РЕКФЭЙСИС

ID-GATE

ТЕХНИЧЕСКОЕ ОПИСАНИЕ

IDGT.TI.DOC.990

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ (НАЗНАЧЕНИЕ) 3
2 ОПИСАНИЕ ПРОГРАММНОГО РЕШЕНИЯ 4
2.1 Компоненты Системы 4
2.2 Общая архитектура 4
2.3 Типовая архитектура развертывания 4
2.3.1 Внешняя система в режиме Master 5
2.3.2 Внешняя система в режиме Slave 6
2.4 Используемые технологии 7
2.5 Список сервисов Id-Gate Core 7
3 ТРЕБОВАНИЯ ДЛЯ КОРРЕКТНОЙ РАБОТЫ 9
3.1 Сервер Id-Gate 9
3.2 Установка оборудования 10
3.2.1 Рекомендации по установке терминалов 10
3.2.2 Рекомендации по установке камер 10
4 ЯЗЫКОВАЯ ПОДДЕРЖКА 12
5 ПЕРЕЧЕНЬ ДОКУМЕНТАЦИИ 12
6 ПРОИЗВОДИТЕЛЬ ПО 12

1 ВВЕДЕНИЕ (НАЗНАЧЕНИЕ)

Система Id-Gate (далее — «Система») разработана для биометрического подтверждения личности в системах контроля и управления доступом.

Id-Gate обогащает существующие или создаваемые СКУД дополнительными современными функциями с использованием технологии распознавания лиц, повышает достоверность идентификации и увеличивает простоту прохода для сотрудников/гостей.

Система Id-Gate предназначена для управления доступом на территории и объекты с помощью биометрической идентификации. Предоставляемые возможности позволяют организовать пропускной режим или улучшить процесс предоставления доступа сотрудникам в организациях или на предприятиях. Система обеспечивает совместную работу СКУД, биометрических терминалов и устройств на проходной, а также контроллеров турникетов и другого пропускного оборудования.

Система предназначена для:

- контроля, учета и управления доступом на объект посредством биометрической идентификации;
- возможности создания и ведения специализированных списков сотрудников и посетителей (VIP, черный список и другие);
- бесперебойной работы с отправкой мгновенных уведомлений службе безопасности при попытке несанкционированного прохода на объект человека, не попавшего в список допуска или, например, из «черного списка»;
- аналитики по количеству посетителей и времени нахождения на объекте;
- возможности разграничения прав доступа как сотрудников, так и посетителей в отдельные зоны объекта;
- возможности функционирования СКУД с интегрированной Системой распознавания лиц для снижения риска подделки карт сотрудников, их потери, передачи третьим лицам, доступа нескольких человек по одной карте;
- интеграции со СКУД с синхронизацией информации по сотрудникам: ФИО, карты доступа, фото и т. д. Реализованы интеграции с системами: Bosch Building Integration System, Honeywell Pro-Watch, Lenel OnGuard, Schneider Electric Security Expert, Perco, Dormakaba, Moxa, Robos, Sigur, Rusguard.

