УСЛОВИЯ ИСПОЛЬЗОВАНИЯ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

1. Общие определения

Банк – ПАО РОСБАНК.

Договор о системе электронного документооборота (далее - Договор) **–** совокупность настоящих Условий и надлежащим образом оформленное Заявление Организации с отметкой Банка о его принятии. Впервые представленное Клиентом в Банк Заявление является заявлением с целью заключения Договора.

Генеральное соглашение о проведении депозитных операций - соглашение, заключенное между Банком и Клиентом, предметом которого является определение порядка заключения и исполнения депозитных сделок, под которыми понимается привлечение Банком денежных средств в валюте Российской Федерации и/или иностранной валюте на условиях договора банковского вклада, согласованных сторонами в подтверждении.

Организация – юридическое лицо или индивидуальный предприниматель, не имеющее (-ий) в Банке открытых расчетных счетов, заключившее (-ий) с ПАО РОСБАНК Договор о предоставлении услуг по переводу денежных средств на счета физических лиц, открытые в ПАО РОСБАНК и/или Генеральное соглашение о проведении депозитных операций и/или заключившее(-ий) Договор о системе электронного документооборота.

Система электронного документооборота (далее – **Система ЭДО)** – комплекс программно-технических средств и организационных мероприятий для создания и передачи электронных документов Сторонами – участниками Договора по телекоммуникационным каналам, в том числе и сети Интернет. Система ЭДО состоит из двух частей – подсистемы «Клиент» и подсистемы «Банк», установленных соответственно у Организации и Банка. Порядок использования Электронной Подписи в Системе ЭДО устанавливается Банком как оператором Системы ЭДО.

Администратор Системы ЭДО – физическое лицо, уполномоченное Банком подписывать от имени Банка Сертификаты ключей Организации, а также регистрировать соответствующие Ключи проверки электронной подписи в Системе ЭДО.

Правила обмена электронными документами (Правила) – правила, регламентирующие формирование и обмен ЭД, указанные в Приложении № 2.

Заявление Организации - заявление в ПАО РОСБАНК на заключение Договора об использовании системы электронного документооборота по форме Приложения № 4.

Заявление об изменении списка Пользователей – заявление в ПАО РОСБАНК на изменение пользователей системы электронного документооборота по форме Приложения № 5.

Организация, относящаяся к корпоративному сегменту – юридические лица (некредитные организации) и индивидуальные предприниматели, соответствующие утвержденным в ПАО РОСБАНК критериям сегментации.

Организация, относящаяся к сегменту предпринимателей – юридические лица, индивидуальные предприниматели, а также физические лица, занимающиеся в установленном порядке частной практикой, соответствующие утвержденным в ПАО РОСБАНК критериям сегментации.

Ключ проверки электронной подписи (Открытый ключ) – связанная с Ключом электронной подписи особым математическим соотношением уникальная последовательность символов, полученная в результате работы программы генерации Комплекта ключей. Ключ проверки электронной подписи предназначен для проверки подлинности ЭП.

Ключ электронной подписи (Закрытый ключ) – уникальная последовательность символов, полученная в результате работы программы генерации Комплекта ключей. Ключ электронной подписи предназначен для выработки Системой ЭДО ЭП в ЭД.

Комплект ключей – комплект из Ключа электронной подписи и соответствующего ему Ключа проверки электронной подписи.

Компрометация ключей – утрата, хищение, несанкционированное копирование или подозрение на копирование Ключа электронной подписи, а также другие ситуации, при которых достоверно неизвестно, что произошло с Ключом электронной подписи.

Пользователь Системы ЭДО – физическое лицо, уполномоченное Организацией с помощью своего Ключа электронной подписи подписывать ЭП от имени Организации отправляемые в соответствии с настоящим Порядком в Банк ЭД, а также получать из Банка ЭД, предназначенные Организации. Соответствующий Ключу электронной подписи Ключ проверки электронной подписи регистрируется Банком за Пользователем Системы ЭДО на основании подписания Сторонами в установленном Договором порядке Сертификата ключа.

Сертификат ключа проверки электронной подписи (далее – **Сертификат ключа)** – автоматически создаваемый Банком (как Удостоверяющим центром), и выдаваемый Организации средствами Системы при генерации Ключа электронной подписи и Ключа проверки электронной подписи электронный документ, подписанный электронной подписью уполномоченного представителя Банка, или документ на бумажном носителе установленной формы, подписываемый Сторонами, удостоверяющий принадлежность приведенного в нем Ключа проверки электронной подписи и соответствующего ему Ключа электронной подписи физическому лицу – Пользователю Системы ЭДО. Подписанный в установленном Договором порядке Сертификат ключа подтверждает факт наделения данного физического лица правами на использование Системы ЭДО в соответствии с данным Порядком использования электронных документов (далее – Порядок). Сертификат ключа в форме документа на бумажном носителе создается в двух экземплярах, для Организации и для Банка.

Условия - настоящие Условия использования системы электронного документооборота, опубликованные на сайте Банка в сети Интернет (www.rosbank.ru).

Электронная Подпись (далее – **ЭП)** – реквизит ЭД, защищающий ЭД от подделки (определяющий подлинность ЭД).

ЭП представляет собой уникальную последовательность символов, полученную в результате криптографического преобразования информации, содержащейся в ЭД с использованием Ключа электронной подписи.

ЭП создается с использованием Средств электронной подписи.

Определение подлинности ЭД, производимое с помощью Сертификата ключа, предполагает:

установление факта отсутствия (наличия) искажений в ЭД с момента подписания ЭП;

идентификацию владельца соответствующего Ключа электронной подписи (Пользователь Системы ЭДО), как лица, подписавшего ЭД.

Используемая в Системе ЭДО ЭП является усиленной неквалифицированной электронной подписью, за исключением случаев, когда Договором прямо предусмотрена возможность подписания определенных ЭД простой электронной подписью.

В случае, если условиями Договора прямо предусмотрена возможность использования простой электронной подписи для подписания ЭД, сведения о подписании ЭД простой электронной подписью Пользователем Системы ЭДО (дата подписания, ФИО Пользователя Системы ЭДО, наименование Организации, идентификатор Организации) содержатся в подписанном ЭД.

Электронный документ (далее – **ЭД)** – документ, в котором информация

представлена в электронно-цифровой форме (в виде последовательности двоичных символов);

хранится в базе данных либо в файле;

защищена от искажений с помощью одной или более электронных цифровых подписей;

с помощью средств Системы ЭДО преобразуется в форму, пригодную для однозначного восприятия человеком.

