«Газпромбанк» (Акционерное общество)
Банк ГПБ (АО)

УТВЕРЖДАЮ

Заместитель Председателя
Правления Банка ГПБ (АО)

_____ А.Ю. Муранов

Рег. № И/47

« 09 » июня 2018 г.

РЕГЛАМЕНТ
удостоверяющего центра
Банка ГПБ (АО)

Москва
2018

Содержание

1. Общие положения

1.1. Настоящий Регламент разработан в соответствии с законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров, отношения в области использования Электронных подписей при совершении гражданско-правовых сделок и при совершении иных юридически значимых действий.

1.2. Перечень терминов и условных сокращений приведен в приложении № 1.

1.3. Удостоверяющий центр осуществляет свою деятельность на территории Российской Федерации на основании имеющейся у Банка лицензии ФСБ России на деятельность, связанную с использованием шифровальных (криптографических) средств, а также лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации.

1.4. Распространение настоящего Регламента, в том числе опубликование его в сети Интернет на официальном сайте Банка, должно рассматриваться клиентами как оферта Банка, адресованная физическим и юридическим лицам, о заключении с Банком Договора на условиях, изложенных в настоящем Регламенте.

1.5. Заключение Договора производится на условиях, предусмотренных статьей 428 Гражданского кодекса Российской Федерации, для договора присоединения путем акцепта оферты Банка о заключении Договора без каких-либо изъятий, оговорок и условий, в порядке и на условиях, которые установлены настоящим Регламентом.

1.6. Для заключения Договора клиент должен представить в Банк Заявление об акцепте условий Регламента и изготовлении сертификата ключа проверки электронной подписи по форме приложения № 2 или 3 или Заявление об акцепте условий Регламента и изготовлении технологического сертификата ключа проверки электронной подписи по форме приложения № 4 или 5. С даты регистрации Заявления об акцепте условий Регламента и изготовлении сертификата ключа проверки электронной подписи или Заявления об акцепте условий Регламента и изготовлении технологического сертификата ключа проверки электронной подписи лицо, подавшее данное заявление, является Стороной Договора.

1.7. Настоящий Регламент определяет условия предоставления и правила пользования услугами Удостоверяющего центра для Систем ЭДО, оператором которых является Банк и в которых обмен Электронными документами осуществляется между Пользователем УЦ и Банком, включая права, обязанности, ответственность Сторон, форматы данных, основные организационно-технические мероприятия, направленные на обеспечение работы Удостоверяющего центра.

1.8. Удостоверяющий центр вправе отказать любому лицу в приеме и регистрации Заявления об акцепте условий Регламента и изготовлении сертификата ключа проверки электронной подписи, Заявления об акцепте условий Регламента и изготовлении технологического сертификата ключа проверки электронной подписи и Запроса на изготовление сертификата ключа проверки электронной подписи без объяснения причин.

1.9. Факт заключения лицом Договора означает полное принятие им условий настоящего Регламента и всех его приложений в редакции, действующей на дату регистрации Заявления об акцепте условий Регламента и изготовлении сертификата ключа проверки электронной подписи или Заявления об акцепте условий Регламента и изготовлении технологического сертификата ключа проверки электронной подписи. Лицо, заключившее Договор, принимает дальнейшие изменения (дополнения), вносимые в настоящий Регламент, в соответствии с условиями настоящего Регламента.

1.10. После заключения Договора Удостоверяющий центр и Сторона вступают в соответствующие договорные отношения на неопределенный срок.

1.11. Действие Договора может быть прекращено по инициативе одной из Сторон в следующих случаях:

1.11.1. В связи с отказом Банка от настоящего Договора (его исполнения) при условии уведомления Стороны о таком отказе не позднее чем за десять дней до прекращения Договора.

1.11.2. В случае нарушении одной из Сторон условий настоящего Регламента.

1.11.3. В иных случаях, предусмотренных законодательством Российской Федерации.

1.12. Прекращение действия настоящего Регламента не освобождает Стороны от ответственности за его неисполнение (ненадлежащее исполнение).

1.13. В случае расторжения Договора по инициативе одной из Сторон такая Сторона письменно уведомляет другую Сторону о своих намерениях за четырнадцать календарных дней до предполагаемой даты расторжения Договора. Договор считается расторгнутым после выполнения Сторонами своих обязательств.

1.14. В случае расторжения Договора одной из Сторон все Сертификаты ключей проверки электронной подписи, владельцами которых являются Пользователи УЦ – полномочные представители данной Стороны, прекращают свое действие.

1.15. Прекращение деятельности Удостоверяющего центра может быть осуществлено на основании решения Банка и в порядке, установленном внутренними нормативными документами Банка и действующим законодательством Российской Федерации. При этом все Сертификаты ключей проверки электронной подписи пользователей, выданные Удостоверяющим центром, прекращают свое действие и уничтожаются, если иное не предусмотрено действующим законодательством Российской Федерации.

1.16. При использовании Электронных подписей, Средств электронной подписи и Систем ЭДО возникают следующие основные риски:

1.16.1. Неправомерное использование Ключа ЭП Пользователя УЦ третьими лицами в случае его компрометации.

1.16.2. Нарушение работы Системы ЭДО в результате технических сбоев Средств электронной подписи, связи, программных средств и др.

1.16.3. Несоответствие технологий проведения операций, внутренних порядков и процедур проведения операций, процедур управления, учета и контроля за соблюдением требований законодательства Российской Федерации.

1.17. В целях обеспечения безопасности Системы ЭДО Стороны обязаны назначить Администраторов безопасности.

1.18. Все приложения и изменения к настоящему Регламенту являются его неотъемлемой частью.

1.19. Настоящий Регламент распространяется в форме Электронного документа, публикуемого на официальном сайте Банка.

1.20. Списки отозванных сертификатов и Сертификаты ключей проверки электронной подписи Уполномоченного лица УЦ публикуются на ресурсе http://cs.gazprombank.ru.

1.21. Реквизиты Удостоверяющего центра:

- наименование: «Удостоверяющий центр Банка ГПБ (АО)»;
- почтовый адрес: 117420, город Москва, улица Наметкина, дом 16, корпус 1;
- фактический адрес: 117418, город Москва, улица Новочеремушкинская, дом 63;
- телефон: (495) 287- 61-61, e-mail: ca.gpb@gazprombank.ru.

2. Порядок пользования услугами Удостоверяющего центра

2.1. Изготовление ключей Пользователя УЦ

2.1.1. Пользователь УЦ самостоятельно генерирует свой Ключ электронной подписи и Ключ проверки электронной подписи, а также формирует электронный Запрос на изготовление сертификата ключа проверки электронной подписи в формате PKCS#10 и заполняет Заявление об акцепте условий Регламента и изготовлении сертификата ключа проверки электронной подписи по форме приложения № 2 или 3. Идентификационные данные запроса на изготовление Сертификата ключа проверки электронной подписи должны соответствовать Заявлению об акцепте условий Регламента и изготовлении сертификата ключа проверки электронной подписи. При этом данные заполняются в соответствии с «Правилами заполнения заявлений и запросов на изготовление сертификатов ключей проверки электронной подписи», приведенными в приложении № 6. Данные в Заявлении об акцепте условий Регламента и

изготовлении сертификата ключа проверки электронной подписи также заполняются в соответствии с приложением № 6.

2.1.2. В случае если Заявление об акцепте условий Регламента и изготовлении сертификата ключа проверки электронной подписи подается лицом, действующим по доверенности, такая доверенность должна в явном виде содержать согласие доверителя на использование при взаимодействии с Банком Систем ЭДО с применением Средств электронной подписи. Если доверитель является физическим лицом, то в Заявлении об акцепте условий Регламента и изготовлении сертификата ключа проверки электронной подписи в качестве Владельца сертификата ключа проверки электронной подписи указывается лицо, действующее по доверенности. Если доверитель является юридическим лицом, то лицо, действующее по доверенности, подписывает Заявление об акцепте условий Регламента и изготовлении сертификата ключа проверки электронной подписи как руководитель организации.

2.1.3. Заявление об акцепте условий Регламента и изготовлении сертификата ключа проверки электронной подписи подписывается лично Владельцем сертификата ключа проверки электронной подписи и не может быть делегировано другому лицу.

2.1.4. Используемое в Запросе на изготовление сертификата ключа проверки электронной подписи и Заявлении об акцепте условий Регламента и изготовлении сертификата ключа проверки электронной подписи поле наименования организации для различных СКЗИ ограничивается 64 или 128 символами. В случае если полное и краткое наименование организации Пользователя УЦ превышает это значение, необходимо дополнительно оформить Заявление об использовании сокращенного наименования организации в сертификате ключа проверки электронной подписи в соответствии с приложением № 7. Для каждой организации допускается использование только одного сокращенного наименования.

2.1.5. Формирование Запроса на изготовление сертификата ключа проверки электронной подписи производится посредством Средств электронной подписи, встроенных в Систему ЭДО, либо с помощью СКЗИ, передаваемых Пользователю УЦ в соответствии с подразделом 2.6.

2.1.6. Передача Запроса на изготовление сертификата ключа проверки электронной подписи и Заявления об акцепте условий Регламента и изготовлении сертификата ключа проверки электронной подписи в Банк должна производиться не позднее двух месяцев с момента формирования Пользователем УЦ Ключа электронной подписи.

2.1.7. Заполненное Заявление об акцепте условий Регламента и изготовлении сертификата ключа проверки электронной подписи передается Менеджеру Системы ЭДО (лично, курьером или по почте). Передача Запроса на изготовление сертификата ключа проверки электронной подписи может производиться:

2.1.7.1. Через Менеджера Системы ЭДО на заранее оговоренном с Менеджером Системы ЭДО носителе информации либо по электронной почте.

2.1.7.2. С помощью транспортной подсистемы Системы ЭДО.

2.1.8. Менеджер Системы ЭДО фиксирует в соответствующей графе Заявления об акцепте условий Регламента и изготовлении сертификата ключа проверки электронной подписи дату и время его поступления, осуществляет проверку указанных в нем данных, визирует его и не позднее следующего рабочего дня направляет в Удостоверяющий центр вместе с электронным Запросом на изготовление сертификата ключа проверки электронной подписи.

2.1.9. Менеджер Системы ЭДО может отказать в приеме Заявления об акцепте условий Регламента и изготовлении сертификата ключа проверки электронной подписи в случае его ненадлежащего оформления или указания недостоверной информации. Порядок и сроки уведомления Пользователя УЦ об отказе в изготовлении Сертификата ключа проверки электронной подписи зависят от Системы ЭДО и указаны в документах, определяющих порядок работы с ней.

2.1.10. Уполномоченное лицо УЦ проверяет данные, указанные в Запросе на изготовление сертификата ключа проверки электронной подписи, на соответствие Заявлению об акцепте условий Регламента и изготовлении сертификата ключа проверки электронной

подписи. Если данные совпадают, Уполномоченное лицо УЦ изготавливает Сертификат ключа проверки электронной подписи и направляет его Менеджеру Системы ЭДО для дальнейшей передачи Пользователю УЦ. Передача Сертификата ключа проверки электронной подписи Пользователю УЦ может производиться теми же способами, которые предусмотрены для передачи Запроса на изготовление сертификата ключа проверки электронной подписи и приведены в подпункте 2.1.7.

2.1.11. Уполномоченное лицо УЦ обрабатывает поступившие Заявления об акцепте условий Регламента и изготовлении сертификата ключа проверки электронной подписи и Запросы на изготовление сертификатов ключей проверки электронной подписи не позднее следующего рабочего дня.

2.1.12. В случае отказа Уполномоченным лицом УЦ в изготовлении Сертификата ключа проверки электронной подписи Уполномоченное лицо УЦ в тот же рабочий день информирует об этом Менеджера Системы ЭДО. Менеджер Системы ЭДО не позднее рабочего дня, следующего за датой получения информации об отказе в изготовлении Сертификата ключа проверки электронной подписи от Уполномоченного лица УЦ, уведомляет об этом Пользователя УЦ в письменном виде (по электронной почте) с указанием причины отказа.

2.2. **Изготовление Технологических ключей Пользователя УЦ**

2.2.1. Изготовление Технологических ключей и технологических Сертификатов ключей проверки электронной подписи осуществляется только в тех случаях, когда это предусмотрено порядком использования Системы ЭДО.

2.2.2. Изготовление Технологического ключа Электронной подписи и технологического Сертификата ключа проверки электронной подписи осуществляется на основании Заявления об акцепте условий Регламента и изготовлении технологического сертификата ключа проверки электронной подписи по форме приложения № 4 или 5.

2.2.3. Заявление об акцепте условий Регламента и изготовлении технологического Сертификата ключа проверки электронной подписи заполняется в соответствии с «Правилами заполнения заявлений и запросов на изготовление сертификатов ключей проверки электронной подписи», приведенными в приложения № 6.

2.2.4. Заполненное Заявление об акцепте условий Регламента и изготовлении технологического сертификата ключа проверки электронной подписи передается Менеджеру Системы ЭДО (лично, курьером или по почте).

2.2.5. Используемое в Заявлении об акцепте условий Регламента и изготовлении технологического сертификата ключа проверки электронной подписи поле наименования организации ограничивается 128 символами. В случае если полное и краткое наименование организации Пользователя УЦ превышает это значение, необходимо дополнительно оформить «Заявление об использовании сокращенного наименования организации в сертификате ключа проверки электронной подписи» в соответствии с приложением № 7.

2.2.6. Менеджер Системы ЭДО фиксирует в соответствующей графе Заявления об акцепте условий Регламента и изготовлении технологического сертификата ключа проверки электронной подписи дату и время его поступления, осуществляет проверку указанных в нем данных, визирует его и не позднее следующего рабочего дня направляет в Удостоверяющий центр.

2.2.7. Менеджер Системы ЭДО может отказать в приеме Заявления об акцепте условий Регламента и изготовлении технологического Сертификата ключа проверки электронной подписи в случае его ненадлежащего оформления или указания недостоверной информации.