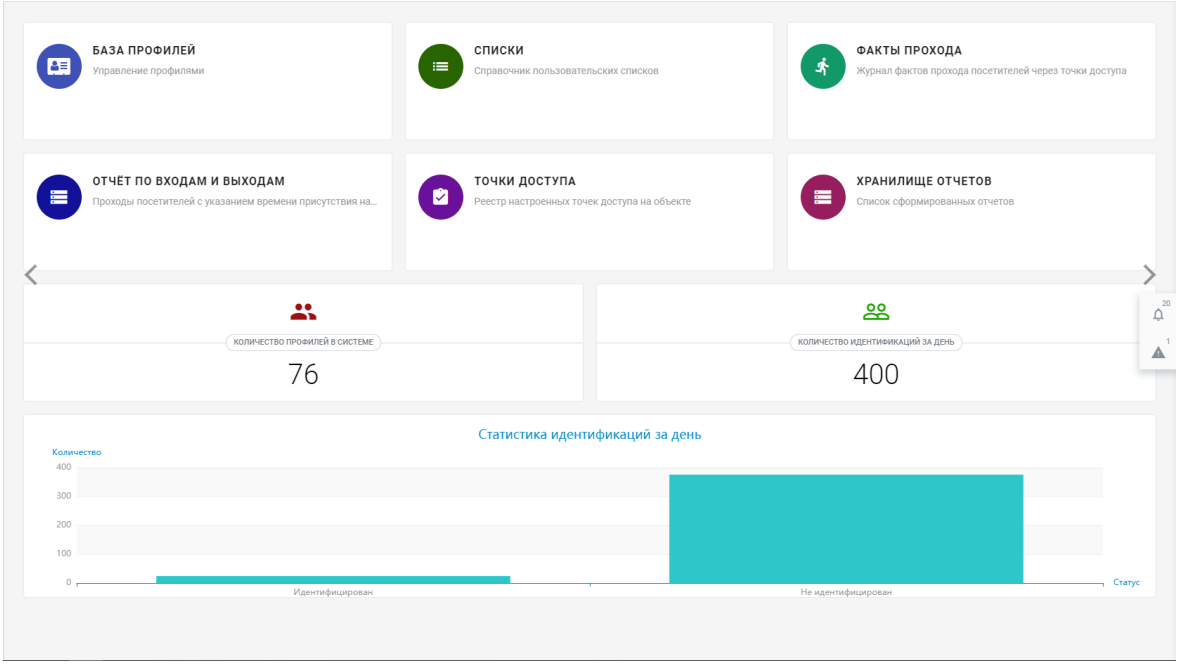

Рисунок 1. Рабочий стол Системы

2 ОПИСАНИЕ ПРОГРАММНОГО РЕШЕНИЯ

2.1 КОМПОНЕНТЫ СИСТЕМЫ

Для корректного функционирования Системы необходим следующий минимальный состав оборудования:

- сервер для ядра Системы;
- сервер(-ы) предобработки видео (при необходимости);
- ПК Операторов (при необходимости);
- камеры сетевые или USB в зависимости от назначения и архитектуры Системы;
- терминалы контроля доступа;
- сетевые коммутаторы для обеспечения передачи данных между компонентами Системы.

Подробное описание рекомендуемых характеристик оборудования указано ниже.

2.2 ОБЩАЯ АРХИТЕКТУРА

Система состоит из следующих компонентов:

- **Id-Gate Core** — серверная часть Системы, состоящая из отдельных сервисов, включающих в себя интерфейс настройки Системы, алгоритмы распознавания, базу данных и отчеты;
- **Id-Gate Tracker** — сервер предобработки видео;
- **ACS Adapter** — сервис, обеспечивающий обмен данными с внешней системой и отправку уведомлений;
- **Id-Gate Terminal** — приложение для ОС Android, отвечающее за взаимодействие с терминалами на проходной и контроль доступа в режиме offline.

Система может быть интегрирована:

- со СКУД
- с реле турникета или другого проходного устройства
- с терминалом
- с Wiegand

Схемы архитектуры Системы при разных вариантах использования представлены ниже.

2.3 ТИПОВАЯ АРХИТЕКТУРА РАЗВЕРТЫВАНИЯ

Перед развертыванием Системы и настройкой интеграции со СКУД (ACS) требуется определить основные источники мастер-данных в зависимости от планируемых алгоритмов функционирования Системы в целом. А именно: определить, где будут вводиться первичные данные (Master), в каком порядке и с какими системами они должны синхронизироваться. В общем случае Id-Gate позволяет настроить интеграцию, определив внешние подключаемые системы в режимах ведущей (Master), ведомой (Slave), а также в комбинированном режиме.

2.3.1 ВНЕШНЯЯ СИСТЕМА В РЕЖИМЕ MASTER

Для случаев, когда интегрируемая СКУД является источником мастер-данных о профилях, картах доступа и фотографиях профилей, в настройках Id-Gate для адаптера соответствующей СКУД включается режим **Master**. Для такой интеграции производится двухсторонний обмен данными между системами. Схема такого решения показана ниже (**Рисунок 2**).

