- Идентификация водителей
- Различные интерфейсы: USB, RS232, RS485, OSDP, Wiegand, эмуляция клавиатуры ПК

ОСОБЕННОСТИ СЧИТЫВАТЕЛЕЙ ST-ID

СТАНДАРТ БЕЗОПАСНОСТИ

СЧИТЫВАТЕЛИ ОБЕСПЕЧИВАЮТ ЗАЩИЩЕННУЮ ИДЕНТИФИКАЦИЮ ПОЛЬЗОВАТЕЛЕЙ И ВОЗМОЖНОСТЬ РАБОТЫ С УЖЕ ИСПОЛЬЗУЕМЫМИ НА ОБЪЕКТЕ КАРТАМИ ЗА СЧЕТ РАБОТЫ С РАЗЛИЧНЫМИ ТИПАМИ ИДЕНТИФИКАТОРОВ:

- Мобильные идентификаторы: виртуальные карты Bluetooth® и NFC
- MIFARE Ultralight® и Ultralight® C
- MIFARE® Classic и Classic EV1/EV2
- MIFARE Plus® (S/X) и MIFARE Plus® EV1
- MIFARE DESFire® 256, EV1, EV2 и EV3
- PicoPass® (считывание серийного номера)
- iCLASS™ (считывание серийного номера)

NXP MIFARE NFC Bluetooth

ВСТРОЕННЫЙ АКСЕЛЕРОМЕТР

- При выявлении попытки взлома считывателя выполняется автоматическое удаление ключей шифрования

СЧИТЫВАТЕЛИ ДЛЯ КОНТРОЛЯ АВТОТРАНСПОРТА

КОНТРОЛЬ АВТОТРАНСПОРТА

СТАНДАРТ БЕЗОПАСНОСТИ

- Считыватели дальнего радиуса действия для контроля доступа движущегося или неподвижного автотранспорта
- Дальность считывания пассивных RFID-меток до 13 м
- Настраиваемая дальность считывания
- Зашифрованный канал связи между RFID-меткой и считывателем
- Одновременная идентификация водителя и автомобиля за счет использования мобильного идентификатора (Bluetooth®) и RFID-метки дальнего действия
- Возможность использования одного и того же мобильного идентификатора на смартфоне для проезда на автомобиле и доступа через считыватели в здании
- Возможность идентификации посетителей только с использованием мобильного идентификатора

КОНТРОЛЬ АВТОТРАНСПОРТА

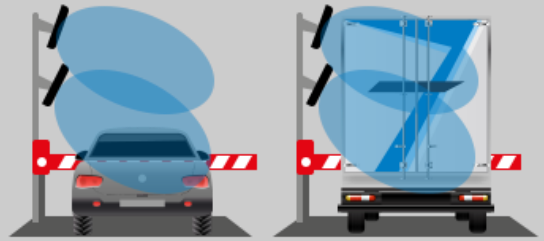
СТАНДАРТ БЕЗОПАСНОСТИ

ПОДКЛЮЧЕНИЕ ЧЕТЫРЕХ АНТЕНН К ОДНОМУ МОДУЛЮ СЧИТЫВАТЕЛЯ

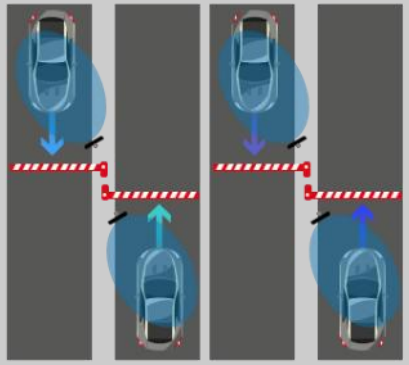
РАЗЛИЧНЫЕ КОНФИГУРАЦИИ

- Подключение внешних антенн к считывателю или использование интегрированной антенны
- Одновременный контроль одним считывателем нескольких въездов и выездов автотранспорта

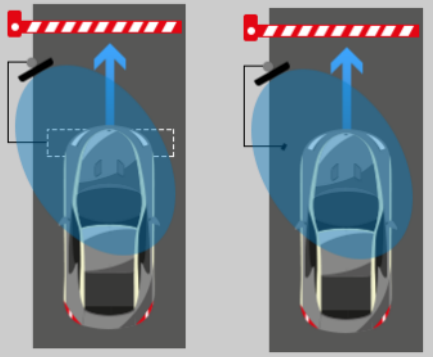
Одна полоса движения с идентификацией водителя и/или транспортного средства



