

СОГЛАСОВАНО

Министр цифрового развития и
связи Кузбасса


_____/М.В. Садиков/
« 01 » 02 2021 г.

УТВЕРЖДАЮ

Заместитель Губернатора Кузбасса -
Председатель совета по
информационной безопасности
Кузбасса


_____/В.А. Догадов/
« 01 » 02 2021 г.

РЕГЛАМЕНТ

ПОДКЛЮЧЕНИЯ К ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ «ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ ПРАВИТЕЛЬСТВА КУЗБАССА»

2020 г.

Содержание

Введение	3
1. Основные положения	5
2. Порядок подключения	6
3. Технические требования	8
4. Контроль реализации подключения	14
5. Перечень нормативно-правовых актов	14
Приложение № 1 Форма заявки на подключение АРМ Пользователей к ГИС «ЭДО Правительства Кузбасса»	16
Приложение № 2 Форма заявки на актуализацию учетных записей.....	20
Приложение № 3 Форма заявки на закрытие учетных записей.....	21

Введение

Настоящий Регламент подключения к государственной информационной системе «Электронный документооборот Правительства Кузбасса» (далее – Регламент) определяет состав участников информационного взаимодействия, порядок подключения и технические требования автоматизированных рабочих мест пользователей при использовании государственной информационной системы «Электронный документооборот Правительства Кузбасса» (далее соответственно – АРМ пользователя, «ЭДО Правительства Кузбасса»), с использованием ГИС «ЭДО Правительства Кузбасса».

Требования настоящего Регламента распространяются на АРМ пользователей, которым необходимо подключение к информационным ресурсам ГИС «ЭДО Правительства Кузбасса» для исполнения своих служебных обязанностей.

Функции по обеспечению создания, развития ГИС «ЭДО Правительства Кузбасса», по формированию требований к защите информации и реализации мероприятий по защите информации в ГИС «ЭДО Правительства Кузбасса» осуществляет Министерство цифрового развития и связи Кузбасса (далее – Оператор ГИС).

Функции по обеспечению организационного, технического и технологического сопровождения функционирования ГИС «ЭДО Правительства Кузбасса» осуществляет государственное казенное учреждения «Центр информационных технологий Кузбасса» (далее – Администратор ГИС).

Администратор ГИС формирует учетные данные пользователя с целью обеспечения санкционированного доступа к информационным ресурсам ГИС «ЭДО Правительства Кузбасса».

Администратор ГИС формирует матрицу доступа подключенных АРМ пользователя к ГИС «ЭДО Правительства Кузбасса» и поддерживает ее в актуальном состоянии.

Состав участников информационного взаимодействия с использованием ГИС «ЭДО Правительства Кузбасса» включает пользователей и иных пользователей.

1. Пользователи ГИС «ЭДО Правительства Кузбасса»:

Правительство Кемеровской области – Кузбасса;

Администрация Правительства Кузбасса;

Исполнительные органы государственной власти Кузбасса.

2. Иные пользователи ГИС «ЭДО Правительства Кузбасса»:

Законодательное Собрание Кемеровской области – Кузбасса;

Избирательная комиссия Кемеровской области – Кузбасса;

Контрольно-счетная палата Кемеровской области – Кузбасса;

Уполномоченный по правам человека в Кемеровской области - Кузбассе;

Уполномоченный по правам ребенка в Кемеровской области – Кузбассе;

Уполномоченный по защите прав предпринимателей в Кемеровской

области – Кузбассе;

Подведомственные учреждения исполнительных органов государственной власти Кемеровской области – Кузбасса;

Органы местного самоуправления муниципальных образований Кемеровской области – Кузбасса и подведомственные им учреждения;

Территориальные органы федеральных органов исполнительной власти в Кемеровской области – Кузбассе;

Иные организации, участвующие в информационном взаимодействии с исполнительными органами государственной власти Кузбасса.

Подключение пользователей Правительства Кемеровской области – Кузбасса, Администрации Правительства Кузбасса, исполнительных органов государственной власти Кузбасса к ГИС «ЭДО Правительства Кузбасса» является обязательным.

