

ДОПОЛНИТЕЛЬНОЕ СОГЛАШЕНИЕ № 4
к Соглашению о взаимодействии между государственным казенным
учреждением Ростовской области «Уполномоченный многофункциональный
центр предоставления государственных и муниципальных услуг» и
министерством экономического развития Ростовской области
от 28.10.2015 № 21

г. Ростов-на-Дону

«10» апреля 2019 г

Государственное казенное учреждение Ростовской области «Уполномоченный многофункциональный центр предоставления государственных и муниципальных услуг» в лице директора Алехина Алексея Владимировича, действующего на основании Устава, утвержденного распоряжением Правительства Ростовской области от 29.04.2013 № 131 «Об утверждении устава государственного казенного учреждения Ростовской области «Уполномоченный многофункциональный центр предоставления государственных и муниципальных услуг», далее именуемое Уполномоченный МФЦ, с одной стороны, и министерство экономического развития Ростовской области в лице заместителя министра Шеховцова Романа Викторовича действующего на основании указа Губернатора Ростовской области от 14.12.2018 № 98, Положения о министерстве экономического развития Ростовской области, утвержденного постановлением Правительства Ростовской области от 12.08.2016 № 568 «Об утверждении положения о министерстве экономического развития Ростовской области», приказа министерства экономического развития Ростовской области от 21.03.2019 № 51-о, далее именуемое Орган, с другой стороны, совместно именуемые Стороны, на основании части 1.3 статьи 16, статьи 18 Федерального закона от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», постановления Правительства Российской Федерации от 27.09.2011 № 797 «О взаимодействии между многофункциональными центрами предоставления государственных и муниципальных услуг и федеральными органами исполнительной власти, органами государственных внебюджетных фондов, органами государственной власти субъектов Российской Федерации, органами местного самоуправления», постановления Правительства Российской Федерации от 22.12.2012 № 1376 «Об утверждении Правил организации деятельности многофункциональных центров предоставления государственных и муниципальных услуг» (далее – Правила) заключили настоящее Дополнительное соглашение о нижеследующем:

1. Приложение № 1 изложить в редакции:

«Приложение № 1
к Соглашению
от 28 октября 2015 года № 21

Перечень
государственных услуг Органа, предоставляемых на базе МФЦ

№ п/п	Наименование государственной услуги
1.	Предоставление льгот по налогам инвесторам, осуществляющим реализацию инвестиционных проектов
2.	Предоставление субсидий субъектам инновационной деятельности малого и среднего предпринимательства
3.	Предоставление субсидий организациям независимо от организационно-правовой формы на возмещение части затрат по созданию объектов капитально-го строительства инженерной инфраструктуры, являющихся неотъемлемой частью инвестиционного проекта, и (или) их подключению (технологическому присоединению) к инженерным системам электро-, газо-, водоснабжения и водоотведения».

1. Приложение № 6 изложить в редакции:

**«Приложение № 6
к Соглашению
от 28 октября 2015 года № 21**

Порядок организации защищенного электронного взаимодействия при обмене электронными документами между МФЦ и Органом

1. Общие положения

1. Настоящий Порядок разработан на основании статьи 18 Федерального закона от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 22.12.2012 № 1376 «Об утверждении Правил организации деятельности многофункциональных центров предоставления государственных и муниципальных услуг» и является неотъемлемой частью настоящего Соглашения.

2. Целью настоящего Порядка является определение условий и процедур, при соблюдении которых обеспечивается защита от несанкционированного доступа, целостность, а также подтверждение авторства электронных документов, передаваемых по телекоммуникационным каналам связи между МФЦ и Органом.

Термины и определения

Администратор безопасности – лицо, назначенное руководителем организации, производящее установку, настройку СКЗИ и контролирующее работу с СКЗИ пользователей. Администратор безопасности может быть доверенным лицом УЦ, подписывающим своей электронной подписью сертификаты ключей проверки электронных подписей пользователей.