SMS-код – последовательность символов, направляемая Банком на номер телефона Пользователя Системы ЭДО, указанный в Заявлении и/или предоставленный Банку Пользователем Системы ЭДО в процессе обслуживания в Системе ЭДО, в целях использования ее для подписания ЭД, формируемых Пользователем Системы ЭДО. В случаях, установленных Договором, последовательность символов, указанная в SMS-коде, рассматривается в качестве ключа простой электронной подписи.

2. Порядок заключения Договора, предмет и условия

2.1. В рамках Договора Банк предоставляет Организации услуги по дистанционному обслуживанию путем электронного документооборота (обмена ЭД) с использованием Системы ЭДО, и регулирует отношения, возникающие в связи с этим между Сторонами. Началом оказания услуг, предусмотренных настоящим пунктом, считается дата подписания Банком первого подписанного Организацией Сертификата ключа Пользователя Системы ЭДО.

2.2. Заключение Договора между Сторонами осуществляется путем присоединения Организации к настоящим Условиям на основании Заявления Организации, надлежащим образом заполненного, подписанного уполномоченными лицами Организации и надлежащим образом принятого и подписанного Банком после успешной процедуры идентификации Организации и проверки полномочий лица (лиц), подписавшего(-их) Заявление Организации.

2.3. Договор вступает в силу с даты, следующей за датой подписания Банком Заявления Организации.

2.4. Публикация Условий (включая приложения) и изменений к ним осуществляется на сайте Банка в сети Интернет по адресу: www.rosbank.ru.

2.5. Банк вправе в одностороннем порядке вносить изменения и/или дополнения в Условия (включая приложения к ним). Банк обязуется уведомить Клиента о таких изменениях за 10 (десять) рабочих дней до даты вступления в силу изменений путем размещения информации об изменениях и обновленных версий документов на сайте Банка по адресу: www.rosbank.ru. При этом изменения и дополнения, внесенные Банком, становятся обязательными для Сторон в дату введения изменений и/или дополнений в действие.

2.6. Организация обязана самостоятельно обращаться на сайт Банка в сети Интернет по адресу: www.rosbank.ru с целью проверки информации об изменении Условий и дате вступления их в силу.

2.7. Организация имеет право направлять в адрес Банка создаваемые Системой ЭДО ЭД, список которых приведен в Таблице 1.2 раздела II Электронный документооборот Заявления Организации. Пересылка файлов неоговоренного Сторонами формата, а также файлов, содержащих различные активные (исполняемые) элементы, вирусы и т.п., недопустима. Ответственность за причиненный ущерб несет Сторона, являющаяся отправителем файла.

2.8. Стороны признают используемые в Системе ЭДО процедуры (п.1.2 Правил) и средства (п.3 Правил) достаточными для защиты, подтверждения целостности и подлинности ЭД, а также идентификации лиц, подписывающих ЭД, передаваемые по телекоммуникационным каналам общего пользования, в том числе и сети Интернет.

2.9. Стороны договорились признавать действие Комплекта ключей каждой Стороны на основании Сертификата ключа без обращения за удостоверением Сертификата ключа к какой-либо третьей стороне. Ключи проверки электронной подписи Банка и копии соответствующих Сертификатов размещаются Банком на сервере Системы ЭДО.

2.10. Стороны признают, что Ключ электронной подписи Пользователя Системы ЭДО создается средствами Системы ЭДО в единственном экземпляре, соответствует Ключу проверки электронной подписи, приведенному в Сертификате ключа, и известен только Пользователю Системы ЭДО. Стороны признают, что доступ (регистрация) Пользователя Системы ЭДО в Систему ЭДО, а также создание корректной ЭП в ЭД невозможны без знания Ключа электронной подписи и кодовой фразы к нему.

2.11. ЭД, подписанный ЭП Пользователя Системы ЭДО, а в случае указания Организацией в Таблице 1.2 раздела II Электронный документооборот Заявления Организации, подписанный соответствующим количеством дополнительных ЭП Пользователя/Пользователей Системы ЭДО, признается Сторонами документом, имеющим равную юридическую силу с надлежащим образом оформленным документом на бумажном носителе, подписанным собственноручными подписями уполномоченных лиц и заверенным печатью Организации (при ее наличии).

ЭД, подписанный ЭП Банка, признается Сторонами документом, имеющим равную юридическую силу с надлежащим образом оформленным документом на бумажном носителе, подписанным собственноручными подписями уполномоченных лиц и заверенным печатью Банка.

2.12. Применение электронного документооборота в рамках Договора не исключает применение существующего между Сторонами документооборота с использованием бумажных носителей.

2.13. Форматы ЭД определяются Банком и приведены в документе - Руководство Пользователя Системы ЭДО, размещенном на веб-сайте https://www.bankline.ru. Банк посредством Системы ЭДО обеспечивает доступ Организации к описанию форматов и правилам заполнения ЭД. Банк может в

одностороннем порядке изменять формат и правила заполнения электронных документов. Сведения о таких изменениях Банк размещает по указанному в настоящем пункте адресу веб-сайта.

2.14. В связи с использованием электронного документооборота в рамках настоящих Условий Стороны обязуются строго выполнять требования Правил. Сторона, не выполняющая требования Правил, несет полную ответственность за возникающие в результате этого последствия.

2.15. Стороны при работе с Системой ЭДО производят отсчет времени по московскому времени. Контрольным является время системных часов на аппаратных средствах Банка (сервере Системы ЭДО).

2.16. Банк обязан проводить идентификацию Пользователей системы ЭДО, в порядке, установленном Программой идентификации клиента, представителя клиента, выгодоприобретателя, бенефициарного владельца, включенной в состав Правил внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (если идентификация указанного лица не проводилась ранее).

2.17. Банк вправе не проводить операции, не исполнять обязательства по принятым ЭД Организации в порядке и в случаях, установленных действующим законодательством РФ.

2.18. Банк вправе приостановить или прекратить оказание услуг по Договору при нарушении Организацией Правил. При этом приостановление или прекращение оказания Банком услуг по Договору не прекращает обязательств Организации и Банка, возникших до момента приостановления или прекращения оказания услуг по Договору.

