

# КОМПЛЕКСНАЯ ИНТЕГРИРОВАННАЯ СИСТЕМА БЕЗОПАСНОСТИ НА БАЗЕ ОБОРУДОВАНИЯ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ **РОСТАБ®**

ЕДИНЫЕ ТЕХНИЧЕСКИЕ РЕШЕНИЯ АО «СТАНДАРТ БЕЗОПАСНОСТИ»

# Предлагаемое АО «Стандарт безопасности» техническое решение позволит:



- Создать единую и масштабируемую интегрированную систему безопасности на объектах предприятия
- 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 внедряемое оборудование и ПО на объектах предприятия
- Интегрировать системы контроля доступом, видеонаблюдения и охранной сигнализации
- Внедрить на предприятии единый формат карт доступа российского производства с надежной защитой от клонирования



# Что такое РОСТАБ®?

**РОСТАБ** – оборудование и программное обеспечение для мониторинга и управления системами безопасности

- Полнофункциональное решение в части СКУД, охранной сигнализации, IP-видеонаблюдения и контроля персонала
- Отличная визуализация событий от различных подсистем безопасности на графических планах
- Поддержка кластера высокой доступности и многосерверной архитектуры
- Поддержка электронных систем хранения ключей, беспроводных замков и систем учета посетителей
- Видеоаналитика с генеративным ИИ
- Поддержка биометрических терминалов распознавания лиц
- Поддержка веб-интерфейса для рабочих станций операторов



# Ключевые особенности программного обеспечения РОСТАБ-А



- Поддержка контроллеров СКУД и охранной сигнализации 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 виде виртуальной машины
- СУБД – PostgreSQL или Jatoba (Газинформсервис)
- 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
- Шифрование каналов связи с контроллерами, модулями расширения и считывателями СКУД (TLS 1.3)
- «Горячее» резервирование серверов СКУД с автоматическим переключением на резервный сервер без необходимости приобретения дополнительного ПО
- Поддержка работы с биометрическими терминалами VisionPass и MorphoWave

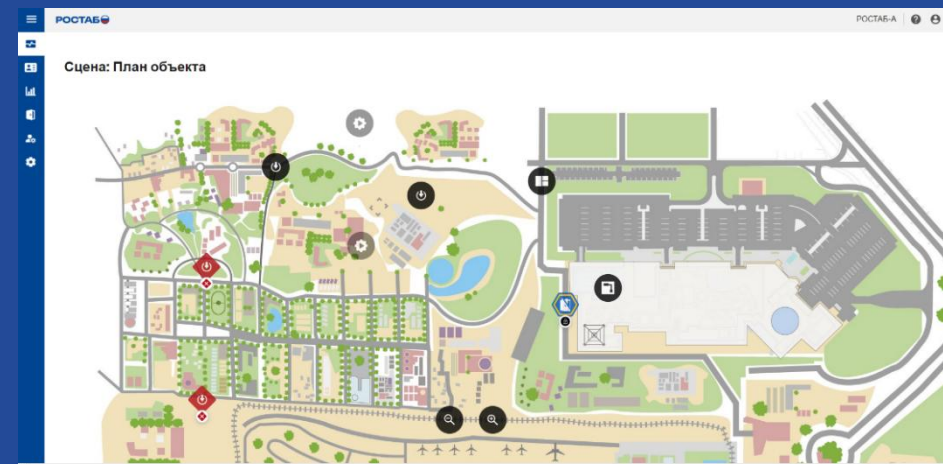
# Программное обеспечение РОСТАБ-А



## «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 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
- управление биометрическими терминалами, не подпадающими под требования Закона №572-ФЗ

The screenshot displays the user management interface for Ivanov, Ivan, Ivanovich. The interface includes a sidebar with navigation options like 'Личности' (Persons) and 'Профили' (Profiles). The main content area shows the user's profile with a photo and various fields for personal information, including name, surname, date of birth, and contact details. There are also checkboxes for roles and permissions.

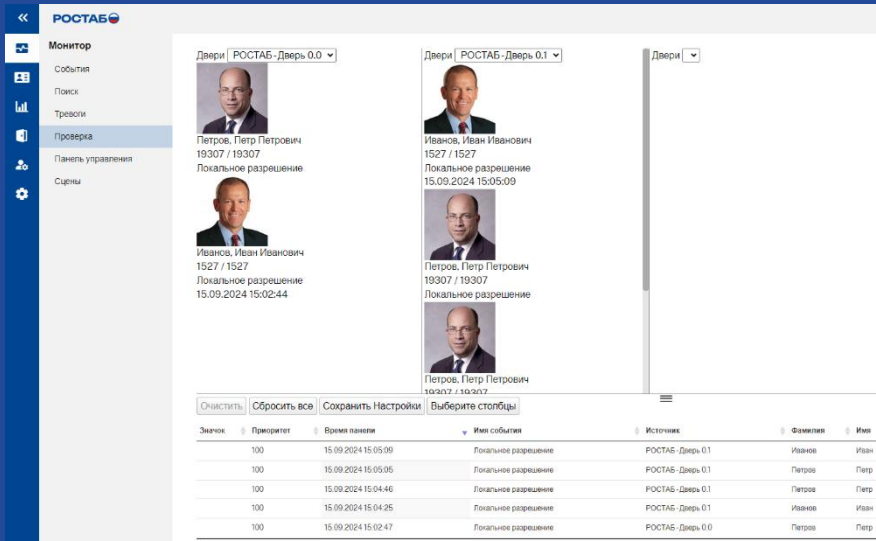
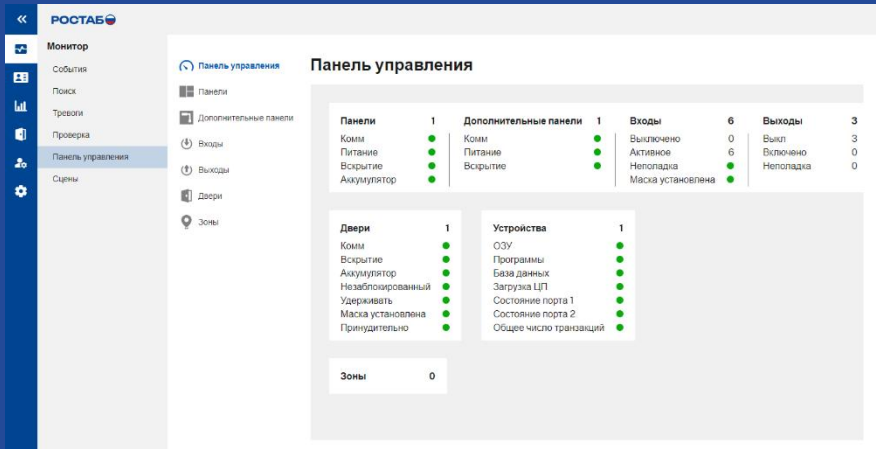


# Программное обеспечение РОСТАБ-А



ПО «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.

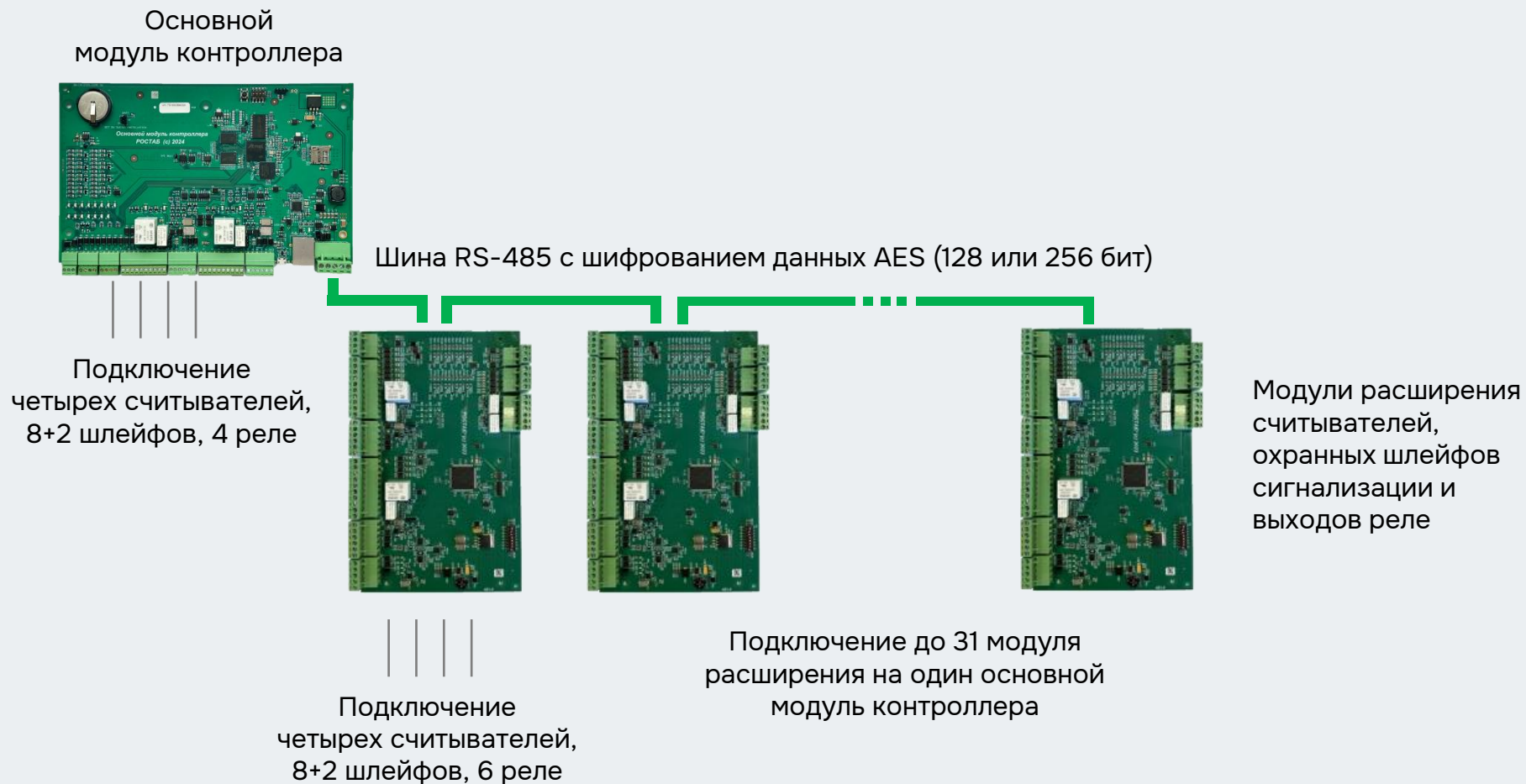
Программирование, мониторинг и управление контроллерами осуществляется с использованием ПО «РОСТАБ-А»

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



Варианты корпусов для контроллера

# Структура контроллера РОСТАБ



# Основной модуль контроллера

## C-PW-IC



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



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



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



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.

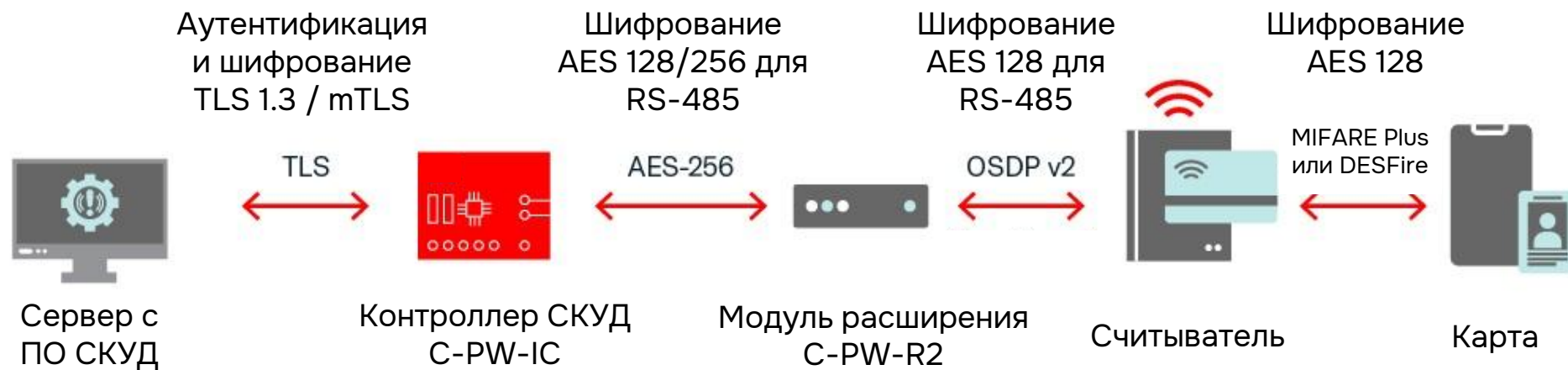
Модуль может быть сконфигурирован для управления различными внешними устройствами на объекте, такими как устройства освещения, обогрева, кондиционирования, управление дверьми и лифтами. Устройства могут быть активированы по командам от выбранных системных устройств, локально и без вмешательства сервера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



Реализовано шифрование данных между всеми элементами системы контроля и управления доступом

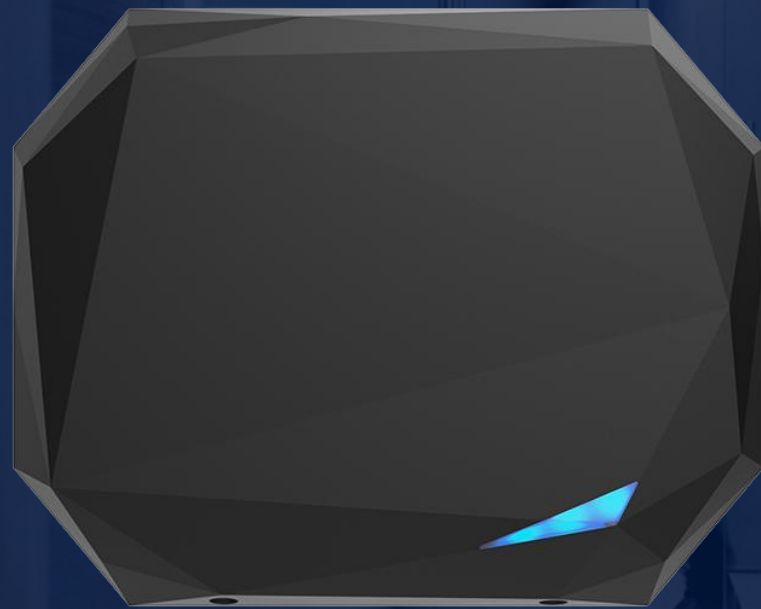
# Кибербезопасная инфраструктура



В контроллерах РОСТАБ реализованы функции для противодействия угрозам информационной безопасности:

- Шифрование связи между сервером СКУД и контроллером (AES 128/256) или TLS 1.3.
- Взаимная TLS-аутентификация контроллера и сервера с ПО СКУД для установления доверенного соединения с помощью сертификатов X.509. Реализована возможность создания сертификатов X.509 непосредственно в веб-интерфейсе контроллера РОСТАБ. Возможна также загрузка в контроллер цепочки сертификатов X.509 в формате PEM.
- Данные в контроллере зашифрованы, в т.ч. в выключенном состоянии: реализуется концепция «data encryption at rest». Шифрование позволяет хранить данные конфигурации в зашифрованном контейнере в памяти контроллера СКУД, при этом эти данные недоступны для чтения и не могут быть расшифрованы за разумное время, если не используются правильная процедура доступа к ним внутри контроллера СКУД.
- Шифрование связи между контроллером и подключенными к нему модулями расширения по интерфейсу RS-485 (AES 128/256).
- Для связи между модулями расширения и считывателями используется интерфейс OSDP v2. Данные, передаваемые по OSDP защищены с помощью симметричного ключа шифрования. В отличие от интерфейса Виганда, интерфейс OSDP обеспечивает криптографическую защиту данных.
- Поддержка стандарта 802.1x для аутентификации и авторизации в сети передачи данных.
- Используется протокол HTTPS для доступа к веб-интерфейсу контроллера для его первоначальной конфигурации: задания сетевой конфигурации и определения параметров связи с сервером.
- Соответствие программно-аппаратного комплекса РОСТАБ актуальным требованиям по кибербезопасности подтверждено независимым тестированием защищенности в специализированной компании по управлению цифровыми рисками ООО «БИЗон» (BI.ZONE).

