



**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ И СВЯЗИ КУЗБАССА
(МИНЦИФРА КУЗБАССА)**

ПРИКАЗ

от «25» сентября 2023 г. № 98-п
г. Кемерово

**Об утверждении регламента доступа пользователей к сведениям,
содержащимся в информационной системе «Региональная
автоматизированная интеграционная платформа видеонаблюдения и
видеоаналитики Кузбасса»**

Во исполнении распоряжения Правительства Кемеровской области – Кузбасса от 13.07.2022 № 380-р «Об информационной системе «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса» п р и к а з ы в а ю:

1. Утвердить прилагаемый регламент доступа пользователей к сведениям, содержащимся в информационной системе «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса».

2. Настоящий приказ подлежит опубликованию на сайте «Электронный бюллетень Правительства Кемеровской области – Кузбасса».

3. Контроль за исполнением настоящего приказа оставляю за собой.

Министр

М.В. Садиков

УТВЕРЖДЕН

приказом Министерства цифрового
развития и связи Кузбасса
от 25.09.2023 № 98-п

РЕГЛАМЕНТ

**ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ К СВЕДЕНИЯМ, СОДЕРЖАЩИМСЯ В
ИНФОРМАЦИОННОЙ СИСТЕМЕ «РЕГИОНАЛЬНАЯ
АВТОМАТИЗИРОВАННАЯ ИНТЕГРАЦИОННАЯ ПЛАТФОРМА
ВИДЕОНАБЛЮДЕНИЯ И ВИДЕОАНАЛИТИКИ КУЗБАССА»**

2023 г.

Содержание

1. Основные положения	4
2. Срок хранения в Системе архивной информации и порядок предоставления архивной информации в отношении объекта видеонаблюдения по запросу заявителя.....	6
3. Порядок предоставления Оператором Системы доступа к содержащейся в Системе информации на постоянной основе в режиме реального времени	9
4. Права и обязанности участников информационного взаимодействия	17
5. Ответственность за несанкционированное разглашение информации, содержащейся в Системе	19
Приложение № 1 к Регламенту	20
Приложение к Форме запроса	22
Приложение № 2 к Регламенту	23
Приложение № 3 к Регламенту	24
Приложение к Согласию.....	27
Приложение № 4 к Регламенту	29
Приложение № 5 к Регламенту	31
Приложение № 6 к Регламенту	33
Приложение № 7 к Регламенту	35
Приложение № 8 к Регламенту	43
Приложение № 9 к Регламенту	45
Приложение № 10 к Регламенту	46

1. Основные положения

1.1. Настоящий Регламент доступа пользователей к сведениям, содержащимся в информационной системе «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса» (далее — Регламент) определяет виды предоставления доступа к информации содержащейся в информационной системе «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса» (далее – Система), термины и определения, сроки хранения архивной информации, порядок предоставления доступов с отражением последовательности действий и содержания процедур по предоставлению органам государственной власти, органам местного самоуправления, подведомственным организациям и иным лицам, указанным в настоящем Регламенте, в целях осуществления ими функций и полномочий согласно компетенции, а также в целях развития Системы, доступа к содержащейся в Системе информации об объектах видеонаблюдения, а также условия и требования, выполнение которых обеспечивает доступ к информации, содержащейся в Системе, в том числе с помощью соответствующих сервисов Системы, включая выгрузку архивной информации, содержащейся в Системе, права и обязанности вышеуказанных организаций, а также ответственность в рамках предоставления доступа к информации содержащейся в Системе.

1.2. Настоящий Регламент разработан в соответствии с пунктом 1.2 распоряжения Правительства Кемеровской области – Кузбасса от 13.07.2022 № 380-р «Об информационной системе «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасс» (далее – Распоряжение).

1.3. Виды предоставления доступа:

1.3.1. Доступ к содержащейся в Системе информации предоставляется путем предоставления архивной информации в отношении объекта видеонаблюдения по запросу заявителя.

1.3.2. Доступ к содержащейся в Системе информации может предоставляться на постоянной основе, в режиме реального времени.

1.4. В настоящем Регламенте используются следующие термины и их определения:

API – Application Programming Interface – прикладной программный интерфейс.

Автоматизированное рабочее место (АРМ) – аппаратно-программный комплекс, технические средства, которые расположены на рабочем месте и находятся в ведении Пользователя информации, имеющий возможность осуществить доступ к информации, содержащейся в Системе.

Авторизационные данные – учетные данные в формате логин/пароль, предоставляемые Пользователю информации, для осуществления доступа к информации, содержащейся в Системе.

Архивная информация – информация об объектах видеонаблюдения, хранящаяся в Системе в пределах регламентных сроков хранения.

Базовая аутентификация – процесс проверки подлинности Пользователя информации на основе запроса Авторизационных данных.

ВИС – внешняя информационная система, взаимодействующая с Системой.

Доступ к информации, содержащейся в Системе (доступ к Системе) – организационно-технические мероприятия, обеспечивающие получение Пользователями информации доступа к информации, содержащейся в Системе.

Информация, содержащаяся в Системе – информация хранящаяся, обрабатываемая в Системе, в том числе архивная информация.

ЛСВН – локальная система видеонаблюдения – совокупность камер видеонаблюдения или источников видеосигнала и источников(а) видеоизображений(ия), объединенных в логическую единицу.

Несанкционированное разглашение информации, содержащейся в Системе – умышленные или неосторожные действия Пользователя информации с содержащейся в Системе информацией, включая Авторизационные данные, в результате которых она стала доступна лицам, не имеющим права доступа к этой информации.

Оператор АРМ – Пользователь информации, имеющий доступ на постоянной основе к Системе в режиме реального времени с функциями просмотра потоковой информации, просмотра архивной информации, сохранения архивной информации на внешних электронных носителях.

Оператор Системы – Министерство цифрового развития и связи Кузбасса, осуществляющее от имени Кемеровской области – Кузбасса правомочия собственника Системы.

Пользователь информации – работник юридического лица, а также иные уполномоченные лица, которым в соответствии с настоящим Регламентом предоставлен доступ к информации, содержащейся в Системе, в режиме реального времени.

Потоковая информация – информация об объектах видеонаблюдения, просмотр которой со средств видеонаблюдения осуществляется с использованием сервисов Системы в режиме реального времени.

Участники Системы – органы государственной власти Кемеровской области – Кузбасса, органы местного самоуправления муниципальных образований Кемеровской области – Кузбасса, территориальные федеральные органы исполнительной власти Кемеровской области – Кузбасса, подведомственные им учреждения и юридические лица.

Сутки – промежуток времени равный 24 часам, исчисляющийся с момента поступления информации в Систему по часовому показателю до аналогичного временного показателя следующего календарного дня (пример исчисления с 12:05:15 21.06.2023 до 12:05:15 22.06.2023).

2. Срок хранения в Системе архивной информации и порядок предоставления архивной информации в отношении объекта видеонаблюдения по запросу заявителя

2.1. Регламентный срок хранения в Системе архивной информации, поступающей с камер видеонаблюдения Оператора Системы, составляет – 30 (тридцать) суток.

2.2. Срок хранения архивной информации (отдельных фрагментов видеоархива), содержащейся в Системе, может быть продлен по заявке, которая направляется Оператору Системы в порядке, определенном настоящим Регламентом. Для продления установленного срока хранения архивной информации об объекте видеонаблюдения уполномоченным лицам или представителям Участников Системы необходимо направить в письменном виде, в том числе с помощью электронной почты, Оператору Системы заявку с обязательным указанием следующих сведений:

2.2.1. Фамилия, имя, отчество (при наличии) лица, обратившегося с соответствующей заявкой (для уполномоченных лиц или представителей Участников Системы).

2.2.2. Полное наименование Участника Системы, от имени и в интересах которого направляется заявка.

2.2.3. Номер телефона для связи с лицом, направляющим заявку о продлении срока хранения архивной информации.

2.2.4. Адрес электронной почты лица, направляющего заявку о продлении срока хранения архивной информации.

2.2.5. Точные адреса размещения средств видеонаблюдения или уникальный идентификатор средства видеонаблюдения в Системе с которых необходимо продлить срок хранения информации.

2.2.6. Точная дата и временной интервал события, в отношении которого необходима архивная информация, содержащаяся в Системе.

2.2.7. Наименование события, в отношении которого необходима архивная информация, содержащаяся в Системе (дорожно-транспортное происшествие, совершение противоправных действий, в том числе совершение преступления и иное).

2.3. Заявка о продлении срока хранения архивной информации может быть направлена не более трех раз и должна поступить Оператору Системы не позднее чем за 2 (двое) суток до истечения срока хранения архивной информации, установленным настоящим Регламентом.

2.4. После получения Оператором Системы в порядке, определенном пунктом 2.2 настоящего Регламента, заявки на продление срока хранения архивной информации при условии соответствия данной заявки определенным настоящим Регламентом требованиям, а также при наличии соответствующей архивной информации в Системе, срок хранения архивной информации продлевается Оператором Системы до 30 (тридцати)

календарных дней, и указанная информация хранится в Системе в течение продленного срока хранения, по истечении которого удаляется из Системы.