АРМ (автоматизированное рабочее место) – компьютер с установленным СКЗИ или другим прикладным (специальным) программным обеспечением;

квалифицированный сертификат ключа проверки электронной подписи (далее – квалифицированный сертификат) – сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи;

ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи;

ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи;

компрометация ключей – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых крипто ключи могут стать доступными другим лицам и (или) процессам;

кросс-сертификация – процедура установления доверительных отношений между удостоверяющими центрами (доверенные УЦ), в результате которой сертификат, выданный доверенным удостоверяющим центром, считается достоверным;

сертификат ключа проверки электронной подписи – электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

средство криптографической защиты информации (СКЗИ) – программное, аппаратное или аппаратно-программное средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности;

удостоверяющий центр – юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ;

уполномоченное лицо – работник, наделенный распорядительным документом Стороны полномочиями по подписанию электронных документов электронной подписью от имени участника информационного взаимодействия;

электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах;

электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая

используется для определения лица, подписывающего информацию, а также обеспечивает достоверность передаваемой информации.

2. Организация защищенного взаимодействия

2.1. Защищенное электронное взаимодействие между МФЦ и Органом строится на базе средств криптографической защиты информации (СКЗИ) ПО ViPNet, версия 3.2 и выше или совместимых с ними СКЗИ.

2.2. Для организации защищенного информационного взаимодействия могут привлекаться специализированные организации, оказывающие услуги в области шифрования информации и удостоверяющего центра (УЦ).

2.3. Юридическая значимость электронных документов в рамках электронного информационного взаимодействия МФЦ и Органа обеспечивается с использованием усиленной квалифицированной электронной подписи (далее – ЭП), вырабатываемой с использованием ключей электронной подписи. Сертификаты ключей проверки ЭП выдаются:

для работников МФЦ – УЦ, оказывающим услуги МФЦ;

для работников Органа – УЦ Органа.

УЦ должны быть аккредитованы Минкомсвязью России.

2.4. ЭП уполномоченного лица МФЦ или Органа в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе. Если в соответствии с федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами документ должен быть заверен печатью, электронный документ, подписанный электронной подписью уполномоченного лица МФЦ или Органа, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью и заверенному печатью.

2.5. Управление инфраструктурой сертификатов ключей проверки электронной подписи уполномоченных лиц МФЦ осуществляет УЦ, оказывающий услуги в соответствии со своим Регламентом работы (далее – Регламент) и на основании договора между УЦ и МФЦ.

2.6. Управление инфраструктурой сертификатов ключей проверки электронной подписи уполномоченных лиц Органа осуществляет УЦ Органа в соответствии с Регламентом.

2.7. Для обеспечения взаимного признания сертификатов ключей проверки электронной подписи уполномоченных лиц удостоверяющих центров УЦ, оказывающий услуги МФЦ, и УЦ Органа при необходимости проводят процедуру кросс-сертификации УЦ.

3. Порядок защищенного электронного взаимодействия

3.1. Для осуществления электронного защищенного взаимодействия на АРМе уполномоченным лицам Сторон должно быть установлено СКЗИ, выработаны и выданы ключи шифрования, ключи электронной подписи, ключи проверки электронной подписи, сертификаты ключей проверки электронной подписи в соответствии с регламентами обслуживающих их УЦ и руководство пользователю

по эксплуатации СКЗИ.

3.2. В качестве транспортной среды для ведения защищенного электронного взаимодействия между МФЦ и Органом используются телекоммуникационные сети, включая сеть Интернет.

3.3. Установку, настройку СКЗИ, средств защиты информации от несанкционированного доступа и обучение уполномоченных лиц правилам работы с ними осуществляют:

в МФЦ – работники МФЦ или представители специализированной организации предоставляющей услуги;

в Органе – структурное подразделение по защите информации Органа.

3.4. Указанный порядок защищенного информационного взаимодействия более подробно описывается применительно к выбранному типу СКЗИ.

4. Порядок действий уполномоченных лиц при осуществлении защищенного электронного взаимодействия

4.1. При отправке электронных документов:

проверить подготовленный для отправки электронный документ и подписать его ЭП, убедиться, что ЭП создана;

убедиться, что имя файла электронного документа соответствует следующему формату передачи электронного документа:

имя файла, содержащего электронный документ:

ZZZZZZ_YYYYMMDD_XX_AAA_NNNNN.PDF

где,

ZZZZZZ – префикс файлов, принимает вид **MFCMER**;

YYYYMMDD – дата создания файла в формате «ГГГГММДД»;

XX – код услуги согласно таблице:

