



ПРАВИТЕЛЬСТВО МОСКВЫ

**ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
ГОРОДА МОСКВЫ**

**ДЕПАРТАМЕНТ ГРАДОСТРОИТЕЛЬНОЙ ПОЛИТИКИ ГОРОДА
МОСКВЫ**

РАСПОРЯЖЕНИЕ

27 июня 2025 г.

№ 64-16-307/25/22

Об утверждении Порядка функционирования и установки биометрических систем контроля и управления доступом на контрольно-пропускных пунктах строительных площадок и Технических требований к биометрическим системам контроля и управления доступом, устанавливаемых на контрольно-пропускных пунктах строительных площадок

В соответствии с решением Антитеррористической комиссии города Москвы от 30 апреля 2025 г. в целях повышения антитеррористической защищенности на строительных площадках:

1. Утвердить Порядок функционирования и установки биометрических систем контроля и управления доступом на контрольно-пропускных пунктах строительных площадок согласно приложению 1 к настоящему распоряжению.

2. Утвердить Технические требования к биометрическим системам контроля и управления доступом, устанавливаемых на контрольно-пропускных пунктах строительных площадок согласно приложению 2 к настоящему распоряжению.

3. Департамент информационных технологий города Москвы определить уполномоченным органом исполнительной власти города Москвы, ответственным за определение технических требований к передаче информации из биометрических систем контроля и управления доступом, устанавливаемых на контрольно-пропускных пунктах строительных площадок (далее –

биометрические СКУД) в государственные информационные системы и ресурсы города Москвы, обеспечение методологической поддержки интеграции биометрических СКУД с государственными информационными системами и ресурсами города Москвы.

4. **Департамент градостроительной политики города Москвы** определить уполномоченным органом исполнительной власти города Москвы, ответственным за определение функциональных требований к биометрическим СКУД и передаче информации из биометрических СКУД в государственные информационные системы и ресурсы города Москвы, ответственным за координацию деятельности по установке биометрических СКУД, включая организацию сбора и передачи данных, в том числе персональных (биометрических персональных) данных лиц, осуществляющих трудовую деятельность на строительных площадках для передачи информации в государственные информационные системы и ресурсы города Москвы.

5. Контроль за выполнением настоящего распоряжения оставляем за собой.

**Министр Правительства
Москвы, руководитель
Департамента информационных
технологий города Москвы**

**Министр Правительства
Москвы, руководитель
Департамента градостроительной
политики города Москвы**



Э.А.Лысенко

В.А.Овчинский

Приложение 1 к распоряжению
Департамента информационных
технологий города Москвы и
Департамента градостроительной
политики города Москвы
от 24 июня 2015 г.
№ 64-Б-307/25/дд

**ПОРЯДОК ФУНКЦИОНИРОВАНИЯ И УСТАНОВКИ
БИОМЕТРИЧЕСКИХ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ
ДОСТУПОМ НА КОНТРОЛЬНО-ПРОПУСКНЫХ ПУНКТАХ
СТРОИТЕЛЬНЫХ ПЛОЩАДОК**

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Для целей настоящего Порядка функционирования и установки биометрических систем контроля и управления доступом на контрольно-пропускных пунктах строительных площадок (далее – Порядок) используются следующие термины и определения:

Аутентификация

Процесс подтверждения подлинности заявленной идентификационной информации лица, осуществляющего деятельность на строительной площадке в городе Москве с использованием биометрической системы контроля и управления доступом

Биометрические СКУД

Комплекс средств системы контроля и управления доступом с применением биометрии (включающий технические и программные средства), подлежащий установке застройщиками на контрольно-пропускных пунктах строительных площадок, обеспечивающий получение, передачу информации о лицах, осуществляющих деятельность на строительных площадках, путем их автоматизированной аутентификации с использованием их биометрических персональных данных

ДИТ

Департамент информационных технологий

города Москвы

ДГП

Департамент градостроительной политики
города Москвы

ЕЦХД

Государственная информационная система
«Единый центр хранения и обработки
данных», функционирующая на основании
постановления Правительства Москвы
от 7 февраля 2012 г. № 24-ПП
«Об утверждении Положения
о государственной информационной
системе «Единый центр хранения
и обработки данных»

Закон № 572-ФЗ

Федеральный закон от 29 декабря 2022 г.
№ 572-ФЗ «Об осуществлении
идентификации и (или) аутентификации
физических лиц с использованием
биометрических персональных данных,
о внесении изменений в отдельные
законодательные акты Российской Федерации
и признании утратившими силу отдельных
положений законодательных актов
Российской Федерации»

Застройщик

физическое или юридическое лицо,
обеспечивающее на принадлежащем ему
земельном участке или на земельном участке
иного правообладателя (на законных
основаниях) строительство, реконструкцию,
капитальный ремонт, снос объектов
капитального строительства, а также
выполнение инженерных изысканий,
подготовку проектной документации для их
строительства, реконструкции, капитального
ремонта

Контрольно-пропускной
пункт

Место, предназначенное (в том числе
временно) для прохода персонала и других
лиц на строительную площадку в городе
Москве

Лица, осуществляющие деятельность на строительных площадках	Физические лица, ведущие деятельность на строительной площадке в городе Москве на основании трудового договора, договора гражданско-правового характера
ОМ РС ЕБС	Общегородской модуль регионального сегмента единой биометрической системы в г. Москве
Соблюдение требований по передаче данных	Соблюдение требований по передаче данных в государственные информационные системы и ресурсы города Москвы, установленными настоящим Порядком
Строительная площадка	Ограждаемая территория, используемая для размещения возводимого объекта капитального строительства, временных зданий и сооружений, техники, отвалов грунта, складирования строительных материалов, изделий, оборудования и выполнения строительно-монтажных работ

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящим Порядком регламентировано взаимодействие между застройщиком, ДИТ и ДГП (далее — стороны) при установке биометрических СКУД на контрольно-пропускных пунктах строительных площадок в городе Москве, обеспечивающих передачу информации в государственные информационные системы города Москвы, а также порядок функционирования биометрических СКУД.

2.2. Биометрические СКУД предназначены для аутентификации и автоматизированного учета лиц, осуществляющих деятельность на строительных площадках.

2.3. Передача информации из биометрических СКУД осуществляется после заключения соответствующего Соглашения о передаче данных с биометрических СКУД на контрольно-пропускных пунктах строительных площадок в городе Москве в государственные информационные системы и ресурсы города Москвы (далее – Соглашение) по форме согласно Приложению 1 к настоящему Порядку.

2.4. Использование биометрических СКУД осуществляется на основании Соглашения об информационном и технологическом взаимодействии при аутентификации физических лиц с использованием ОМ РС ЕБС или ЕЦХД по форме согласно Приложению 3 к настоящему Порядку.

2.5. Аутентификация и автоматизированный учет при проходе на территории строительных площадок осуществляется в отношении:

2.5.1. Граждан Российской Федерации и Республики Беларусь с использованием ОМ РС ЕБС в соответствии с Законом № 572-ФЗ.

2.5.2. Граждан иных государств с использованием ЕЦХД в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

2.6. Настоящий Порядок не применяется в случаях, когда выдача разрешения на строительство не требуется.

2.7. В случаях, когда выдача разрешения на строительство осуществляется федеральным органом исполнительной власти или государственной корпорацией, настоящий Порядок применяется по письменному согласованию соответствующего федерального органа исполнительной власти или государственной корпорации.

3. ПОЛНОМОЧИЯ СТОРОН ПРИ ВЗАИМОДЕЙСТВИИ

3.1. Для обеспечения эффективного взаимодействия при реализации настоящего Порядка:

3.1.1. Застройщики, осуществляющие строительство, обеспечивают:

3.1.1.2. Администрирование доступа на строительные площадки.