2.2.8. Уполномоченное лицо УЦ регистрирует Пользователя УЦ в реестре Удостоверяющего центра, изготавливает Технологический ключ Электронной подписи и технологический Сертификат ключа проверки электронной подписи и передает их Менеджеру Системы ЭДО для дальнейшей передачи Пользователю УЦ.

2.2.9. Уполномоченное лицо УЦ обрабатывает поступившие Заявления об акцепте условий Регламента и изготовлении технологического сертификата ключа проверки

электронной подписи не позднее следующего рабочего дня.

2.2.10. В случае отказа в изготовлении технологического Сертификата ключа проверки электронной подписи Пользователь УЦ уведомляется об этом Менеджером Системы ЭДО в письменном виде (по электронной почте) с указанием причины отказа.

2.2.11. Получив Технологический ключ Электронной подписи и технологический Сертификат ключа проверки электронной подписи, Пользователь УЦ средствами Системы ЭДО формирует свои Рабочие ключи ЭП. При заполнении полей Запроса на изготовление сертификата ключа проверки электронной подписи и Заявления об акцепте условий Регламента и изготовлении сертификата ключа проверки электронной подписи используются данные из технологического Сертификата ключа проверки электронной подписи.

2.3. **Изготовление Тестовых ключей**

2.3.1. Удостоверяющий центр может предоставлять услуги по изготовлению Тестовых ключей и тестовых Сертификатов ключей проверки электронной подписи, предназначенных для тестирования Систем ЭДО.

2.3.2. Изготовление Тестовых ключей и тестовых Сертификатов ключей проверки электронной подписи проводится на основании письменного обращения клиента в Банк, согласованного с Менеджером Системы ЭДО, или на основании заявки самостоятельного структурного подразделения Банка, являющегося организатором Системы ЭДО.

2.3.3. Тестовые Сертификаты ключей проверки электронной подписи в обязательном порядке формируются на конкретных лиц, осуществляющих тестирование. Использование в тестовых Сертификатах ключей проверки электронной подписи вымышленных данных не допускается.

2.3.4. Указанные в тестовых Сертификатах ключей проверки электронной подписи данные заполняются в соответствии с «Правилами заполнения заявлений и запросов на изготовление сертификатов ключей проверки электронной подписи», приведенными в приложении № 6.

2.4. **Изготовление Сертификата ключа проверки электронной подписи Пользователя УЦ на бумажном носителе**

2.4.1. Удостоверяющий центр осуществляет выдачу Сертификатов ключей проверки электронной подписи в виде Электронных документов. По желанию Пользователя УЦ Удостоверяющий центр может осуществить выдачу Сертификата ключа проверки электронной подписи в форме документа на бумажном носителе.

2.4.2. При необходимости выдачи Пользователю УЦ Сертификата ключа проверки электронной подписи в форме документа на бумажном носителе этот сертификат оформляется на бланке Удостоверяющего центра, заверяется подписью Уполномоченного лица УЦ, а также печатью Удостоверяющего центра (приложения № 8 и 9).

2.4.3. Для получения Сертификата ключа проверки электронной подписи в форме документа на бумажном носителе Пользователь УЦ:

2.4.3.1. Отправляет на электронный адрес ca.gpb@gazprombank.ru заявку в произвольной форме на выдачу Сертификата ключа проверки электронной подписи в форме документа на бумажном носителе. В заявке Пользователь УЦ указывает организацию, фамилию, имя и отчество Владельца сертификата ключа проверки электронной подписи, на чье имя необходимо получить сертификат, серийный номер сертификата и способ получения бланка Сертификата ключа проверки электронной подписи: лично в Удостоверяющем центре, у Менеджера Системы ЭДО или по почте. В последнем случае указывается точный почтовый адрес, куда необходимо выслать бланк Сертификата ключа проверки электронной подписи.

2.4.3.2. Лично прибывает в Удостоверяющий центр, согласовав время прибытия путем направления запроса на электронный адрес ca.gpb@gazprombank.ru, лично прибывает к Менеджеру Системы ЭДО, согласовав с ним время прибытия, либо получает бланк Сертификата ключа проверки электронной подписи, отправленный по почте.

2.5. **Прекращение действия Сертификата ключа проверки электронной подписи Пользователя УЦ**

2.5.1. Прекращение действия Сертификата ключа проверки электронной подписи Пользователя УЦ производится Удостоверяющим центром на основании «Заявления о прекращении действия сертификата ключа проверки электронной подписи» по форме приложений № 10 и 11.

2.5.2. Прекращение действия Сертификата ключа проверки электронной подписи должно быть осуществлено не позднее рабочего дня, следующего за рабочим днем, в течение которого «Заявление о прекращении действия сертификата ключа проверки электронной подписи» (приложения № 10 и 11) было зарегистрировано в Удостоверяющем центре.

2.5.3. Официальным уведомлением о факте прекращения действия Сертификата ключа проверки электронной подписи является опубликование Списка отозванных сертификатов, содержащего сведения о прекратившем действие Сертификате ключа проверки электронной подписи. Временем прекращения действия Сертификата ключа проверки электронной подписи признается время издания Списка отозванных сертификатов.

2.5.4. В случае отказа в прекращении действия Сертификата ключа проверки электронной подписи Удостоверяющий центр через Менеджера Системы ЭДО уведомляет об этом Пользователя УЦ.

2.5.5. Удостоверяющий центр может самостоятельно (без соответствующего Заявления о прекращении действия сертификата ключа проверки электронной подписи Пользователя УЦ) принять решение о прекращении действия Сертификата ключа проверки электронной подписи Пользователя УЦ в следующих случаях:

2.5.5.1. В случае прекращения действия настоящего Регламента.

2.5.5.2. При получении Удостоверяющим центром от Менеджера Системы ЭДО сведений о Компрометации Ключа ЭП Пользователя УЦ.

2.5.5.3. При получении Удостоверяющим центром от Менеджера Системы ЭДО сведений о ставших недействительными данных, содержащихся в Сертификате ключа проверки электронной подписи.

2.5.5.4. При Компрометации Ключа ЭП Уполномоченного лица УЦ.

2.5.6. В случае вынесения решения о прекращении действия Сертификата ключа проверки электронной подписи Удостоверяющий центр уведомляет Менеджера Системы ЭДО.

2.6. **Предоставление СКЗИ**

2.6.1. Удостоверяющий центр может предоставлять СКЗИ Пользователям УЦ, если это предусмотрено установленным организатором Системы ЭДО порядком ее использования.

2.6.2. Порядок передачи и использования СКЗИ регламентируется правилами работы в Системе ЭДО, установленными ее организатором и согласованными с Удостоверяющим центром.

2.6.3. При передаче СКЗИ должны соблюдаться права правообладателя.

2.6.4. Передаваемые СКЗИ подлежат поэкземплярному учету в соответствии с требованиями регуляторов.

2.6.5. Передача прав на СКЗИ осуществляется на основании заключаемого с Банком Соглашения об использовании Системы ЭДО, содержащего элементы сублицензионного договора.

2.6.6. По умолчанию, в рамках одного Соглашения об использовании Системы ЭДО передается одна лицензия на СКЗИ. В случаях, когда требуется большее количество лицензий на СКЗИ, их выдача осуществляется на основании официального письма с обоснованием необходимости.

3. Права и обязанности Сторон

3.1. **Удостоверяющий центр обязан:**

3.1.1. Информировать Пользователей УЦ об условиях и о порядке использования Электронных подписей и Средств электронной подписи, рисках, связанных с использованием

Электронных подписей, и мерах, необходимых для обеспечения безопасности Электронных подписей и их проверки. Информирование осуществляется путем размещения информации в настоящем Регламенте и его приложениях, изменениях к настоящему Регламенту, информационных рассылках, направляемых Пользователям УЦ через Системы ЭДО.

3.1.2. Обеспечивать актуальность информации, содержащейся в реестре Удостоверяющего центра, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.

3.1.3. Предоставлять информацию, содержащуюся в реестре Удостоверяющего центра, в том числе информацию о прекративших действие и аннулированных Сертификатах ключей проверки электронной подписи в установленном настоящим Регламентом порядке.

3.1.4. Обеспечивать конфиденциальность созданных Удостоверяющим центром Ключей электронных подписей. В том числе обеспечить защиту Ключа электронной подписи Уполномоченного лица УЦ от несанкционированного доступа.

3.1.5. Отказать заявителю в создании Сертификата ключа проверки электронной подписи в случае, если не было подтверждено то, что заявитель владеет Ключом электронной подписи, который соответствует Ключу проверки электронной подписи, указанному заявителем для получения Сертификата ключа проверки электронной подписи.

3.1.6. Отказать заявителю в создании Сертификата ключа проверки электронной подписи в случае отрицательного результата проверки в реестре сертификатов уникальности Ключа проверки электронной подписи, указанного заявителем для получения Сертификата ключа проверки электронной подписи.

3.1.7. Изготовить Сертификат ключа проверки электронной подписи Пользователя УЦ на основании Заявления об акцепте условий Регламента и изготовлении сертификата ключа проверки электронной подписи в соответствии с порядком, определенным в настоящем Регламенте.

3.1.8. Изготовить Технологический ключ и технологический Сертификат ключа проверки электронной подписи Пользователя УЦ на основании Заявления об акцепте условий Регламента и изготовлении технологического сертификата ключа проверки электронной подписи в соответствии с порядком, определенным в настоящем Регламенте.

3.1.9. Изготовить Тестовый ключ и тестовый Сертификат ключа проверки электронной подписи в соответствии с порядком, определенным в настоящем Регламенте.

3.1.10. Предоставить Пользователю УЦ Сертификат ключа проверки электронной подписи Уполномоченного лица УЦ в электронной форме.

3.1.11. Предоставить по запросу Пользователя УЦ заверенную подписью начальника УЦ и печатью УЦ копию Сертификата ключа проверки электронной подписи Уполномоченного лица УЦ в форме документа на бумажном носителе.

3.1.12. Обеспечить уникальность серийных номеров изготавливаемых Сертификатов ключей проверки электронной подписи.

3.1.13. Обеспечить уникальность значений Ключей проверки электронной подписи в изготовленных Сертификатах ключей проверки электронной подписи Пользователей УЦ.

3.1.14. Внести в реестр УЦ информацию о прекращении действия Сертификата ключа проверки электронной подписи Пользователя УЦ по соответствующему заявлению о прекращении действия Сертификата ключа проверки электронной подписи в соответствии с порядком, определенным в настоящем Регламенте, или аннулировать Сертификат ключа проверки электронной подписи путем внесения записи о его аннулировании в реестр сертификатов по решению суда, вступившему в законную силу.

3.1.15. Внести в реестр УЦ запись о прекращении действия Сертификата ключа проверки электронной подписи Пользователя УЦ в случае Компрометации Ключа ЭП Уполномоченного лица УЦ, с использованием которого был издан Сертификат ключа проверки электронной подписи.

3.1.16. Организовать свою работу по московскому времени. Удостоверяющий центр обязан синхронизировать по времени все свои программные и технические средства

обеспечения деятельности.

3.2. **Пользователь УЦ обязан:**

3.2.1. Хранить в тайне Ключ электронной подписи, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования.

3.2.2. Соблюдать требования по обеспечению безопасности при работе со Средствами криптографической защиты информации, приведенные в приложении № 12.

3.2.3. При формировании Запросов на изготовление сертификатов ключей проверки электронной подписи и Заявлений об акцепте условий Регламента и изготовлении сертификата ключа проверки электронной подписи руководствоваться правилами, приведенными в приложении № 6.

3.2.4. Передавать в Банк Запрос на изготовление сертификата ключа проверки электронной подписи и Заявление об акцепте условий Регламента и изготовлении сертификата ключа проверки электронной подписи не позднее двух месяцев с момента формирования соответствующего Ключа электронной подписи.

3.2.5. Применять для формирования Электронной подписи только действующий Ключ электронной подписи.

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

3.2.7. Немедленно обратиться в Удостоверяющий центр с заявлением о прекращении действия Сертификата ключа проверки электронной подписи в случае потери, раскрытия, искажения Ключа электронной подписи, а также в случае, если Пользователю УЦ стало известно, что этот ключ несанкционированно используется или использовался ранее другими лицами.

3.2.8. Не использовать Ключ электронной подписи, связанный с Сертификатом ключа проверки электронной подписи, который внесен в реестр УЦ как прекративший свое действие (в том числе аннулирован по решению суда).

3.2.9. Не использовать Ключ электронной подписи до получения от Удостоверяющего центра Сертификата ключа проверки электронной подписи, соответствующего данному Ключу электронной подписи.

3.2.10. Самостоятельно контролировать сроки действия своих ключей и своевременно инициировать процедуру их плановой смены в соответствии с пунктом 6.5.

3.2.11. Письменно известить Менеджера Системы ЭДО об изменениях в карточке с образцами подписей и оттиска печати, местонахождения, правового статуса, телефонов, внесения изменений и дополнений в учредительные документы, иных сведений, содержащихся в Сертификате ключа проверки электронной подписи, в течение трех рабочих дней. До поступления сообщения об указанных изменениях все действия, совершенные по ранее указанным Пользователем УЦ реквизитам, считаются совершенными законно и засчитываются как выполнение Сторонами своих обязательств.

3.2.12. По требованию Удостоверяющего центра предоставить документы, приведенные в подпункте 3.3.1, в течение трех рабочих дней.

3.2.13. Не вывозить предоставленные Удостоверяющим центром СКЗИ за пределы таможенной границы Таможенного союза. Ввоз СКЗИ на территорию стран-участников Таможенного союза осуществляется при условии соблюдения национального законодательства.

3.2.14. Не использовать Ключи электронной подписи за пределами таможенной границы Российской Федерации, если иное не оговорено в Соглашении об использовании Системы ЭДО.

3.3. **Удостоверяющий центр имеет право:**

3.3.1. Запросить у Стороны, заключившей Договор, документы, подтверждающие следующую информацию:

3.3.1.1. В случае если Пользователь УЦ является Полномочным представителем юридического лица, заключившего Договор:

3.3.1.1.1. Полное фирменное наименование юридического лица и ОГРН.