2.5. Доступ к содержащейся в Системе архивной информации в отношении конкретного объекта видеонаблюдения может быть предоставлен Участникам Системы (далее – Заявитель).

2.6. Доступ к содержащейся в Системе архивной информации в отношении конкретного объекта видеонаблюдения осуществляется на основании направленной заявки по форме согласно приложению № 1 к настоящему Регламенту в адрес Оператора Системы, посредством использования государственной информационной системы «Единая почтовая система Правительства Кемеровской области – Кузбасса» или государственной информационной системы «Электронный документооборот Правительства Кемеровской области – Кузбасса», а также при личном обращении.

2.7. Заявка направляется Оператору Системы не позднее чем за 12 (двенадцать) рабочих часов до истечения установленного срока хранения информации либо до истечения срока хранения архивной информации, продленного в порядке, определенном настоящим Регламентом.

2.8. Заявка рассматривается Оператором Системы в течение 3 (трех) рабочих дней.

При условии соответствия данной заявки требованиям настоящего Регламента, а также при наличии соответствующей архивной информации в Системе.

Доступ к архивной информации, лицу Участника Системы, указанному в Заявке, предоставляется после готовности архивной информации к выдаче. Участнику Системы необходимо предъявить служебное удостоверение/документ, удостоверяющий личность, в рабочие дни с 08.30 до 17.30 по адресу: г. Кемерово, ул. Арочная, д.37А. Оператор Системы предоставляет доступ к архивной информации путем демонстрации архивной информации на экране монитора и (или) ее сохранения на внешнем электронном носителе в 1 (одном) экземпляре. Выгрузка архивной информации не осуществляется в присутствии Участника Системы.

Внешний электронный носитель, используемый для сохранения архивной информации, содержащейся в Системе, предоставляется Участником Системы, обратившимся с Заявкой о доступе к соответствующей архивной информации, либо лицом, указанным Участником Системы в такой Заявке. Внешний электронный носитель должен иметь свободную для записи емкость в размере не менее чем объем архивной информации, подлежащей выдаче, на основании одной соответствующей Заявки и не должен содержать программ, которые могут оказать вредоносное воздействие на Систему.

Оператор Системы не несет ответственность за сохранность и (или) неизменность информации с момента ее записи на предоставленный Заявителем (лицом, указанным Заявителем в запросе) электронный носитель.

2.9. При предоставлении доступа к архивной информации, содержащейся в Системе, в отношении конкретного объекта видеонаблюдения путем демонстрации архивной информации на экране монитора, запрещается фотографировать, осуществлять видеозапись экранной формы Системы, демонстрирующий, в том числе порядок функционирования Системы. Находясь в помещении Оператора Системы, Участник Системы должен руководствоваться указаниями работника Оператора Системы.

2.10. Все факты доступа к информации, содержащейся в Системе, в том числе факты демонстрации архивной информации, факты ее сохранения на внешних электронных носителях, регистрируются представителем Оператора Системы, осуществляющим доступ к содержащейся в Системе архивной информации, в Журналах учета доступа к информации, содержащейся в Системе, которые оформляются согласно приложению № 9 к настоящему Регламенту. Участник Системы в указанном журнале ставит подпись, подтверждая факт получения запрашиваемых сведений в определенном объеме и факт уведомления о том, что полученные сведения являются информацией ограниченного доступа.

2.11. Заполненные Журналы, предусмотренные пунктом 2.10 настоящего Регламента, хранятся Оператором Системы не менее 3 (трех) лет со дня последней записи.

2.12. Оператор Системы отказывает в предоставлении доступа к архивной информации, содержащейся в Системе, по запросам, оформленным и направленным Оператору Системы с нарушениями требований, установленных законодательством Российской Федерации, правовыми актами Кемеровской области – Кузбасса и настоящим Регламентом, включая запросы от лиц, не обладающих соответствующими полномочиями.

3. Порядок предоставления Оператором Системы доступа к содержащейся в Системе информации на постоянной основе в режиме реального времени

3.1. В соответствии с настоящим Регламентом доступ в Систему для получения информации в режиме реального времени предоставляется Участникам Системы в соответствии с нормативными правовыми актами Российской Федерации в целях осуществления ими своих функций и полномочий и организациям, интегрирующим ЛСВН с Системой, а также в целях повышения эффективности и развития возможностей использования Системы.

3.2. При подключении ЛСВН к Системе, доступ к Системе предоставляется к информации, поступающей с интегрированных камер видеонаблюдения на основании соглашения о взаимодействии при предоставлении информации в информационную систему «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса» (далее – Соглашение) и после проведения мероприятий по подключению ЛСВН к Системе согласно приложению № 7 к настоящему Регламенту.

3.3. Для получения доступа к информации, содержащейся в Системе, в режиме реального времени, Участники Системы, указанные в пункте 3.1, направляют в адрес Оператора Системы заявку на предоставление доступа на постоянной основе в режиме реального времени к информации, содержащейся в Системе (далее – Заявка о доступе на постоянной основе), по форме согласно приложению № 2 к настоящему Регламенту.

3.3.1. При необходимости получения доступа к Системе подведомственным организациям Участников Системы заявку на предоставление доступа на постоянной основе, направляет соответствующий Участник Системы в части своей подведомственной организации в адрес Оператора Системы, в том числе при предоставлении доступа на основании заключенных Соглашений в рамках подключения ЛСВН к Системе.

3.3.2. В случае, если организация, указанная в пункте 3.1 настоящего Регламента, не является подведомственной организацией Участников Системы, заключивших Соглашение в рамках подключения ЛСВН с Системой, направляют самостоятельно заявку о доступе на постоянной основе в адрес Оператора Системы.

3.4. Заявки, оформленные не в соответствии с требованиями пункта 3.3 настоящего Регламента, рассмотрению не подлежат.

3.5. Порядок получения доступа к информации, содержащейся в Системе, установленный пунктом 3.3 настоящего Регламента, не распространяется на работников Оператора Системы и подведомственные ему организации, которые получают доступ к Системе на основании письменного запроса, направленного в рабочем порядке.

3.6. Одновременно с заявкой о доступе на постоянной основе организации, указанные в пункте 3.1 настоящего Регламента, направляют в адрес Оператора Системы Согласие с условиями регламента доступа пользователей к информации, содержащейся в информационной системе «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса» (далее – Согласие) по форме, определенной приложением № 3 к настоящему Регламенту, которое соответствует требованиям установленным приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Согласие такой организацией может не предоставляется только в случае наличия Соглашения (или иного документа, требующего двустороннего подписания), заключённого между Оператором Системы и такой организацией.

Согласия, подписанные уполномоченными лицами организаций, указанных в пункте 3.1 настоящего Регламента, направляются централизованно соответствующей организацией.

3.7. Учитывая наличие либо отсутствие у Оператора Системы технической возможности для предоставления доступа к Системе, а также оснований для предоставления доступа к Системе, Оператор Системы в течение 30 (тридцати) календарных дней с момента получения заявки о доступе на постоянной основе, принимает решение о предоставлении либо отказе в предоставлении доступа к информации, содержащейся в Системе.

3.7.1. О принятом решении Оператор Системы уведомляет в установленном порядке организации, указанные в пункте 3.1 настоящего Регламента, направившие Оператору Системы заявку о доступе на постоянной основе. В случае отсутствия технической возможности для предоставления доступа к Системе Оператор Системы информирует вышеуказанных лиц об условиях проведения дополнительных мероприятий для предоставления доступа к Системе.

3.7.2. При проведении дополнительных мероприятий и наличии оснований предоставления доступа к Системе организациям, указанным в пункте 3.1 настоящего Регламента, предоставляется доступ в соответствии с условиями настоящего Регламента.

3.8. В случае удовлетворения Оператором Системы заявки о доступе на постоянной основе:

3.8.1. Оператор Системы вносит пользователей в реестр Пользователей Системы и предоставляет Авторизационные данные с соответствующими правами для осуществления доступа к информации, содержащейся в Системе, в течение 30 (тридцати) рабочих дней со дня принятия такого решения.

3.8.2. Оператор Системы предоставляет Авторизационные данные Пользователю информации любым возможным способом, отвечающим критериям сохранности информации, под личную подпись по Акту передачи Авторизационных данных, который составляется по форме согласно приложению № 4 к настоящему Регламенту.

3.8.3. Авторизационные данные не подлежат разглашению и передаче третьим лицам.

3.9. Пользователи информации и Операторы АРМ, получившие в установленном порядке доступ к информации, содержащейся в Системе, должны предоставить свое согласие на сбор, хранение и обработку своих персональных данных согласно приложению № 10 к настоящему Регламенту.

3.10. В случае невыполнения Пользователем информации и Оператором АРМ условий, указанных в пунктах 3.6, 3.9 настоящего Регламента, доступ к информации, содержащейся в Системе, не предоставляется.

3.11. Доступ Пользователей и Оператора АРМ к информации, содержащейся в Системе, должен осуществляться по каналам связи, организованным в соответствии с требованиями, согласно приложению № 8 к настоящему Регламенту либо с помощью иных способов предоставления доступа.