# СЧИТЫВАТЕЛИ РОСТАБ ST-ID



# КИБЕРБЕЗОПАСНАЯ ЭКОСИСТЕМА



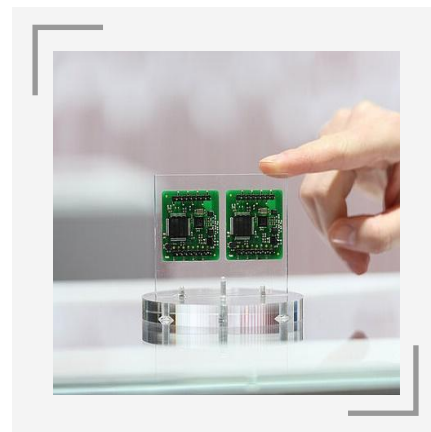
## ЗАЩИЩЕННЫЕ СЧИТЫВАТЕЛИ И ИДЕНТИФИКАТОРЫ



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



Считыватели для контроля автотранспорта и идентификаторы дальнего радиуса действия

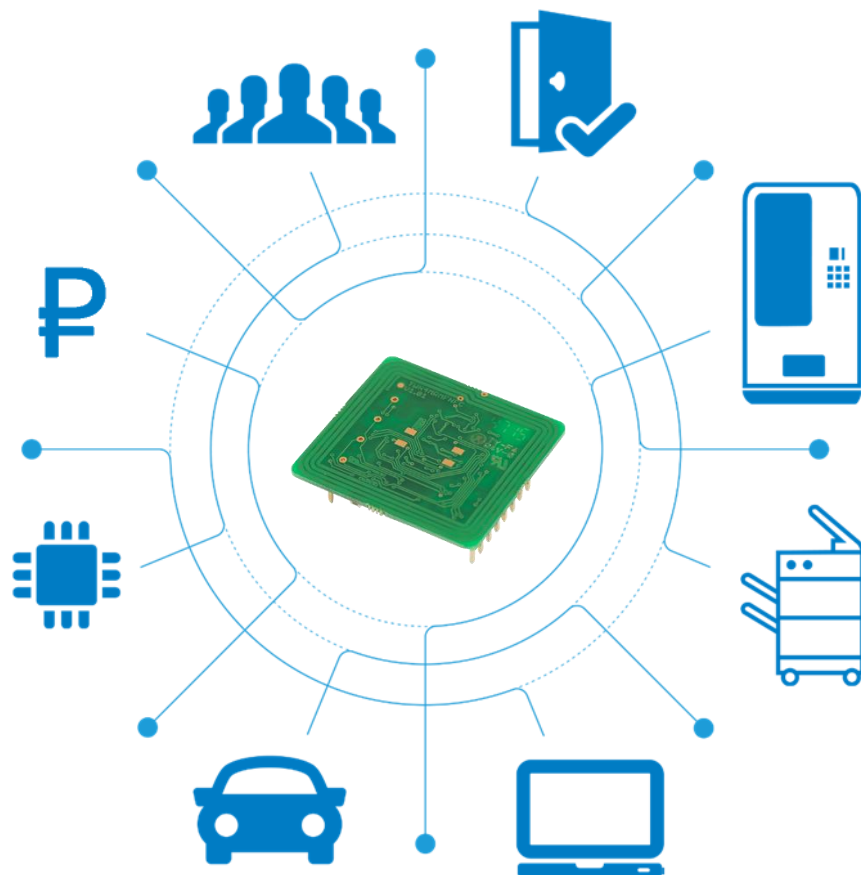


Встраиваемые модули считывателей для любых типов устройств



Решение для автоматизации процесса кодирования карт MIFARE

# СЧИТЫВАТЕЛИ ДЛЯ РАЗЛИЧНЫХ ОБЛАСТЕЙ ПРИМЕНЕНИЯ



- 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



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

- 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)



## ВСТРОЕННЫЙ АКСЕЛЕРОМЕТР

- При выявлении попытки взлома считывателя выполняется автоматическое удаление ключей шифрования



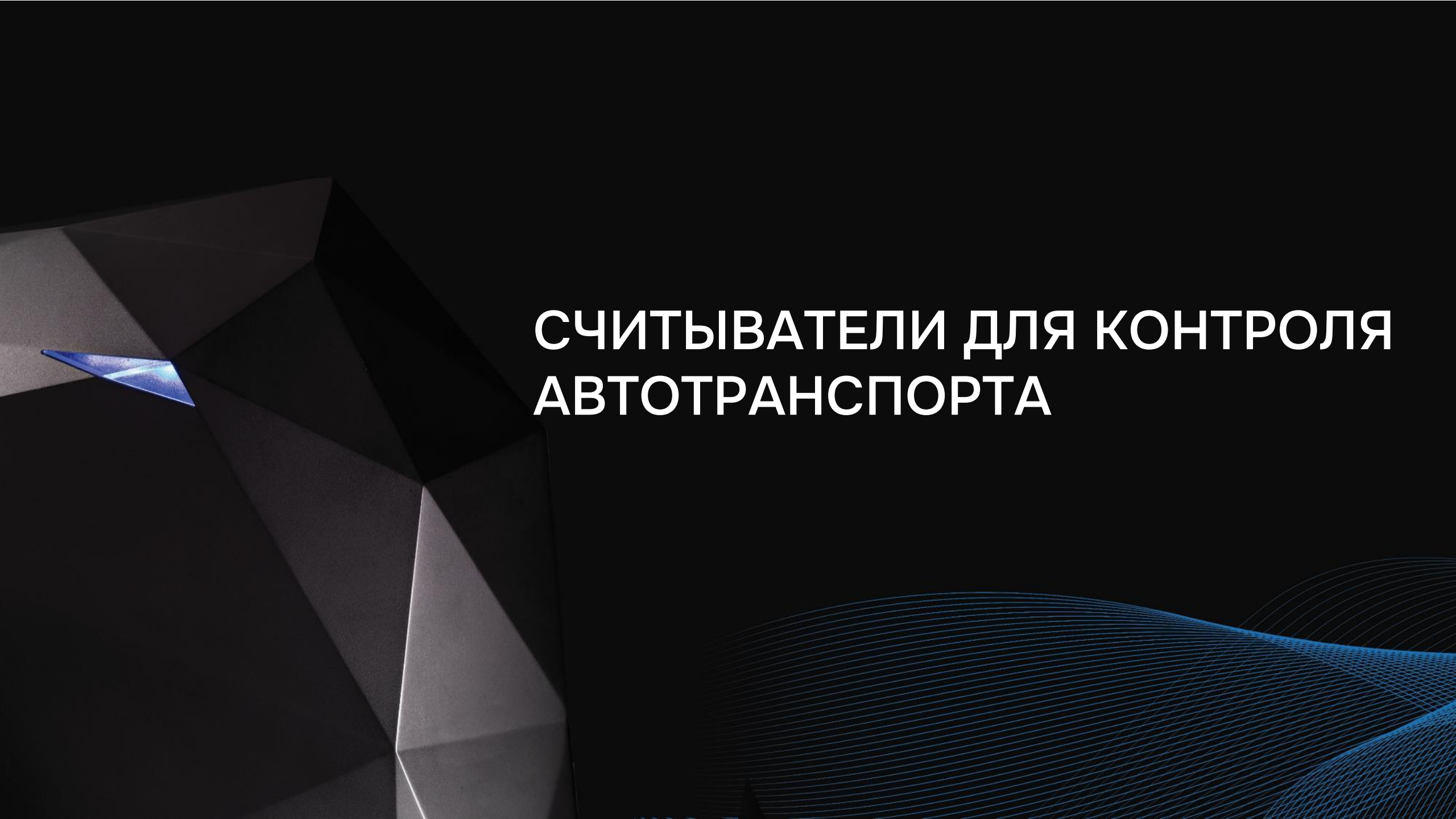
# СЧИТЫВАТЕЛИ ST-ID С КЛАВИАТУРОЙ



## ВЕРСИИ СЧИТЫВАТЕЛЯ С КНОПОЧНОЙ КЛАВИАТУРОЙ ИЛИ СЕНСОРНЫМ ЭКРАНОМ

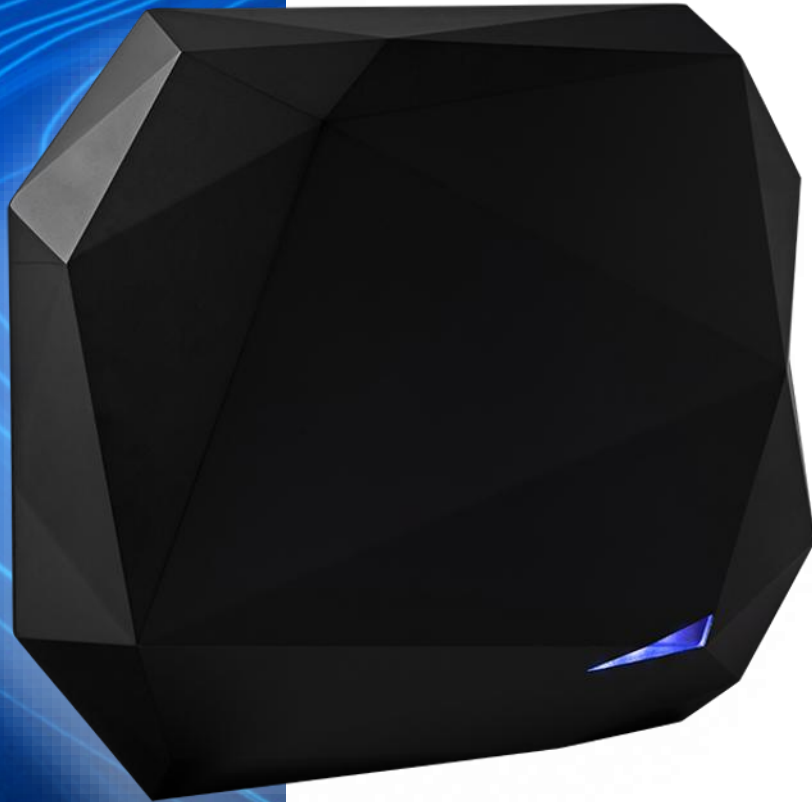
- Полностью конфигурируемые интерфейсы Виганда и OSDP
- Возможность выбора цвета корпуса
- Размеры корпуса 107 x 81 x 26 мм
- Возможность использования клавиатуры для функций контроля доступа и/или управления системой охранной сигнализации
- Версия считывателя с сенсорным экраном позволяет случайным образом изменять расположение клавиш для уменьшения вероятности подбора кода злоумышленником
- Сенсорный экран позволяет отображать настраиваемую пользователем информацию: виртуальные кнопки для управления системой охранной сигнализации и внешними устройствами, логотип компании и т.п.





# СЧИТЫВАТЕЛИ ДЛЯ КОНТРОЛЯ АВТОТРАНСПОРТА

# КОНТРОЛЬ АВТОТРАНСПОРТА



- ✚ 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



✚ 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



Внешний вид считывателя для контроля автотранспорта со встроенной антенной

# ИДЕНТИФИКАТОРЫ ДЛЯ АВТОТРАНСПОРТА



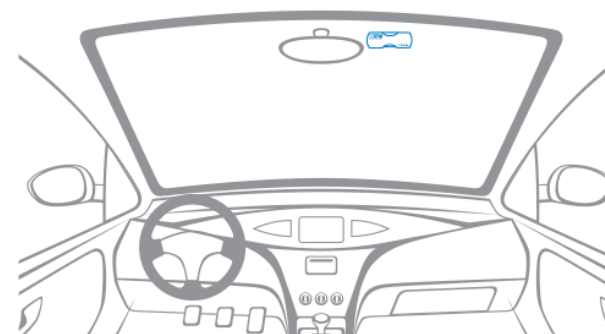
ПАССИВНЫЕ RFID-МЕТКИ НЕ ТРЕБУЮТ ЗАМЕНЫ ИСТОЧНИКА ПИТАНИЯ



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



## 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 или MIFARE DESFire
- 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

# БЕСКОНТАКТНЫЕ БИОМЕТРИЧЕСКИЕ СЧИТЫВАТЕЛИ ОТПЕЧАТКОВ ПАЛЬЦЕВ **MORPHOWAVE**



# Использование биометрических считывателей 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



# Бесконтактное считывание отпечатков пальцев в СКУД



MorphoWave является полностью бесконтактным считывателем, обеспечивающим надежную идентификацию и/или аутентификацию пользователей по изображениям четырех пальцев одной руки. Для идентификации достаточно провести рукой через считыватель. Считывание происходит «на лету». Это обеспечивает высокую скорость прохода и удобство для пользователей.

В отличие от контактных считывателей отпечатков пальцев MorphoWave позволяет полностью исключить проблемы, связанные с загрязнением контактного сенсора и эффективно распознавать сухие и влажные пальцы.

Система биометрической идентификации не подпадает под требования Федерального закона № 572-ФЗ и не требует подключения к ЕБС/КБС и защиты каналов связи.