3.3.1.1.2. ИНН или КИО.

3.3.1.1.3. Нотариально заверенную копию устава юридического лица.

3.3.1.1.4. Нотариально заверенную копию свидетельства ФНС России о государственной регистрации.

3.3.1.1.5. Копии протоколов либо иных документов о назначении руководителя юридического лица (в соответствии с учредительными документами).

3.3.1.1.6. Сведения, необходимые для идентификации руководителя юридического лица: фамилия, имя, отчество, номер паспорта, дата и кем выдан, место регистрации.

3.3.1.1.7. Доверенность.

3.3.1.2. В случае если Пользователь УЦ является физическим лицом:

3.3.1.2.1. Сведения, необходимые для его идентификации: фамилия, имя, отчество, номер паспорта, дата выдачи, орган, выдавший документ, место регистрации.

3.3.1.2.2. СНИЛС.

3.3.1.2.3. ИНН.

3.3.2. Отказать в изготовлении Сертификата ключа проверки электронной подписи Пользователя УЦ в случае ненадлежащего оформления Запроса на изготовление сертификата ключа проверки электронной подписи или Заявления об акцепте условий Регламента и изготовлении сертификата ключа проверки электронной подписи.

3.3.3. Отказать в занесении информации о прекращении действия Сертификата ключа проверки электронной подписи Пользователя УЦ в случае ненадлежащего оформления соответствующего заявления.

3.3.4. Отказать в занесении информации о прекращении действия Сертификата ключа проверки электронной подписи Пользователя УЦ в случае, если срок действия данного сертификата истек.

3.3.5. В одностороннем порядке внести в реестр сертификатов Удостоверяющего центра информацию о прекращении действия Сертификата ключа проверки электронной подписи Пользователя УЦ с обязательным уведомлением Владельца сертификата ключа проверки электронной подписи через Менеджера Системы ЭДО и указанием причин.

3.4. **Пользователь УЦ имеет право:**

3.4.1. Обращаться в Удостоверяющий центр с Заявлением об акцепте условий Регламента и изготовлении сертификата ключа проверки электронной подписи.

3.4.2. Обратиться в Удостоверяющий центр с Заявлением об акцепте условий Регламента и изготовлении технологического Сертификата ключа проверки электронной подписи.

3.4.3. Обратиться в Удостоверяющий центр за получением Тестовых ключей и тестовых Сертификатов ключей проверки электронной подписи.

3.4.4. Обратиться в Удостоверяющий центр с «Заявлением о прекращении действия сертификата ключа проверки электронной подписи» (приложения № 10 и 11), владельцем которого он является, в течение срока действия данного сертификата.

3.4.5. Обратиться в Удостоверяющий центр за получением информации о статусе своих Сертификатов ключей проверки электронной подписи и их действительности на определенный момент.

3.4.6. Обратиться в Удостоверяющий центр за Подтверждением подлинности ЭП в электронном документе, сформированной с использованием Ключа электронной подписи, связанного с Сертификатом ключа проверки электронной подписи, изданного Удостоверяющим центром.

3.4.7. Получить Сертификат ключа проверки электронной подписи Уполномоченного лица УЦ в электронном виде или в форме документа на бумажном носителе.

3.4.8. Получить Список отозванных сертификатов в электронном виде, изготовленный и подписанный Уполномоченным лицом УЦ.

3.4.9. Применять Сертификат ключа проверки электронной подписи Пользователя УЦ

для проверки Электронной подписи Электронных документов в соответствии со сведениями, указанными в Сертификате ключа проверки электронной подписи.

3.4.10. Применять Сертификат ключа проверки электронной подписи Уполномоченного лица УЦ для проверки Электронной подписи Уполномоченного лица УЦ в Сертификатах ключей проверки электронной подписи, изготовленных Удостоверяющим центром.

3.4.11. Для хранения Ключа электронной подписи применять носитель, поддерживаемый Средством электронной подписи и программным обеспечением Системы ЭДО.

4. Ответственность Сторон

4.1. За невыполнение или ненадлежащее выполнение обязательств по настоящему Регламенту Стороны несут имущественную ответственность в пределах суммы доказанного реального ущерба, причиненного Стороне невыполнением или ненадлежащим выполнением обязательств другой Стороной. Ни одна из Сторон не отвечает за неполученные доходы (упущенную выгоду), которые бы получила другая Сторона.

4.2. Банк не несет ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случае, если Удостоверяющий центр обоснованно полагался на сведения, указанные в заявлениях Пользователя УЦ.

4.3. Банк не несет ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случае в случае потери, раскрытия, искажения Пользователем УЦ Ключа электронной подписи, несанкционированного использования Пользователем УЦ Ключа электронной подписи и/или нарушения конфиденциальности Ключа электронной подписи; использования Ключа электронной подписи соответствующего аннулированному Сертификату ключа проверки электронной подписи; несвоевременной плановой/внеплановой смены Ключа электронной подписи; несоблюдения требований по обеспечению безопасности при работе со Средствами криптографической защиты информации.

4.4. Ответственность Сторон, не урегулированная положениями настоящего Регламента, регулируется в соответствии с законодательством Российской Федерации.

5. Состав Сертификатов ключей проверки электронной подписи и Списков отозванных сертификатов

5.1. Сертификат ключа проверки электронной подписи содержит следующую информацию:

5.1.1. Наименование Удостоверяющего центра, который выдал Сертификат ключа проверки электронной подписи (поле Issuer).

5.1.2. Даты начала и окончания срока его действия (поле Validity Period).

5.1.3. Фамилия, имя и отчество Владельца сертификата ключа проверки электронной подписи (поле Subject).

5.1.4. Уникальный серийный номер сертификата (поле Serial Number).

5.1.5. Ключ проверки электронной подписи (поле Public Key).

5.1.6. Наименование используемого Средства электронной подписи и/или стандарты, которым соответствуют Ключ электронной подписи и Ключ проверки электронной подписи (поле Signature Algorithm).

5.1.7. Электронная подпись Уполномоченного лица УЦ (поле Issuer Sign).

5.1.8. Иная информация (по решению Удостоверяющего центра).

5.2. Список отозванных сертификатов (CRL) Удостоверяющего центра содержит следующую информацию:

5.2.1. Наименование Удостоверяющего центра, издавшего Список отозванных сертификатов (поле Issuer).

5.2.2. Дата и время издания Списка отозванных сертификатов (поле thisUpdate).

5.2.3. Дата и время, по которое действителен Список отозванных сертификатов (поле nextUpdate).

5.2.4. Список отозванных сертификатов Ключей проверки электронной подписи (поле revokedCertificates).

5.2.5. Наименование используемого Средства электронной подписи и/или стандарты, которым соответствуют Ключ электронной подписи и Ключ проверки электронной подписи (поле Signature Algorithm).

5.2.6. Электронная подпись Уполномоченного лица УЦ (поле Issuer Sign).

5.2.7. Иная информация (по решению Удостоверяющего центра).

6. Сроки действия ключей и порядок их смены

6.1. **Сроки действия ключей Пользователей УЦ**

6.1.1. Срок действия Ключа электронной подписи Пользователя УЦ составляет один год и три месяца, при этом ограничивается периодом действия соответствующего Сертификата ключа проверки электронной подписи.

6.1.2. Срок действия Сертификата ключа проверки электронной подписи Пользователя УЦ (рабочий Сертификат ключа проверки электронной подписи) составляет один год.

6.2. **Сроки действия Технологических ключей Пользователей УЦ**

6.2.1. Срок действия Технологического ключа Пользователя УЦ ограничивается периодом действия соответствующего технологического Сертификата ключа проверки электронной подписи.

6.2.2. Срок действия технологического Сертификата ключа проверки электронной подписи Пользователя УЦ составляет два месяца.

6.3. **Сроки действия Тестовых ключей Пользователей УЦ**

6.3.1. Срок действия Тестового ключа Пользователя УЦ ограничивается периодом действия соответствующего тестового Сертификата ключа проверки электронной подписи.

6.3.2. Срок действия тестового Сертификата ключа проверки электронной подписи Пользователя УЦ составляет два месяца.

6.4. **Сроки действия ключей Уполномоченного лица УЦ**

6.4.1. Срок действия Ключа электронной подписи Уполномоченного лица УЦ составляет три года.

6.4.2. Для формирования Сертификатов ключей проверки электронной подписи Пользователей УЦ Ключ электронной подписи Уполномоченного лица УЦ применяется в течение одного года и трех месяцев, в остальное время данный ключ используется исключительно для формирования Списка отозванных сертификатов. Начало периода действия Ключа электронной подписи Уполномоченного лица УЦ исчисляется с даты и времени его формирования.

6.4.3. Срок действия Сертификата ключа проверки ЭП Уполномоченного лица составляет десять лет.

6.4.4. Для формирования Сертификатов ключей проверки электронной подписи Пользователей УЦ через один год и три месяца формируется новый Ключ электронной подписи Уполномоченного лица УЦ.

6.4.5. При создании и хранении Ключа электронной подписи Уполномоченного лица УЦ посредством ПАКМ «КриптоПро HSM» срок его действия составляет пять лет. Для формирования Сертификатов ключей проверки электронной подписи Пользователей УЦ Ключ электронной подписи Уполномоченного лица УЦ применяется в течение трех лет, в остальное время данный ключ используется исключительно для формирования Списка отозванных сертификатов. Срок действия Сертификата ключа проверки электронной подписи Уполномоченного лица УЦ составляет двадцать лет. Для формирования Сертификатов ключей проверки электронной подписи Пользователей УЦ через три года формируется новый Ключ электронной подписи Уполномоченного лица УЦ.

6.5. **Плановая смена ключей Пользователя УЦ**

6.5.1. Плановую смену ключей Пользователя УЦ рекомендуется проводить не ранее двух месяцев и не позднее одного месяца до окончания срока действия Сертификата ключа проверки электронной подписи Пользователя УЦ. При этом Пользователь УЦ обязан самостоятельно контролировать сроки действия своих ключей и Сертификатов ключей проверки электронной подписи, и своевременно инициировать их плановую смену.

6.5.2. Порядок проведения плановой смены ключей Пользователя УЦ аналогичен порядку изготовления ключей Пользователя УЦ, приведенному в подразделе 2.1.

6.5.3. Допускается изготовление нового Сертификата ключа проверки электронной подписи Пользователя УЦ на основании электронного Запроса на изготовление Сертификата ключа проверки электронной подписи, подписанного действующим Ключом электронной подписи Пользователя УЦ. Для этого необходимо соблюдение следующих условий:

- Соглашение об использовании Системы ЭДО должно содержать согласие Сторон на изготовление нового Сертификата ключа проверки электронной подписи Пользователя УЦ без оформления Заявления об акцепте условий Регламента и изготовлении сертификата ключа проверки электронной подписи, на основании электронного Запроса на изготовление сертификата ключа проверки электронной подписи, подписанного действующим Ключом электронной подписи Пользователя УЦ;
- Запрос на изготовление сертификата ключа проверки электронной подписи должен быть указан в перечне Электронных документов, которые допускается передавать в Системе ЭДО. Данный перечень должен являться неотъемлемой частью Соглашения об использовании Системы ЭДО;
- поля Запроса на изготовление сертификата ключа проверки электронной подписи совпадают с полями ранее оформленного и переданного Пользователем УЦ в Банк Заявления об акцепте условий Регламента и изготовлении сертификата ключа проверки электронной подписи, за исключением поля, содержащего Ключ проверки электронной подписи. В противном случае (несовпадение одного или нескольких полей), оформляется новое Заявление об акцепте условий Регламента и изготовлении сертификата ключа проверки электронной подписи с указанием актуальных данных;
- на момент получения Удостоверяющим центром Запроса на изготовление нового сертификата ключа проверки электронной подписи не истек срок действия Сертификата ключа проверки электронной подписи, соответствующего действующему Ключу электронной подписи Пользователя УЦ, которым подписан данный запрос;
- на момент отправки в Банк Запроса на изготовление нового сертификата ключа проверки электронной подписи, действующий Ключ электронной подписи Пользователя УЦ, которым подписан данный запрос, не скомпрометирован.

6.5.4. В случае отказа в изготовлении нового Сертификата ключа проверки электронной подписи Пользователь УЦ уведомляется об этом, с указанием причины отказа.

6.6. **Плановая смена ключей Уполномоченного лица УЦ**

6.6.1. Плановая смена ключей Уполномоченного лица УЦ (Ключа электронной подписи и соответствующего ему Ключа проверки электронной подписи) выполняется в период действия Ключа электронной подписи Уполномоченного лица УЦ.

6.6.2. Процедура плановой смены ключей Уполномоченного лица УЦ осуществляется в следующем порядке:

6.6.2.1. Уполномоченное лицо УЦ генерирует новый Ключ электронной подписи и соответствующий ему Ключ проверки электронной подписи.

6.6.2.2. Уполномоченное лицо УЦ изготавливает новый Сертификат ключа проверки электронной подписи Уполномоченного лица УЦ.

6.6.2.3. Удостоверяющий центр оповещает Пользователей УЦ о проведении смены ключей Уполномоченного лица УЦ через Менеджеров Систем ЭДО и/или путем распространения нового Сертификата ключа проверки электронной подписи Уполномоченного лица УЦ средствами Систем ЭДО. Сертификат ключа проверки электронной подписи

Уполномоченного лица УЦ публикуется на сайте cs.gazprombank.ru. Старый Ключ электронной подписи Уполномоченного лица УЦ используется в течение своего срока действия для формирования Списков отозванных сертификатов, изданных Удостоверяющим центром в период действия старого Ключа электронной подписи Уполномоченного лица УЦ.

6.7. **Внеплановая смена ключей**

6.7.1. Внеплановая смена ключей осуществляется в следующих случаях:

6.7.1.1. При Компрометации Ключа ЭП Пользователя УЦ.

6.7.1.2. При Компрометации Ключа ЭП Уполномоченного лица УЦ.

6.7.1.3. В случае если Пользователь УЦ по каким-либо причинам не смог осуществить плановую смену ключей в установленные для этой процедуры сроки.