3.1.1.3. Установку, ввод в эксплуатацию, функционирование биометрических СКУД на контрольно-пропускных пунктах строительных площадок до начала основных строительных работ, одновременно с установкой ограждений на строительной площадке. При этом строительная площадка должна быть ограждена согласно установленному образцу.

Обязательство по использованию биометрических СКУД прекращается в момент демонтажа ограждений на строительной площадке до начала работ по благоустройству.

3.1.1.4. Техническое сопровождение и непрерывную круглосуточную бесперебойную работу биометрических СКУД на строительных площадках.

3.1.1.5. Соблюдение требований по передаче данных.

3.1.1.6. Контроль за размещением биометрических персональных данных лицами, осуществляющими деятельность на строительных площадках, для последующего использования в биометрических СКУД следующими способами:

3.1.1.6.1. Для граждан Российской Федерации и Республики Беларусь – путем размещения биометрических персональных данных в региональном сегменте единой биометрической системы в городе Москве посредством мобильного приложения «Мой id».

3.1.1.6.2. Для граждан иных государств – путем фотографирования и передачи иных персональных данных в установленном порядке в Многофункциональном миграционном центре города Москвы при получении карты иностранного гражданина.

3.1.1.7. Загрузку в биометрические СКУД сведений, предназначенных для последующей передачи в государственные информационные системы и ресурсы города Москвы, в том числе информации, предусмотренной пунктом 3 Технических требований к биометрическим системам контроля и управления доступом.

3.1.1.8. Проход на территорию строительных площадок города Москвы

лицам, осуществляющими деятельность на строительных площадках, после их аутентификации с использованием биометрических персональных данных.

3.1.2. ДГП обеспечивает:

3.1.2.1. Координацию взаимодействия с застройщиками при установке биометрических СКУД на всех контрольно-пропускных пунктах строительных площадок в соответствии с требованиями настоящего Порядка.

3.1.2.2. Организацию контроля за соблюдением застройщиками положений, установленных настоящим Порядком.

3.1.3. ДИТ обеспечивает:

3.1.3.1. Сопровождение и методологическую поддержку по интеграции биометрических СКУД с государственными информационными системами и ресурсами города Москвы.

3.1.3.2. Функционирование государственных систем и ресурсов города Москвы, осуществляющих взаимодействие с биометрическими СКУД.

3.1.3.3. Контроль за соблюдением технических условий и требований по передаче данных, получаемых с биометрических СКУД.

4. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ

4.1. Застройщик обеспечивает:

4.1.1. Направление в ДГП подписанных Соглашения и заявки на подключение биометрических СКУД для обеспечения передачи данных в государственные информационные системы и ресурсы города Москвы по форме, установленной Приложением 2 к настоящему Порядку.

4.1.2. Проведение мероприятий по подключению биометрических СКУД к информационным системам и ресурсам города Москвы в соответствие с настоящим Порядком.

4.2. ДГП обеспечивает:

4.2.1. Рассмотрение поступивших от застройщика Соглашения и заявки на подключение биометрических СКУД на предмет соответствия требованиям настоящего Порядка в срок, не превышающий 5 (пяти) рабочих дней с момента их поступления.

4.2.2. Направление в ДИТ подписанного застройщиком и ДГП Соглашения, заявки застройщика на подключение биометрических СКУД для проведения организационно-технических мероприятий по интеграции биометрических СКУД с информационными системами и ресурсами города Москвы, в случае соответствия требованиям настоящего Порядка.

4.3. ДИТ обеспечивает:

4.3.1. Рассмотрение и подписание Соглашения, прием в работу заявки застройщика на подключение биометрических СКУД, поступивших от ДГП.

4.3.2. Проведение организационно-технических мероприятий по подключению биометрических СКУД к информационным системам и ресурсам города Москвы в срок, не превышающий 10 (десяти) рабочих дней с момента поступления заявки застройщика из ДГП.

4.4. При наличии замечаний по представленным застройщиком к соглашению и\или заявке на подключение биометрических СКУД,

орган исполнительной власти города Москвы, выявивший недостатки в соответствующем соглашению и\или заявке, в срок не позднее 5 (пяти) рабочих дней с даты поступления соответствующего документа в указанный орган направляет застройщику уведомление с указанием на выявленные недостатки. При этом в случае, если таким органом является ДИТ, одновременно с направлением уведомления застройщику копия указанного уведомления направляется в ДГП. Застройщик обязан в срок, не превышающий 5 (пяти) рабочих дней, провести мероприятия по устранению замечаний и повторно представить соглашение и\или заявку на рассмотрение.

4.5. В случае завершения мероприятий, предусмотренных пунктами 4.1.2, 4.3.2 ДИТ с застройщиком и ДГП подписывают Протокол тестирования подключения биометрических СКУД к информационным системам и ресурсам города Москвы.

Приложение 1
к Порядку функционирования и установки
биометрических систем контроля и
управления доступом на контрольно-
пропускных пунктах строительных
площадок

ФОРМА

**СОГЛАШЕНИЕ
О ПЕРЕДАЧЕ ДАННЫХ С БИОМЕТРИЧЕСКИХ
СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА КОНТРОЛЬНО-
ПРОПУСКНЫХ ПУНКТАХ СТРОИТЕЛЬНЫХ ПЛОЩАДОК В
ГОСУДАРСТВЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ И РЕСУРСЫ
ГОРОДА МОСКВЫ**

№ _____

г.Москва

«___» 20___

Департамент информационных технологий города Москвы в лице _____, действующего на основании доверенности от _____ № _____, именуемый в дальнейшем «Оператор», с одной стороны, Департамент градостроительной политики города Москвы в лице _____, действующего на основании доверенности от _____ № _____, именуемое в дальнейшем «Департамент» с другой стороны, _____, в лице _____, действующего на основании _____, именуемое в дальнейшем «Застройщик», с другой стороны, в дальнейшем по отдельности или совместно именуемые «Сторона» и «Стороны» соответственно, руководствуясь распоряжением Департамента информационных технологий города Москвы Департамента градостроительной политики города Москвы от _____ № _____ «Об утверждении Порядка функционирования и установки биометрических систем контроля и управления доступом на контрольно-пропускных пунктах строительных площадок и Технических требований к биометрическим системам контроля и управления доступом, устанавливаемых на контрольно-пропускных пунктах строительных площадок», заключили настоящее Соглашение о передаче данных с биометрических систем контроля и управления доступом на контрольно-пропускных пунктах строительных площадок в государственные информационные системы и ресурсы города Москвы, о следующем:

1. Предмет Соглашения

1.1. В соответствии с настоящим Соглашением Стороны определяют порядок взаимодействия.

1.2. Настоящее Соглашение носит безвозмездный характер и не создает для Сторон каких-либо финансовых обязательств.

2. Организация взаимодействия Сторон

2.1. Стороны оказывают друг другу необходимую консультационную и методологическую поддержку по вопросам реализации настоящего Соглашения.

2.2. Во исполнение настоящего Соглашения Стороны обязуются обеспечить:

2.2.1. Своевременное и полное выполнение обязательств, необходимых для реализации настоящего Соглашения.

2.2.2. Достоверность и объективность предоставляемой информации.

2.2.3. Неразглашение информации, предоставленной в рамках настоящего Соглашения, в отношении которой установлен режим конфиденциальности.

2.2.4. Рассмотрение вопросов, возникающих в процессе реализации настоящего Соглашения, и принятие по ним согласованных решений.

2.3. Сторона обеспечивает контроль:

2.3.1. Осуществления корректной передачи информации.

2.3.2. Качества, полноты и достоверности передаваемых данных.

2.4. В целях подтверждения соответствия обеспечения передачи данных проводится интеграционное тестирование.

2.5. Готовность передачи данных подтверждается Протоколом тестирования подключения биометрических СКУД к информационным системам и ресурсам города Москвы, составляемым по форме, являющейся приложением 1 к настоящему Соглашению, на каждый объект капитального строительства. В случае передачи данных по одному объекту капитального строительства протокол интеграционного тестирования составляется на данный конкретный объект.