Идентификация автотранспорта с различной высотой



Одновременный контроль до четырех полос движения



Совместная работа считывателя с датчиком присутствия автомобиля

КОНТРОЛЬ АВТОТРАНСПОРТА

СТАНДАРТ БЕЗОПАСНОСТИ

Внешний вид считывателя для контроля автотранспорта со встроенной антенной

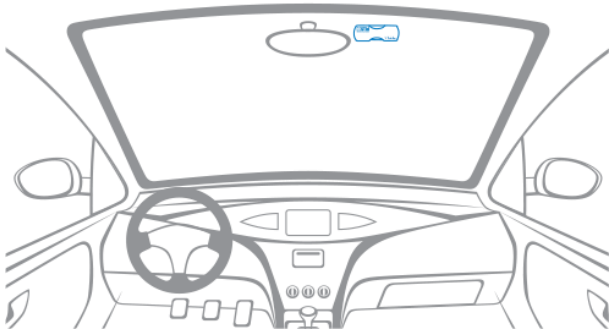
ИДЕНТИФИКАТОРЫ ДЛЯ АВТОТРАНСПОРТА

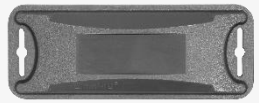
СТАНДАРТ БЕЗОПАСНОСТИ

ПАССИВНЫЕ RFID-МЕТКИ НЕ ТРЕБУЮТ ЗАМЕНЫ ИСТОЧНИКА ПИТАНИЯ

Несъемные разрушаемые RFID-метки для идентификации автомобиля

Съемные идентификаторы для установки на лобовое стекло





Метка для наружной установки на металлический корпус автомобиля

Карта или брелок большой дальности действия

АВТОМАТИЗАЦИЯ КОДИРОВАНИЯ КАРТ

СТАНДАРТ БЕЗОПАСНОСТИ

РЕШЕНИЕ ОТ КОМПАНИИ АО «СТАНДАРТ БЕЗОПАСНОСТИ» ПОЗВОЛЯЕТ АВТОМАТИЗИРОВАТЬ ПРОЦЕСС КОДИРОВАНИЯ КАРТ

- Ключи шифрования для программирования карт загружаются администратором системы в энергонезависимую память платы модуля кодирования и не могут быть извлечены. Это исключает несанкционированный доступ персонала бюро пропусков к ключам шифрования.
- Загрузка 100 карт в лоток (по умолчанию). Возможность установки лотка емкостью 200 карт (опционально)
- Перевод карт MIFARE Plus на уровень безопасности SL3
- Запись пользовательского ключа шифрования AES128 на карту MIFARE Plus
- Запись идентификатора пользователя в выбранный защищенный блок памяти
- Проверка записи идентификатора
- Отдельный лоток для карт, не прошедших тестирование
- Возможность импорта идентификаторов из файла
- Возможность печати изображения на карте
- Версии ПО для управления кодированием карт под ОС Windows и Linux

СТАНДАРТ БЕЗОПАСНОСТИ

VisionPass

Биометрические терминалы распознавания лиц

Биометрические терминалы в СКУД

Для многих современных организаций приоритетной задачей является не только предотвращение несанкционированного доступа посторонних лиц на контролируемый объект, но и слежение за перемещением своих сотрудников для учета рабочего времени, расследования инцидентов и т.п. В этой связи биометрические терминалы могут эффективно использоваться в качестве элемента системы контроля персонала

Ключевым преимуществом биометрических систем является их способность одновременно решать задачи как идентификации, так и аутентификации, позволяя проверять правомочность владения человеком предъявленным им идентификатором

В этом состоит их основное преимущество по сравнению с использованием карты или пароля, которые могут быть легко переданы другому лицу

Ключевые особенности терминалов VisionPass

Ультрасовременная оптическая система, сочетающая 2D, 3D и инфракрасные камеры с алгоритмом обработки стереоскопических изображений

Требуется менее одной секунды для распознавания лица из базы в 40000 пользователей