3. Обязанности Сторон

3.1. Организация обязана:

3.1.1. Обеспечить наличие технических и программных средств, необходимых для эксплуатации подсистемы «Клиент», в соответствии с требованиями, указанными в приложении № 1. Организовать подключение технических средств к телекоммуникационным каналам, обеспечивающим выбранный Организацией способ соединения с сервером Банка.

3.1.2. При заключении Договора Организация обязана назначить из штата своих работников Пользователей Системы, наделив их соответствующими полномочиями. Информацию о Пользователях Системы и объеме их полномочий (статусе ЭП) Организация обязана включить в Заявление Организации, при этом должным образом заверенные копии документов подтверждающих полномочия Пользователей Системы, Организация обязана предоставить в Банк при предоставлении Заявления Организации. Организация обязуется в течение срока действия Договора уведомлять Банк об изменении круга Пользователей Системы и/или изменении объема их полномочий (статуса ЭП) не позднее 1 (одного) рабочего дня, следующего за датой такого изменения, следующим образом:

- об изменении круга Пользователей – путем предоставления в Банк документа на бумажном носителе, составленного по форме **Заявления об изменении списка Пользователей**, подписанного уполномоченным лицом Организации с приложением печати (при наличии таковой) или отправкой соответствующего сообщения посредством Системы в адрес Администратора Системы. К данному документу должны быть приложены должным образом заверенные копии документов, подтверждающих полномочия Пользователей Системы;

- об изменении полномочий Пользователя (присвоения дополнительного статуса ЭП/изменения статуса ЭП) – путем предоставления в Банк документа на бумажном носителе, составленного по форме **Заявления об изменении списка Пользователей** подписанного уполномоченным лицом Организации с приложением печати (при наличии таковой), или отправкой соответствующего сообщения посредством Системы в адрес Администратора Системы. Организация вправе уведомить Банк о сокращении объема полномочий Пользователя (присвоения дополнительного статуса ЭП/изменения удаление одного из статуса ЭП) по телефону Администратора Системы в случае, если такое изменение полномочий Пользователя не приводит к перераспределению полномочий между Пользователями Системы, с обязательным последующим (не позднее следующего рабочего дня) письменным уведомлением или уведомлением посредством Системы в адрес Администратора Системы. Документы, подтверждающие измененный объем полномочий Пользователя Системы, должны быть предоставлены в Банк не позднее 1 (одного) рабочего дня, следующего за датой изменения полномочий.

Настоящим Организация заверяет Банк о том, что Пользователь Системы, подписавший ЭД, предоставляемый Банку, является должным образом уполномоченным представителем Организации и обладает действительными полномочиями на подписание соответствующего ЭД, в том числе, но не исключительно, на основании действующей доверенности, которая не была отозвана.

Организация принимает на себя всю ответственность за полномочия Пользователя Системы, сведения о котором получены Банком в порядке, предусмотренном первым абзацем настоящего пункта. Организация настоящим подтверждает и заверяет Банк в том, что ЭД, полученный Банком и содержащий ЭП одного из Пользователей Системы Организации, должен рассматриваться в качестве ЭД, подписанного данным Пользователем Системы.

3.1.3. В соответствии с порядком, предусмотренным Правилами обеспечить генерацию Комплекта ключей каждым назначенным Пользователем Системы ЭДО лично.

3.1.4. Обеспечить передачу в Банк установленным порядком (п. 2 Правил) Ключей проверки электронной подписи, сгенерированных Пользователями Системы ЭДО, и соответствующих им Сертификатов ключей Пользователей, подписанных Организацией.

3.1.5. Не передавать третьим лицам программное обеспечение, Ключи электронной подписи и Ключи проверки электронной подписи, Сертификаты ключей, а также прочие сведения, относящиеся к настоящему Порядку.

3.1.6. Немедленно известить Банк о лишении Пользователя Системы ЭДО права подписывать ЭП создаваемые с помощью Системы ЭДО ЭД, используя кодовую фразу, указанную в Сертификате ключа.

3.1.7. Направить уведомление Банку о Компрометации ключей, об использовании ключей ЭП без согласия Организации в порядке, предусмотренном Правилами, незамедлительно после обнаружения факта Компрометации ключей ЭП и (или) их использования без согласия Организации, но не позднее дня, следующего за днем получения от Банка уведомления о совершенной операции.

3.1.8. Своевременно просматривать (обрабатывать) все получаемые от Банка ЭД.

3.1.9. Обеспечить наличие законных оснований для передачи Банку персональных данных Пользователей системы ЭДО и (или) иных физических лиц. По отношению к полученным от Организации

персональным данным Банк будет являться лицом, осуществляющим обработку персональных данных по поручению Организации.

3.1.10. По письменному запросу Банка предоставить подтверждение наличия законного основания (например, письменное согласие конкретного физического лица), подтверждающего соблюдение требований п.3.1.9.

3.1.11. Обеспечить соблюдение Пользователем Системы ЭДО конфиденциальности ключа простой электронной подписи в случаях, если по условиям Договора допускается подписание ЭД простой электронной подписью.

3.1.12. Незамедлительно информировать Банк обо всех случаях утраты, компрометации, прекращения использования сим-карты, компрометации SMS-кода, утраты мобильного телефона Пользователя Системы ЭДО, номер которого указан в Заявлении и/или предоставлен Банку Пользователем Системы ЭДО в процессе обслуживания в Системе ЭДО.

3.2. Банк обязан:

3.2.1. Предоставить Организации программные средства для генерации Комплекта ключей. Указанные в настоящем пункте программные средства предоставляются Банком без дополнительной оплаты.

3.2.2. Оказать представителю Организации консультации по установке программного обеспечения подсистемы «Клиент». Консультировать Организацию по вопросам эксплуатации Системы ЭДО.

3.2.3. Проводить операции, исполнять поручения, принимать и исполнять обязательства, содержащиеся в полученных от клиента ЭД, в соответствии с Договором.

3.2.4. Предоставлять по запросу Организации сведения о Пользователе Системы ЭДО, подписавшем документ простой электронной подписью в случаях, установленных Договором.

4. Ответственность Сторон

За неисполнение или ненадлежащее исполнение обязательств по Договору Стороны несут имущественную ответственность в порядке, предусмотренном действующим законодательством Российской Федерации.

