

**ПРАВИЛА ПОЛЬЗОВАНИЯ
ЦЕНТРАЛИЗОВАННОЙ СИСТЕМОЙ
ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ
БАНКА «ВОЗРОЖДЕНИЕ» (ПАО)**

Версия 3.3

СОДЕРЖАНИЕ

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ	4
2. ПРЕДМЕТ РЕГУЛИРОВАНИЯ.....	9
3. РЕГУЛИРОВАНИЕ ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ, ПОРЯДОК ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ В СИСТЕМЕ ДБО.....	9
4. ПОРЯДОК И УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ ДОСТУПА КЛИЕНТУ К ОСУЩЕСТВЛЕНИЮ ДОКУМЕНТООБОРОТА В СИСТЕМЕ ДБО	10
5. ПОРЯДОК ВСТУПЛЕНИЯ В СИЛУ НАСТОЯЩИХ ПРАВИЛ, ВНЕСЕНИЯ В НИХ ИЗМЕНЕНИЙ И ПРЕКРАЩЕНИЯ ДЕЙСТВИЯ.....	13
6. ПОРЯДОК УВЕДОМЛЕНИЯ О ВНЕСЕНИИ ИЗМЕНЕНИЙ В ПРАВИЛА.....	13
7. ОБЩИЕ ПОЛОЖЕНИЯ	13
8. ЭЛЕКТРОННЫЙ ДОКУМЕНТ	19
8.1. Требования, предъявляемые к электронному документу	19
8.2. Электронная подпись и шифрование электронного документа	19
8.3. Подлинник электронного документа	19
8.4. Копии электронного документа на бумажном носителе	19
8.5. Электронные документы, используемые в Системе ДБО	19
9. ОРГАНИЗАЦИЯ ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ	21
9.1. Обмен электронными документами	21
9.2. Формирование электронного документа.....	21
9.3. Отправка и доставка электронного документа.....	21
9.4. Проверка подлинности доставленного электронного документа	22
9.5. Подтверждение получения электронного документа	22
9.6. Отзыв электронного документа	22
10. ОБЯЗАННОСТИ КЛИЕНТА	22
11. ПОРЯДОК ОПЛАТЫ УСЛУГ.....	23
12. СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	25
12.1. Порядок формирования криптографических профилей, ключей ЭП и СКП ЭП клиента, организация обслуживания клиента.....	25
12.2. Особенности оформления пакета документов для Клиентов при подключении Системы ДБО в конфигурации «Корпоративный контроль»	31
12.3. Проведение плановой замены криптографических ключей и СКП ЭП клиента.....	33
12.4. Порядок действий при компрометации криптографических ключей или физической порче носителя ключевой и парольной информации.....	34
13. ОТВЕТСТВЕННОСТЬ СТОРОН. ОБСТОЯТЕЛЬСТВА, ИСКЛЮЧАЮЩИЕ ОТВЕТСТВЕННОСТЬ СТОРОН (ФОРС-МАЖОР).....	36
14. ПОРЯДОК УРЕГУЛИРОВАНИЯ СПОРНЫХ СИТУАЦИЙ.....	37
15. ПОРЯДОК ДЕЙСТВИЙ ПРИ ВЫЯВЛЕНИИ ПОДОЗРЕНИЙ НА МОШЕННИЧЕСКИЕ ДЕЙСТВИЯ, СОВЕРШЕННЫЕ С ИСПОЛЬЗОВАНИЕМ ЦС ДБО	40

ПРИЛОЖЕНИЕ 1 ЗАЯВЛЕНИЕ О ПРИСОЕДИНЕНИИ	43
ПРИЛОЖЕНИЕ 2 ЗАЯВЛЕНИЕ НА РЕГИСТРАЦИЮ ПОЛЬЗОВАТЕЛЯ УЦ И ВЫПУСК СКП ЭП.....	44
ПРИЛОЖЕНИЕ 2А ЗАЯВЛЕНИЕ НА ВЫПУСК СКП ЭП.....	45
ПРИЛОЖЕНИЕ 3 ЗАЯВЛЕНИЕ НА АННУЛИРОВАНИЕ СКП ЭП.	46
ПРИЛОЖЕНИЕ 4 ДОВЕРЕННОСТЬ НА ПОЛУЧЕНИЕ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ....	47
ПРИЛОЖЕНИЕ 4А ДОВЕРЕННОСТЬ НА ПОЛНОМОЧНОГО ПРЕДСТАВИТЕЛЯ КЛИЕНТА..	48
ПРИЛОЖЕНИЕ 5 ЗАЯВЛЕНИЕ НА УСТАНОВКУ (НАСТРОЙКУ) СИСТЕМЫ ДБО.....	49
ПРИЛОЖЕНИЕ 6 АКТ О ПЕРЕДАЧЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СИСТЕМЫ ДБО И КЛЮЧЕЙ ЭП.....	50
ПРИЛОЖЕНИЕ 7 РУКОВОДСТВО ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ И СРЕДСТВ ЭЛЕКТРОННОЙ ПОДПИСИ... 	52
ПРИЛОЖЕНИЕ 8 АКТ О СОБЛЮДЕНИИ КЛИЕНТОМ ТРЕБОВАНИЙ РУКОВОДСТВА.	54
ПРИЛОЖЕНИЕ 9 АНКЕТА О РЕЗУЛЬТАТАХ ВЫПОЛНЕНИЯ КЛИЕНТОМ ТРЕБОВАНИЙ РУКОВОДСТВА.	57
ПРИЛОЖЕНИЕ 10 АКТ ОБ ОКАЗАНИИ УСЛУГ ПО ВЫПУСКУ СКП ЭП.....	60
ПРИЛОЖЕНИЕ 11 ПЕРЕЧЕНЬ ДОГОВОРОВ И СПИСОК ЛИЦ.	61
ПРИЛОЖЕНИЕ 12 АКТ ОБ ОКАЗАНИИ УСЛУГ ПО УСТАНОВКЕ И НАСТРОЙКЕ.	62
ПРИЛОЖЕНИЕ 13 ПРАВИЛА ПРИМЕНЕНИЯ ПРОСТОЙ ЭП В СИСТЕМЕ ДБО.....	62
ПРИЛОЖЕНИЕ 14 АКТ О ПЕРЕДАЧЕ МИКРО-КОМПЛЕКТА ПОДКЛЮЧЕНИЯ	65

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем документе применяются следующие термины и определения к ним:

АРМ Системы ДБО	автоматизированное рабочее место (АРМ) – совокупность компонентов Системы ДБО устанавливаемых на всех рабочих станциях Клиента
Банк	Банк «Возрождение» (ПАО)
Владелец сертификата ключа проверки электронной подписи (Владелец СКП ЭП)	лицо, которому в установленном Федеральным законом от 06.04.2011 № 63-ФЗ "Об электронной подписи" порядке выдан сертификат ключа проверки электронной подписи
Вредоносное программное обеспечение (ПО), вредоносный код	компьютерная программа, предназначенная для внедрения в автоматизированные Системы, ПО, средства вычислительной техники, телекоммуникационное оборудование Банка и (или) его Клиентов, приводящего к уничтожению, созданию, копированию, блокированию, модификации и (или) передаче информации (в том числе защищаемой в соответствии с пунктом 2.1 Положения Банка России от 09.06.2012 № 382-П «Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»), а также к созданию условий для такого уничтожения, создания, копирования, блокирования, модификации и (или) передачи
Выписка из лицевого счета	итоговый отчет об операциях по банковскому счету Клиента, совершенных в течение операционного дня, представляемый Банком Клиенту после завершения всех операций по счету и завершения операционного дня в форме ЭД либо на бумажном носителе в случае получения письменного заявления Клиента о предоставлении ему дубликата выписки и копий подтверждающих документов на бумажном носителе
Запрос на СКП ЭП	электронный документ, сформированный Клиентом с использованием Системы ДБО, подписанный электронной подписью Клиента, содержащий ключ проверки ЭП, предназначенный для передачи в УЦ для создания СКП ЭП
Заявление	один из следующих документов, оформленных на бумажном носителе: Заявление о присоединении к Регламенту Удостоверяющего центра и Правилам пользования Системой ДБО (Приложение 1 к настоящим Правилам) или Заявление на предоставление комплексного обслуживания Клиентов – юридических лиц, индивидуальных предпринимателей и лиц, занимающихся частной практикой, в Банке «Возрождение» (ПАО) (далее – Заявление на предоставление комплексного обслуживания) по форме Банка.
Клиент	юридическое лицо (в том числе кредитная организация), индивидуальный предприниматель, физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой, которое заключило с Банком договор о банковском обслуживании
Ключ электронной подписи (ключ ЭП)	уникальная последовательность символов, предназначенная для создания электронной подписи

Ключ проверки электронной подписи (ключ проверки ЭП)	уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи
Комплект подключения	комплект программных и аппаратных средств с документацией, представляемый Банком Клиенту для подключения Клиента к Системе ДБО. Состав Комплекта подключения зависит от выбранной Клиентом подсистемы Системы BS-Client ДБО или Системы Correpts и описан в соответствующих разделах данных Правил
Криптографический профиль (криптопрофиль)	информация в Системе ДБО, содержащая сведения о пользователе Системы ДБО, определяющая права пользователя в Системе ДБО и используемая для идентификации Пользователя в Системе ДБО
Ключ простой ЭП	уникальная пара логин/пароль, вырабатываемая Банком и передаваемая Клиенту в PIN-конверте, однозначно связанная с уполномоченным лицом Клиента – владельцем простой ЭП. Каждый PIN-конверт с ключом простой ЭП маркируется уникальным ID (идентификатором)
Менеджер	работник Банка, ответственный за взаимодействие с Клиентом в рамках заключенного с ним Договором ДБО
Микро-комплект подключения	содержит только ключ простой ЭП. Используется в случаях предусмотренных п.12.3.11 настоящих Правил
Мошеннические действия	действия, квалифицируемые как «Мошенничество в сфере компьютерной информации» в соответствии со ст. 159.6. Уголовного кодекса Российской Федерации
Носитель ключевой и парольной информации (НКПИ)	носитель информации, предназначенный для записи, хранения, воспроизведения ключа ЭП (ключ ЭП и сертификат ключа проверки ЭП) в рамках Системы ДБО является средством ЭП
Плановая смена ключей	процедура смены ключа ЭП и СКП ЭП в связи с окончанием срока действия СКП ЭП. Включает создание ключа ЭП, Запроса на СКП ЭП Владелец СКП ЭП и выдачу нового СКП ЭП Владелецу
Произвольный документ	электронный документ свободного содержания, для которого в Системе ДБО в соответствующих разделах не предусмотрен шаблон для составления и передачи документа в Банк Клиентом
Представитель Клиента	лицо, действующее от имени Клиента в силу полномочия, основанного на доверенности, указании закона, либо акте уполномоченного государственного органа или органа местного самоуправления
Промежуточный отчет об операциях по счету	ЭД, содержащий сведения об операциях по банковскому счету Клиента, отправляемый Банком Клиенту по его запросу в течение операционного дня. Не является итоговым отчетом по операциям
Регламент Удостоверяющего центра Банка «Возрождение» (ПАО) (Регламент)	утвержденный Правлением Банка и введенный в действие документ, определяющий условия предоставления и правила пользования услугами УЦ

Специальный голографический знак (СГЗ)	специальный защитный знак в виде наклейки, 6-го класса защиты. Используется Банком для обеспечения режима «Коммерческой тайны» при передаче Клиенту ключа простой ЭП
Сертификат ключа проверки электронной подписи (СКП ЭП)	электронный документ или документ на бумажном носителе, выданный УЦ, подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи
Список аннулированных (отозванных) сертификатов (СОС)	электронный документ с ЭП уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров СКП ЭП, которые на момент времени формирования списка были отозваны или действие которых было приостановлено
Средства криптографической защиты информации (СКЗИ), шифровальные (криптографические) средства	аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства, реализующие алгоритмы криптографического преобразования информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче
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
Технологический ключ для подсистемы Клиент-Банк Системы BS-Client	соответствует технологическому СКП ЭП и предназначен для 2-х факторной авторизации Клиента при первичном входе в Систему и выработки электронной подписи электронного сообщения с использованием СКЗИ при отправке Клиентом в Банк запроса на выпуск первого рабочего СКП ЭП
Технологический СКП ЭП для подсистемы Клиент-Банк Системы BS-Client	соответствует технологическому ключу и предназначен для 2-х факторной авторизации Клиента при первичном входе в Систему и проверки Банком электронной подписи электронного сообщения с использованием СКЗИ при и отправке Клиентом в Банк запроса на выпуск первого рабочего СКП ЭП
Технологический ключ для Системы Correpts	соответствует технологическому СКП ЭП и предназначен для 2-х факторной авторизации Клиента при первичном входе в Систему, выработки электронной подписи электронного сообщения с использованием СКЗИ при отправке Клиентом в Банк запроса на выпуск первого рабочего СКП ЭП, а так же для выработки электронной подписи электронного сообщения с использованием СКЗИ при отправке Клиентом в Банк Акта об оказании услуг по выпуску первого рабочего СКП ЭП
Технологический СКП ЭП для Системы Correpts	соответствует технологическому ключу и предназначен для 2-х факторной авторизации Клиента при первичном входе в Систему, проверки Банком электронной подписи электронного сообщения с использованием СКЗИ при отправке Клиентом в Банк запроса на выпуск первого рабочего СКП ЭП, а так же для проверки Банком электронной подписи электронного сообщения с использованием СКЗИ при отправке Клиентом в Банк Акта об оказании услуг по выпуску первого рабочего СКП ЭП
Удостоверяющий центр	Банк «Возрождение» (ПАО)

(УЦ)	
Централизованная система дистанционного банковского обслуживания Банка «Возрождение» (ПАО) (Система)	<p>корпоративная информационная система дистанционного банковского обслуживания представляет собой комплекс программно-технических средств и организационных мероприятий для создания, защиты, передачи и обработки ЭД с использованием информационно-телекоммуникационной сети «Интернет».</p> <p>Владельцем и Оператором Системы ДБО является Банк.</p> <p>В Банке эксплуатируются следующие Системы ДБО:</p> <ol style="list-style-type: none"> 1. Система ДБО «BS-Client» (Система BS-Client). В Систему BS-Client входят следующие подсистемы: <ol style="list-style-type: none"> а) подсистема Интернет-Клиент, доступ к которой осуществляется с использованием сайта Банка в сети "Интернет"; б) подсистема Клиент-Банк, доступ к которой осуществляется с использованием специального программного обеспечения, устанавливаемого на рабочие станции Клиента; 2. Система ДБО «BSS CORREQTS Corporate» (Система Correqts). В Систему Correqts входят следующие подсистемы: <ol style="list-style-type: none"> а) подсистема Интернет-Клиент, предоставляет Клиентам банка доступ к Системе Correqts посредством технологии "тонкий клиент" – Клиенты работают с Системой с ПК через поддерживаемые браузеры;
Электронный документ (ЭД)	документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием средств вычислительной техники или мобильных устройств, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах и мобильных приложениях
Электронный документооборот (ЭДО)	электронное взаимодействие между Клиентом и Банком, в соответствии с настоящими Правилами
Электронное сообщение (ЭС)	служебный ЭД, автоматически создаваемый системой ДБО
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
SafeTouch	средство, которое путём визуализации и контроля документов, отправляемых на подпись в смарт-карту или токен в доверенной среде, позволяет защитить денежные средства Клиента от удаленных интернет-атак на систему ДБО
SMS/ e-mail информирование	дополнительная услуга по направлению Клиенту на телефонный номер или на адрес электронной почты Клиента соответствующего уведомления, связанного с исполнением Банком и/или Клиентом Договора ДБО и/или иного договора о банковском обслуживании
Заявление	один из следующих документов, оформленных на бумажном носителе: Заявление о присоединении к Регламенту Удостоверяющего центра и Правилам пользования Системой ДБО

	(Приложение 1 к настоящим Правилам) или Заявление на предоставление комплексного обслуживания Клиентов – юридических лиц, индивидуальных предпринимателей и лиц, занимающихся частной практикой, в Банке «Возрождение» (ПАО) (далее – Заявление на предоставление комплексного обслуживания) по форме Банка.
--	--

2. ПРЕДМЕТ РЕГУЛИРОВАНИЯ

2.1. Настоящие Правила пользования централизованной системой дистанционного банковского обслуживания Банка «Возрождение» (ПАО) (далее – Правила) определяют условия Договора дистанционного банковского обслуживания (далее – Договор ДБО), в том числе устанавливают принципы и порядок обслуживания Клиентов с использованием Системы ДБО в целях предоставления услуг по дистанционному банковскому обслуживанию, осуществления ЭДО между Банком и Клиентом (далее – Стороны), права и обязанности Сторон в целях обеспечения ЭДО с использованием Системы ДБО при проведении расчетных операций, а также обмене ЭС и ЭД между Банком и Клиентом в соответствии с договорами Сторон.

2.2. Заключение Договора ДБО осуществляется в соответствии со ст. 428 ГК РФ путем присоединения Клиента к настоящим Правилам и Регламенту на основании поданного в Банк Заявления на бумажном носителе. Клиент полностью и безусловно присоединяется к Регламенту и Правилам, принимает порядок и условия ЭДО в Системе ДБО. Права и обязанности Сторон по Договору ДБО возникают с момента проставления Банком на Заявлении отметки о принятии (акцепте) Заявления.

2.3. Банк вправе без объяснения причин отказать Клиенту в принятии (акцепте) Заявления (заключении Договора ДБО).

2.4. Настоящие Правила составлены в соответствии с требованиями действующего законодательства РФ в области использования электронной подписи, в том числе Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее – Закон об электронной подписи).

2.5. Требования к содержанию электронных документов, порядок их исполнения не являются предметом регулирования настоящих Правил.

2.6. Положения настоящих Правил применяются Сторонами при использовании в зависимости от выбора Клиента подсистем Системы BS-Client или Системы Correpts, если иное не предусмотрено законодательными или иными правовыми актами РФ, включая нормативные акты Банка России.

2.7. Если специально не оговорено, что действие конкретного пункта Правил распространяется исключительно на Систему BS-Client либо на Систему Correpts, то считается, что действие пункта Правил распространяется на обе Системы ДБО, включая их подсистемы.

3. РЕГУЛИРОВАНИЕ ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ, ПОРЯДОК ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ В СИСТЕМЕ ДБО

3.1. ЭДО в Системе ДБО регулируется действующим законодательством РФ, нормативными актами Банка России и настоящими Правилами. В случае изменения законодательства Российской Федерации Правила до момента их изменения Банком применяются в части, не противоречащей требованиям законодательства Российской Федерации.

3.2. Все ЭД, передаваемые в Системе подписываются усиленной квалифицированной ЭП.

3.3. В случае невозможности использования усиленной квалифицированной ЭП в соответствии с п. 3.2, используется усиленная неквалифицированная ЭП, соответствующая ГОСТ Р 34.10-2001 / ГОСТ Р 34.10-2012. Квалифицированные СКП ЭП, применяемые в Системе, заменяются на СКП ЭП соответствующие неквалифицированной ЭП ГОСТ Р 34.10-2001 / ГОСТ Р 34.10-2012.

3.4. В случае невозможности использования усиленной квалифицированной ЭП в соответствии с п 3.2 и усиленной неквалифицированной ЭП по ГОСТ Р 34.10-2001 / ГОСТ Р 34.10-2012 в соответствии с п. 3.3, используется усиленная неквалифицированная ЭП с использованием алгоритма подписи sha2RSA. СКП ЭП, применяемые в Системе, заменяются на СКП ЭП соответствующие алгоритму подписи sha2RSA.

3.5. Если применение усиленной ЭП в соответствии с пунктами 3.2 – 3.4 не возможно, применяется простая ЭП в соответствии с Правилами применения простой ЭП ([Приложение 13](#) к настоящим Правилам).

3.6. Стороны признают, что ЭД, подписанные в Системе в соответствии с пунктами 3.3 – 3.5 настоящих Правил, признаются равнозначными совершенным в письменной форме на бумажном носителе, подписанными собственноручной подписью и заверенными печатью (если необходимо). Юридическая значимость указанных документов не может быть оспорена только на том основании, что они совершены в электронном виде.

3.7. Используемые в Системе ДБО средства криптографической защиты информации (СКЗИ) имеют подтверждение соответствия требованиям ГОСТ и требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС1, требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011г. № 796, установленным в соответствии с положениями Федерального закона «Об электронной подписи» от 06.04.2011 № 63-ФЗ (за исключением средств ЭП, применяющих алгоритм подписи sha2RSA). Их применение в Системе ДБО признается Сторонами достаточным для обеспечения конфиденциальности, целостности, авторства и неотказуемости передаваемой между Сторонами информации и невозможности ее фальсификации после момента её подписания.