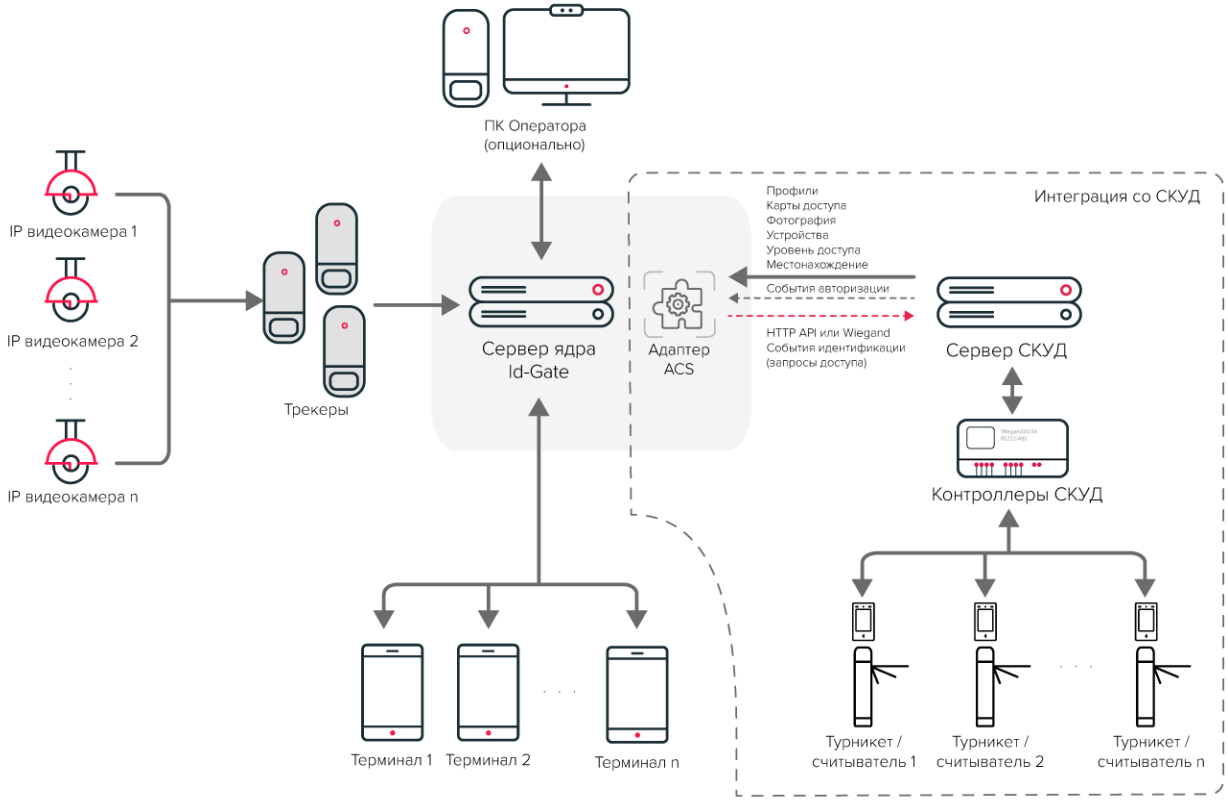

Рисунок 2. Схема развертывания интеграции Id-Gate с внешней системой в режиме Master

На стороне СКУД ведется база сотрудников и посетителей с фотографиями и идентификационными картами, вводится информация о местонахождениях исполнительных устройств, уровнях доступа, а также данные о считывателях и контроллерах. Информация из СКУД в результате периодической синхронизации поступает в Id-Gate, обновляя информацию об устройствах, местоположениях исполнительных устройств, профилях и уровнях доступа.

На стороне Id-Gate в режиме реального времени производится обработка потоков с камер видеонаблюдения, подключенных к Системе, а также с терминалов. По результатам работы подсистемы биометрии выполняется идентификация всех обнаруженных лиц по базе профилей, синхронизированной со СКУД. Возникающие события идентификации проверяются по набору настроенных правил, уровней доступа по устройствам и в результате обработки формируются события, которые отправляются в СКУД. В зависимости от настроек это могут быть команды через HTTP API или команды для Wiegand на открытие устройств доступа (турникеты, двери, шлагбаумы), которые подключены к СКУД.