3.12. Рекомендуемые технические требования к стационарным АРМ Пользователя, подключаемым к Системе, для осуществления доступа к информации, содержащейся в Системе:

3.12.1. Персональный компьютер с характеристиками не хуже:

- Intel Core i3-4130 или более производительный (например, Intel Core i5-4xxx);
- оперативная память – не менее 4 ГБ, частота не менее 1600 МГц;
- размер жесткого диска – не менее 40 ГБ;
- пропускная способность сетевого интерфейса - 100 Мбит/с, для просмотра несжатого видео с множества камер одновременно рекомендуется не менее 1000 Мбит/с.

3.12.2. Программные средства:

- Windows 10 – все редакции; Windows Server 2016 – Standard, Datacenter; Windows Server 2019 – Standard, Datacenter; Windows Server 2022 – Datacenter, Astra Linux Special Edition не ниже 1.7.

- программное обеспечение SecurOS (версия не ниже 11.5).

3.13. Программно-технические требования по соблюдению требований информационной безопасности 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» (далее - Приказ) необходимых для осуществления доступа к информации, содержащейся в Системе:

3.13.1. Требования сетевого подключения:

Канал связи пропускной способностью не менее 20 Мбит/с (для одновременного просмотра до 5 (пяти) видеопотоков со средств видеонаблюдения в высоком качестве).

Для доступа к Системе необходимо иметь защищенный канал связи с Оператором Системы на следующих условиях:

- соглашение об информационном взаимодействии;
- соглашение о межсетевом взаимодействии или соглашение о подключении к защищенной сети (форма соглашения о межсетевом взаимодействии или соглашения о подключении к защищенной сети расположена на сайте Оператора Системы (digital42.ru), раздел «Документы», подраздел «Информационная безопасность», пункт меню «Шаблоны документов»);
- наличие технической возможности в соответствии с предложенными схемами защищённого взаимодействия:

Таблица 1. Схемы защищенного взаимодействия

Номер схемы подключ ения	Средство защиты информации	Описание
1	2	3
Схема № 1.1	VIPNet Client 4	Для обработки защищаемой информации АРМ пользователя должно быть оснащено: программным комплексом VIPNet Client 4 для VIPNet сети № 2301, имеющим сертификат соответствия ФСТЭК России и ФСБ России (подключение осуществляет администратор защищенной VIPNet сети № 2301).
Схема № 1.2	VIPNet Coordinator HW 4	Для обработки защищаемой информации АРМ пользователя должно быть оснащено: межсетевым экраном VIPNet Coordinator HW 4, имеющего сертификат соответствия ФСТЭК России и ФСБ России, обеспечивающего туннелирование трафика с VIPNet сетью № 2301 (подключение осуществляет администратор защищенной VIPNet сети № 2301).
Схема № 1.3	VIPNet (Межсетевое взаимодействи е)	Для обработки защищаемой информации АРМ пользователя должно быть оснащено: организовано подключение VIPNet сети Организации к VIPNet сети № 2301 для обеспечения межсетевого взаимодействия.

1	2	3
Схема № 2.1	СКЗИ Континент АП	Для обработки защищаемой информации АРМ пользователя должно быть оснащено: СКЗИ Континент-АП, имеющим сертификат соответствия ФСБ России; межсетевым экраном (программным), имеющим сертификат соответствия ФСТЭК России.
Схема № 2.2	АПКШ Континент	Для организации взаимодействия АРМ пользователя должны использоваться каналы связи, защищенные с использованием шлюза безопасности аппаратно-программного комплекса шифрования Континент, обеспечивающего криптографическую защиту информации между сегментом локальной вычислительной сети Организации и сегментом ЛВС Администрации Правительства Кузбасса. Для обработки защищаемой информации АРМ пользователя должно быть оснащено: межсетевым экраном АПКШ «Континент», имеющего сертификат соответствия ФСТЭК России и ФСБ России.
Схема № 2.3	АПКШ Континент	Для обработки защищаемой информации АРМ пользователя должно быть: организовано подключение VPN сети на базе АПКШ «Континент» Организации к VPN сети на базе АПКШ «Континент» Оператора Системы для обеспечения межсетевого взаимодействия.

3.13.2. Требования к антивирусной защите:

На рабочем месте Пользователя информации и Оператора АРМ должна быть установлена антивирусная защита, имеющая сертификат соответствия ФСТЭК России, соответствующая требованиям настоящего Регламента.

3.13.3. Требования к защите от несанкционированного доступа:

На рабочем месте Пользователя информации и Оператора АРМ должно быть установлено средство защиты информации от несанкционированного доступа, имеющее сертификат соответствия ФСТЭК России и удовлетворяющее требованиям настоящего Регламента.

3.13.4. Требования к межсетевому экранированию и обнаружению вторжений:

Рабочее место Пользователя информации и Оператора АРМ должно быть отделено от информационно-телекоммуникационных сетей общего

пользования, сертифицированным ФСТЭК России межсетевым экраном, удовлетворяющее требованиям настоящего Регламента.

3.13.5. Требования к анализу защищенности:

Программное обеспечение на рабочем месте Пользователя информации и Оператора АРМ должно на постоянной основе проверяться средством анализа защищенности, удовлетворяющее требованиям настоящего Регламента.

3.13.6. Требования к защите технических средств:

Рабочее место Пользователя информации и Оператора АРМ в части защиты технических средств должно соответствовать требованиям настоящего Регламента.

3.13.7. Требования к регистрации событий безопасности:

На рабочем месте Пользователя информации и Оператора АРМ и оборудовании внутри контролируемой зоны Участников Системы, должна осуществляться регистрация событий безопасности, соответствующая требованиям настоящего Регламента.

3.13.8. Требования к ограничению программной среды:

На рабочем месте Пользователя информации и Оператора АРМ должна быть ограничена программная среда, соответствующая требованиям приказа о разрешенном программном обеспечении, утвержденного Оператором Системы. Приказ о разрешенном программном обеспечении размещается на официальном сайте Оператора Системы.

3.14. Оператор Системы имеет право прекратить доступ Пользователя информации и Оператора АРМ к информации, содержащейся в Системе, в следующих случаях:

3.14.1. Нарушения Пользователя информации и Оператора АРМ положений настоящего Регламента, а также действующего законодательства Российской Федерации и Кемеровской области – Кузбасса.

3.14.2. В случае прекращения доступа к информации, содержащейся в Системе, в связи с неиспользованием Пользователя информации и Оператора АРМ своих Авторизационных данных, доступ к информации, содержащейся в Системе, восстанавливается согласно порядку, установленному пунктами 3.2 - 3.13 настоящего Регламента.

3.15. Доступ организаций, указанных в пункте 3.1 настоящего Регламента, являющихся операторами ВИС (далее – Оператор ВИС), к информации, содержащейся в Системе, осуществляется в рамках проведения технической интеграции ВИС и Системы.

3.15.1. Проведение технической интеграции ВИС и Системы осуществляется на основании письменной заявки на техническую интеграцию ВИС и Системы (далее – Заявка на интеграцию) Оператора ВИС, направленной посредством использования государственной информационной системы «Единая почтовая система Правительства Кемеровской области – Кузбасса» или государственной информационной системы «Электронный документооборот Правительства Кемеровской области – Кузбасса» в адрес

Оператора Системы по форме согласно приложению № 6 к настоящему Регламенту.

3.15.2. Оператор Системы при рассмотрении Заявки на интеграцию, вправе запросить дополнительную детализированную информацию, направленную в виде запроса с прилагаемой опросной формой (далее – опросная форма) для заполнения, связанную с интеграцией ВИС.

3.15.3. Оператор ВИС обязан предоставить дополнительную детализированную информации в виде опросной формы путем направления официального письма посредством использования государственной информационной системы «Единая почтовая система Правительства Кемеровской области – Кузбасса» или государственной информационной системы «Электронный документооборот Правительства Кемеровской области – Кузбасса» в адрес Оператора Системы.

3.15.4. Оператор Системы принимает решение об осуществлении интеграции ВИС и Системы и предоставлении уполномоченным лицам Оператора ВИС доступа к информации, содержащейся в Системе, в соответствии с техническими возможностями Системы, либо об отказе в осуществлении такой интеграции. При этом, Оператор Системы имеет право отказать в интеграции ВИС и Системы и оставить заявку на интеграцию без удовлетворения в случае отсутствия технической возможности такой интеграции, либо в случае нецелесообразности проведения такой интеграции.

3.15.5. Оператор Системы уведомляет Оператора ВИС о результатах рассмотрения заявки на интеграцию и принятом решении в течение 30 (тридцати) календарных дней со дня получения заявки на интеграцию.

3.15.6. При принятии решения о наличии возможности для интеграции ВИС и Системы, Оператор Системы направляет в адрес Оператора ВИС описание возможностей API Системы (спецификация интерфейса интеграции ВИС и Системы) и в рамках рабочего взаимодействия принимает решение по следующим направлениям:

3.15.6.1. Определение типа интеграции.

3.15.6.2. Утверждение архитектуры и требований к интеграции.

