РЕКФРЭЙСИС

ID-LOGON

ТЕХНИЧЕСКОЕ ОПИСАНИЕ

IDLG.TI.DOC.990

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ (НАЗНАЧЕНИЕ)

Система Id-Logon (далее — «Система») разработана для обеспечения биометрического контроля доступа в операционную или информационные системы.

Решение предназначено для проверки прав доступа в системы при помощи биометрической идентификации и верификации и обеспечивает достоверность данных о личности, находящейся перед компьютером. Предоставление доступа в операционную или информационные системы через биометрическое подтверждение личности исключает риск подмены пользовательских данных.

Идентификация пользователя производится через специально установленные веб-камеры/сканеры на компьютере путем «захвата» биометрических данных человека. Затем Id-Logon выполняет проверку на соответствие полученных образцов с данными в базе профилей. По результатам проверки человеку либо предоставляется доступ в систему, либо отказ в доступе.

Верификация доступа в систему осуществляется с использованием биометрии и через ввод пароля.

Решение предназначено для:

- безопасной биометрической аутентификации пользователей в различных корпоративных информационных системах;
- удобной беспарольной аутентификации с использованием биометрических данных пользователей;
- использования дополнительного режима двухфакторной аутентификации: через биометрические данные и пин-код/пароль;
- периодической проверки статуса пользователя, находящегося перед экраном клиентского устройства;
- выполнения различных сценариев ограничения доступа и информирования службы информационной безопасности при несоответствии статуса пользователя;
- оперативного уведомления служб информационной безопасности при работе более чем одного пользователя с клиентским устройством;
- своевременной обработки вызовов от информационных корпоративных и DLP-систем на биометрическую верификацию пользователя при совершении значимых операций или подозрении на возможную утечку информации;
- интеграции с Microsoft Active Directory (готовая интеграция); также возможна интеграции с другими LDAP-каталогами, такими как: Oracle Internet Directory, IBM Tivoli Directory Server;
- дополнительной проверки прихода сотрудника в офис организации при выполнении аутентификации в информационных системах путем взаимодействия с Id-Gate — программным продуктом оснащения биометрическими возможностями систем контроля доступа.

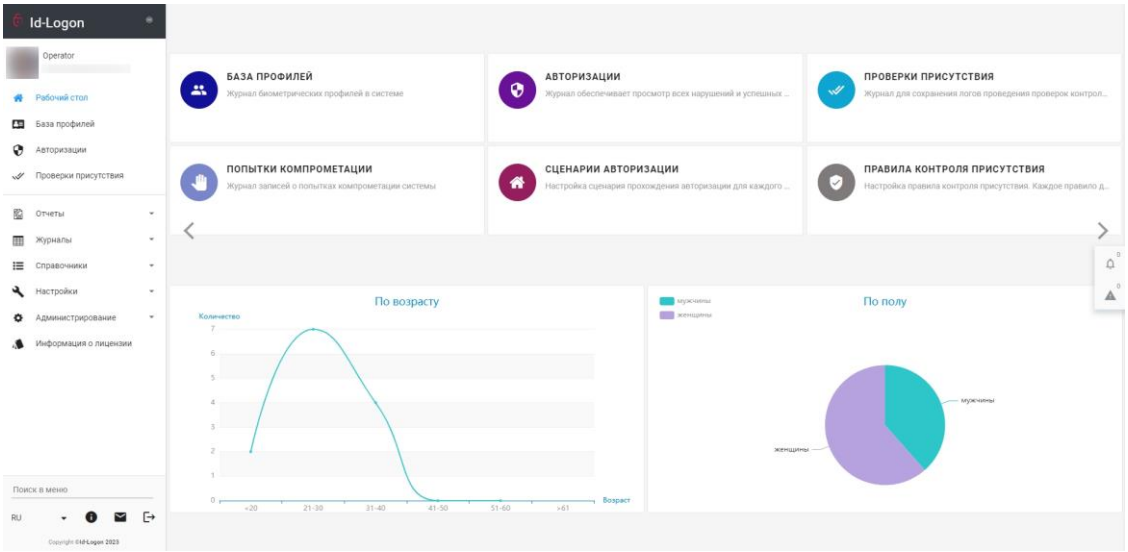

Рисунок 1. Рабочий стол Системы

2 ОПИСАНИЕ ПРОГРАММНОГО РЕШЕНИЯ

2.1 КОМПОНЕНТЫ СИСТЕМЫ

Для корректного функционирования Системы необходим следующий минимальный состав оборудования:

- сервер для ядра Решения;
- сервер(-ы) предобработки видео (при необходимости);
- клиентский ПК;
- камеры;
- 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-Logon Core** — серверная часть Системы, состоящая из отдельных сервисов, включающих в себя интерфейс настройки Системы, алгоритмы распознавания, базу данных и отчеты;
- **Id-Logon Tracker** — сервер предобработки видео;
- **WinLogon** — клиентское приложение для ОС Windows, обеспечивающее биометрическую аутентификацию для доступа в операционную систему Windows;
- **AppLogon** — клиентское приложение для ОС Windows, обеспечивающее биометрическую аутентификацию для доступа в приложения и информационные системы;
- **UserControl** — клиентское приложение для ОС Windows, обеспечивающее биометрический контроль присутствия и иных правил нахождения за ПК.

Система может быть интегрирована с:

- **Active Directory (LDAP)**, с помощью адаптера, поставляемого в комплекте с Решением.

2.3 СХЕМЫ ОРГАНИЗАЦИИ СИСТЕМЫ

2.3.1 ОБЩАЯ СХЕМА

Id-Logon обеспечивает аутентификацию в операционной системе или корпоративном приложении с использованием локальных или доменных учетных данных и локальной web-камеры, а также позволяет реализовать контроль присутствия за ПК с помощью web-камеры персонально или IP-камеры для контроля группы сотрудников (**Рисунок 2**).