2.3.2 ВНЕШНЯЯ СИСТЕМА В РЕЖИМЕ SLAVE

Для случаев, когда Id-Gate является источником мастер-данных о профилях, картах доступа и фотографиях профилей, интегрируемая внешняя система включается в режиме **Slave**. Для такой интеграции производится двухсторонний обмен данными между системами. Схема такого решения показана ниже (**Рисунок 3**).

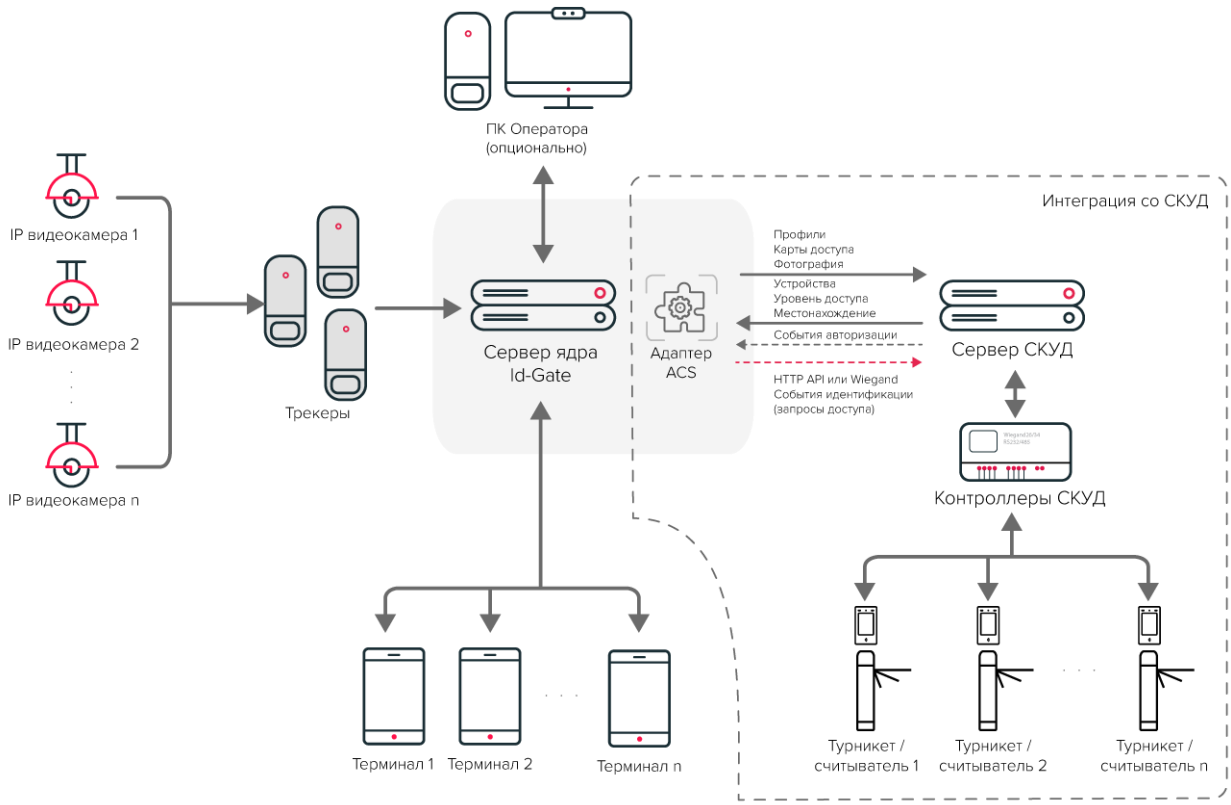

Рисунок 3. Схема развертывания интеграции Id-Gate с внешней системой в режиме Slave

На стороне Id-Gate ведется база профилей с фотографиями и картами доступа. В режиме реального времени производится обработка потоков с камер видеонаблюдения, подключенных к Системе, а также с терминалов. По результатам работы подсистемы биометрии выполняется идентификация всех обнаруженных лиц.