3.15.6.3. Определение требований к каналам связи в зависимости от потребностей информационной системы.

3.15.6.4. Определение параметров по настройке сервисов взаимодействия в рамках опытной эксплуатации.

3.15.6.5. Определение требований к информационной безопасности интеграции с Системой.

3.15.6.6. Проведение итогового тестирования.

3.15.6.7. Иные вопросы информационно-технического взаимодействия.

3.15.7. Интеграция ВИС и Системы осуществляется на основании подписанного Оператором ВИС и Оператором Системы Соглашения о взаимодействии между Оператором Системы и Оператором ВИС (далее - Соглашение о взаимодействии) по форме, согласно приложению № 7 к

настоящему Регламенту. Соглашение о взаимодействии не заключается с Операторами ВИС, указанными в подпункте 3.15.2 настоящего Регламента.

3.15.8. Уполномоченные лица Оператора ВИС получают доступ к Системе после подписания акта передачи Авторизационных данных в соответствии с приложением № 5 к настоящему Регламенту, через интегрированную с Системой ВИС.

3.15.9. Уполномоченным лицам Оператора ВИС могут быть переданы Авторизационные данные для доступа к Системе, согласно приложению № 4 к настоящему Регламенту.

3.15.10. Уполномоченным лицам Оператора ВИС, Пользователям ВИС запрещается использовать полученную из Системы информацию в целях извлечения прибыли и иных коммерческих целях, в том числе в предпринимательской деятельности.

4. Права и обязанности участников информационного взаимодействия

4.1. Организации, указанные в пункте 3.1 настоящего Регламента, в рамках предоставления доступа к информации, содержащейся в Системе в режиме реального времени, обязуются:

4.1.1. Сформировать соответствующий перечень Пользователей информации и Операторов АРМ для получения доступа к информации, содержащейся в Системе, в целях осуществления своих функций и полномочий.

4.1.2. Уведомить Оператора Системы об изменениях перечня Пользователей информации и Операторов АРМ в случае, если такие изменения влекут прекращение доступа Пользователя информации и/или Оператора АРМ к Системе в срок не менее 1 рабочего со дня соответствующих изменений.

4.1.3. Организовать защиту АРМ Пользователя информации и/или Оператора АРМ и канала связи, посредством выполнения комплекса мероприятий и применения технических средств защиты информации в соответствии с требованиями законодательства Российской Федерации о техническом регулировании и Согласия.

4.1.4. Довести до Пользователей информации и Операторов АРМ, имеющих право доступа к информации, содержащейся в Системе обязательство использовать только персональные Авторизационные данные (выданные конкретному должностному лицу) для доступа к информации, содержащейся в Системе.

4.1.5. Довести до Пользователей информации и Операторов АРМ, имеющих право доступа к информации, содержащейся в Системе необходимость ознакомления с требованиями Руководства Пользователя, включая все последующие обновления указанного Руководства, и необходимость соблюдения требований к информационной безопасности Системы.

4.2. Заявители, указанные в разделе 2 настоящего Регламента, получившие доступ к архивной информации в отношении конкретного объекта видеонаблюдения и организации, указанные в пункте 3.1 настоящего Регламента, получившие доступ к Системе в режиме реального времени, обязуются:

4.2.1. Использовать информацию, обрабатываемую в Системе, полученную в соответствии с настоящим Регламентом, исключительно для реализации своих функций и полномочий и на условиях настоящего Регламента.

4.2.2. Обеспечить защиту информации, обрабатываемую в Системе, от распространения третьим лицам и размещения в открытом доступе, а также от посягательств и попыток их обнародования третьими лицами.

4.2.3. Сведения, полученные в соответствии с настоящим Регламентом, не использовать в коммерческих целях и для нужд третьих лиц, вне

зависимости от имеющихся у Организации обязательств перед третьими лицами.

4.3. Организации, указанные в пункте 3.1 настоящего Регламента, в рамках предоставления доступа к Системе вправе регламентировать права и обязанности Пользователей информации и Операторов АРМ с учетом применения Методических рекомендаций, организациям, работники которых являются Пользователями информации и Операторами АРМ информационной системы «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса», согласно приложению к приложению № 3 настоящего Регламента.

4.4. Оператор Системы в рамках предоставления доступа к информации, содержащейся в Системе, обязуется реализовать организационно-технические меры защиты информации, обрабатываемой в Системе, включая меры по обеспечению ее конфиденциальности, целостности и доступности в соответствии с требованиями законодательства Российской Федерации.

4.5. Оператор Системы в рамках предоставления доступа к информации, содержащейся в Системе вправе:

4.5.1. Прекратить доступ Пользователям информации и Операторов АРМ к информации, содержащейся в Системе, в случаях, предусмотренных подпунктом 3.14 настоящего Регламента.

4.5.2. Использовать и обрабатывать любую информацию, полученную от Пользователя информации и Оператора АРМ в рамках взаимодействия по настоящему Регламенту, в своей деятельности при организации функционирования Системы, в соответствии с действующим законодательством Российской Федерации.

4.5.3. Обрабатывать любую информацию, в своей деятельности при организации функционирования Системы, полученную от Пользователя информации и Оператора АРМ, в рамках взаимодействия по настоящему Регламенту, посредством информационно-телекоммуникационных сервисов третьих лиц, незапрещенных на территории Российской Федерации в целях авторизации Пользователя информации и Оператора АРМ при получении доступа к информации, содержащейся в Системе, а также для оперативного оповещения Пользователей информации и Операторов АРМ о событиях, связанных с объектами видеонаблюдения.

5. Ответственность за несанкционированное разглашение информации, содержащейся в Системе

5.1. Авторизационные данные, предоставленные Пользователю информации и Оператору АРМ для доступа к информации, содержащейся в Системе, являются индивидуальными и не подлежат передаче иным лицам.

5.2. Информация, обрабатываемая в Системе и полученная лицами, указанными в разделах 2 и 3 настоящего Регламента, включает в том числе информацию ограниченного доступа и не подлежит разглашению и передаче третьим лицам, а также использованию в целях извлечения прибыли и иных коммерческих целях, в том числе в предпринимательской деятельности.

5.3. За использование Системы не в соответствии с целями, установленными пунктом 1.1 настоящего Регламента, разглашение сведений, указанных в пункте 5.2 настоящего Регламента, и (или) использование Авторизационных данных иным лицам для получения доступа к информации, содержащейся в Системе, Пользователи информации и Операторы АРМ несут ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение № 1 к Регламенту
доступа пользователей к сведениям,
содержащимся в информационной
системе «Региональная
автоматизированная интеграционная
платформа видеонаблюдения и
видеоаналитики Кузбасса»

**Форма запроса
на предоставление архивной информации, содержащейся в
информационной системе «Региональная автоматизированная
интеграционная платформа видеонаблюдения и видеоаналитики
Кузбасса», в отношении конкретного объекта видеонаблюдения**

Угловой штамп Организации

Министру цифрового развития и
связи Кузбасса

Дата, Исх. №

(ФИО)

В целях (указываются цели использования архивной информации, в том числе номера дел, находящихся в производстве судов, арбитражных судов, органов дознания или следствия, номера КУСП и т.п.)

на основании (указываются ссылки на правовые нормы и (или) документы, подтверждающие функции и полномочия, в рамках реализации которых запрашивается информация) _____ прошу Вас предоставить _____

(должность)

(Ф.И.О.)

путем просмотра/сохранения на внешнем электронном носителе информацию, содержащуюся в Системе и поступившую с видеочамеры в период времени с _____:____ час. «____» _____ 202__ года до _____:____ час «____» _____ 202__ года, расположенной по адресу: _____.

Обязуюсь использовать полученную информацию в соответствии с Регламентом доступа пользователей к информации, содержащейся в информационной системе «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса» исключительно в указанных в настоящем запросе целях и не передавать ее каким-либо иным лицам, за исключением суда, арбитражного суда, органов

дознания (следствия), органов и должностных лиц, осуществляющих производство по делу об административном правонарушении, в рамках которого запрашивается информация.

(должность)

(подпись)

(ФИО)¹

¹ Если письменный запрос направляется не самим Заявителем, а уполномоченным им лицом, к письменному запросу должен быть приложен документ, подтверждающий полномочия лица на подписание данного запроса и его направление в адрес Министерства цифрового развития и связи Кузбасса

Приложение к Форме запроса на предоставление архивной информации, содержащейся в информационной системе «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса», в отношении конкретного объекта видеонаблюдения

Правила заполнения запроса на предоставление архивной информации, содержащейся в информационной системе «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса»

Письменный запрос на предоставление архивной информации, содержащейся в информационной системе «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса», в отношении конкретного объекта видеонаблюдения, должен быть оформлен на бланке Заявителя (при наличии), зарегистрирован Заявителем, закреплен печатью (при наличии) и содержать:

1. Наименование Заявителя с указанием ИНН, ОГРН (при наличии) или других идентифицирующих Заявителя признаков (Фамилия, имя, отчество, номер удостоверения/справки (при наличии)).
2. Номер заявки, присвоенный заявителю при обращении (при наличии).
3. Обоснование необходимости просмотра или предоставления архивной информации, содержащейся в Системе, с указанием ссылки на правовые нормы и (или) документы, подтверждающие функции, полномочия, в рамках реализации которого Заявителю необходима содержащаяся в Системе архивная информация.
4. Точный временной интервал события, в отношении которого Заявителю необходима архивная информация, содержащаяся в Системе.
5. Точный адрес места размещения средства видеонаблюдения, архивная информация с которого запрашивается или уникальный идентификатор средства видеонаблюдения в Системе.
6. Фамилию, имя, отчество (при наличии) лица, обратившегося с заявкой на сохранение архивной информации с камер видеонаблюдения для ее последующего предоставления Заявителю в соответствии со сроками хранения, установленными настоящим Регламентом.