# Ключевые особенности считывателей MorphoWave



Требуется менее одной секунды для распознавания пользователя из базы в 10000 пользователей

Пропускная способность 40 человек в минуту

Память на 10000 пользователей (2 руки для каждого) для работы в режиме идентификации (1:N)

Память на 250000 пользователей (2 руки для каждого) для работы в режиме аутентификации с использованием карты или QR-кода (1:1)

Возможность использования встроенного или внешнего считывателя карт для двухфакторной идентификации

Защита от использования муляжей, подтвержденная тестами международной лаборатории NIST

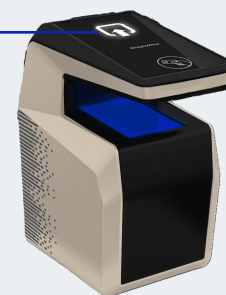
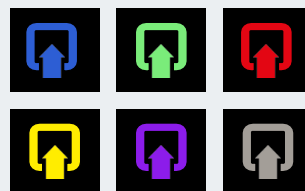
Встроенный считыватель QR-кодов



# Ключевые преимущества MorphoWave



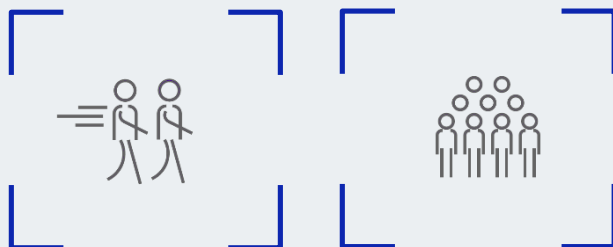
Для считывания четырех пальцев и идентификации требуется менее 1 с



Удобная индикация при проходе



Работа в режиме идентификации или аутентификации (карта или QR-код)



Проход до 60 пользователей в минуту  
Память до 100000 пользователей (1:N)



Нет физического контакта со считывателем



Возможность хранения биометрических шаблонов на картах MIFARE DESFire

# Различные варианты установки и подключения MorphoWave



Биометрический считыватель MorphoWave может быть установлен на стене, встроен в турникет или закреплен на отдельно стоящей колонне

Компактный корпус – размеры 250 x 152 x 216 мм

Степень защиты IP65

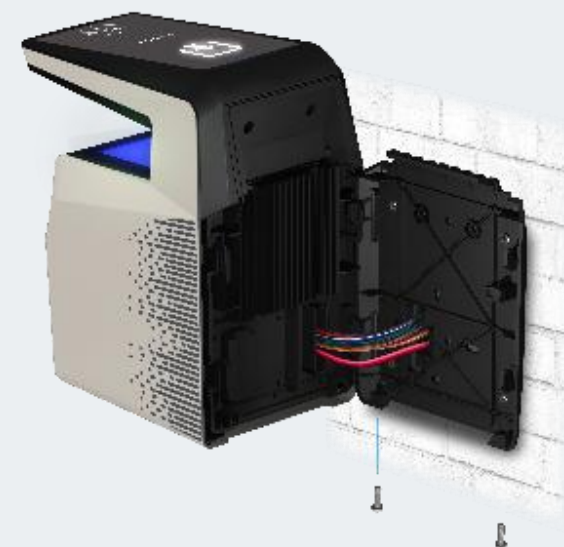
Интерфейсы Виганда (вход и выход с программируемым числом и размещением бит), OSDP v2, Ethernet, RS-485/422

Питание 12-24 В пост. тока (2,5 А) или PoE+

Встроенный выход реле, 3 входа шлейфов сигнализации и 3 выхода (GPIO)



# Различные варианты установки и подключения MorphoWave



# Технические характеристики MorphoWave

|                             |                                                                                                                                                                                                                                                                                                        |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Размеры терминала           | 250 x 152 x 216 мм                                                                                                                                                                                                                                                                                     |
| Экран                       | Светодиодный (SP) или сенсорный 4,3" WVGA (XP)                                                                                                                                                                                                                                                         |
| Объем базы данных           | <b>Версия MorphoWave SP:</b><br>10000 пользователей в режиме 1:N<br>250000 пользователей в режиме 1:1<br>Протокол на 1000000 событий<br><br><b>Версия MorphoWave XP:</b><br>40000 пользователей, расширение до 100000 в режиме 1:N<br>250000 пользователей в режиме 1:1<br>Протокол на 1000000 событий |
| Встроенный считыватель      | MIFARE Classic, MIFARE Plus, DESFire 3DES, DESFire AES                                                                                                                                                                                                                                                 |
| 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, выход реле                                                                                                                                                                                                           |
| Питание                     | 12-24 В постоянного тока (2,5 А при 12 В) или PoE+                                                                                                                                                                                                                                                     |
| Диапазон рабочих температур | -10 ... +55°C, IP65                                                                                                                                                                                                                                                                                    |



# Примеры внедрения MorphoWave





СТАНДАРТ  
БЕЗОПАСНОСТИ

# БИОМЕТРИЧЕСКИЕ ТЕРМИНАЛЫ РАСПОЗНАВАНИЯ ЛИЦ **VISIONPASS**

# 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

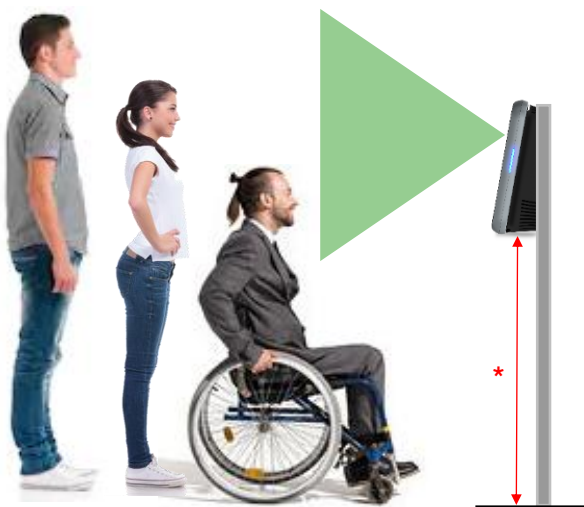


# Ключевые особенности терминалов VisionPass



# Ключевые особенности терминалов VisionPass

Считывание изображения лица во время прохода при естественном положении тела человека



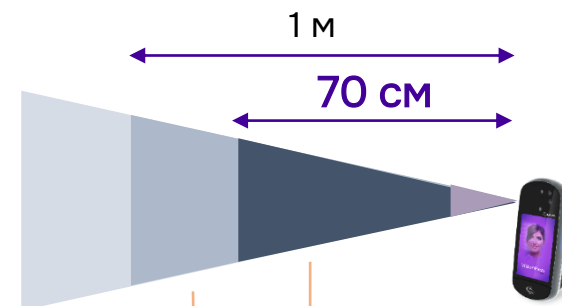
- ✓ Подходит для людей любого роста, в т.ч. для лиц с ограниченными возможностями

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

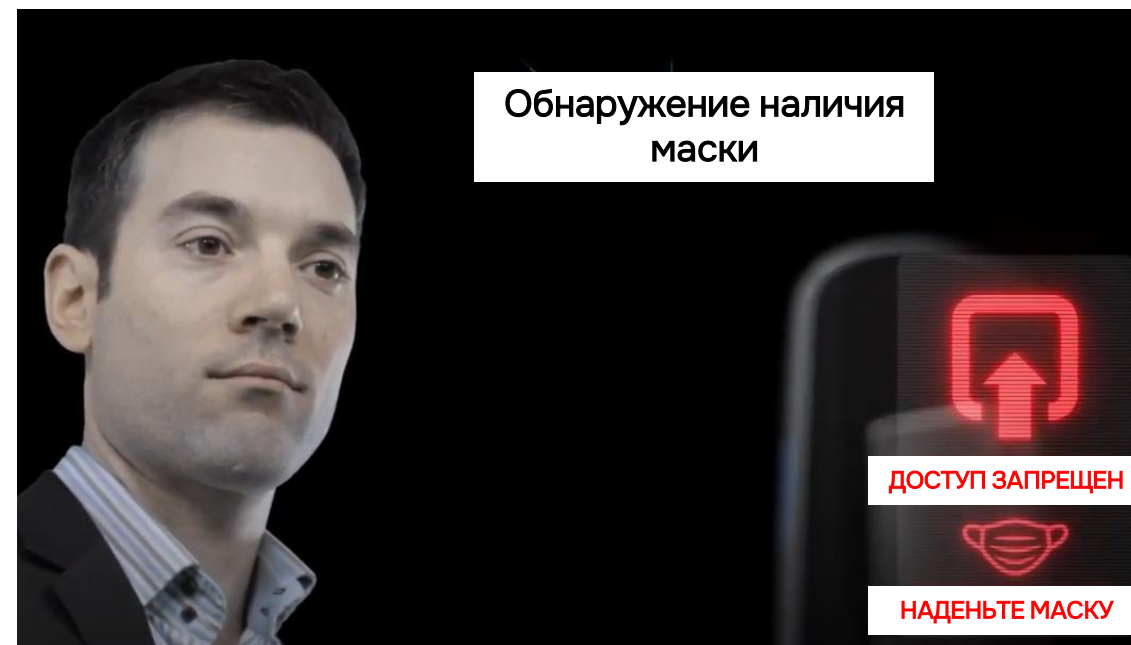
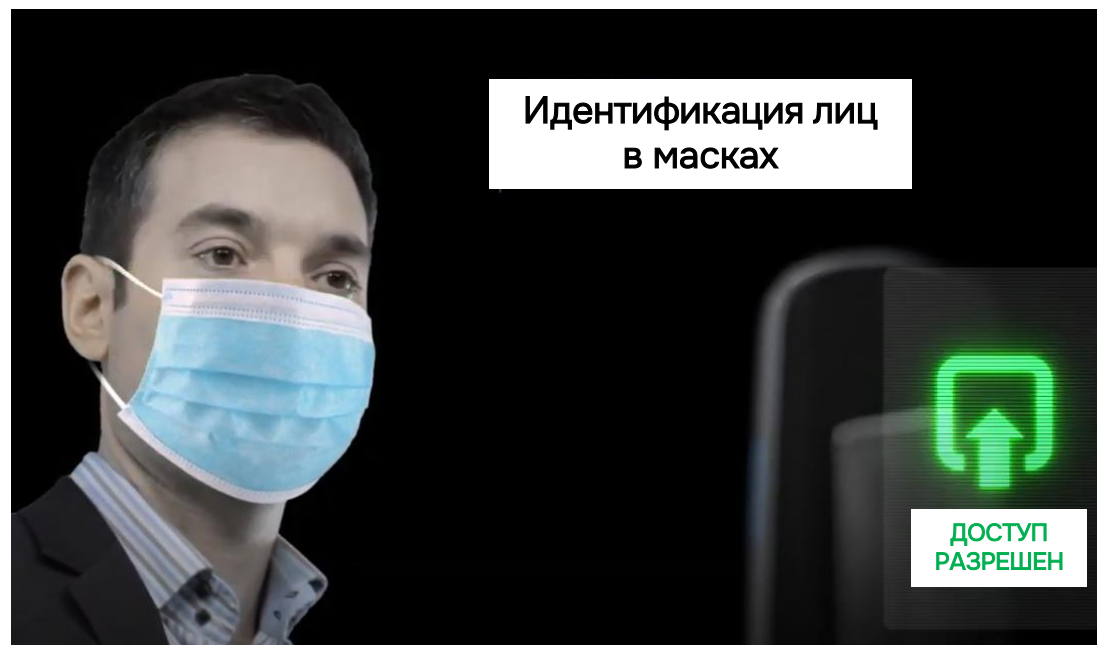


- Область идентификации
- Область запуска процесса распознавания
- Область начала отслеживания приближения

\*Оптимальная высота установки терминала VisionPass - 115 см от пола

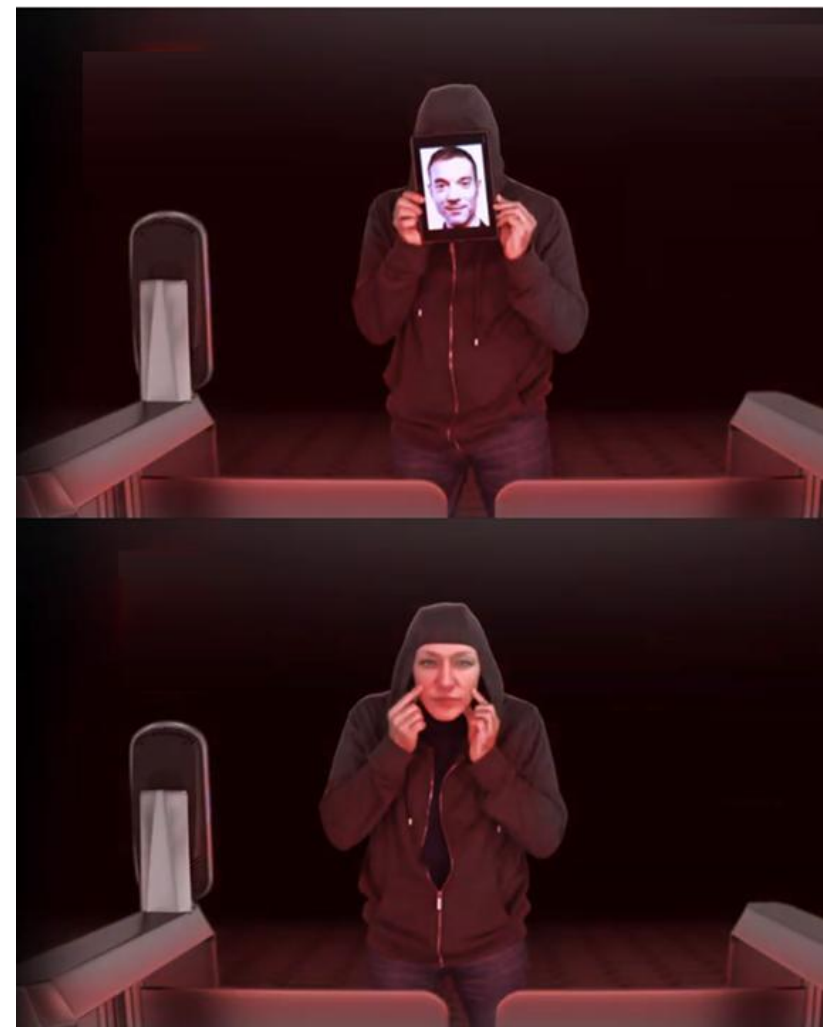
# Надежная идентификация лиц в масках

- 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, разработанный и периодически обновляемый Национальным институтом стандартов и технологий (NIST). Разработчики тестов 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.



# Защита от использования муляжей и фотографий лиц

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.

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 VisionPass в сценариях «один ко многим» (1:N). VisionPass имеет наилучшие показатели точности – 99,88% правильных совпадений из 12 миллионов изображений лиц.



# 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)<br>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°C, возможность расширения температурного диапазона с помощью установки уличного кожуха                                                                                                                 |
| 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?