2.6. В случае, если по результатам интеграционного тестирования будет установлено несоответствие требованиям Приложения 2 к Распоряжению Департамента информационных технологий города Москвы и Департамента градостроительной политики города Москвы от _____ № _____ «Об утверждении Порядка функционирования и установки биометрических систем контроля и управления доступом на контрольно-пропускных пунктах строительных площадок и Технических требований к биометрическим системам контроля и управления доступом, устанавливаемых на контрольно-пропускных пунктах строительных площадок», настоящее Соглашение в отношении данного объекта капитального строительства прекращает свое действие. При этом, Стороны обязуются предпринять все разумные усилия для устранения причин, препятствующих интеграции, и проведения повторного интеграционного тестирования после их устранения.

3. Прочие условия

3.1. Настоящее Соглашение вступает в силу с момента его подписания Сторонами и действует в течение 3 (трех) лет. Если ни одна из Сторон не позднее 30 календарных дней до истечения соответствующего периода не уведомит в письменной форме другую Сторону о своем намерении прекратить его действие, то настоящее Соглашение продлевается на последующие три года.

3.2. Внесение изменений в настоящее Соглашение осуществляется по взаимному согласию Сторон, выраженному в письменной форме путем подписания соответствующих дополнительных соглашений, являющихся неотъемлемой частью настоящего Соглашения.

3.3. Оператор и/или Департамент вправе в одностороннем порядке отказаться от настоящего Соглашения путем направления соответствующего уведомления в письменной форме другим Сторонам не менее чем за 20 календарных дней до даты предполагаемого прекращения настоящего Соглашения. Действие настоящего Соглашения прекращается с даты, указанной в уведомлении, но не ранее чем по истечении 20 календарных дней со дня направления соответствующего уведомления другой Стороне.

3.4. Настоящее Соглашение составлено и подписано в трех экземплярах, имеющих равную юридическую силу, по одному для каждой из Сторон.

Реквизиты и подписи Сторон

Оператор: Департамент информационных технологий города Москвы	Департамент: Департамент градостроительной политики города Москвы	Наименование организации: _____
Место нахождения: 123112, г. Москва, 1-й Красногвардейский пр., д. 21, стр. 1 Фактический (почтовый) адрес: 105064, г. Москва, Яковоапостольский пер., д. 12, стр. 1 ИИН 7710878000, КПП 770301001 ОГРН 1107746943347	Место нахождения: 125009, г. Москва, Никитский пер., д. 5, стр.6 Фактический (почтовый) адрес: 125009, г. Москва, Никитский пер., д. 5, стр.6 ИИН 7703742961, КПП 770301001 ОГРН 1117746321219	Место нахождения: _____ _____ _____ ИИН _____, КПП _____, ОГРН _____
М.П. _____	М.П. _____	М.П. _____

Приложение
к Соглашению о передаче данных с
биометрических систем контроля и
управления доступом на контрольно-
пропускных пунктах строительных
площадок в государственные
информационные системы и ресурсы
города Москвы
от _____ № _____

ПРОТОКОЛ ИСПЫТАНИЙ ПОДКЛЮЧЕНИЯ БИОМЕТРИЧЕСКОЙ СКУД К ИНФОРМАЦИОННЫМ СИСТЕМАМ И РЕСУРСАМ ГОРОДА МОСКВЫ

Настоящий документ представляет собой Протокол испытаний подключения биометрической системы контроля и управления доступом, обеспечивающей передачу информации в государственные информационные системы и ресурсы города Москвы, размещенной на строительной площадке (*наименование организации*) (*кадастровый номер земельного участка*) (*УИН объекта капитального строительства*): _____ в рамках Соглашения о передаче данных с биометрических систем контроля и управления доступом на контрольно-пропускных пунктах строительных площадок в государственные информационные системы и ресурсы города Москвы между (*наименование организации*), Департаментом информационных технологий города Москвы (далее - Оператор) и Департаментом градостроительной политики города Москвы.

В испытаниях участвуют:

Члены комиссии:

1. ФИО, должность, наименование органа исполнительной власти, подведомственной организации.
2. ФИО, должность, наименование органа исполнительной власти, подведомственной организации.
3. ФИО, должность, наименование органа исполнительной власти, подведомственной организации).

Организации, обеспечивающие проведение испытаний:

1. ФИО (должность, наименование организации).

1. Наименование объекта испытаний

Биометрические СКУД (указать технические характеристики, марку, заводской номер) на объекте (указать наименование организации) кадастровый номер: _____. Условное обозначение: биометрические СКУД.

2. Место и продолжительность испытаний:

Адрес, кадастровый номер земельного участка _____.

УИН объекта капитального строительства _____

Испытания проводятся: дата.

3. Организации, участвующие в испытаниях:

4. Цель испытаний:

Целью испытаний является проверка обеспечения информационного взаимодействия при передаче данных между биометрической СКУД и государственными информационными системами и ресурсами города Москвы требованиям Приложения 2 к распоряжению Департамента информационных технологий города Москвы и Департамента градостроительной политики города Москвы от _____ №_____.

5. Сведения о продолжительности испытаний:

5.1. Дата начала испытания:

5.2. Дата окончания испытания:

6. Сведения о результатах испытаний:

Указывается перечень проверок выполнения требований Приложения 2 к Распоряжению.

7. Иная информация:

8. Заключение:

В результате проведенных испытаний установлено, что интеграция биометрических СКУД (указать технические характеристики, марку, заводской номер) на объекте (указать наименование организации) кадастровый номер _____ с государственными информационными системами и ресурсами города Москвы **выполнена**. Биометрические СКУД соответствуют техническим требованиям к биометрическим СКУД.

или

В результате проведенных испытаний установлено, что интеграция биометрических СКУД (указать технические характеристики, марку, заводской номер) на объекте (указать наименование организации) с государственными информационными системами и ресурсами города Москвы **не выполнена**. Замечания по интеграции: (Перечислить замечания по результатам испытаний).

Члены комиссии

подпись

дата

подпись

дата

Приложение 2
к Порядку функционирования и
установки биометрических систем
контроля и управления доступом на
контрольно-пропускных пунктах
строительных площадок

ФОРМА

**ЗАЯВКА НА ПОДКЛЮЧЕНИЕ БИОМЕТРИЧЕСКИХ СИСТЕМ КОНТРОЛЯ
И УПРАВЛЕНИЯ ДОСТУПОМ**

Заявитель (*наименование организации*) в лице (*должность, ФИО*) в соответствии с требованиям Порядка функционирования и установки биометрических систем контроля и управления доступом на контрольно-пропускных пунктах строительных площадок (далее – Порядок) просит провести мероприятия по подключению биометрической системы контроля и управления доступом, установленной на объекте капитального строительства (далее – биометрическая СКУД) к государственным информационным системам и ресурсам города Москвы и направляет Схемы организации прохода на строительную площадку, в именно: размещение контрольно-пропускных пунктов, размещение средств видеофиксации или фотофиксации, с указанием направления прохода (вход или выход), а также сведения в соответствии с Приложением № 1 к настоящей заявке.

Приложения к заявке:

1. Сведения об объекте капитального строительства и состав технических средств биометрической СКУД в табличной форме.
2. Схемы организации прохода на строительную площадку, включая размещение контрольно-пропускных пунктов и средств видеофиксации или фотофиксации.

Наименование организации:

Место нахождения:

ИИН _____,
КПП _____,
ОГРН _____

Должность _____
ФИО _____
М.П. _____

Приложение 3
к Порядку функционирования и
установки биометрических систем
контроля и управления доступом на
контрольно-пропускных пунктах
строительных площадок

Форма

Соглашение
об информационном и технологическом взаимодействии между
Департаментом информационных технологий города Москвы,
Государственным казенным учреждением города Москвы «Московское
городское агентство по телекоммуникациям» и
_____ (наименование застройщика) при аутентификации
физических лиц с использованием общегородского модуля
регионального сегмента единой биометрической системы в г. Москве
или государственной информационной системы «Единый центр
хранения и обработки данных»

г. Москва

«_____» 2025 г.