Подключение иных пользователей к ГИС «ЭДО Правительства Кузбасса» осуществляется администратором ГИС «ЭДО Правительства Кузбасса» на основании соглашения об информационном взаимодействии, заключенного с оператором ГИС «ЭДО Правительства Кузбасса».

ГИС «ЭДО Правительства Кузбасса» присвоен третий класс защищенности (К3).

ГИС «ЭДО Правительства Кузбасса» имеет Аттестат соответствия требованиям безопасности информации от 20.10.2020 № СИБА.АС.836.

1. Основные положения

1.1. Общее описание информационного обмена.

Обмен информацией между ГИС «ЭДО Правительства Кузбасса» и участниками информационного взаимодействия (далее – Организация) осуществляется в электронном виде с использованием сетей связи общего пользования (сети Интернет) и локальной вычислительной сети (далее – ЛВС) Администрации Правительства Кузбасса.

В ГИС «ЭДО Правительства Кузбасса» для защиты информации конфиденциального характера при ее передаче по открытым каналам связи используются сертифицированные шифровальные (криптографические) средства защиты информации.

Основным сетевым телекоммуникационным протоколом при осуществлении информационного обмена между ГИС «ЭДО Правительства Кузбасса» и АРМ пользователя, являются протоколы семейства ТСР/ІР.

1.2. Общие требования по защите информации.

Хранение и обработка информации, содержащейся в ГИС «ЭДО Правительства Кузбасса» и АРМ пользователей, а также обмен информацией должны осуществляться после принятия необходимых мер по защите указанной информации от утечки по техническим каналам, компрометации, повреждения или утраты, предусмотренных нормативными правовыми актами Российской Федерации в области защиты информации.

АРМ пользователей Организации должны быть размещены в служебных помещениях с принятием организационных и технических мер, исключающих несанкционированный доступ к обработке информации посторонними лицами.

Руководитель Организации правовым актом назначает ответственное должностное лицо за организацию подключения к ГИС «ЭДО Правительства Кузбасса» и принятие мер по защите информации, содержащейся на подключаемых АРМ пользователя.

Подключение АРМ пользователей к ГИС «ЭДО Правительства Кузбасса» должна осуществляться с использованием средств защиты информации (далее – СЗИ) и средств криптографической защиты информации (далее – СКЗИ) в соответствии с требованиями:

законодательства Российской Федерации, регулирующего отношения в области обеспечения информационной безопасности;

нормативно-технических и методических документов федерального органа исполнительной власти в области обеспечения безопасности (далее – ФСБ России) и федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации (далее – ФСТЭК России);

настоящего Регламента.

2. Порядок подключения и изменения сведений

2.1. Содержание и результаты каждого этапа работ для подключения АРМ пользователя Организации к ГИС «ЭДО Правительства Кузбасса» перечислены в таблице.

Таблица

Этап	Содержание работ	Результаты работ
1.	Разработка комплекта организационно-распорядительной документации, регламентирующей обработку и обеспечение защищенного взаимодействия с ГИС «ЭДО Правительства Кузбасса»	Рабочая документация (ведомость эксплуатационных документов, перечень сертифицированных СЗИ и СКЗИ, технический паспорт). Правовой акт о создании комиссии*. Правовой акт о назначении ответственного должностного лица за обеспечение организации подключения и мер по защите информации АРМ пользователей
2.	Выбор схемы защищенного взаимодействия АРМ пользователя с ГИС «ЭДО Правительства Кузбасса»	Выбор применения сертифицированного средства криптографической защиты информации
3.	Установка и настройка СЗИ/СКЗИ на АРМ пользователя организацией, имеющей лицензии ФСБ России и (или) ФСТЭК России по соответствующим видам деятельности или штатными специалистами Организации, прошедшие необходимое обучение	Акт установки и настройки СЗИ/СКЗИ с фиксации параметров настроек
4.	Обучение лиц с правилами работы СЗИ ГИС «ЭДО Правительства Кузбасса»	Инструкция пользователя по организации работы защищенного взаимодействия с ГИС «ЭДО Правительства Кузбасса», с отметками пользователей об ознакомлении
5.	Формирование заявки на подключение АРМ пользователя	Сопроводительное письмо оператору ГИС на подключение АРМ пользователя по форме, согласно приложению

* Правовым актом назначается комиссия, которая проверяет условия подключения и подтверждает их выполнение.