Приложение № 2 к Регламенту
доступа пользователей к сведениям,
содержащимся в информационной
системе «Региональная
автоматизированная интеграционная
платформа видеонаблюдения и
видеоаналитики Кузбасса»

Министру цифрового развития и
связи Кузбасса

(ФИО)

**Форма заявки²
на предоставление доступа на постоянной основе в режиме реального
времени к информации, содержащейся в информационной системе
«Региональная автоматизированная интеграционная платформа
видеонаблюдения и видеоаналитики Кузбасса»**

(Наименование организации) _____ в
(Ф.И.О., должность) _____
просит предоставить доступ на постоянной основе в режиме реального
времени с функциями просмотра потоковой информации, просмотра архивной
информации информационной системы «Региональная автоматизированная
интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса»
следующим работникам:

№ п/ п	ФИО	Подразделение организации, должность	Контактный номер телефона	Адрес электронной почты

Уполномоченное на взаимодействие с Оператором Системы по
вопросам получения доступа к информации, содержащейся в Системе, лицо:

(ФИО, должность, рабочий и мобильный телефон, адрес электронной
почты)

(должность) _____
(подпись) _____
(ФИО)

² Заявка подписывается уполномоченным на ее подписание лицом и направляется в Министерство цифрового развития и связи Кузбасса в письменной форме по почте, с использованием системы электронного документооборота либо предъявляется непосредственно в Министерство

Приложение № 3 к Регламенту
доступа пользователей к сведениям,
содержащимся в информационной
системе «Региональная
автоматизированная интеграционная
платформа видеонаблюдения и
видеоаналитики Кузбасса»

Форма согласия с условиями Регламента доступа Пользователей информации и Операторов АРМ к информации, содержащейся в информационной системе «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса».

« ___ » _____ года

1. Изучив текст Регламента доступа Пользователей информации и Операторов АРМ к информации, содержащейся в информационной системе «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса», утвержденного приказом Министерства цифрового развития и связи Кузбасса от « ___ » _____ 202__ г. № _____ «Об утверждении регламента доступа пользователей к сведениям, содержащимся в информационной системе «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса» (далее – Регламент), _____ (Наименование организации, далее – Организация) подтверждает свое согласие с условиями, предусмотренными Регламентом.

2. Организация уведомлена, что:

2.1. Авторизационные данные Пользователя информации и Оператора АРМ, предоставленные Организации для доступа к информации, содержащейся в информационной системе «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса» (далее – Система), являются индивидуальными и не подлежат разглашению и передаче третьим лицам.

2.2. Информация, обрабатываемая в Системе, а также иная информация, полученная Организацией в соответствии с Регламентом, содержит в том числе информацию ограниченного доступа.

2.3. Оператор Системы вправе использовать и обрабатывать любую информацию, полученную от Пользователя информации и Оператора АРМ в рамках взаимодействия по настоящему Регламенту, в своей деятельности при организации функционирования Системе, в соответствии с действующим законодательством Российской Федерации.

2.4. Оператор Системы вправе обрабатывать любую информацию, при организации функционирования Системы, полученную от Пользователя

информации и Оператора АРМ, в рамках взаимодействия по настоящему Регламенту, посредством информационно-телекоммуникационных сервисов третьих лиц, незапрещенных на территории Российской Федерации в целях авторизации Пользователя информации и Оператора АРМ при получении доступа к информации, содержащейся в Системе, а также для оперативного оповещения Пользователей информации и Операторов АРМ о событиях, связанных с объектами видеонаблюдения.

3. В целях соблюдения требований Регламента, Организация обязуется:

3.1. Использовать информацию, обрабатываемую в Системе, полученную в соответствии с настоящим Регламентом, исключительно для реализации своих функций и полномочий и на условиях Регламента.

3.2. Обеспечить защиту информации, обрабатываемую в Системе, от распространения третьим лицам и размещения в открытом доступе, а также от посягательств и попыток их обнародования третьими лицами.

3.3. Сведения, полученные в соответствии с настоящим Регламентом, не использовать в коммерческих целях и для нужд третьих лиц, вне зависимости от имеющихся у Организации обязательств перед третьими лицами.

3.4. Довести до Пользователей информации и Операторов АРМ обязательства о запрете передачи информации, содержащейся в Системе, в средства массовой информации.

3.5. Принять организационно-технические меры для защиты информации в системах Организации, в которых идет обработка полученной из Системы информации, включая меры по обеспечению конфиденциальности и целостности полученной из Системы информации, включая:

3.5.1. Обработку указанной информации и размещение систем, в которых осуществляется ее обработка, в выделенных помещениях, защищенных от несанкционированного доступа.

3.5.2. Обеспечение защиты компонентов систем Организации, в которых осуществляется обработка полученной из Системы информации, от несанкционированного доступа.

3.5.3. Использование средств защиты на компонентах систем Организации, в которых осуществляется обработка полученной из Системы информации.

3.5.4. Доведение требований безопасности и ответственности за их нарушение до работников Организации, которым предоставляется доступ к Системе.

3.6. Сформировать соответствующий перечень Пользователей информации и Операторов АРМ для получения доступа к информации, содержащейся в Системе, в целях осуществления своих функций и полномочий.

3.7. Уведомить Оператора Системы об изменениях перечня Пользователей информации и Операторов АРМ информации в случае, если такие изменения влекут прекращение доступа Пользователей информации и

Операторов АРМ к Системе в срок не более 1 рабочего со дня соответствующих изменений.

3.8. Довести до Пользователей информации и Операторов АРМ, имеющих право доступа к информации, содержащейся в Системе обязательство использовать только персональные Авторизационные данные (выданные конкретному должностному лицу) для доступа к информации, содержащейся в Системе.

3.9. Довести до Пользователей информации и Операторов АРМ, имеющих право доступа к информации, содержащейся в Системе, необходимость ознакомления с требованиями Руководства Пользователя, включая все последующие обновления указанного Руководства, и необходимость соблюдения требований к информационной безопасности Системы.

3.10. Довести до Пользователей информации и Операторов АРМ обязательства о необходимости своевременно проводить обновление программного и аппаратного обеспечения, используемого при подключении к информационной системе «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса».

4. Организация проинформирована о том, что:

4.1. Вправе регламентировать права и обязанности Пользователей информации и Операторов АРМ Системы с учетом применения Методических рекомендаций организациям, работники которых являются Пользователями информационной системы «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса», согласно приложению к настоящему Соглашению.

4.2. Несет ответственность в соответствии с действующим законодательством Российской Федерации за использование информации, находящейся в Системе не в соответствии с определенными Регламентом целями, а также разглашение информации ограниченного доступа, указанной в разделе 5 Регламента и разделе 1 настоящего Соглашения.

(должность)

(подпись)

(ФИО)

Приложение к Соглашению
с условиями Регламента доступа
пользователей к сведениям,
содержащимся в информационной
системе «Региональная
автоматизированная интеграционная
платформа видеонаблюдения и
видеоаналитики Кузбасса»

**Методические рекомендации организациям, работники которых
являются Пользователями информационной системы «Региональная
автоматизированная интеграционная платформа видеонаблюдения и
видеоаналитики Кузбасса»**

В договоре, должностной инструкции или ином документе работника³, являющегося пользователем информационной системы «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса» (далее – Система), необходимо предусмотреть следующее:

1. Обязательство об использовании персональных Авторизационных данных (выданные конкретному работнику) для доступа к информации, содержащейся в Системе.

2. Обязательство о предоставлении согласия на обработку, а также передачу персональных данных работника третьим лицам, в том числе Министерству цифрового развития и связи Кузбасса, включая подведомственные ему организации, в целях использования указанной информации при решении вопросов, связанных с предоставлением доступа к информации содержащейся в Системе, в том числе использования такой информации, в соответствии с действующим законодательством Российской Федерации. При этом не допускать распространение полученной информации, содержащейся в Системе, третьим лицам.

3. Обязанность работника руководствоваться в своей работе установленными документами (положениями и иное), а так же Регламентом доступа пользователей к информации, содержащейся в информационной системе «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса», утвержденным приказом Министерства цифрового развития и связи Кузбасса от «__» _____ 202__ г. № «__» «Об утверждении регламента доступа пользователей к сведениям, содержащимся в информационной системе «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса».

4. Обязательства по соблюдению требований информационной

³ Должностное лицо назначается на должность из числа штатных работников организации.