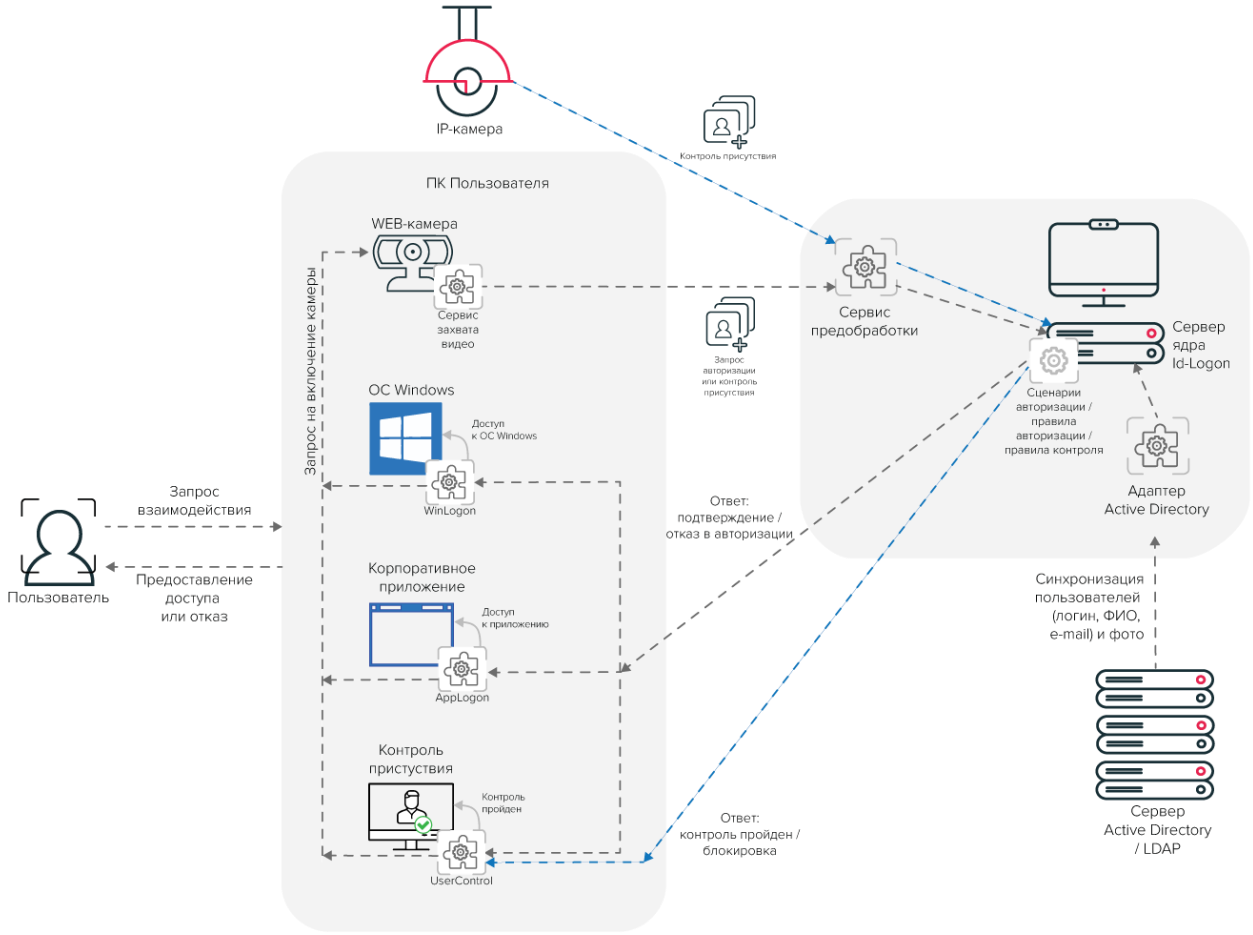

Рисунок 2. Общая схема развертывания системы Id-Logon

Для реализации соответствующих возможностей на локальный ПК пользователя необходимо установить следующие приложения из комплекта поставки:

- **WinLogon** — приложение для аутентификации в ОС Windows;
- **AppLogon** — приложение для аутентификации в корпоративной ИС и специализированные приложения;
- **UserControl** — приложение для обеспечения контроля присутствия или иных правил нахождения за ПК. UserControl может автоматически заблокировать ПК в случае выявления нарушения правил контроля.

2.3.2 РЕШЕНИЕ ДЛЯ АУТЕНТИФИКАЦИИ В WINDOWS ЧЕРЕЗ WINLOGON

Клиентское приложение WinLogon обеспечивает биометрическую аутентификацию для доступа в операционную систему Windows.

Схема развертывания Решения содержит следующие шаги (**Рисунок 3**):

- приложение WinLogon в соответствии со своими настройками инициирует запрос на включение web-камеры;
- с видеопотока камеры данные фиксируются (в зависимости от настроек) сервисом захвата видео и передаются в сервис предобработки видео, где предварительно обрабатываются с использованием процессорных мощностей ПК клиента;
- обработанные фото и биометрические шаблоны отправляются на сервер ядра Id-Logon, где производится идентификация и (или) верификация пользователя;
- на основе результата идентификации и настроенных сценариев авторизации Система предоставляет или отказывает в доступе и возвращает на ПК клиента ответ;
- на основании полученного ответа сервис предоставляет доступ или отклоняет запрос пользователя на вход в ОС Windows.

Сервер ядра с помощью специального адаптера может быть интегрирован с Active Directory (LDAP), который становится первичным источником сведений о пользователях, их правах доступа, списках доступа и фото. На основании этих сведений в Id-Logon заполняются как база профилей, так и различные справочники, определяющие доступ к системам.