2.2. Для получения доступа к ГИС «ЭДО Правительства Кузбасса» участнику информационного взаимодействия, необходимо направить заявку на регистрацию своих сотрудников оператору ГИС по форме, приведенной в приложении № 1 к настоящему Регламенту.

2.3. Заявка подается следующим способом:

- с использованием электронного документооборота (при наличии доступа к «Электронному документообороту Правительства Кузбасса»);
- с использованием защищенного канала связи на абонентский пункт «АП Минцифра_Кузбасса_канцелярия» (при наличии доступа к сети № 2301);
- на бумажном носителе (допускается направление приложений на компакт-диске).

2.4. Оператор ГИС рассматривает представленные сведения на предмет соответствия требованиям законодательства Российской Федерации, регулирующего отношения в области обеспечения информационной безопасности, и (или) настоящего Регламента, в срок не позднее 3 рабочих дней с даты получения заявки на подключение АРМ пользователя.

2.5. По результатам рассмотрения заявки Оператор ГИС принимается решение о предоставлении доступа к ГИС «ЭДО Правительства Кузбасса», либо заявка отклоняется с указанием соответствующих комментариев для устранения замечаний.

2.6. В случае положительного результата рассмотрения заявки на подключение АРМ пользователя Оператор ГИС в срок не позднее 5 рабочих дней, с даты получения заявки на подключение, передает заявку Администратору ГИС.

2.7. Администратор ГИС формирует учетные данные (логин, пароль) пользователя с целью обеспечения санкционированного доступа к информационным ресурсам ГИС «ЭДО Правительства Кузбасса».

2.8. Администратор ГИС направляет логин и временный пароль (без содержания персональных данных) на адрес электронной почты каждого пользователя, указанной в заявке на подключение, в срок не позднее 3 рабочих дней после произведенного подключения АРМ пользователя.

2.9. При первом входе в ГИС «ЭДО Правительства Кузбасса» пользователю необходимо сменить пароль доступа. Пароль должен состоять из 8 и более символов, прописных латинских букв (A, B, C, D, ...), строчных латинских букв (a, b, c, d, ...), цифр (1, 2, 3, 4, ...), знаков пунктуации (!, ?, +, =, ...).

2.10. Запрещается передавать другому лицу учетные данные для работы в ГИС «ЭДО Правительства Кузбасса».

2.11. В случаях изменения сведений о пользователях в Организации (фамилия, имя, отчество, структурное подразделение, должность, контактный телефон, адрес электронной почты) руководителю Организации необходимо направить заявку на актуализацию сведений о пользователях Организации оператору ГИС по форме, приведенной в приложении № 2 к настоящему Регламенту.

2.12. Оператор ГИС направляет Администратору ГИС заявку на

актуализацию сведений о пользователе Организации. Администратор ГИС информирует пользователя Организацию о произведенных изменениях на адрес электронной почты, указанной в заявке на подключение, в срок не позднее 3 рабочих дней.

2.13. Прекращение доступа участникам информационного взаимодействия к ГИС «ЭДО Правительства Кузбасса» производится в следующих случаях:

- увольнения сотрудника участника информационного взаимодействия;
- ликвидации Организации;
- решения руководителя Организации.

В таких случаях Организация направляет соответствующую заявку на закрытие учетных данных сотрудников по форме, приведенной в приложении № 3 к настоящему Регламенту.

2.14. По решению Оператора и Администратора ГИС «ЭДО Правительства Кузбасса» доступ к ГИС «ЭДО Правительства Кузбасса» может быть прекращен в случаях:

2.14.1. Обнаружения нарушений правил использования учетных записей, установленных п. 2.10. настоящего Регламента.

2.14.2. Компрометации или подозрению на компрометацию (утрата, передача или иной факт распространения сведений) учетных данных, а также ключа усиленной квалифицированной электронной подписи участника информационного взаимодействия.

2.14.3. Отсутствия информации об использовании учетной записи участника информационного взаимодействия в течение трех месяцев.