Пропускная способность 40 человек в минуту

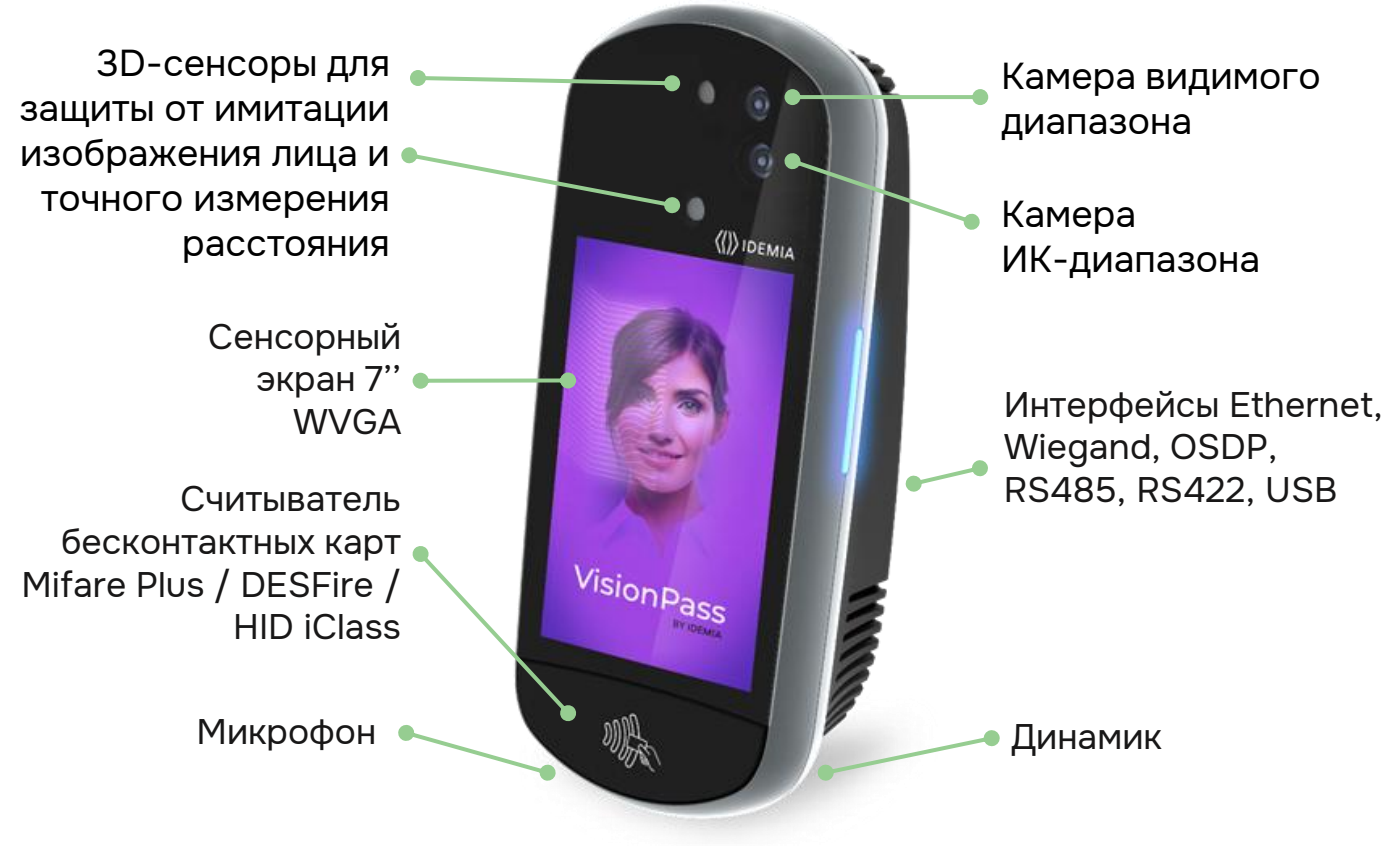
Для доступа необходимо приблизиться к терминалу на расстояние 70 см

Защита от использования муляжей и фотографий лиц, подтвержденная тестами международной лаборатории NIST

Возможность использования встроенного или внешнего считывателя карт для двухфакторной идентификации

Встроенный считыватель QR-кодов

Ключевые особенности терминалов VisionPass



Ключевые особенности терминалов VisionPass

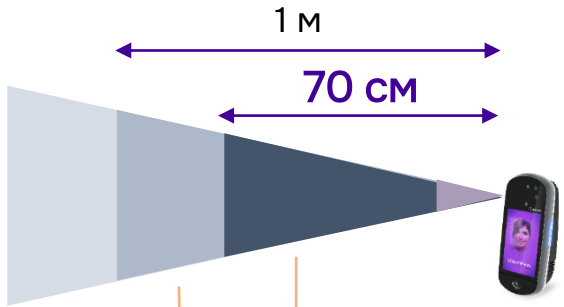
Считывание изображения лица во время прохода при естественном положении тела человека

✓ Подходит для людей любого роста, в т.ч. для лиц с ограниченными возможностями

Оптимальный угол обзора по горизонтали

✓ Надежное считывание лица человека, приближающегося сбоку или повернутого в сторону

Объемно-пространственный сканер обеспечивает оптимальную дальность считывания для исключения ложных срабатываний