6.7.1.4. Изменения регистрационных данных Пользователя УЦ.

6.7.1.5. В иных случаях, вызванных форс-мажорными обстоятельствами.

6.7.2. Порядок проведения внеплановой смены ключей Пользователя УЦ аналогичен порядку изготовления ключей Пользователя УЦ, приведенному в подразделе 2.1.

7. Компрометация Ключей электронной подписи

7.1. **Компрометация Ключа ЭП Пользователя УЦ**

7.1.1. Пользователь УЦ самостоятельно принимает решение о факте или угрозе Компрометации принадлежащего ему Ключа ЭП.

7.1.2. В случае Компрометации или угрозы Компрометации Ключа ЭП Пользователь УЦ направляет в Удостоверяющий центр «Заявление на прекращение действия сертификата ключа проверки электронной подписи» (приложения № 10 и 11), соответствующего скомпрометированному Ключу ЭП, после чего Пользователь УЦ осуществляет внеплановую смену ключей в соответствии с подразделом 6.7.

7.2. **Компрометация Ключа ЭП Уполномоченного лица УЦ**

7.2.1. В случае Компрометации Ключа ЭП Уполномоченного лица УЦ Сертификат ключа проверки электронной подписи Уполномоченного лица УЦ прекращает свое действие. Удостоверяющий центр оповещает Пользователей УЦ о факте Компрометации Ключа ЭП через Менеджеров Систем ЭДО и/или с использованием средств Систем ЭДО.

7.2.2. Все Сертификаты ключей проверки электронной подписи, подписанные с использованием скомпрометированного Ключа ЭП Уполномоченного лица УЦ, считаются прекратившими свое действие.

7.2.3. При Компрометации Ключа ЭП Уполномоченного лица УЦ временем прекращения действия Сертификата ключа проверки электронной подписи Пользователя УЦ признается время Компрометации Ключа ЭП Уполномоченного лица УЦ, фиксирующееся в реестре Удостоверяющего центра. В случае Компрометации Ключа ЭП Уполномоченного лица УЦ информация о Сертификате ключа проверки электронной подписи Пользователя УЦ в Список отозванных сертификатов не заносится.

7.2.4. После прекращения действия Сертификата ключа проверки электронной подписи Уполномоченного лица УЦ выполняется процедура внеплановой смены Ключа электронной подписи Уполномоченного лица УЦ. Данная процедура аналогична процедуре плановой смены ключей Уполномоченного лица УЦ (подраздел 6.6).

7.2.5. Все действовавшие на момент Компрометации Ключа ЭП подписи Уполномоченного лица УЦ Сертификаты ключей проверки электронных подписей подлежат внеплановой смене.

8. Конфиденциальность информации

8.1. Ключ электронной подписи, соответствующий Сертификату ключа проверки электронной подписи, является конфиденциальной информацией лица, зарегистрированного в Удостоверяющем центре. Удостоверяющий центр не осуществляет хранение Ключей электронной подписи Пользователей УЦ.

8.2. Персональная и корпоративная информация о лицах, зарегистрированных в

Удостоверяющем центре, содержащаяся в реестре Удостоверяющего центра, не подлежащая непосредственной рассылке в качестве части Сертификата ключа проверки электронной подписи, считается конфиденциальной.

8.3. Информация, не являющаяся конфиденциальной информацией, считается открытой информацией.

8.4. Открытая информация может публиковаться по решению Удостоверяющего центра. Место, способ и время публикации открытой информации определяется Удостоверяющим центром.

8.5. Информация, включаемая в Сертификаты ключей проверки электронной подписи и Списки отозванных сертификатов, издаваемые Удостоверяющим центром, не являются конфиденциальными.

8.6. Информация, содержащаяся в настоящем Регламенте, не является конфиденциальной.

8.7. Удостоверяющий центр имеет право раскрывать конфиденциальную информацию третьим лицам только в случаях, установленных законодательством Российской Федерации.

9. Разрешение споров

9.1. Сторонами в споре (в случае его возникновения) считаются:

9.1.1. Банк и Пользователь УЦ для Систем ЭДО, организатором которых является Банк и в которых обмен Электронными документами осуществляется между Пользователем УЦ и Банком.

9.1.2. Пользователи УЦ, осуществляющие обмен Электронными документами между собой.

9.2. При возникновении споров Стороны предпринимают все необходимые шаги для урегулирования спорных вопросов, которые могут возникнуть в рамках настоящего Регламента, путем переговоров.

9.3. Сторона, получившая от другой Стороны претензию, обязана в течение двадцати календарных дней удовлетворить заявленные в претензии требования или направить другой Стороне мотивированный отказ с указанием оснований отказа. К ответу должны быть приложены все необходимые документы.

9.4. По желанию Стороны Удостоверяющий центр может привлекаться при разрешении споров для проведения процедуры технической экспертизы, заключающейся в Подтверждении подлинности ЭП в электронных документах в отношении выданных им Сертификатов ключей проверки электронной подписи, а также подтверждении подлинности Электронной подписи Уполномоченного лица УЦ в изданных им Сертификатах ключей проверки электронной подписи. Процедура проведения технической экспертизы при разрешении споров описана в приложении № 13.

9.5. Стороны будут принимать все необходимые меры к тому, чтобы в случае возникновения спорных вопросов решить их, прежде всего, в претензионном порядке.

9.6. Спорные вопросы между Сторонами, не урегулированные в претензионном порядке, решаются в Арбитражном суде города Москвы.

10. Форс-мажор

10.1. Стороны освобождаются от ответственности за полное или частичное неисполнение своих обязательств по настоящему Регламенту, если это неисполнение явилось следствием форс-мажорных обстоятельств, возникших после заключения Договора.

10.2. Форс-мажорными обстоятельствами признаются чрезвычайные (т.е. находящиеся вне разумного контроля Сторон) и не предотвратимые при указанных условиях обстоятельства, включая военные действия, массовые беспорядки, стихийные бедствия, забастовки, технические сбои функционирования аппаратно-программного обеспечения, пожары, взрывы и иные техногенные катастрофы, действия (бездействие) государственных и муниципальных органов, повлекшие невозможность исполнения Стороной/Сторонами своих обязательств по

настоящему Регламенту.

10.3. В случае возникновения форс-мажорных обстоятельств срок исполнения Сторонами своих обязательств по настоящему Регламенту отодвигается соразмерно периоду, в течение которого действуют такие обстоятельства.

10.4. Сторона, для которой создалась невозможность исполнения своих обязательств по настоящему Регламенту, должна немедленно известить в письменной форме другую Сторону о наступлении, предполагаемом сроке действия и прекращении форс-мажорных обстоятельств, а также представить доказательства существования названных обстоятельств.

10.5. Неизвещение или несвоевременное извещение о наступлении обстоятельств непреодолимой силы влечет за собой утрату права ссылаться на эти обстоятельства, в форме документа, выданного торгово-промышленной палатой, либо документа уполномоченного органа государственной власти соответствующего региона, в подтверждение наступления указанных обстоятельств и их влияния на исполнение настоящего Договора.

10.6. При невозможности полного или частичного исполнения Сторонами какого-либо обязательства по настоящему Регламенту, обусловленной действием форс-мажорных обстоятельств и существующей свыше одного месяца, каждая из Сторон вправе отказаться в одностороннем порядке от дальнейшего исполнения этого обязательства. В этом случае ни одна из Сторон не вправе требовать возмещения возникших у нее убытков другой Стороной.

11. Внесение изменений в настоящий Регламент

11.1. Внесение изменений (дополнений) в настоящий Регламент, включая приложения к нему, производится Банком в одностороннем порядке.

11.2. Новая редакция Регламента публикуется на официальном сайте Банка.

11.3. Уведомление о внесении изменений (дополнений) в настоящий Регламент осуществляется Удостоверяющим центром путем рассылки Пользователям УЦ электронных сообщений через Менеджеров Систем ЭДО. Рассылка производится в день размещения информации на официальном сайте Банка.

11.4. Все изменения (дополнения), вносимые в настоящий Регламент в установленном порядке по инициативе Удостоверяющего центра и не связанные с изменением действующего законодательства Российской Федерации, вступают в силу и становятся обязательными по истечении одного месяца с даты публикации новой редакции Регламента на официальном сайте Банка.

11.5. Все изменения (дополнения), вносимые в настоящий Регламент в установленном порядке в связи с изменением действующего законодательства Российской Федерации, вступают в силу одновременно с вступлением в силу изменений (дополнений) указанных в соответствующих нормативно-правовых актах.

11.6. Любые изменения (дополнения), вносимые в настоящий Регламент, с даты их вступления в силу равно распространяются на всех лиц, заключивших Договор, в том числе заключивших Договор ранее даты вступления изменений (дополнений) в силу. В случае несогласия с изменениями (дополнениями) Сторона, заключившая Договор, имеет право до вступления в силу таких изменений (дополнений) на расторжение Договора в порядке, предусмотренном пунктом 1.13.

12. Заключительные положения

С даты публикации настоящего Регламента признается утратившим силу «Регламент удостоверяющего центра ГПБ (ОАО)» от 21.03.2012 № И/9.

Приложение № 1

к «Регламенту удостоверяющего центра Банка ГПБ (АО)» от 09.06.2018 № И/47.

Перечень терминов и условных сокращений

Администратор безопасности – лицо, ответственное за осуществление комплекса организационно-технических мер, направленных на обеспечение безопасности и отвечающее за:

- контроль целостности программного обеспечения;
- управление ключевой системой (генерация Ключей электронной подписи и Ключей проверки электронной подписи, хранение, ввод в действие и смена ключей);
- управление доступом к программному обеспечению и данным, включая установку и периодическую смену паролей, управление средствами защиты коммуникаций, передаваемых, хранимых и обрабатываемых данных.

Банк – «Газпромбанк» (Акционерное общество), Банк ГПБ (АО)**.**

Владелец сертификата ключа проверки электронной подписи – лицо, которому в установленном законодательством Российской Федерации порядке выдан Сертификат ключа проверки электронной подписи.

Договор – договор об оказании услуг Удостоверяющего центра Банка.

Запрос на изготовление сертификата ключа проверки электронной подписи – электронный документ в формате PKCS#10.

Заявление об акцепте условий Регламента и изготовлении сертификата ключа проверки электронной подписи по форме – заявление об акцепте условий «Регламента удостоверяющего центра Банка ГПБ (АО)» и изготовлении сертификата ключа проверки электронной подписи.

Заявление об акцепте условий Регламента и изготовлении технологического сертификата ключа проверки электронной подписи по форме приложения – заявление об акцепте условий «Регламента удостоверяющего центра Банка ГПБ (АО)» и изготовлении технологического сертификата ключа проверки электронной подписи.

ИНН – идентификационный номер налогоплательщика.

КИО – код иностранной организации.

Ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с Ключом электронной подписи и предназначенная для проверки подлинности Электронной подписи (далее – проверка электронной подписи).

Ключ электронной подписи (Ключ ЭП) – уникальная последовательность символов, предназначенная для создания Электронной подписи.

Компрометация Ключа ЭП – утрата доверия к тому, что используемые Ключи электронной подписи недоступны посторонним лицам. К событиям, связанным с Компрометацией Ключей электронной подписи, в том числе, относятся:

- утрата носителей ключевой информации;
- увольнение работников, имевших доступ к ключевой информации;
- временный доступ посторонних лиц к ключевой информации;
- иные обстоятельства, прямо или косвенно свидетельствующие о наличии возможности несанкционированного доступа к Ключу электронной подписи третьих или неуполномоченных лиц.

Менеджер Системы ЭДО – ответственный работник Банка (филиала Банка), являющегося организатором Системы ЭДО, уполномоченный осуществлять взаимодействие с Пользователями УЦ в рамках Системы ЭДО. Менеджер системы ЭДО назначается

организационно-распорядительным документом по Банку (филиалу Банка, дочернему или зависимому обществу Банка).

ОГРН – основной государственный регистрационный номер.

ПАКМ «КриптоПро HSM» – программно-аппаратный криптографический модуль, предназначенный для генерации и защищенного хранения ключевой информации, а также для создания и проверки электронной подписи.

Подтверждение подлинности ЭП в электронном документе – положительный результат проверки соответствующим Средством электронной подписи с использованием Сертификата ключа проверки электронной подписи, принадлежности Электронной подписи в Электронном документе Владельцу сертификата ключа проверки электронной подписи и отсутствия искажений в подписанном данной Электронной подписью Электронном документе.

Полномочный представитель юридического лица – физическое лицо, зарегистрированное в удостоверяющем центре, представляющее Сторону, заключившую с Банком договор об оказании услуг Удостоверяющего центра.

Пользователи удостоверяющего центра (Пользователи УЦ) – Полномочные представители юридических лиц, заключивших с Банком договор об оказании услуг Удостоверяющего центра и зарегистрированные в Удостоверяющем центре или физические лица, заключившие с Банком договор об оказании услуг Удостоверяющего центра и зарегистрированные в Удостоверяющем центре.

Рабочий ключ ЭП – Ключ электронной подписи Пользователя УЦ, изготавливаемый Пользователем УЦ самостоятельно и предназначенный для подписи Электронных документов в рамках Системы электронного документооборота**.**

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.

Система электронного документооборота (Система ЭДО) – организационно-техническая система, представляющая собой совокупность программного, информационного и аппаратного обеспечения, реализующая обмен Электронными документами.

СНИЛС – страховой номер индивидуального лицевого счета.

Соглашение об использовании Системы ЭДО – соглашение, заключаемое между Банком и физическим или юридическим лицом – участником электронного документооборота.

Список отозванных сертификатов (CRL) – Электронный документ с Электронной подписью Уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров Сертификатов ключей проверки электронной подписи, которые на определенный момент были аннулированы или прекратили свое действие, за исключением случаев, когда установленный срок действия Сертификата ключа проверки электронной подписи истек.

Средства криптографической защиты информации (СКЗИ) – программные средства, реализующие алгоритмы криптографического преобразования информации и предназначенные для обеспечения ее конфиденциальности и (или) целостности.