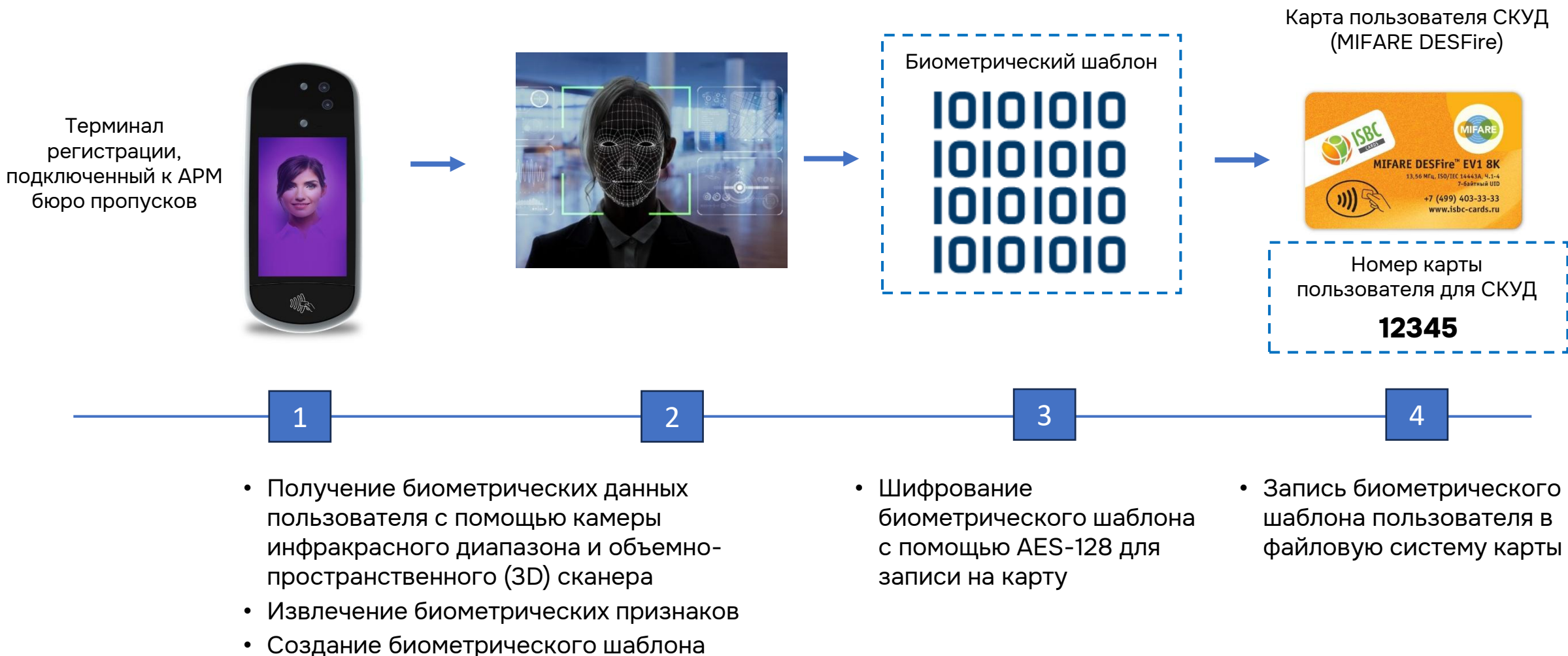
Биометрические терминалы VisionPass поддерживают режим аутентификации, при котором шаблон пользователя хранится на бесконтактной смарт-карте. Вот, что происходит в VisionPass при хранении биометрических шаблонов пользователей на картах:

1. Биометрический шаблон пользователя хранится на бесконтактной смарт-карте, принадлежащей этому пользователю. На карте нет ФИО пользователя или каких-либо данных, позволяющих осуществить установление сведений о лице или такого лица. Вместе с биометрическим шаблоном пользователя хранится только некоторый порядковый номер карты (ID).
2. Пользователь предъявляет карту встроенному в терминал считывателю, терминал считывает (загружает) с нее данные биометрического шаблона и номер карты (ID) в свою память. Безопасность хранения биометрического шаблона обеспечивается шифрованием данных AES-128, хранящихся на бесконтактной смарт-карте (российского производства). Доступ к биометрическому шаблону на карте невозможен без знания ключа шифрования.
3. Выполняется сравнение предъявленных биометрических признаков (лица человека) с «эталонными» данными биометрического шаблона, полученными с карты. После этого принимается решение о правомочности владения пользователем картой.
4. В случае успешной проверки на контроллер СКУД пересылается номер карты через интерфейс Виганда или OSDP.
5. После завершения шагов 2-4 загруженный с карты биометрический шаблон удаляется из памяти терминала.

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 не хранятся ни в каком виде в биометрических терминалах или на сервере

# Регистрация биометрического шаблона



Биометрический шаблон пользователя хранится на бесконтактной смарт-карте, принадлежащей пользователю. На карте нет ФИО пользователя или каких-либо данных, позволяющих осуществить установление сведений о лице или такого лица. Вместе с биометрическим шаблоном пользователя хранится только порядковый номер карты (номер пользователя для использования в СКУД).

# Проход через точку доступа



# Регистрация биометрического шаблона с записью на карту



# Проход пользователя через точку доступа

Пользователь



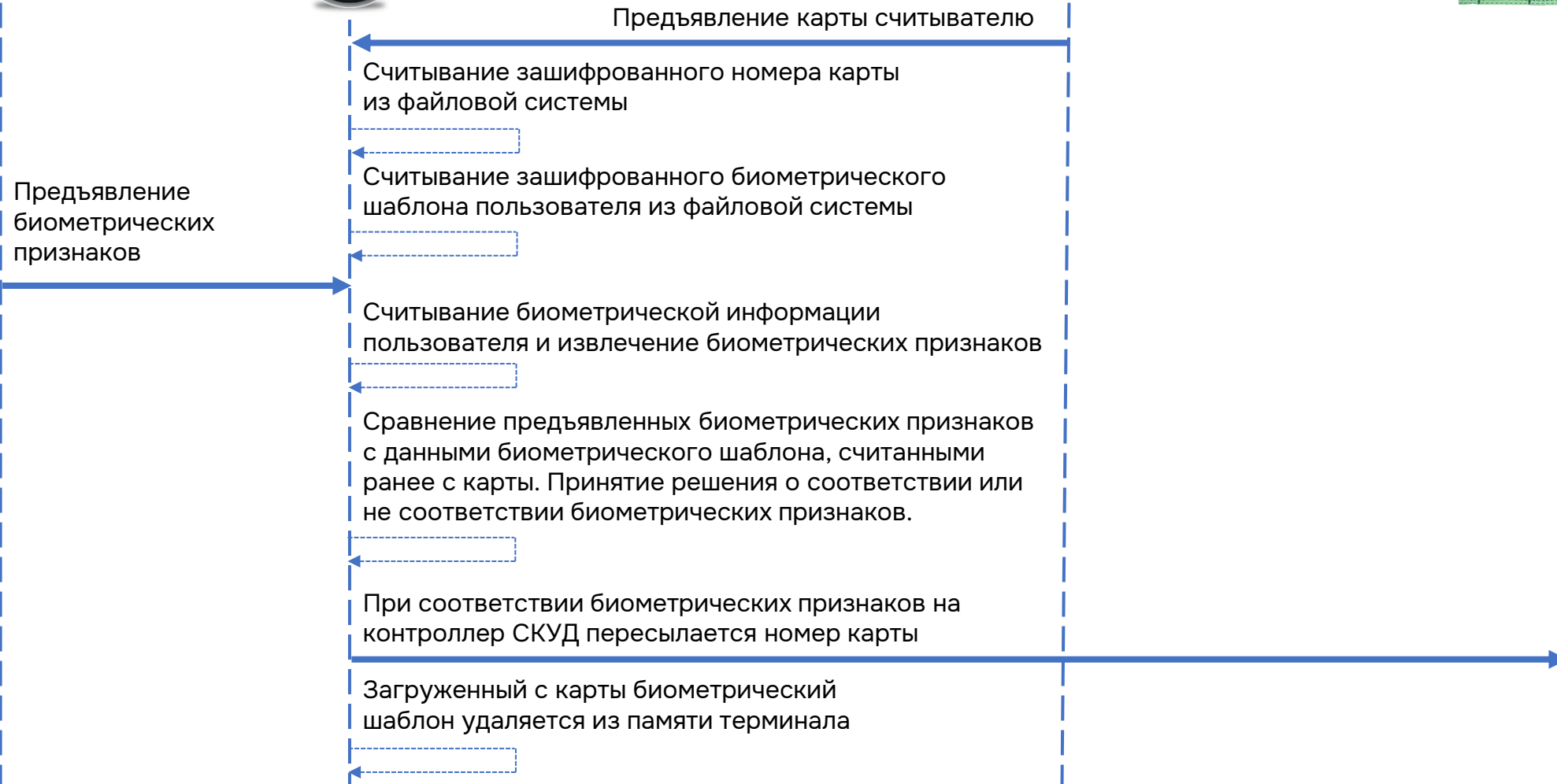
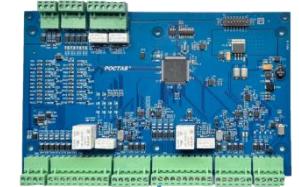
Биометрический терминал со считывателем карт



Карта с запрограммированным номером (ID) и биометрическим шаблоном пользователя



Контроллер системы контроля и управления доступом





СТАНДАРТ  
БЕЗОПАСНОСТИ



# ПОЛНОРОСТОВЫЕ ТУРНИКЕТЫ СЕРИИ РОСТАБ RS

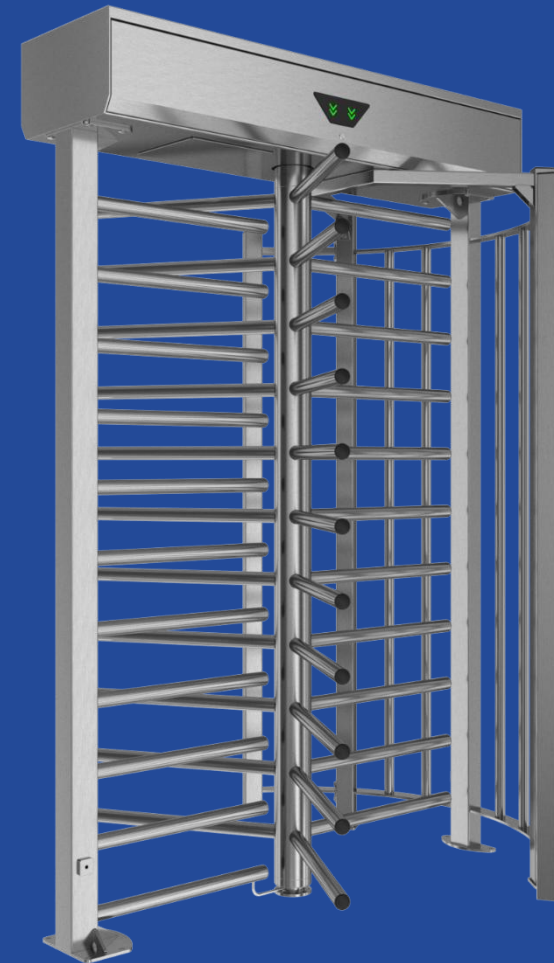
# Турникеты РОСТАБ



- Компания АО «Стандарт безопасности» в новых современных реалиях выбрала путь организации локального производства в сочетании с продолжением взаимовыгодного сотрудничества с зарубежными компаниями-разработчиками компонентов для турникетов, автоматизированных проходных и шлюзовых кабин
- Результатом такого сотрудничества стала организация совместного производства, что позволяет эффективно реализовать стратегию импортозамещения путем интеграции передовых технологий и использования потенциала локального производства компонентов и сборки
- Мы предлагаем полный функциональный ряд моделей турникетов, изготовленных с использованием самых современных технологий и имеющих фирменную гарантию в России
- Широкий ассортимент поставляемого оборудования соответствует высоким требованиям по дизайну входной группы, являющейся визитной карточкой современного предприятия или организации
- Все турникеты и шлюзовые кабины интегрируются с системой контроля доступа РОСТАБ и биометрическими терминалами VisionPass и MorphoWave

# Ключевые особенности серии **RS**

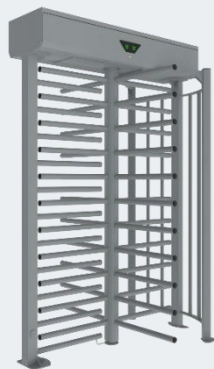
- Управляющий механизм из титанового сплава
- Опциональный демпфер для плавной и бесшумной работы
- Индикаторы прохода входят в комплект
- Подсветка прохода с датчиком освещенности входит в комплект
- Верхняя панель может устанавливаться различными способами для реализации прохода справа или слева
- Площадка 60 x 60 мм для удобной установки считывателя



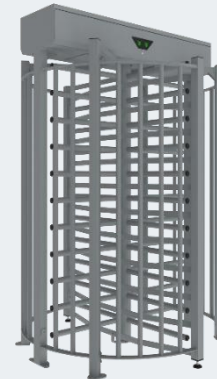
# Турникеты РОСТАБ серии RS



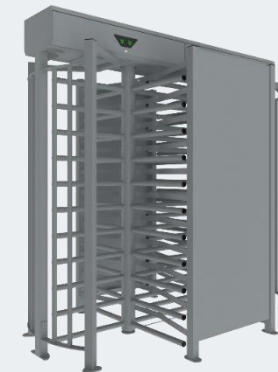
Один проход  
(исполнение 1), угол  
между лопастями  $90^\circ$



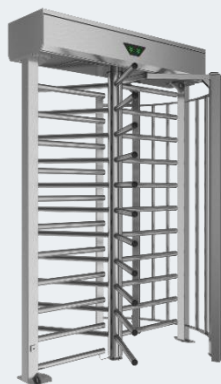
Один проход  
(исполнение 2), угол  
между лопастями  $90^\circ$



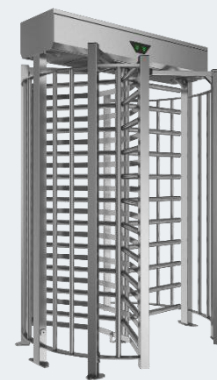
Два прохода, угол  
между лопастями  $90^\circ$



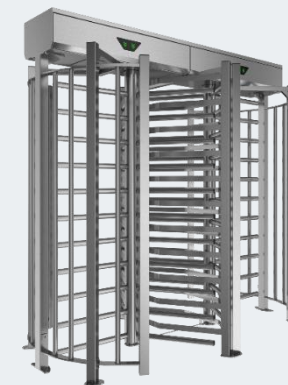
Один проход  
(исполнение 1), угол  
между лопастями  $120^\circ$