На стороне СКУД вводится информация об устройствах (контроллерах, считывателях, исполнительных устройствах), местонахождениях исполнительных устройств и уровнях доступа. В результате периодической синхронизации информация о правах доступа и устройствах доставляется в Id-Gate и должна быть применена для формирования правил обработки событий идентификации.

Возникающие события идентификации на стороне Id-Gate или поступившие из внешней системы события авторизации проверяются по набору настроенных правил, уровней доступа по устройствам, и в результате обработки формируются команды на предоставление или отказ доступа, которые отправляются во внешнюю систему. В зависимости от настроек это могут быть команды через HTTP API или команды для Wiegand на открытие устройств доступа (турникеты, двери, шлагбаумы), которые подключены к внешней системе.

ВНИМАНИЕ! Перед настройкой внешней системы в режиме Slave необходимо обязательно выполнить полное резервное копирование подключаемой СКУД. Система Id-Gate, работающая в режиме Master, автоматически заменит все данные в подключаемой системе при первой синхронизации.

2.4 ИСПОЛЬЗУЕМЫЕ ТЕХНОЛОГИИ

Система разработана с использованием следующих языков программирования и ПО:

- Golang
- C#
- AngularJS
- Rabbit MQ
- Nginx
- PostgreSQL
- Redis

2.5 СПИСОК СЕРВИСОВ ID-GATE CORE

Id-Gate Core включает в себя следующие сервисы:

Таблица 1. Описание сервисов Id-Gate Core

Сервис	Описание	Порт
Nginx	Веб-сервер и почтовый прокси-сервер	80, 443, 23231
PostgreSQL	Свободная объектно-реляционная система управления базами данных (СУБД)	5432
RabbitMQ	Сервис, обеспечивающий работу с очередями данных	5672, 15672
Redis	Система управления базами данных класса NoSQL с открытым исходным кодом	6379
mkvz-tracker	Сервис предобработки потокового видео (трекер)	8001
mkvz-launcher	Сервис управления клиентскими приложениями	8876
mkv-server-report	Сервис отчетов	11084
mu-server-api	Сервис уведомлений	11090
support-server-api	Сервис обслуживания системы	11091
mkv-server-url-shortener	Сервис для укорачивания URL	11092
mas-server-api	Back-end для модуля администрирования системы	11101
mas-server-settings	Сервис настроек	11102
mpdn-secret-vault-api	Сервис хранения персональных данных	11204
mdc-server-api	Сервис работы с динамическими классификаторами	11205
mfs-server-api	Сервис работы с файлами фотографий	11300
mfs-server-thumbnail	Сервис для работы с миниатюрами фотографий файлового хранилища	11301
fs-server-api	Сервис файлового хранилища	11302
mi-sender-email	Сервис отправки email	11400
mi-sender-http	Сервис отправки сообщения по http	11401
mi-sender-smsmodem	Сервис отправки SMS с помощью usb gsm модема	11402
mi-server-api	Сервис реализатор функций API для работы с сервисами	11403
mi-sender-telegram	Сервис отправки сообщений в Telegram	11404
mi-controller-acs	Бизнес интегратор и реализатор маршрутизации запросов	11406