Средства удостоверяющего центра – программные и (или) аппаратные средства, используемые для реализации функций Удостоверяющего центра.

Средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание Электронной подписи, проверка Электронной подписи, создание Ключа электронной подписи и Ключа проверки электронной подписи.

Сторона (Стороны) – Банк и/или юридическое или физическое лицо, заключившее с Банком Договор.

Таможенный союз – объединение нескольких государств-участников, которые проводят совместные мероприятия в сфере таможенной политики.

Тестовый ключ – ключ, изготавливаемый Удостоверяющим центром и

предназначенный для тестирования Систем ЭДО, не находящихся в промышленной эксплуатации.

Технологический ключ – ключ Пользователя УЦ, изготавливаемый Удостоверяющим центром и предназначенный для технологической процедуры формирования Запроса на получение сертификата ключа проверки электронной подписи для самостоятельного формирования Рабочего ключа ЭП Пользователем УЦ.

Удостоверяющий центр (УЦ) – подразделение Банка, осуществляющее функции по созданию и выдаче Сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные законодательством Российской Федерации.

Уполномоченное лицо Удостоверяющего центра (Уполномоченное лицо УЦ) – работник Банка, наделенный полномочиями по заверению электронной подписью сертификатов ключей проверки электронных подписей и списков отозванных сертификатов, а также своей личной подписью бланков сертификатов ключей проверки электронной подписи.

ФНС России – Федеральная налоговая служба Российской Федерации.

ФСБ России – Федеральная служба безопасности Российской Федерации.

ФСТЭК России – Федеральная служба по техническому и экспортному контролю.

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. В рамках настоящего Регламента под Электронной подписью понимается усиленная неквалифицированная Электронная подпись.

Электронный документ (документ в электронном виде) – документ, информация в котором представлена в электронно-цифровой форме, созданный с использованием носителей и способов записи, обеспечивающих его обработку техническими и программными средствами Системы ЭДО.

Public Key Cryptography Standarts (PKCS) – стандарты криптографии с открытым ключом, разработанные компанией RSA Security. Удостоверяющий центр осуществляет свою работу в соответствии со следующими стандартами PKCS:

- PKCS#7 – стандарт, определяющий формат и синтаксис криптографических сообщений. Удостоверяющий центр использует описанный в PKCS#7 тип данных PKCS#7 Signed – подписанные данные,
- PKCS#10 – стандарт, определяющий формат и синтаксис Запроса на изготовление сертификата ключа проверки электронной подписи.

Приложение № 2

к «Регламенту удостоверяющего центра Банка ГПБ (АО)» от 09.06.2018 № И/47.

ЗАЯВЛЕНИЕ
об акцепте условий «Регламента удостоверяющего центра Банка ГПБ (АО)» и изготовлении Сертификата ключа проверки электронной подписи
(форма для юридических лиц)

1. Настоящим заявляю о своем присоединении (акцепте условий) к «Регламенту удостоверяющего центра Банка ГПБ (АО)» (далее – Регламент) в порядке, предусмотренном ст. 428 Гражданского кодекса Российской Федерации, принимаю на себя обязательства соблюдать положения Регламента.

2. Прошу изготовить Сертификат ключа проверки электронной подписи в соответствии со следующими идентификационными данными:

Индивидуальный номер налогоплательщика (ИНН): [_____]
Основной государственный регистрационный номер (ОГРН): [_____]
Название организации: [_____]
Подразделение: [_____]
Должность: [_____]
Населенный пункт: [_____]
Субъект РФ/ Штат, Кантон и т.п.: [_____]
Страна: [_____]
Адрес электронной почты: [_____]
Фамилия, имя, отчество Владельца сертификата ключа проверки электронной подписи:
[_____]
Паспорт серия: [_____] **номер**: [_____] **выдан**: [_____
_____] **дата выдачи:**[_____]
Ключ проверки электронной подписи: [_____] [*технологический QR-код*]
Средство электронной подписи: СКЗИ «_____» версии _____.
Алгоритм подписи: ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.»
Срок действия сертификата: один год.

3. При изменении данных, указанных в настоящем заявлении, обязуюсь немедленно письменно проинформировать об этом Банк ГПБ (АО) и передать соответствующие документы.

Владелец сертификата ключа проверки электронной подписи _____ _____
(подпись) (Ф.И.О.)

Руководитель организации _____ _____
(подпись) (Ф.И.О.)

«___»_____ 20__г. М.П.

(заполняется Менеджером Системы ЭДО и Уполномоченным лицом удостоверяющего центра)

Отметка о получении Менеджером Системы ЭДО: ___ ч. ___ мин. «____» _____ 20___ г.

Личные данные о Владельце сертификата ключа проверки электронной подписи верны: _____
(Подпись и Ф.И.О. Менеджера Системы ЭДО)

Отметка о получении Уполномоченным лицом УЦ: ___ ч. ___ мин. «____» _____ 20___ г.

Ключ проверки электронной подписи проверен.
Сертификат проверки электронной подписи изготовлен. _____
(Подпись и Ф.И.О. Уполномоченного лица УЦ)

Приложение № 3

к «Регламенту удостоверяющего центра Банка ГПБ (АО)» от 09.06.2018 № И/47.

ЗАЯВЛЕНИЕ
об акцепте условий «Регламента удостоверяющего центра Банка ГПБ (АО)» и изготовлении Сертификата ключа проверки электронной подписи
(форма для физических лиц)

1. Настоящим заявляю о своем присоединении (акцепте условий) к «Регламенту удостоверяющего центра Банка ГПБ (АО)» (далее – Регламент) в порядке, предусмотренном ст. 428 Гражданского кодекса Российской Федерации, принимаю на себя обязательства соблюдать положения Регламента.

2. Прошу изготовить Сертификат ключа проверки электронной подписи в соответствии со следующими идентификационными данными:

Индивидуальный номер налогоплательщика (ИНН): [_____]

Населенный пункт: [_____]

Субъект РФ/ Штат, Кантон и т.п.: [_____]

Страна: [_____]

Адрес электронной почты: [_____]

Фамилия, имя, отчество Владельца сертификата ключа проверки электронной подписи:

[_____]

Паспорт серия: [_____] **номер**: [_____] **выдан**: [_____

_____] **дата выдачи:** [_____]

Ключ проверки электронной подписи: [_____] [*технологический QR-код*]

Средство электронной подписи: СКЗИ «_____» версии _____.

Алгоритм подписи: ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.»

Срок действия сертификата: один год.

3. При изменении данных, указанных в настоящем заявлении, обязуюсь немедленно письменно проинформировать об этом Банк ГПБ (АО) и передать соответствующие документы.

Владелец сертификата ключа проверки электронной подписи _____ _____
(подпись) (Ф.И.О.)

(заполняется Менеджером Системы ЭДО и Уполномоченным лицом удостоверяющего центра)

Отметка о получении Менеджером Системы ЭДО: ___ ч. ___ мин. «____» _____ 20___ г.

Личные данные о Владельце сертификата ключа проверки электронной подписи верны: _____
(Подпись и Ф.И.О. Менеджера Системы ЭДО)

Отметка о получении Уполномоченным лицом УЦ: ___ ч. ___ мин. «____» _____ 20___ г.

Ключ проверки электронной подписи проверен.
Сертификат проверки электронной подписи изготовлен. _____
(Подпись и Ф.И.О. Уполномоченного лица УЦ)

Приложение № 4

к «Регламенту удостоверяющего центра Банка ГПБ (АО)» от 09.06.2018 № И/47.

ЗАЯВЛЕНИЕ
об акцепте условий «Регламента удостоверяющего центра Банка ГПБ (АО)» и изготовлении технологического Сертификата ключа проверки электронной подписи
(форма для юридических лиц)

1. Настоящим заявляю о своем присоединении (акцепте условий) к «Регламенту удостоверяющего центра Банка ГПБ (АО)» (далее – Регламент) в порядке, предусмотренном ст. 428 Гражданского кодекса Российской Федерации, принимаю на себя обязательства соблюдать положения Регламента.
2. Прошу изготовить технологический Сертификат ключа проверки электронной подписи в соответствии со следующими идентификационными данными:

Индивидуальный номер налогоплательщика (ИНН): [_____]
Основной государственный регистрационный номер (ОГРН): [_____]
Название организации: [_____]
Подразделение: [_____]
Должность: [_____]
Населенный пункт: [_____]
Субъект РФ/ Штат, Кантон и т.п.: [_____]
Страна: [_____]
Адрес электронной почты: [_____]
Фамилия, имя, отчество Владельца сертификата ключа проверки электронной подписи:
[_____]
Паспорт серия: [_____] **номер**: [_____] **выдан**: [_____
_____] **дата выдачи:** [_____]
Средство электронной подписи: СКЗИ «_____» версии _____.
Алгоритм подписи: ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.»
Срок действия сертификата: два месяца.

Владелец сертификата ключа проверки электронной подписи _____ _____
(подпись) (Ф.И.О.)

Руководитель организации _____ _____
(подпись) (Ф.И.О.)

«___»_____ 20__г. М.П.

(заполняется Менеджером Системы ЭДО и Уполномоченным лицом удостоверяющего центра)

Отметка о получении Менеджером Системы ЭДО: ___ ч. ___ мин. «____» _____ 20___ г.

Личные данные о Владельце сертификата ключа проверки электронной подписи верны. _____
(Подпись и Ф.И.О. Менеджера Системы ЭДО)

Отметка о получении Уполномоченным лицом УЦ: ___ ч. ___ мин. «____» _____ 20___ г.

Технологические ключи и технологический Сертификат ключа проверки электронной подписи изготовлены. _____
(Подпись и Ф.И.О. Уполномоченного лица УЦ)

Приложение № 5

к «Регламенту удостоверяющего центра Банка ГПБ (АО)» от 09.06.2018 № И/47.

ЗАЯВЛЕНИЕ
об акцепте условий «Регламента удостоверяющего центра Банка ГПБ (АО)» и изготовлении технологического Сертификата ключа проверки электронной подписи
(форма для физических лиц)

1. Настоящим заявляю о своем присоединении (акцепте условий) к «Регламенту удостоверяющего центра Банка ГПБ (АО)» (далее – Регламент) в порядке, предусмотренном ст. 428 Гражданского кодекса Российской Федерации, принимаю на себя обязательства соблюдать положения Регламента.

2. Прошу изготовить технологический сертификат ключа проверки электронной подписи в соответствии со следующими идентификационными данными:

Индивидуальный номер налогоплательщика (ИНН): [_____]
Населенный пункт: [_____]
Субъект РФ/ Штат, Кантон и т.п.: [_____]
Страна: [_____]
Адрес электронной почты: [_____]
Фамилия, имя, отчество Владельца сертификата ключа проверки электронной подписи:
[_____]
Паспорт серия: [_____] **номер**: [_____] **выдан**: [_____
_____] **дата выдачи:** [_____]
Средство электронной подписи: СКЗИ «_____» версии _____.
Алгоритм подписи: ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.»
Срок действия сертификата: два месяца.

Владелец сертификата ключа проверки электронной подписи _____ _____
(подпись) (Ф.И.О.)

(заполняется Менеджером Системы ЭДО и Уполномоченным лицом удостоверяющего центра)

Отметка о получении Менеджером Системы ЭДО: ___ ч. ___ мин. «____» _____ 20___ г.

Личные данные о Владельце сертификата ключа проверки электронной подписи верны: _____
(Подпись и Ф.И.О. Менеджера Системы ЭДО)

Отметка о получении Уполномоченным лицом УЦ: ___ ч. ___ мин. «____» _____ 20___ г.

Технологические ключи и технологический Сертификат ключа проверки электронной подписи изготовлены: _____
(Подпись и Ф.И.О. Уполномоченного лица УЦ)

Приложение № 6

к «Регламенту удостоверяющего центра Банка ГПБ (АО)» от 09.06.2018 № И/47.

Правила заполнения Запросов на изготовление сертификатов ключей проверки электронной подписи и Заявлений об акцепте условий Регламента и изготовлении сертификатов ключей проверки электронной подписи

1. Общие положения.

1.1. Настоящие Правила определяют порядок формирования электронных Запросов на изготовление сертификатов ключей проверки электронной подписи и оформления Заявлений об акцепте условий Регламента и изготовлении сертификатов ключей проверки электронной подписи, направляемых в Удостоверяющий центр Банка.

1.2. В части настоящих Правил определены форматы заполнения основных атрибутов, содержащихся в запросе на сертификат: C, S, L, O, OU, T, CN, E (в соответствии со стандартом x.509), дополнительных атрибутов: ИНН, ОГРН.

1.3. Список атрибутов, подлежащих заполнению, может быть изменен правилами работы в Системе ЭДО, в которой будет использован Сертификат ключа проверки электронной подписи.

1.4. При нарушении данных правил в выдаче сертификата может быть отказано.

2. Правила заполнения полей электронных запросов.

2.1. **Общие для всех полей требования**

2.1.1. Каждое слово в поле должно быть отделено ровно одним пробелом.

2.1.2. Не разрешается использовать пробел в начале и в конце текста.

2.1.3. Необходимо использовать заглавные и строчные буквы так, как это продиктовано правилами русского языка.

2.1.4. Наименование атрибутов с использованием букв латинского алфавита допускается только в случаях, когда наименование атрибута на русском языке отсутствует.

2.1.5. При использовании символов, не перечисленных в пункте 2.11 настоящих Правил в выдаче Сертификата ключа проверки электронной подписи может быть отказано.

2.2. **Формат фамилии, имени, отчества Владельца сертификата ключа проверки электронной подписи**

2.2.1. Фамилия, имя, отчество Владельца сертификата ключа проверки электронной подписи записываются в атрибут «CN» субъекта Сертификата ключа проверки электронной подписи, атрибут является обязательным.

2.2.2. Длина текста – не более 64 символов.

2.2.3. Фамилия, имя, отчество должны быть указаны полностью; в соответствии с записью в общегражданском паспорте Владельца сертификата ключа проверки электронной подписи. Первое слово – фамилия, первая буква фамилии – прописная, остальные – строчные; второе слово - имя, первая буква имени – прописная, остальные – строчные; остальные слова (если есть) могут быть отнесены к Отчеству, в зависимости от контекста обработки.