В случае если для разрешения спора Сторон создана Согласительная комиссия для установления подлинности ЭД (Раздел 4 Правил) и в результате ее работы установлено, что претензии, предъявленные одной из Сторон, были не обоснованы, данная Сторона обязана возместить другой Стороне по ее требованию все расходы, связанные с работой Согласительной комиссии и подтвержденные соответствующими документами, содержащими суммы понесенных расходов. Возмещение расходов производиться в течение 10 (Десяти) рабочих дней, исчисляемых со дня получения Стороной, предъявившей необоснованные претензии, указанного требования, оформленного на бумажном носителе, с приложенными копиями расходных документов. Возмещение производится путем безналичного перечисления денежных средств по реквизитам, указанным в требовании о возмещении расходов.

Банк не несет ответственности за ущерб, возникший вследствие разглашения уполномоченными лицами Организации собственного ключа ЭП, его утраты или передачи, вне зависимости от причин, неуполномоченным лицам.

Банк не несет ответственности последствия исполнения ЭД в случае неисполнения Организацией обязательств, установленных п. 3.1.12 Условий.

Банк не несет ответственности за последствия исполнения электронного платежного документа, защищенного корректной ЭП Организации, в том числе в случае использования ключей ЭП и программно-аппаратных средств клиентской части Системы неуполномоченным лицом.

Банк не несет ответственности в случае реализации угроз несанкционированного доступа неуполномоченных лиц к части Системы, установленной у Организации, и Ключам Организации, включая угрозы со стороны внутренних (локальных) и внешних (глобальных) сетей связи.

Банк не несет ответственности за неработоспособность оборудования и программных средств Организации и третьих лиц, повлекшую за собой невозможность доступа Организации к банковской части Системы и возникшие в результате задержки в осуществлении платежей Организации, а также за возможное уничтожение (в полном или частичном объеме) информации, содержащейся на вычислительных средствах Организации, подключенных к сети Интернет для обеспечения предоставления услуг по настоящему Договору.

Стороны взаимно освобождаются от имущественной ответственности за неисполнение или ненадлежащее исполнение обязательств по Договору, если оно вызвано факторами непреодолимой силы: авариями телекоммуникационного оборудования, задействованного в Системе, принадлежащего третьим лицам, чрезвычайными обстоятельствами, стихийными бедствиями, военными действиями, актами органов власти, Центрального банка Российской Федерации.

Сторона, которая не в состоянии выполнить свои обязательства по Договору в силу вышеуказанных причин, обязана незамедлительно проинформировать другую Сторону в письменной форме об их наступлении и прекращении.

5. Срок действия Договора и порядок его расторжения

5.1. Договор вступает в действие с даты, следующей за датой подписания Банком Заявления Организации, и действует бессрочно.

5.2. Любая из Сторон вправе в одностороннем порядке расторгнуть Договор до истечения его срока, направив другой Стороне письменное уведомление о расторжении Договора за 30 (тридцать) календарных дней до предполагаемой даты расторжения Договора. В этом случае Договор считается расторгнутым с даты, указанной Стороной в письменном уведомлении.

5.3. В случае открытия Клиентом расчетного счета в Банке, Банк вправе в одностороннем порядке расторгнуть настоящий Договор путем направления Клиенту письменного уведомления о расторжении Договора за 5 (пять) календарных дней до предполагаемой даты расторжения Договора. В этом случае Договор считается расторгнутым с даты, указанной Стороной в письменном уведомлении.

6. Дополнительные условия

6.1. Банк вправе в одностороннем порядке расторгнуть Договор в случае выявления в деятельности Организации признаков необычных и/или сомнительных операций либо при проведении Организацией операций, совершаемых в целях легализации (отмывания) доходов, полученных преступным путем или финансирования терроризма, письменно уведомив Организацию о расторжении Договора без соблюдения срока, установленного пунктом 5.2. При этом Договор будет считаться расторгнутым в дату, указанную в уведомлении Банка, направленном в соответствии с пунктом 6.4.

6.2. Банк вправе путем направления Организации письменного уведомления в одностороннем порядке приостановить на неограниченный срок предоставление услуг по Договору в случае подозрения или выявления в деятельности Организации признаков необычных и/или сомнительных операций либо при проведении Организацией операций, совершаемых в целях легализации (отмывания) доходов, полученных преступным путем или финансирования терроризма. При этом датой приостановления услуг считается дата, указанная в письменном уведомлении Банка. С даты приостановления услуг Организация вправе осуществлять распоряжение банковским счетом посредством предоставления распоряжений на бумажном носителе, оформленных и представленных Организацией в Банк в соответствии с требованиями законодательства Российской Федерации, нормативных актов Банка России и договором банковского счета на расчетно-кассовое обслуживание, заключенным между Банком и Организацией.

6.3. Банк вправе возобновить предоставление услуг по Договору в случае предоставления Организацией запрашиваемых документов и сведений, полностью удовлетворяющих требованиям Банка по форме и существу. Настоящим Организация соглашается с тем, что принятие решения о возобновлении предоставления услуг является правом, а не обязанностью Банка, и такое решение принимается исключительно по усмотрению Банка.

6.4. Стороны признают, что надлежащим письменным уведомлением, будет являться факт уведомления Организацией любым из следующих способов:

• по электронной почте – в таком случае уведомление считается полученным Организацией в дату отправления уведомления, указанную в электронном протоколе передачи уведомления. Уведомление направляется по электронному адресу, указанному Организацией.

• через отделения почтовой связи заказным письмом с уведомлением о вручении – уведомление считается полученным Организацией в дату, указанную в уведомлении о вручении. Уведомления направляются по последнему известному Банку почтовому адресу и считаются доставленными и в тех случаях, когда по обстоятельствам, зависящим от Организации, они не были вручены или Организация не ознакомился с ними (в том числе при изменении почтового адреса, о котором Организация не уведомила Банк);

• посредством передачи уведомления работнику Организации при его обращении в отделение Банка – уведомление считается полученным Организацией в дату вручения;

• через систему «Интернет Клиент-Банк» – считается полученным Организацией в дату отправления уведомления Банком.

6.5. Заключая Договор на условиях, изложенных в настоящем документе, Стороны исходят из соображений взаимовыгодного сотрудничества. За оказание услуг по Договору вознаграждение не взимается, если иное не будет установлено дополнительно соглашением между Банком и Организацией.

Условия, включая все приложения к нему, Заявление Организации, а также Руководство Пользователя Системы ЭДО, размещенное на веб-сайте Системы ЭДО, представляют собой исчерпывающий объем информации и документации, которые на момент подписания Договора должны быть предоставлены Организации в соответствии Федеральным законом от 27.06.2011 года № 161-ФЗ "О национальной платежной системе" и необходимы для использования Комплектов ключей Организации.