Департамент информационных технологий города Москвы, в
лице _____, действующего на основании доверенности
_____, (далее – ДИТ), Государственное казенное учреждение города Москвы
«Московское городское агентство по телекоммуникациям», в лице
_____, действующего на основании
доверенности _____ (далее – ГКУ «Мосгортелеком»), и
_____ (наименование
_____ (должность, ФИО), действующий(ая) на основании
_____ (доверенность, устав) и совместно именуемые в дальнейшем
«Стороны», руководствуясь Порядком применения биометрических систем
контроля и управления доступом на строительных площадках города Москвы,
обеспечивающих передачу информации в государственные информационные
системы и ресурсы города Москвы, утвержденным распоряжением Департамента
информационных технологий города Москвы Департамента градостроительной
политики города Москвы, Департамента гражданского строительства города
Москвы от _____ № _____, правовыми актами Российской Федерации и
города Москвы, заключили настояще Соглашение (далее – Соглашение) о
нижеследующем.

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1. В Соглашении используются следующие термины и определения:
 - 1.1. Аутентификация – совокупность мероприятий с использованием биометрических персональных данных физического лица по проверке

физического лица на принадлежность ему идентификаторов с использованием векторов единой биометрической системы, реализуемых общегородским модулем регионального сегмента единой биометрической системы в г. Москве, без использованием векторов единой биометрической системы, реализуемых государственной информационной системы «Единый центр хранения и обработки данных».

1.2. Биометрическая СКУД (информационная система) – комплекс средств системы контроля и управления доступом с возможностью аутентификации с использованием биометрических персональных данных, обеспечивающий получение, обработку, передачу информации о проходе на территорию строительных площадок лиц, осуществляющих трудовую деятельность на строительных площадках города Москвы путем их автоматической аутентификации.

1.3. Система биометрической аутентификации (СБА) –

1.3.1. общегородской модуль регионального сегмента единой биометрической системы в г. Москве, функции оператора которого, в части обеспечения создания, развития (модернизации) и эксплуатации государственных информационных систем и (или) их технологических, организационных, вспомогательных элементов, необходимых для функционирования ОМ РС ЕБС, а также обеспечения информационной безопасности и технического сопровождения Потребителей ОМ РС ЕБС возложены на ГКУ «Мосгортелеком» (для граждан Российской Федерации и республики Беларусь);

1.3.2. государственная информационная система «Единый центр хранения и обработки данных», функции оператора которой возложены на ГКУ «Мосгортелеком» (для граждан иных государств).

1.4. Потребитель – организация, использующая Биометрическую СКУД.

1.5. РС ЕБС – региональный сегмент единой биометрической системы, созданный в городе Москве.

1.6. API – application programming interface (спецификация интерфейса интеграции), прикладной программный интерфейс – набор способов и правил для организации информационного обмена между компонентами информационных систем.

2. ПРЕДМЕТ СОГЛАШЕНИЯ

2.1. Предметом Соглашения является информационное и технологическое взаимодействие Сторон в целях обеспечения аутентификации физических лиц на строительных площадках с использованием биометрических персональных данных, реализуемой СБА.

2.2. В рамках реализации Соглашения Стороны осуществляют информационное и технологическое взаимодействие при использовании СБА и Биометрической СКУД в целях организации прохода на строительные площадки.

3. УСЛОВИЯ ВЗАИМОДЕЙСТВИЯ СТОРОН

3.1. В рамках реализации Соглашения ГКУ «Мосгортелеком»:

3.1.1. Предоставляет доступ Биометрической СКУД к СБА путем передачи авторизационных данных технологической учетной записи в соответствии с формой Акта, являющейся приложением к настоящему Соглашению.

3.1.2. Обеспечивает функционирование СБА.

3.1.3. Осуществляет прием и обработку в СБА видеопотока, передаваемого с камер видеонаблюдения, установленных в контрольно-пропускных пунктах Потребителя для целей аутентификации.

3.1.4. Осуществляет прием и обработку в СБА фотоизображений, полученных с камеры терминала биометрической СКУД Потребителя для целей аутентификации.

3.1.5. Обеспечивает проведение аутентификации в отношении лиц, информация о которых предварительно предоставлена Потребителем в СБА посредством API, и направляет информацию о результатах аутентификации посредством API.

3.2. В рамках реализации Соглашения Потребитель:

3.2.1. Обеспечивает техническую готовность Биометрической СКУД к интеграции и взаимодействию с СБА¹.

3.2.2. Обеспечивает использование в Биометрической СКУД программных и технических средств систем контроля и управления доступом, совместимых с СБА.

3.2.3. Обеспечивает автоматическую передачу в СБА видеопотока и (или) кадров видеопотоков, а также иной информации, предусмотренной API СБА, для целей аутентификации.

3.2.4. Обеспечивает обработку в Биометрической СКУД результатов аутентификации, полученных из СБА, при реализации целей, установленных п.2.2 Соглашения.

3.3. ДИТ, при необходимости, обеспечивает методическое сопровождение в рамках информационного взаимодействия.

3.4. Стороны назначают ответственных представителей за информационное взаимодействие, и направляют соответствующие контактные данные в рабочем порядке.

3.5. Стороны имеют право направлять друг другу запросы в любых формах и получать ответы на указанные запросы в установленные в них сроки.

4. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

4.1. Любая информация, предоставленная одной Стороной другой Стороне в рамках настоящего Соглашения, считается информацией ограниченного доступа и не подлежит разглашению или передаче третьим лицам без согласования с передающей Стороной.

4.2. Стороны, являющимся операторами информационных систем и/или использующие их обязуются:

4.2.1. Назначить ответственное лицо за информационную безопасность и направить его контактные данные на электронную почту другой Стороны для оперативного взаимодействия в случае инцидентов информационной безопасности. Электронная почта ГКУ «Мосгортелеком» - oib_video@it.mos.ru, электронная почта _____ - _____.

4.2.2. Организовать криптографическую защиту каналов связи с использованием средств криптографической защиты класса КС3 в соответствии с

¹ Интеграция осуществляется в соответствии с требованиями Регламента передачи информации об объектах видеонаблюдения в государственную информационную систему «Единый центр хранения и обработки данных» из внешних систем видеонаблюдения, утвержденного распоряжением Департамента информационных технологий города Москвы от 31 июля 2015 г. N 64-16-241/15

приказом Минцифры России от 05.05.2023 № 445 «Об утверждении перечня угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица в единой биометрической системе, а также актуальных при взаимодействии информационных систем государственных органов, органов местного самоуправления, Центрального банка Российской Федерации, организаций, за исключением организаций финансового рынка, индивидуальных предпринимателей, нотариусов с единой биометрической системой, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных». Организация канала связи осуществляется посредством криптошлюза VipNet Coordinator HW. Обмен информацией, необходимой для организации криптографического межсетевого взаимодействия (номера сетей, ключевая информация и иная), осуществляется в рабочем порядке.

4.2.3. Обеспечить выполнение требований приказа Федеральной службы безопасности Российской Федерации от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требованиям к защите персональных данных для каждого из уровней защищенности», а также приказа Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» в отношении средств криптографической защиты информации, установленных в информационной системе Стороны.

4.2.4. Выполнять требования по защите информации в соответствии с Федеральным законом от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации».

4.2.5. Незамедлительно принять меры по устранению нарушений требований по защите информации, которые могут привести к утечкам информации (неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват) и (или) нарушению функционирования информационных систем Сторон.