3.8. Клиент осознает и принимает на себя все риски, связанные с использованием Системы ДБО в сети Интернет, которая является незащищенным каналом связи.

3.9. В случае использования Клиентом НКПИ в форм-факторе смарт-карта снижение рисков, связанных с использованием подсистем Интернет-Клиент или Клиент-банк Системы BS-Client, дополнительно обеспечивается средством визуализации ЭП (например, SafeTouch).

4. ПОРЯДОК И УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ ДОСТУПА КЛИЕНТУ К ОСУЩЕСТВЛЕНИЮ ДОКУМЕНТООБОРОТА В СИСТЕМЕ ДБО

4.1. Клиенту предоставляется доступ к работе в корпоративной информационной Системе ДБО после выполнения Сторонами совокупности следующих действий:

- а) представления Клиентом и одобрения Банком пакета документов, необходимых для заключения Договора ДБО и выпуска СКП ЭП Представителям Клиента в соответствии с разделом [12.1](#) настоящих Правил;
- б) оплаты Клиентом комиссии в соответствии с разделом 11 настоящих Правил;
- в) создания Банком и последующей передачи Клиенту комплекта подключения для первичной регистрации в Системе ДБО;
- г) подписания Сторонами на бумажном носителе Акта о передаче программного обеспечения и ключей ЭП, необходимых для подключения к Системе ДБО по форме [Приложения 6](#) к настоящим Правилам либо подтверждения Клиентом факта получения программного обеспечения в составе Заявления на предоставление комплексного обслуживания;

- д) установки Клиентом на свои рабочие станции необходимых для подключения к соответствующей подсистеме Системы ДБО аппаратных средств и специального программного обеспечения, представленного Банком Клиенту;
- е) приведения Клиентом своих рабочих станций в соответствие требованиям Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ Системы ДБО ([Приложение 7](#) к настоящим Правилам);
- ж) оформления Сторонами Акта либо подписания Клиентом Анкеты о соблюдении Клиентом требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ Системы ДБО ([Приложение 8](#) или [Приложение 9](#) к настоящим Правилам). Указанные документы не представляются в случае, если Заявление подано в составе Заявления на предоставление комплексного обслуживания;
- з) создания Клиентом своих рабочих ключей электронной подписи, получения рабочих СКП ЭП и подписания Клиентом Акта об оказании услуг по выпуску сертификата ключа проверки электронной подписи ([Приложение 10](#) к настоящим Правилам).

4.2. Банк приостанавливает доступ Клиента к Системе ДБО на основании полученного от Клиента и составленного в произвольной форме уведомления об отказе от использования Системы ДБО или по инициативе Банка при нарушении либо подозрении о нарушении Клиентом порядка использования Системы ДБО в соответствии с настоящими Правилами в следующих случаях:

непредставления информации и/или документов, либо представления ненадлежащим образом оформленных документов согласно требованиям любых договоров, заключенных между Клиентом и Банком;

невыполнения Клиентом обязанностей, предусмотренных разделом 11 настоящих Правил;

возникновения у работников Банка сомнений в законном характере операций, совершаемых с использованием Системы ДБО или подозрений, что для подписи документов используются скомпрометированные ключи электронной подписи или документы подписываются не Представителями Клиента;

не представлена информация о целях финансово-хозяйственной деятельности, финансового положения и деловой репутации Клиента, а также документы, подтверждающие представленные Клиентом сведения;

не представлены документы, необходимые для идентификации Клиента и его Представителей, бенефициарных владельцев, обновления сведений о Клиенте и его Представителях, бенефициарных владельцах, а также для установления и идентификации выгодоприобретателей по проводимым Клиентом операциям;

не представлена информация и/или документы, необходимые для фиксирования информации об проводимых/ранее проведенных операциях/сделках, раскрывающие экономический смысл этих операций/сделок и подтверждающие законность их проведения;

Банк располагает информацией об отсутствии Клиента – юридического лица по адресу, указанному в Едином государственном реестре юридических лиц;

у Банка возникают подозрения, что Клиент осуществляет операции в целях легализации (отмывания) доходов, полученных преступным путём, или финансирования терроризма;

в иных случаях когда, по мнению работников Банка, использование Системы ДБО может нанести вред Клиенту или Банку;

в случае просрочки Клиентом более чем, на 30 календарных дней уплаты комиссий за услуги Банка по дистанционному банковскому обслуживанию (в том числе по причине отсутствия на счете Клиента денежных средств или невозможности проведения по счету операций по списанию комиссий Банка) до момента погашения Клиентом задолженности по оплате комиссий.

4.3. В случае отсутствия со стороны Клиента сеансов связи с Банком в течение более чем трех месяцев подряд Банк приостанавливает доступ Клиента к Системе ДБО. Для возобновления доступа к Системе ДБО Клиент должен представить в Банк письменное заявление в свободной форме с просьбой возобновить работу по Системе ДБО.

4.4. Клиент вправе в одностороннем порядке отказаться от использования Системы ДБО (расторгнуть Договор ДБО) в любое время при условии полной оплаты оказанных услуг по дистанционному банковскому обслуживанию.

4.5. Банк вправе в одностороннем порядке расторгнуть Договор ДБО в следующих случаях:

при использовании Клиентом Системы ДБО не по прямому назначению;

при нарушении Клиентом, путем использования Системы ДБО, законодательства РФ;

при непоступлении от Клиента оплаты за дистанционное банковское обслуживание (в том числе по причине отсутствия на счете Клиента денежных средств или невозможности проведения по счету операций по списанию комиссий Банка) в течение более трех месяцев;

при отсутствии со стороны Клиента сеансов связи в Системе ДБО в течение более одного календарного года;

при неисполнении или ненадлежащем исполнении Клиентом обязанностей, предусмотренных Правилами и Регламентом;

при неустранении Клиентом оснований для приостановления использования Системы ДБО, указанных в п. 4.2 настоящих Правил;

в иных случаях по усмотрению Банка.

4.6. Клиент должен уведомить Банк о своем желании приостановить использование Системы ДБО/расторгнуть Договор ДБО в соответствии с пп. 4.2. и 4.4 настоящих Правил в письменном виде не менее чем за пять рабочих дней до даты предполагаемого приостановления использования Системы ДБО/расторжения Договора ДБО. Уведомление может быть направлено посредством Системы ДБО.

4.7. Банк уведомляет Клиента о приостановлении использования Системы ДБО в соответствии с пп. 4.2 и 4.3 настоящих Правил путем направления сообщения в момент приостановления.

Банк уведомляет Клиента о расторжении Договора ДБО в соответствии с п. 4.5 настоящих Правил путем направления сообщения не позднее, чем за 5 (пять) рабочих дней до дня расторжения посредством направления сообщения по Системе ДБО, а если это невозможно – на бумажном носителе. При этом если в сообщении Банка не указано иное Договор ДБО прекращается в день, следующий за пятым рабочим днем после направления Банком сообщения о его расторжении.

4.8. Действие Договора ДБО прекращается в связи с истечением его срока с прекращением (расторжением) последнего договора между Банком и Клиентом, в рамках которого производился электронный документооборот в соответствии с настоящими Правилами.

5. ПОРЯДОК ВСТУПЛЕНИЯ В СИЛУ НАСТОЯЩИХ ПРАВИЛ, ВНЕСЕНИЯ В НИХ ИЗМЕНЕНИЙ И ПРЕКРАЩЕНИЯ ДЕЙСТВИЯ

5.1. Настоящие Правила, включая все Приложения, утверждаются Правлением Банка и публикуются на сайте Банка – <http://www.vbank.ru>.

5.2. Изменения и дополнения в настоящие Правила вносятся Банком в одностороннем порядке и утверждаются Правлением Банка. Правление Банка также определяет сроки и порядок вступления в силу изменений и дополнений в Правила.

5.3. Настоящие Правила прекращают свое действие на основании решения Правления Банка. Прекращение действия Правил и Приложений к ним не влияет на юридическую значимость ЭД, которыми Стороны обменивались до прекращения действия Правил и Приложений к ним.

6. ПОРЯДОК УВЕДОМЛЕНИЯ О ВНЕСЕНИИ ИЗМЕНЕНИЙ В ПРАВИЛА

6.1. Изменения и дополнения в настоящие Правила и Приложения к ним, а также сроки и порядок вступления в силу вносимых в Правила изменений и дополнений публикуются на сайте Банка – <http://www.vbank.ru> и, если иное не предусмотрено решением Правления Банка, считаются доведенными до сведения Клиентов и вступившими в силу по истечении семи календарных дней с даты размещения такой публикации.

6.2. Клиент имеет право запрашивать копии текстов Правил и Приложений к ним, а также копии изменений и дополнений к Правилам на бумажном носителе. Указанные в настоящем пункте документы представляются Банком Клиенту в течение 15 (пятнадцати) рабочих дней после получения соответствующего запроса.

7. ОБЩИЕ ПОЛОЖЕНИЯ

7.1. ЭДО в Системе ДБО регулируется действующим законодательством РФ, нормативными актами Банка России, Регламентом и настоящими Правилами.

7.2. Банк обеспечивает эксплуатацию СКЗИ в Системе ДБО с обязательным использованием в качестве носителей ключей ЭП НКПИ. Представляемые Банком НКПИ являются персональным средством аутентификации и хранения данных.

7.3. Применяемые в Системе ДБО СКЗИ и программные средства работы с СКП ЭП в процессе их использования автоматически выполняют контроль срока действия СКП ЭП. Участник Системы ДБО не может подписать ЭД своей ЭП / проверить корректность ЭП или произвести зашифрование / расшифрование информации в текущий момент времени, если к этому времени истек срок действия его СКП ЭП.

Запрещается использовать один и тот же НКПИ для хранения ключей ЭП разных Представителей Клиента.

7.4. Банком и Клиентом используются в Системе ДБО только сертифицированные ФСБ России СКЗИ, представляемые Банком Клиенту (за исключением средств ЭП, применяющих алгоритм подписи sha2RSA). Формируемые Клиентом ключи ЭП имеют признак – «не экспортируемые». Применяемые в Системе ДБО сертифицированные СКЗИ обеспечивают невозможность копирования (экспорта) ключа ЭП с одного НКПИ на другой.

7.5. Создание первых ключей ЭП Клиента производится работником Банка или самостоятельно Клиентом/Представителем Клиента – будущими владельцами СКП ЭП

в соответствии п.п. 9.4, 9.5, 9.7 Регламента. Создание последующих ключей ЭП производится самостоятельно владельцами СКП ЭП.

7.6. Стороны признают, что используемые в Системе ДБО средства ЭП обеспечивают достаточную конфиденциальность ЭДО и позволяют идентифицировать владельца СКП ЭП, а также позволяют установить факт изменения подписанного ЭД после момента его подписания.

7.7. Клиент обязуется:

использовать на своих рабочих станциях и/или мобильных устройствах, применяемых для подключения к подсистемам Системы ДБО только лицензионное ПО;

соблюдать требования лицензионного соглашения на СКЗИ;

ежедневно заходить в систему ДБО для ознакомления с направленной ему информацией.

7.8. Услуги Банка по изготовлению технологических ключей подписи, СКП ЭП, предоставлению СКЗИ, НКПИ и иных программно-технических средств, а также услуги, связанные с организацией ЭДО в соответствии с настоящими Правилами, являются платными. Размер платы за данные услуги определяется в соответствующих тарифах, утверждаемых Банком в рамках Положения о Тарифной политике Банка «Возрождение» (ПАО), опубликованных на сайте Банка <http://www.vbank.ru>.

7.9. В процессе эксплуатации АРМ Системы ДБО Клиент обязуется выполнять требования Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации Клиентом АРМ Системы ДБО (Приложение 7 к настоящим Правилам)¹. Подтверждение выполнения Клиентом требований Руководства по обеспечению информационной безопасности должно быть оформлено Актом о соблюдении Клиентом требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ Системы ДБО (Приложение 7 к настоящим Правилам) либо Анкетой о соблюдении Клиентом требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ Системы ДБО (Приложение 8 к настоящим Правилам) либо подписанием Клиентом пункта 3 Заявления на предоставление комплексного обслуживания. При невыполнении или неполном выполнении Клиентом обязательных требований Руководства по обеспечению информационной безопасности Клиент принимает на себя риски возможных потерь (ущерба).

Банк не возвращает сумму операции, совершенной с использованием Системы ДБО без согласия Клиента, в случае, если Клиентом не были соблюдены требования Руководства по обеспечению информационной безопасности (Приложение 7 к настоящим Правилам) и другие условия Правил в части использования Клиентом электронной подписи и средств электронной подписи.

7.10. Владельцами СКП ЭП в Системе ДБО являются физические лица – уполномоченные Представители Клиента и Банка.

Полномочия владельцев ключа ЭП и СКП ЭП Клиента подтверждаются карточкой с образцами подписей и оттиска печати², иными предусмотренными действующим законодательством документами, а также выданными данным лицам доверенностями для работы с СКП ЭП (при необходимости).

Полномочия владельцев ключа ЭП и СКП ЭП сотрудников Банка подтверждаются Приказами о назначении на должность.

¹ Далее – Руководство по обеспечению информационной безопасности.

² Далее – КОПОП.

Присоединяясь к настоящим Правилам, Клиент уполномочивает любое лицо, указанное в Перечне договоров (Приложение 11 к настоящим Правилам) и/или в Заявлении на предоставление комплексного обслуживания и наделенное правами доступа к Системе ДБО с Полномочиями «Подпись 1», «Подпись 2», «Единственная подпись» заключать с Банком посредством обмена по Системе ДБО электронными документами, подписанными электронной подписью, соглашения об изменении условий Договора ДБО и его расторжении, иные договоры (за исключением кредитных и обеспечительных договоров), в том числе договоры об использовании Сторонами нового(-ых) вида(-ов) электронной подписи, устанавливающие случаи признания Сторонами электронных документов, подписанных электронной подписью (в т.ч. усиленной неквалифицированной подписью), равнозначными документам на бумажных носителях, подписанным собственноручной подписью и скрепленным печатью, а также соглашения о внесении изменений в договоры, заключенные между Банком и Клиентом (за исключением кредитных и обеспечительных договоров).

7.11. ЭДО осуществляется в связи с исполнением договоров Сторон, указанных в Перечне договоров (Приложение 11 к настоящим Правилам) / Договора комплексного банковского обслуживания и всех договоров, заключенных в его рамках (если Заявление подано в составе Заявления на предоставление комплексного обслуживания) / Договора ДБО.

7.12. При изменении списка договоров, состава и полномочий Представителей Клиента, а также состава и/или наименования ЭД, передаваемых со стороны Клиента или передаваемых со стороны Банка в соответствии с разделом 8.5 настоящих Правил, Клиент представляет новый Перечень договоров и Список лиц, имеющих доступ к Системе ДБО ([Приложение 11](#) к настоящим Правилам). Ключи ЭП и соответствующие им СКП ЭП изготавливаются только новым Представителям Клиента в случае добавления их в Список лиц, имеющих доступ к Системе ДБО. Для Представителей Клиента, полномочия которых в соответствии с новым Списком лиц прекращены, выполняются мероприятия по аннулированию СКП ЭП в соответствии с разделом 12.5 настоящих Правил, если к моменту прекращения полномочий не истек срок действия данного СКП ЭП.

7.13. Клиент передает Банку Список лиц, имеющих доступ к Системе ДБО с указанием полномочий и оснований для доступа к Системе ДБО. На каждое лицо, указанное в Списке лиц, имеющих доступ к Системе ДБО, Клиентом должен быть представлен в Банк комплект документов в соответствии с формами, указанными в Приложениях к настоящим Правилам. Список лиц может быть передан Клиентом по форме Приложения 11 к настоящим Правилам или в составе Заявления на предоставление комплексного обслуживания.

При представлении новой карточки с образцами подписей и оттиском печати (КОПОП) в случае, если изменения относятся к лицам, имеющим доступ к Системе ДБО, или при предоставлении Клиентом права доступа к Системе ДБО новым лицам Клиент одновременно с новой КОПОП представляет Банку новый Список лиц, имеющих доступ к Системе ДБО (Приложение 11 к настоящим Правилам), и документы, подтверждающие полномочия Представителей, указанных в Списке лиц, если такие документы не были представлены в Банк ранее и их срок действия не истек. Банк предоставляет доступ к Системе ДБО в соответствии с предоставленными полномочиями только лицам, указанным Клиентом в новом Списке лиц.

7.14. Банк обеспечивает хранение СКП ЭП Клиентов в форме ЭД и возможность получения СКП ЭП Клиентов в форме ЭД в течение всего срока действия СКП ЭП.

7.15. Для оповещения Клиента о принятии к исполнению Банком ЭД «Платежное поручение» используется подсистема «Сервер нотификации».

В адрес Клиента, подключившего дополнительную услугу SMS/e-mail информирования, Банк направляет соответствующее уведомление на номер

мобильного телефона и/или на адрес электронной почты Клиента, указанный в Заявлении на установку (настройку) Системы ДБО BS-Client и подключение/отключение услуги «SMS/e-mail информирование» (Приложение 5 к настоящим Правилам) или в Заявлении на предоставление комплексного банковского обслуживания в зависимости от того, на основании какого Заявления Клиенту была подключена указанная услуга.

Для оповещения Клиента о принятии к исполнению Банком ЭД «Платежное поручение» в адрес Клиента, подключившего дополнительную услугу СМС информирования на основании Заявления на предоставление комплексного обслуживания Банк направляет соответствующее уведомление на номер мобильного телефона, указанный в таком Заявлении.

7.16. Подключение/отключение Услуги «SMS/e-mail информирование» или Услуги СМС информирование проводится только в том офисе Банка, в котором Клиент оформил Заявление. SMS-сообщения и/или e-mail сообщения будут направляться только по тем банковским счетам, которые подключены к Системе ДБО.

7.17. Итоговой выпиской из лицевого счета, подключенного к Системе ДБО, является выписка, направленная Банком Клиенту не ранее рабочего дня, следующего за днем совершения операций по счету.

7.18. Подключение банковского счета Клиента к Системе ДБО освобождает Банк от обязанности представления выписок по счетам с приложением подтверждающих операции документов на бумажном носителе.

7.19. В случае необходимости уточнения платежных инструкций при переводе денежных средств на основании распоряжения Клиента, поступившего по Системе ДБО, Банк имеет право, но не обязанность, обратиться к Клиенту за дополнительной информацией.

7.20. Банк извещает Клиента в рабочие дни не менее чем за 24 часа о предстоящем проведении профилактических и/или ремонтных работ, которые будут осуществляться в сроки, указанные в извещении.

7.21. Стороны признают в качестве единой шкалы времени при работе в Системе ДБО московское поясное время. Контрольным является время системных часов аппаратных средств Банка.

7.22. Банк гарантирует Клиенту тайну сведений о Клиенте, о счетах и операциях Клиента. Информация и справки о Клиенте, состоянии счетов, операциях Клиента могут быть предоставлены третьим лицам только в случаях и в порядке, предусмотренных действующим законодательством Российской Федерации, настоящими Правилами, включая приложения к ним.

Присоединяясь к настоящим Правилам, Клиент предоставляет Банку право передавать любую информацию, полученную от Клиента, Представителей Клиента, а также полученную Банком на иных законных основаниях в целях заключения и в процессе исполнения Договора ДБО, а также иных договоров, заключенным между Банком и Клиентом, в соответствии с которыми Стороны обмениваются электронными документами согласно настоящим Правилам, в том числе информацию, составляющую банковскую тайну, включая персональные данные Клиента – индивидуального предпринимателя, физического лица, занимающегося частной практикой, (далее – Конфиденциальная информация) в случаях, когда Конфиденциальная информация разглашается:

- в соответствии с законодательством Российской Федерации;
- Банком с письменного согласия Клиента;
- следующим лицам, которые должны принять на себя обязательство, в свою очередь, соблюдать конфиденциальность, что обеспечивается Банком:

- должностным лицам и служащим Банка в связи с их деятельностью;
 - независимым консультантам, экспертам и советникам, привлекаемым Банком в рамках исполнения Договора ДБО либо реализации своих прав по Договору ДБО;
- налоговым органам при проведении мероприятий налогового контроля;
 - государственным органам, включая Банк России, при осуществлении ими полномочий, предусмотренных законодательством Российской Федерации;
 - аудиторским организациям и индивидуальным аудиторам, осуществляющим аудит и/или оказывающим Банку сопутствующие аудиту услуги;
 - третьим лицам, которым Конфиденциальная информация стала известной до того, как Банк ее разгласил;
 - при обращении в судебные и следственные органы;
 - организациям, осуществляющим перевозку, сканирование, хранение, в том числе архивное, и/или уничтожение документов;
 - лицам, входящим в один банковский холдинг с Банком / аффилированным лицам Банка.