2.3. **Формат адреса электронной почты Владельца сертификата ключа проверки электронной подписи**

2.3.1. Адрес электронной почты Владельца сертификата ключа проверки электронной подписи записывается в атрибут «E» субъекта Сертификата ключа проверки электронной подписи, атрибут не является обязательным.

2.3.2. Длина текста – не более 128 символов.

2.3.3. При заполнении адреса электронной почты необходимо руководствоваться правилами, определенными в стандарте текстовых сообщений Internet RFC 822.

2.3.4. Разрешается указывать только реальный адрес электронной почты.

2.4. **Формат названия организации Владельца сертификата ключа проверки электронной подписи**

2.4.1. Название организации Владельца сертификата ключа проверки электронной подписи записывается в атрибут «O» субъекта Сертификата ключа проверки электронной подписи, атрибут является обязательным для Владельцев сертификата ключа проверки электронной подписи – физических лиц – представителей юридического лица. Для физических лиц поле не заполняется.

2.4.2. Длина текста этого поля для различных СКЗИ ограничивается 64 или 128 символами. В случае если длина полного названия организации превышает это значение, следует указывать официальное краткое наименование организации. Если официальное краткое наименование отсутствует или его длина превышает это значение, следует использовать сокращенное наименование от полного официального наименования. В этом случае необходимо оформить заявление согласно приложению № 7 к настоящему Регламенту.

2.4.3. Кавычки, точки и прочие знаки пунктуации разрешается использовать только в том случае, если они встречаются внутри официального названия организации.

2.5. **Формат подразделения организации Владельца сертификата ключа проверки электронной подписи**

2.5.1. Подразделение организации Владельца сертификата ключа проверки электронной подписи записывается в атрибут OU субъекта сертификата ключа проверки электронной подписи, атрибут не является обязательным.

2.5.2. Длина текста – не более 64 символов.

2.5.3. Кавычки, точки и прочие знаки пунктуации разрешается использовать только в том случае, если они встречаются внутри официального названия подразделения организации.

2.6. **Формат должности Владельца сертификата ключа проверки электронной подписи**

2.6.1. Должность Владельца сертификата ключа проверки электронной подписи записывается в атрибут «T» субъекта Сертификата ключа проверки электронной подписи, атрибут не является обязательным.

2.6.2. Длина текста – не более 64 символов.

2.6.3. Кавычки, точки и прочие знаки пунктуации разрешается использовать только в том случае, если они встречаются внутри официального названия должности.

2.7. **Формат названия населенного пункта**

2.7.1. Название населённого пункта, где зарегистрирована организация Владельца сертификата ключа проверки электронной подписи, записывается в атрибут «L» субъекта Сертификата ключа проверки электронной подписи, атрибут является обязательным.

2.7.2. Длина текста – не более 128 символов.

2.7.3. Вид населённого пункта указывается в начале текста без сокращения.

2.7.4. В случае, когда населённый пункт по административно-территориальному делению входит в состав округа, района и т.п., их названия перечисляются после названия населённого пункта через знак «/», в этом случае до и после знака «/» пробелы не ставятся.

2.7.5. Кавычки, точки и прочие знаки пунктуации разрешается использовать только в том случае, если они встречаются внутри официального названия населённого пункта.

2.8. **Формат названия региона (области)**

2.8.1. Название региона, где зарегистрировано юридическое лицо, индивидуальный предприниматель или физическое лицо – Владелец сертификата ключа проверки электронной подписи записывается в атрибут «S» субъекта Сертификата ключа проверки электронной подписи, атрибут является обязательным.

2.8.2. Длина текста – не более 128 символов.

2.8.3. Разрешается использовать только наименования из следующей таблицы:

Таблица 1

Справочник регионов

Название региона	
Республика Адыгея (Адыгея)	Кировская область
Республика Башкортостан	Костромская область
Республика Бурятия	Курганская область
Республика Алтай	Курская область
Республика Дагестан	Ленинградская область
Республика Ингушетия	Липецкая область
Кабардино-Балкарская Республика	Магаданская область
Республика Калмыкия	Московская область
Карачаево-Черкесская Республика	Мурманская область
Республика Карелия	Нижегородская область
Республика Коми	Новгородская область
Республика Крым	Новосибирская область
Республика Марий Эл	Омская область
Республика Мордовия	Оренбургская область
Республика Саха (Якутия)	Орловская область
Республика Северная Осетия - Алания	Пензенская область
Республика Татарстан	Пермский край
Республика Тыва	Псковская область
Удмуртская Республика	Ростовская область
Республика Хакасия	Рязанская область
Чеченская Республика	Самарская область
Чувашская Республика - Чувашия	Саратовская область
Алтайский край	Сахалинская область
Краснодарский край	Свердловская область
Красноярский край	Смоленская область
Приморский край	Тамбовская область
Ставропольский край	Тверская область
Хабаровский край	Томская область
Амурская область	Тульская область
Архангельская область	Тюменская область
Астраханская область	Ульяновская область
Белгородская область	Челябинская область
Брянская область	Забайкальский край
Владимирская область	Ярославская область
Волгоградская область	Город Москва
Вологодская область	Город Санкт-Петербург
Воронежская область	Город Севастополь
Ивановская область	Еврейская автономная область
Иркутская область	Ханты-Мансийский автономный округ - Югра
Калининградская область	Ненецкий автономный округ
Калужская область	Чукотский автономный округ
Камчатский край	Ямало-Ненецкий автономный округ
Кемеровская область	

2.8.4. Разрешается использовать наименование, отличное от указанного в таблице 1, в случае изменения наименований регионов Российской Федерации, а также в том случае, если

Сертификат ключа проверки электронной подписи будет выдаваться на нерезидента Российской Федерации.

2.9. **Формат ИНН**

2.9.1. Идентификационный номер налогоплательщика – юридического лица или физического лица.

2.9.2. Текст, длиной 12 цифр. Для юридического лица 10 цифр дополняются слева двумя нулями до 12 цифр. Для иностранной организации код иностранной организации (КИО) дополняется слева нулями до 12 цифр.

2.9.3. Разрешено использовать только цифровые символы 0123456789.

2.9.4. Запрещено использование ИНН, не проходящих проверку корректности на контрольные разряды.

2.10. **Формат ОГРН. Основной государственный регистрационный номер юридического лица**

2.10.1. Текст длиной 13 цифр - только для юридического лица.

2.10.2. Разрешено использовать только цифровые символы 0123456789.

2.10.3. Запрещено использование ОГРН, не проходящих проверку корректности на контрольные разряды.

2.11. **Набор разрешенных символов в Запросе на сертификат ключа проверки электронной подписи**

2.11.1. При использовании в тексте полей Сертификата ключа проверки электронной подписи символов UNICODE, коды которых не указаны в таблице 2, в выдаче Сертификата ключа проверки электронной подписи может быть отказано.

Таблица 2

Разрешенные символы

Символ	Название	Код UNICODE
	пробел	0x0020
"	прямые кавычки	0x0022
(	левая скобка	0x0028
)	правая скобка	0x0029
,	запятая	0x002C
-	дефис	0x002D
.	точка	0x002E
/	слэш	0x002F
0	цифра ноль	0x0030
1	цифра один	0x0031
2	цифра два	0x0032
3	цифра три	0x0033
4	цифра четыре	0x0034
5	цифра пять	0x0035
6	цифра шесть	0x0036
7	цифра семь	0x0037
8	цифра восемь	0x0037
9	цифра девять	0x0039
@	коммерческое ат «собачка»	0x0040
A	латинская заглавная буква A	0x0041
B	латинская заглавная буква B	0x0042
C	латинская заглавная буква C	0x0043
D	латинская заглавная буква D	0x0044
E	латинская заглавная буква E	0x0045

Символ	Название	Код UNICODE
F	латинская заглавная буква F	0x0046
G	латинская заглавная буква G	0x0047
H	латинская заглавная буква H	0x0048
I	латинская заглавная буква I	0x0049
J	латинская заглавная буква J	0x004A
K	латинская заглавная буква K	0x004B
L	латинская заглавная буква L	0x004C
M	латинская заглавная буква M	0x004D
N	латинская заглавная буква N	0x004E
O	латинская заглавная буква O	0x004F
P	латинская заглавная буква P	0x0050
Q	латинская заглавная буква Q	0x0051
R	латинская заглавная буква R	0x0052
S	латинская заглавная буква S	0x0053
T	латинская заглавная буква T	0x0054
U	латинская заглавная буква U	0x0055
V	латинская заглавная буква V	0x0056
W	латинская заглавная буква W	0x0057
X	латинская заглавная буква X	0x0058
Y	латинская заглавная буква Y	0x0059
Z	латинская заглавная буква Z	0x005A
_	подчёркивание	0x005F
№	номер	0x2116
a	латинская строчная буква a	0x0061
b	латинская строчная буква b	0x0062
c	латинская строчная буква c	0x0063
d	латинская строчная буква d	0x0064
e	латинская строчная буква e	0x0065
f	латинская строчная буква f	0x0066
g	латинская строчная буква g	0x0067
h	латинская строчная буква h	0x0068
i	латинская строчная буква i	0x0069
j	латинская строчная буква j	0x006A
k	латинская строчная буква k	0x006B
l	латинская строчная буква l	0x006C
m	латинская строчная буква m	0x006D
n	латинская строчная буква n	0x006E
o	латинская строчная буква o	0x006F
p	латинская строчная буква p	0x0070
q	латинская строчная буква q	0x0071
r	латинская строчная буква r	0x0072
s	латинская строчная буква s	0x0073
t	латинская строчная буква t	0x0074
u	латинская строчная буква u	0x0075
v	латинская строчная буква v	0x0076
w	латинская строчная буква w	0x0077
x	латинская строчная буква x	0x0078
y	латинская строчная буква y	0x0079
z	латинская строчная буква z	0x007A

Символ	Название	Код UNICODE
ё	кириллическая строчная буква ё	0x0451
А	кириллическая заглавная буква А	0x0410
Б	кириллическая заглавная буква Б	0x0411
В	кириллическая заглавная буква В	0x0412
Г	кириллическая заглавная буква Г	0x0413
Д	кириллическая заглавная буква Д	0x0414
Е	кириллическая заглавная буква Е	0x0415
Ж	кириллическая заглавная буква Ж	0x0416
З	кириллическая заглавная буква З	0x0417
И	кириллическая заглавная буква И	0x0418
Й	кириллическая заглавная буква Й	0x0419
К	кириллическая заглавная буква К	0x041A
Л	кириллическая заглавная буква Л	0x041B
М	кириллическая заглавная буква М	0x041C
Н	кириллическая заглавная буква Н	0x041D
О	кириллическая заглавная буква О	0x041E
П	кириллическая заглавная буква П	0x041F
Р	кириллическая заглавная буква Р	0x0420
С	кириллическая заглавная буква С	0x0421
Т	кириллическая заглавная буква Т	0x0422
У	кириллическая заглавная буква У	0x0423
Ф	кириллическая заглавная буква Ф	0x0424
Х	кириллическая заглавная буква Х	0x0425
Ц	кириллическая заглавная буква Ц	0x0426
Ч	кириллическая заглавная буква Ч	0x0427
Ш	кириллическая заглавная буква Ш	0x0428
Щ	кириллическая заглавная буква Щ	0x0429
Ъ	кириллическая заглавная буква Ъ	0x042A
Ы	кириллическая заглавная буква Ы	0x042B
Ь	кириллическая заглавная буква Ь	0x042C
Э	кириллическая заглавная буква Э	0x042D
Ю	кириллическая заглавная буква Ю	0x042E
Я	кириллическая заглавная буква Я	0x042F
а	кириллическая строчная буква а	0x0430
б	кириллическая строчная буква б	0x0431
в	кириллическая строчная буква в	0x0432
г	кириллическая строчная буква г	0x0433
д	кириллическая строчная буква д	0x0434

Символ	Название	Код UNICODE
е	кириллическая строчная буква е	0x0435
ж	кириллическая строчная буква ж	0x0436
з	кириллическая строчная буква з	0x0437
и	кириллическая строчная буква и	0x0438
й	кириллическая строчная буква й	0x0439
к	кириллическая строчная буква к	0x043A
л	кириллическая строчная буква л	0x043B
м	кириллическая строчная буква м	0x043C
н	кириллическая строчная буква н	0x043D
о	кириллическая строчная буква о	0x043E
п	кириллическая строчная буква п	0x043F
р	кириллическая строчная буква р	0x0440
с	кириллическая строчная буква с	0x0441
т	кириллическая строчная буква т	0x0442
у	кириллическая строчная буква у	0x0443
ф	кириллическая строчная буква ф	0x0444
х	кириллическая строчная буква х	0x0445
ц	кириллическая строчная буква ц	0x0446
ч	кириллическая строчная буква ч	0x0447
ш	кириллическая строчная буква ш	0x0448
щ	кириллическая строчная буква щ	0x0449
ъ	кириллическая строчная буква ъ	0x044A
ы	кириллическая строчная буква ы	0x044B
ь	кириллическая строчная буква ь	0x044C
э	кириллическая строчная буква э	0x044D
ю	кириллическая строчная буква ю	0x044E
я	кириллическая строчная буква я	0x044F

3. Оформление заявлений на бумажном носителе

3.1. Все заявления, направляемые на бумажном носителе, должны соответствовать формам, приведенным в настоящем Регламенте.

3.2. Печать организации (при наличии) должна четко просматриваться, сведения, содержащиеся в печати, должны соответствовать сведениям, указанным в заявлении на бумажном носителе и в Запросе на изготовление сертификата ключа проверки электронной подписи.

3.3. Заявление должно распечатываться строго на одной стороне одного листа формата А4.

3.4. Внесение исправлений в заявления не допускаются.

3.5. В случае неразборчивого заполнения заявления в его приеме может быть отказано.