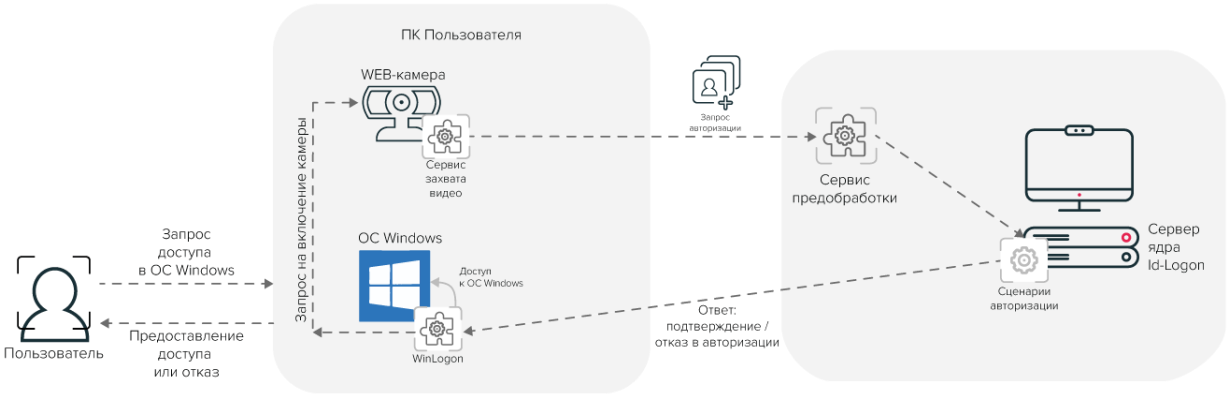

Рисунок 3. Схема развертывания решения для аутентификации пользователя в ОС Windows

2.3.3 РЕШЕНИЕ ДЛЯ АУТЕНТИФИКАЦИИ В КОРПОРАТИВНОМ ПРИЛОЖЕНИИ ЧЕРЕЗ APPLOGON

Сервис AppLogon обеспечивает биометрическую аутентификацию по лицу в одном или нескольких приложениях, определяемых настройками Системы.

Схема развертывания Решения в данном случае практически идентична упомянутой выше схеме аутентификации пользователя через приложение WinLogon (**Рисунок 4**):

- приложение AppLogon в соответствии со своими настройками инициирует запрос на включение web-камеры;
- с видеопотока камеры данные фиксируются (в зависимости от настроек) сервисом захвата видео и передаются в сервис предобработки видео, где предварительно обрабатываются с использованием процессорных мощностей ПК клиента;
- обработанные фото и биометрические шаблоны отправляются на сервер ядра Id-Logon, где производится идентификация и (или) верификация пользователя;
- на основе результата идентификации и настроенных правил для приложений авторизации Система предоставляет или отказывает в доступе и возвращает на ПК клиента ответ;
- на основании полученного ответа сервис предоставляет доступ или отклоняет запрос пользователя на вход в корпоративное приложение.

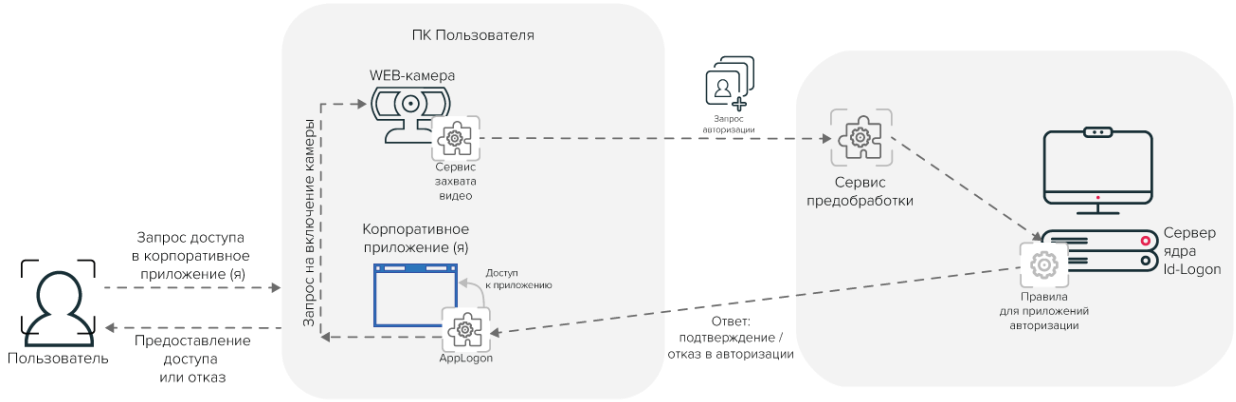

Рисунок 4. Схема развертывания решения для аутентификации пользователя в выбранном приложении

2.3.4 РЕШЕНИЕ ДЛЯ КОНТРОЛЯ ПРИСУТСТВИЯ ЧЕРЕЗ USERCONTROL

Сервис UserControl предназначен для биометрического контроля присутствия/отсутствия пользователя за рабочим местом, а также нахождения перед компьютером посторонних (**Рисунок 5**).