7.23. Присоединяясь к настоящим Правилам, Клиент, являющийся индивидуальным предпринимателем/физическим лицом, занимающимся частной практикой, в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» свободно, своей волей и в своем интересе дает согласие (далее – Согласие) Банку в лице его уполномоченных работников и иных лиц, привлекаемых Банком, совершать с персональными данными (в т.ч. биометрическими персональными данными), содержащимися в представленных Клиентом Банку документах в соответствии с настоящими Правилами и приложениями к ним и/или полученных Банком иными законными способами, следующие действия (с использованием и без использования средств автоматизации): сбор; запись; систематизация; накопление; хранение; уточнение (обновление, изменение); извлечение; использование; передача (распространение, предоставление, доступ), в том числе передача уполномоченным работникам Банка, лицам, входящим в один банковский холдинг с Банком/ аффилированным лицам Банка; обезличивание; блокирование; удаление; уничтожение персональных данных (далее – «обработка»), в целях заключения и исполнения Договора ДБО, договоров, заключенных между Банком и Клиентом, в соответствии с которыми Стороны обмениваются электронными документами согласно настоящим Правилам, в том числе в целях осуществления банковских операций и предоставления всех видов банковских услуг, заключения и исполнения иных договоров с Банком, а также осуществления хранения, в том числе в электронном виде, и защиты Конфиденциальной информации (в том числе персональных данных).

Согласие, выраженное в настоящем пункте Правил, действует до прекращения Договора ДБО, а также в течение следующих 5 лет. По истечении указанного срока действие согласия считается продленным на следующие 5 лет, при условии отсутствия у Банка сведений о его отзыве.

В случае отзыва Клиентом данного согласия на обработку персональных данных Клиента, Банк обязан прекратить обработку персональных данных Клиента и уничтожить их после прекращения Договора ДБО, за исключением персональных данных, дальнейшая обработка которых является обязанностью Банка, установленной законодательством Российской Федерации. При этом дополнительное уведомление Клиента Банком об уничтожении персональных данных предоставляется Банком по запросу Клиента.

7.24. Присоединяясь к настоящим Правилам, Клиент в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» поручает Банку в лице его уполномоченных работников и иных лиц, привлекаемых Банком, совершать с персональными данными (в т.ч. биометрическими персональными данными), содержащимися в представленных Клиентом Банку документах в соответствии с настоящими Правилами и приложениями к ним и/или полученных Банком иными законными способами, следующие действия (с использованием и без использования средств автоматизации): сбор; запись; систематизация; накопление; хранение; уточнение (обновление, изменение); извлечение; использование; передача (распространение, предоставление, доступ), в том числе передача уполномоченным работникам Банка, лицам, входящим в один банковский холдинг с Банком/аффилированным лицам Банка; обезличивание; блокирование; удаление; уничтожение персональных данных (далее – «обработка»), в целях исполнения Договора ДБО, а также осуществления хранения, в том числе в электронном виде, и защиты Конфиденциальной информации (в том числе персональных данных).

Клиент подтверждает, что им получено письменное согласие субъектов персональных данных, чьи персональные данные (в т.ч. биометрические персональные данные) содержатся в представленных Клиентом Банку документах, полученных Банком в соответствии с настоящими Правилами и/или иными законными способами, на обработку Банком, лицами, входящими в один банковский холдинг с Банком / аффилированными лицами Банка, этих персональных данных в целях исполнения Договора ДБО и осуществления хранения, в том числе в электронном виде, и защиты Конфиденциальной информации (в том числе персональных данных). Клиент обязуется передавать Банку документы, материалы, содержащие персональные данные, только при наличии согласия субъектов персональных данных, чьи персональные данные содержатся в таких документах, материалах. Обязанность по получению согласий субъектов персональных данных возложена на Клиента. Клиент несет все неблагоприятные последствия, связанные с неполучением Клиентом таких согласий.

Требования к защите обрабатываемых персональных данных, в т.ч. необходимые правовые, организационные и технические меры по защите персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения и иных неправомерных действий в отношении персональных данных определяются Банком самостоятельно с учетом требований ст. 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Присоединяясь к настоящим Правилам, Клиент подтверждает, что персональные данные (в т.ч. биометрические персональные данные), содержащиеся в представляемых Клиентом Банку документах, полученных Банком в соответствии с настоящими Правилами и/или иными законными способами, не является тайной частной жизни, личной и/или семейной тайной.

7.25. Стороны имеют право в порядке, предусмотренном Договором ДБО, в т.ч. настоящими Правилами, заключать с использованием Системы ДБО соглашения об использовании Сторонами нового(-ых) вида(-ов) электронной подписи и устанавливающие случаи признания Сторонами электронных документов, подписанных электронной подписью (в т.ч. усиленной неквалифицированной подписью), равнозначными документам на бумажных носителях, подписанным собственноручной подписью и скрепленных печатью, а также соглашения об изменении условий Договора ДБО и его расторжении, иные договоры (за исключением кредитных и обеспечительных договоров) между Банком и Клиентом, а также соглашения о внесении изменений в договоры, заключенные между Банком и Клиентом (за исключением кредитных и обеспечительных договоров).

Указанные в настоящем пункте договоры (соглашения), заключенные с использованием Системы ДБО, удовлетворяют требованиям совершения сделки в простой письменной форме в случаях, предусмотренных гражданским законодательством РФ, и влекут юридические последствия, аналогичные последствиям совершения сделок с физическим присутствием лица (взаимном присутствии лиц), совершающего (-их) сделку.

8. ЭЛЕКТРОННЫЙ ДОКУМЕНТ

8.1. Требования, предъявляемые к электронному документу

8.1.1. ЭД считается надлежащим образом оформленным, имеет юридическую силу и влечет предусмотренные действующим законодательством и соответствующим договором Сторон для данного документа правовые последствия, если он сформирован в Системе ДБО в соответствии с действующим законодательством, настоящими Правилами и Регламентом.

8.1.2. ЭД, оформленный с нарушением установленных п. 8.1.1 Правил, не считается электронным документом в соответствии с настоящими Правилами и не влечет никаких правовых последствий для Сторон.

8.2. Электронная подпись и шифрование электронного документа

8.2.1. ЭД считается подписанным уполномоченным лицом, если он подписан ключом ЭП, для которого УЦ Банка изготовлен СКП ЭП.

8.2.2. Замена ключей ЭП не влияет на статус ЭД, если он был подписан действующим на момент подписания ключом ЭП в соответствии с Регламентом и Правилами.

8.2.3. У каждого Представителя Стороны имеется СКП ЭП, с использованием которого он подписывает ЭД.

8.3. Подлинник электронного документа

8.3.1. ЭД может иметь неограниченное количество экземпляров.

8.3.2. Все экземпляры ЭД являются подлинниками данного ЭД.

ЭД не может иметь копий в электронном виде.

8.3.3. Подлинник ЭД считается не существующим в случаях если:

не существует ни одного учтенного Сторонами экземпляра данного ЭД и восстановление такого ЭД невозможно;

не существует способа установить подлинность ЭП, которой подписан данный электронный документ.

8.4. Копии электронного документа на бумажном носителе

8.4.1. Копии ЭД могут быть изготовлены (распечатаны) на бумажном носителе и должны быть заверены собственноручной подписью лица, уполномоченного Стороной, являющейся отправителем или получателем ЭД.

8.4.2. ЭД и его копии на бумажном носителе должны быть идентичными.

8.5. Электронные документы, используемые в Системе ДБО

8.5.1. ЭД, передаваемые со стороны Клиента, могут включать, в том числе, но не ограничиваясь:

документы, для которых установлен формат:

платежное поручение;

поручение на перевод валюты;
поручение на покупку валюты;
поручение на продажу валюты;
поручение на покупку одной валюты за другую иностранную валюту (конверсия валюты);
поручение на списание валюты с транзитного счета;
справка о валютных операциях;
справка о подтверждающих документах;
паспорт сделки по контракту;
паспорт сделки по кредитному договору;
заявление на оформление паспорта сделки;
заявление о переоформлении паспорта сделки;
заявление о закрытии паспорта сделки;
запрос выписки из лицевого счета³;
запрос на отзыв документа;
документы, для которых формат не установлен - произвольные документы в банк⁴.

В случае если формат ЭД не определен соответствующей экранной формой Системы ДБО, разрешается передавать ЭД в свободном формате.

Перечень и виды ЭД, передаваемые по Системе ДБО со стороны Клиента, могут меняться в зависимости от требований законодательства РФ, включая нормативные акты Банка России. Банк может вводить дополнительно новые виды ЭД в случае расширения функциональных возможностей Системы ДБО.

8.5.2. ЭД, передаваемые со стороны Банка, могут включать, в том числе, но не ограничиваясь:

выписки из лицевого счета (представляются только за предыдущие (завершенные) операционные дни); отчет по операциям по лицевому счету в российских рублях (представляется за текущий (незавершенный) операционный день)⁵;

подтверждение результатов обработки ЭД Клиента (квитанция банка);

справочник курсов валют;

справочник российских банков;

справочник Банки мира;

произвольные документы (письма Клиенту);

уведомление о поступлении иностранной валюты на транзитный валютный счет резидента;

³ Диапазон дат в «Запросе выписки из лицевого счета» не может превышать 3 рабочих дней.

В исключительных случаях на основании письменного заявления Клиента об увеличении диапазона дат по решению руководства филиала запрашиваемая выписка формируется Администратором ДБО и направляется в адрес Клиента.

⁴ Предназначенный для отправки в Банк текстового сообщения или присоединенного файла (файлов)

⁵ Направляется Банком Клиенту по запросу последнего в течение текущего операционного дня; не является итоговым отчетом по операциям; может отражать ошибочные сведения.

уведомление о поступлении валюты Российской Федерации на расчетный счет резидента;

платежное поручение в формате МТ103⁶.

Перечень и виды ЭД, передаваемые по Системе ДБО со стороны Банка, могут меняться в зависимости от требований законодательства РФ, включая нормативные акты Банка России. Банк может вводить дополнительно новые виды ЭД в случае расширения функциональных возможностей Системы ДБО.

8.5.3. Клиент признает, что в случае его отказа от подключения услуги «SMS/e-mail информирование», Услуги СМС информирование направление Банком выписки по счету в электронном виде по Системе ДБО в соответствии с пп. 7.17 и 8.5.2 настоящих Правил является надлежащим исполнением Банком обязанности по уведомлению Клиента о совершении операции с использованием электронного средства платежа в соответствии со ст.9 Федерального закона от 27.06.2011 г. №161-ФЗ «О национальной платежной Системе».

8.5.4. Клиент признает, что отказ от подключения Услуги «SMS/e-mail информирование», Услуги СМС информирование предоставляемой Банком в соответствии с пп. 7.15 настоящих Правил, является сознательным и добровольным принятием на себя риска неполучения либо несвоевременного получения Клиентом информации о проведенных операциях по счету в электронном виде по Системе ДБО в случае совершения в отношении Клиента мошеннических действий, сопровождаемых поломкой или выводом из строя клиентского АРМ Системы ДБО.

9. ОРГАНИЗАЦИЯ ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ

9.1. Обмен электронными документами

Обмен ЭД включает:

формирование ЭД;

подпись (отправку) и доставку ЭД;

проверку ЭД;

подтверждение получения ЭД;

отзыв ЭД;

хранение ЭД (ведение архивов ЭД);

создание дополнительных экземпляров ЭД;

создание бумажных копий ЭД.

9.2. Формирование электронного документа

Формирование ЭД осуществляется следующим образом:

формирование ЭД в формате, установленном Банком, или в свободном формате, если формат соответствующего ЭД не установлен;

подписание сформированного ЭД электронной подписью.

9.3. Отправка и доставка электронного документа

9.3.1. В отношениях между отправителем и получателем ЭД считается исходящим от отправителя, если ЭД отправлен:

⁶ Кредитовое авизо о поступлении валютной выручки из Центрального аппарата в филиал является приложением к уведомлению о поступлении иностранной валюты на транзитный валютный счет резидента

самим отправителем, или

лицом, уполномоченным действовать от имени отправителя в отношении данного ЭД.

9.3.2. Документ считается доставленным получателю, если отправитель получил подтверждение о доставке.

9.4. Проверка подлинности доставленного электронного документа

9.4.1. Проверка ЭД включает:

проверку ЭД на соответствие формату, установленному Банком;

проверку подлинности всех электронных подписей ЭД.

9.4.2. В случае положительного результата проверки ЭД принимается к исполнению или подлежит дальнейшей обработке. В противном случае данный ЭД считается не полученным, о чем получатель должен послать уведомление отправителю с указанием причины неполучения ЭД.

9.4.3. При получении зашифрованного ЭД, для проведения проверки подлинности ЭД сначала выполняется расшифрование ЭД. В случае невозможности расшифрования ЭД получатель должен послать уведомление отправителю с указанием причины неполучения документа.

9.5. Подтверждение получения электронного документа

9.5.1. Подтверждение получения Банком ЭД производится путем автоматической отправки в адрес Клиента электронного сообщения «Квитанция банка», содержащего информацию о результатах обработки и изменении статуса ЭД.

9.5.2. Если иное не предусмотрено договорами, заключаемыми между Сторонами, ЭД считается не полученным Банком до тех пор, пока Клиент не получил соответствующего ЭС.

9.5.3. Если ЭС об изменении статуса ЭД не получено в течение одного часа с момента отправки ЭД, а статус ЭД сохраняется «Отправлен», ЭД Клиента считается не полученным. В данном случае Клиент должен связаться с Банком для разъяснения причин сбоя и определения дальнейшего порядка доставки документа в Банк.

9.6. Отзыв электронного документа

9.6.1. Участник Системы ДБО вправе отозвать отправленный электронный документ путем отправки Банку электронного документа «Запрос на отзыв документа», подписанного ЭП Клиента.

9.6.2. В ЭД «Запрос на отзыв документа» указываются реквизиты отзываемого ЭД и причина его отзыва.

9.6.3. После получения Банком «Запроса на отзыв документа» соответствующий ЭД (расчетный документ) будет отозван в том случае, если на момент получения «Запроса на отзыв документа» ЭД (расчетный документ) Банком не исполнен⁷.

Повторное направление отозванного ЭД (при необходимости) выполняется только после успешного отзыва ранее направленного ЭД.

10. ОБЯЗАННОСТИ КЛИЕНТА

10.1. ЭДО осуществляется в соответствии с настоящими Правилами и Регламентом. Не реже одного раза в семь календарных дней Клиент обязан знакомиться с публикуемой на сайте Банка информацией о Системе ДБО и возможных изменениях в Правилах.

⁷ Статус документа в системе ДБО - «Принят»

10.2. Установить необходимые для подключения к Системе ДБО аппаратные средства, клиентское программное и информационное обеспечение, а также поддерживать их в работоспособном состоянии.

10.3. Выполнить всю совокупность действий, необходимых для получения допуска к осуществлению ЭДО, предусмотренных Регламентом и настоящими Правилами, выполнять требования по плановой смене ключей ЭП, своевременно уведомлять Банк о компрометации ключей ЭП, а также соблюдать требования Руководства по обеспечению информационной безопасности (Приложение 7 к настоящим Правилам), организационно-технические требования по обеспечению безопасности информации, установленные в Регламенте и настоящих Правилах.

10.4. Обеспечить использование ключей ЭП в Системе ДБО только их владельцами (с установленными правами подписи). Клиенту запрещается использовать для подписи документов скомпрометированные ключи ЭП Представителей Клиента. Клиент обязан немедленно известить Банк о фактах компрометации по телефону и в письменной форме путем направления заявления на аннулирование (отзыв) соответствующих СКП ЭП.

10.5. Использовать полученные в Банке программно-аппаратные средства только для целей осуществления ЭДО в рамках Системы ДБО и не передавать без письменного согласия Банка данные средства третьим лицам.

10.6. Не производить декомпиляцию, модификацию программных средств, не совершать относительно указанных средств других действий, способных привести к нарушению целостности информации, передаваемой через систему ДБО, а также нарушающих действующее законодательство. Клиенту надлежит незамедлительно сообщать Банку о ставших известными Клиенту попытках третьих лиц совершить действия, способные привести к нарушению целостности Системы ДБО.

10.7. При возникновении в Системе ДБО ситуаций, признаваемых чрезвычайными в соответствии с Регламентом, Клиент признает и исполняет решения, принимаемые Банком в соответствии с Регламентом и настоящими Правилами.

10.8. Соблюдать Порядок урегулирования спорных ситуаций и споров, установленный Регламентом и разделом 14 настоящих Правил.

11. ПОРЯДОК ОПЛАТЫ УСЛУГ

11.1. До получения комплекта подключения Системы ДБО Клиент уплачивает Банку комиссионное вознаграждение за подключение к Системе ДБО (в выбранной им подсистеме и конфигурации) согласно тарифам Банка. Если у Клиента в Банке открыт банковский счет в российских рублях, на котором имеются денежные средства в сумме достаточной для удержания комиссии за подключение к Системе ДБО и отсутствуют действующие ограничения по счету, уплата комиссионного вознаграждения осуществляется в соответствии с условиями договора банковского счета путем списания Банком суммы комиссионного вознаграждения с банковского счета Клиента в российских рублях без дополнительного согласия (акцепта) Клиента.

В случае отсутствия у Клиента открытого в Банке банковского счета в российских рублях или отсутствия на банковском счете Клиента в российских рублях денежных средств в сумме, достаточной для удержания комиссии за подключение к Системе ДБО, или наличия действующих ограничений по счету, не позволяющих оплатить комиссию, Клиент оплачивает комиссионное вознаграждение наличными денежными средствами через кассу Банка. Передача Комплекта подключения Системы ДБО сопровождается подписанием Сторонами Акта передачи программного обеспечения Системы ДБО по форме Приложения 6 к настоящим Правилам либо подтверждения

Клиентом факта получения программного обеспечения в составе Заявления на предоставление комплексного обслуживания.

11.2. При использовании услуг по установке Банком Системы ДБО Клиент уплачивает Банку комиссионное вознаграждение за установку Системы ДБО согласно тарифам Банка и Акту об оказании услуг по установке и настройке программного обеспечения Системы ДБО (Приложение 12 к настоящим Правилам). Если у Клиента в Банке открыт банковский счет в российских рублях, на котором имеются денежные средства в сумме, достаточной для удержания комиссии за подключение к Системе ДБО, и отсутствуют действующие ограничения по счету, уплата комиссионного вознаграждения осуществляется в соответствии с условиями договора банковского счета путем списания Банком суммы комиссионного вознаграждения с банковского счета Клиента в российских рублях без дополнительного согласия (акцепта) Клиента не позднее рабочего дня, следующего за днем подписания Акта об оказании услуг по установке и настройке программного обеспечения Системы ДБО (Приложение 12 к настоящим Правилам). В случае отсутствия у Клиента открытого в Банке банковского счета в российских рублях или отсутствия на банковском счете Клиента в российских рублях денежных средств в сумме, достаточной для удержания комиссии за подключение к Системе ДБО, или наличия действующих ограничений по счету, не позволяющих оплатить комиссию, Клиент оплачивает комиссионное вознаграждение за установку Банком Системы ДБО наличными денежными средствами через кассу Банка, не позднее рабочего дня, следующего за днем подписания Акта об оказании услуг по установке и настройке программного обеспечения Системы ДБО (Приложение 12 к настоящим Правилам).

В случае невнесения наличных денежных средств в указанный срок взимание комиссионного вознаграждения за установку Банком Системы ДБО осуществляется Банком без дополнительного согласия Клиента с банковского счета Клиента, открытого в иной кредитной организации, реквизиты которого указаны в документах, представленных Клиентом в соответствии с п. 11.4 настоящих Правил, не позднее второго рабочего дня, следующего за днем подписания Акта об оказании услуг по установке и настройке программного обеспечения Системы ДБО (Приложение 12 к настоящим Правилам).

11.3. Клиент обязуется оплачивать услуги по дистанционному банковскому обслуживанию в соответствии с тарифами Банка.

11.3.1. Если к Системе ДБО подключен банковский счет Клиента (за исключением кредитных организаций), сроки и порядок оплаты услуг Банка по дистанционному банковскому обслуживанию устанавливаются соответствующим договором банковского счета.

11.3.2. В случае отсутствия у Клиента открытого в Банке банковского счета взимание комиссионного вознаграждения за предоставленные услуги по ДБО осуществляется Банком без дополнительного согласия Клиента с банковского счета Клиента, открытого в иной кредитной организации, реквизиты которого указаны в документах, представленных Клиентом в соответствии с п. 11.4 настоящих Правил, ежемесячно в последний рабочий день текущего месяца.