2.14.4. Выявления неправомерного использования информационных ресурсов ГИС «ЭДО Правительства Кузбасса».

3. Технические требования

3.1. Технические требования к технологической совместимости, организации информационного взаимодействия, стандартам и протоколам обмена между ГИС «ЭДО Правительства Кузбасса» и АРМ пользователей Организации, устанавливаются оператором ГИС «ЭДО Правительства Кузбасса».

3.2. Требования к организации подключения.

Мероприятия по организации схемы защищенного взаимодействия АРМ пользователя должны учитывать требования организационно-технической, организационно-распорядительной и эксплуатационной документацией на созданную систему защиты информации ГИС «ЭДО Правительства Кузбасса».

При настройке СЗИ от несанкционированного доступа требуется выполнить настройки параметров с применением шаблона по классу защищенности ГИС КЗ.

При необходимости дополнительно рассмотреть организационные меры для обеспечения требований по защите информации.

До начала выполнения работ по подключению АРМ пользователей к ГИС «ЭДО Правительства Кузбасса» Организация определяет схему защищенного взаимодействия.

Для организации информационного взаимодействия Организация самостоятельно реализует систему защиты информации в соответствии с выбранной схемой защищенного взаимодействия АРМ пользователя с ГИС «ЭДО Правительства Кузбасса».

3.3. Требования к реализации защищенного взаимодействия с ГИС «ЭДО Правительства Кузбасса».

На АРМ пользователей, подключаемых к ГИС, должны быть выполнены организационные и технические мероприятия, обеспечивающие соответствие системы защиты информации требованиям безопасности информации, в соответствии с настоящего Регламентом:

- наличие правового акта о назначении ответственного должностного лица за обеспечение организации подключения и мер по защите информации АРМ пользователей;
- произведена установка и настройка средств защиты информации по определенной схеме защищенного взаимодействия;
- наличие оформленного акта установки сертифицированных средств защиты информации или аттестата соответствия требованиям безопасности информации на объект информатизации.

Для проведения работ по установке и настройке средств защиты информации АРМ пользователя, в соответствии с законодательством Российской Федерации, необходимо привлекать организации, имеющие лицензии ФСБ России и (или) ФСТЭК России по соответствующим видам деятельности.

Допускается проведение работ по установке и настройке средств защиты информации специалистами Организации, прошедших обучение по программам повышения квалификации в области защиты информации (не менее 72 академических часа).

Для организации доступа АРМ пользователя к информационным ресурсам между Организацией и оператором ГИС заключается соглашение:

- об установлении межсетевого взаимодействия;
- об информационном обмене.

3.3.1. Схема № 1 защищенного взаимодействия

Взаимодействие АРМ пользователя осуществляется с помощью использования ЛВС Администрации Правительства Кузбасса.

Для реализации защищенного взаимодействия АРМ пользователя должно быть оснащено:

средством защиты от несанкционированного доступа, имеющим сертификат соответствия ФСТЭК России;

средством антивирусной защиты, имеющим сертификат соответствия ФСТЭК России и ФСБ России;

а) для пользователей Администрации Правительства Кузбасса, подключенные к ЛВС – доверенными каналами и (или) защищенными волоконно-оптическими линиями связи;

б) для иных пользователей органов государственной власти Кемеровской области - Кузбасса – межсетевым экраном (семейства Континент или ViPNet), имеющим сертификат соответствия ФСТЭК России, для АРМ пользователей, находящихся за пределами контролируемой зоны здания (г. Кемерово, пр. Советский, д. 62).

3.3.2. Схема № 2 защищенного взаимодействия.

Взаимодействие АРМ пользователя осуществляется с использованием СКЗИ семейства ViPNet, входящего в состав ЛВС Администрации Правительства Кузбасса. В данном случае используется ViPNet сеть № 2301, аттестованная по требованиям безопасности информации, оператором которой является Министерство цифрового развития и связи Кузбасса.

Возможны три варианта реализации схемы защищенного взаимодействия.

3.3.2.1. Схема № 2.1 защищенного взаимодействия.