Решение с использованием UserControl работает следующим образом:

- сервис UserControl в соответствии со своими настройками инициирует запрос на включение web-камеры;
- с видеопотока камеры данные фиксируются (в зависимости от настроек) Сервисом захвата видео и передаются в Сервис предобработки видео и предварительно обрабатываются с использованием процессорных мощностей ПК клиента;
- обработанные фото и биометрические шаблоны отправляются на сервер ядра Id-Logon, где производится идентификация и (или) верификация пользователя, а также проверка на соответствие Правилам контроля присутствия;
- на основе результата идентификации и настроенных правил Решение возвращает на ПК клиента ответ;
- на основании полученного ответа сервис фиксирует успешно пройденную проверку в журнале проверок присутствия или блокирует доступ по факту нарушения правил контроля.

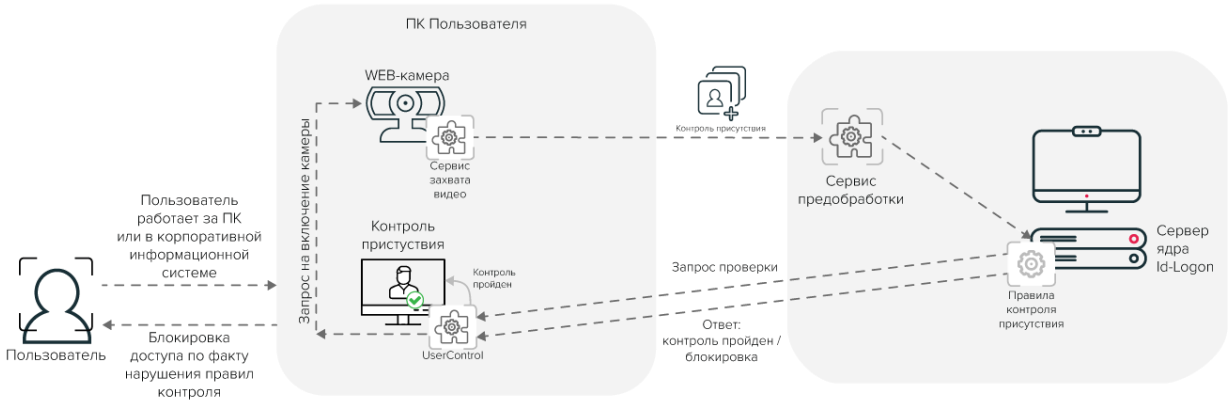

Рисунок 5. Схема развертывания решения для контроля присутствия через UserControl

2.3.5 РЕШЕНИЕ ДЛЯ КОНТРОЛЯ ПРИСУТСТВИЯ С ПОМОЩЬЮ IP-КАМЕРЫ

В случае если ПК пользователей не оснащены web-камерами, есть возможность установить одну IP-камеру для контроля присутствия группы сотрудников. В этом случае на каждом компьютере должен быть установлен сервис UserControl.

Подробные шаги развертывания Решения (**Рисунок 6**):

- сервис UserControl в соответствии со своими настройками инициирует запрос на считывание данных IP-камерой;
- с видеопотока камеры данные передаются в Сервис предобработки видео и предварительно обрабатываются с использованием процессорных мощностей ПК клиента;
- обработанные фото и биометрические шаблоны отправляются на сервер ядра Id-Logon, где производится идентификация и (или) верификация пользователя, а также проверка на соответствие Правилам контроля присутствия;
- на основе результата идентификации и настроенных правил Решение возвращает на ПК клиента ответ;
- на основании полученного ответа сервис фиксирует успешно пройденную проверку в журнале проверок присутствия или блокирует доступ по факту нарушения правил контроля.