11.4. В случае отсутствия у Клиента открытого в Банке банковского счета в российских рублях, Клиент в течение пяти рабочих дней с даты получения копии Заявления с отметкой Банка о принятии/акцепте Заявления, представляет Банку экземпляр дополнительного соглашения к договору банковского счета в российских рублях, открытому в иной кредитной организации (далее – дополнительное соглашение), о праве кредитной организации на списание по требованию Банка без дополнительного согласия Клиента со счета Клиента денежных средств в счет уплаты за предоставленные Клиенту услуги в соответствии Договором ДБО, с указанием в дополнительном соглашении полных реквизитов банковского счета и условий об

обязательном информировании Банка иной кредитной организацией о факте закрытия Клиентом банковского счета и/или прекращения действия дополнительного соглашения. Вместо дополнительного соглашения Клиентом может быть представлен иной документ (заявление о заранее данном акцепте, распоряжение с информацией о Банке и обязательстве Клиента) с отметкой кредитной организации о его принятии, подтверждающий право иной кредитной организации списывать со счета Клиента по требованию Банка суммы комиссионного вознаграждения по дистанционному банковскому обслуживанию в соответствии с Договором ДБО.

12. СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

12.1. Порядок формирования криптографических профилей, ключей ЭП и СКП ЭП клиента, организация обслуживания клиента

12.1.1. Клиент передает Менеджеру пакет заверенных надлежащим образом документов, необходимых для формирования криптографического профиля и ключей Клиента.

12.1.2. Пакет документов включает следующие документы:

а) Заявление о присоединении к Регламенту Удостоверяющего центра Банк «Возрождение» (ПАО) и Правилам пользования централизованной системой дистанционного банковского обслуживания Банка «Возрождение» (ПАО) ([Приложение 1](#) к настоящим Правилам) или информация в составе Заявления на комплексное обслуживание по форме Банка.

б) Заявление на регистрацию пользователя Удостоверяющего центра Банка «Возрождение» (ПАО) и выпуск сертификата ключа проверки электронной подписи для использования в ЦС ДБО ([Приложение 2](#) к настоящим Правилам) или информация в составе Заявления на предоставление комплексного обслуживания. Если лицо зарегистрировано в качестве пользователя Удостоверяющего центра и имеется его согласие на обработку персональных данных – подается Заявление на выпуск сертификата ключа проверки электронной подписи ([Приложение 2а](#) к настоящим Правилам).

в) Перечень договоров и Список лиц, имеющих доступ к Системе ДБО ([Приложение 11](#) к настоящим Правилам) или информация в составе Заявления на предоставление комплексного обслуживания. Для назначения полномочий лицам Клиента, в графе «Полномочия» Списка лиц по форме Приложения 11 к настоящим Правилам, имеющих доступ к Системе ДБО, необходимо проставить отметки «+» / в графе «Полномочия» соответствующего раздела Заявления на предоставление комплексного обслуживания указать назначаемое полномочие. При этом:

назначение полномочия «единственная подпись» означает, что лицо имеет право распоряжаться денежными средствами, находящимися на банковском счете Клиента, используя систему ДБО, подписывать распоряжения и иные документы Клиента, которые будут приниматься к исполнению Банком при наличии одной электронной подписи;

полномочие «единственная подпись» назначается индивидуальному предпринимателю, физическому лицу, занимающемуся в установленном законодательством Российской Федерации порядке частной практикой. Основанием для присвоения полномочия «единственная подпись» указанным лицам является включение в КОПОП. Доверенность на подписание ЭД Клиента электронной подписью (вторая часть Заявления на регистрацию пользователя Удостоверяющего центра Банк «Возрождение» (ПАО) и выпуск сертификата ключа проверки электронной подписи для использования в ЦС ДБО) для указанных лиц не требуется;

полномочие «единственная подпись» назначается иным физическим лицам, наделенным правом подписи на основании доверенности, выданной индивидуальным предпринимателем, физическим лицом, занимающимся частной практикой. Основанием для присвоения полномочия «единственная подпись» указанным лицам является включение в КОПОП и доверенность на подписание ЭД Клиента электронной подписью (вторая часть Заявления на регистрацию пользователя Удостоверяющего центра Банк «Возрождение» (ПАО) и выпуск сертификата ключа проверки электронной подписи для использования в ЦС ДБО);

полномочие «единственная подпись» назначается руководителю Клиента – юридического лица, а также его работникам и иным лицам (в предусмотренных действующим законодательством случаях), наделенным правом подписи на основании распорядительного акта или доверенности Клиента, если Клиент – юридическое лицо определил, что распоряжения по счету и иные документы Клиента должны быть подписаны одной электронной подписью. Основанием для присвоения полномочия «единственная подпись» руководителю Клиента – юридического лица является включение в КОПОП. Доверенность на подписание ЭД Клиента ЭП для указанного лица не требуется. Основанием для присвоения полномочия «единственная подпись» работникам Клиента – юридического лица и иным лицам является включение в КОПОП и доверенность на подписание ЭД Клиента ЭП, при этом ЭД Клиента подписывается одной электронной подписью. Все подписи лиц с полномочием «единственная подпись» равнозначны и ЭД Клиента могут быть подписаны любой из них;

одному из представителей Клиента назначается дополнительно полномочие «шифрование». Допускается назначать полномочие «шифрование» нескольким лицам;

назначение полномочия «подпись 1» или «подпись 2» означает, что лицо имеет право распоряжаться денежными средствами на банковском счете Клиента, используя систему ДБО, подписывать распоряжения и иные документы Клиента, которые будут приниматься к исполнению Банком при наличии двух электронных подписей;

полномочие «подпись 1» или «подпись 2» назначается руководителю Клиента – юридического лица, его работникам и иным лицам (в установленных действующим законодательством случаях), если Клиент – юридическое лицо определил, что распоряжения по счету и иные документы Клиента должны быть подписаны двумя подписями. Основанием для присвоения полномочий «подпись 1» или «подпись 2» руководителю Клиента – юридического лица является включение в КОПОП. Доверенность на подписание ЭД Клиента ЭП для указанного лица не требуется. Основанием для присвоения полномочий «подпись 1» или «подпись 2» работникам Клиента – юридического лица и иным лицам является включение в КОПОП и доверенность на подписание ЭД Клиента ЭП.

Если указано хотя бы одно лицо с полномочием «подпись 1», то должно быть в обязательном порядке указано лицо с полномочием «подпись 2» и наоборот, при этом ЭД Клиента – юридического лица должны быть подписаны двумя электронными подписями: подписью любого из представителей с полномочием «подпись 1» и подписью любого из представителей с полномочием «подпись 2». «Подпись 1» и «подпись 2» могут проставляться уполномоченными лицами Клиента в произвольном порядке;

Одновременно полномочия «подпись 1» и «подпись 2» могут быть назначены одному лицу, при указании более трех Представителей Клиента с равнозначными правами подписи и если Клиент – юридическое лицо определил, что распоряжения по счету и иные документы Клиента должны быть подписаны двумя подписями;

Одному из Представителей Клиента с полномочием «подпись 1» и/или «подпись 2» назначается дополнительно полномочие «шифрование». Допускается назначать полномочие «шифрование» нескольким лицам.

Полномочие «единственная визирующая подпись» применяется после простановки в ЭД одной или двух электронных подписей (согласно предоставленным полномочиям) и может назначаться нескольким Представителям Клиента. При этом все «единственные визирующие подписи» равнозначны и ЭД Клиента могут быть завизированы любой из них.

Полномочия «визирующая подпись 1» и «визирующая подпись 2» применяется после простановки в ЭД одной или двух электронных подписей (согласно предоставленным полномочиям), в случае, если ЭД по счету Клиента должны быть завизированы двумя визирующими подписями, «визирующая подпись 1» и «визирующая подпись 2» могут проставляться уполномоченными лицами Клиента в произвольном порядке.

В случае создания у Клиента АРМ с предоставлением сотруднику только полномочия «шифрование» иные полномочия никому не назначаются. Отметка «+» в графе «Полномочия» указывается только в колонке «Шифрование». Данный АРМ используется только для просмотра документов.

г) Анкета физического лица на Представителя Клиента, на чье имя будет изготавливаться СКП ЭП Клиента, в случае если данная анкета не представлялась в Банк ранее;

д) Копия страниц документа, удостоверяющего личность физического лица – Представителя Клиента с его персональными данными (фамилия, имя, отчество, серия и номер документа, дата выдачи, кем выдан, дата рождения клиента, дата и адрес последней регистрации), в случае, если данные копии не представлялись в Банк ранее;

е) Доверенность на получение ключей ЭП, документов, программного и информационного обеспечения для работы с СКП ЭП ([Приложение 4](#) к настоящим Правилам) в случае получения Комплекта подключения Клиента и эксплуатационной документации на систему ДБО Представителем Клиента, не являющимся владельцем СКП ЭП;

ж) Заявление на установку (настройку) Системы ДБО и подключение/отключение услуги «SMS/e-mail информирование» ([Приложение 5](#) к настоящим Правилам) или Заявление на предоставление комплексного обслуживания;

з) Акт или Анкету о соблюдении Клиентом требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ Системы ДБО ([Приложения 8](#) или [9](#) к настоящим Правилам) или Заявление на предоставление комплексного обслуживания по форме Банка;

и) Учредительные документы Клиента – юридического лица;

12.1.3. В случае **первоначального подключения к подсистеме Интернет-Клиент Системы BS-Client** и при положительных результатах проверки Менеджером указанной Клиентом информации в переданных документах в Банк на каждого Представителя Клиента в соответствии со Списком лиц Клиента, имеющих доступ к Системе ДБО, Менеджер Банка передает Клиенту Комплект подключения, в составе:

Конверт, опечатанный СГЗ и маркированный уникальным ID комплекта подключения. Конверт содержит отформатированный USB-ключ с предустановленными PIN-кодами администратора и пользователя, а так же PIN-конверт с ключом простой ЭП – уникальной парой логин/пароль вырабатываемой Банком и однозначно связанной с уполномоченным лицом Клиента – владельцем простой ЭП, PIN-кодами администратора и пользователя USB-ключа для создания ключей ЭП и направления запроса на СКП ЭП в УЦ посредством подсистемы Интернет-Клиент Системы BS-Client;

диск с дистрибутивом СКЗИ, эксплуатационной документацией к СКЗИ, набором драйверов для работы с USB-ключом и Руководством «Быстрая установка Системы Интернет-Клиент»;

бумажная копия лицензии на использование СКЗИ Клиента;

2 бумажных экземпляра Акта о передаче программного обеспечения Системы ДБО и ключей ЭП ([Приложение 6](#) к настоящим Правилам). Акт о передаче программного обеспечения Системы ДБО и ключей ЭП не оформляется, если Заявление подано Клиентом в составе Заявления на предоставление комплексного обслуживания;

брошюра «Информация клиенту Системы дистанционного банковского обслуживания Банка «Возрождение» (ПАО)»;

средство визуализации электронной подписи⁸ SafeTouch.

12.1.4. В случае первоначального подключения к **подсистеме Интернет-Клиент Системы Correpts** и при положительных результатах проверки Менеджером указанной Клиентом информации в переданных документах в Банк на каждого Представителя Клиента в соответствии со Списком лиц Клиента, имеющих доступ к Системе ДБО, Менеджер Банка передаёт Клиенту Комплект подключения, в составе:

Конверт, опечатанный СГЗ и маркированный уникальным ID комплекта подключения. Конверт содержит отформатированный USB-ключ с технологическим ключом и технологическим СКП ЭП, предустановленными PIN-кодами администратора и пользователя, а так же PIN-конверт с ключом простой ЭП – уникальной парой логин/пароль вырабатываемой Банком и однозначно связанной с уполномоченным лицом Клиента – владельцем простой ЭП, PIN-кодами администратора и пользователя USB-ключа для создания ключей ЭП и направления запроса на СКП ЭП в УЦ посредством подсистемы Интернет-Клиент Системы Correpts;

2 бумажных экземпляра Акта о передаче программного обеспечения Системы ДБО и ключей ЭП ([Приложение 6](#) к настоящим Правилам). Акт о передаче программного обеспечения Системы ДБО и ключей ЭП не оформляется, если Заявление подано Клиентом в составе Заявления на предоставление комплексного обслуживания;

брошюра «Информация клиенту Системы дистанционного банковского обслуживания Банка «Возрождение» (ПАО)»;

12.1.5. Подключение новых Клиентов к **подсистеме Клиент-Банк Системы BS-Client**, не производится. В случае восстановления подключения существующего Клиента и необходимости формирования Комплекта подключения при положительных результатах проверки Менеджером указанной Клиентом информации в переданных документах, Банк в течение трех рабочих дней, следующих за днем представления Клиентом пакета документов, в соответствии с разделом 12.1.2 настоящих Правил формирует комплект подключения подсистемы Клиент-Банк Системы BS-Client, который включает в себя:

на каждого Представителя Клиента в соответствии со Списком лиц Клиента, имеющих доступ к Системе ДБО (Приложение 11 к настоящим Правилам):

конверт с НКПИ, содержащий USB-ключ с технологическим ключом ЭП и технологическим СКП ЭП подсистемы Клиент-Банк Системы BS-Client, администраторским и пользовательским PIN-кодами доступа к НКПИ в PIN-конвертах;

⁸ Представляется в случае изъявления Клиентом желания использовать НКПИ в форм-факторе смарт-карты.

диск с дистрибутивом СКЗИ, эксплуатационной документацией к нему, набором драйверов для работы с USB-ключом, дистрибутивом АРМ Клиента и эксплуатационной документацией для клиентского АРМ Системы ДБО;

бумажную копию лицензии на использование СКЗИ Клиента.

2 бумажных экземпляра Акта о передаче программного обеспечения Системы ДБО и ключей ЭП ([Приложение 6](#) к настоящим Правилам).

12.1.6. Каждый комплект подключения вскрывается Менеджером Банка в присутствии представителя Клиента, после чего Сторонами подписывается Акт о передаче программного обеспечения и ключей ЭП по форме Приложения 6 к настоящим Правилам или Клиент подтверждает факт получения программного обеспечения в составе Заявления на предоставление комплексного обслуживания.

12.1.7. Клиент обязан при получении Комплекта подключения от Менеджера Банка и в его присутствии сверить учетные, серийные номера и идентификаторы содержимого комплекта подключения на соответствие с данными, указанными в Акте о передаче программного обеспечения и ключей ЭП, подписать два экземпляра Акта (Приложение 6 к настоящим Правилам или в составе Заявления на предоставление комплексного обслуживания) и вернуть один экземпляр Менеджеру Банка.

12.1.8. В случае получения Комплекта подключения Представителем Клиента, не являющимся владельцем данного Комплекта, Представитель Клиента должен предоставить Менеджеру Банка доверенность на получение ключей ЭП, документов, программного, аппаратного и информационного обеспечения для работы с СКП ЭП ([Приложение 4](#) к настоящим Правилам).

12.1.9. Клиент самостоятельно проводит установку Системы ДБО на свои рабочие станции, соответствующие требованиям Руководства по обеспечению информационной безопасности ([Приложение 7](#) к настоящим Правилам). В этом случае соответствие АРМ Системы ДБО требованиям по обеспечению информационной безопасности подтверждается Актом либо Анкетой Клиента о соблюдении требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи (Приложения [8](#) либо [9](#) к настоящим Правилам) либо подписанием Клиентом пункта 3 Заявления на предоставление комплексного обслуживания.

При невыполнении или неполном выполнении Клиентом обязательных требований по обеспечению информационной безопасности АРМ Системы ДБО, в соответствии с п.7.9 настоящих Правил Клиент принимает на себя риски возможных потерь (ущерба).

12.1.10. В случае выбора Клиентом услуг по установке Банком Системы ДБО в течение пяти рабочих дней, следующих за днем представления в Банк документов, указанных в п. 12.1.2 настоящих Правил и при условии оплаты Клиентом комиссии за подключение к Системе ДБО Банк осуществляет установку Клиенту Системы ДБО, а также проводит консультацию Клиента по работе с программным обеспечением. По окончании установки Клиенту Системы ДБО стороны оформляют двусторонний Акт об оказании услуг по установке и настройке программного обеспечения Системы ДБО ([Приложение 12](#) к настоящим Правилам) , а также Акт о соблюдении требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи (Приложение 8 к настоящим Правилам).

12.1.11. После установки Системы ДБО на свои рабочие станции Клиент самостоятельно вырабатывает свой ключ ЭП с записью на НКПИ – USB-ключ, формирует, подписывает и отправляет в Банк запрос на СКП ЭП. С целью исключения возможности записи ключей ЭП при генерации или при регенерации на любые другие НКПИ, запрещается регистрировать на рабочих станциях Клиента какие-либо

считыватели кроме считывателя смарт-карт, запрещается регистрировать все съёмные диски и реестр.

12.1.12. Банк проверяет подлинность запроса на выпуск СКП ЭП. В случае соблюдения требований Регламента и настоящих Правил, УЦ выполняет комплекс работ по выпуску Клиенту рабочего СКП ЭП.

12.1.13. В Системе ДБО Банка формируется и отправляется Клиенту документ свободного формата с вложениями: файлом СКП ЭП Клиента и Актом об оказании услуг по выпуску сертификата в Системе ДБО ([Приложение 10](#) к настоящим Правилам). Акт оформляется каждому физическому лицу (Клиенту, Представителю Клиента) – владельцу СКП ЭП на каждый СКП ЭП.

12.1.14. В случае использования Системы BS-Client Клиент просматривает полученный файл СКП ЭП, сравнивает серийный номер в СКП ЭП с номером в Акте, самостоятельно распечатывает Акт в двух экземплярах с помощью текстового редактора, подписывает и передает два экземпляра Акта Менеджеру Банка.

12.1.15. В случае использования Системы Correpts Банк формирует и отправляется Клиенту документ свободного формата с вложениями: файлом СКП ЭП Клиента и Актом об оказании услуг по выпуску сертификата в Системе ДБО ([Приложение 10](#) к настоящим Правилам) подписанным ЭП Администратора Банка. Клиент просматривает полученный файл СКП ЭП, сравнивает серийный номер в СКП ЭП с номером в Акте, создает письмо в Банк (произвольный документ) с вложением проверенного Акта, подписывает Акт своей технологической ЭП и отправляет письмо в Банк.

12.1.16. В случае использования Системы BS-Client Менеджер Банка после предоставления подписанного Клиентом Акта оказания услуг по выпуску сертификата (Приложение 10 к настоящим Правилам) заполняет реквизиты и поля Акта, подлежащие ручному заполнению, подписывает Акт в двух экземплярах. Один экземпляр Акта возвращает Клиенту. После этого проводит работу по вводу в эксплуатацию СКП ЭП Клиента в систему ЦС ДБО Банка.

12.1.17. В случае использования Системы Correpts Менеджер Банка проверяет корректность ЭП Администратора Банка и корректность технологической ЭП Клиента и проводит работу по вводу в эксплуатацию СКП ЭП Клиента в систему ЦС ДБО Банка.

12.1.18. После ввода Банком в эксплуатацию нового СКП ЭП процедура создания ключей ЭП завершается, Клиент может приступить к работе с новым комплектом ключей ЭП.

12.1.19. Стороны признают, что подпись Представителя Клиента как владельца СКП ЭП в Акте означает, что на его имя Удостоверяющим центром выдан СКП ЭП и, что он владеет соответствующим ключом ЭП, позволяющим с помощью средств ЭП создавать свою электронную подпись в ЭД (подписывать ЭД).

12.1.20. Срок действия технологического СКП ЭП Клиента устанавливается в соответствие с Регламентом. Клиент обязуется в течение срока действия технологического СКП ЭП провести установку Системы ДБО, самостоятельно сформировать рабочий ключ ЭП Клиента (обновление ключа Клиента или удаленную регенерацию). Технологический ключ, для которого истек срок действия технологического СКП ЭП, должен быть самостоятельно удален из памяти НКПИ уполномоченным представителем Клиента.

12.1.21. В случае использования подсистемы Клиент-Банк Системы BS-Client, ключ ЭП и соответствующий ему СКП ЭП, которые выдаются Клиенту с Комплектом подключения, являются технологическими и предназначены для использования Клиентом при проведении им самостоятельного формирования новых ключей ЭП Клиента (обновления ключей Клиента или удаленной регенерации). Банк

обеспечивает невозможность использования технологических ключей ЭП и соответствующим им СКП ЭП для подписания электронных документов. После регистрации в Системе нового ключа ЭП Клиента технологический ключ становится не активным, даже если срок действия технологического СКП ЭП не истек.

12.1.22. Так как сертифицированный НКПИ является высоконадежным носителем ключей ЭП, а сам ключ ЭП имеет признак «Не экспортируемый» создание дубликата НКПИ не производится.

12.1.23. Каждому ключу ЭП, записанному на НКПИ, в Системе ДБО соответствует только один СКП ЭП Клиента. Аппаратно-программный комплекс УЦ Банка гарантирует уникальность значения ключа проверки ЭП и серийного номера СКП ЭП в каждом выпущенном Удостоверяющим центром СКП ЭП.