4.3. Потребитель обязуется:

4.3.1. Определить требования по защите информации, предъявляемые к их информационным системам в соответствии с нормативно-правовыми актами Российской Федерации, в том числе с учетом требований приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и Приказа ФСТЭК России от 18.02.2013 № 21 «Об

утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

4.3.2. Направить ГКУ «Мосгортелеком» подтверждение выполнения мер по защите информации, определенных в соответствии с п.4.3.1 Соглашения, посредством электронной почты до начала взаимодействия.

4.3.1. Уведомлять ГКУ «Мосгортелеком» посредством электронной почты о возникновении угроз и фактах сбоя и (или) нарушения в работе, возникновении угроз и фактах утечки информации, а также о нарушениях требований по защите информации, которые могут привести к нарушению функционирования информационных систем Сторон, в течение 24 часов с момента возникновения соответствующего события.

4.4. Направление Сторонами сведений, составляющих государственную тайну, в рамках Соглашения не допускается.

5. ОТВЕТСТВЕННОСТЬ

5.1. Стороны несут ответственность за неисполнение или ненадлежащее исполнение своих обязательств по Соглашению в соответствии с законодательством Российской Федерации и Соглашением.

6. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

6.1. Стороны договорились, что вопросы по урегулированию разногласий, возникающих в связи с толкованием и реализацией Соглашения, будут рассматриваться путем проведения переговоров и консультаций.

6.2. Соглашение вступает в силу с момента его подписания и действует в течение одного года. Если любая из Сторон не заявила о прекращении действия Соглашения до момента прекращения срока его действия, определенного настоящим пунктом Соглашения, Соглашение подлежит автоматическому продлению на следующий год, с момента истечения его срока действия. Данный порядок продления срока действия Соглашения применяется ежегодно.

6.3. Любая из Сторон вправе в одностороннем порядке расторгнуть настоящее Соглашение путем направления соответствующего письменного уведомления другим Сторонам не менее чем за 30 рабочих дней до предполагаемой даты расторжения настоящего Соглашения.

6.4. Действие настоящего Соглашения прекращается с даты, указанной в уведомлении, но не ранее чем через 30 рабочих дней со дня направления Сторонам соответствующего уведомления.

6.5. В случае расторжения Соглашения обязательства Сторон, установленные разделом 3 Соглашения, прекращаются, если иное не предусмотрено законодательством Российской Федерации.

6.6. В настоящее Соглашение могут вноситься изменения и дополнения путем оформления дополнительных соглашений, протоколов, являющихся неотъемлемыми частями Соглашения.

6.7. Соглашение составлено в 3 (трех) экземплярах, по одному для каждой из Сторон, имеющих одинаковую юридическую силу.

**Департамент информационных
технологий города Москвы**

(наименование застройщика)

Адрес юридического лица:
123112, г.Москва, 1-й
Красногвардейский пр-д, д.21, стр.1
Фактический (почтовый) адрес:
105064, г.Москва, Яковоапостольский
пер., д.12, стр.1

ГКУ Мосгортелеком

Адрес юридического лица:
121059, г. Москва, ул. 1-я
Бородинская ул., д.2А,

Адрес юридического лица:

Фактический (почтовый) адрес:

ПОДПИСИ СТОРОН:

**Департамент информационных
технологий города Москвы**

(наименование застройщика)

_____ / _____ /

_____ (ФИО)

ГКУ «Мосгортелеком»

_____ / _____ /

Приложение
к Соглашению об информационном и технологическом и
технологическом взаимодействии между Департаментом
информационных технологий города Москвы,
Государственным казенным учреждением города Москвы
«Московское городское агентство по телекоммуникациям» и
_____ (наименование застройщика) при аутентификации
физических лиц с использованием общегородского модуля
регионального сегмента единой биометрической системы в г.
Москве или государственной информационной системы
«Единый центр хранения и обработки данных»

Форма

Акт
передачи Авторизационных данных технологической учетной записи

г.Москва

« ____ » 20 ____ г.

1. ГКУ «Мосгортелеком» в лице _____ (*ФИО, должность*) предоставил
технологический доступ к Системе биометрической аутентификации (СБА) для целей
интеграции, посредством передачи Авторизационных данных технологической учетной
записи (далее – Авторизационные данные), а Потребитель (_____) (*наименование
застройщика*), в лице _____ (*ФИО, должность*) далее по тексту - Пользователь, принял
указанную информацию, согласно таблице:

Таблица

Н п/п	ФИО	Авторизационные данные

2. Настоящим Пользователь подтверждает, что:

2.2. Уведомлен о том, что Авторизационные данные, являются информацией
ограниченного доступа и не подлежат разглашению и передаче третьим лицам и
обязуется не передавать такую информацию третьим лицам.

2.4. Уведомлен, что несет административную, гражданскую и дисциплинарную
ответственность в соответствии с действующим законодательством Российской
Федерации, за разглашение информации ограниченного доступа.

3. Настоящий акт составлен в двух экземплярах по одному для каждой из Сторон,
имеющих одинаковую юридическую силу.

Передал документы:

Принял документы:

(должность) (подпись) (ФИО) (должность) (подпись) (ФИО)

Сведения об объекте капитального строительства и состав технических средств биометрической СКУД в табличной форме

Общие сведения										Сведения для подключения к биометрической системе аутентификации															
№ п/п	Наименование застройщика	ИИНН застройщика	Тип объекта	УИН объекта капитального строительства	Адрес строительной площадки	Средства видеонаблюдения (перечень с указанием наименований камер, интегрированных в ЕГИСД)	Средства видеонаблюдения (перечень с указанием наименований камер, интегрированных в ЕГИСД)	Средства управления биометрической СКУД в составе аппаратных устройств, с указанием производителей и моделей	Средства обеспечения защиты информации (однократного использования, обнуления, идентификации сети VipNet)	Средства обеспечения защиты информации (однократного использования, обнуления, идентификации сети VipNet)	Место установки оборудования	GPS координаты	IP адрес камеры	Наименование	Логин	Пароль	Уличный адрес/номер внутри помещения (КИН/номер)	Часовой пояс	Режим работы	Режим Старт/стоп	Метод выделения изображения	Метод для распознавания	Порядковый номер сервера СКУД		
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Приложение 2 к распоряжению
Департамента информационных
технологий города Москвы и
Департамента градостроительной
политики города Москвы
от 27 июня 2015 г.
№ 64-16-304/25/дд

ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К БИОМЕТРИЧЕСКИМ СИСТЕМАМ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ, УСТАНАВЛИВАЕМЫХ НА КОНТРОЛЬНО-ПРОПУСКНЫХ ПУНКТАХ СТРОИТЕЛЬНЫХ ПЛОЩАДОК

1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящие Технические требования к биометрическим системам контроля и управления доступом, устанавливаемых на контрольно-пропускных пунктах строительных площадок (далее – Технические требования) определяют технические параметры и требования к биометрическим СКУД.

2. Биометрические СКУД обеспечивают передачу данных в государственные информационные системы и ресурсы города Москвы в соответствии с Техническими требованиями.

2. ТРЕБОВАНИЯ К СОСТАВУ БИОМЕТРИЧЕСКИХ СКУД

2.1. Биометрические СКУД включают в себя следующие компоненты:

2.1.1. Преграждающие управляемые устройства (турникеты).

2.1.2. Считывающие устройства.

2.1.3. Средства видеофиксации или фотофиксации.

2.1.4. Средства управления биометрическими СКУД в составе аппаратных устройств и (или) программных средств.

2.1.5. Средства обеспечения защиты информации

2.2. Преграждающие управляемые устройства (турникеты), должны ограничивать свободный проход физических лиц (вход, выход), создавая физическую преграду перед входом или выходом на территорию строительной площадки и соответствовать следующим требованиям:

2.2.1. Моторизованный турникет из нержавеющей стали.

2.2.2. Ширина перекрываемого прохода не менее 560 мм.

2.2.3. Пропускная способность: в режиме однократного прохода от 20 чел./мин., в режиме свободного прохода от 40 чел./мин.