Один проход  
(исполнение 2), угол  
между лопастями  $120^\circ$



Два прохода, угол  
между лопастями  
 $120^\circ$



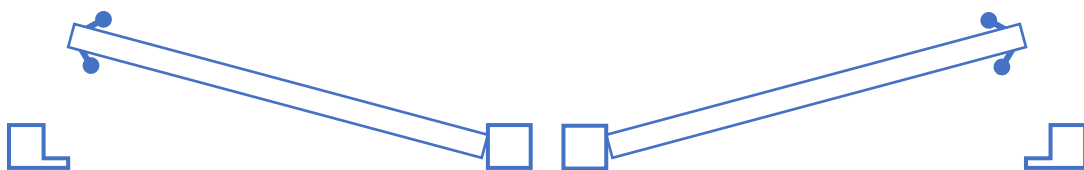
# Стандартные функции серии RS



- Управляющий механизм из титанового сплава, хорошо зарекомендовавший себя на многочисленных объектах в России и по всему миру
  - Блокировка лопастей при попытке одновременного прохода двух человек.
  - Если лопасть была повернута более чем на 32°, ее обратный поворот блокируется. Человек, начавший проход, не может незаметно вернуться обратно. В момент прохода через турникет в прямом направлении доступ в обратном направлении блокируется.
  - Самоцентрирующийся механизм для точного возврата лопастей в исходную позицию.
- Продолжительный срок службы:
  - Двухслойная защита от коррозии
  - Ресурс работы турникета – не менее 5 миллионов циклов
- Датчики прохода для надежной работы функции контроля повторного прохода (anti-passback)
- Безопасность в любой ситуации:
  - При отключении питания или в случае пожарной тревоги турникет позволяет обеспечить беспрепятственный выход. Данная функция может быть применена к обоим направлениям прохода или только к одному направлению (свободный выход при заблокированном входе).
  - Возможность блокировки турникета при отключении питания

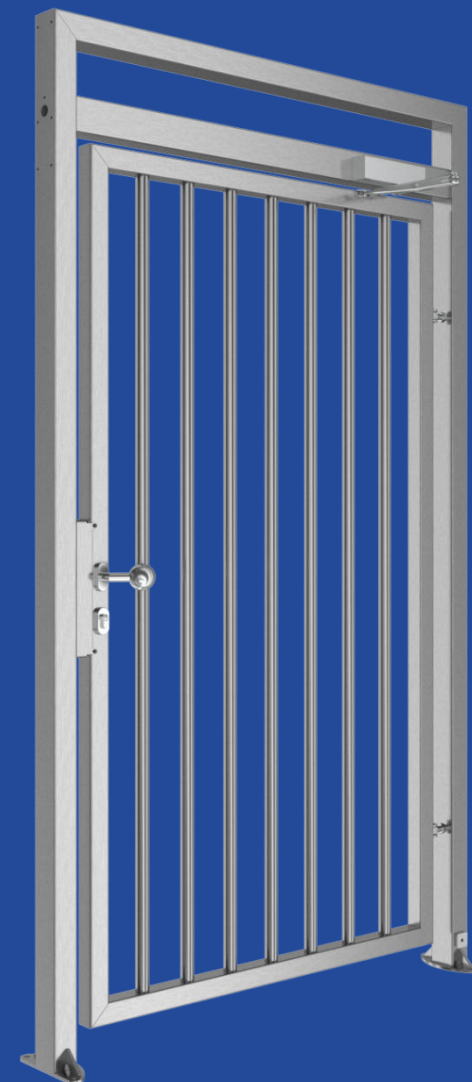
# Калитка для турникетов серии RS

- Калитка подходит к турникету серии RS по размерам и оформлению
- Ширина прохода 1100 мм
- По умолчанию поставляется вариант калитки под открывание правой рукой
- Замок с цилиндром европейского стандарта
- Автоматический доводчик



Вариант под правую руку

Вариант под левую руку



# Навес для турникетов и калитки серии RS

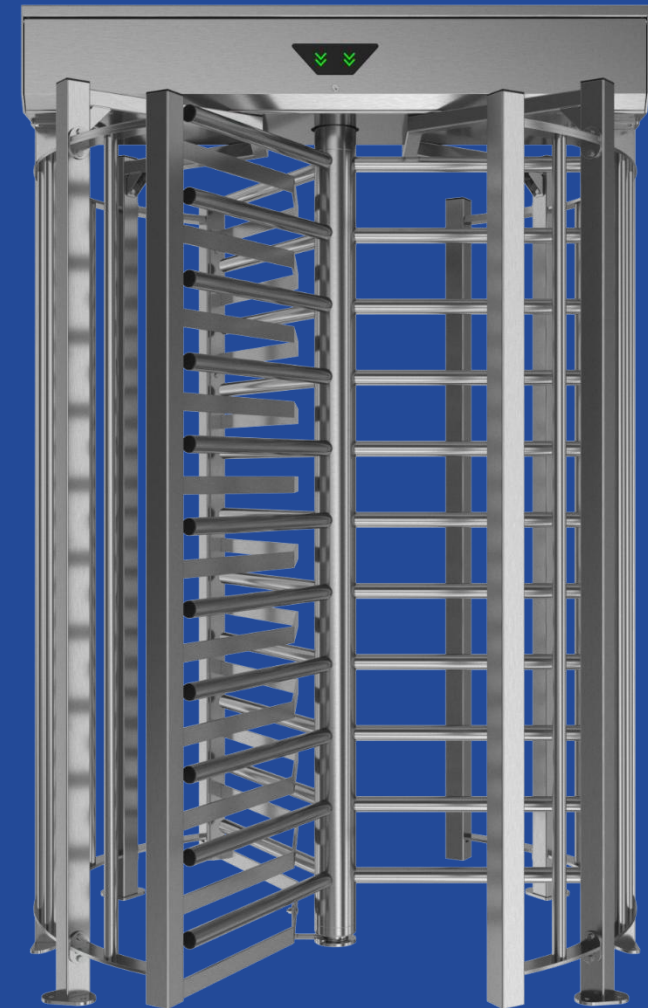


- Стандартные материалы и отделка:
  - Каркас: алюминий с порошковым покрытием RAL 7040, окраска в цвет турникета, если не выбран альтернативный цвет
  - Материал вставки: поликарбонат толщиной 10 мм
- Слив воды:
  - Стандартный вариант – слив из угла навеса со стороны, противоположной проходу
  - Опционально – дренаж через корпус (требуется наличие отверстия в полу, чтобы вода могла стекать)



# Удобные монтаж и подключение

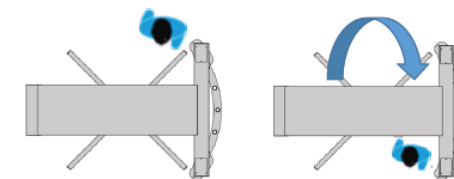
- Квадратная площадка размером 60 x 60 мм для легкой установки считывателя:
  - для самостоятельной установки считывателя
  - возможность поставки турникета со считывателем
- Опциональный шаблон для сверления:
  - оцинкованный шаблон из мягкой стали для облегчения сверления в полу для установки
  - конструкция «пазл» упрощает хранение и транспортировку
- Дополнительная напольная пластина:
  - стальная опорная плита с напольным покрытием из сверхпрочного ПВХ
  - скошенные края из нержавеющей стали
- Опциональные монтажные основания:
  - основание с анкерами: металлическое основание с точками крепления, которые можно установить в бетонный пол на этапе строительства
  - мобильное основание: тяжелое основание подходит для установки и позволяет перемещать его с помощью вилочного погрузчика



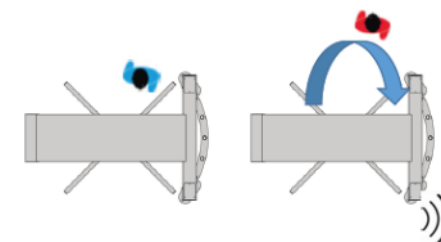
# Датчик подтверждения прохода



- Датчик доступен для всех версий турникетов серии RS
- Используется для объектов, где необходимо убедиться в том, что человек действительно прошел через турникет:
  - Объекты критической инфраструктуры
  - Горнодобывающая и химическая отрасли
- Регистрация нормального прохода через турникет:
  1. Разрешен проход по карте/биометрии или сигналу разблокировки. Ротор турникета разблокирован и может перемещаться вручную.
  2. Правильный проход выполнен. Человек проходит через турникет.
  3. Датчики обнаруживают и подтверждают факт совершения прохода.
- Обнаружение имитации прохода:
  1. Разрешен проход по карте/биометрии или сигналу разблокировки. Ротор турникета разблокирован и может перемещаться вручную.
  2. Проход через ворота не осуществляется. Нарушитель вручную вращает роторные рычаги для имитации прохода.
  3. Датчики обнаруживают, что проход НЕ осуществлялся, и подается сигнал тревоги.



Правильный проход



Имитация прохода – ротор проворачивается без реального прохода

Интегрированная  
IP-система  
видеонаблюдения  
**РОСТАБ®**



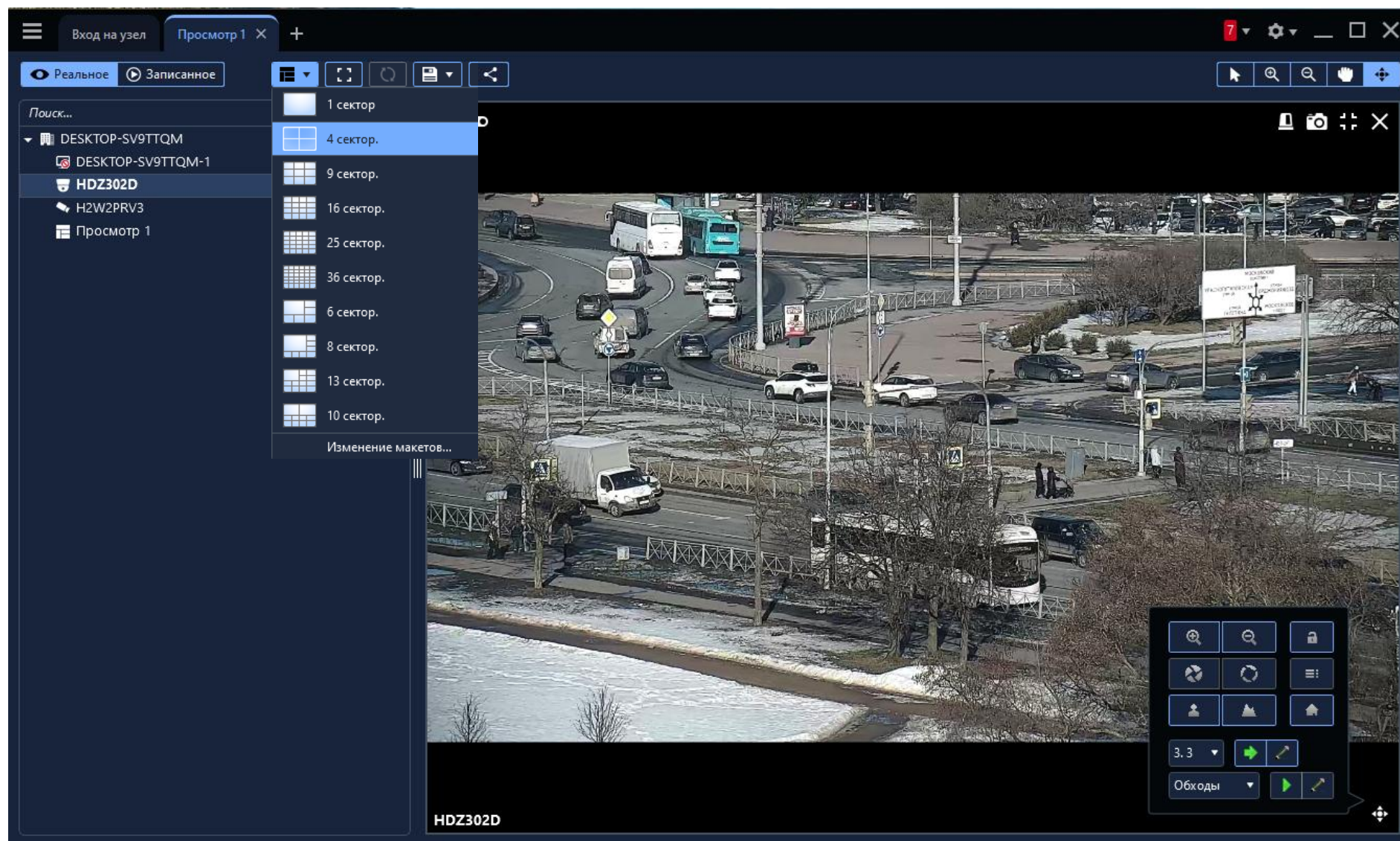
# Преимущества интегрированного решения РОСТАБ

- На рынке присутствует множество компаний, предлагающих "интегрирующие" программные продукты для систем безопасности, позволяющие осуществлять мониторинг и управление оборудованием различных фирм-производителей. Обычно такие компании не производят «железо», а лишь предлагают программную оболочку для работы с оборудованием. Эти решения нельзя назвать интегрированными. У пользователей таких решений могут возникнуть проблемы, связанные с расширением системы, выходом обновлений и новых версий аппаратного обеспечения (поскольку оно производится сторонними компаниями), а также – с технической поддержкой от нескольких независимых компаний.
- В этой связи полноценная интеграция возможна только для решений, выпускаемых одной компанией-производителем, имеющей достаточные ресурсы не только для написания программного обеспечения, но и выпуска оборудования.
- Только в случае, когда все элементы системы изначально разрабатываются с учетом дальнейшего полноценного взаимодействия, становится практически возможным реализовать все заявленные функциональные возможности оборудования. При этом важно, чтобы компания-производитель данного решения являлась разработчиком не только программного, но и аппаратного обеспечения.
- АО «Стандарт безопасности» является разработчиком и производителем IP-контроллеров СКУД и охранной сигнализации, программного обеспечения для видеоанализа, записи и управления видеоизображениями. Именно в этом состоит уникальность предлагаемых решений, поскольку все элементы изначально разрабатываются с учетом полноценной интеграции.