4. Примеры заполнения полей Запросов на изготовление сертификатов ключей проверки электронной подписи

4.1. C=RU, S=город Москва, L=город Москва, CN=Петров Иван Васильевич, ИНН=123456789047

4.2. C=RU, S=город Москва, L=город Зеленоград, CN=Петров Иван Васильевич, O=Индивидуальный предприниматель Петров Иван Васильевич, ИНН=123456789047, ОГРН(ИП)=123456789012302

4.3. C=RU, S=Ленинградская область, L=город Выборг, CN=Петров Иван Васильевич, O=Акционерное общество «Ценных мех», ИНН=001234567894, ОГРН(ИП)=1234567890105

4.4. C=RU, S=Краснодарский край, L=станица Бородинская/Приморско-Ахтарский район, O=ООО «УК НПФ с заведомо чрезвычайно длинным полным наименованием», OU=Бухгалтерия, T=Главный бухгалтер, E=no@ya.ru, CN=Королёв Дмитрий Семенович, ИНН=001111111117, ОГРН(ИП)=1111111111110

Приложение № 7

к «Регламенту удостоверяющего центра Банка ГПБ (АО)» от 09.06.2018 № И/47.

ЗАЯВЛЕНИЕ
об использовании сокращенного наименования организации в Сертификате ключа проверки электронной подписи

В связи превышением в полном и кратком наименованиях организации допустимого количества символов, прошу использовать сокращенное наименование организации в Сертификатах ключа проверки подписи работников нашей организации.

Полное наименование организации: _____

_____

Краткое наименование организации: _____

_____

Сокращенное наименование организации:

_____

Руководитель организации _____ _____
(подпись) (Ф.И.О.)

«___»_____ 20__г. М.П.

(заполняется Менеджером Системы ЭДО и Уполномоченным лицом удостоверяющего центра)

Отметка о получении Менеджером Системы ЭДО: ___ ч. ___ мин. «____» _____ 20___ г.

Менеджер Системы ЭДО _____ _____
(подпись) (Ф.И.О.)

Отметка о получении Уполномоченным лицом УЦ: ___ ч. ___ мин. «____» _____ 20___ г.

Уполномоченное лицо УЦ _____ _____
(подпись) (Ф.И.О.)

Приложение № 8

к «Регламенту удостоверяющего центра Банка ГПБ (АО)» от 09.06.2018 № И/47.

ГАЗПРОМБАНК

«Газпромбанк» (Акционерное общество)
Банк ГПБ (АО)

Бланк Сертификата ключа проверки электронной подписи

(форма для юридических лиц)

Номер сертификата: [_____]
Срок действия сертификата: с [_____] по [_____]

Сведения о владельце сертификата
Наименование юридического лица: [_____]
Основной государственный регистрационный номер: [_____]
Индивидуальный номер налогоплательщика: [_____]
Место нахождения юридического лица: [_____]
Уполномоченный представитель юридического лица: [_____]

Сведения об издателе сертификата
Наименование удостоверяющего центра: ***Удостоверяющий центр Банка ГПБ (АО)***
Место нахождения удостоверяющего центра: ***117418, г. Москва, ул. Новочеремушкинская, д. 63***
Наименование средства электронной подписи: [_____]
Наименование средства удостоверяющего центра: [_____]

Сведения о ключе проверки электронной подписи
Используемый алгоритм: ***ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»***
Значение ключа: [_____
_____]

Электронная подпись под сертификатом
Используемый алгоритм: ***ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»***
Значение электронной подписи: [_____
_____]

Уполномоченное лицо удостоверяющего центра _____ _____
(подпись) (Ф.И.О.)

Начальник удостоверяющего центра _____ _____
(подпись) (Ф.И.О.)

«___»_____ 20___г. М.П.

Приложение № 9

к «Регламенту удостоверяющего центра Банка ГПБ (АО)» от 09.06.2018 № И/47.

«Газпромбанк» (Открытое акционерное общество)
Банк ГПБ (АО)

Бланк Сертификата ключа проверки электронной подписи

(форма для физических лиц)

Номер сертификата: [_____]
Срок действия сертификата: с [_____] по [_____]

Сведения о владельце сертификата
Фамилия, имя, отчество: [_____]
Индивидуальный номер налогоплательщика: [_____]

Сведения об издателе сертификата
Наименование удостоверяющего центра: ***Удостоверяющий центр Банка ГПБ (АО)***
Место нахождения удостоверяющего центра: ***117418, г. Москва, ул. Новочеремушкинская, д. 63***
Наименование средства электронной подписи: [_____]
Наименование средства удостоверяющего центра: [_____]

Сведения о ключе проверки электронной подписи
Используемый алгоритм: ***ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»***
Значение ключа: [_____
_____]

Электронная подпись под сертификатом
Используемый алгоритм: ***ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»***
Значение электронной подписи: [_____
_____]

Уполномоченное лицо удостоверяющего центра _____ _____
(подпись) (Ф.И.О.)

Начальник удостоверяющего центра _____ _____
(подпись) (Ф.И.О.)

«___»_____ 20___г. М.П.

Приложение № 10

к «Регламенту удостоверяющего центра Банка ГПБ (АО)» от 09.06.2018 № И/47.

ЗАЯВЛЕНИЕ
о прекращении действия Сертификата ключа проверки электронной подписи
(форма для юридических лиц)

Прошу внести в реестр Удостоверяющего центра информацию о прекращении действия Сертификата ключа проверки электронной подписи:

_____
(Ф.И.О. Владельца сертификата ключа проверки электронной подписи)

Серийный номер сертификата: _____
(Поле обязательное для заполнения!)

Причина прекращения действия сертификата: _____

_____

Руководитель организации _____ _____
(подпись) (Ф.И.О.)

«___»_____ 20___г. М.П.

(заполняется Менеджером Системы ЭДО и Уполномоченным лицом удостоверяющего центра)

Отметка о получении Менеджером Системы ЭДО: ___ ч. ___ мин. «____» _____ 20___ г.

Данные, указанные в заявлении, верны. _____
(Подпись и Ф.И.О. Менеджера Системы ЭДО)

Отметка о получении Уполномоченным лицом УЦ: ___ ч. ___ мин. «____» _____ 20___ г.

Сведения о прекращении действия Сертификата ключа проверки электронной подписи занесены в реестр УЦ. _____
(Подпись и Ф.И.О. Уполномоченного лица УЦ)

Приложение № 11

к «Регламенту удостоверяющего центра Банка ГПБ (АО)» от 09.06.2018 № И/47.

ЗАЯВЛЕНИЕ
о прекращении действия Сертификата ключа проверки электронной подписи
(форма для физических лиц)

Прошу внести в реестр Удостоверяющего центра информацию о прекращении действия Сертификата ключа проверки электронной подписи:

_____
(Ф.И.О. Владельца сертификата ключа проверки электронной подписи)

Серийный номер сертификата: _____
(Поле обязательное для заполнения!)

Причина прекращения действия сертификата: _____

_____

Владелец сертификата ключа
проверки электронной подписи _____ _____
(подпись) (Ф.И.О.)

«___»_____ 20___г.

(заполняется Менеджером Системы ЭДО и Уполномоченным лицом удостоверяющего центра)

Отметка о получении Менеджером Системы ЭДО: ___ ч. ___ мин. «____» _____ 20___ г.

Данные, указанные в заявлении, верны. _____
(Подпись и Ф.И.О. Менеджера Системы ЭДО)

Отметка о получении Уполномоченным лицом УЦ: ___ ч. ___ мин. «____» _____ 20___ г.

Сведения о прекращении действия Сертификата ключа проверки электронной подписи занесены в реестр УЦ. _____
(Подпись и Ф.И.О. Уполномоченного лица УЦ)

Приложение № 12

к «Регламенту удостоверяющего центра Банка ГПБ (АО)» от 09.06.2018 № И/47.

Требования по обеспечению безопасности при работе со Средствами криптографической защиты информации

Использование Электронных подписей сопровождается рисками финансовых потерь при несанкционированном получении злоумышленниками Ключей электронной подписи или несанкционированного использования рабочего места пользователя, на котором осуществляется выработка Электронной подписи. В связи с этим необходимо выполнение приведенных ниже организационно-технических и административных мер по обеспечению правильного функционирования средств обработки и передачи информации.

1. Требования по размещению

При размещении СКЗИ:

- должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены СКЗИ, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями и обеспечена невозможность негативных действий с их стороны на СКЗИ и передаваемую информацию;
- внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию;

2. Требования по установке СКЗИ, общесистемного и специального программного обеспечения

К установке общесистемного и специального программного обеспечения, а также программного обеспечения СКЗИ, допускаются лица, прошедшие соответствующую подготовку и изучившие документацию на соответствующее программное обеспечение.

При установке программного обеспечения СКЗИ следует:

- на технических средствах, на которые устанавливаются СКЗИ, использовать только лицензионное программное обеспечение фирм-изготовителей;
- инсталляция программного обеспечения СКЗИ должна производиться только с дистрибутива, полученного от Банка. При инсталляции СКЗИ должны быть обеспечены организационно-технические меры по исключению подмены дистрибутива и внесения изменений в СКЗИ после установки;
- на технических средствах с установленными СКЗИ не должны устанавливаться средства разработки программного обеспечения и отладчики. Если средства отладки приложений нужны для технологических потребностей пользователя, то их использование должно быть санкционировано Администратором безопасности. При этом должны быть реализованы меры, исключающие возможность использования этих средств для редактирования кода и памяти программного обеспечения СКЗИ в процессе обработки СКЗИ защищаемой информации и/или при загруженной ключевой информации;
- предусмотреть меры, исключающие возможность несанкционированного изменения аппаратной части технических средств, на которых установлены СКЗИ (например, путем опечатывания системного блока и разъемов);
- Программное обеспечение, используемое на технических средствах с установленными СКЗИ, не должно содержать возможностей, позволяющих:
  - модифицировать содержимое произвольных областей памяти;

– модифицировать собственный код и код других подпрограмм;

– модифицировать память, выделенную для других подпрограмм;

– передавать управление в область собственных данных и данных других подпрограмм;

– несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;

– повышать предоставленные привилегии;

– модифицировать настройки операционной системы;

– использовать недокументированные фирмой-разработчиком функции операционной системы.

3. Меры по обеспечению защиты от несанкционированного доступа

При использовании СКЗИ должны выполняться следующие меры по защите информации от несанкционированного доступа:

• Необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), использовать фильтры паролей в соответствии со следующими правилами:

– длина пароля должна быть не менее 8 символов;

– в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, дат рождения и т.д.), а также общепринятые сокращения (USER, ADMIN и т.д.);

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

– личный пароль пользователь не имеет права никому сообщать;

– периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 50 дней.

• Запрещается:

– оставлять технические средства с установленными СКЗИ без контроля, после ввода ключевой информации либо иной конфиденциальной информации;

– вносить какие-либо изменения в программное обеспечение СКЗИ;

– осуществлять несанкционированное Администратором безопасности копирование ключевых носителей;

– разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и иные средства отображения информации;

– использовать ключевые носители в режимах, не предусмотренных функционированием СКЗИ;

– записывать на ключевые носители постороннюю информацию.

Администратор безопасности должен сконфигурировать операционную систему и осуществлять периодический контроль сделанных настроек в соответствии со следующими требованиями:

• не использовать нестандартные, измененные или отладочные версии операционных систем;

• исключить возможность загрузки и использования операционной системы, отличной от предусмотренной штатной работой;

• исключить возможность удаленного управления, администрирования и модификации операционной системы и ее настроек;

• на технических средствах с установленными СКЗИ должна быть установлена только одна операционная система;

- правом установки и настройки операционной системы, а также СКЗИ должен обладать только Администратор безопасности;
- все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.);
- режимы безопасности, реализованные в операционной системе, должны быть настроены на максимальный уровень;
- всем пользователям и группам, зарегистрированным в операционной системе, необходимо назначить минимально возможные для нормальной работы права;
- необходимо предусмотреть меры, максимально ограничивающие доступ к следующим ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):
  - системный реестр;
  - файлы и каталоги;
  - временные файлы;
  - журналы системы;
  - файлы подкачки;
  - кэшируемая информация (пароли и т.п.);
  - отладочная информация.

Кроме того, необходимо организовать стирание (по окончании сеанса работы СКЗИ) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы СКЗИ. Если это не выполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям.

- Должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками операционной системы, повышать предоставленные привилегии.
- Необходимо регулярно устанавливать пакеты обновления безопасности операционной системы (Service Packs, Hot fix и т.п.), обновлять антивирусные базы, а так же исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий.
- В случае подключения технических средств с установленными СКЗИ к общедоступным сетям передачи данных необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов, полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети. С целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты (например: установка межсетевых экранов, организация VPN-сетей и т.п.). При этом предпочтение должно отдаваться средствам защиты, имеющим сертификат уполномоченного органа по сертификации.
- Организовать и использовать систему аудита, организовать регулярный анализ результатов аудита.
- Организовать и использовать комплекс мероприятий антивирусной защиты.

НЕ ДОПУСКАЕТСЯ:

- осуществлять несанкционированное копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер (за исключением случаев, предусмотренных данными требованиями);
- вставлять ключевой носитель в устройство считывания в режимах, не предусмотренных штатным режимом использования ключевого носителя;

- подключать к техническим средствам с установленными СКЗИ дополнительные устройства и соединители, не предусмотренные штатной комплектацией;
- работать на технических средствах с установленными СКЗИ, если во время его начальной загрузки не проходит встроенный тест ОЗУ;
- вносить какие-либо изменения в программное обеспечение СКЗИ;
- изменять настройки, установленные программой установки СКЗИ или Администратором безопасности;
- обрабатывать на технических средствах с установленными СКЗИ информацию, содержащую государственную тайну;
- осуществлять несанкционированное вскрытие корпуса технического средства с установленными СКЗИ;
- работать с СКЗИ при включенных в техническое средство штатных средствах выхода в радиоканал;
- приносить и использовать в помещении, где размещены средства СКЗИ, радиотелефоны и другую радиопередающую аппаратуру (требование носит рекомендательный характер).