2.2.4. Исполнение для размещения вне помещений в климатической зоне города Москвы.

2.3. Считывающие устройства должны соответствовать следующим требованиям:

2.3.1. Исполнение для размещения вне помещений в климатической зоне города Москвы.

2.3.2. Устойчивость к взлому или вскрытию, отсутствие сигнала

на открытие преграждающего устройства при взломе, вскрытии, обрыве или коротком замыкании электрических цепей.

2.4. Средства видеофиксации должны быть подключены к ЕЦХД в соответствии с Порядком применения технических средств, осуществляющих видеонаблюдение на месте проведения работ по строительству, реконструкции объектов капитального строительства в городе Москве и учет параметров движения транспортных средств в процессе проведения работ по строительству, реконструкции объектов капитального строительства на месте проведения работ по строительству, реконструкции объектов капитального строительства в городе Москве, утвержденным распоряжением Комитета государственного строительного надзора города Москвы и департамента информационных технологий города Москвы от 12 февраля 2025 г. № 10-Р/64-16-55/25 и соответствовать следующим требованиям:

2.4.1. Обеспечение фиксации изображения лица с размером не менее 100 пикселей по ширине на расстоянии 0,5–1,5 метра.

2.5. Средства фотофиксации должны соответствовать следующим требованиям:

2.5.1. Разрешение сенсора камеры не менее 2 мегапикселей.

2.5.2. Возможность формирования фотоизображения разрешением не менее 1920 x 1080 пикселей.

2.5.3. Обеспечение фиксации изображения лица с размером не менее 100 пикселей по ширине на расстоянии 0,5–1,5 метра.

2.5.4. Наличие экрана размером по диагонали не менее 5 дюймов.

2.5.5. Исполнение для размещения вне помещений в климатической зоне города Москвы.

2.5.6. Возможность передачи кадров фотофиксации, содержащих изображения лиц физических лиц, в отношении которых биометрические СКУД осуществляет процедуру аутентификации, в ОМ РС ЕБС и ЕЦХД, в случае, если применяемые биометрические СКУД не обеспечивают передачу таких кадров.

2.6. Средства управления биометрическими СКУД в составе аппаратных устройств и (или) программных средств должны соответствовать следующим требованиям:

2.6.1. Обеспечение информационного взаимодействия с ОМ РС ЕБС и ЕЦХД для проведения аутентификации физических лиц с использованием их биометрических персональных данных.

2.6.2. Управление преграждающими устройствами (турникетами) в количестве не менее 1 точки доступа.

2.7. Средства обеспечения защиты информации должны обеспечивать криптографическую защиту каналов связи для информационного обмена биометрических СКУД с использованием СКЗИ класса КС3 в соответствии с приказом Минцифры России от 5 мая 2023 г. № 445 посредством криптошлюза VipNet Coordinator HW.

3. ТРЕБОВАНИЯ К СОСТАВУ, ФОРМАТУ И СПОСОБУ ПЕРЕДАЧИ ДАННЫХ

3.1. Информация о лицах, осуществляющих деятельность на строительных площадках, передается в следующие информационные системы города Москвы:

- 3.1.1. АИС «ЦД».
- 3.1.2. ОМ РС ЕБС.
- 3.1.3. ЕЦХД.

3.2. При передаче информации в рамках п. 3.1.1 Технических требований:

3.2.1. Передача информации осуществляется в соответствии с Приложением к Техническим требованиям.

3.2.2. Обеспечивается передача следующей информации о физических лицах:

3.2.2.1. Фамилия, имя, отчество, дата рождения, гражданство лиц, осуществляющих трудовую деятельность на строительных площадках (далее – работник).

3.2.2.2. Страховой номер индивидуального лицевого счёта (далее – СНИЛС) для граждан Российской Федерации и Республики Беларусь.

3.2.2.3. Номер карты иностранного гражданина (далее – КИГ) для граждан иных государств.

3.2.2.4. Идентификационный номер налогоплательщика (далее – ИНН) работника.

3.2.2.5. Наименование, ИНН, код причины постановки на учет организации трудоустройства.

3.2.2.6. Функциональные обязанности в соответствии с постановлением Госстандарта Российской Федерации от 26 декабря 1994 г. № 367 «О принятии и введении в действие Общероссийского классификатора профессий рабочих, должностей служащих и тарифных разрядов ОК 016-94».

3.2.2.7. Уникальный идентификационный номер объекта капитального строительства.

3.2.2.8. Дата и время прохода через контрольно-пропускной пункт строительной площадки.

3.2.2.9. Тип прохода: вход на строительную площадку, выход со строительной площадки.

3.2.2.10. Идентификатор способа аутентификации при проходе (карта доступа или биометрический персональный).

3.2.2.11. Иная информация, необходимая для реализации решения протокола заседания Антитеррористической комиссии города Москвы от 30 апреля 2025 г. №4-20-109/25.

3.3. При передаче информации в рамках п. 3.1.2 Технических требований:

3.3.1. Информационный обмен осуществляется в соответствии с техническими требованиями, установленными в Регламенте информационного взаимодействия при биометрической аутентификации посредством ЕЦХД, утвержденном распоряжением Департамента информационных технологий города Москвы от 10 июня 2025 г. № 64-16-273/25.

3.3.2. Обеспечивается передача следующей информации:

3.3.2.1. СНИЛС для граждан Российской Федерации и Республики

Беларусь.

3.3.2.2. Кадры фотофиксации, содержащие изображения лиц физических лиц, в отношении которых биометрические СКУД осуществляют процедуру аутентификации (при использовании в составе биометрических СКУД средств фотофиксации).

3.4. При передаче информации в рамках п. 3.1.3 Технических требований:

3.4.1. Информационный обмен осуществляется в соответствии с техническими требованиями, установленными в Регламенте взаимодействия при использовании общегородского модуля регионального сегмента города Москвы, утвержденном распоряжением Департамента информационных технологий города Москвы от 10 июня 2025 г. № 64-16-273/25.

3.4.2. Обеспечивается передача следующей информации:

3.4.2.1. Номер КИГ для иностранных граждан, за исключением граждан Республики Беларусь.

3.4.2.2. Кадры фотофиксации, содержащие изображения лиц физических лиц, в отношении которых биометрические СКУД осуществляют процедуру аутентификации (при использовании в составе биометрических СКУД средств фотофиксации).

Приложение
к Техническим требованиям
к биометрическим системам
контроля и управления доступом,
устанавливаемых на контрольно-
пропускных пунктах
строительных площадок

Инструкция передачи данных застройщиком в АИС «Цифровой двойник»

1. Авторизация.

1.1. Общий алгоритм использования методов сервисов платформы во внешних системах:

1.2. Запрос OAuth-токена авторизации;

1.3. Вызов необходимого метода с данными для авторизации клиента и токеном из пункта 1.

1.4. Адрес получения токена: {Стенд}/auth/realm/{realm}/protocol/openid-connect/token

1.5. Здесь и далее:

1.5.1. {Стенд} – DNS, выдаваемый по запросу ответственными лицами ДИТ

1.5.2. {realm} – адрес области маршрутизации, выдаваемый по запросу ответственными лицами ДИТ

2. Пример вызова метода платформы с авторизацией.

Например, необходимо отправить данные в справочник 46. Для этого можно воспользоваться методом загрузки данных в справочник («2.1 Загрузка данных в справочник «Получаемые сообщения ПД»). Здесь также требуется авторизация.

2.1. Пример авторизации с помощью curl.