# Что такое РОСТАБ® VMS?

- РОСТАБ VMS (Video Management System) – это программная платформа для управления видеоизображениями в цифровых системах телевизионного наблюдения
- РОСТАБ VMS обеспечивает удобный графический интерфейс для управления мониторингом, записью и анализом видеоизображений и используется для организации ситуационных центров и центров мониторинга видеоинформации
- РОСТАБ VMS использует сервера записи видео (Network Video Recorder) на базе ОС Linux
- РОСТАБ VMS реализует интеграцию с системой контроля и управления доступом
- Интегрированная высокоточная видеоаналитика использует технологии искусственного интеллекта с возможностью создания запросов на естественном языке (GenAI и LLM)
- Поддержка высокоэффективного GPU-рендеринга видеопотоков H.264 и H.265 на сетевых рабочих станциях операторов, групповой передачи видео (multicast), нескольких потоков видео от IP-камер и динамического переключения между потоками видео
- Поддержка ONVIF Profile G – резервирование видеоархива с помощью карты памяти, встроенной в IP-камеру
- Обратная совместимость сетевых видеорегистраторов РОСТАБ с системами видеонаблюдения Honeywell на базе ПО MAXPRO VMS – возможность обновления системы без замены установленного оборудования и ПО

# Пример интерфейса оператора РОСТАБ® VMS



# Экосистема **РОСТАБ** для работы с видеоизображениями



# Структура системы на базе РОСТАБ VMS

Система контроля  
и управления  
доступом



Сервер  
интегрированной  
системы безопасности  
на базе ПО РОСТАБ



Сервер видеоаналитики  
РОСТАБ с резервированием



Компьютерная сеть

Видеостена



Рабочая станция с клиентским ПО  
интегрированной системы безопасности



Рабочая станция РОСТАБ VMS



Видеосерверы для записи и анализа видео



РОСТАБ NVR



РОСТАБ NVR



РОСТАБ NVR



Резервный  
РОСТАБ NVR

Сеть для IP-камер

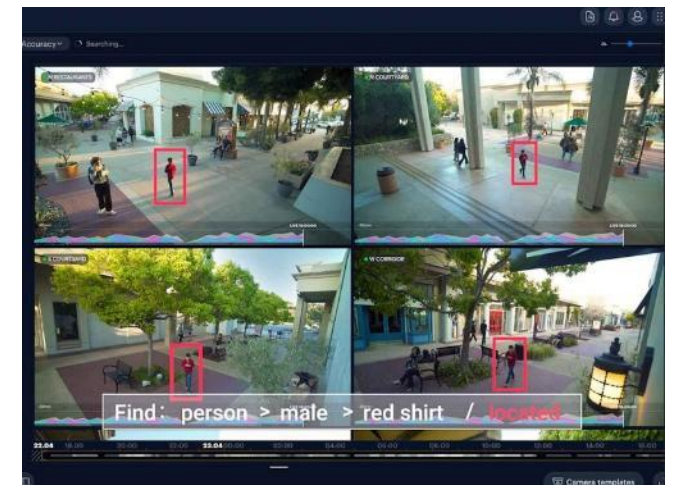


# Преимущества видеоаналитики с использованием технологий искусственного интеллекта

- Основная задача применения видеоаналитики – повышение эффективности функционирования системы видеонаблюдения и автоматизация работы операторов
- Самый важный результат внедрения видеоаналитики состоит в том, что служба безопасности сможет реагировать на потенциально опасные действия на более ранних стадиях, а не после того, как инцидент уже произошел
- Система осуществляет оперативное информирование операторов о происходящих событиях на основе слежения за перемещением объектов:
  - снижается утомляемость и вероятность ошибки оператора при оценке ситуации
  - уменьшается число операторов: один оператор может контролировать большее число камер
- Видеоаналитика позволяет решать задачи охранной сигнализации и контроля периметра
- ПО видеоаналитики функционирует на серверах видеозаписи (NVR), использующих ОС Linux
- Реализуется полнофункциональная интеграция с подсистемами контроля доступа и охранной сигнализации



ПОИСК ЛЮДЕЙ ПО ЗАДАНЫМ КРИТЕРИЯМ

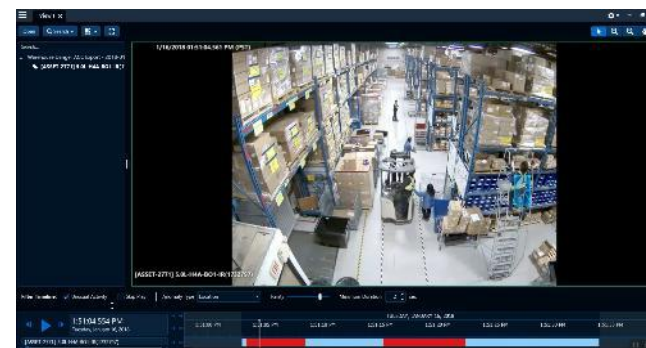


ПОИСК И ОТСЛЕЖИВАНИЕ ОБЪЕКТОВ

# Штатная видеоаналитика в составе РОСТАБ® VMS

## Видеоаналитические функции сетевых видеорегистраторов:

- распознавание, верификация и подсчет лиц
- определение принадлежности человека к возрастной группе
- определение гендерной принадлежности человека
- определение цвета одежды человека в кадре
- обнаружение и отслеживание человека или транспортного средства с помощью нескольких камер
- распознавание регистрационных знаков транспортных средств, включая интеграцию со СКУД
- обнаружение образования очереди или толпы, подсчет количества людей
- подсчет проезжающего автотранспорта по полосам движения
- обнаружение движения автотранспорта в неверном направлении, обнаружение образования затора
- определение типа и цвета транспортного средства



# Штатная видеоаналитика в составе РОСТАБ® VMS

Видеоаналитические функции сетевых видеорегистраторов – обучение видеоаналитики на примерах

Вход на узел

Просмотр 1

Настройка

Обучение на примерах

| Время               | Ответ | Класс | Автор       | Время создания      |
|---------------------|-------|-------|-------------|---------------------|
| 06.03.2026 10:09:11 | Верно | Автом | administrat | 06.03.2026 10:16:19 |
| 06.03.2026 10:09:11 | Верно | Автом | administrat | 06.03.2026 10:16:24 |
| 06.03.2026 10:09:11 | Верно | Автом | administrat | 06.03.2026 10:16:28 |
| 06.03.2026 10:09:11 | Верно | Автом | administrat | 06.03.2026 10:16:30 |
| 06.03.2026 10:09:11 | Верно | Автом | administrat | 06.03.2026 10:16:26 |
| 06.03.2026 10:09:11 | Верно | Автом | administrat | 06.03.2026 10:16:21 |
| 06.03.2026 10:09:11 | Верно | Автом | administrat | 06.03.2026 10:16:17 |
| 06.03.2026 10:09:11 | Верно | Автом | administrat | 06.03.2026 10:16:13 |
| 06.03.2026 10:09:22 | Верно | Автом | administrat | 06.03.2026 10:17:00 |
| 06.03.2026 10:09:27 | Верно | Автом | administrat | 06.03.2026 10:17:13 |

Маркер обучения

Время:

Кем отмечено:

Когда отмечено:

Метки примеров 10 «Истина»: 0 «Ложь»

Удалить все маркеры

10:09:34.330

6 марта 2026 г.

HDZ302D

6 МАРТА 2026 Г.

Распознавание движения классифицированных объектов

Типы объектов:

Чувствительность:

Время обнаружения

Время записи перед движением

Время записи после движения

Человек, Автомобиль

☒ Человек

☒ Автомобиль

☐ Велосипед

☐ Автомобиль

☐ Мотоцикл

☐ Автобус

☐ Грузовой автомобиль

5 секунд

# Штатная видеоаналитика в составе РОСТАБ® VMS

Видеоаналитические функции сетевых видеорегистраторов – поиск объектов по внешнему виду

Вход на узел

Просмотр 1

Настройка

Поиск: Внешний вид

Изменить камеры

Результаты поиска по внешнему виду

Описание внешнего вида

Пол: Мужчина    Цвет волос: Черные  
Возраст: Взрослый

Полный профиль

Изменить описание

Релевантность

Камера

☐ Показать только избранные результаты

06.03.2026 11:03:30.395

HDZ302D

00:00.000

Диаграмма результатов поиска

06.03.2026 11:00:00    06.03.2026 12:00:00    [Список результатов]

11:03:30.398

6 марта 2026 г.

HDZ302D

6 МАРТА 2026 Г.

Параметры поиска по внешнему виду

Человек

Автом.

Отличительные признаки

Одежда

Цвет одежды - верх

Цвет одежды - низ

Параметры поиска по внешнему виду

Человек

Автомобиль

Изображение

Отличительные признаки

Пол

Цвет волос

Возраст

Одежда

Диапазон дат

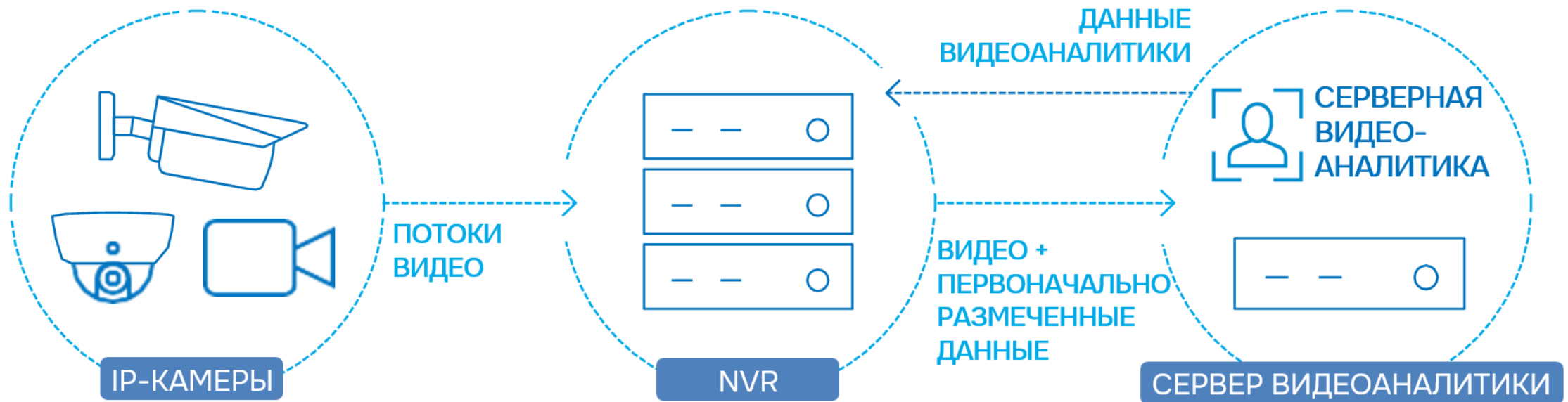
Камеры (DESKTOP-SV9TTQM)

Поиск

Отмена

# Преимущества видеоаналитики с использованием технологий искусственного интеллекта

- Сервер видеоаналитики использует генеративный искусственный интеллект (GenAI) и большую языковую модель (LLM) для возможности формирования запросов на естественном языке
- Сервер использует ОС Linux и современные высокопроизводительные GPU Nvidia L4



# Преимущества видеоаналитики с использованием технологий искусственного интеллекта

## Примеры запросов на естественном языке для видеоанализа:

- Обнаружение людей, скрывающих свое лицо
- Обнаружение падения коробки с конвейера
- Обнаружение автомобиля доставки, съезжающего с заднего пандуса склада
- Обнаружение охранника с собакой
- Обнаружение скопления людей
- Обнаружение группы людей, направляющихся к зданию
- Обнаружение человека без средств индивидуальной защиты
- Обнаружение дыма и/или огня
- Обнаружение опрокидывания автомобиля или дорожно-транспортного происшествия
- Обнаружение человека с тележкой или корзиной для покупок
- Обнаружение разлива жидкости на полу
- Обнаружение человека в полицейской форме
- Обнаружение курящего человека
- Обнаружение остановившегося автомобиля на скоростном шоссе
- Обнаружение появления животного на железнодорожных путях
- Обнаружение оставленной сумки или рюкзака
- Предупреждение, когда у человека в руках находится каска
- Обнаружение птиц на взлетной полосе аэродрома
- Обнаружение лежащего человека
- Обнаружение оружия в руках
- Обнаружение митинга
- Обнаружение человека с сотовым телефоном в руках
- Обнаружение ребенка, находящегося без присмотра взрослого в бассейне
- Обнаружение летящего дрона

# Примеры запросов для работы видеоаналитики

## Примеры запросов для обеспечения высокой точности и эффективности визуальных оповещений

### 1. Описывайте события, связанные с одним изображением

Система анализирует отдельные видеокadres. Запросы для работы системы видеоанализа должны описывать события, которые оператор может видеть на одном изображении, а не события, происходящие в нескольких кадрах.

- Рекомендуется: «Оповещение, если человек лежит на земле»
- Не рекомендуется: «Оповещение, если человек поскользнется и упадет»

### 2. Добавьте подробности, избегайте расплывчатых терминов

Конкретные описания повышают точность обнаружения событий.

- Рекомендуется: «Оповещение, если выходная дверь заблокирована или перекрыта коробкой»
- Не рекомендуется: «Оповещение, если что-то блокирует дверь»

### 3. Включайте информацию о местоположении интересующего объекта относительно других объектов

Указание информации о местоположении объекта относительно других объектов улучшает обнаружение.

- Рекомендуется: «Оповещение, если на полу возле двери лежит посылка»
- Не рекомендуется: «Оповещение, если посылка будет доставлена»

### 4. Избегайте отрицательных подсказок

Отрицательные подсказки, как правило, имеют более низкую точность.

- Рекомендуется: «Оповещение, когда парковка освободится»
- Не рекомендуется: «Оповещение, когда на парковке **не будет автомобилей**»

# Примеры запросов для работы видеоаналитики

Расположение камеры, освещение и качество изображения могут влиять на точность обнаружения событий. Для достижения наилучших результатов рекомендуется соблюдать минимальное количество пикселей на метр:

| Тип события                           | Описание                                                                                                     | Примеры объектов, действий или событий                                  | Минимальное количество пикселей на метр |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|-----------------------------------------|
| Объект обнаружения                    | Подтверждает наличие объекта в определенной области                                                          | Человек, собака, автомобиль                                             | 80                                      |
| Подробности объекта обнаружения       | Анализирует конкретные атрибуты, состояние или особенности объекта (например: цвет, одежду, тип автомобиля). | Человек в красной куртке, грузовик                                      | 245                                     |
| Взаимодействие с объектом обнаружения | Анализирует пространственные взаимоотношения или взаимодействие между двумя или более отдельными объектами   | Мужчина выгуливает собаку. Грузовик припаркован перед выходом из здания | 165                                     |
| Обнаружение события                   | Подтверждает наличие события в пределах определенной области                                                 | Наводнение, дым, огонь, протечка воды                                   | 165                                     |

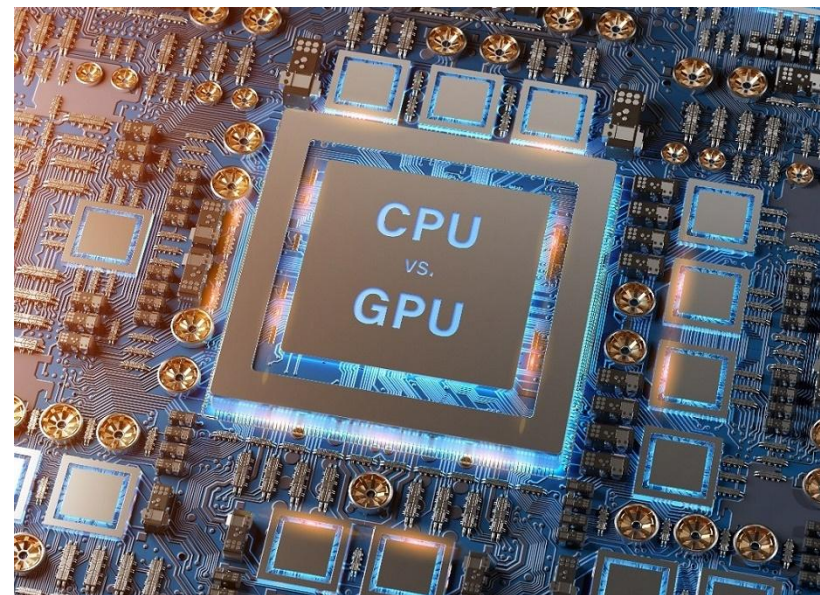
# Возможности серверов видеозаписи и аналитики