Для обработки защищаемой информации АРМ пользователя должно быть оснащено:

средством защиты от несанкционированного доступа, имеющим сертификат соответствия ФСТЭК России;

средством антивирусной защиты, имеющим сертификат соответствия ФСТЭК России и ФСБ России;

программным комплексом ViPNet Client 4 для ViPNet сети № 2301, имеющим сертификат соответствия ФСБ России (подключение осуществляет администратор защищенной ViPNet сети № 2301).

3.3.2.2. Схема № 2.2 защищенного взаимодействия.

Для обработки защищаемой информации АРМ пользователя должно быть оснащено:

средством защиты от несанкционированного доступа, имеющего сертификат соответствия ФСТЭК России;

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);

средством антивирусной защиты, имеющего сертификат соответствия ФСТЭК России и ФСБ России.

3.3.2.3. Схема № 2.3 защищенного взаимодействия.

Для обработки защищаемой информации для АРМ пользователя должны быть выполнены следующие условия:

установлено средство защиты от несанкционированного доступа, имеющее сертификат соответствия ФСТЭК России;

установлено средство антивирусной защиты, имеющее сертификат соответствия ФСТЭК России и ФСБ России;

организовано подключение ViPNet сети Организации к ViPNet сети № 2301 для обеспечения межсетевого взаимодействия.

3.3.3. Схема № 3 защищенного взаимодействия.

Взаимодействие АРМ пользователя осуществляется с использованием СКЗИ семейства Континент, входящего в состав ЛВС Администрации Правительства Кузбасса. В данном случае возможны три варианта реализации схемы защищенного взаимодействия.

3.3.3.1. Схема № 3.1 защищенного взаимодействия.

Для обработки защищаемой информации АРМ пользователя должно быть оснащено:

средством защиты от несанкционированного доступа, имеющим сертификат соответствия ФСТЭК России;

средством антивирусной защиты, имеющим сертификат соответствия ФСТЭК России и ФСБ России.

СКЗИ Континент-АП, имеющим сертификат соответствия ФСБ России. межсетевым экраном (программным), имеющим сертификат соответствия ФСТЭК России.

3.3.3.2. Схема № 3.2 защищенного взаимодействия.

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:

средством защиты от несанкционированного доступа, имеющего сертификат соответствия ФСТЭК России;

межсетевым экраном, имеющего сертификат соответствия ФСТЭК России (АПКШ «Континент» версии 3.7 или 3.9);

средством антивирусной защиты, имеющего сертификат соответствия ФСТЭК России и ФСБ России.

3.3.3.3. Схема № 3.3 защищенного взаимодействия.

Для обработки защищаемой информации для АРМ пользователя должны быть выполнены следующие условия:

установлено средство защиты от несанкционированного доступа, имеющее сертификат соответствия ФСТЭК России;

установлено средство антивирусной защиты, имеющее сертификат соответствия ФСТЭК России и ФСБ России;

организовано подключение VPN сети на базе АПКШ «Континент» Организации к VPN сети на базе АПКШ «Континент» ЛВС Администрации Правительства Кузбасса для обеспечения межсетевого взаимодействия.

3.3.4. Схема № 4 защищенного взаимодействия (при осуществлении доступа с помощью Web-приложения).

Взаимодействие АРМ пользователя должно осуществляться с использованием средства криптографической защиты информации VipNet TLS Gateway.

Для обработки защищаемой информации АРМ пользователя должно быть оснащено:

средством защиты от несанкционированного доступа, имеющим сертификат соответствия ФСТЭК России;

универсальным программным комплексом VipNet PKI Client;

межсетевым экраном, имеющим сертификат соответствия ФСТЭК России;

средством антивирусной защиты, имеющим сертификат соответствия ФСТЭК России и ФСБ России.

3.3.5. Схема № 5 защищенного взаимодействия.

Взаимодействие АРМ пользователя осуществляется с применением мобильного устройства (типа ноутбук), подключаемого с использованием СКЗИ. В данном случае возможны два варианта реализации схемы защищенного взаимодействия.

3.3.5.1. Схема № 5.1 защищенного взаимодействия.