Запрос curl для получения токена доступа:

```
curl -d "client_id=***** -d "client_secret=*****" -d  
"grant_type=client_credentials" https://pudsmpl-stage.mos.ru/auth/realm/pudsmp/protocol/openid-connect/token
```

Составьте запрос к необходимому методу, передайте в него токен доступа:

```
curl --location --request POST 'https://pudsmpl-stage.mos.ru/dictionaries/v1/46/values' |\n--header 'Content-Type: application/json' |\n--header 'Authorization: Bearer *****'
```

2.2. Пример авторизации с помощью библиотеки requests на Python

```

# Подключите библиотеку requests для составления и обработки запросов
import requests

# Определите данные конфиденциального клиента как переменные (при
необходимости)

client_id = "*****"
client_secret = "*****"
auth = "https://puds-mpl-stage.mos.ru/auth"
realm = "pudsmp"

# Составьте запрос для получения токена доступа, передайте в него данные
конфиденциального клиента

token_query = requests.post(
    f'{auth}/realms/{realm}/protocol/openid-connect/token',
    data={
        "client_id": client_id,
        "client_secret": client_secret,
        "grant_type": "client_credentials"
    }
)

# Извлеките токен доступа из ответа

data = token_query.json()
access_token = data["access_token"]

# Составьте запрос к необходимому методу сервиса платформы, передайте в
него токен доступа

response = requests.get(
    'https://puds-mpl-stage.mos.ru/dictionaries/v1/46/values',
    headers = {
        'accept': 'application/json',
        'Authorization': f"Bearer {access_token}"
    }
)

```

3. Загрузка данных в справочник

Для загрузки данных в справочник необходимо использовать следующий метод: POST /v1/{id}/values.

Параметры	Описание
integer(\$int32) id (path)	идентификатор справочника, значение разное для каждого контура (обязательный параметр)
string Namespace (header)	пространство, заполнить значением «puds-rb» (обязательный параметр)

Шаблон тела запроса:

Массив	Описание
attributes	массив с перечислением кодов атрибутов, в которые необходимо записать значения
elements	массив объектов значений (один объект = одна строка в таблице)
values	массив значений одного элемента (одна строка), значения перечисляются через запятую, соответствуют порядку атрибутов в attributes

```
{
  "attributes": [
    "string"
  ],
  "elements": [
    {
      "values": [
        "string"
      ]
    }
  ]
}
```

4. Загрузка данных в справочник «Получаемые сообщения ПД»

Пример тела запроса для загрузки одного элемента в справочник (одна строка):

- Справочник с новыми элементами

Атрибут	Описание
int ID	Идентификатор элемента события
Json MESSAGE	Сообщение

```
{
  "attributes": [
    "MESSAGE"
  ],
  "elements": [
    {
      "values": [
        {
          "client": "",
          "data": [
            {
              "empId": "",
              "name": "",
              "snils": "",
              "kigID": "",
              "dBrth": "",
              "orgInn": "",
              "kpp": "",
              "funRes": "",
              "citizen": "",
              "staffinn": "",
              "isDelEm": ""
            }
          ]
        }
      ]
    }
  ]
}
```

Curl:

Название JSON	Название СКУП	Тип	Область письма	Примечание
<code>curl -X 'POST' \ncli 'https://\{Сменд\}/dictionaries/v1/\{Id справочника\}/values' \n\n{\n \"attributes\": [\n \"MESSAGE\"\n],\n \"elements\": [\n {\n \"values\": [\n {\\"client\\\": \\"\\\", \\"data\\\": [\n {\\"empId\\\": \\"\\\", \\"name\\\": \\"\\\", \\"snils\\\": \\"\\\", \\"kigID\\\": \\"\\\", \\"dBrth\\\": \\"\\\", \\"or\\n\\gInn\\\": \\"\\\", \\"kpp\\\": \\"\\\", \\"funRes\\\": \\"\\\", \\"citizen\\\": \\"\\\", \\"staffinn\\\": \\"\\\", \\"isD\\n\\elEm\\\": \\"\\\"},\n {\\"empId\\\": \\"\\\", \\"name\\\": \\"\\\", \\"snils\\\": \\"\\\", \\"kigID\\\": \\"\\\", \\"dBrth\\\": \\"\\\", \\"or\\n\\gInn\\\": \\"\\\", \\"kpp\\\": \\"\\\", \\"funRes\\\": \\"\\\", \\"citizen\\\": \\"\\\", \\"staffinn\\\": \\"\\\", \\"isD\\n\\elEm\\\": \\"\\\"}\n]\n }\n]\n }\n}</code>				
citizen	Гражданство	Integer	Да	от 14 декабря 2001 года N 529-ст "О принятии и введении в действие Общероссийского классификатора стран мира (в ред. Изменений N 1/2003 ОКСМ, N 2/2003 ОКСМ, N 3/2004 ОКСМ, N 4/2004 ОКСМ, N 5/2005 ОКСМ, N 6/2006 ОКСМ, утв. Госстандартом РФ)"
staffinn	ИНН сотрудника	Long	Да	
isDelEm	Признак удаления сотрудника	Boolean	Нет	0 – false (не удалён) 1 – true(удалён)

5. Загрузка данных в справочник «Получаемые сообщения Организации трудоустройства»

Пример тела запроса для загрузки **одного** элемента в справочник (одна строка):

- Справочник с новыми элементами

Атрибут	Описание
int ID	Идентификатор элемента события
Json MESSAGE	Сообщение

```
{
  "attributes": [
    "MESSAGE"
  ],
  "elements": [
    {
      "values": [
        {
          "client": "\",
          "data": [
            {
              "orgInn": "\",
              "orgName": "\",
              "kpp": "\",
              "isDelOrg": "\"
            }
          ]
        }
      ]
    }
  ]
}
```

Название JSON	Название СКУД	Тип данных	Обязательность	Примечание
client	-	String	Да	Клиент, переданный подрядчику для авторизации
orgInn	ИНН организации, где сотрудник трудоустроен	Long	Да	
orgName	Наименование организации трудоустройства	String	Да	
kpp	КПП организации	Long	Да	
isDelOrg	Признак удаления организации	Boolean	Нет	0 – false(не удалён) 1 – true(удалён)

Curl:

```
curl -X 'POST' \
'https://Стенд/dictionaries/v1/{Id справочника}/values' \
-H 'accept: application/json' \
-H 'Namespace: puds-rb' \
-H 'Authorization: {Токен_пользователя}' \
-H 'Content-Type: application/json' \
-d'{
  "attributes": [
    "MESSAGE"
  ],
  "elements": [
    {
      "values": [
        {"client": "\",
         "data": [
           {
             "orgInn": "\",
             "orgName": "\",
             "kpp": "\",
             "isDelOrg": "\"
           }
         ]
       }
    ]
  }
}'
```

Пример тела запроса для загрузки **нескольких** элементов в справочник (несколько строк, загрузка пачкой):

```
{
  "attributes": [
    "MESSAGE"
  ],
  "elements": [
    {
      "values": [
        {
          "client": "\",\"data\": [
            {
              "orgInn": "111", "orgName": "\",", "kpp": "\",",
              "isDelOrg": "\"
            },
            {
              "orgInn": "222", "orgName": "\",", "kpp": "\",", "isDelOrg": "
            }
          ]
        }
      ]
    }
  ]
}
```

6. Загрузка данных в справочник «Получаемые сообщения Объекты»

Пример тела запроса для загрузки **одного** элемента в справочник (одна строка):

- Справочник с новыми элементами

Атрибут	Описание
int ID	Идентификатор элемента события
Json MESSAGE	Сообщение

```
{
  "attributes": [
    "MESSAGE"
  ],
  "elements": [
    {
      "values": [
        {
          "client": "\",
          "data": [
            {
              "objName": "\",
              "uin": "\",
              "ad": "\",
              "orgInn": "\",
              "kpp": "\",
              "date_s": "\",
              "date_f": "\",
              "isDelObj": "\"
            }
          ]
        }
      ]
    }
  ]
}
```