безопасности при работе с Системой, установленных действующим законодательством Российской Федерации.

5. Обязательства о недопустимости совершения неправомерных действий, которые могут нарушить конфиденциальность, целостность или доступность информации, обрабатываемой в Системе.

6. Обязанность предоставлять Оператору Системы разъяснения, объяснения и иное при необходимости, с целью выявления нарушения конфиденциальности, целостности или доступности обрабатываемой в Системе информации и на оборудовании организации.

7. Ответственность в виде применения мер дисциплинарного взыскания к работнику таких как: замечания, выговора, увольнения или иное в случае разглашения персональных Авторизационных данных, информации, содержащейся в Системе и (или) использования Авторизационных данных иного Пользователя для получения доступа к информации, содержащейся в Системе, или за правонарушения, повлекшие нарушение конфиденциальности, целостности или доступности информации, обрабатываемой в Системе и на оборудовании организации, а также Системы в целом, в соответствии с законодательством Российской Федерации.

Приложение № 4 к Регламенту
доступа пользователей к сведениям,
содержащимся в информационной
системе «Региональная
автоматизированная интеграционная
платформа видеонаблюдения и
видеоаналитики Кузбасса»

**Форма акта
передачи Авторизационных данных Пользователю**

г. Кемерово

« ___ » _____ 202__ г.

1. Оператор Системы в лице _____ (ФИО, должность) предоставил доступ к информационной системе «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса» (далее – Система), посредством передачи Авторизационные данные для доступа к информации, содержащейся в Системе, а _____ (наименование Организации) в лице _____, далее по тексту – Пользователь, принял указанную информацию, согласно Таблице:

Таблица

№	ФИО	ЛОГИН	ПАРОЛЬ

2. Настоящим Пользователь подтверждает, что:

2.1. Ознакомлен с условиями Регламента доступа пользователей к информации, содержащейся в информационной системе «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса», утвержденного приказом Министерства цифрового развития и связи Кузбасса от « ___ » _____ 202__ г. № « ___ » (далее – Регламент).

2.2. Уведомлен о том, что Авторизационные данные, а также информация, содержащаяся в Системе, являются информацией ограниченного доступа и не подлежат разглашению и передаче третьим лицам.

2.3. Обязуется не разглашать информацию ограниченного доступа, полученную посредством Системы и не передавать полученные Авторизационные данные третьим лицам для доступа к Системе.

2.4. Уведомлен, что несет административную, гражданскую и дисциплинарную ответственность в соответствии с действующим законодательством Российской Федерации, за разглашение информации ограниченного доступа, полученной посредством Системы и за использование информации, находящейся в Системе не в соответствии с определенными Регламентом целями.

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

Передал документы:

(должность) _____
(подпись) _____
(ФИО)

Принял документы:

(должность) _____
(подпись) _____
(ФИО)

Приложение № 5 к Регламенту
доступа пользователей к сведениям,
содержащимся в информационной
системе «Региональная
автоматизированная интеграционная
платформа видеонаблюдения и
видеоаналитики Кузбасса»

**Форма акта
передачи Авторизационных данных Оператору ВИС**

г. Кемерово

« ___ » _____ 202__ г.

1. Оператор Системы в лице _____ (ФИО, должность) предоставил доступ к информационной системе «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса» (далее – Система) для интеграции ВИС _____ (наименование) и Система, посредством передачи Авторизационных данных для доступа к информации, содержащейся в Системе, а Оператора ВИС _____ (наименование Организации) в лице _____, далее по тексту – Оператору ВИС, принял указанную информацию, согласно Таблице:

Таблица

№ п/п	ФИО	ЛОГИН	ПАРОЛЬ

2. Настоящим Оператор ВИС подтверждает, что:

2.1. Ознакомлен с условиями Регламента доступа пользователей к информации, содержащейся в информационной системе «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса», утвержденного приказом Министерства цифрового развития и связи Кузбасса от « ___ » _____ 202__ г. № « ___ » (далее – Регламент).

2.2. Уведомлен о том, что Авторизационные данные, а также информация, содержащаяся в Системе, являются информацией ограниченного доступа и не подлежат разглашению и передаче третьим лицам.

2.3. Обязуется не разглашать информацию ограниченного доступа, полученную посредством Системы и не передавать полученные Авторизационные данные третьим лицам для доступа к Системе.

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

информации, находящейся в Системе не в соответствии с определенными Регламентом целями.

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)

Приложение № 6 к Регламенту
доступа пользователей к сведениям,
содержащимся в информационной
системе «Региональная
автоматизированная интеграционная
платформа видеонаблюдения и
видеоаналитики Кузбасса»

**Форма заявки
на техническую интеграцию внешней информационной системы и
информационной системы «Региональная автоматизированная
интеграционная платформа видеонаблюдения и видеоаналитики
Кузбасса»**

г. Кемерово

«___» _____ 202__ г.

В соответствии с Регламентом доступа пользователей к информации, содержащейся в информационной системе «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса», утвержденным приказом Министерства цифрового развития и связи Кузбасса от «___» _____ 202__ г. № _____ «Об утверждении регламента доступа пользователей к сведениям, содержащимся в информационной системе «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса» (далее - Регламент), (*Наименование организации – Оператора ВИС*) просит Вас в соответствии с _____ (*обоснование необходимости осуществления интеграции с информационной системой «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса» (далее – Система)*) согласовать проведение работ по интеграции информационной системы _____ (*наименование ВИС*) с Системой.

Контактные данные уполномоченного представителя от Оператора ВИС представлены в Таблице.

Таблица

Наименование информационной системы	Ответственный представитель от Оператора информационной системы			
	ФИО	Должность	Контактный телефон	Электронная почта

_____ (*ФИО ответственного представителя от Оператора ВИС*) предупрежден о том, что он должен обеспечить контроль действий Пользователей внешней информационной системы (*наименование*

ВИС) и информирование их о том, что за разглашение Авторизационных данных, в том числе посредством передачи их третьим лицам, а также за несанкционированное разглашение и нецелевое использование информации, содержащейся в Системе, Пользователи несут ответственность, предусмотренную законодательством Российской Федерации. Ответственный представитель от Оператора ВИС, в рамках своей деятельности, обязуется руководствоваться положениями, предусмотренными в Регламенте.

(должность)

(подпись)

(ФИО)⁴

⁴ Заявка должна быть подписана уполномоченным лицом от Оператора ВИС

Приложение № 7 к Регламенту
доступа пользователей к сведениям,
содержащимся в информационной
системе «Региональная
автоматизированная интеграционная
платформа видеонаблюдения и
видеоаналитики Кузбасса»

Форма типового соглашения

**о взаимодействии между Министерством цифрового развития и связи
Кузбасса и _____ (Наименование организации – Оператора ВИС)**

г. Кемерово

«___» _____ 202__ г.

Министерство цифрового развития и связи Кузбасса в лице _____ (должность и ФИО полностью), действующего на основании Положения, далее – Оператор Системы, с одной стороны, и _____ (Наименование организации – Оператора ВИС), именуемое в дальнейшем Оператор ВИС, в лице (должность и ФИО полностью), действующего на основании (Устав, доверенность или иное), совместно именуемые в дальнейшем «Стороны», по отдельности - «Сторона», в целях повышения эффективности использования информационной системы «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса» заключили настоящее Соглашение о нижеследующем:

В целях настоящего Соглашения используются следующие термины и определения:

Авторизационные данные – учетные данные в формате логин/пароль, предоставляемые Оператором Системы для осуществления доступа ВИС к сервисам АРІ Системы.

АРІ – прикладной программный интерфейс.

ВИС – внешняя информационная система, подключаемая к Системе.

Система – информационная система «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса».

Оператор ВИС – организация, осуществляющая полномочия оператора в соответствии с решением органа государственной власти Кемеровской области – Кузбасса, а также иные организации.

Оператор Системы – Министерство цифрового развития и связи Кузбасса. Ответственный представитель – уполномоченное лицо, ответственное за решение вопросов организации взаимодействия в рамках проведения технической интеграции и уполномоченное на взаимодействие от имени и в интересах Стороны, а также ответственное за использование полученной информации, содержащейся в ВИС.

Пользовательский интерфейс – набор программных компонентов для

предоставления функциональных возможностей просмотра и управления проигрываемых видеопотоков из внешних приложений.

Пользователь – лицо, которому Оператором ВИС предоставлен доступ к данным, хранящимся и обрабатываемым в Системе.

Регламент доступа – регламент доступа пользователей к информации, содержащейся в информационной системе «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса», утвержденный приказом Министерства цифрового развития и связи Кузбасса от «___» _____ 202__ г. № _____ «Об утверждении регламента доступа пользователей к сведениям, содержащимся в информационной системе «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса».