Для обработки защищаемой информации АРМ пользователя должно быть оснащено:

средством защиты от несанкционированного доступа, имеющим сертификат соответствия ФСТЭК России;

средством антивирусной защиты, имеющим сертификат соответствия ФСТЭК России и ФСБ России;

программным комплексом VipNet Client 4 для VipNet сети № 2301, имеющим сертификат соответствия ФСБ России.

3.3.5.2. Схема № 5.2 защищенного взаимодействия.

Для обработки защищаемой информации АРМ пользователя должно быть оснащено:

средством защиты от несанкционированного доступа, имеющим сертификат соответствия ФСТЭК России;

средством антивирусной защиты, имеющим сертификат соответствия ФСТЭК России и ФСБ России.

СКЗИ Континент-АП, имеющим сертификат соответствия ФСБ России; межсетевым экраном (программным), имеющим сертификат соответствия ФСТЭК России.

3.3.6. Схема № 6 защищенного взаимодействия.

Взаимодействие осуществляется с применением планшета (смартфона) пользователя, подключаемого с использованием клиентского приложения удаленного доступа. В данном случае возможны два варианта реализации схемы защищенного взаимодействия.

3.3.6.1. Схема № 6.1 защищенного взаимодействия.

Для обработки защищаемой информации АРМ пользователя должно быть оснащено:

средством защиты от несанкционированного доступа, имеющим сертификат соответствия ФСТЭК России;

средством антивирусной защиты, имеющим сертификат соответствия ФСТЭК России и ФСБ России;

программным комплексом ViPNet Client Mobile для ViPNet сети № 2301, имеющим сертификат соответствия ФСБ России.

3.3.6.2. Схема № 6.2 защищенного взаимодействия.

Для обработки защищаемой информации АРМ пользователя должно быть оснащено:

средством защиты от несанкционированного доступа, имеющим сертификат соответствия ФСТЭК России;

средством антивирусной защиты, имеющим сертификат соответствия ФСТЭК России и ФСБ России.

клиентским приложением Континент-АП (Мобильный), имеющим сертификат соответствия ФСБ России.

межсетевым экраном (программным), имеющим сертификат соответствия ФСТЭК России.

3.4. Схема защищенного взаимодействия АРМ пользователя с ГИС «ЭДО Правительства Кузбасса», а также необходимые для их корректного функционирования настройки должны быть согласованы с оператором ГИС.

3.5. Выполнение требуемых мер по защите информации на АРМ пользователя в зависимости от выбранной схемы защищенного взаимодействия подтверждается актом готовности подключения АРМ пользователя Организации к ГИС «ЭДО Правительства Кузбасса».

3.6. Помещения для размещения технических средств АРМ пользователей должны удовлетворять эксплуатационной документации на используемые средства защиты информации.

3.7. Работы по установке, монтажу и настройке средств защиты информации, включая СКЗИ должны выполняться в соответствии с требованиями настоящего Регламента и эксплуатационной документации на данные средства защиты информации.

3.8. Обеспечение защиты информации в ходе эксплуатации АРМ пользователя осуществляется в соответствии с организационно - технической, организационно-распорядительной, эксплуатационной документацией на систему защиты информации ГИС «ЭДО Правительства Кузбасса» и требованиями нормативно-технических и методических документов ФСТЭК России и ФСБ России.

3.9. Требования к составу технических средств и операционным системам АРМ пользователя:

процессор – тактовая частота не менее 1,6 ГГц;

объем оперативной памяти – не менее 1 ГБайта;

свободное пространство на жестком диске – не менее 500 Мбайт;

операционная система – Windows 7/ Windows 10, 32/64-разрядная.

В состав АРМ пользователя могут входить другие технические средства обеспечения технологических процессов: принтеры, сканеры.

На АРМ пользователя должна быть установлена одна ОС. Установку и настройку должен проводить системный администратор. Для настройки необходимо:

в BIOS установить пароль и определить один вариант загрузки ОС с жесткого диска, все альтернативные варианты загрузки должны быть отключены, в том числе сетевая загрузка;

создать и использовать только персонифицированные учетные данные пользователей с правами администратора и с правами пользователя, в соответствии с матрицей доступа (список доступа, разработанного и утвержденного для ИС внутри организации, подключаемой к ГИС «ЭДО Правительства Кузбасса»);

заблокировать учетные данные пользователя «Гость».