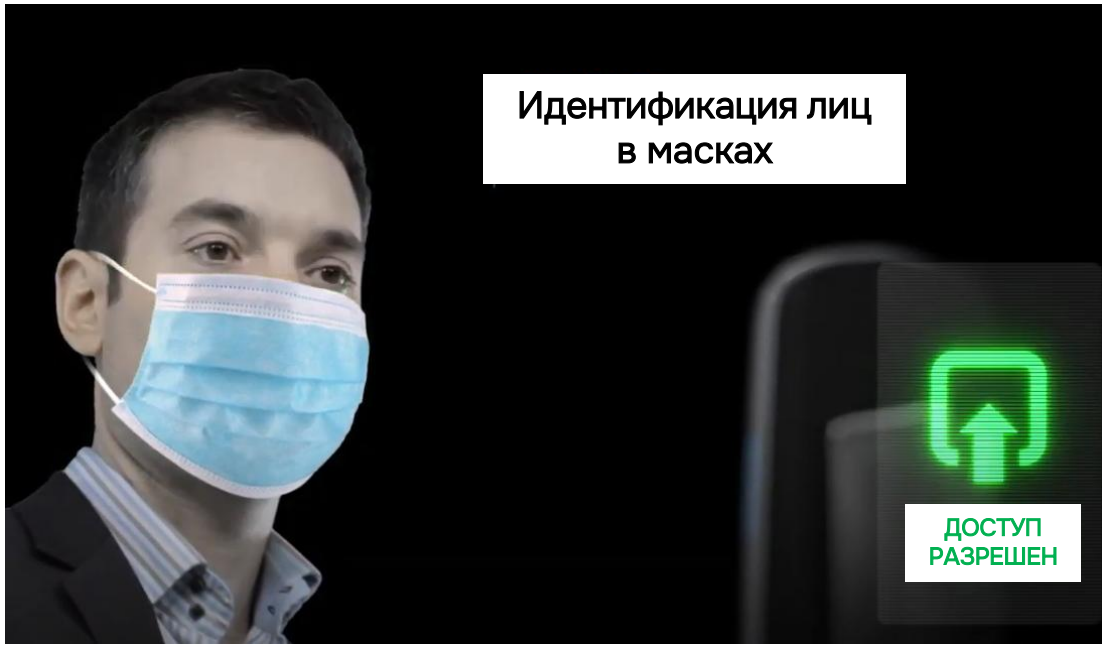


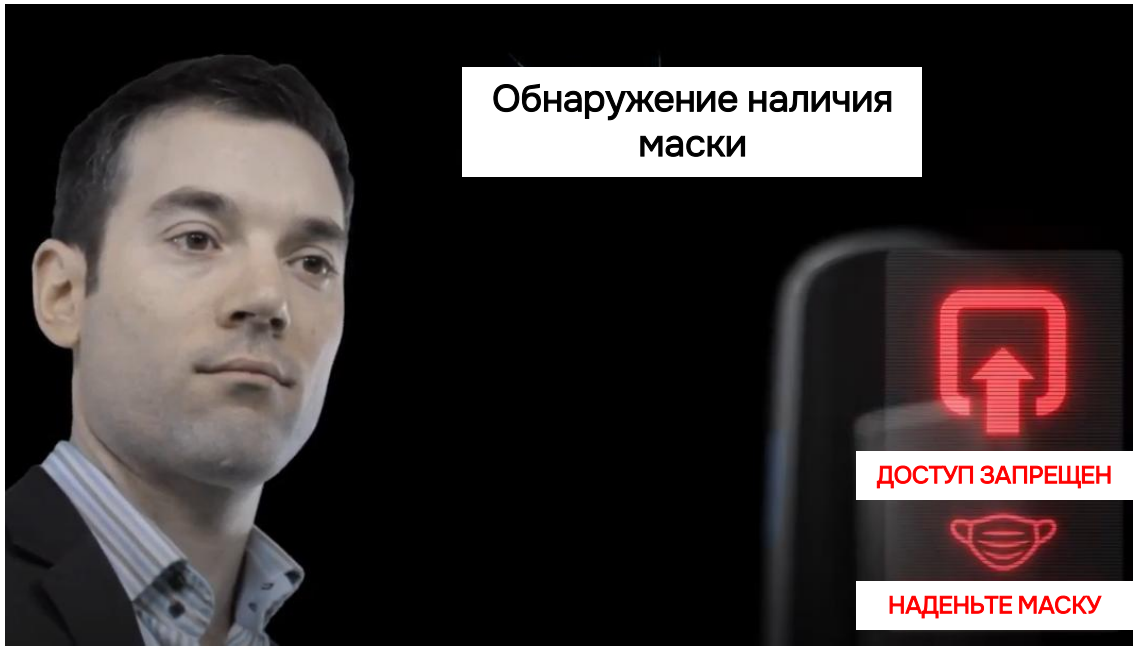
- Область идентификации
- Область запуска процесса распознавания
- Область начала отслеживания приближения