1. Предмет соглашения

1.1. Настоящее Соглашение устанавливает порядок взаимодействия Сторон при предоставлении доступа Оператору ВИС, уполномоченному лицу Оператора ВИС к Системе в рамках проведения технической интеграции ВИС (*Наименование ВИС*) с Системой и определяет условия взаимодействия Сторон в целях осуществления ими функций и полномочий согласно компетенции Сторон, доступа к информации содержащейся и обрабатываемой в Системе, в соответствии с правовыми актами Кемеровской области Кузбасса, в том числе с выполнением условий и требований правовых актов Оператора Системы, а также иных требований действующего законодательства Российской Федерации, а также в целях повышения эффективности использования Системы, развития возможностей использования информации об объектах, за которыми ведется видеонаблюдение в Кемеровской области – Кузбассе и повышения эффективности управления городским хозяйством, комфорта и антитеррористической безопасности граждан.

1.2. Настоящее Соглашения заключено и исполняется Сторонами в соответствии с приказом Министерства цифрового развития и связи Кузбасса от «___» _____ 202__ г. № _____ «Об утверждении регламента доступа пользователей к сведениям, содержащимся в информационной системе «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса», а также иными требованиями действующего законодательства Российской Федерации.

1.3. В соответствии с _____ (*правовой акт, в соответствии с которым функционирует ВИС*) _____ (*наименование Оператора ВИС*) является Оператором ВИС (*наименование ВИС*).

1.4. Оператор ВИС использует информацию, содержащуюся в Системе, в целях _____ (*цели использования информации, содержащейся в Системе*).

2. Порядок организации взаимодействия сторон

2.1. Стороны назначают ответственных представителей за взаимодействие в рамках настоящего Соглашения.

2.2. Проведение технической интеграции ВИС и Системы осуществляется на основании заявки и заполненной опросной формы, направленных Оператором ВИС в адрес Оператора Системы в соответствии с разделом 3 Регламента доступа.

2.3. По требованию ответственного представителя Системы Оператор ВИС подготавливает и направляет документацию, содержащую:

- описание информационного обмена ВИС с Системой;
- диаграмму последовательностей;
- частное техническое задание на информационное взаимодействие ВИС и Системы (с указанием спецификации каналов связи);
- иные технические документы, отражающие информационное взаимодействие ВИС с Системой.

2.4. По результатам настройки сервисов взаимодействия Оператор Системы организует проверку готовности программно-технических средств и программного обеспечения систем к совместной работе.

2.5. При успешном результате итогового испытания работы сервисов взаимодействия обеими Сторонами подписывается акт интеграции ВИС и Системы.

3. Права сторон в рамках предоставления доступа к Системе

3.1. Оператор ВИС имеет право использовать сведения, полученные из Системы, исключительно для реализации своих функций и только на условиях настоящего Соглашения.

3.2. Оператор Системы имеет право:

3.2.1. Использовать и обрабатывать информацию, полученную от ВИС в рамках взаимодействия Сторон, в своей деятельности при решении вопросов, связанных с организацией функционирования Системы, в рамках ограничений, установленных действующим законодательством Российской Федерации.

3.2.2. Расторгнуть настоящее Соглашение, в случае неоднократного нарушения Оператором ВИС условий настоящего Соглашения, предварительно уведомив об этом Оператора ВИС не позднее чем за 7 рабочих дней.

3.2.3. Осуществлять управление доступом к Системе, включая блокировку доступа ВИС к Системе в связи с угрозами информационной безопасности и нарушением условий настоящего Соглашения.

3.3. В случае блокировки доступа к Системе, восстановление доступа производится согласно порядку, установленному разделом 3 Регламента доступа.

3.4. Стороны имеют право направлять друг другу запросы, в части касающейся настоящего Соглашения, в любых формах и требовать ответы на указанные запросы в установленные в них сроки.

4. Обязанности Сторон в рамках предоставления доступа к Системе

4.1. Оператор Системы обязуется:

4.1.1. Определить ответственных лиц для организации взаимодействия с Оператором ВИС.

4.1.2. Уведомлять Оператора ВИС об изменении ответственных представителей по вопросам организации подключения к Системе, и направить соответствующие контактные данные, включая Ф.И.О., должности, номера телефонов и адреса электронной почты.

4.1.3. Обеспечивать работоспособность Системы.

4.1.4. Уведомлять Оператора ВИС о проведении плановых технических работ в Системе до начала проведения указанных технических работ.

4.1.5. Уведомлять Оператора ВИС в случае изменений технического обеспечения Системы, которые требуют доработки системы ВИС для сохранения интеграционного взаимодействия.

4.2. Оператор ВИС обязуется:

4.2.1. Определить ответственных лиц для организации взаимодействия с Оператором Системы.

4.2.2. Уведомлять Оператора Системы о изменении ответственных представителей по вопросам организации подключения к Системе, и направить соответствующие контактные данные, включая Ф.И.О., должности, номера телефонов и адреса электронной почты.

4.2.3. По требованию Оператора Системы обеспечить доступ Ответственному представителю Системы к ВИС посредством предоставления Авторизационных данных к ВИС для обеспечения контроля выполнения требований, определенных в Регламенте доступа, а также в целях развития двусторонней оценки необходимых мероприятий по повышению качества работы сервисов интеграции, модуля трансляции Системы, разработке дополнительного функционала и механизмов проверок при настройке сервисов взаимодействия.

4.2.4. Уведомлять Оператора Системы о проведении плановых технических работ ВИС до начала проведения указанных технических работ.

4.2.5. Уведомлять Оператора Системы в случае изменения технического или программного обеспечения ВИС, которое требует изменения установленных настроек сервисов взаимодействия ВИС и Системы.

4.2.6. Предоставлять информацию о работниках Оператора ВИС, получившим доступ к Системе для целей интеграции ВИС и Системы, по запросу Оператора Системы.

4.2.7. Доводить до Пользователей ВИС необходимость соблюдения требований к информационной безопасности Системы.

4.2.8. Для организации и осуществления информационного взаимодействия в рамках настоящего Регламента Стороны обязуются самостоятельно обеспечивать эксплуатацию технических и программных средств, необходимых для каждой из Сторон.

5. Информационная безопасность

5.1. Требования информационной безопасности к ВИС, подключаемым к Системе, определяют особенности информационно-технологического взаимодействия и обеспечиваются комплексом средств и мер информационной безопасности, состоящих из программно-аппаратных средств защиты информации и организационных мероприятий по противодействию потенциальным угрозам, которые направлены на информацию, передаваемую и обрабатываемую в информационных системах.

5.2. Оператор ВИС осуществляет защиту обрабатываемой информации, от несанкционированного доступа, искажения, уничтожения, блокирования, модификации либо неправомерного копирования, а также технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.

5.3. Для обеспечения защиты информации, содержащейся в информационной системе, Оператором ВИС назначается структурное подразделение или должностное лицо (работник), ответственное за защиту информации.

5.4. Меры обеспечения информационной безопасности ВИС, подключаемых к Системе, должны содержать следующие минимальные требования:

5.4.1. Должна использоваться система идентификации и аутентификации Пользователей и осуществляться разграничение прав доступа, а также регистрация действий Пользователей Оператора ВИС.

5.4.2. При доступе в информационную систему должна осуществляться идентификация и аутентификация Пользователей, являющихся работниками оператора (внутренних Пользователей), и процессов, запускаемых от имени этих Пользователей, а также процессов, запускаемых от имени системных учетных записей и внешних Пользователей ВИС.

5.4.3. Должно осуществляться управление доступом к информационной системе.

5.5. Оператором ВИС должны быть установлены и реализованы следующие функции управления учетными записями Пользователей, в том числе внешних Пользователей:

5.5.1. Определение типа учетной записи (внутреннего Пользователя, внешнего Пользователя; системная, приложения; гостевая (анонимная), временная и (или) иные типы записей).

5.5.2. Верификация Пользователя (проверка личности Пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи Пользователя.

5.5.3. Заведение, активация, блокирование и уничтожение учетных записей Пользователей.

5.5.4. Пересмотр и, при необходимости, корректировка учетных записей Пользователей с периодичностью, определяемой оператором.

5.5.5. Порядок заведения и контроля использования гостевых (анонимных) и временных учетных записей Пользователей, а также привилегированных учетных записей администраторов.

5.5.6. Оповещение администратора, осуществляющего управление учетными записями Пользователей, об изменении сведений о Пользователях, их ролях, обязанностях, полномочиях, ограничениях.

5.5.7. Уничтожение временных учетных записей Пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе.

5.5.8. Предоставление Пользователям прав доступа к объектам доступа информационной системы, основываясь на задачах, решаемых Пользователями в информационной системе и взаимодействующими с ней информационными системами.

5.6. Правила и процедуры управления учетными записями Пользователей должны регламентироваться в организационно-распорядительных документах Оператора ВИС.

5.7. Должен быть регламентирован порядок заведения и контроля учетных записей Пользователей, а также привилегированных учетных записей администраторов.

5.8. Правила и процедуры управления учетными записями Пользователей должны регламентироваться в организационно-распорядительных документах, определяющих порядок функционирования ВИС.

5.9. Должна быть обеспечена защита от несанкционированного доступа, в том числе при использовании средств телекоммуникаций, включая подключение и активность стороннего устройства в сети (например, устройства видеозахвата изображения).

5.10. Организация дополнительных мер информационной безопасности:

5.10.1. Принять и реализовать организационно-технические меры для защиты информации, включая меры по обеспечению конфиденциальности и целостности полученной из Системы информации и доступности в соответствии с требованиями законодательства Российской Федерации.