Временные учетные данные могут быть заведены администратором для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования ИС, для организации гостевого доступа, при этом администратором информационной безопасности организации должен осуществляться полный контроль за совершаемыми действиями данным пользователем;

выполнить корректные настройки часового пояса, даты и времени.

3.10. Требования к каналам связи:

Рекомендуемая пропускная способность канала связи общего пользования (Интернет) должна быть не менее 1024 Кбит/с.

4. Контроль реализации подключения

4.1. Ответственность за соблюдение требований настоящих технических условий по реализации защищенного взаимодействия и обеспечении защиты информации, а также за соблюдение требований к эксплуатации СЗИ и СКЗИ, используемых на АРМ пользователей, лежит на Организации.

4.2. В целях предотвращения угрозы безопасности учетные записи пользователей блокируются оператором ГИС в случае увольнения сотрудников Организации, при получении информации о компрометации (или подозрении на компрометацию) учетной записи сотрудников и в иных случаях по решению непосредственных руководителей Организации. Оператор ГИС уведомляет Организацию о блокировании учетной записи с указанием обнаруженных нарушений безопасности информации.

4.3. По запросу руководителя Организации возможно разблокирование учетной записи пользователя после устранения всех выявленных нарушений безопасности информации.

5. Перечень нормативно-технических актов

5.1 Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

5.2 Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

5.3 Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных»;

5.4 Постановление Правительства РФ от 21.03.2012 № 211 «Об утверждении Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

5.5 Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

5.6 Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Составы 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 требований к защите персональных данных для каждого из уровней защищенности»;

5.7 Приказ ФАПСИ России 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»;

5.8 Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

5.9 Приказ 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»;

5.10 Методический документ ФСТЭК России от 11.02.2014 «Меры защиты информации в государственных информационных системах».

Приложение № 1
к Регламенту подключения к
государственной информационной
системе «Электронный
документооборот Правительства
Кузбасса»

**Форма заявки
на подключение АРМ пользователей к ГИС «ЭДО Правительства
Кузбасса»**

Угловой штамп Организации

Дата, Исх. №

Министру цифрового развития
и связи Кузбасса

Прошу провести подключение к государственной информационной системы «Электронный документооборот Правительства Кузбасса» (далее – ГИС «ЭДО Правительства Кузбасса») удаленного автоматизированного рабочего места (далее – АРМ) Организации.

При организации защищенного взаимодействия с информационными ресурсами ГИС «ЭДО Правительства Кузбасса» выполнены требования нормативно-правовых и руководящих документов уполномоченных органов в сфере защиты информации ФСТЭК России, ФСБ России.

Перечень АРМ пользователей представлен в Приложении № 1 к заявке на подключение.

Требования к программному, техническому обеспечению и к защите информации АРМ пользователей ГИС «ЭДО Правительства Кузбасса» выполнены в полном объеме.

С требованиями Регламента подключения к ГИС «ЭДО Правительства Кузбасса», ознакомлены и обязуемся их выполнять.

Приложения: 1. Копия правового акта о назначении ответственного должностного лица за обеспечение организации подключения и мер по защите информации АРМ пользователей в Организации;
2. Копия правового акта о создании комиссии по защите конфиденциальной информации в Организации;
3. Перечень АРМ пользователей (приложение № 1);
4. Акт готовности подключения АРМ пользователя (приложение № 2).

Руководитель Организации

Подпись

Приложение № 1
к заявке на подключение АРМ
пользователей Организации к
ГИС «ЭДО Правительства
Кузбасса»
от «__» _____ 202__ г.

Перечень АРМ пользователей

Таблица 1 – Сведения об организации

Наименование Организации	
Должность руководителя Организации	
Фамилия, имя, отчество руководителя Организации	
Адрес Организации (для переписки)	
Контактные телефоны Организации	
Ответственное должностное лицо за обеспечение подключения и мер по защите информации АРМ пользователя	

Таблица 2 – Сведения о пользователях

№ п/п	ФИО (полностью)	Структурное подразделение	Должность	Контактный телефон	Адрес электронной почты *

* Для пользователей локальной вычислительной сети Администрации Правительства Кузбасса указывается адрес электронной почты почтового сервера «АКО» (например: ivanov-ab@ako.ru)

Приложение № 2
к заявке на подключение АРМ
пользователей Организации к
ГИС «ЭДО Правительства
Кузбасса»
от «__» _____ 202__ г.