- Локальный анализ видеоизображений в режиме реального времени и в видеоархиве с использованием встроенных GPU Nvidia
- До 400 каналов записи на один сервер
- 12 отсеков для жестких дисков, поддержка RAID
- Сетевая пропускная способность на запись 900-1500 Мбит/с в зависимости от конфигурации сервера
- Сетевая пропускная способность на трансляцию текущего видео 900-2100 Мбит/с в зависимости от конфигурации сервера
- Сетевая пропускная способность на воспроизведение записанного видео 600 Мбит/с
- Поддержка IP-камер различных фирм-производителей: поддержка ONVIF-профилей S, G, Q, протоколов RTSP, VAPIX
- Поддержка многопоточности и автоматического переключения потоков от IP-камер
- Поддержка записи звука
- Поддержка оперативного и долговременного архива видеозаписей



# GPU-рендеринг и автоматическое переключение видеопотоков на рабочих станциях операторов

- GPU-рендеринг позволяет задействовать ресурсы интегрированной в процессор видеокарты и/или дискретных видеокарт. Это увеличивает количество одновременно просматриваемых камер на рабочей станции оператора
- Функция GPU-рендеринга не требует использования на рабочих станциях дорогостоящих высокопроизводительных видеокарт
- Поддержка функции переключения видеопотоков позволяет использовать разные потоки от IP-камер при просмотре видеоизображений в разных режимах
- Возможность использования видеопотока с хорошим качеством при просмотре камеры в полноэкранном режиме и автоматическое переключение на поток с более низким качеством при просмотре видеокамеры в раскладке с большим количеством видеокамер, например, в режиме 4x4 и более



# Системы охраны периметра и протяженных объектов на основе оптоволоконного кабеля

ПЕРВЫЙ РУБЕЖ ОХРАНЫ

# Принцип действия системы охраны периметра на основе оптоволоконного кабеля



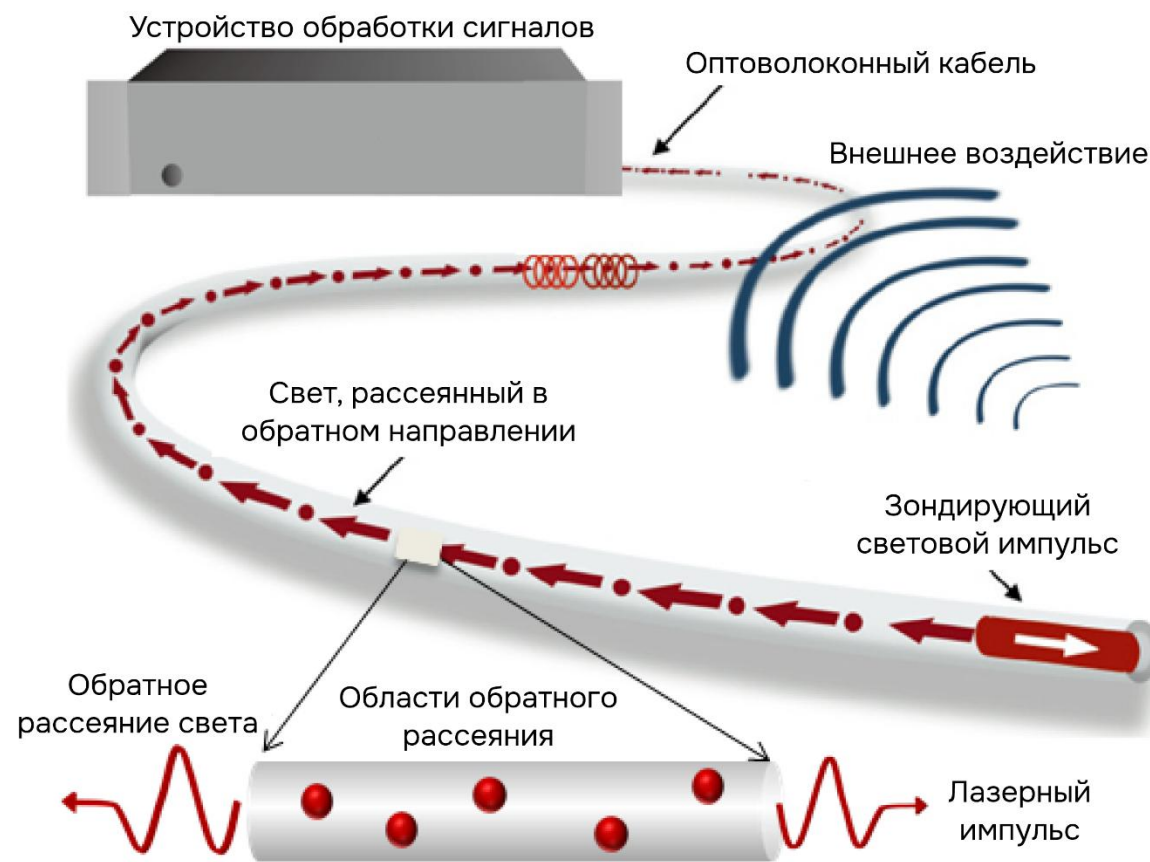
Современные системы защиты периметра и мониторинга состояния протяженных объектов (таких, как трубопроводы и кабельная инфраструктура) требуют от охранных извещателей высокой чувствительности, надежности и устойчивости к внешним воздействиям. Одной из сравнительно новых технологий, используемой в системах охранной сигнализации является распределенное акустическое зондирование (англ. DAS – Distributed acoustic sensing). Эта технология использует оптоволоконный кабель в качестве линейного массива виртуальных акустических датчиков, реагирующих на механические воздействия.

Принцип действия системы основан на рефлектометрических измерениях. Осуществляется мониторинг рассеянного в обратном направлении оптического излучения при прохождении по оптическому волокну зондирующего импульса. Оптическое волокно в этом случае можно представить как совокупность индивидуально опрашиваемых датчиков, расположенных последовательно, сигналы от которых приходят в разные моменты времени. Благодаря этому существует возможность определить точное расположение каждого из таких датчиков.

# Принцип действия системы охраны периметра на основе оптоволоконного кабеля



При прохождении импульса света по оптоволокну каждый участок волокна рассеивает часть света. Свет, рассеянный в обратном направлении, принимается фотоприемником, который вместе с излучающим лазерным светодиодом находится в начале оптоволоконного кабеля. Осуществляется запись рефлектограммы. При этом каждому участку записи соответствует свой участок оптоволоконного кабеля. Если при прохождении следующего импульса обратное рассеяние на этом участке изменится, значит, оптоволоконный кабель подвергается воздействию. Тем самым оптическое волокно используется одновременно для передачи информации и в качестве набора чувствительных датчиков.



# Система охраны периметра и протяженных объектов на основе оптоволоконного кабеля



- Системы охраны периметра РОСТАБ ФП400 и ФП1150 используют распределенное акустическое зондирование на основе рэлеевского рассеяния. Лазерный импульс передается по оптическому волокну, а рассеивающие участки внутри волокна заставляют волокно действовать как распределенный интерферометр с длиной элементарного датчика, приблизительно равной длине импульса. Интенсивность отраженного света измеряется как функция времени после передачи лазерного импульса. Этот процесс называется когерентной рэлеевской оптической рефлектометрией C-OTDR (англ. - Coherent Optical Time Domain Reflectometer).
- Когда импульс света проходит всю длину волокна и обратно, по волокну передается следующий импульс. Данный тип системы очень чувствителен к деформации. Измерения могут проводиться практически одновременно на всех участках волокна.
- Основным элементом системы является обычный оптоволоконный кабель, устанавливаемый на ограждении, например, на 3D-заборе.



# Система охраны периметра и протяженных объектов на основе оптоволоконного кабеля



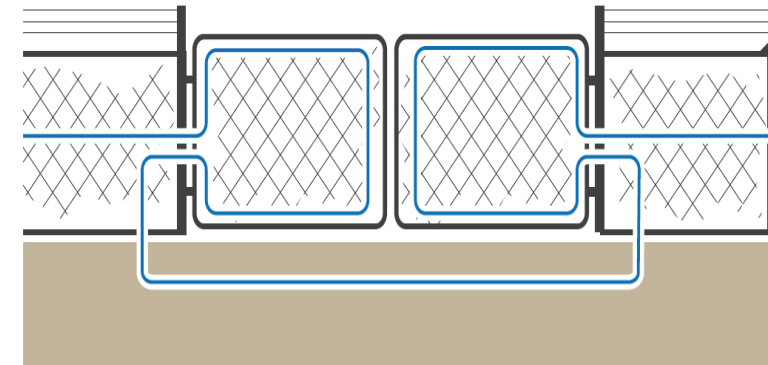
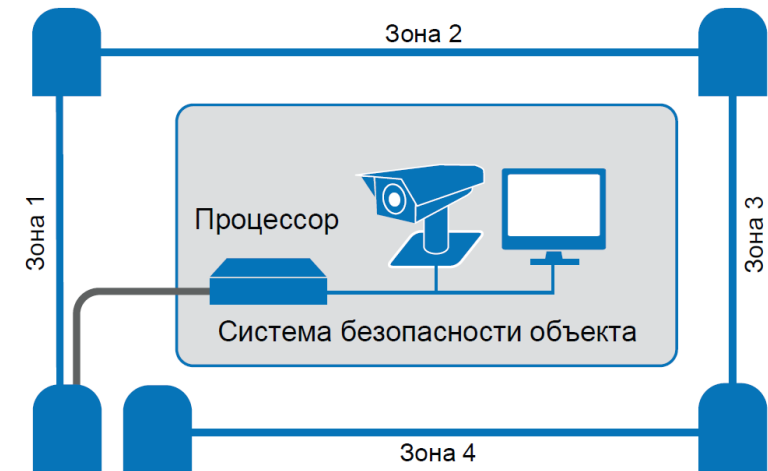
- Системы охраны периметра РОСТАБ ФП400 и ФП1150 не подвержены влиянию электромагнитных помех в любых диапазонах.
- Отличительной особенностью является размер одной зоны обнаружения, который может составлять от 300 м до 80 км. На протяжении этого расстояния кабель системы не использует электронные устройства и не требует применения дополнительных источников питания. Обеспечивается точность обнаружения проникновения в пределах нескольких метров.
- Проложенный кабель не требует какого-либо обслуживания и при случайных повреждениях быстро ремонтируется.
- В отличие от вибрационного чувствительного кабеля, система контролирует не одну зону целиком, а является распределенным детектором воздействий на протяжении всей длины своего плеча с точным указанием конкретного места проникновения.



# Система охраны периметра и протяженных объектов на основе оптоволоконного кабеля ФП400



- РОСТАБ ФП400 – это система контроля периметра и протяженных объектов, использующая волоконно-оптический кабель. Кабель устанавливается непосредственно на ограждение и обнаруживает различные варианты попыток его преодоления нарушителем.
- Чувствительный кабель полностью защищен от электромагнитных помех, а также является взрыво- и пожаробезопасным. Это позволяет использовать систему для контроля любых протяженных объектов, включая электрические и насосные станции, трубопроводы, нефтяные и газовые скважины и другие объекты критической инфраструктуры.
- Для работы системы не требуются источники питания, размещаемые в контролируемой зоне.
- Кабель можно устанавливать на распашные ворота, а сама зона ворот может быть программно сконфигурирована как независимая зона обнаружения для исключения тревог во время открывания. Герконы дверей и другие извещатели с выходом реле можно подключать к встроенным выходам шлейфов сигнализации.



# Система охраны периметра и протяженных объектов на основе оптоволоконного кабеля **ФП400**

## Ключевые особенности:

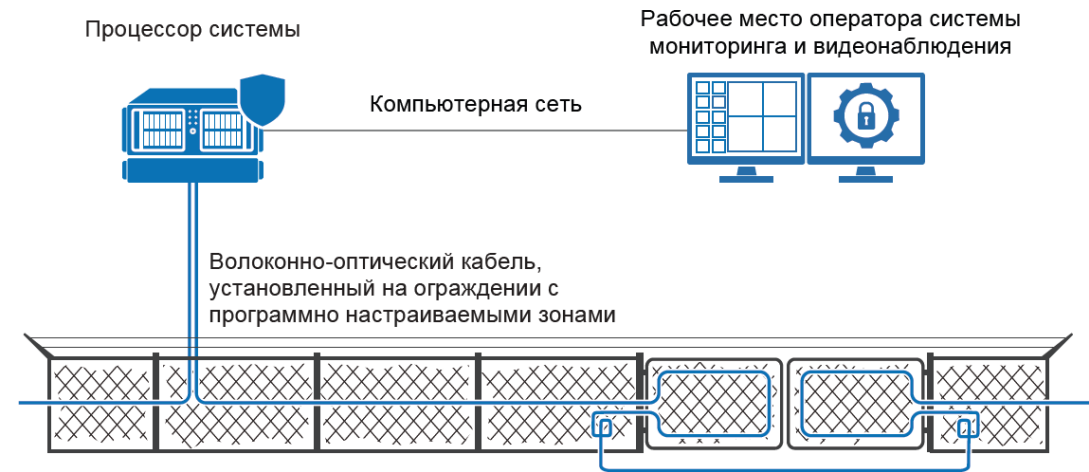
- Возможность установки на любых типах ограждений
- 4 зоны обнаружения на один процессор с максимальной длиной зоны 300 м
- Точное обнаружение нескольких одновременных вторжений
- Мгновенное обнаружение обрыва кабеля
- Возможность использования до 20 км нечувствительного кабеля до начала зоны
- Диапазон рабочих температур  $-40...+70^{\circ}\text{C}$
- Срок службы чувствительного кабеля до 25 лет
- Шесть программируемых выходов реле для прямого подключения к охранной панели
- Программное обеспечение для мониторинга и интеграции с системой видеонаблюдения