5.10.2. Организовать защиту канала связи посредством выполнения комплекса мероприятий и применения технических средств защиты

информации в соответствии с требованиями законодательства Российской Федерации о техническом регулировании, включая меры по обеспечению ее конфиденциальности, целостности и доступности, которые должны включать защиту от несанкционированного доступа в ВИС.

5.10.3. Осуществлять обработку указанной информации и размещение систем, в которых происходит ее обработка, в отдельных помещениях, защищенных от несанкционированного доступа.

5.10.3. Использовать средства антивирусной защиты на компонентах систем.

5.10.4. Обеспечить защиту компонентов систем, от несанкционированного доступа, персональную идентификацию и аутентификацию работников на данных компонентах.

5.10.5. Обеспечить защиту компонентов систем от несанкционированного доступа из внешних сетей (включая общедоступную сеть информационного обмена Интернет) с использованием средств межсетевого экранирования.

5.10.6. Довести требования безопасности и ответственности за нарушение работниками правил доступа Пользователей ВИС в Системе, установленных Регламентом доступа.

6. Ограничение использования информации

6.1. Авторизационные данные, предоставленные Оператору ВИС в соответствии с приложением № 6 к Регламенту доступа, Оператору Системы или уполномоченным (от Операторов) лицам для технической интеграции ВИС и Системы, считаются конфиденциальными и не подлежат разглашению или передаче третьим лицам.

6.2. Информация, обрабатываемая в Системе и полученная Оператором ВИС в соответствии с настоящим Соглашением, включает, в том числе информацию ограниченного доступа, не составляющую государственную или служебную тайну, не подлежит разглашению или передаче третьим лицам и организациям, средствам массовой информации, в том числе размещению информации в сети Интернет.

7. Порядок взаимодействия с организациями

7.1. В случае необходимости привлечения третьих лиц к выполнению работ в интересах Оператора ВИС в рамках интеграции ВИС и Системы, Оператором Системы предоставляются Авторизационные данные указанной организации по запросу Оператора ВИС.

7.2. Оператор ВИС указывает в запросе полный перечень лиц, уполномоченных на получение Авторизационных данных для технической интеграции ВИС и Системы.

7.3. Оператор ВИС несет ответственность перед Оператором Системы, в случае нарушения работниками организации, выполняющей подрядные работы для ВИС, требований установленных разделах 5 и 6 настоящего Соглашения.

8. Ответственность

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

8.2. Стороны и уполномоченные ими лица несут ответственность за разглашение информации ограниченного доступа в соответствии с законодательством Российской Федерации.

9. Заключительные положения

9.1. Настоящее соглашение вступает в силу с момента его подписания Сторонами и действует неопределенный срок (до момента, когда одна из сторон не выступит с запросом на прекращение действия настоящего Соглашения, или перестанут действовать обстоятельства, послужившие основанием для информационного взаимодействия Сторон).

9.2. В случае возникновения любых противоречий, претензий и разногласий, а также споров, связанных с информационным взаимодействием в рамках настоящего Соглашения, Стороны предпринимают усилия для урегулирования таких противоречий, претензий и разногласий путем переговоров.

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

9.4. Настоящее Соглашение составлено в 2 (двух) экземплярах, по одному для каждой из Сторон, имеющих одинаковую юридическую силу.

Министерство цифрового (наименование организации ВИС)
развития и связи Кузбасса

Приложение № 8 к Регламенту
доступа пользователей к сведениям,
содержащимся в информационной
системе «Региональная
автоматизированная интеграционная
платформа видеонаблюдения и
видеоаналитики Кузбасса»

**Технические требования
к услуге связи для подключения АРМ Пользователей к Системе**

1. Для организации подключения к Системе используется услуга «Виртуальная частная сеть третьего уровня» (L3 VPN).

1.1. Виртуальная частная сеть VPN (Virtual Private Network) представляет собой виртуальную изолированную среду, созданную в сети передачи данных IP/MPLS Организации, позволяющую обеспечивать связанность точек, подключенных к этой среде, по схеме «каждый с каждым». Точками, которые подключаются к VPN, могут быть порты сети передачи данных Организации или удаленные точки, «привязанные» к VPN «плечами» - виртуальными каналами доступа к VPN, организованными в сети передачи данных IP/MPLS Организации.

1.2. Для каналов доступа к L3 VPN используются отдельные порты Ethernet на оконечном оборудовании Организации. При организации на одном объекте канала доступа к L3 VPN совместно с другими услугами передачи данных по требованию Организации должен быть предоставлен 1 (один) транковый порт Ethernet 802.1 q (с поддержкой VLAN). В этом случае каждой услуге будет соответствовать определенный номер VLAN (VLAN ID) в физическом стыке Ethernet.

1.3. При предоставлении услуги «Виртуальная частная сеть третьего уровня» скорость передачи данных от Организации в Систему должна быть равна скорости передачи данных от Системы в Организацию.

1.4. Тип физического интерфейса, который может использоваться Организацией при предоставлении ей услуги «виртуальная частная сеть третьего уровня», - Ethernet 100 Base-TX.

1.5. Требуемый Организации класс качества указан в таблице.

1.5.1. Приведенные параметры качества поддерживаются при загрузке канала доступа к L3 VPN не более 75% от установленной полосы пропускания.

Таблица

Время задержки пакетов, не более, мс	100
Вариация времени задержки пакетов, не более, мс	50
Потери пакетов, не более, %	0,10

1.5.2. Параметры передачи сигналов электросвязи при оказании услуг «Виртуальная частная сеть» должны соответствовать приказу Министерства

цифрового развития, связи и массовых коммуникаций Российской Федерации от 18.02.2022 № 123 «Об утверждении Требований к порядку ввода сетей связи в эксплуатацию», приказу Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 25.11.2021 № 1229 «Об утверждении Требований к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования» и ITU-T Y.1541, МСЭ-Т Y.1561.

2. Рекомендуемая скорость услуги «Виртуальная частная сеть третьего уровня» для подключения 1 (одного) рабочего места Пользователя Системы – 10 Мбит/с (для одновременного просмотра до 5 видеопотоков со средств видеонаблюдения в высоком качестве).

3. Услуга связи организуется между точками «А» и «Б», где точка «А» - место расположения выделенного рабочего места Пользователя, точка «Б» - Система, находящаяся по адресу: г. Кемерово, ул. Арочная, д. 37А.

Приложение № 10 к Регламенту
доступа пользователей к сведениям,
содержащимся в информационной
системе «Региональная
автоматизированная интеграционная
платформа видеонаблюдения и
видеоаналитики Кузбасса»

Министру цифрового развития и
связи Кузбасса

(ФИО)

СОГЛАСИЕ
НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, _____,
(ФИО)

паспорт _____ выдан _____,
(серия, номер) (когда и кем выдан)

адрес регистрации: _____,

даю свое согласие на обработку в Министерство цифрового развития и связи Кузбасса, расположенного по адресу: 650056, Кемеровская область – Кузбасса, г. Кемерово, ул. Арочная, дом 37А, моих персональных данных, относящихся исключительно к перечисленным ниже категориям персональных данных: фамилия, имя, отчество; пол; дата рождения; тип документа, удостоверяющего личность; данные документа, удостоверяющего личность; гражданство.

Я даю согласие на использование персональных данных исключительно в целях:

- регистрации и предоставления доступа к функционалу информационной системе «Региональная автоматизированная интеграционная платформа видеонаблюдения и видеоаналитики Кузбасса» (далее – Система);

- идентификации;

- установления обратной связи, включая направление уведомлений, запросов, касающихся Системы;

- введение истории активности;

- проведение статистических и иных исследований на основе обезличенных данных;

- обеспечения соблюдения требований законодательства Российской Федерации,

- хранение данных об этих результатах на электронных носителях.

Настоящее согласие предоставляется мной на осуществление действий в отношении моих персональных данных, которые необходимы для достижения указанных выше целей, включая (без ограничения) сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, передачу третьим лицам для осуществления действий по обмену информацией, обезличивание, блокирование персональных данных, а также осуществление любых иных действий, предусмотренных действующим законодательством Российской Федерации.

Я проинформирован, что Министерство цифрового развития и связи Кузбасса гарантирует обработку моих персональных данных в соответствии с действующим законодательством Российской Федерации как неавтоматизированным, так и автоматизированным способами.

Данное согласие действует до достижения целей обработки персональных данных или в течение срока хранения информации.

Данное согласие может быть отозвано в любой момент по моему письменному заявлению. Мне разъяснено, что отзыв в моего согласия на обработку персональных данных влечёт за собой удаление моей учётной записи в Системе, а также уничтожение записей, содержащих ваши персональные данные, в информационной системе Оператора.

Я подтверждаю, что, давая такое согласие, я действую по собственной воле и в своих интересах.

Срок действия Вашего согласия является неограниченным, однако, Вы вправе в любой момент отозвать настоящее согласие, путём направления письменного уведомления на адрес Оператора.

" ____ " _____ 202__ г.

Подпись

Расшифровка подписи