Код	Наименование государственной услуги
01	Предоставление льгот по налогам инвесторам, осуществляющим реализацию инвестиционных проектов
02	Предоставление субсидий субъектам инновационной деятельности малого и среднего предпринимательства
03	Предоставление субсидий организациям независимо от организационно-правовой формы на возмещение части затрат по созданию объектов капитального строительства инженерной инфраструктуры, являющихся неотъемлемой частью инвестиционного проекта, и (или) их подключению (технологическому присоединению) к инженерным системам электро-, газо-, водоснабжения и водоотведения

AAA – код МФЦ, согласно таблице:

МФЦ в муниципальном образовании Ростовской области	Код МФЦ
в Азовском районе	201
в Аксайском районе	202
в Багаевском районе	205
в Боковском районе	207
в Верхнедонском районе	208
в Веселовском районе	209

в Волгодонском районе	212
в Дубовском районе	213
в Егорлыкском районе	215
в Заветинском районе	217
в Зерноградском районе	218
в Зимовниковском районе	219
в Кагальницком районе	222
в Каменском районе	223
в Кашарском районе	224
в Константиновском районе	225
в Куйбышевском районе	227
в Мартыновском районе	230
в Матвеево-Курганском районе	231
в Милютинском районе	233
в Морозовском районе	234
в Мясниковском районе	235
в Неклиновском районе	236
в Обливском районе	240
в Октябрьском районе	241
в Орловском районе	242
в Песчанокопском районе	244
в Пролетарском районе	245
в Ремонтненском районе	247
в Родионово-Несветайском районе	248
в Семикаракорском районе	251
в Тарасовском районе	253
в Тацинском районе	254
в Усть-Донецком районе	255
в Целинском районе	256
в Цимлянском районе	257
в Чертковском районе	258
в Шолоховском районе	211
в Советском районе	252
в г.Азове	404
в г.Батайске	407
в г.Белая Калитва	206
в г.Волгодонске	412
в г.Гуково	415
в г.Донецке	417
в г.Каменск-Шахтинский	419
в г.Красный Сулин	226
в г.Миллерово	232
в г.Новочеркасске	427
в г.Новошахтинске	430
в г.Сальске и Сальском районе	250
в г.Таганроге	437
в г.Шахты	440
в г.Зверево	418
в Первомайском районе г. Ростова-на-Дону	401
в Пролетарском районе г. Ростова-на-Дону	401
в Кировском районе г. Ростова-на-Дону	401

в Октябрьском районе г. Ростова-на-Дону	401
в Ленинском районе г. Ростова-на-Дону	401
в Железнодорожном районе г. Ростова-на-Дону	401
в Советском районе г. Ростова-на-Дону	401
в Ворошиловском районе г. Ростова-на-Дону	401

NNNNN – порядковый номер электронного сообщения за указанный день (00001-99999).

- отправить зашифрованный файл получателю;
- убедиться, что письмо доставлено получателю. Фактом доставки информации в электронном виде при использовании программного обеспечения «ViPNet Client [Деловая почта]» является изменение третьего символа атрибута электронного сообщения с «О» на «Д».

4.2. При получении электронных документов:

- расшифровать полученный файл;
- проверить наличие ЭП уполномоченного лица другой Стороны на полученном документе, ее целостность и действительность;
- в случае если ЭП нарушена или недействительна, направить ответное сообщение (письмо) с указанием причины, по которой электронный документ не может быть принят к исполнению;
- при ответе на письмо убедиться, что имя файла электронного документа соответствует формату:

Имя файла, содержащего электронный документ:

ZZZZZZ_YYYYMMDD_XX_AAA_NNNNN.PDF

где,

ZZZZZZ – префикс файлов, при отправке электронных документов из Органа в МФЦ, принимает вид **MKUMFC**,

Последовательность **YYYYMMDD_XX_AAA_NNNNN** совпадает с аналогичной частью имени файла запроса МФЦ, ответом на который является данный файл.

4.3. Принятые электронные документы обрабатываются в соответствии с установленным порядком внутреннего электронного документооборота Органа и МФЦ.

4.4. Имя файла, содержащего скан-образ результата услуги, подписанного заявителем/уведомления о не востребоованности результата:

ZZZZZZ_YYYYMMDD_Закрытие_дела_№_NNNNN*.PDF

где

ZZZZZZ – префикс файлов, принимает вид **MFCMER**;

YYYYMMDD – дата создания файла в формате «ГГГГММДД»;

NNNNN* - номер дела в системе МФЦ до от 4 до 10 символов.