Руководство Пользователя Системы ЭДО, содержащее описание Системы ЭДО и правила ее функционирования, изменяется Банком в одностороннем порядке и предоставляется Организации в срок не позднее 10 (десяти) рабочих дней до даты внесения изменений путем размещения на веб-сайте www.rosbank.ru.

Организация согласна на дальнейшую модификацию Банком технологии работы Системы ЭДО с целью ее совершенствования.

Контактные телефоны для решения организационно-технических вопросов, связанных с функционированием Системы ЭДО:

От Банка Служба поддержки пользователей Системы ЭДО.

с 8.00 до 20.30 по телефонам:

для Москвы: (495) 725-55-95; (495) 518-99-11

для регионов: 8 (800) 700-20-70

Приложение № 1

к Условиям использования системы
электронного документооборота

СПИСОК

технических и программных средств, необходимых для работы подсистемы “Клиент”

1. Один или несколько компьютеров с одной из рекомендованных операционных систем: Windows 7 и выше. Компьютеры должны иметь работоспособный USB-порт и доступ в сеть Интернет. Остальные настройки по умолчанию.

2. При наличии в организации межсетевого экрана должна быть обеспечена возможность устанавливать TCP-соединения через порт 443.

3. На компьютере должны быть установлены:

- обозреватель Microsoft Internet Explorer версии 9.0 (минимальная версия) и выше, (11.0 – рекомендованная версия). Работа с аналогичными программными продуктами других фирм (Netscape и т.д.) не допускается. Настройки обозревателя – по умолчанию. При работе с WEB-сервером Системы ЭДО:
  - права Пользователя Системы ЭДО должны позволять обновление и выполнение элементов Active X;
  - блокирование всплывающих окон должно быть отключено.
- Средство Криптографической Защиты Информации (СКЗИ) КриптоПро CSP версии 4.0 и выше (разработчик - ООО "КРИПТО-ПРО"), с учетом совместимости его с операционной системой, необходимое для защиты соединения по протоколу TLS. Программное обеспечение и документация находятся в открытом доступе на сайте http://www.cryptopro.ru, после прохождения процедуры регистрации.
- Сертификаты уполномоченного Удостоверяющего центра ООО "КРИПТО-ПРО" в корневом контейнере доверенных сертификатов. Сертификаты расположены на сайте Удостоверяющего центра по ссылке: http://q.cryptopro.ru/

4. Дополнительное программное обеспечение, доступное для копирования с WEB-сервера Системы ЭДО:

- программа генерации Комплектов ключей
- программа проверки ЭП в ЭД Cryptomanager.exe.

5. Доступ на WEB-сервер Системы ЭДО осуществляется по адресу: https://www.bankline.ru.

Приложение № 2

к Условиям использования системы
электронного документооборота

ПРАВИЛА ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ

1. Обмен Электронными документами

1.1. Для работы в Системе ЭДО Пользователь Системы ЭДО использует программно-технические средства, удовлетворяющие требованиям, приведенным в Приложении № 1 к Условиям.

1.2. В процессе работы Пользователь Системы ЭДО выполняет в Системе ЭДО следующие действия:

Регистрация в Системе ЭДО – формирование специального ЭД “регистрация”, подписанного ЭП Клиента (далее – ЭПК). Работа в Системе ЭДО возможна только после успешной проверки ЭПК сервером Системы ЭДО.

Работа с ЭД, исходящими от Организации, предполагает формирование новых ЭД на основе ЭД, имеющихся в Системе ЭДО и предусмотренных Заявлением Организации. Для каждого типа ЭД в Системе ЭДО имеется соответствующая экранная форма;

Проставление для каждого ЭД одной или нескольких ЭПК. Количество для каждого типа ЭД определено в Заявлением Организации. После подписания ЭД всеми необходимыми ЭПК в соответствии с Заявлением Организации происходит автоматическая пересылка ЭД в Банк для исполнения;

И иные действия, предусмотренные функционалом Системы ЭДО.

1.3. Процедура обработки ЭД сервером Системы ЭДО происходит следующим образом:

По окончании формирования ЭД Пользователи Системы ЭДО проставляют свои ЭПК в количестве, определенном в Заявлением Организации, и отправляют ЭД в Банк.

Сервер Банка получает ЭД и проверяет корректность всех имеющихся в нем ЭПК.

Основанием для принятия Банком ЭД, переданного Организацией по Системе ЭДО, является наличие в количестве, установленном в соответствии с Заявлением Организации, и корректность всех ЭПК документа. При положительном результате проверки сервер Банка проставляет в документе отметку о времени и ЭП Банка (далее – ЭПБ), свидетельствующую о получении документа Банком, и сохраняет данный документ в Системе ЭДО. При отрицательном результате проверки ЭПК ЭПБ в документе не проставляется, Организация получает сообщение об ошибке средствами Системы ЭДО. Ключи проверки электронной подписи Банка и копии соответствующих Сертификатов размещаются на сервере системы https://www.bankline.ru. Сертификат Ключа проверки электронной подписи Банка подписывается только уполномоченным представителем Банка. Срок действия Комплекта ключей Банка составляет 5 лет.

1.4. Процедуры, описанные в п.1.3 настоящих Правил, представляют собой единый и неделимый на части процесс получения Банком ЭД, не могут быть выполнены в другой последовательности и рассматриваться независимо друг от друга.

1.5. Документ считается переданным Организацией в Банк, если он сохранен в архиве исходящих документов Организации на сервере Банка. Организация может сохранить любой исходящий документ в файл для ведения собственного архива. Файл содержит ЭПК, отметку о времени приема документа Банком и ЭПБ. Файлы с сервера Банка и из архива Организации могут затем использоваться при процедуре разрешения разногласий между Сторонами.

1.6. Переданный Организацией в Банк документ в каждый момент времени имеет на сервере Банка определенный статус с отметкой времени его получения. Статус документа изменяется Банком. Организация имеет возможность постоянно получать на сервере Банка информацию об изменении статуса (в том числе о времени его изменения) переданного в Банк документа. Сервер Банка присваивает полученным от Организации документам следующие статусы:

“получен банком”;
“документ отправлен на исполнение”;
“сообщение отправлено в филиал“.

Стороны признают, что надлежащим уведомлением Банком Организации о приеме к исполнению ЭД Организации будет являться присвоение Банком ЭД Организации статуса “документ отправлен на исполнение”.