12.1.24. СКП ЭП уполномоченных лиц Клиента и Администраторов Системы ДБО Банка в форме документов на бумажном носителе предоставляются Клиентам по их запросу в виде копий, заверенных Банком. Указанные в настоящем пункте документы представляются Банком Клиенту в течение 15 (пятнадцати) рабочих дней после получения соответствующего запроса Клиента.

12.2. Особенности оформления пакета документов для Клиентов при подключении Системы ДБО в конфигурации «Корпоративный контроль»

12.2.1. Услуга «Корпоративный контроль» предназначена для холдингов (основное и дочерние юридические лица) либо юридических лиц с территориально распределенной сетью обособленных подразделений. Она позволяет основному юридическому лицу холдинга контролировать или управлять счетами дочерних юридических лиц, либо юридическому лицу контролировать или управлять счетами, открытыми для обособленных подразделений. При этом в одном из филиалов Банка обслуживаются счета юридического лица/основного юридического лица холдинга, а в других филиалах Банка – счета обособленных подразделений юридического лица / дочерних юридических лиц холдинга.

12.2.2. При предоставлении услуги «Корпоративный контроль» Представителям основного юридического лица холдинга или головного подразделения юридического лица, не требуется выпуск нового СКП ЭП.

12.2.3. В рамках данной услуги для Представителей основного юридического лица холдинга или головного подразделения юридического лица по счетам дочерних юридических лиц или счетам, открытым для обособленных подразделений, в других филиалах/ДО Банка, предоставляется возможность реализовать следующие полномочия:

просмотр;

единственная визирующая подпись;

визирующая подпись 1;

визирующая подпись 2;

единственная подпись (только для юридических лиц с сетью обособленных подразделений),

подпись 1 (только для юридических лиц с сетью обособленных подразделений);

подпись 2 (только для юридических лиц с сетью обособленных подразделений).

12.2.4. Для холдингов:

12.2.4.1. Для предоставления Представителям основного юридического лица холдинга полномочий просмотра и визирования ЭД дочерних юридических лиц в

филиале Банка, обслуживающем основное юридическое лицо холдинга, необходимо оформить следующие документы:

новый Перечень договоров ([Приложение 11](#) к настоящим Правилам), где будут указаны все подключаемые счета дочерних юридических лиц и соответствующие полномочия для Представителей основного юридического лица;

доверенность ([Приложение 4а](#) к настоящим Правилам) от дочерних юридических лиц, подтверждающую полномочия Представителей основного юридического лица холдинга на просмотр информации по счетам и/или визирование ЭД дочернего юридического лица в Системе ДБО;

12.2.4.2. В целях предоставления Представителем основного юридического лица холдинга полномочий визирования, дополнительно к вышеуказанным документам в филиалах/ЦА Банка, обслуживающих счета дочерних юридических лиц, необходимо заключить дополнительное соглашение к договору банковского счета о приеме Банком ЭД по Системе ДБО при наличии визирующей подписи Представителя основного юридического лица холдинга.

12.2.5. Для Клиентов с территориально распределенной сетью обособленных подразделений:

12.2.5.1. Для предоставления Представителю головного подразделения Клиента полномочий просмотра и визирования, в филиал/ДО Банка, обслуживающий головное подразделение Клиента, необходимо предоставить следующие документы:

новый Перечень договоров ([Приложение 11](#) к настоящим Правилам), в котором указываются все подключаемые счета обособленных подразделений Клиента и соответствующие полномочия для Представителей головного подразделения Клиента;

доверенность на Представителя головного подразделения Клиента на просмотр информации по счетам и/или визирование ЭД соответствующих филиалов Клиента в Системе ДБО. В случае если Представителем головного подразделения Клиента является единоличный исполнительный орган Клиента (иное лицо, действующее от имени Клиента без доверенности), данная доверенность не требуется;

12.2.5.2. В целях предоставления Представителям головного подразделения Клиента полномочий визирования дополнительно к вышеуказанным документам в филиалах Банка, обслуживающих обособленные подразделения Клиента, необходимо заключить дополнительное соглашение к договорам банковского счета о приеме Банком ЭД по Системе ДБО при наличии визирующей подписи Представителя головного подразделения Клиента с указанием такого лица.

12.2.5.3. В целях предоставления Представителям головного подразделения Клиента полномочий «единственная подпись» «подпись 1» или «подпись 2», дополнительно к документам, указанным в п. 12.3.5.1 настоящих Правил в филиалах Банка, обслуживающих обособленные подразделения Клиента, необходимо включить обеспечить включение соответствующих Представителей головного подразделения Клиента в КОПОП, оформленным к счетам, открытым для обособленных подразделений с представлением необходимых для этого документов:

доверенность или приказ о наделении правом подписи Представителя головного подразделения Клиента (кроме лиц, действующих без доверенности от имени юридического лица).

12.2.6. Доверенности, указанные в разделе 12.2 настоящих Правил должны быть выданы на срок, равный или превышающий срок действия СКП ЭП Представителя основного юридического лица холдинга или головного подразделения юридического лица.

12.2.7. На основании принятого от Клиента Заявления и/или Перечня договоров и Списка лиц (Приложения 11 к настоящим Правилам) в случае, если система ДБО уже установлена у Клиента, взимается комиссия за подключение Системы ДБО в конфигурации «Корпоративный контроль» согласно тарифам Банка. Комиссия взимается с расчетного счета юридического лица (исключая обособленные подразделения) или основного юридического лица холдинга в соответствии с договором банковского счета.

12.3. Проведение плановой замены криптографических ключей и СКП ЭП клиента

12.3.1. За 30 (тридцать) календарных дней (по умолчанию) на АРМ Системы ДБО выводится сообщение о приближающемся окончании срока действия СКП ЭП. Плановая смена СКП ЭП должна быть выполнена владельцами СКП ЭП не позднее, чем за три рабочих дня до завершения срока действия СКП ЭП.

12.3.2. Клиент самостоятельно выполняет процедуру формирования ключа ЭП (обновление ключей Клиента или удаленную регенерацию) согласно Руководству пользователя и отправку в Банк запроса на выпуск СКП ЭП.

12.3.3. При формировании Клиентом новых ключей ЭП замена НКПИ не требуется. Новые ключи ЭП записываются на ранее полученный НКПИ. Старые ключи ЭП, если таковые имеются, для которых истекли сроки действия СКП ЭП, должны быть самостоятельно удалены из памяти НКПИ уполномоченным Представителем Клиента.

12.3.4. На стороне Банка, по получению запроса на изготовление СКП ЭП Клиента/Представителя Клиента, проводятся работы по проверке соответствия данных из запроса на СКП ЭП с данными Заявления на регистрацию пользователя Удостоверяющего центра/Заявления на выпуск СКП ЭП и другим документам, находящимся в юридическом деле Клиента, и при положительных результатах проверки запрос на СКП ЭП обрабатывается и осуществляется выпуск нового СКП ЭП.

12.3.5. В случае использования Системы BS-Client после выпуска нового СКП ЭП в Системе ДБО Банка формируется и отправляется Клиенту ЭД свободного формата с вложениями: файлом нового СКП ЭП Клиента и Актом. Клиент просматривает полученный файл СКП ЭП, сравнивает серийный номер в СКП ЭП с номером в Акте, самостоятельно распечатывает Акт в двух экземплярах, подписывает и передает два экземпляра Акта Менеджеру Банка.

12.3.6. После получения подписанного установленным порядком Акта оказания услуг по выпуску сертификата (Приложение 10 к настоящим Правилам) Менеджер заполняет реквизиты и поля Акта, подлежащие ручному заполнению, подписывает Акт в двух экземплярах. Один экземпляр Акта возвращает Клиенту. После этого Менеджер проводит работу по вводу в эксплуатацию сертификата ключа проверки электронной подписи Клиента в систему ЦС ДБО Банка.

12.3.7. В случае использования Системы Correpts Банк формирует и отправляется Клиенту документ свободного формата с вложениями: файлом нового СКП ЭП Клиента и Актом об оказании услуг по выпуску сертификата в Системе ДБО ([Приложение 10](#) к настоящим Правилам) подписанным ЭП Администратора Банка. Клиент просматривает полученный файл СКП ЭП, сравнивает серийный номер в СКП ЭП с номером в Акте, создает письмо в Банк с вложением проверенного Акта, подписывает Акт своей действующей ЭП и отправляет письмо в Банк.

12.3.8. Менеджер Банка проверяет корректность ЭП Администратора Банка, корректность ЭП Клиента и проводит работу по вводу в эксплуатацию нового сертификата ключа проверки электронной подписи Клиента в систему ЦС ДБО Банка.

12.3.9. После ввода Банком в эксплуатацию нового СКП ЭП процедура создания ключей ЭП завершается, Клиент может приступить к работе с новым

комплект ключей ЭП.

12.3.10. Новые СКП ЭП Представителей Клиента в форме документов на бумажном носителе предоставляются Клиентам в течение пятнадцати рабочих дней после получения соответствующего запроса Клиента.

12.3.11. В случаях:

- а) истечения срока действия СКП ЭП клиента и невозможности подписать запрос в Банк на выработку нового СКП ЭП;
- б) изменения реквизитов действующего уполномоченного лица клиента, включаемых в СКП ЭП;
- в) смены уполномоченного лица клиента (при сохранении ключевого носителя);
- г) ошибочного удаления Клиентом действующего ключа электронной подписи с ключевого носителя;
- д) полной блокировки ключевого носителя (превышении допустимого количества попыток входа с PIN-кодом администратора),

Клиент должен выполнить действия, предусмотренные разделом 12.1 настоящих Правил, с учетом следующего:

новый НКПИ Клиенту может не предоставляться;

В случае использования Клиентом подсистем Интернет-Клиент Системы BS-Client или Системы Corrects для доступа в Систему ДБО Клиенту необходимо получить в обслуживающем ДО/филиале Банка Микро-комплект подключения – новый ключ простой ЭП, по Акту о передаче программного обеспечения Системы ДБО и ключей ЭП ([Приложение 6](#) к настоящим Правилам) либо отдельному Акту о передаче Микро-комплекта подключения к Системе ДБО ([Приложение 14](#)). Для Клиента формируется новый криптографический профиль. Новые технологические ключ и СКП ЭП в данном случае Клиенту подсистемы Интернет-Клиент Системы Corrects не вырабатываются. Действия, предусмотренные п.п. 12.3.7 – 12.3.8 не производятся. После выпуска нового СКП ЭП в Системе ДБО Банка формируется и отправляется Клиенту ЭД свободного формата с вложениями: файлом нового СКП ЭП Клиента и Актом. Клиент просматривает полученный файл СКП ЭП, сравнивает серийный номер в СКП ЭП с номером в Акте, самостоятельно распечатывает Акт в двух экземплярах, собственноручно подписывает и передает два экземпляра Акта Менеджеру Банка. После получения подписанного установленным порядком Акта оказания услуг по выпуску сертификата ([Приложение 10](#) к настоящим Правилам) Менеджер заполняет реквизиты и поля Акта, подлежащие ручному заполнению, подписывает Акт в двух экземплярах. Один экземпляр Акта возвращает Клиенту. После этого Менеджер проводит работу по вводу в эксплуатацию сертификата ключа проверки электронной подписи Клиента в систему ЦС ДБО Банка;

В случае использования Клиентом подсистемы Клиент-Банк Системы BS-Client ДБО Банк предоставляет Клиенту информацию о новом криптографическом профиле Клиента на сменном носителе, записанный на новый НКПИ новый технологический ключ ЭП, а так же новый технологический СКП ЭП Клиента, Клиент должен выполнить действия, предусмотренные п. 12.1 настоящих Правил.

12.4. Порядок действий при компрометации криптографических ключей или физической порче носителя ключевой и парольной информации

12.4.1. В случае компрометации ключей ЭП или физической порчи носителя ключевой и парольной информации владелец скомпрометированных ключей ЭП или испорченного носителя ключевой информации обязан действовать в соответствии с порядком, установленным настоящими Правилами.

12.4.2. При получении ЭД, подписанного скомпрометированным ключом ЭП, данный ЭД считается не полученным, о чем получатель обязан отправить

уведомление отправителю с указанием причины неполучения ЭД.

12.4.3. В случае принятия решения Клиентом о компрометации своих ключей ЭП уполномоченное лицо Клиента обязано по телефону сообщить Менеджеру и на горячую линию Банка и прекратить использование скомпрометированных ключей ЭП для информационного обмена.

12.4.4. С целью проверки информации о компрометации ключей ЭП Клиента Менеджер выполняет ответный звонок уполномоченному лицу Клиента. В случае положительной проверки Менеджер дает указание Администратору Системы ДБО заблокировать в Системе ДБО соответствующий криптографический профиль Представителя Клиента.

12.4.5. В течение того же рабочего дня, когда Клиент уведомил Менеджера по телефону о компрометации ключей ЭП, Клиент обязан направить на имя Руководителя Банка/управляющего филиалом Банка Заявление на аннулирование СКП ЭП пользователя Удостоверяющего центра Банка⁹, подписанное руководителем Клиента и заверенное (при наличии) печатью Клиента ([Приложение 3](#) к настоящим Правилам). Заявление регистрируется как входящая корреспонденция в установленном в Банке порядке и обязательно помещается в юридическое дело Клиента на бумажном носителе.

12.4.6. Официальным уведомлением о факте аннулирования СКП ЭП является опубликование СОС, содержащего сведения об аннулированном сертификате, изданного ранее всех последующих СОС. Временем аннулирования СКП ЭП признается время издания СОС, изданного ранее всех последующих СОС и содержащего сведения об аннулированном сертификате, указанное в поле «thisUpdate» (действителен с) СОС.

12.4.7. Информация о размещении СОС заносится в изданные Удостоверяющим центром сертификаты ключей подписей в поле CRLDistributionPoint.

12.4.8. СКП ЭП, соответствующий скомпрометированному ключу ЭП, из ключевой базы Организатора не удаляется и хранится в течение трех лет после аннулирования СКП ЭП для проведения (в случае необходимости) разбора конфликтных ситуаций, связанных с применением ЭП.

12.4.9. В случае компрометации ключа ЭП Клиент должен выполнить действия, предусмотренные п.12.1 настоящих Правил с учетом следующих особенностей:

в случае использования Клиентом подсистем Интернет-Клиент Системы BS-Client и Системы Corrects новый НКПИ Клиенту не предоставляется. Для доступа в подсистему Интернет-Клиент Клиенту необходимо получить в обслуживающем ДО/филиале Банка новый ключ простой ЭП по Акту о передаче программного обеспечения Системы ДБО и ключей ЭП ([Приложение 6](#) к настоящим Правилам) либо отдельному Акту о передаче Микро-комплекта подключения к Системе ДБО ([Приложение 14](#));

в случае использования Клиентом подсистемы Клиент-Банк Банк Системы BS-Client ДБО Клиент должен выполнить действия, предусмотренные п. 12.1 настоящих Правил.

12.4.10. В случае физической порчи НКПИ Клиент должен выполнить действия, предусмотренные разделом 12.1 настоящих Правил.

12.4.11. Для возобновления ЭДО с Банком Клиент выполняет самостоятельную процедуру формирования ключей ЭП Клиента (обновления ключей Клиента, удаленной регенерации или начальной генерации).

⁹ Далее – Заявление.

13. ОТВЕТСТВЕННОСТЬ СТОРОН. ОБСТОЯТЕЛЬСТВА, ИСКЛЮЧАЮЩИЕ ОТВЕТСТВЕННОСТЬ СТОРОН (ФОРС-МАЖОР)

13.1. Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации за действия своих сотрудников, а также иных лиц, получивших или имеющих доступ (независимо от того был ли этот доступ прямо санкционирован Стороной или произошел по ее вине) к используемым ими аппаратным средствам, программному, информационному обеспечению, криптографическим ключам и иным средствам, обеспечивающим ЭДО в соответствии с Регламентом и Правилами. Банк не несет ответственности в случае исполнения распоряжений, поданных с использованием Системы ДБО, если будут установлены факты несоблюдения Клиентом обязательных для исполнения пунктов требований Руководства по обеспечению информационной безопасности (Приложение 7 к настоящим Правилам).

13.2. Клиент осведомлен о рисках при использовании Системы ДБО и признает свою ответственность в случае использования ключей ЭП неуполномоченными на это лицами.

13.3. Банк не несет ответственность за последствия исполнения распоряжений, в случаях не уведомления Клиентом Банка о фактах компрометации ключей ЭП Представителей Клиента.

13.4. Банк не несет ответственности за ущерб, причиненный Клиенту в результате использования третьими лицами ключа ЭП Представителей Клиента.

13.5. Банк не несет ответственности за неблагоприятные для Клиента последствия, наступившие в результате несанкционированного доступа к Системе ДБО неуполномоченных третьих лиц, возникшего не по вине Банка.

13.6. Банк не несет ответственности в случае невозможности осуществления обмена ЭД с Клиентом, если это вызвано неисправностями используемых Клиентом программных и аппаратных средств и каналов связи, предоставленных третьими лицами.

13.7. За невыполнение или ненадлежащее выполнение обязательств, предусмотренных настоящими Правилами и Регламентом, Стороны несут ответственность в пределах суммы доказанного реального ущерба, причиненного Стороне невыполнением или ненадлежащим выполнением обязательств другой Стороной.

13.8. Банк не несет ответственности за неполучение Клиентом выписки из лицевого счета в соответствии с п. 8.5.2 настоящих Правил вследствие выхода из строя Системы ДБО, при неполучении заявления от Клиента согласно п. 15.1 настоящих Правил. В случае сообщения Клиентом Банку о выходе из строя Системы ДБО либо компьютера, на котором установлен АРМ Системы ДБО Клиента, Банк согласовывает с Клиентом иной способ уведомления об операциях, совершенных с использованием электронных средств платежа.

13.9. Стороны освобождаются от ответственности за частичное или полное неисполнение своих обязательств в соответствии с Регламентом и Правилами, если это неисполнение явилось следствием обстоятельств непреодолимой силы, возникших после присоединения к Регламенту и настоящим Правилам, или в результате событий чрезвычайного характера, а также сбоев, неисправностей и отказов оборудования; сбоев и ошибок программного обеспечения; сбоев, неисправностей и отказов систем связи, энергоснабжения, кондиционирования и других систем жизнеобеспечения, не позволяющих осуществлять эксплуатацию необходимого для выполнения Регламента и настоящих Правил оборудования, которые Стороны не могли предвидеть или предотвратить.

13.10. В случае возникновения обстоятельств непреодолимой силы срок выполнения Сторонами своих обязательств в соответствии с настоящими Правилами отодвигается соразмерно времени, в течение которого действуют такие обстоятельства и их последствия.

13.11. Сторона, для которой стало невозможным выполнение своих обязательств в виду действия обстоятельств непреодолимой силы, обязана в течение трех календарных дней сообщить другой Стороне о начале и прекращении действия обстоятельств, воспрепятствовавших выполнению договорных обязательств.

13.12. Обязанность доказывать существование обстоятельств непреодолимой силы лежит на Стороне, которая ссылается на их действие.

13.13. По прошествии обстоятельств непреодолимой силы Стороны обязуются принять все меры для ликвидации последствий и уменьшения причиненного реального ущерба.

14. ПОРЯДОК УРЕГУЛИРОВАНИЯ СПОРНЫХ СИТУАЦИЙ

14.1. В случае возникновения между Сторонами спорных ситуаций при использовании Системы ДБО, Стороны предпримут все меры для их разрешения путем переговоров.

14.2. При возникновении спорной ситуации одна Сторона направляет другой Стороне соответствующую письменную претензию.

14.3. До создания технической комиссии из уполномоченных представителей Стороны самостоятельно проводят проверку спорного ЭД на АРМ Системы ДБО с использованием сервисной функции «Разбор конфликтных ситуаций». По результатам проверки Стороны проводят переговоры.

14.4. Если Сторонам не удастся разрешить спорную ситуацию путем переговоров, совместным решением обеих Сторон для проведения технической экспертизы создается техническая комиссия из уполномоченных представителей Сторон. Указанное решение принимается Сторонами в течение 3 (трех) рабочих дней с момента обращения одной Стороны к другой. В случае уклонения одной из Сторон от принятия данного решения другая Сторона вправе самостоятельно привлечь экспертов для выяснения обстоятельств конфликтной ситуации.

14.5. По согласованию Сторон к участию в работе технической комиссии могут привлекаться эксперты в области защиты информации. Стороны согласны с тем, что в качестве экспертов, прежде всего, должны привлекаться сотрудники следующих организаций:

разработчика Системы ДБО;

разработчика средства криптографической защиты информации;

специалисты Федеральной Службы Безопасности Российской Федерации.