*Оптимальная высота установки терминала VisionPass - 115 см от пола

Надежная идентификация лиц в масках

- Терминалы VisionPass надежно идентифицируют людей, использующих медицинские маски и защитные очки
- Возможность контроля наличия маски
- Терминалы имеют возможность подключения внешнего тепловизора для бесконтактного измерения температуры и принятия решения о доступе на основании измеренной температуры

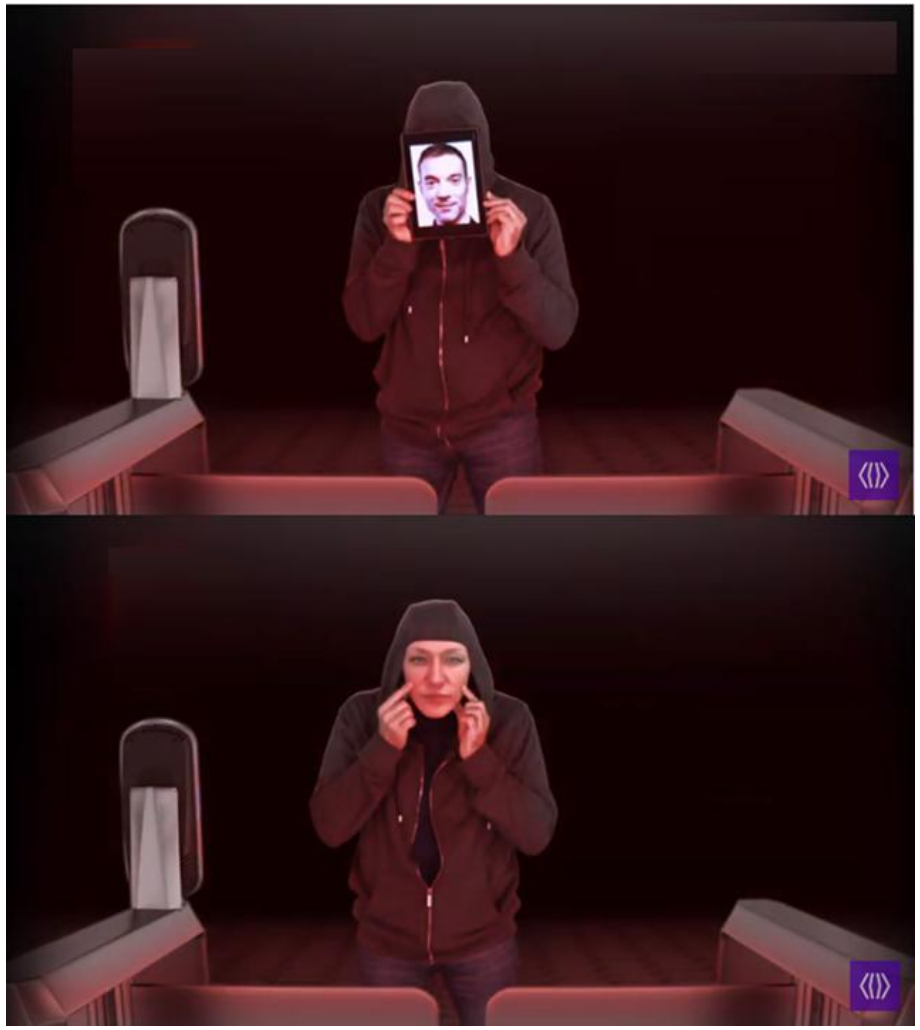




Защита от использования муляжей и фотографий лиц

Технология распознавания лиц, используемая в терминалах VisionPass, занимает первые места по точности по результатам тестов FRVT (Face Recognition Vendor Test). Для технологий распознавания лиц существует множество сравнительных испытаний, но общепринятым международным стандартом принято считать пакет специализированных тестов FRVT (Face Recognition Vendor Test), разработанный и периодически обновляемый Национальным институтом стандартов и технологий (NIST, National Institute of Standards and Technology). Разработчики тестов FRVT приложили значительные усилия для того, чтобы создать объективную методику тестирования и систему рейтингов, доступную для понимания пользователями. При этом методика тестирования совершенствуется на протяжении более 20 лет и сохраняет независимость экспертизы.

Тестирование алгоритмов распознавания лиц, проводимое NIST, является наиболее авторитетным на сегодняшний день «чемпионатом мира» среди данного класса систем. Среди участников данного "чемпионата" есть как крупные мировые корпорации, такие как Microsoft, Intel, Samsung, так и учебные заведения. Например, из России в тестировании NIST в 2023 г. участвовали решения от МГУ имени М.В. Ломоносова и университета ИТМО. В рейтинге NIST можно встретить как компании, специализирующиеся на видеоаналитике (например, российские VisionLabs и NtechLab), так и те организации, для которых это направление не является основным.