mi-adapter-acs-biostar2	Сервис адаптера интеграции со СКУД Biostar2	11413
mi-adapter-acs-moxa	Сервис адаптера интеграции с Moxa 1214	11414
mi-adapter-acs-suprema-fs2	Сервис-адаптер	11415
mi-adapter-acs-honeywell-pro-watch	Сервис адаптера интеграции со СКУД Honeywell Pro Watch	11416
mi-adapter-acs-bosch	Сервис адаптера интеграции со СКУД Bosch BIS	11417
mi-adapter-acs-se	Сервис адаптера интеграции со СКУД Security Expert	11418
mi-adapter-acs-sigur	Сервис адаптера интеграции со СКУД Sigur	11419
mi-adapter-acs-exos	Сервис адаптера интеграции со СКУД Dormakaba EXOS	11421
mi-adapter-acs-onguard	Сервис адаптера интеграции со СКУД Lenel OnGuard	11422
mi-adapter-acs-rusguard	Сервис адаптера интеграции со СКУД RusGuard	11424
mi-adapter-acs-bolid	Сервис-адаптер	11436
mkv-server-admin	Сервис пользовательского администрирования системы	11500
mkv-server-api	Сервис клиентского взаимодействия	11501
mkv-server-auth	Сервис авторизации	11502
mkv-server-ws	Back-end для приложения работы с клиентом через WebSocket	11503
backup-client-server-api	Сервис резервного копирования	11506
logging-server-api	Сервис логирования	11509
event-configuration-api	Сервис настройки обработчика событий системы	11510
event-storage-server-api	Сервис обработчик событий системы	11511
mkv-client-profiles-import	Сервис импорта профилей	11514
mas-meta-server-api	Сервис мета информации	11515
monitoring-server-api	Сервис мониторинга	11517
statistics-server-api	Сервис ведения статистики о работе системы	11518
audit-server-api	Сервис аудита и логирования	11521
mkv-server-auth-ldap	Сервис авторизации в системе через LDAP/AD	11522
mkvz-onvif-cameras	Сервис поиска и подключения камер по протоколу ONVIF	11550
discovery-server-api	Сервис поиска мобильных приложений DSN-SD	11551
adb-server-api	Сервис управления мобильных приложений по протоколу ADB	11552
mas-server-report	Сервис отчетов для MAS	11553
medical-server-api	Сервис медицинского контроля	11554
mie-export-api	Сервис экспорта настраиваемых наборов данных в CSV	11555
mie-import-api	Сервис импорта настраиваемых наборов данных из CSV	11556
logging-server-siem	Сервис логирования SIEM	11557
mmpd	Сервис менеджер процессов детектирования	11600
mobile-service-api	API работы с мобильными приложениями	11601
gate-server-api	Сервис процессов предоставления доступа	11602
compromise-server-api	Сервис контроля компрометации	11605
modi-image-worker	Сервис обработки фотографий	11700
modi-server-api	Сервис обработки дискретных изображений	11701

modi-ubda-tevian-[01-04]	Сервис обработки фотографий	11710 у [01], 11711 у [02], 11712 у [03], 11713 у [04]
modi-ubda-tevian-alg1	Сервис обработки фотографий	11714
mrp-server-api	Сервис обработки данных	11800
mrp-server-ubt-broker	Сервис проксирования UBT в другие системы	11801
mrp-matching-tevian-go	Сервис матчинга для движка Tevian	11806
mrp-server-broker	Сервис управления	11821
mrp-server-image-broker	Сервис распределения изображений по трекерам	11822
ms-server-filecache	Сервис кэширования	11900
mkv-scheduler-api	Сервис, реализующий работу с задачами по расписанию	11910
video-restreamer-server	Сервис ретрансляции видео	40000, 40001

Одним из требований к серверу для установки программного комплекса Id-Gate Core является отсутствие на сервере ПО, указанного в таблице выше, и наличие свободных портов, указанных в таблице.

3 ТРЕБОВАНИЯ ДЛЯ КОРРЕКТНОЙ РАБОТЫ

3.1 СЕРВЕР ID-GATE

На сервер производится установка Id-Gate Core. Характеристики сервера напрямую зависят от количества обрабатываемой Системой информации, полученной с камер. Примерный расчет для наиболее частых значений представлен в таблице ниже.

Таблица 2. Требования к серверу

Количество камер	CPU (Core)	RAM (GB)	HDD (GB)	SSD (GB)
1	5	16	600	240
2	6	16	700	240
3	8	16	700	240
5	10	32	800	240
7	14	32	900	240
10	18	64	1000	240

Операционная система: Windows 10 Pro (2004 и выше, согласно срокам окончания поддержки операционных систем), Windows Server 2016/2019 и выше, Ubuntu 20.04 или выше, Astra Linux 1.7 SE. Если у вас установлена редакция ОС Windows 10 Pro N, дополнительно необходимо установить компонент Media Feature Pack. Учетная запись (логин/пароль) (в т. ч. для удаленного пользователя) должна оставаться неизменной на протяжении всей инсталляции. Учетная запись (логин/пароль) должна позволять повышать привилегии до Администратора при необходимости.