Банк информирует Организацию об исполнении каждого ЭД Организации путем направления Организации соответствующего уведомления посредством Системы ЭДО.

1.7. При формировании ЭД для Организации Банк проставляет в нем ЭПБ. Документ считается переданным Банком Организации, если он подписан ЭПБ и выложен на сервер Банка, то есть имеется в списке входящих документов Организации на сервере Банка. Организация может сохранить любой входящий документ в файл для ведения собственного архива. Файлы архива могут затем использоваться при разрешении разногласий.

1.8. Банк фиксирует электронные архивы полученных от Организации ЭД, содержащих ЭПК и ЭПБ, и доставленных Организации ЭД, содержащих ЭПБ, способом, обеспечивающим Организации доступ к данным документам на сервере Банка.

1.9. Организация с помощью программы проверки ЭП CryptoManager.exe имеет возможность в любой момент времени проверить ЭПБ и ЭПК любого файла архива. Вышеуказанная программа проверки ЭП позволяет выполнять проверку типов ЭП (п. 3.1 настоящих Правил), разрешенных для использования в Системе ЭДО.

1.10. Программу проверки ЭП CryptoManager.exe можно получить у фирмы-разработчика Системы ЭДО – ЗАО “ИНИСТ” (Лицензия ФСБ России № 12818Н от 16.04.2013), зарегистрированной по адресу 115035, г. Москва, Космодамианская наб., д.40-42, стр.3.

2. Порядок получения, замены и хранения ключей

2.1. Для Комплектов ключей, сгенерированных для работы на Персональном компьютере Организациями, относящимися к корпоративному сегменту:

2.1.1. Организация может генерировать Комплекты ключей своих Пользователей Системы ЭДО согласно Заявлению Организации с помощью программных средств, предоставленных Банком, на своих технических средствах.

2.1.2. Ключ проверки электронной подписи каждого Пользователя Системы ЭДО регистрируется Банком на основании подписанного Сторонами Сертификата ключа.

2.1.3. Срок действия Комплекта ключей указывается в Сертификате ключа. Рекомендуемый Банком срок действия Комплекта ключей не может превышать срок действия полномочий Пользователя Системы в соответствии с документами, подтверждающими его полномочия. В случае, если исходя из представленных Организацией документов не представляется возможным установить срок действия полномочий Пользователя Системы, срок действия Комплекта ключей не может превышать 3 (трех) лет. До истечения установленного срока Организация обязана инициировать процедуру смены Комплектов ключей. По заявлению Организации, направленному в Банк средствами Системы ЭДО до окончания срока действия Комплекта ключей, его действие может быть продлено на срок не более 3 (трех) месяцев. По инициативе Организации Комплект ключей может быть заменен в любой момент его действия. Каждый новый Сертификат ключа, подписанный Сторонами, автоматически отменяет действие Сертификата ключа данного Пользователя Системы ЭДО, выпущенного ранее.

2.1.4 Оформленные со стороны Банка Сертификаты ключей Организации вручаются лично представителю Организации, курьеру Организации, либо направляются Организации посредством почтовой связи. Сертификаты ключей должны храниться у каждой из Сторон не менее 5 (пяти) лет после окончания их срока действия.

2.1.5 Обязательная замена Комплекта ключей проводится в следующих случаях:

истек срок действия Комплекта ключей;

произошла Компрометация ключей.

2.1.6 В случае лишения Организацией Пользователя Системы ЭДО права подписывать ЭП ЭД соответствующие Комплекты ключей выводятся из действия на основании письменного заявления Организации или ЭД свободного формата, отправленного средствами Системы ЭДО.

2.2. Для Комплектов ключей, сгенерированных для работы на Персональном компьютере Организациями, относящимися к сегменту предпринимателей:

2.2.1. Организация может генерировать Комплекты ключей своих Пользователей Системы ЭДО согласно Заявлению Организации на иных носителях информации (жесткий диск, съемные носители (флеш-память, внешний винчестер) и т.п.) с использованием своих технических средств.

2.2.2. Первый Ключ проверки электронной подписи каждого Пользователя Системы ЭДО регистрируется Банком на основании подписанного Сторонами Сертификата ключа, оформленного на бумажном носителе.

2.2.3. Второй и последующий Ключи проверки электронной подписи регистрируется Банком на основании подписанного Сторонами Сертификата ключа, оформленного на бумажном носителе, или на основании электронного запроса на выдачу Сертификата ключа, подписанного действующей на момент подписания электронной подписью Пользователя Системы ЭДО, и направленного в Банк с использованием Системы ЭДО. Указанный запрос также может быть подписан простой электронной подписью Пользователя Системы ЭДО, сформированной на основании SMS-кода, ранее направленного Банком на номер телефона данного Пользователя Системы ЭДО, указанный в Заявлении и/или предоставленный Банку Пользователем Системы ЭДО в процессе обслуживания. Пользователь Системы ЭДО должен обладать полномочиями на направление в Банк соответствующего электронного запроса . При этом, Банк вправе запрашивать, а Организация обязана по запросу Банка предоставлять в Банк документы (в виде подлинников или надлежащим образом заверенных копий), подтверждающие полномочия Пользователя Системы ЭДО по направлению в Банк электронного запроса на выдачу Сертификата ключа.

2.2.4. Срок действия Комплекта ключей определяется Банком и указывается в Сертификате ключа. Срок действия Комплекта ключей не может превышать срок действия полномочий Пользователя Системы ЭДО в соответствии с документами, подтверждающими его полномочия. В случае, если исходя из представленных Организацией документов не представляется возможным установить срок действия полномочий Пользователя Системы ЭДО, срок действия Комплекта ключей не может превышать 3 (трех) лет. До истечения установленного срока действия Комплекта ключей Организация обязана инициировать процедуру смены Комплектов ключей. При этом, до окончания срока действия Комплекта ключей Организация может продлить его действие на срок не более 3 (трех) месяцев, направив в Банк заявление посредством Системы ЭДО. По инициативе Организации Комплект ключей может быть заменен в любой момент его действия. Каждый новый Сертификат ключа, подписанный Банком, автоматически отменяет действие Сертификата ключа данного Пользователя Системы ЭДО, выпущенного ранее.