14.6. Стороны согласны с тем, что оплачивать услуги привлеченных экспертов в области защиты информации должна Сторона, предъявившая претензию.

14.7. Техническая комиссия осуществляет свою работу на территории Банка.

14.8. Техническая комиссия создаётся и приступает к работе в течение 3 (трех) рабочих дней со дня поступления письменного заявления к одной из Сторон. Бремя доказательства лежит на Стороне, заявившей о нарушении ее прав и законных интересов. Все действия, предпринимаемые комиссией для выяснения фактических обстоятельств, а также выводы, сделанные комиссией, заносятся в Протокол работы

технической комиссии. Протокол работы технической комиссии должен содержать следующие данные:

состав комиссии с указанием сведений о квалификации каждого из членов комиссии;

краткое изложение обстоятельств возникшей конфликтной ситуации;

мероприятия, проводимые комиссией для установления причин и последствий возникшей конфликтной ситуации, с указанием даты времени и места их проведения;

выводы, к которым пришла комиссия в результате проведенных мероприятий;

подписи всех членов комиссии.

14.9. При проведении технической экспертизы проводится проверка соответствия АРМ Системы ДБО Клиента требованиям Руководства по обеспечению информационной безопасности (Приложение 7 к настоящим Правилам), по результатам которой составляется Акт о соблюдении Клиентом требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ Системы ДБО (Приложение 8 к настоящим Правилам). Акт технической экспертизы подписывается членами комиссии.

14.10. В случае если мнение члена (или членов) комиссии относительно порядка, методики, целей проводимых мероприятий не совпадает с мнением большинства членов комиссии, об этом в Протоколе составляется соответствующая запись, которая подписывается членом (или членами комиссии), чье особое мнение отражает соответствующая запись.

14.11. Протокол составляется на бумажном носителе в двух экземплярах, имеющих одинаковую силу. Экземпляры Протокола хранятся у Банка и Клиента.

14.12. По итогам работы технической комиссии составляется акт, в котором содержится краткое изложение выводов технической комиссии. Помимо изложения выводов о работе технической комиссии, акт должен также содержать следующие данные:

состав комиссии;

дату и место составления акта;

даты и время начала и окончания работы комиссии;

краткий перечень мероприятий, проведенных комиссией;

подписи членов комиссии;

указание на особое мнение члена (или членов комиссии), в случае наличия такового.

14.13. Акт составляется на бумажном носителе в двух экземплярах, имеющих одинаковую силу. Экземпляры акта хранятся у Банка и Клиента.

14.14. К акту может прилагаться особое мнение члена (или членов комиссии), не согласных с выводами технической комиссии, указанными в акте. Особое мнение составляется в произвольной форме и составляет приложение к акту.

14.15. Техническая комиссия проводит техническую экспертизу спорных ситуаций в соответствии с Регламентом и настоящими Правилами.

14.16. Для проведения технической экспертизы спорного ЭД техническая комиссия проводит следующие подготовительные мероприятия:

определяет СКП ЭП или несколько СКП ЭП, необходимые для проверки ЭП спорного ЭД;

получает в УЦ:

СКП ЭП уполномоченного лица УЦ, соответствующий времени выработки ЭП спорного ЭД;

СКП ЭП или несколько СКП ЭП, необходимые для проверки ЭП спорного ЭД;

СОС, необходимый для проверки ЭП спорного ЭД.

у каждой из Сторон производит копирование баз данных, лицензионных и регистрационных файлов;

получает у Администратора Системы ДБО Банка технологический дистрибутив Системы ДБО, с которого производилась установка Системы;

на выделенном компьютере Банка, соответствующем требованиям по установке банковской и клиентской частей Системы ДБО производит:

форматирование жесткого диска компьютера;

установку операционной Системы, соответствующей требованиям банковской и клиентской частей Системы ДБО;

установку банковской и клиентской частей Системы ДБО;

средствами АРМ Системы ДБО выгружает файл спорного ЭД с ЭП отправителя.

14.17. Проведение технической экспертизы спорного ЭД включает в себя выполнение следующих действий:

проверку ЭП выгруженного файла спорного ЭД с использованием каждого СКП ЭП из отобранных для разбора конфликтной ситуации;

проверку ЭП уполномоченного лица УЦ для каждого СКП ЭП, отобранного для разбора конфликтной ситуации;

проверку действительности СКП ЭП, отобранных для разбора конфликтной ситуации, на текущий момент времени;

проверку действительности СКП ЭП, отобранных для разбора конфликтной ситуации, на момент формирования ЭП;

проверку того, что все проверяемые ЭП в ЭД используются в соответствии со сведениями, указанными в СКП ЭП;

проверку отсутствия СКП ЭП, отобранных для разбора конфликтной ситуации, в СОС.

14.18. Если СКП ЭП, необходимый для проверки ЭП, находится в СОС, техническая комиссия принимает решение о действительности ЭП спорного ЭД, используя дату создания ЭД и дату помещения СКП ЭП в СОС.

14.19. В случае, если:

все проверяемые ЭП для данного спорного ЭД верны;

ЭП уполномоченного лица УЦ для каждого СКП ЭП, отобранного для разбора конфликтной ситуации, верна;

СКП ЭП, отобранные для разбора конфликтной ситуации, отсутствуют в СОС;

все проверяемые ЭП в ЭД используются в соответствии со сведениями, указанными в СКП ЭП,

считается установленным:

что проверяемый спорный ЭД был сформирован в соответствии с настоящими Правилами;

проверяемый спорный ЭД был подписан на ключах ЭП, соответствующих СКП ЭП, использовавшихся при проведении технической экспертизы;

владельцами СКП ЭП являются Представители Клиента, зарегистрированные Организатором.

14.20. Стороны признают решения технической комиссии обязательными и обязуются добровольно их исполнять.

14.21. В случае недостижения Сторонами согласия в течение 30 (тридцати) календарных дней после получения письменной претензии Стороной, в том числе в случае отказа одной из Сторон от участия в создании, работе или исполнении решения технической комиссии, спор подлежит разрешению в Арбитражном суде г. Москвы.

15. ПОРЯДОК ДЕЙСТВИЙ ПРИ ВЫЯВЛЕНИИ ПОДОЗРЕНИЙ НА МОШЕННИЧЕСКИЕ ДЕЙСТВИЯ, СОВЕРШЕННЫЕ С ИСПОЛЬЗОВАНИЕМ ЦС ДБО

15.1. Клиент обязуется сообщать Банку об известных ему:

попытках третьих лиц совершить действия, способные привести к нарушению целостности Системы ДБО – незамедлительно, но не позднее рабочего дня, следующего за днем выявления факта;

сбоях в работе Системы ДБО, выходе из строя Системы ДБО либо компьютера, на котором установлен АРМ Системы ДБО – незамедлительно, но не позднее рабочего дня, следующего за днем выявления факта;

операциях, совершенных без согласия Клиента – незамедлительно, но не позднее рабочего дня, следующего за днем получения от Банка уведомления о совершенной операции в соответствии п.7.15 и п.8.5.3 настоящих Правил.

15.2. Информирование Банка осуществляется Клиентом по телефону клиентской поддержки 8 800 775-90-09 или по региональному телефонному номеру, который используется для связи с обслуживаемым филиалом.

15.3. С целью повышения качества обслуживания и снижению риска мошеннических действий в отношении Клиентов, а также своих операционных рисков, Банк выполняет дополнительный контроль расчетных документов, получаемых от Клиентов Банка в электронном виде по Системе ДБО. В процессе выполнения такого контроля возможны обращения работников Банка к Клиенту с целью подтверждения правомерности полученных распоряжений, по которым у Банка при приеме к исполнению возникли подозрения на совершение мошеннических действий в отношении Клиента.

15.4. В случае если при приведении дополнительных проверок при обработке ЭД у Банка возникают подозрения на мошеннические действия в отношении Клиента Банк в обязательном порядке извещает об этом Клиента.

15.5. При получении Банком информации от Клиента в соответствии с п.15.1 настоящих Правил или при наступлении событий, описанных в п.15.4 настоящих Правил, до выяснения всех обстоятельств по инциденту Банком выполняется блокирование АРМ Клиента и перевод его на прием распоряжений на бумажном носителе.

15.6. После блокирования Банком АРМ Клиента в соответствии с п. 15.5 настоящих Правил Клиент в течение трех рабочих дней обязан подать письменное заявление на приостановление действия СКП ЭП. В заявлении, составленном в произвольной форме, должны быть подробно изложены все известные Клиенту обстоятельства по выявленным фактам. После подачи заявления Клиентом Стороны проводят совместное расследование выявленного инцидента.

15.7. В случае если по результатам совместного расследования выяснится отсутствие фактов компрометации ключа ЭП, перечисленных в разделе 1 «Термины и

определения», мероприятия в соответствии с требованиями раздела 12.4 настоящих Правил не проводятся.

15.8. При наступлении событий, указанных в п.15.1 и 15.4 настоящих Правил, Клиент обязуется:

установить факт наличия/отсутствия отправленных ЭД в период не работоспособности персонального компьютера¹⁰ с установленным АРМ Системы ДБО;

прекратить работу на ПК, с использованием которого, по мнению Клиента, совершены мошеннические действия, в том числе не допустить проверку ПК антивирусными средствами, либо другие действия, которые способны внести изменения в информацию, содержащуюся на жестком диске, до снятия его образа, так как это уничтожит временные атрибуты файлов и, возможно, тела вредоносного программного обеспечения, что сделает невозможным проведение полноценного исследования;

завершить работу ПК путем отключения его электропитания, зафиксировать факт отключения, обеспечить невозможность включения ПК и его физическую недоступность до прибытия сотрудников правоохранительных органов или специалистов из организаций, специализирующихся в расследовании компьютерных преступлений;

собрать и представить в Банк дополнительную информацию по инциденту при наличии журналов сетевого доступа, а также возможно других журналов из информационной структуры Клиента.

15.9. Если в результате расследования обнаружен или предполагается факт установки на АРМ Клиента Системы ДБО вредоносного ПО Клиент согласует с представителем Банка срок удаления с АРМ Системы ДБО вредоносного ПО и приведения АРМ в соответствие требованиям Руководства по обеспечению информационной безопасности (Приложение 7 к настоящим Правилам).

15.10. Банк в согласованный с Клиентом, по возможности минимальный срок, проводит выездной контроль АРМ Системы ДБО на соответствие требованиям вышеуказанного Руководства по обеспечению информационной безопасности, с составлением Акта о соблюдении Клиентом требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ Системы ДБО (Приложение 8 к настоящим Правилам).

15.11. В случае отказа от проведения выездного контроля, Клиент в недельный срок направляет в Банк письмо, подтверждающее удаление вредоносного ПО и Анкету о соблюдении Клиентом требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ Системы ДБО (Приложение 9 к настоящим Правилам).

15.12. В случае отказа Клиента от письменного подтверждения удаления вредоносного ПО с АРМ Клиента Системы ДБО и предоставления Анкеты о соблюдении требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ Системы ДБО (Приложение 9 к настоящим Правилам) Банк вправе приостановить использование Клиентом Системы ДБО на неопределенный срок.

15.13. Разблокировка АРМ Клиента осуществляется только после проведения работ согласно пп. 15.9 и 15.10 настоящих Правил, приведения АРМ в соответствие требованиям Руководства по обеспечению информационной безопасности (Приложение 7 к настоящим Правилам) и получения Банком Акта или Анкеты о соблюдении требований Руководства по обеспечению безопасности использования

¹⁰ Далее – ПК

электронной подписи и средств электронной подписи при эксплуатации АРМ Системы ДБО (Приложения 8 или 9 к настоящим Правилам).

Приложение 1.

Заявление о присоединении к Регламенту Удостоверяющего центра и Правилам пользования централизованной системой ДБО

В Банк «Возрождение» (ПАО)

Заявление о присоединении

(Для юридических лиц: полное наименование юридического лица, включая организационно-правовую форму, ИНН,

ОГРН. Для индивидуальных предпринимателей: фамилия, имя, отчество индивидуального предпринимателя,

ИНН, ОГРНИП)

(адрес: область, город,¹¹)

в лице _____

(должность, фамилия, имя, отчество)

действующего на основании _____

в соответствии со ст. 428 ГК РФ полностью и безусловно присоединяется к Регламенту Удостоверяющего центра Банка «Возрождение» (ПАО) и Правилам пользования централизованной системой дистанционного банковского обслуживания Банка «Возрождение» (ПАО), условия которых определены Банком «Возрождение» (ПАО) и опубликованы на сайте Банка «Возрождение» (ПАО) <http://www.vbank.ru/> и принимает порядок и условия электронного документооборота. Об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки проинформирован(а).

(Должность и Ф.И.О. руководителя организации/ИП)

(Подпись руководителя организации/ИП)

« ____ » _____ 20 ____ г.

(дата подписания заявления)

(м.п.)

Отметки Банка:

Заявление принято: « ____ » _____ 20 ____ г.

Договор № _____

(должность)

(подпись)

(Ф.И.О.)

Приложение 2.

Заявление на регистрацию пользователя УЦ и выпуск сертификата ключа проверки электронной подписи для использования в ЦС ДБО.

В Удостоверяющий центр Банка «Возрождение» (ПАО)

Заявление на регистрацию пользователя Удостоверяющего центра Банка «Возрождение» (ПАО) и выпуск сертификата ключа проверки электронной подписи для использования в ЦС ДБО

Прошу:

1. Зарегистрировать меня в качестве пользователя Удостоверяющего центра Банка «Возрождение» (ПАО), изготовить мне технологический ключ *, выпустить технологический СКП ЭП * и выпустить СКП ЭП в соответствии с предоставленными мной идентификационными данными.

2. Настоящим я, _____
(должность, фамилия, имя, отчество)

(серия и номер удостоверения личности, кем и когда выдано)

предоставляю УЦ Банка «Возрождение» (ПАО) в соответствии с Федеральным законом от 27 июля 2006г. №152-ФЗ «О персональных данных» свое: согласие на обработку моих персональных данных для целей заключения и исполнения договоров, в том числе на осуществление банковских операций и предоставление всех видов банковских услуг, иных договоров с Банком.

Согласие дано на срок 5 лет, и считается продлённым на тот же срок, если не отозвано путём предоставления в УЦ заявления в простой письменной форме.

3. С условиями и порядком использования ЭП и средств ЭП, рисках, связанных с использованием ЭП, мерах, необходимых для обеспечения безопасности ЭП ознакомлен.

Владелец СКП ЭП - полномочный
представитель организации

(подпись) (фамилия, имя, отчество)

« ____ » _____ 20__ г.

(фамилия, имя, отчество владельца СКП ЭП), номер моб. телефона для SMS-информирования)

уполномочивается выступать в роли **Пользователя Удостоверяющего центра** Банка «Возрождение» (ПАО) и совершать действия в рамках Регламента Удостоверяющего центра Банка «Возрождение» (ПАО) и Правил пользования централизованной системой дистанционного банковского обслуживания Банка «Возрождение» (ПАО), от имени и в интересах

(для юридических лиц: полное наименование, ИНН, ОГРН, для ИП: ФИО, ИНН, ОГРН)

использовать ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной подписи, владельцем которого является указанное доверенное лицо, в том числе подписывать распоряжения на проведение операций по счетам и иные электронные документы в соответствии с полномочиями, указанными в Списке лиц, имеющих доступ к Системе ДБО.

Настоящие полномочия действуют до прекращения полномочий по распоряжению денежными средствами на счетах, подключенных к Системе ДБО, либо полномочий предоставленных в соответствии с другими договорами, подключенными к Системе ДБО.

(должность и ФИО руководителя организации / ФИО ИП)

(подпись руководителя организации / ИП)

« ____ » _____ 20__ г.

(дата подписания заявления)

(печать)

* – отметки проставляются для Клиентов подсистемы Интернет-Клиент Системы Corrects и подсистемы Клиент-Банк Системы BS-Client

Приложение 2а.

Заявление на выпуск сертификата ключа проверки электронной подписи для использования в ЦС ДБО.

В Удостоверяющий центр Банка «Возрождение» (ПАО)

Заявление на выпуск сертификата ключа проверки электронной подписи для использования в ЦС ДБО

Прошу:

1. Выпустить сертификат ключа проверки электронной подписи (СКП ЭП) в соответствии с предоставленными мной идентификационными данными.
2. С условиями и порядком использования ЭП и средств ЭП, рисках, связанных с использованием ЭП, мерах, необходимых для обеспечения безопасности ЭП ознакомлен.

Владелец СКП ЭП - полномочный
представитель организации

(подпись)

(фамилия, имя, отчество)

« ____ » _____ 20__ г.

(фамилия, имя, отчество владельца СКП ЭП), номер моб. телефона для SMS-информирования)

уполномочивается выступать в роли **Пользователя Удостоверяющего центра** Банка «Возрождение» (ПАО) и совершать действия в рамках Регламента Удостоверяющего центра Банка «Возрождение» (ПАО) и Правил пользования централизованной системой дистанционного банковского обслуживания Банка «Возрождение» (ПАО), от имени и в интересах

(для юридических лиц: полное наименование, ИНН, ОГРН, для ИП: ФИО, ИНН, ОГРН)

использовать ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной подписи, владельцем которого является указанное доверенное лицо, в том числе подписывать распоряжения на проведение операций по счетам и иные электронные документы в соответствии с полномочиями, указанными в Списке лиц, имеющим доступ к Системе ДБО. Настоящие полномочия действуют до прекращения полномочий по распоряжению денежными средствами на счетах, подключенных к Системе ДБО, либо полномочий предоставленных в соответствии с другими договорами, подключенными к Системе ДБО.

(должность и ФИО руководителя организации / ФИО ИП)

(подпись руководителя организации / ИП)

« ____ » _____ 20__ г.

(дата подписания заявления)

(печать)

Приложение 3.

Заявление на аннулирование сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра

В Удостоверяющий центр Банка «Возрождение» (ПАО)

**Заявление
на аннулирование сертификата ключа проверки электронной подписи
пользователя Удостоверяющего центра Банка «Возрождение» (ПАО)**

_____ (наименование Клиента, включая организационно-правовую форму, ИНН)

в лице _____ (должность)

_____ (фамилия, имя, отчество)

действующего на основании _____

в связи с _____ (причина аннулирования сертификата)

Просит аннулировать сертификат ключа проверки электронной подписи своего уполномоченного представителя – Пользователя Удостоверяющего центра Банка «Возрождение» (ПАО):

_____ (фамилия, имя, отчество)

SerialNumber (SN)	Серийный номер сертификата ключа проверки электронной подписи
-------------------	---

_____ (Должность и Ф.И.О.)

_____ (Подпись)

« ____ » _____ 20__ г.
(дата подписания заявления)

(м.п.)

Данное заявление на аннулирование сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра Банка «Возрождение» (ПАО) зарегистрировано в филиале Банка.

Регистрационный № _____ от « ____ » _____ 20__ г.

Ответственный сотрудник Банка

_____ (Подпись)

_____ (Фамилия, инициалы)

Приложение 4.

Доверенность на получение криптографических ключей, документов, программного и информационного обеспечения для работы с СКП ЭП

Доверенность № _____

Г. _____ " ____ " _____ 20__ г.
(место выдачи)

_____, далее – Клиент,
(полное наименование Клиента, включая организационно-правовую форму, ИНН)

В лице _____, действующего на
(должность, фамилия, имя, отчество)

основании _____, уполномочивает

(должность, фамилия, имя, отчество уполномоченного представителя)

(Гражданство, Дата и место рождения)

(Паспортные данные: серия, номер, орган, выдавший паспорт, дата выдачи, код подразделения)

(Адрес места жительства или места пребывания)

Реквизиты документа, подтверждающего право иностранного гражданина или лица без гражданства временно или постоянно проживать на территории РФ (в случае, если лицо является иностранным гражданином или лицом без гражданства), Телефон для связи.

на выполнение следующих действий:

- получать Комплекты подключения;
- получать отдельные компоненты из состава Комплекта подключения (при необходимости);
- получать технологические ключи электронной подписи и технологические СКП ЭП уполномоченных представителей Клиента;
- получать СКП ЭП УЦ, СКП ЭП уполномоченных представителей Клиента в виде электронного документа с электронной подписью УЦ;
- получать ключи простой ЭП уполномоченных представителей Клиента (Микро-комплекты подключения);
- подписывать все необходимые для выполнения вышеуказанных действий документы.

Настоящая доверенность действительна до " ____ " _____ 20__ года.

Образец подписи уполномоченного представителя Клиента

_____/_____
(подпись) (Фамилия и инициалы)

Руководитель Клиента _____/_____
(подпись) (Фамилия и инициалы)

М.П.

Примечание: СКП ЭП Уполномоченных представителей Клиента, а так же СКП ЭП УЦ на бумажном носителе представляются по отдельному запросу Клиента.