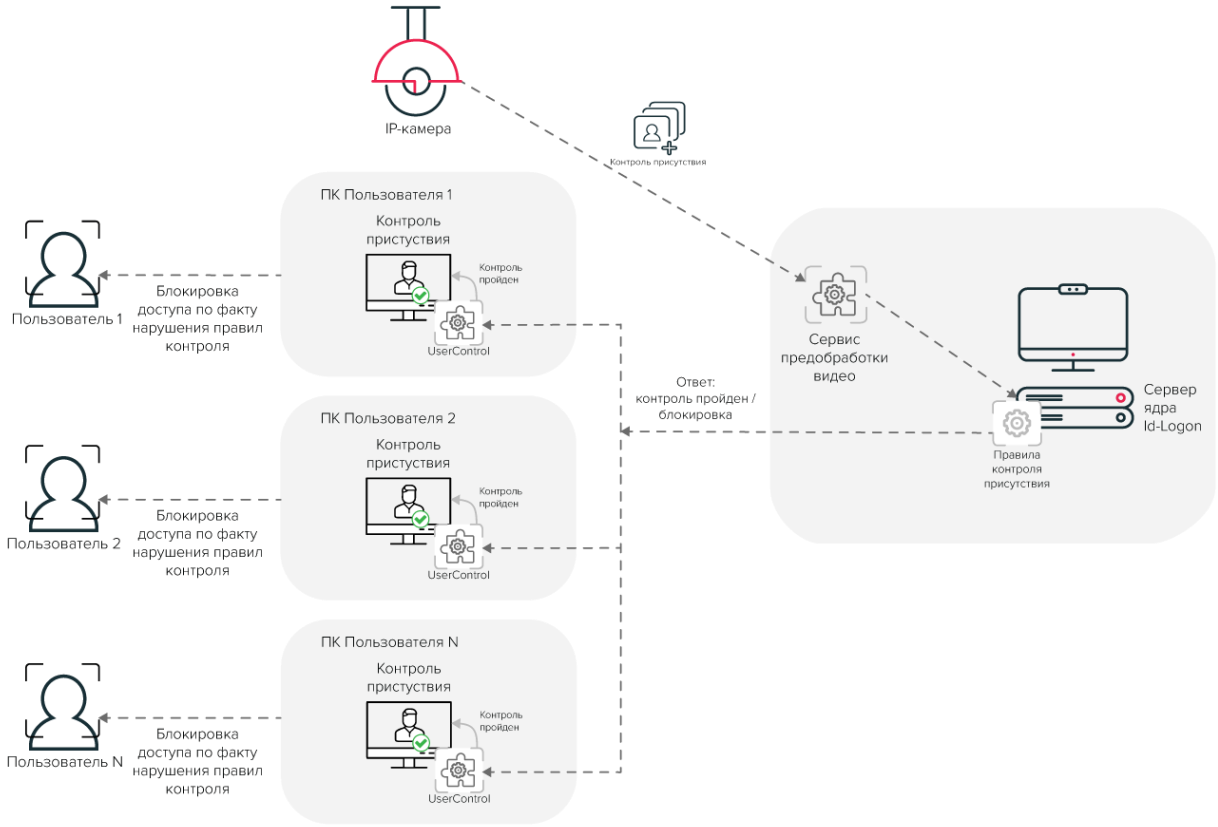

Рисунок 6. Схема развертывания решения для контроля присутствия с помощью IP-камеры

2.4 ИСПОЛЬЗУЕМЫЕ ТЕХНОЛОГИИ

Система разработана с использованием следующих языков программирования и ПО:

- Golang
- C#
- Angular JS
- Rabbit MQ
- Nginx
- PostgreSQL
- Redis

2.5 СПИСОК СЕРВИСОВ ID-LOGON CORE

Id-Logon Core включает в себя следующие сервисы:

Таблица 1. Описание сервисов Id-Logon Core

Название	Наименование	Внутренний порт
mauth-win-logon	Клиентское приложение для аутентификации в Windows	Отсутствует
mauth-client-app-config	Сервис клиентских настроек	Отсутствует
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
mauth-server-api	Сервис для управления выполнения аутентификаций в Windows и приложениях	11200
mauth-server-report	Сервис формирования отчетов ПО	11201
user-control-server-api	Сервис контроля	11202
user-control-server-report	Сервис построения отчетов для модуля user контроля	11203
mpdn-secret-vault-api	Сервис хранения персональных данных	11204
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-controller-idm	Бизнес интегратор и реализатор маршрутизации запросов	11407
mi-adapter-idm-ad	Адаптер для интеграции с AD	11431
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
mas-server-report	Сервис отчетов для MAS	11553
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
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]
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-Logon 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-LOGON

На сервер производится установка Id-Logon Core. Характеристики сервера напрямую зависят от количества обрабатываемых Системой 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. 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.