Защита от использования муляжей и фотографий лиц

В тест FRVT входит несколько оценочных тестов, однако с точки зрения практического использования технологии распознавания лиц наиболее известны сценарии Face Recognition Technology Evaluation (FRTE) **1:1 Verification** и **1:N Identification**. Первый из них (1:1 Verification) — это оценка качества верификации «1 к 1», когда алгоритм должен определить принадлежность двух предъявленных образцов данных одному человеку. Второй тип сценария (1:N Identification) — это тест на качество работы алгоритма идентификации при сравнении данных по принципу «1 к N» («один ко многим»), например, для распознавания лиц при проходе через точку доступа при сравнении с лицами из имеющейся базы данных.

Результаты испытаний показали исключительную производительность технологии распознавания лиц IDEMIA в сценариях «один ко многим» (1:N). IDEMIA имеет наилучшие показатели точности — 99,88% правильных совпадений из 12 миллионов изображений лиц.

Table 1 Summary of Test Results

	Test Species	Idemia VisionPass		
		PAs	IAPM	IAPMR
1.	2D photo on matte paper with edges cut	10 per subject	0 of 60	0%
2.	2D photo curved	10 per subject	0 of 60	0%
3.	2D mask with eyes cut out	10 per subject	0 of 60	0%
4.	3D Layered paper photo	10 per subject	0 of 60	0%
5.	Photo displayed on laptop	10 per subject	0 of 60	0%
6.	Video displayed on laptop	10 per subject	0 of 60	0%
Total per species			0 of 60	0%
Total for all species			0 of 360	0%

Table 1 Summary of Test Results

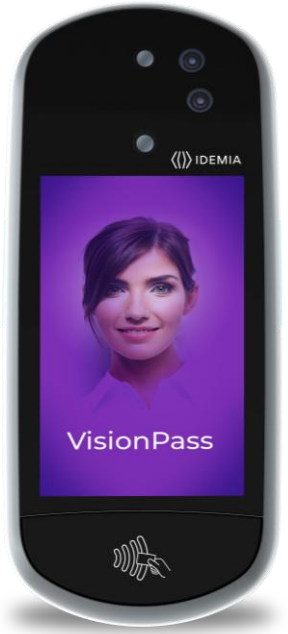
	Test Species	Idemia VisionPass		
		PAs	IAPM	IAPMR
1.	Curved paper mask	60	0 of 60	0%
2.	Latex Mask	50	0 of 50	0%
3.	CrazyTalk	60	0 of 60	0%
4.	Resin Mask	10	0 of 10	0%
5.	Transparent 2D	60	0 of 60	0%
6.	3D stacked paper photos	60	0 of 60	0%
Total for all species		300	0 of 300	0%

iBeta QUALITY ASSURANCE — TESTED — LEVEL 1 — ISO 30107-3 — Presentation Attack Detection — COMPLIANT

iBeta QUALITY ASSURANCE — TESTED — LEVEL 2 — ISO 30107-3 — Presentation Attack Detection — COMPLIANT

Технические характеристики терминала VisionPass

Размеры терминала	33 x 14 x 11 см
Экран	Сенсорный 7"
Объем базы данных	20000 пользователей, расширение до 100000 (1:N) Протокол на 1000000 событий
Расстояние распознавания человека	от 30 см до 1 м (настраиваемое)
Встроенный считыватель карт	MIFARE Classic, MIFARE Plus, DESFire 3DES, DESFire AES, SmartMX
Интерфейсы	Ethernet TCP/IP (TLS 1.2), Wi-Fi (опция) WPA2, OSDP V2, OSDP V2 Secure Channel, RS-485, Wiegand OUT (выход для подключения к контроллеру СКУД), Wiegand IN (вход для подключения к терминалу внешнего считывателя)
Встроенные входы/выходы	Три входа шлейфов сигнализации и три выхода для управления внешними устройствами
Питание	12-24 В постоянного тока (3 А при 12 В)
Диапазон рабочих температур	-10 ... +45˚С, возможность расширения температурного диапазона с помощью установки уличного кожуха
Степень защиты корпуса	IP65



Технические характеристики терминала VisionPass SP

Размеры терминала	10,2 x 21 x 3,5 см
Экран	Сенсорный 5"
Объем базы данных	10000 пользователей, расширение до 50000 (1:N) Протокол на 1000000 событий
Расстояние распознавания человека	от 30 см до 1 м (настраиваемое)
Встроенный считыватель карт	MIFARE Classic, MIFARE Plus, DESFire 3DES, DESFire AES, SmartMX
Интерфейсы	Ethernet TCP/IP (TLS 1.2), OSDP V2, OSDP V2 Secure Channel, RS-485, Wiegand OUT (выход для подключения к контроллеру СКУД), Wiegand IN (вход для подключения к терминалу внешнего считывателя)
Встроенные входы/выходы	Три входа шлейфов сигнализации и три выхода для управления внешними устройствами
Питание	12-24 В постоянного тока (2,5 А при 12 В) или PoE+
Диапазон рабочих температур	-10 ... +45˚С
Степень защиты корпуса	IP65