ФОРМА АКТА
готовности подключения АРМ пользователя
к ГИС «ЭДО Правительства Кузбасса»

г. Кемерово

«__» _____ 20__ г.

- Мы, нижеподписавшиеся, председатель комиссии: _____
члены комиссии _____
составили настоящий АКТ о нижеследующем:
1. Комиссией установлено наличие следующих средств защиты информации:
средство криптографической защиты информации, наименование и номер версия: _____;
межсетевой экран, наименование номер версия: _____;
средство антивирусной защиты информации, наименование и номер версия: _____;
средство защиты информации от несанкционированного доступа, наименование номер и версия: _____.
 2. Структурное подразделение Организации _____.
 3. Адрес размещения АРМ пользователя _____.
 4. АРМ находится в ЛВС Администрации Правительства Кузбасса: *да / нет*;
 5. Схема защищенного взаимодействия АРМ пользователя № _____.
 6. Статический IP адрес / номер подсети ЛВС, маска: _____.
 7. Инвентарный номер АРМ пользователя: _____.
 8. Пользователь АРМ (должность, Ф.И.О.): _____.
 9. Установка и настройка СЗИ/СКЗИ осуществлена (*наименование юридического лица*) _____.
 10. Реквизиты акта установки и настройки:
средства криптографической защиты информации (№_, дата);
межсетевого экрана (№_, дата);
средства антивирусной защиты информации (№_, дата);
средства защиты информации от несанкционированного доступа (№_, дата),
с указанием класса защищенности ГИС КЗ.
 11. Сведения о соглашениях: об информационном взаимодействии (обязательно) и межсетевом взаимодействии (при наличии).
 12. Программное обеспечение на АРМ пользователя установлено в

соответствии с перечнем программного обеспечения, утвержденным приказом Минцифры Кузбасса. *(если не соответствует, то предоставить отчет с установленным ПО для каждого рабочего места).*

Комиссия провела проверку выполнения технических и организационных мер по созданию защищенного взаимодействия с ГИС «ЭДО Правительства Кузбасса».

Комиссия сообщает о готовности подключения АРМ инв. № _____ к ГИС «ЭДО Правительства Кузбасса».

Председатель комиссии:

(подпись)

(Ф.И.О.)

Члены комиссии:

(подпись)

(Ф.И.О.)

ФИО исполнителя
контактный телефон

Приложение № 2
к Регламенту подключения к
государственной информационной
системе «Электронный
документооборот Правительства
Кузбасса»

**Форма заявки
на актуализацию учетных записей**

Угловой штамп Организации

Дата, Исх. №

Министру цифрового развития
и связи Кузбасса

Прошу актуализировать сведения о пользователях Организации в государственной информационной системе «Электронный документооборот Правительства Кузбасса» для следующих сотрудников:

№ п/п	ФИО (полностью)	Инвентарный номер АРМ пользователя	Структурное подразделение, должность	Контактный телефон	Адрес электронной почты *

Руководитель

ФИО исполнителя
контактный телефон

* Для пользователей локальной вычислительной сети Администрации Правительства Кузбасса указывается адрес электронной почты почтового сервера «АКО» (например: ivanov-ab@ako.ru)

Приложение № 3
к Регламенту подключения к
государственной информационной
системе «Электронный
документооборот Правительства
Кузбасса»

**Форма заявки
на закрытие учетных записей**

Угловой штамп Организации
Дата, Исх. №

Министру цифрового развития
и связи Кузбасса

В связи с увольнением (ликвидацией Организации, решением руководителя) прошу закрыть учетные записи для доступа к государственной информационной системе «Электронный документооборот Правительства Кузбасса» следующим сотрудникам:

№ п\п	ФИО полностью	Организация	Подразделение, должность

Руководитель

ФИО исполнителя
контактный телефон