Также на сервере **не должны** быть предустановлены:

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

3.2 РЕКОМЕНДАЦИИ ПО ИСПОЛЬЗОВАНИЮ КАМЕР

3.2.1 ВЫБОР КАМЕРЫ

Камера должна обладать следующими характеристиками:

- разрешение получаемого изображения: не менее 720p;
- частота кадров видеопотока: не менее 25 fps;
- угол обзора: не меньше 65 градусов, рекомендуется 75 и выше;
- наличие ИК подсветки (опционально);
- фокус: фиксированный/автофокус;
- **без** эффекта «рыбий глаз»;
- соотношение сторон 16:9.

Для обеспечения естественной цветопередачи кожи рекомендуется, чтобы цветовая температура приборов освещения составляла 4800–6500К и была однородной (одинаковой во всем помещении). Требуемая цветовая температура обеспечивается люминесцентными или светодиодными источниками освещения.

Используемые источники освещения должны создавать в области лица освещенность:

- для камер без автоматической коррекции освещенности не менее 300 лк;
- для камер с автоматической коррекцией освещенности не менее 100 лк.

3.2.2 УСТАНОВКА КАМЕРЫ

При получении лицевых биометрических данных необходимо выполнить условия (**Рисунок 7**):

- камера должна находиться на уровне глаз;
- сотрудник должен смотреть прямо в камеру, держать голову прямо и плечи ровно по отношению к камере;
- лицо должно быть равномерно освещено, чтобы на изображении отсутствовали тени, блики, области пересвета;
- на изображении должно присутствовать только одно лицо;
- выражение лица должно быть нейтральным (без улыбки), оба глаза нормально открыты (т. е. не широко) и четко различимы (волосы не должны падать на глаза, рот должен быть закрыт);
- отсутствие яркого контрового, бокового света и теней;
- расстояние между зрачками на изображении должно составлять не менее 120 пикселей.

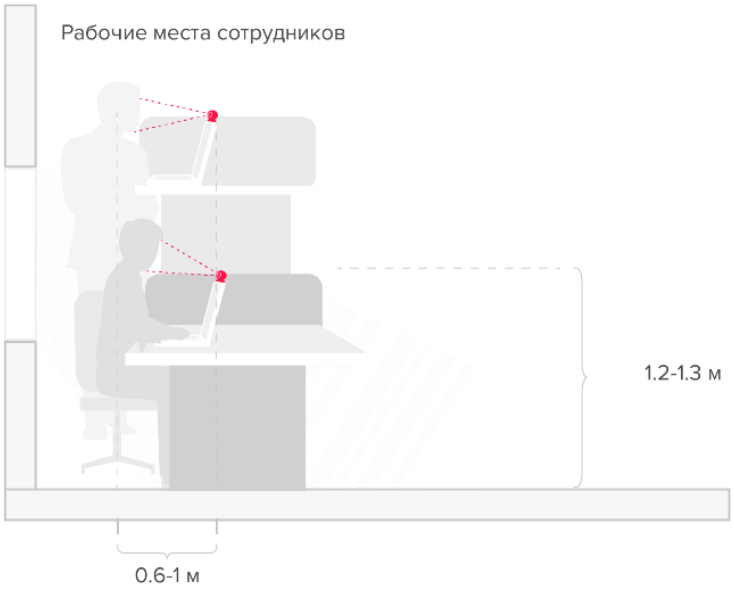

Рисунок 7. Рекомендации по размещению камер

4 ЯЗЫКОВАЯ ПОДДЕРЖКА

Программное обеспечение Id-Logon 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-Logon
- Руководство Оператора Id-Logon
- Руководство по установке и настройке приложения WinLogon
- Руководство по установке и настройке приложения AppLogon
- Руководство по установке и настройке приложения UserControl

6 РАЗРАБОТЧИК 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-logon@recfaces.ru