# Система охраны периметра и протяженных объектов на основе оптоволоконного кабеля **ФП1150**



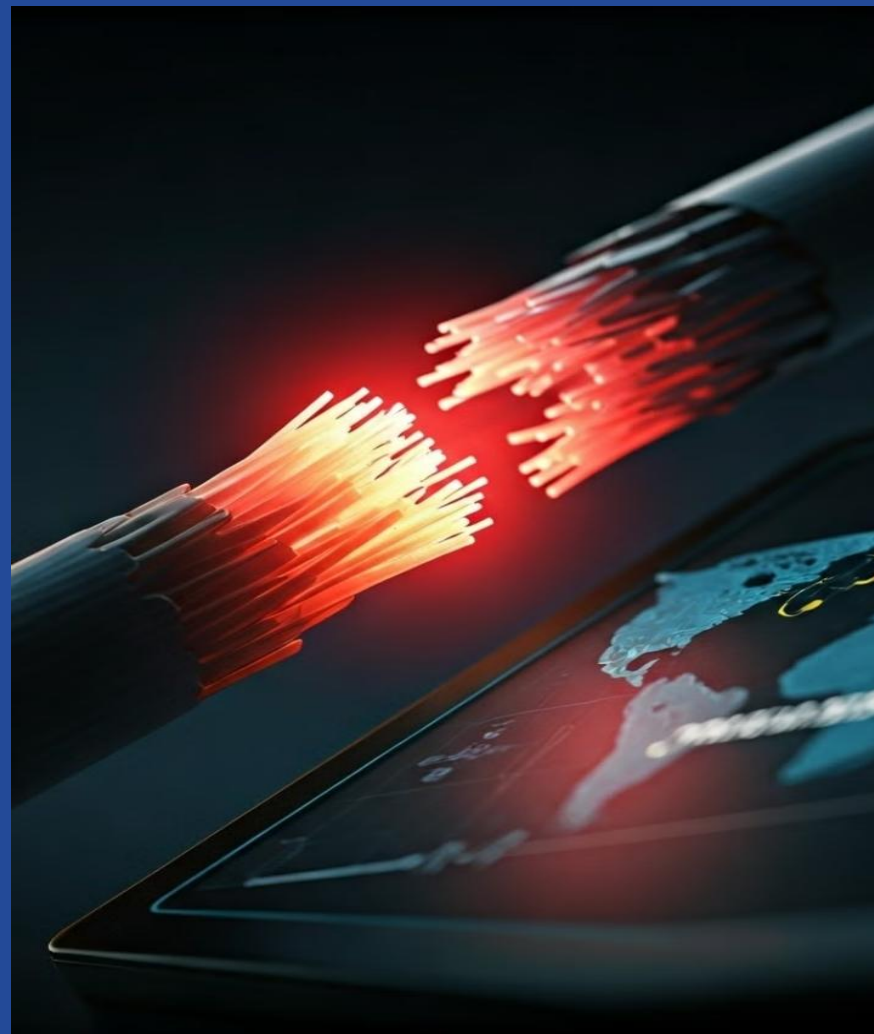
- Система на базе ФП1150 обеспечивает защиту периметра протяженностью до 80 км на один модуль процессора с точностью определения местоположения нарушения в пределах 4 м
- ФП1150 использует сложные алгоритмы классификации для различения реальных угроз и вибраций от случайных источников, позволяя одновременно обнаруживать несколько нарушений даже при наличии нелокализованных воздействий окружающей среды (дождь, снег, град, сильный ветер и т.п.)
- Волоконно-оптический когерентный рэлеевский рефлектометр не требует наличия полевых элементов с питанием, что делает чувствительный элемент полностью невосприимчивым к электромагнитным помехам и разрядам молнии



Поддерживается программное определение до 1440 зон обнаружения

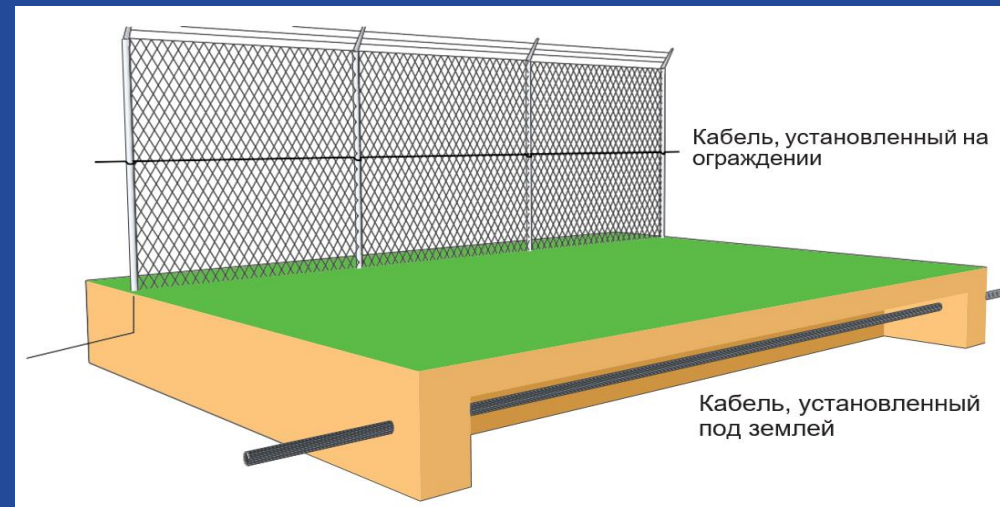
# Система охраны периметра и протяженных объектов на основе оптоволоконного кабеля **ФП1150**

- При обрыве оптоволоконного кабеля (как случайном, так и при умышленной попытке вывести систему из строя), ФП1150 немедленно сообщает о происшествии, включая точное местоположение обрыва
- Извещатель сохраняет способность обнаруживать и локализовать вторжения до точки обрыва
- При установке в отказоустойчивой конфигурации с кольцевой топологией извещатель продолжает обеспечивать обнаружение на всем периметре даже после обрыва кабеля
- Максимальная длина периметра, контролируемого одним процессором системы в отказоустойчивой конфигурации составляет 40 км



# Система охраны периметра и протяженных объектов на основе оптоволоконного кабеля **ФП1150**

- ФП1150 использует одномодовое волокно в стандартном кабеле телекоммуникационного класса. Для работы извещателя требуется только одно волокно. Дополнительные волокна могут использоваться для передачи данных
- Для контроля стандартных типов ограждений используется кабель без бронированной оболочки
- Для подземной установки или для установки на спиральной колючей проволоке рекомендуется использовать бронированный кабель
- ФП1150 можно использовать на большинстве типов металлических ограждений, включая 3D-заборы, сварную сетку и стальные конструкции. Один проход кабеля обеспечивает эффективную защиту ограждений высотой до 4,3 м



# Система охраны периметра и протяженных объектов на основе оптоволоконного кабеля **ФП1150**



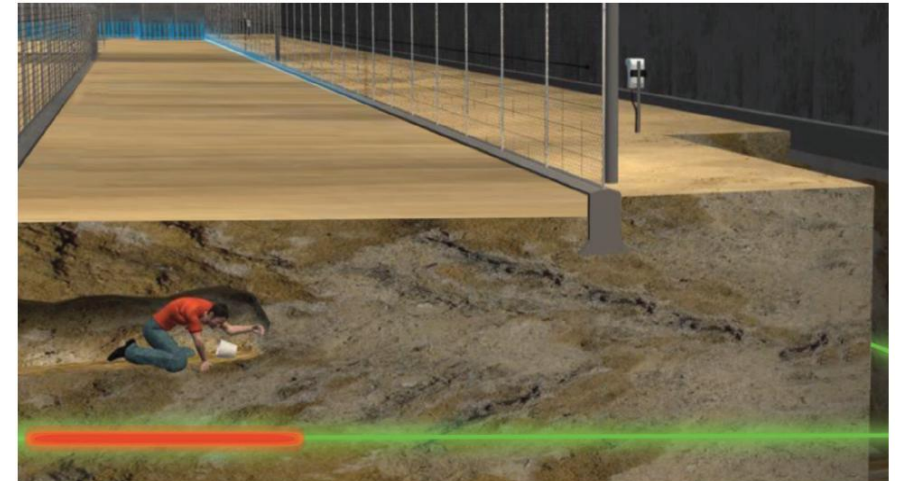
- Извещатель можно установить на распашные ворота. ФП1150 обеспечивает отдельные настройки обнаружения для контроля перелезания через ограждение и разрушения ограждения.
- Чувствительный кабель можно использовать для охраны верхней поверхности бетонных и кирпичных конструкций. Для этого кабель устанавливается на верхних углах стены с помощью крепежного элемента Р-образной формы. Для обеспечения максимального уровня безопасности датчик можно установить как с внутренней, так и с внешней стороны стены.



# Система охраны периметра и протяженных объектов на основе оптоволоконного кабеля **ФП1150**



- ФП1150 обнаруживает подкопы, а также ручные и машинные работы по рытью и прокладке тоннелей на расстоянии до 20 м от кабеля в любом направлении. Можно обнаруживать действия внутри существующих туннелей.
- Когда нарушитель перемещается над установленным в земле волоконно-оптическим кабелем (ходьба, бег или ползание), создаются характерные вибрации. Система отличает их от фоновых воздействий. ФП1150 не только обнаруживает сжатие и смещение грунта вблизи закопанного в землю кабеля, но и регистрирует сейсмические волны, вызванные человеческими шагами.
- Высокая чувствительность обеспечивает гибкость применения, позволяя не только обнаруживать шаги непосредственно над чувствительным кабелем, но и перемещение на расстоянии до нескольких метров от него.



# Использование **ФП1150** для охраны кабельной инфраструктуры



- ФП1150 используется для контроля кабельной инфраструктуры. Обнаружитель может использовать существующие оптические волокна в кабеле для обнаружения внешних воздействий в любом месте проложенного кабеля. ФП1150 определяет и сообщает точное местоположение такого события.
- Обеспечивая раннее предупреждение и точное местоположение инцидента, ФП1150 помогает предотвратить дорогостоящие перебои в обслуживании, повреждение кабельной инфраструктуры и кражу данных.
- ФП1150 также можно использовать для обнаружения местоположения кабелепровода путем мониторинга при воздействии на землю над предполагаемым местоположением кабелепровода.
- ФП1150 использует сложные алгоритмы для различения реальных угроз кабелю и вибраций от естественных источников.
- Алгоритмы обнаружения используют пороговые значения магнитуды возмущения, пространственные параметры и временные параметры. ФП1150 исключительно прост в настройке, что позволяет персоналу оптимизировать систему для конкретных условий применения.
- Обнаружитель работает, передавая импульсы лазерного света в одномодовое оптическое волокно и точно измеряя мельчайшие отражения света, происходящие по его длине.
- Нарушение волокна, вызванное вибрациями, изменяет количество света, возвращаемого из этой точки. Технология, основанная на рефлектометрии, не требует, чтобы свет проходил по всей длине кабеля. Если кабель перерезан, ФП1150 сохраняет способность обнаруживать и локализовать место вторжения вплоть до точки обрыва, что позволяет системе поддерживать конфигурации, устойчивые к повреждениям.

# Использование **ФП1150** для охраны кабельной инфраструктуры



## Особенности и преимущества ФП1150 для контроля кабельной инфраструктуры

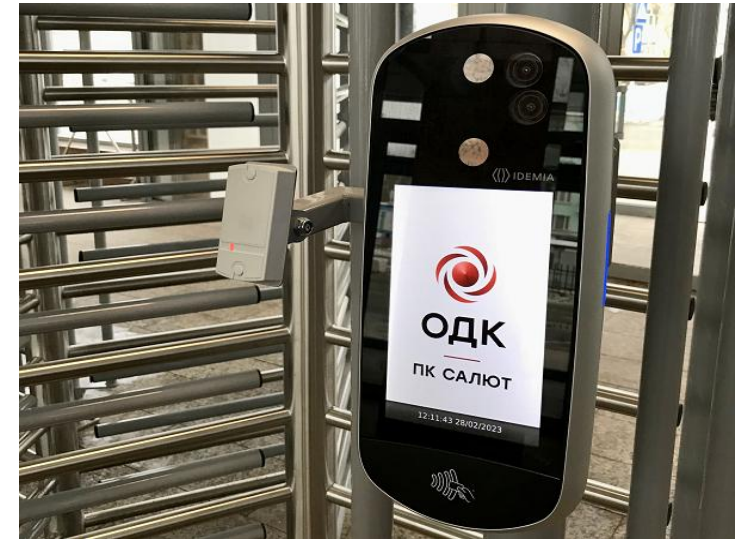
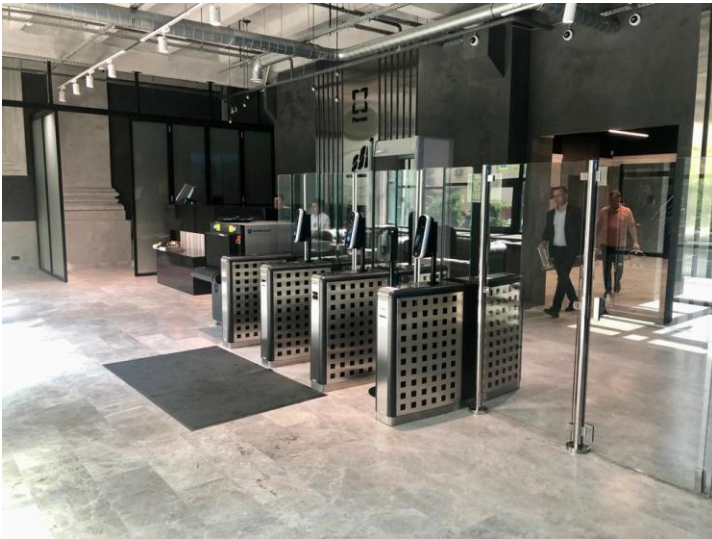
- Обнаружение и локализация событий, связанных с воздействием на кабельную инфраструктуру, таких как раскопки, присутствие тяжелых транспортных средств и прямые манипуляции с кабелями с целью перехвата данных или кражи кабеля.
- Дальность обнаружения воздействий – до 100 км от оптоволоконного сенсорного блока.
- Для измерения требуется только одно оптическое волокно в кабеле или группе кабелей.
- Регистрация событий с точностью  $\pm 4$  м.
- Точное определение местоположения нескольких одновременных вторжений.
- При повреждении кабеля обнаружитель продолжает работать до места физического обрыва кабеля.
- Высокая вероятность правильного обнаружения и низкая вероятность ложных тревог.
- Программно-конфигурируемые зоны обнаружения.
- Не требуется внешнее электроснабжение или вспомогательная инфраструктура.
- Не требуются точки заземления в местах прокладки оптоволоконного кабеля.
- Тревоги формируются по номерам зон, расстоянию по кабелю и/или координатам.
- Простая установка.
- Нет необходимости подключения к активным волокнам, нет возможности несанкционированного доступа к данным или искажения сигналов с помощью внешних воздействий.

# 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. Нижневартонск



- Подробное описание примеров внедрения – на сайте [www.secst.ru](http://www.secst.ru)

# Наши клиенты



# О КОМПАНИИ



**АО «СТАНДАРТ БЕЗОПАСНОСТИ» – технологический и бизнес-партнер компаний – лидеров российского рынка и государственных организаций**

Среди клиентов крупнейшие российские компании (из рейтинга РБК «500 крупнейших по выручке компаний России»), государственные структуры и международные корпорации

## 2002

год создания  
компании

## 100+

высоко-  
квалифицированных  
сотрудников

## 5

офисов разработки  
решений и  
обслуживания клиентов  
в России

## 300+

реализованных  
объектов



# 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](http://www.secst.ru)  
[info@secst.ru](mailto:info@secst.ru)