Не должно быть предустановлено:

- Postgre SQL
- Rabbit MQ
- Redis
- Web server, использующий 80 и 443 порты

3.2 УСТАНОВКА ОБОРУДОВАНИЯ

3.2.1 РЕКОМЕНДАЦИИ ПО УСТАНОВКЕ ТЕРМИНАЛОВ

При установке терминалов внутри помещений устройство необходимо разместить на расстоянии не менее 2 метров от источника света для исключения засветок и бликов и не менее 0,3–0,5 метра от окна или двери (**Рисунок 4**).

При установке терминала избегать:

- сильной задней засветки;
- попадания на терминал прямых солнечных лучей;
- близкого расположения ярких источников света.

Монтажная поверхность должна выдерживать нагрузку, в два раза превышающую вес оборудования.

Рекомендуемая высота установки терминала: 1,45–1,55 м от уровня пола до встроенного в терминал модуля с камерами. Указанная высота установки терминала является рекомендуемой и может быть изменена по вашим потребностям.

Во время установки необходимо обеспечить безопасность используемого оборудования и монтажных средств.

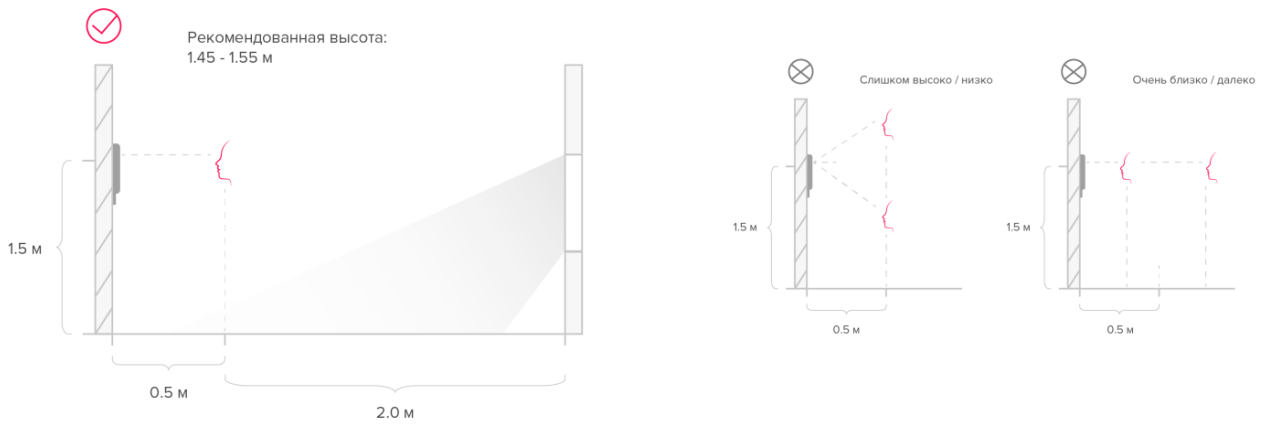

Рисунок 4. Рекомендации по установке терминала

3.2.2 РЕКОМЕНДАЦИИ ПО УСТАНОВКЕ КАМЕР

- Видеокамера должна быть жестко зафиксирована с помощью специального кронштейна, чтобы максимально уменьшить эффект смазывания, вызываемый движением камеры. Допускается размещение видеокамеры на штативе, высота установки камеры при этом от 1,5 до 2 м.
- Рекомендуемое расположение видеокамеры: объектив камеры должен смотреть в направлении людей таким образом, чтобы объекты двигались в направлении камеры вдоль линии визирования.
- Путь движения человека не должен блокироваться дисплеями, информационными стойками, табло, баннерами.
- Для целей распознавания и идентификации предпочтительней использовать видеокамеры с варифокальными объективами.
- Фокусное расстояние объектива необходимо выбирать в диапазоне 9–40 мм.
- Угол наклона видеокамеры в конце области определения лиц должен быть в пределах 15°.
- Оптимальная высота установки видеокамеры от пола — 2,2 м, желательно, чтобы начало области определения лиц располагалось далее 8,0–8,5 м.