Приложение 4А.

Доверенность на полномочного представителя клиента для работы с СКП ЭП (для конфигураций «Корпоративный контроль» и «Мультиклиент»)

Доверенность № _____

Г. _____ " ____ " _____ 20__ г.
(место выдачи)

_____, далее – Клиент,
(полное наименование Клиента, включая организационно-правовую форму, ИНН)

в лице _____, действующего на
(должность, фамилия, имя, отчество)

основании _____, уполномочивает владельца СКПЭП

(должность, фамилия, имя, отчество уполномоченного представителя)

(Гражданство, Дата и место рождения)

(Паспортные данные: серия, номер, орган, выдавший паспорт, дата выдачи, код подразделения)

(Адрес места жительства или места пребывания)

Реквизиты документа, подтверждающего право иностранного гражданина или лица без гражданства временно или

постоянно проживать на территории РФ (в случае, если лицо является иностранным гражданином или лицом без

гражданства), Телефон для связи.

серийный номер _____,
(указывается серийный номер сертификата ключа подписи, владельцем которого является уполномоченный представитель)

выпущенного Удостоверяющим центром Банка «Возрождение» (ПАО), на выполнение следующих действий по счетам организации (необходимое отметить):

- просмотр
- единственная визирующая подпись
- визирующая подпись 1
- визирующая подпись 2
- единственная подпись
- подпись 1
- подпись 2

Настоящая доверенность действительна до¹² " ____ " _____ 20__ года.

Образец подписи владельца СКП ЭП - полномочного представителя организации

_____/_____
(подпись) (Фамилия и инициалы)

Руководитель Клиента _____/_____
(подпись) (Фамилия и инициалы)

М.П.

¹² Срок действия доверенности не может превышать срока действия СКП ЭП, указанного в сертификате.

Приложение 5.

Заявление на установку (настройку) Системы ДБО

В Банк «Возрождение» (ПАО)

ЗАЯВЛЕНИЕ на установку (настройку) Системы ДБО и подключение/отключение услуги «SMS/e-mail информирование»¹³

(сокращенное наименование юридического лица, включая организационно-правовую форму, ИНН, или фамилия, имя, отчество физического лица

(индивидуального предпринимателя), ИНН)

На основании Правил пользования Системой ДБО просим:

1. **Установить / изменить / восстановить (ненужное зачеркнуть)** Систему ДБО в следующей конфигурации:

<input type="checkbox"/> Подсистема Интернет-Клиент Системы Corrects (рекомендуется) В том числе в конфигурации: <input type="checkbox"/> «Корпоративный Контроль» <input type="checkbox"/> «Мультиклиент»	<input type="checkbox"/> Подсистема Интернет-Клиент Системы BS-Client В том числе в конфигурации: <input type="checkbox"/> «Корпоративный Контроль» <input type="checkbox"/> «Мультиклиент»
--	---

Сведения для установки Системы:

Требуется предоставление СКЗИ

Установка Системы будет произведена

Тип НКПИ

Адрес места установки Системы ДБО

ДА НЕТ

Клиентом самостоятельно

специалистом Банка

USB

Смарт-карта, средство визуализации ЭП SafeTouch¹⁴

Сведения о контактном лице Клиента, ответственном за эксплуатацию Системы ДБО

(Ф.И.О.)

Телефон (ы)

E-mail

Время работы (перерыв)

2. **Предоставить (рекомендуется) / не предоставлять / отключить (ненужное зачеркнуть)** услугу по отправке SMS/email сообщений с информацией об операциях по банковским счетам Клиента¹⁵:

Реквизиты для направления Клиенту уведомления при информировании о каждой операции с использованием Системы ДБО (поля заполняются машинописным способом).

Вид уведомления (отметить все необходимые варианты)	Номер телефона сотовой связи	Адрес электронной почты
<input type="checkbox"/> SMS <input type="checkbox"/> Email		

(должность и ФИО руководителя организации или ФИО физического лица)

(подпись руководителя организации или физического лица)

« ____ » _____ 20__ г.
(дата подписания заявления)

¹³ Не предоставляется в случае подписания Клиентом Заявления на предоставление комплексного банковского обслуживания.

¹⁴ Только для подсистемы Интернет-Клиент Системы BS-Client

¹⁵ Перечень операций, о которых направляются сообщения, определяется настоящими Правилами.

Приложение 6.

Акт о передаче программного обеспечения Системы ДБО и ключей ЭП

Акт № - _____ -BSS

о передаче программного обеспечения Системы ДБО и ключей ЭП

от «_____» «_____» 20__ г.

Мы, нижеподписавшиеся, уполномоченный представитель Банка «Возрождение» (ПАО) в лице _____ с одной стороны и уполномоченный представитель: _____ в лице _____, действующий (ей) на основании _____, с другой стороны, составили настоящий акт о том, что уполномоченный представитель Банка передал, а уполномоченный представитель Клиента получил программное и аппаратное обеспечение Системы ДБО и ключи ЭП, которые будут установлены на компьютер(ы) _____ Клиента, находящийся по адресу: _____

№ п/п	Переданные средства	Отметка о передаче
1	Диск № _____ с дистрибутивом СКЗИ, эксплуатационной документацией к нему, ПО для работы с сертифицированными НКПИ, дистрибутивом АРМ Клиента и эксплуатационной документацией для клиентского АРМ Системы ДБО	
2	Лицензия на использование СКЗИ КриптоПро CSP на бумажном носителе серийный номер – _____	
3	НКПИ в комплекте, ID _____ в форм-факторе: <input type="checkbox"/> - USB <input type="checkbox"/> - Смарт-карта *, Дополнительно <input type="checkbox"/> - SafeTouch *	
4	Ключ простой ЭП – PIN-конверт с логином и паролем **, ID _____ для уполномоченного лица Клиента – будущего владельца СКП ЭП _____ (фамилия, имя, отчество будущего владельца СКП ЭП)	
5	Технологический ключ в НКПИ и технологический СКП ЭП **, ID _____, серийный № СКП ЭП _____	
6	АРМ Клиента сконфигурирован в следующей комплектации (нужное подчеркнуть) <input type="checkbox"/> Комплект Интернет-Клиент Системы BS-Client <input type="checkbox"/> Комплект Интернет-Клиент Системы Correqts <input type="checkbox"/> Комплект Интернет-Клиент Системы BS-Client в конфигурации "Мультиклиент" <input type="checkbox"/> Комплект Интернет-Клиент Системы BS-Client в конфигурации "Корпоративный контроль" <input type="checkbox"/> Комплект Системы BS-Client "Клиент-Банк Офис"	

Стороны признают, что на основании пунктов 4, 5 данного Акта Уполномоченное лицо Клиента, указанное в п. 4, является владельцем технологического СКП ЭП, серийный № СКП ЭП _____.

Настоящий Акт является основанием для удержания Банком комиссионного вознаграждения за оказание услуги по подключению Клиента к Системе дистанционного банковского обслуживания Банка в соответствии с Тарифами Банка и составлен в двух экземплярах, имеющих одинаковую юридическую силу – по одному экземпляру для каждой стороны.

Уполномоченный представитель Клиента

Уполномоченный представитель Банка

(должность представителя Клиента)

(должность представителя Банка)

(подпись, фамилия, инициалы представителя Клиента)

(подпись, фамилия, инициалы представителя Банка)

* - используется только в Системе BS-Client

** - используется в Системах BS-Client и Correqts

Инструкция по оформлению Акта о передаче программного обеспечения Системы ДБО

1. Акт оформляется во всех случаях передачи программного обеспечения, указанных в таблице, и оформляется на каждое физическое лицо Клиента – владельца СКП ЭП и на каждый его новый рабочий СКП ЭП.
2. В графе «Уполномоченный представитель Клиента» в нижней левой части Акта должно расписаться физическое лицо – уполномоченный представитель Клиента, самостоятельное выработавшее себе новый рабочий ключ ЭП, получившее соответствующий данному рабочему ключу ЭП рабочий СКП ЭП и ознакомившееся с его содержанием.
3. Специалист Банка в присутствии Клиента заполняет в обоих экземплярах Акта реквизиты, подлежащие ручному заполнению.
4. Один экземпляр Акта возвращается Клиенту.

Приложение 7.

Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации Клиентом АРМ Системы ДБО

Для обеспечения безопасности использования электронной подписи и средств электронной подписи Клиенту необходимо обеспечить соблюдение следующих требований по обеспечению информационной безопасности при эксплуатации Клиентом АРМ Системы ДБО

№ п/п	Требования по обеспечению информационной безопасности при эксплуатации Клиентом АРМ Системы ДБО	Признак обязательности
1	а. АРМ Системы ДБО обслуживается уполномоченными лицами Клиента.	++
	б. Клиентом обеспечивается контроль доступа в помещение, в котором размещен АРМ Системы ДБО.	++
	в. Администратор локальной вычислительной сети (ЛВС) и администратор безопасности (при их наличии) ознакомлены с настоящим Руководством.	++
2	а. На АРМ Системы ДБО отсутствуют программы удаленного администрирования (например, RAdmin).	++
	б. Осуществляется периодический контроль активного программного обеспечения (ПО), установленного на АРМ Системы ДБО.	++
3	а. НКПИ и PIN-коды доступа к ним постоянно находятся исключительно у их владельцев, не оставляются ими без присмотра и подключаются к USB-порту АРМ только на время сеанса работы с Банком.	++
	б. По окончании сеанса работы с Банком приложение Системы ДБО закрывается, НКПИ извлекаются из АРМ, при уходе с рабочего места НКПИ и носители с PIN-кодами доступа хранятся в недоступном для посторонних месте.	++
4	Режим «Включить кэширование» в настройках средства криптографической защиты информации (СКЗИ) КриптоПро CSP не включен.	++
5	При использовании настройки СКЗИ КриптоПро CSP «Запомнить пароль» сразу после завершения сеанса работы с Банком запомненные пароли обязательно удаляются.	++
6	а. Доступ к АРМ Системы ДБО по сети (локальной, Интернет) запрещен.	+
	б. Запрещен доступ неуполномоченных лиц к каталогам с установленной Системой ДБО.	++
7	Дистрибутив СКЗИ КриптоПро CSP получен на учетном носителе информации по акту приема-передачи, подписанным сотрудником Банка и уполномоченным представителем Клиента и хранится как эталонная копия. Установка СКЗИ КриптоПро CSP проведена с полученного дистрибутива.	++
8	а. На АРМ Системы ДБО установлены все рекомендованные производителем обновления безопасности операционной Системы.	++
	б. АРМ Системы ДБО используется только для работы с Банком, для обновления ПО и антивирусных баз и не используется для посещения любых других ресурсов информационно-телекоммуникационной сети Интернет.	++
9	а. Работа на АРМ Системы ДБО производится под учетной записью обычного пользователя. Администраторские права используются только для установки СКЗИ КриптоПро и Системы ДБО.	++
	б. Стандартная учетная запись «Гость» отключена.	++
	в. Выполнены требования по парольной защите, предусмотренные Руководством пользователя по установке и настройке клиентского АРМ: пароль состоит из прописных и строчных латинских букв и цифр, длина пароля – не менее 8 символов, пароль сменен после первого входа, далее пароль меняется каждые 6 месяцев.	++
10	а. На АРМ Системы ДБО установлено антивирусное ПО в соответствии с требованиями, указанными в формуляре на применяемое СКЗИ. Например, п. 4 раздел 2 Формуляра КриптоПро CSP ЖТЯИ.00050-02 30 01:	++

	«СКЗИ ЖТЯИ. 00050-02 должно использоваться со средствами антивирусной защиты, сертифицированными ФСБ России». Перечень средств защиты информации, сертифицированных ФСБ России: http://clsz.fsb.ru/certification.htm , http://clsz.fsb.ru/files/download/sved_po_certif.pdf .	
	б. Включены настройки антивирусного ПО, установленные разработчиком по умолчанию. Включена защита настроек паролем.	++
	в. На АРМ Системы ДБО дополнительно установлены средства защиты от спама, вредоносного ПО и злоумышленного воздействия.	*
	г. Антивирусные базы обновляются в автоматическом режиме с рекомендуемым разработчиком периодом обновления.	++
	д. Полная проверка АРМ Системы ДБО на наличие вирусов и вредоносного ПО производится в автоматическом режиме с рекомендуемым разработчиком периодом проверки.	++
11	На АРМ Системы ДБО установлен и настроен персональный межсетевой экран, с помощью которого разрешен доступ только к доверенным ресурсам информационно-телекоммуникационной сети Интернет, необходимым для работы с Банком и для обновления лицензионного ПО и антивирусных баз.	*
12	При уходе пользователя АРМ Системы ДБО с рабочего места в течение рабочего дня АРМ блокируется пользователем, после завершения рабочего дня – выключается.	++
13	В случае установки на ноутбук ПО АРМ Системы ДБО, Клиентом обеспечивается раздельное хранение трех компонент: – ноутбука; – НКПИ; – PIN-кодов к НКПИ, логинов и паролей.	++
14	Клиенту известен установленный Банком порядок уведомления обслуживающего филиала Банка о блокировке доступа к счетам в случае утраты НКПИ или PIN-кода доступа к нему.	++
15	Клиенту известен установленный Банком порядок немедленного уведомления обслуживающего филиала Банка о блокировке доступа к счетам в случае внезапной остановки работы Системы ДБО.	++
16	По завершении операционного времени обслуживающего филиала Банка Клиентом контролируется состояние счета путем отправки в Банк запроса промежуточного отчета об операциях по счету.	++
17	Клиенту известен порядок обращения по вопросам работы Системы ДБО в рабочее время по телефонам обслуживающего филиала Банка, круглосуточно – по телефону технической поддержки Системы ДБО 8 800 775-90-09.	+

Примечания:

- пункты Руководства, отмеченные знаком «++», обязательны и должны быть выполнены Клиентом на момент составления Акта/Анкеты/передачи в Банк Заявления на предоставление комплексного обслуживания;
- пункты Руководства, отмеченные знаком «+», обязательны и должны быть выполнены Клиентом в течение 2-х недель после составления Акта/Анкеты/передачи в Банк Заявления на предоставление комплексного обслуживания;
- пункты Руководства, отмеченные знаком «*», имеют рекомендательный характер.

Приложение 8.

Акт о соблюдении Клиентом требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ Системы ДБО

«Утверждаю» от Клиента _____ (должность Руководителя Клиента) _____ (подпись, фамилия, инициалы Руководителя Клиента) М.П.	«Утверждаю» от Банка _____ (должность уполномоченного представителя Банка) _____ (подпись, фамилия, инициалы уполномоченного представителя Банка) М.П.
--	--

Акт № - -BSS

о соблюдении Клиентом требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ Системы ДБО

г. _____ Дата « ____ » « _____ » 20__ г.

Мы, нижеподписавшиеся, представитель Банка «Возрождение» (ПАО) _____, действующий на основании _____, с одной стороны, и представитель: _____,

_____ действующий (ей) на основании _____, с другой стороны, составили настоящий Акт о соответствии АРМ Клиента Требованиям по обеспечению информационной безопасности при эксплуатации Клиентом АРМ Системы ДБО:

№ п/п	Требования по обеспечению информационной безопасности при эксплуатации Клиентом АРМ Системы ДБО	Признак обязательности	Оценка соответствия Требованиям (Да/Нет)
1	а. АРМ Системы ДБО обслуживается уполномоченными лицами Клиента.	++	
	б. Клиентом обеспечивается контроль доступа в помещение, в котором размещен АРМ Системы ДБО.	++	
	в. Администратор локальной вычислительной сети (ЛВС) и администратор безопасности (при их наличии) ознакомлены с Руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации Клиентом АРМ Системы ДБО.	++	
2	а. На АРМ Системы ДБО отсутствуют программы удаленного администрирования (например, RAdmin).	++	
	б. Осуществляется периодический контроль активного программного обеспечения (ПО), установленного на АРМ Системы ДБО.	++	
3	а. НКПИ и PIN-коды доступа к ним постоянно находятся исключительно у их владельцев, не оставляются ими без присмотра и подключаются к USB-порту АРМ только на время сеанса работы с Банком.	++	
	б. По окончании сеанса работы с Банком приложение Системы ДБО закрывается, НКПИ извлекаются из АРМ, при уходе с рабочего места НКПИ и носители с PIN-кодами доступа хранятся в недоступном для посторонних месте.	++	
4	Режим «Включить кэширование» в настройках средства криптографической защиты информации (СКЗИ) КриптоПро CSP не включен.	++	

5	При использовании настройки СКЗИ КриптоПро CSP «Запомнить пароль» сразу после завершения сеанса работы с Банком запомненные пароли обязательно удаляются.	++	
6	а. Доступ к АРМ Системы ДБО по сети (локальной, Интернет) запрещен.	+	
	б. Запрещен доступ неуполномоченных лиц к каталогам с установленной Системой ДБО.	++	
7	Дистрибутив СКЗИ КриптоПро CSP получен на учетном носителе информации по акту приема-передачи, подписанным сотрудником Банка и уполномоченным представителем Клиента и хранится как эталонная копия. Установка СКЗИ КриптоПро CSP проведена с полученного дистрибутива.	++	
8	а. На АРМ Системы ДБО установлены все рекомендованные производителем обновления безопасности операционной Системы.	++	
	б. АРМ Системы ДБО используется только для работы с Банком, для обновления ПО и антивирусных баз и не используется для посещения любых других ресурсов информационно-телекоммуникационной сети Интернет.	++	
9	а. Работа на АРМ Системы ДБО производится под учетной записью обычного пользователя. Администраторские права используются только для установки СКЗИ КриптоПро и Системы ДБО.	++	
	б. Стандартная учетная запись «Гость» отключена.	++	
	в. Выполнены требования по парольной защите, предусмотренные Руководством пользователя по установке и настройке клиентского АРМ: пароль состоит из прописных и строчных латинских букв и цифр, длина пароля – не менее 8 символов, пароль сменен после первого входа, далее пароль меняется каждые 6 месяцев.	++	
10	а. На АРМ Системы ДБО установлено антивирусное ПО в соответствии с требованиями, указанными в формуляре на применяемое СКЗИ. Например, п. 4 раздел 2 Формуляра КриптоПро CSP ЖТЯИ.00050-02 30 01: «СКЗИ ЖТЯИ. 00050-02 должно использоваться со средствами антивирусной защиты, сертифицированными ФСБ России». Перечень средств защиты информации, сертифицированных ФСБ России: http://clsz.fsb.ru/certification.htm , http://clsz.fsb.ru/files/download/sved_po_sertif.pdf .	++	
	б. Включены настройки антивирусного ПО, установленные разработчиком по умолчанию. Включена защита настроек паролем.	++	
	в. На АРМ Системы ДБО дополнительно установлены средства защиты от спама, вредоносного ПО и злоумышленного воздействия.	*	
	г. Антивирусные базы обновляются в автоматическом режиме с рекомендуемым разработчиком периодом обновления.	++	
	д. Полная проверка АРМ Системы ДБО на наличие вирусов и вредоносного ПО производится в автоматическом режиме с рекомендуемым разработчиком периодом проверки.	++	
11	На АРМ Системы ДБО установлен и настроен персональный межсетевой экран, с помощью которого разрешен доступ только к доверенным ресурсам информационно-телекоммуникационной	*	

	сети Интернет, необходимым для работы с Банком и для обновления лицензионного ПО и антивирусных баз.		
12	При уходе пользователя АРМ Системы ДБО с рабочего места в течение рабочего дня АРМ блокируется пользователем, после завершения рабочего дня – выключается.	++	
13	В случае установки на ноутбук ПО АРМ Системы ДБО, Клиентом обеспечивается раздельное хранение трех компонент: – ноутбука; – НКПИ; – PIN-кодов к НКПИ, логинов и паролей.	++	
14	Клиенту известен установленный Банком порядок уведомления обслуживающего филиала Банка о блокировке доступа к счетам в случае утраты НКПИ или PIN-кода доступа к нему.	++	
15	Клиенту известен установленный Банком порядок немедленного уведомления обслуживающего филиала Банка о блокировке доступа к счетам в случае внезапной остановки работы Системы ДБО.	++	
16	По завершении операционного времени обслуживающего филиала Банка Клиентом контролируется состояние счета путем отправки в Банк запроса промежуточного отчета об операциях по счету.	++	
17	Клиенту известен порядок обращения по вопросам работы Системы ДБО в рабочее время по телефонам обслуживающего филиала Банка, круглосуточно – по телефону технической поддержки Системы ДБО 8 800 775-90-09.	+	

Настоящий Акт составлен в двух экземплярах, имеющих одинаковую юридическую силу – по одному экземпляру для каждой стороны

Примечания:

- пункты Требований, отмеченные знаком «++», обязательны и должны быть выполнены Клиентом на момент составления Акта;
- пункты Требований, отмеченные знаком «+», обязательны и должны быть выполнены Клиентом в течение 2-х недель после составления Акта;
- пункты Требований, отмеченные знаком «*», имеют рекомендательный характер.