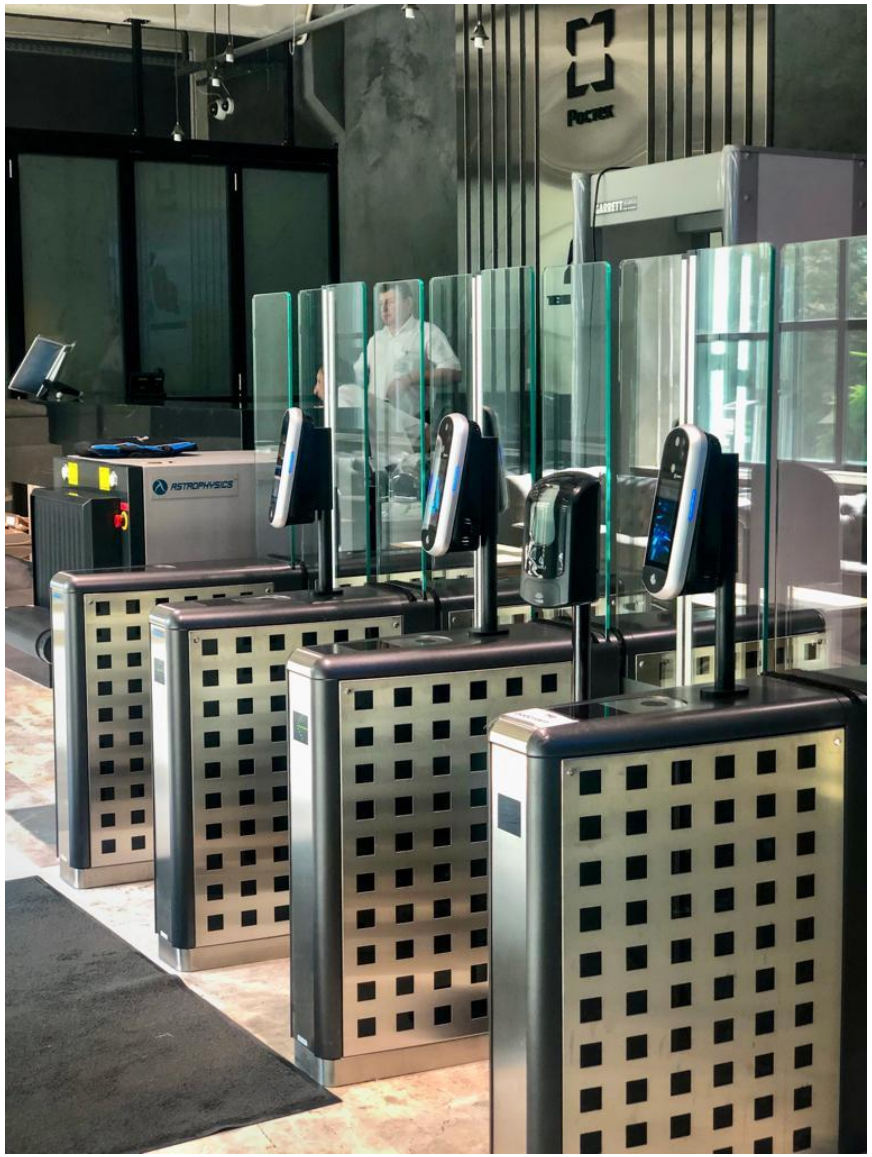
Можно ли использовать терминалы VisionPass в соответствии с Федеральным законом № 572-ФЗ?