5. Обеспечение информационной безопасности

5.1. Хранение информации, содержащей персональные данные, на АРМах уполномоченных лиц осуществляется только на период, необходимый для ее

гарантированной доставки адресату и обработки в соответствии с принятой технологией.

5.2. На АРМах уполномоченных лиц, участвующих в электронном документообороте, должна обеспечиваться следующая общая политика безопасности:

- информационный обмен между АРМами осуществляется в зашифрованном виде. Открытый IP-трафик блокируется;

- для работы АРМ внутри корпоративной сети устанавливается персональный сетевой экран, и производятся дополнительные настройки фильтров IP-пакетов;

- в список адресатов защищенной сети для конкретного АРМа включаются только санкционированные АРМы, участвующие в электронном документообороте;

- правила доступа для пропуска трафика от адресатов защищенной сети должны быть настроены только для работы по разрешенным протоколам и портам;

- права изменения настроек (конфигурации) АРМов предоставляются только администраторам безопасности Сторон.

5.3. Для защиты информации от несанкционированного доступа на АРМах уполномоченных лиц дополнительно устанавливаются средства защиты информации от несанкционированного доступа типа «Аккорд» или «Соболь», сертифицированные ФСТЭК России. По согласованию с ФСБ России допускается замена на иные аппаратно-программные модули доверенной загрузки (АПМДЗ).

5.4. Оборудование помещений, где размещаются АРМы с СКЗИ, порядок допуска в них и их охрана должны соответствовать требованиям ФСБ России по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.

5.5. При компрометации ключей электронной подписи или шифрования администратор безопасности Стороны, где произошла компрометация, обязан незамедлительно сообщить об этом администратору безопасности другой Стороны.

Стороны принимают меры по замене скомпрометированных ключей в соответствии с правилами работы СКЗИ и Регламентами работы обслуживающих их удостоверяющих центров.

6. Порядок разбора конфликтных ситуаций

Разбор конфликтных ситуаций, связанных с формированием и использованием в электронных документах ЭП, проводится в соответствии с порядком, предусмотренным Регламентом работы УЦ, выдавшего сертификат ключа проверки ЭП.».

2. Приложение № 7 изложить в редакции:

**«Приложение № 7
к Соглашению
от 28 октября 2015 года № 21**

Технологические схемы государственных услуг, предоставляемые на базе сети МФЦ Ростовской области

№ п/п	Наименование государственной услуги	Технологическая схема предоставления государственной услуги
1.	Предоставление льгот по налогам инвесторам, осуществляющим реализацию инвестиционных проектов	Приложение № 24 к Протоколу к протоколу заседания комиссии по повышению качества и доступности предоставления государственных и муниципальных услуг и организации межведомственного взаимодействия в Ростовской области от 27.12.2016 № 4
2.	Предоставление субсидий субъектам инновационной деятельности малого и среднего предпринимательства	Приложение № 28 к Протоколу к протоколу заседания комиссии по повышению качества и доступности предоставления государственных и муниципальных услуг и организации межведомственного взаимодействия в Ростовской области от 27.12.2016 № 4
3.	Предоставление субсидий организациям независимо от организационно-правовой формы на возмещение части затрат по созданию объектов капитального строительства инженерной инфраструктуры, являющихся неотъемлемой частью инвестиционного проекта, и (или) их подключению (технологическому присоединению) к инженерным системам электро-, газо-, водоснабжения и водоотведения	Приложение № 105 к протоколу заседания комиссии по повышению качества и доступности предоставления государственных и муниципальных услуг и организации межведомственного взаимодействия в Ростовской области от 15.02.2019 № 1».

4. Настоящее Дополнительное соглашение вступает в силу со дня его подписания Сторонами.

5. Настоящее Дополнительное соглашение составлено в двух экземплярах, имеющих одинаковую юридическую силу, по одному для каждой из Сторон.

Министерство экономического
развития Ростовской области

344050, г. Ростов-на-Дону,
ул. Социалистическая, 112

Заместитель министра экономического
развития Ростовской области


Р.В. Шеховцов
(подпись)
МП 

Государственное казенное
учреждение Ростовской области
«Уполномоченный
многофункциональный центр
предоставления государственных и
муниципальных услуг»

344082, г. Ростов-на-Дону,
ул. Береговая, 8

Директор


А.В. Алехин
(подпись)
МП 