



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 –

Приложение 1 к распоряжению
Департамента информационных
технологий города Москвы и
Департамента градостроительной
политики города Москвы
от 24 июня 2015 г.
№ 64-16-307/025/022

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. ДПП 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 ДПП 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 соответствии с настоящим Порядком.

4.2. ДПП 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 ДПП 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 ДПП.

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 ДПП.

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 соглашении 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.

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 КСЗ 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 межсетевое 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 Состав 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