- Наибольшее количество вопросов у пользователей биометрических систем возникает относительно применения принятого в 2022 г. ФЗ № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц <...>». Согласно этому закону, биометрические персональные данные для целей идентификации (или) аутентификации субъектов данных должны храниться в Единой биометрической системе (ЕБС).
- Важным моментом является то, что в ЕБС размещается и обрабатывается только два следующих вида биометрических данных:
  1. изображение лица человека, полученное с помощью фотовидеоустройств;
  2. запись голоса человека, полученная с помощью звукозаписывающих устройств.
- Ключевым фактором, из-за которого использование биометрических терминалов VisionPass нельзя относить к Закону № 572-ФЗ, является то, что в ЕБС для идентификации используются только фото- или видеоизображение лица человека в оптическом диапазоне и голос.
- Терминал VisionPass получает данные о пользователе и обрабатывает их, применяя технологию трехмерного сканирования. Он использует биометрические данные, отличающиеся от приведенного в Законе № 572-ФЗ варианте плоского изображения – фотографии. VisionPass для идентификации и аутентификации использует сенсор глубины (объемно-пространственный сканер) и изображение в инфракрасном диапазоне. Модуль из камер и сенсоров строит и распознает не плоский портрет человека, а его объемную модель. Таким образом, VisionPass использует другой физический принцип получения биометрии, не имеющий отношения к указанному в Законе.
- Использование принципов биометрической идентификации, основанных на считывании радужной оболочки глаза, отпечатков пальцев, рельефа лица или термографии лица/рук не запрещены законодательством РФ, если соблюдаются правила работы с биометрией и Закон № 152-ФЗ ("О персональных данных"). Кроме того, биометрические терминалы VisionPass не хранят и не используют для распознавания фотографию пользователя. Используемые шаблоны не позволяют восстановить изображение, полученное при занесении образа пользователя в систему.

Можно ли использовать терминалы VisionPass в соответствии с Федеральным законом № 572-ФЗ?

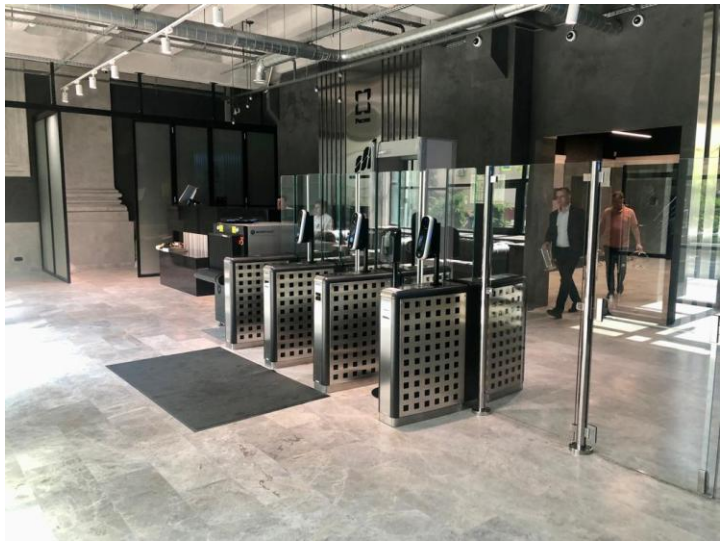
- Биометрические терминалы VisionPass поддерживают режим аутентификации, при котором шаблон пользователя хранится на бесконтактной смарт-карте
- Для идентификации пользователь предъявляет карту, терминал считывает с нее данные биометрического шаблона, а затем выполняется сканирование лица. Терминал выполняет сравнение предъявленного лица с его «эталонными» данными (полученными с карты), и принимает решение о правомочности владения пользователем картой. В случае успешной проверки на контроллер СКУД пересылается идентификатор пользователя.
- Безопасность такого решения обеспечивается шифрованием данных, хранящихся на карте, и передаваемых между картой и считывателем. Такой способ имеет три основных преимущества:
    1. снимается ограничение на максимальное количество пользователей в системе, поскольку вся информация о шаблонах хранится на картах пользователей
    2. при работе нескольких биометрических терминалов в системе исключается необходимость в организации канала связи между терминалами (Ethernet) для пересылки и синхронизации базы данных шаблонов
    3. биометрические данные или шаблоны пользователей не хранятся ни в каком виде в биометрических терминалах или на сервере

Примеры внедрения в РФ



Примеры внедрения в РФ

- холдинг «Технодинамика», Москва
- ПК «Салют» АО «ОДК», Москва
- ПО «Туламашзавод», г. Тула
- ПАО «ОДК-УМПО» г. Уфа
- аэропорты в г. Калуга и г. Нижневартовск



- Подробное описание примеров внедрения – на сайте www.secst.ru

СТАНДАРТ БЕЗОПАСНОСТИ

Благодарим за внимание!

Центральный офис и сервисный центр:

105568, Москва,
ул. Чечулина, д. 11, к. 1
тел.: +7 (495) 223-33-32
факс: +7 (495) 232-44-39

Офис в Санкт-Петербурге

196084, Санкт-Петербург,
Московский проспект, д. 79 А
тел.: +7 (812) 388-72-34
факс: +7 (812) 369-22-77

Офис и центр разработок в Ярославле

150047, г. Ярославль,
ул. Белинского, д. 16В
тел.: +7 (4852) 587-300

www.secst.ru
info@secst.ru