2.2.5. Оформленные со стороны Банка Сертификаты ключей Организации на бумажных носителях вручаются уполномоченному представителю Организации либо направляются Организации посредством почтовой связи по адресу Организации, указанному в Договоре. Сертификаты ключей должны храниться у каждой из Сторон не менее 5 (пяти) лет после окончания их срока действия.

2.2.6. При поступлении электронного запроса на выдачу Сертификата ключа, подписанного действующей на момент подписания электронной подписью Пользователя Системы ЭДО, Банк направляет Организации с использованием Системы ЭДО Сертификат ключа, подписанный электронной подписью уполномоченного представителя Банка. При этом Организация вправе обратиться в Банк с целью получения копии Сертификата ключа на бумажном носителе, заверенной Банком как удостоверяющим центром.

3. Обеспечение безопасности процедуры обмена документами

3.1. Безопасность обмена ЭД достигается за счет применения следующих средств:

Средство криптографической защиты информации (СКЗИ) на базе Программного комплекса «Бикрипт 5.0.», разработанного ООО Фирма «ИнфоКрипт» (сертификат соответствия ФСБ РФ СФ/114-3021 от 30 декабря 2016 года);

Шифрования данных в телекоммуникационных каналах с использованием СКЗИ КриптоПро CSP версии 4.0 и выше; Для защиты данных от несанкционированного доступа в телекоммуникационных каналах используется протокол TLS (Transport Layer Security), применяются криптографические алгоритмы шифрования и хеширования;

Удостоверения принадлежности сервера Системы ПАО РОСБАНК с помощью сертификата, выданного ПАО РОСБАНК аккредитованным Удостоверяющим центром ООО "КРИПТО-ПРО".

3.2. На основании дополнительных соглашений между Сторонами возможно применение других технических средств защиты информации.

3.3. Организации рекомендуется обеспечить комплекс организационно-технических мер, направленных на выполнение следующих требований безопасности:

Организовать выделенный компьютер подсистемы «Клиент», предназначенный исключительно для работы с Банком;

Ввести ограничение сетевого взаимодействия компьютера подсистемы «Клиент» только с необходимым доверенным перечнем IP-адресов;

Проверять, что установлено защищенное SSL-соединение с официальным ресурсом сервиса https://www.bankline.ru/;

Обеспечить на выделенном компьютере наличие средств защиты от вредоносного программного обеспечения, их работоспособность и регулярное обновление;

Исключить на выделенном компьютере открытие писем с вложениями, полученными от неизвестных или недоверенных источников;

Средствами подсистемы «Клиент» закрепить за Пользователями Системы ЭДО IP-адрес/список IP-адресов компьютеров подсистемы «Клиент» в целях обеспечения контроля на стороне Банка;

Обеспечить использование исключительно лицензионного программного обеспечения и операционной системы;

Организовать регулярную установку обновлений безопасности программного обеспечения и операционной системы;

Исключить использование средств удаленного администрирования;

Обеспечить применение лицензионного межсетевого экрана (допускается использование персонального межсетевого экрана;

Выполнить комплекс организационных мероприятий по обеспечению информационной безопасности (настройка безопасности операционной системы, ограничение прав доступа информационной системы, организация парольной защиты, подготовка процедур реагирования на инциденты и т.п.);

Контролировать соблюдение требований безопасности.

3.4. Организация обязана:

Исключить появление в компьютере подсистемы “Клиент” вирусов и других программ деструктивного действия, которые могут разрушить или модифицировать программное обеспечение подсистемы, скомпрометировать ключи Пользователя Системы ЭДО. Для чего обязательно применение лицензионных средств защиты от вредоносного кода и регулярного их обновления;

Исключить возможность несанкционированных Банком изменений в технических и программных средствах Организации, определенных в Приложении 1;

Исключить возможность Компрометации ключей в процессе их транспортировки, эксплуатации и хранения.

3.5. Стороны обязаны:

обеспечивать конфиденциальность Ключей электронных подписей, в частности не допускать использование принадлежащих им Ключей электронных подписей без их согласия;

уведомлять другую Сторону о нарушении конфиденциальности Ключа электронной подписи (Компрометации ключа) в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;

не использовать Ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

3.6. Банк вправе в одностороннем порядке заблокировать ключ Пользователя в случае появления обоснованных подозрений в наличии на компьютере Пользователя вирусов или других программ деструктивного действия. Блокировка ключа Пользователя снимается Банком по факту получения от Организации подтверждения об удалении с компьютера Пользователя вирусов или других программ деструктивного действия.

3.7. В случае возникновения угрозы Компрометации ключей регламентируется следующая последовательность действий Сторон.

Если произошла Компрометация ключей любого Пользователя Организации, последняя обязана:

В случае доступности Комплекта ключей (подозрение на несанкционированное копирование) немедленно послать в Банк ЭД “Блокировка ключа”. При этом Система автоматически заблокирует возможность использования данного Комплекта ключей Пользователя Системы ЭДО;

В случае недоступности (утрата, хищение и т.п.) Комплекта ключей сообщить Администратору Системы ЭДО по телефону (телефон и электронный адрес Администратора Системы ЭДО указаны в реквизитах Банка Заявления Организации), используя для авторизации кодовую фразу, приведенную в Сертификате ключа, о факте Компрометации ключей.

В случае утраты Пользователем Системы ЭДО кодовой фразы Администратор Системы ЭДО вправе произвести дополнительные действия по авторизации Пользователя Системы ЭДО (обратный звонок по указанному в Заявлении Организации телефону, запрос на предоставление дополнительной информации: о фамилии куратора Организации в Банке/уполномоченного сотрудника Банка, номере Договора, количестве пользователей и т.п.).

В случае компрометации (утраты, разглашения) SMS-кода незамедлительно сообщить Администратору Системы ЭДО по телефону (телефон и электронный адрес Администратора Системы ЭДО указаны на сайте www.bankline.ru, а также в Заявлении).

В срок не более 3 (трех) рабочих дней после сообщения по телефону о факте Компрометации ключей направить в Банк на бланке Организации письменное объяснение случившегося, заверенное надлежащим образом подписями уполномоченных лиц и печатью Организации.

В письме должно содержаться распоряжение Банку о приостановлении дальнейшей обработки ЭД до устранения причин случившегося и (или) замены ключей;

В случае принятия решения о замене Комплекта ключей сгенерировать новый Комплект ключей самостоятельно и направить своего представителя в Банк для его регистрации.