4. Требования по обеспечению информационной безопасности при работе в системах обмена электронными документами

- Недопустимо пересылать файлы с ключевой информацией для работы в системах обмена электронными документами по электронной почте сети Интернет или по внутренней электронной почте (кроме запросов на сертификат и открытых ключей).
- Ключевая информация должна размещаться на сменном носителе информации (floppy-диск, USB-flash накопитель, e-Token и др.). Размещение ключевой информации на локальном или сетевом диске, а также во встроенной памяти технического средства с установленными СКЗИ, способствует реализации многочисленных сценариев совершения мошеннических действий злоумышленниками.
- Носители ключевой информации должны использоваться только их владельцем либо лицом, уполномоченным на использование данного носителя, и храниться в месте не доступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик и т.д.).
- Носитель ключевой информации должен быть вставлен в считывающее устройство только на время выполнения СКЗИ операций зашифрования и расшифрования, а также формирования и проверки электронной подписи. Размещение носителя ключевой информации в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами.
- На носителе ключевой информации недопустимо хранить иную информацию (в том числе рабочие или личные файлы).
- С целью контроля исходящего и входящего подозрительного трафика, технические средства с установленными СКЗИ должны быть защищены от внешнего доступа программными или аппаратными средствами межсетевого экранирования. Эти средства должны пресекать отправку в Интернет информации, инициированную программами, не имеющими соответствующих полномочий.
- На технических средствах, используемых для работы в системах обмена электронными документами:
  - на учетные записи пользователей операционной системы должны быть установлены пароли, удовлетворяющие требованиям, приведенным в разделе 3;
  - должно быть установлено только лицензионное программное обеспечение;
  - должно быть установлено лицензионное антивирусное программное обеспечение с регулярно обновляемыми антивирусными базами данных;
  - должны быть отключены все неиспользуемые службы и процессы операционной системы Windows (в т.ч. службы удаленного администрирования и управления, службы общего доступа к ресурсам сети, системные диски C$ и т.д.);

– должны регулярно устанавливаться обновления операционной системы;

– должен быть исключен доступ (физический и/или удаленный) к техническим средствам с установленными СКЗИ третьих лиц, не имеющих полномочий для работы в системе обмена электронными документами;

– должна быть активирована подсистема регистрации событий информационной безопасности;

– должна быть включена автоматическая блокировка экрана после ухода ответственного сотрудника с рабочего места.

• В качестве автоматизированного рабочего места для работы в системах обмена электронными документами крайне не рекомендуется выбирать переносной компьютер (ноутбук). Если выбран ноутбук, недопустимо его подключение к сетям общего доступа в местах свободного доступа в Интернет (Интернет-кафе, гостиницы, офисные центры и т.д.), при этом для хранения ключевой информации должен использоваться сменный носитель информации.

В случае передачи (списания, выброса, сдачи в ремонт) сторонним лицам технических средств, на которых были установлены СКЗИ, необходимо гарантированно удалить с него всю информацию, использование которой третьими лицами может потенциально нанести вред финансовой деятельности или имиджу Вашей организации (в том числе программное обеспечение АРМ системы «Клиент-Банк», СКЗИ, журналы работы систем обмена электронными документами и т.д.).

5. Дополнительные требования

Дополнительные требования по обеспечению информационной безопасности при работе в системах обмена электронными документами могут дополнительно устанавливаться правилами систем ЭДО, требованиями по эксплуатации и безопасности СКЗИ.

Приложение № 13

к «Регламенту удостоверяющего центра Банка ГПБ (АО)» от 09.06.2018 № И/47.

Процедура проведения технической экспертизы при разрешении споров

1. Подтверждение подлинности ЭП в электронном документе.

1.1. По желанию Стороны, заключившей Договор, Удостоверяющий центр осуществляет проведение экспертных работ по Подтверждению ЭП в электронном документе.

1.2. Сторона, которой требуется проведение экспертных работ, направляет в Удостоверяющий центр «Заявление на подтверждение подлинности электронной подписи в электронном документе» (приложение № 14 и № 15).

1.3. Проведение работ по Подтверждению подлинности ЭП в электронном документе осуществляет комиссия, сформированная из числа работников Удостоверяющего центра.

1.4. Результатом проведения работ по Подтверждению подлинности ЭП в электронном документе является заключение Удостоверяющего центра. Заключение содержит:

1.4.1. Время и место проведения проверки.

1.4.2. Состав комиссии, осуществлявшей проверку.

1.4.3. Основание для проведения проверки.

1.4.4. Содержание и результаты проверки с указанием примененных методов.

1.4.5. Обоснование результатов проверки.

1.4.6. Данные, представленные для проведения проверки.

1.4.7. Результат проверки ЭП в Электронном документе (ЭП в Электроном документе верна/неверна).

1.5. Заключение Удостоверяющего центра по выполненной проверке составляется в простой письменной форме в двух экземплярах, подписывается всеми членами комиссии и заверяется печатью Удостоверяющего центра. Один экземпляр заключения по выполненной проверке предоставляется заявителю.

1.6. Срок проведения работ по Подтверждению подлинности ЭП в электронном документе и предоставления заключения о произведенной проверке составляет пять рабочих дней с даты поступления заявления в Удостоверяющий центр.

1.7. Состав экспертной комиссии, набор исходных данных для проведения указанной экспертизы, состав и содержание отчетных документов (акты, заключения и т.д.), сроки проведения работ, могут также определяться Сторонами на основании заключаемого соглашения об ЭДО.

2. Подтверждение подлинности ЭП Уполномоченного лица удостоверяющего центра в изданных сертификатах

2.1. Для подтверждения подлинности ЭП Уполномоченного лица удостоверяющего центра в Сертификате ключа проверки электронной подписи Пользователь УЦ подает в Удостоверяющий центр заявление на подтверждение подлинности ЭП Уполномоченного лица удостоверяющего центра в Сертификате ключа проверки электронной подписи.

2.2. Заявление должно содержать следующую информацию:

2.2.1. Дата и время подачи заявления;

2.2.2. Идентификационные данные Пользователя УЦ, в Сертификате ключа проверки электронной подписи которого необходимо подтвердить подлинность ЭП Уполномоченного лица удостоверяющего центра.

2.2.3. Серийный номер сертификата Ключа проверки электронной подписи, в котором необходимо подтвердить подлинность ЭП Уполномоченного лица удостоверяющего центра.

2.2.4. Время и дата на момент наступления которых требуется установить статус сертификата.

2.3. Обязательным приложением к заявлению на подтверждение подлинности ЭП Уполномоченного лица удостоверяющего центра в Сертификате ключа проверки электронной подписи является съемный носитель, содержащий файл Сертификата ключа проверки электронной подписи формата PKCS#7 в кодировке Base64 (.CER), подвергающегося процедуре проверки.

2.4. Проведение работ по подтверждению подлинности ЭП Уполномоченного лица удостоверяющего центра в Сертификате ключа проверки электронной подписи осуществляет комиссия, сформированная из числа с работников Удостоверяющего центра.

2.5. Результатом проведения работ по подтверждению подлинности ЭП Уполномоченного лица удостоверяющего центра в Сертификате ключа проверки электронной подписи является заключение удостоверяющего центра. Заключение содержит:

2.5.1. Время и место проведения проверки.

2.5.2. Состав комиссии, осуществлявшей проверку.

2.5.3. Основание для проведения проверки.

2.5.4. Содержание и результаты проверки с указанием примененных методов.

2.5.5. Обоснование результатов проверки.

2.5.6. Данные, представленные для проведения проверки.

2.5.7. Результат проверки ЭП Уполномоченного лица удостоверяющего центра (ЭП Уполномоченного лица удостоверяющего центра в Сертификате ключа подписи верна/неверна).

2.6. Заключение Удостоверяющего центра по выполненной проверке составляется в простой письменной форме в двух экземплярах, подписывается всеми членами комиссии и заверяется печатью Удостоверяющего центра. Один экземпляр заключения по выполненной проверке предоставляется заявителю.

2.7. Срок проведения работ по подтверждению подлинности ЭП Уполномоченного лица удостоверяющего центра и предоставлению пользователю заключения о произведенной проверке составляет пять рабочих дней с даты поступления заявления в Удостоверяющий центр.

3. Подтверждение принадлежности Сертификата ключа проверки электронной подписи Пользователю УЦ.

3.1. Подтверждение принадлежности Сертификата ключа проверки электронной подписи Пользователю УЦ заключается в сопоставлении электронного Запроса на изготовление сертификата ключа проверки электронной подписи, Заявления об акцепте условий Регламента и изготовлении Сертификата ключа проверки электронной подписи и самого Сертификата ключа проверки электронной подписи Пользователя УЦ и подтверждении идентичности указанных в них данных.

3.2. В случае если новый Сертификат ключа проверки электронной подписи Пользователя УЦ был выпущен на основании электронного Запроса на изготовление сертификата ключа проверки электронной подписи, подписанного действующим Ключом электронной подписи Пользователя УЦ, проводится следующая процедура:

3.2.1. Проводится проверка соблюдения условий, приведенных в пункте 6.5.3 настоящего Регламента.

3.2.2. Удостоверяющий центр выгружает файл электронного Запроса на изготовление сертификата ключа проверки электронной подписи и файл, содержащий Электронную подпись, которой этот электронный запрос был подписан.

3.2.3. Производится подтверждение подлинности Электронной подписи, которой был подписан Запрос на изготовление сертификата ключа проверки электронной подписи.

3.2.4. Пункты 3.2.2 и 3.2.3 повторяются столько раз, сколько новые сертификаты Пользователя УЦ выпускались на основании электронных Запросов на изготовление сертификатов ключей проверки электронной подписи, подписанных действующим Ключом электронной подписи Пользователя УЦ, до Сертификата ключа проверки электронной подписи, который был выпущен на основании электронного Запроса на изготовление сертификата ключа проверки электронной подписи и соответствующего ему Заявления об акцепте условий Регламента и изготовлении Сертификата ключа проверки электронной подписи.

Приложение № 14

к «Регламенту удостоверяющего центра Банка ГПБ (АО)» от 09.06.2018 № И/47.

Заявление на Подтверждение подлинности ЭП в Электронном документе

(форма для юридических лиц)

_____

(наименование организации, включая организационно-правовую форму)

в лице _____

(должность)

_____,

(фамилия, имя, отчество)

действующего на основании _____,

просит подтвердить подлинность Электронной подписи в Электронном документе на основании предоставленных исходных данных:

1. Идентификационные данные субъекта, подлинность ЭП которого необходимо подтвердить в Электронном документе:

CommonName (CN)	Общее имя – фамилия, имя, отчество (псевдоним)
E-Mail (E)	Адрес электронной почты
Organization (O)	Наименование организации
Organization Unit (OU)	Подразделение
Locality (L)	Город
State (S)	Область
Contry (C)	Страна

2. Файл _____, содержащий Сертификат ключа проверки электронной подписи Уполномоченного лица удостоверяющего центра, с использованием которого был издан Сертификат ключа проверки электронной подписи в Электронном документе на прилагаемом к заявлению сменном носителе информации – рег. № _____.

3. Файл _____, содержащий Сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить Подтверждение ЭП в электронном документе на прилагаемом к заявлению сменном носителе информации – рег. № _____.

4. Файл _____ стандарта PKCS#7, содержащий подписанные ЭП данные и значение ЭП, (либо файл, содержащий исходные данные, и файл стандарта PKCS#7, содержащий значение ЭП) на прилагаемом к заявлению сменном носителе информации – рег. № _____

5. Время и дата* формирования ЭП Электронного документа:

«_____:_____» «_____/_____/_____»

Час Мин. День Месяц Год

6. Время и дата*, на момент наступления которых требуется подтвердить подлинность ЭП:

«_____:_____» «_____/_____/_____»

Час Мин. День Месяц Год

Руководитель организации _____ _____

(подпись) (Ф.И.О.)

«___»_____ 20___г. М.П.

---

* Время и дата должны быть указаны с учетом часового пояса г. Москвы (по московскому времени). Если время и дата не указаны, то статус сертификата устанавливается на момент подачи заявления в удостоверяющий центр.

Приложение № 15

к «Регламенту удостоверяющего центра Банка ГПБ (АО)» от 09.06.2018 № И/47.

Заявление на Подтверждение подлинности ЭП в Электронном документе

(форма для физических лиц)

Я,_____,
(фамилия, имя, отчество)

прошу подтвердить подлинность Электронной подписи в Электронном документе на основании предоставленных исходных данных:

1. Идентификационные данные субъекта, подлинность ЭП которого необходимо подтвердить в Электронном документе:

CommonName (CN)	Общее имя – фамилия, имя, отчество (псевдоним)
E-Mail (E)	Адрес электронной почты
Organization (O)	Наименование организации
Organization Unit (OU)	Подразделение
Locality (L)	Город
State (S)	Область
Contry (C)	Страна

2. Файл _____, содержащий Сертификат ключа проверки электронной подписи Уполномоченного лица удостоверяющего центра, с использованием которого был издан Сертификат ключа проверки электронной подписи в Электронном документе на прилагаемом к заявлению сменном носителе информации _____.

3. Файл _____, содержащий Сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить Подтверждение ЭП в электронном документе на прилагаемом к заявлению сменном носителе информации _____.

4. Файл _____ стандарта PKCS#7, содержащий подписанные ЭП данные и значение ЭП, (либо файл, содержащий исходные данные, и файл стандарта PKCS#7, содержащий значение ЭП) на прилагаемом к заявлению сменном носителе информации _____.

5. Время и дата* формирования ЭП Электронного документа:
«_____:_____» «_____/_____/_____»
Час Мин. День Месяц Год

6. Время и дата*, на момент наступления которых требуется подтвердить подлинность ЭП:
«_____:_____» «_____/_____/_____»
Час Мин. День Месяц Год

_____ _____
(подпись) (Ф.И.О.)

«___»_____ 20___г.

---

* Время и дата должны быть указаны с учетом часового пояса г. Москвы (по московскому времени). Если время и дата не указаны, то статус сертификата устанавливается на момент подачи заявления в удостоверяющий центр.