Название JSON	Название СКУД	Тип данных	Обязательность	Примечание
client	-	String	Да	Клиент, переданный подрядчику для авторизации
objName	Наименование объекта	String	Нет	
uin	УИН объекта строительства	String	Да	Из нормативной документации https://stroimprosto-msk.ru/map/
ad	Адрес объекта	String	Да	
orgInn	ИНН организации-генподрядчика	Long	Да	
kpp	КПП организации - генподрядчика	Long	Да	
date_s	Дата начала строительства	DateTime	Да	Из нормативной документации https://stroimprosto-msk.ru/map/
date_f	Дата окончания строительства	DateTime	Нет	Из нормативной документации https://stroimprosto-msk.ru/map/

Название JSON	Название СКУД	Тип данных	Обязательность	Примечание
isDelObj	Признак удаления объекта	Boolean	Нет	0 – false (не удалён) 1 – true(удалён)

Curl:

```
curl -X 'POST' \
'https://{{Стенд}}/dictionaries/v1/{{Id справочника}}/values' \
-H 'accept: application/json' \
-H 'Namespace: puds-rb' \
-H 'Authorization: {Токен пользователя}' \
-H 'Content-Type: application/json' \
-d '{
  "attributes": [
    "MESSAGE"
  ],
  "elements": [
    {
      "values": [
        {"\\"client\": \"\",
          \"data\": [
            {
              \"objName\": \"\",
              \"uin\": \"\",
              \"ad\": \"\",
              \"orgInn\": \"\",
              \"kpp\": \"\",
              \"date_s\": \"\",
              \"date_f\": \"\",
              \"isDelObj\": \"\"}
            ]
          }
        ]
      }
    }
  ]
}'
```

Пример тела запроса для загрузки **нескольких** элементов в справочник (несколько строк, загрузка пачкой):

```
{  
  "attributes": [  
    "MESSAGE"  
  ],  
  "elements": [  
    {  
      "values": [  
        {"client": "", "data": [  
          {"objName": "", "uin": "", "ad": "", "orgInn": "", "kpp": "", "date_  
s": "", "date_f": "", "isDelObj": ""},  
          {"objName": "", "uin": "", "ad": "", "orgInn": "", "kpp": "", "date_  
s": "", "date_f": "", "isDelObj": ""}  
        ]}  
      ]  
    }  
  ]  
}
```

7. Загрузка данных в справочник «Получаемые сообщения Оборудование»

Пример тела запроса для загрузки одного элемента в справочник (одна строка):

- Справочник с новыми элементами

Атрибут	Описание
int ID	Идентификатор элемента события
Json MESSAGE	Сообщение

```
{
  "attributes": [
    "MESSAGE"
  ],
  "elements": [
    {
      "values": [
        {
          "client": "",
          "data": {
            "devID": "",
            "mac": "",
            "uin": "",
            "name": "",
            "type": "",
            "sn": "",
            "date_s": "",
            "date_f": "",
            "fix_period": "",
            "isDelEqp": ""
          }
        }
      ]
    }
  ]
}
```

Название JSON	Название СКУД	Тип данных	Обязательность	Примечание
client	-	String	Да	Клиент, переданный подрядчику для авторизации
devID	ID прибора	String	Да	УИН объекта строительства- MAC - адрес прибора (через дефис)
mac	MAC - адрес прибора	String	Да	
uin	УИН объекта строительства	String	Да	Из нормативной документации https://stroimprosto-msk.ru/map/
name	Наименование прибора	String	Да	
type	Тип прибора	String	Да	Всегда равен «СКУД»
sn	SN прибора	String	Да	В случае отсутствия SN у прибора (система представляет из себя ПО), подставляется MAC-адрес
date_s	Дата ввода в эксплуатацию	DateTime	Да	
date_f	Дата снятия прибора с эксплуатации	DateTime	Нет	
fix_period	Даты простоя (технического обслуживания)	String	Нет	Перечисление дат простоя (техобслуживания прибора) в текстовом виде
isDelEqp	Признак удаления прибора	Boolean	Нет	

Curl:

```
curl -X 'POST' \
'https://Стенд/dictionaries/v1/{Id справочника}/values' \
-H 'accept: application/json' \
-H 'Namespace: puds-rb' \
-H 'Authorization: {Токен_пользователя}' \
-H 'Content-Type: application/json' \
-d '{
  "attributes": [
    "MESSAGE"
  ],
  "elements": [
    {
      "values": [
        {"client": "\",
          "data": [
            {"devID": "\",
             "mac": "\",
             "uin": "\",
             "name": "\",
             "type": "\",
             "sn": "\",
             "date_s": "\",
             "date_f": "\",
             "fix_period": "\",
             "isDelEqp": "\"
            }
          ]
        }
      ]
    }
  ]
}'
```

Пример тела запроса для загрузки **нескольких** элементов в справочник (несколько строк, загрузка пачкой):

```
{  
  "attributes": [  
    "MESSAGE"  
  ],  
  "elements": [  
    {  
      "values": [  
        {"client": "", "data": [  
          {"devID": "", "mac": "", "uin": "", "name": "", "type": "", "sn": "",  
          "date_s": "", "date_f": "", "fix_period": "", "isDelEqp": ""},  
          {"devID": "", "mac": "", "uin": "", "name": "", "type": "", "sn": "",  
          "date_s": "", "date_f": "", "fix_period": "", "isDelEqp": ""}  
        ]}  
      ]  
    }  
  ]  
}
```

8. Загрузка данных в Kafka

8.1 Структура JSON для отправки массива сообщений в справочник «Получаемые сообщения КПП»

Для отправки данных в Kafka необходимо использовать следующий метод:
 POST {{Стенд}}/puds/api/KafkaMessage/SendMultipleMessage?topic={topic}.

```
[  
  {  
    "client": "",  
    "f_id": "",  
    "empId": "",  
    "dt": "",  
    "et": "",  
    "devID": "",  
    "pt": "",  
    "type": ""  
  },  
  {  
    "client": "",  
    "f_id": "",  
    "empId": "",  
    "dt": "",  
    "et": "",  
    "devID": "",  
    "pt": "",  
    "type": ""  
  }  
]
```

Название JSON	Название СКУД	Тип данных	Обязательность	Примечание
client	-	String	Да	Клиент, переданный подрядчику для авторизации
f_id	ID события прохода в СКУД	String	Да	УИН объекта строительства-ИД события СКУД(через дефис)

Название JSON	Название СКУД	Тип данных	Обязательность	Примечание
empId	ID сотрудника	String	Да	УИН объекта строительства - ИД сотрудника СКУД(через дефис) Связь с таблицей Сотрудников
dt	Дата/время записи	DateTime	Да	UTC+3 Без приведения Формат 'dd.mm.yyyy HH:MM:ss'
et	Тип события	Integer	Да	1 – Вход 2 – Выход
devID	ID прибора	String	Да	УИН объекта строительства-МАС - адрес прибора (через дефис) Связь с таблицей Оборудования
pt	Вид пропуска	Integer	Да	1 – Биометрия 2 – Пропуск
type	Тип пропуска	Integer	Да	1- Постоянный 2 - Временный 3 - Разовый

Curl:

```

curl -X 'POST' \
'https://{{Стенд}}/puds/api/KafkaMessage/SendMultipleMessage?topic={{Название
топика}}' \
-H 'Namespace: puds-rb' \
-H 'Authorization: {{Токен_пользователя}}' \
-d '[
  {
    "client": "",

    "f_id": "",

    "empId": "",

    "dt": "",

    "et": "",

    "devID": "",

    "pt": "",

    "type": ""

  },
  {
    "client": "",

    "f_id": "",

    "empId": "",

    "dt": "",

    "et": "",

    "devID": "",

    "pt": "",

    "type": ""

  }
]'
```

8. Получение переменных значений

1. Параметры client_id и client_secret выдаются по запросу ответственными лицами ДИТ;
2. Переменные идентификаторы справочников выдаются по запросу ответственными лицами ДИТ;
3. Наименование топика Kafka для записи выдаются по запросу ответственными лицами ДИТ.
4. Размер одного пакета «Получаемые сообщения КПП» не должен превышать 999 событий прохода.