3.8. При получении авторизованного по кодовой фразе телефонного сообщения о возникновении угрозы Компрометации ключей Банк немедленно приостанавливает использование Системы ЭДО данной Организацией. С этого момента операции проводятся только на основании документов, оформленных в бумажном виде. Дальнейшее использование Системы ЭДО Организацией возможно только после устранения угрозы Компрометации ключей Организации.

Если произошла Компрометация ключей Банка, последний обязан:

Известить Организацию о факте компрометации Комплекта ключей Банка, продолжении\приостановлении работы Системы ЭДО и смене Комплекта ключей Банка посредством Системы ЭДО с указанием даты и точного времени смены вышеуказанного Комплекта ключей;

Произвести внеплановую смену Комплекта ключей Банка, опубликовать новый Ключ проверки электронной подписи и копию Сертификата ключа Банка, содержащего новый Ключ проверки электронной подписи Банка, на сервере Системы ЭДО.

4. Порядок проверки ЭД и ЭП при разногласиях

4.1. Для разрешения споров относительно подлинности ЭД по заявлению заинтересованной Стороны, полагающей, что ее права нарушены, Сторонами в двухнедельный срок с даты подачи заявления создается Согласительная комиссия, в присутствии которой производятся все операции по подготовке и проведению процедуры разрешения спора. В состав Согласительной комиссии включаются представители Банка в количестве двух человек и представители Организации в количестве двух человек, а в случае необходимости (по соглашению Сторон) – независимые эксперты. Представителями Банка и Организации могут быть назначены как сотрудники этих организаций, так и иные компетентные лица, полномочия которых подтверждаются соответствующими доверенностями.

4.2. Спорным ЭД является ЭД, в отношении которого одна Сторона предъявляет претензии по его подлинности другой Стороне.

4.3. Процедура проверки подлинности ЭД проводится на оборудовании и в помещении Банка.

4.4. В присутствии членов Согласительной комиссии Банк обязан на свободном от программного обеспечения компьютере установить операционную систему Windows7 и выше и предоставленную фирмой-разработчиком ЗАО “ИНИСТ” программу проверки ЭП, указанную в п.1.10 настоящих Правил.

4.4.1. Сторона, отстаивающая подлинность Спорного ЭД, обязана предоставить Спорный ЭД, действовавшие в момент создания Спорного ЭД Сертификаты ключей Стороны, подписавшей спорный ЭД, а также сами Ключи проверки электронной подписи, записанные на съемном носителе в виде файлов в формате, применяемом Системой ЭДО (в случае если Организация не предоставляет Спорный ЭД, он предоставляется Банком).

4.4.2. Стороны обязаны предоставить все имеющиеся в их распоряжении Сертификаты ключей, информацию о проведенных плановых и внеплановых сменах Комплекта ключей Сторон и документы, удостоверяющие факты смены Комплекта ключей. Стороны также обязаны предоставить служебные ЭД Системы ЭДО, в которых указаны факты получения ЭД из каналов связи и результаты их обработки (проверки).

4.5. Члены Согласительной комиссии должны выполнить следующие действия:

4.5.1. Произвести с помощью программы проверки ЭП, указанной в п.1.10 настоящих Правил, и каждого Ключи проверки электронной подписи, использованного при подписании спорного ЭД, операцию проверки ЭП;

4.5.2. Создать Протокол установления подлинности ЭД – документ на бумажном носителе, создаваемый Системой ЭДО в качестве результата проверки ЭП Спорного ЭД (далее - Протокол). Протокол должен содержать распечатанные на бумажном носителе Ключи проверки электронной подписи, использованные для установления подлинности ЭП, и заключение об итогах проверки ЭП Спорного ЭД. Протокол установления подлинности должен быть подписан собственноручно всеми членами Согласительной комиссии;

4.5.3. Сравнить Ключи проверки электронной подписи, содержащиеся в Сертификатах ключей, с соответствующими Ключами проверки электронной подписи, зафиксированными в Протоколе установления подлинности ЭП Спорного ЭД, и установить, тождественны ли они, внести об этом запись в Протокол (данная запись заверяется подписями членов Согласительной комиссии);

4.5.4. Установить, являлись ли Ключи проверки электронной подписи действующими на момент выработки ЭП Спорного ЭД, и внести запись об этом в Протокол (данная запись заверяется подписями членов Согласительной комиссии). Ключ проверки электронной подписи признается действующим на момент создания ЭП Спорного ЭД в случае, если дата создания Спорного ЭД приходится на период действия Ключа проверки электронной подписи. В противном случае Ключ проверки электронной подписи признается недействующим на момент создания ЭП.

4.6. Согласительная Комиссия признает Электронный документ подлинным, если одновременно выполнены условия:

Ключи проверки электронной подписи в Сертификатах ключей и в Протоколе совпадают,

Все результаты проверки ЭП в Протоколе положительны,

Комиссия признала все Ключи проверки электронной подписи, содержащиеся в Протоколе, действующими на момент выработки ЭП.

– В противном случае Согласительная Комиссия признает ЭД недействительным.

Приложение № 3

к Условиям использования системы
электронного документооборота

Сведения, необходимые для идентификации, в отношении Пользователей Системы ЭДО,

1. Фамилия, имя, отчество;
2. Дата и место рождения;
3. Гражданство;
4. Реквизиты документа, удостоверяющего личность (серия, номер, дата выдачи, наименование выдавшего органа, код подразделения (если имеется);
5. Адрес места жительства (регистрации) или адрес фактического проживания[1];
6. ИНН (если имеется);
7. Номера контактных телефонов;

(дополнительно для иностранных граждан и лиц без гражданства):

8. Данные миграционной карты (номер карты, дата начала срока пребывания и дата окончания срока пребывания);
9. Данные документа, подтверждающего право иностранного гражданина или лица без гражданства на пребывание (проживание) в РФ (серия (если имеется) и номер документа, дата начала срока действия права пребывания (проживания) и дата окончания срока действия права пребывания (проживания)

[1] Информация об адресе места жительства (регистрации) устанавливается на основании предъявленного Пользователем системы ЭДО документа, удостоверяющего личность. При отсутствии в документе, удостоверяющем личность, информации об адресе места жительства (регистрации), сведения об адресе пребывания (фактического проживания) устанавливаются на основании свидетельства о регистрации по адресу пребывания, письма от Организации, составленного в произвольной форме, или иного документа, заверенного подписью и печатью (при наличии) Организации. Допускается получение сведений об адресе пребывания (фактического проживания) Пользователя ЭДО от Организации по системе ЭДО