- Внутри помещения должен быть обеспечен равномерный и постоянный уровень освещенности. Для оптимального распознавания лиц рассеянное освещение должно быть таким, чтобы лица объектов имели равномерное освещение без теней или бликов. Рекомендованная интенсивность света должна составлять около 300 люкс (минимум 150 люкс, максимум 600 люкс).
- В начальной позиции определения лиц необходимо установить и настроить видеокамеру таким образом, чтобы размер лица взрослого человека составлял 160x160 пикселей (поле зрения в ширину более 2 метров — чуть шире, чем расстояние расправленных в стороны рук).

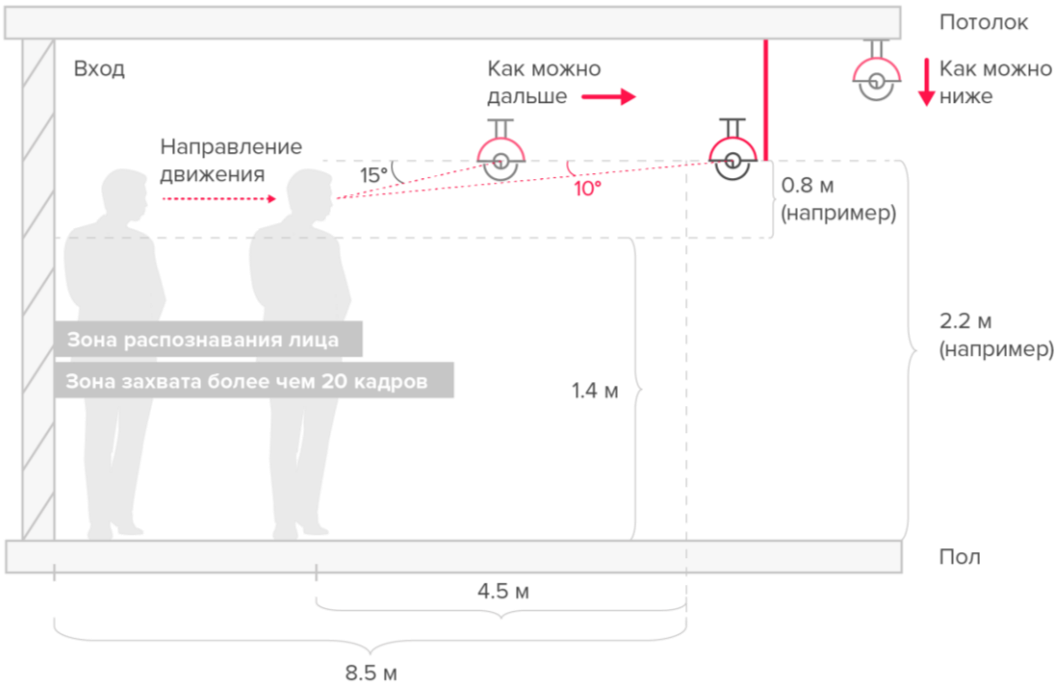

Рисунок 5. Расположение видеокамеры в вертикальной плоскости

4 ЯЗЫКОВАЯ ПОДДЕРЖКА

Программное обеспечение Id-Gate является мультиязычным и позволяет в процессе эксплуатации выполнить выбор среди доступных языков:

- английский (по умолчанию)
- испанский
- русский

Перечень доступных языков может быть дополнен по запросу.

5 ПЕРЕЧЕНЬ ДОКУМЕНТАЦИИ

- Руководство Администратора Id-Gate
- Руководство Оператора Id-Gate
- Руководство пользователя приложения для терминалов с ОС Android

6 ПРОИЗВОДИТЕЛЬ ПО

ООО «РекФэйсис»

Адрес: 119334, г. Москва, 5-й Донской проезд 21Б, стр.10

Тел.: +7 (495) 268-08-93

E-mail:

- Общие вопросы: in@recfaces.com
- Лицензирование и партнерская программа: sales@recfaces.ru
- Технические вопросы и поддержка по продукту: id-gate@recfaces.ru