<p>Уполномоченный представитель Клиента</p> <p>_____</p> <p>(должность представителя Клиента)</p> <p>_____</p> <p>(подпись, фамилия, инициалы представителя Клиента)</p>	<p>Уполномоченный представитель Банка</p> <p>_____</p> <p>(должность представителя Банка)</p> <p>_____</p> <p>(подпись, фамилия, инициалы представителя Банка)</p>
--	--

Приложение 9.

Анкета о результатах выполнения Клиентом требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ Системы ДБО

Анкета № - -BSS

о результатах выполнения Клиентом требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ Системы ДБО

г. _____

Дата « ____ » « _____ » 20__ г.

(полное наименование Клиента, включая организационно-правовую форму, ИНН)

№ п/п	Требования по обеспечению информационной безопасности при эксплуатации Клиентом АРМ Системы ДБО	Признак обязательности	Оценка соответствия Требованиям (Да/Нет)
1	а. АРМ Системы ДБО обслуживается уполномоченными лицами Клиента.	++	
	б. Клиентом обеспечивается контроль доступа в помещение, в котором размещен АРМ Системы ДБО.	++	
	в. Администратор локальной вычислительной сети (ЛВС) и администратор безопасности (при их наличии) ознакомлены с Руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации Клиентом АРМ Системы ДБО.	++	
2	б. На АРМ Системы ДБО отсутствуют программы удаленного администрирования (например, RAdmin).	++	
	в. Осуществляется периодический контроль активного программного обеспечения (ПО), установленного на АРМ Системы ДБО.	++	
3	а. Электронные ключи НКПИ и PIN-коды доступа к ним постоянно находятся исключительно у их владельцев, не оставляются ими без присмотра и подключаются к USB-порту АРМ только на время сеанса работы с Банком.	++	
	б. По окончании сеанса работы с Банком приложение Системы ДБО закрывается, НКПИ извлекаются из АРМ, при уходе с рабочего места НКПИ и носители с PIN-кодами доступа хранятся в недоступном для посторонних месте.	++	
4	Режим «Включить кэширование» в настройках средства криптографической защиты информации (СКЗИ) КриптоПро CSP не включен.	++	
5	При использовании настройки СКЗИ КриптоПро CSP «Запомнить пароль» сразу после завершения сеанса работы с Банком запомненные пароли обязательно удаляются.	++	
6	а. Доступ к АРМ Системы ДБО по сети (локальной, Интернет) запрещен.	+	
	б. Запрещен доступ неуполномоченных лиц к каталогам с установленной Системой ДБО.	++	
7	Дистрибутив СКЗИ КриптоПро CSP получен на учетном носителе информации по акту приема-передачи, подписанным сотрудником Банка и уполномоченным представителем Клиента	++	

	и хранится как эталонная копия. Установка СКЗИ КристоПро CSP проведена с полученного дистрибутива.		
8	а. На АРМ Системы ДБО установлены все рекомендованные производителем обновления безопасности операционной Системы.	++	
	б. АРМ Системы ДБО используется только для работы с Банком, для обновления ПО и антивирусных баз и не используется для посещения любых других ресурсов информационно-телекоммуникационной сети Интернет.	++	
9	а. Работа на АРМ Системы ДБО производится под учетной записью обычного пользователя. Администраторские права используются только для установки СКЗИ КристоПро и Системы ДБО.	++	
	б. Стандартная учетная запись «Гость» отключена.	++	
	в. Выполнены требования по парольной защите, предусмотренные Руководством пользователя по установке и настройке клиентского АРМ: пароль состоит из прописных и строчных латинских букв и цифр, длина пароля – не менее 8 символов, пароль сменен после первого входа, далее пароль меняется каждые 6 месяцев.	++	
10	а. На АРМ Системы ДБО установлено антивирусное ПО в соответствии с требованиями, указанными в формуляре на применяемое СКЗИ. Например, п. 4 раздел 2 Формуляра КристоПро CSP ЖТЯИ.00050-02 30 01: «СКЗИ ЖТЯИ. 00050-02 должно использоваться со средствами антивирусной защиты, сертифицированными ФСБ России». Перечень средств защиты информации, сертифицированных ФСБ России: http://clsz.fsb.ru/certification.htm , http://clsz.fsb.ru/files/download/sved_po_sertif.pdf .	++	
	б. Включены настройки антивирусного ПО, установленные разработчиком по умолчанию. Включена защита настроек паролем.	++	
	в. На АРМ Системы ДБО дополнительно установлены средства защиты от спама, вредоносного ПО и злоумышленного воздействия.	*	
	г. Антивирусные базы обновляются в автоматическом режиме с рекомендуемым разработчиком периодом обновления.	++	
	д. Полная проверка АРМ Системы ДБО на наличие вирусов и вредоносного ПО производится в автоматическом режиме с рекомендуемым разработчиком периодом проверки.	++	
11	На АРМ Системы ДБО установлен и настроен персональный межсетевой экран, с помощью которого разрешен доступ только к доверенным ресурсам информационно-телекоммуникационной сети Интернет, необходимым для работы с Банком и для обновления лицензионного ПО и антивирусных баз.	*	
12	При уходе пользователя АРМ Системы ДБО с рабочего места в течение рабочего дня АРМ блокируется пользователем, после завершения рабочего дня – выключается.	++	
13	В случае установки на ноутбук ПО АРМ Системы ДБО, Клиентом обеспечивается отдельное хранение трех компонент: – ноутбука; – НКПИ; – PIN-кодов к НКПИ, логинов и паролей.	++	

14	Клиенту известен установленный Банком порядок уведомления обслуживающего филиала Банка о блокировке доступа к счетам в случае утраты НКПИ или PIN-кода доступа к нему.	++	
15	Клиенту известен установленный Банком порядок немедленного уведомления обслуживающего филиала Банка о блокировке доступа к счетам в случае внезапной остановки работы Системы ДБО.	++	
16	По завершении операционного времени обслуживающего филиала Банка Клиентом контролируется состояние счета путем отправки в Банк запроса промежуточного отчета об операциях по счету.	++	
17	Клиенту известен порядок обращения по вопросам работы Системы ДБО в рабочее время по телефонам обслуживающего филиала Банка, круглосуточно – по телефону технической поддержки Системы ДБО 8-800-775-90-09..	+	

Примечания:

- пункты Требований, отмеченные знаком «++», обязательны и должны быть выполнены Клиентом на момент составления Анкеты;
- пункты Требований, отмеченные знаком «+», обязательны и должны быть выполнены Клиентом в течение 2-х недель после составления Анкеты;
- пункты Требований, отмеченные знаком «*», имеют рекомендательный характер.

_____ / Должность представителя Клиента

_____ / (подпись)

_____ / Фамилия, инициалы/

М.П.

Приложение 10.

Акт об оказании услуг по выпуску сертификата ключа проверки электронной подписи в Системе ДБО

Акт № - _____ -BSS

об оказании услуг по выпуску сертификата ключа проверки электронной подписи

Я, нижеподписавшийся, уполномоченный представитель Клиента

(наименование организации / ФИО ИП)

(ФИО представителя)

действующий на основании _____, составил настоящий акт о том, что мною самостоятельно выработан ключ электронной подписи с записью в НКПИ, электронный запрос на СКП ЭП и получен СКП ЭП серийный № _____

С информацией, содержащейся в СКП ЭП, а также с указанием, что действие СКП ЭП приостановлено до получения Банком подписанного мной настоящего Акта, ознакомлен и согласен.

Личная подпись владельца СКП ЭП _____

(подпись)

Настоящим подтверждаю самостоятельную выработку ключа электронной подписи:

(должность руководителя организации Клиента)

(подпись)

ФИО руководителя организации/ИП

М.П.

===== отметки Банка (заполняется работником Банка) =====

Акт о выработке рабочего ключа электронной подписи и получения СКП ЭП получил, предоставленные Клиентом сведения проверил:

(наименование должности работника)

(подпись)

(фамилия и инициалы)

Уполномоченный представитель Банка

(должность)

ФИО

М.П.

« ____ » _____ 20 ____ г.

Приложение 11.

Перечень договоров и Список лиц

Перечень договоров

Номер договора	Дата заключения договора	Наименование договора	Номер счета

Список¹ лиц, имеющих доступ к Системе ДБО

Ф.И.О.	№№ счетов ² состав ЭД, передаваемых со стороны Клиента и передаваемых со стороны Банка в соответствии с Приложением и пп. 8.5.1. и 8.5.2. Правил	Полномочия ^{3,4,5,6}						Основание для доступа		Срок полномочий ⁷		
		подпись 1	подпись 2	единственная подпись	единственная визирующая подпись	визирующая подпись 1	визирующая подпись 2	шифрование	Карточка с образцами подписей и оттиска печати	Доверенность	начало	окончание

М.П.

Руководитель Клиента/ИП

_____/_____
(подпись, фамилия, инициалы)

¹ При изменении сведений, указанных в Приложении, Приложение заменяется на новое.

² Указываются №№ счетов и состав ЭД. Если уполномоченному лицу предоставляется доступ к тем же счетам и составу ЭД, что указаны строчкой выше, ставится отметка «-//-». Состав ЭД указывается только в том случае, если полномочия предоставляются не весь перечень ЭД, приведенных в пп. 8.5.1. и 8.5.2. Правил, а на отдельные выборочные ЭД.

³ В графе «Полномочия» проставляются необходимые отметки «+».

⁴ Полномочия «подпись 1» и «подпись 2» назначаются только представителям юридического лица, если ЭД Клиента должны быть подписаны двумя подписями. Одновременно полномочия «подпись 1» и «подпись 2» не могут быть назначены одному лицу. Если указано хотя бы одно лицо с полномочием «подпись 1», то должно быть в обязательном порядке указано лицо с полномочием «подпись 2» и наоборот.

⁵ Полномочие «единственная подпись» назначается индивидуальному предпринимателю, физическому лицу, занимающемуся в установленном законодательством порядке частной практикой, их представителям – во всех случаях, а также представителям юридического лица, если ЭД юридического лица должны быть подписаны одной подписью.

⁶ Полномочие «шифрование», назначается одному лицу. Для АРМ, используемого только для просмотра документов, указывается «только шифрование», как правило, назначается одному лицу.

⁷ В случае если срок окончания полномочий не определено, то в графе «окончание» ставится отметка «-//-».

Приложение 12.

Акт об оказании услуг по установке и настройке программного обеспечения Системы ДБО представителем Банка

Акт № - - BSS

об оказании услуг по установке и настройке программного обеспечения Системы ДБО представителем Банка

г. _____ « ____ » « _____ » 20__ г.

Мы, нижеподписавшиеся, представитель Банка «Возрождение» (ПАО) _____, действующий на основании _____ с одной стороны, и представитель: _____, действующий (ей) на основании _____, с другой стороны, составили настоящий акт о том, что уполномоченный представитель Банка выполнил следующее работы:

№ п/п	Оказанные услуги
1	Программное обеспечение Системы ДБО установлено/восстановлено (нужное подчеркнуть) на компьютер(ы) Клиента, находящийся по адресу: _____ представителем Банка в следующей комплектации (нужное подчеркнуть). Комплект подсистемы Интернет-Клиент Системы Correpts; Комплект подсистемы Интернет-Клиент Системы BS-Client; Комплект подсистемы Клиент-Банк Системы BS-Client.
Трудозатраты представителя Банка составили _____ часов:	

Настоящий Акт составлен в двух экземплярах, имеющих одинаковую юридическую силу – по одному экземпляру для каждой стороны.

Настоящий Акт является основанием для удержания Банком комиссионного вознаграждения за оказание услуги по подключению Клиента к Системе дистанционного банковского обслуживания Банка в соответствии с тарифами Банка

Уполномоченный представитель Клиента _____ (должность представителя Клиента) _____ (подпись, фамилия, инициалы представителя Клиента)	Уполномоченный представитель Банка _____ (должность представителя Банка) _____ (подпись, фамилия, инициалы представителя Банка)
---	---

Приложение 13.

Правила применения простой ЭП в Системе ДБО

1. Правила применения простой ЭП в Системе BS-Client

- 1.1. Ключом простой ЭП в Подсистеме Интернет-Клиент Системы BS-Client является уникальная пара логин/пароль вырабатываемая Банком в PIN-конверт и однозначно связанная с Клиентом (ИП; лицом, занимающимся частной практикой) или Представителем Клиента – владельцем простой ЭП. Каждый PIN-конверт с ключом простой ЭП маркируется уникальным ID.
- 1.2. Стороны признают, что юридически значимым доказательством принадлежности Клиенту (ИП; лицу, занимающемуся частной практикой) / конкретному Представителю Клиента ключа простой ЭП является подписанный Сторонами Акт о передаче программного обеспечения системы ДБО и ключей ЭП ([Приложение 6](#) к Правилам) с отметкой о передаче в строке 4, колонки «Отметка о передаче»:

№ п/п	Переданные средства	Отметка о передаче
4	Ключ простой ЭП – PIN-конверт с логином и паролем, ID _____ для уполномоченного лица Клиента – владельца сертификата ключа проверки электронной подписи (СКП ЭП) <i>(фамилия, имя, отчество владельца СКП ЭП)</i>	✓

либо подписанный Сторонами Акт о передаче Микро-комплекта подключения к системе ДБО ([Приложение 14](#) к Правилам) либо подписанное Клиентом Заявление на предоставление комплексного обслуживания.

- 1.3. При создании ключа простой ЭП Банк обязуется соблюдать его конфиденциальность.
- 1.4. Клиент (ИП, лицо, занимающееся частной практикой)/Представитель Клиента, использующий ключ простой ЭП, обязан соблюдать конфиденциальность ключа простой ЭП.
- 1.5. Ключ простой ЭП используется Клиентом (ИП; лицом, занимающимся частной практикой)/Представителем Клиента только для первого входа в Систему ДБО без сертификата и подписания первого запроса на выпуск СКП ЭП, формируемого в Системе ДБО. Последующие запросы на выпуск СКП ЭП подписываются действующей усиленной ЭП Клиента (ИП, лица, занимающегося частной практикой)/Представителя Клиента.
- 1.6. Определение в Системе ДБО Клиента (ИП, лица, занимающегося частной практикой)/Представителя Клиента, осуществляющего вход в Систему ДБО и подписывающего первый запрос на выпуск СКП ЭП по его простой ЭП производится на основании имеющихся в Банке сведений о принадлежности Клиенту (ИП; лицу, занимающимся частной практикой)/Представителю Клиента ключа простой ЭП, полученных в соответствии с п. 1.2 настоящих Правил.
- 1.7. При первом входе в Систему ДБО возникает окно с предложением сменить пароль. Клиенту (ИП; лицу, занимающемуся частной практикой)/Представителю Клиента необходимо заблаговременно выработать себе новый пароль. Пароль должен состоять из прописных и строчных латинских букв и цифр. Длина пароля должна быть не менее 8 символов. Пароль необходимо хранить в безопасном месте и изменять каждые 6 месяцев. При вводе Пароля латинские и русские символы, а также заглавные и прописные буквы различаются. Имеются только три последовательные попытки на вход в Систему ДБО, после чего вход будет заблокирован. Для решения проблемы необходимо обратиться к Менеджеру обслуживающего ДО/филиала Банка.
- 1.8. В случае окончания срока действия, по вине Клиента/Представителя Клиента, ранее действующего СКП ЭП, изменения сведений о Клиенте (ИП; лице, занимающимся частной практикой)/Представителе Клиента, включаемых в СКП ЭП, при случайном удалении ключевой информации с НКПИ (сам НКПИ в рабочем состоянии) вход в Систему ДБО и подписание запроса на перевыпуск СКП ЭП, формируемого в Системе ДБО, Клиент (ИП, лицо, занимающееся частной практикой)/Представитель Клиента также использует ключ простой ЭП в соответствии с п. 1.2 настоящих Правил. При этом Клиентом должен быть

получен у Менеджера обслуживающего ДО/филиала Банка новый ключ простой ЭП (Микро-комплект подключения) по Акту о передаче программного обеспечения системы ДБО ([Приложение 6](#)) с отметкой о передаче в строке 4 колонки «Отметка о передаче» в соответствии с п. 2 настоящих Правил либо по Акту о передаче Микро-комплекта подключения к системе ДБО ([Приложение 14](#) к Правилам).

1.9. В подсистеме Клиент-Банк Системы BS-Client простая ЭП не используется.

2. Правила применения простой ЭП в Системе Correqlts

- 2.1. Ключом простой ЭП в Подсистеме Интернет-Клиент Системы Correqlts является уникальная пара логин/пароль вырабатываемая Банком в PIN-конверт и однозначно связанная с Клиентом (ИП; лицом, занимающимся частной практикой) или Представителем Клиента – владельцем простой ЭП. Каждый PIN-конверт с ключом простой ЭП маркируется уникальным ID.
- 2.2. Стороны признают, что юридически значимым доказательством принадлежности Клиенту (ИП; лицу, занимающемуся частной практикой) / конкретному Представителю Клиента ключа простой ЭП является подписанный Сторонами Акт о передаче программного обеспечения системы ДБО и ключей ЭП ([Приложение 6 к Правилам](#)) с отметкой о передаче в строке 4, колонки «Отметка о передаче»:

№ п/п	Переданные средства	Отметка о передаче
4	Ключ простой ЭП – PIN-конверт с логином и паролем, ID _____ для уполномоченного лица Клиента – будущего владельца СКП ЭП (фамилия, имя, отчество будущего владельца СКП ЭП)	√

либо подписанный Сторонами Акт о передаче Микро-комплекта подключения к системе ДБО ([Приложение 14](#)) либо подписанное Клиентом Заявление на предоставление комплексного обслуживания.

- 2.3. При создании ключа простой ЭП Банк обязуются соблюдать его конфиденциальность.
- 2.4. Клиент (ИП, лицо, занимающееся частной практикой)/Представитель Клиента, использующий ключ простой ЭП, обязан соблюдать конфиденциальность ключа простой ЭП.
- 2.5. Ключ простой ЭП используется Клиентом (ИП; лицом, занимающимся частной практикой)/Представителем Клиента совместно с технологическим сертификатом для первого входа в Систему ДБО Correqlts с профилем 2-х факторная аутентификация. Запрос на выпуск СКП ЭП, формируемый в Системе ДБО подписывается технологической подписью Клиента (ИП, лица, занимающегося частной практикой)/Представителя Клиента. Последующие запросы на выпуск СКП ЭП подписываются действующей усиленной ЭП Клиента (ИП, лица, занимающегося частной практикой)/Представителя Клиента.
- 2.6. Определение в Системе ДБО Correqlts Клиента (ИП, лица, занимающегося частной практикой)/Представителя Клиента, осуществляющего вход в Систему ДБО и подписывающего запрос на выпуск СКП ЭП производится на основании имеющихся в Банке сведений о принадлежности Клиенту (ИП; лицу, занимающимся частной практикой)/Представителю Клиента ключа простой ЭП в соответствии с п. 2.2 настоящих Правил и по технологической подписи Клиента (ИП, лица, занимающегося частной практикой)/Представителя Клиента.
- 2.7. Стороны признают, что юридически значимым доказательством принадлежности Клиенту (ИП; лицу, занимающемуся частной практикой) / конкретному Представителю Клиента технологического ключа и технологического СКП ЭП является подписанный Сторонами Акт о передаче программного обеспечения системы ДБО и ключей ЭП ([Приложение 6](#)) с отметкой о передаче в строке 5 колонки «Отметка о передаче»:

№ п/п	Переданные средства	Отметка о передаче
5	Технологический ключ в НКПИ и технологический СКП ЭП, ID _____, серийный № СКП ЭП _____	√

либо подписанное Клиентом Заявление на предоставление комплексного обслуживания.

- 2.8. При первом входе в Систему ДБО возникает окно с предложением сменить пароль. Клиенту (ИП; лицу, занимающемуся частной практикой)/Представителю Клиента необходимо заблаговременно выработать себе новый пароль. Пароль должен состоять из прописных и строчных латинских букв и цифр. Длина пароля должна быть не менее 8 символов. Пароль необходимо хранить в безопасном месте и изменять каждые 6 месяцев. При вводе Пароля

латинские и русские символы, а также заглавные и прописные буквы различаются. Имеются только три последовательные попытки на вход в Систему, после чего вход будет заблокирован. Для решения проблемы необходимо обратиться к Менеджеру обслуживающего ДО/филиала Банка.

Приложение 14.

Акт о передаче микро-комплекта подключения к Системе ДБО

Акт № - _____ -BSS

о передаче Микро-комплекта подключения к Системе ДБО

Я, нижеподписавшийся, уполномоченный представитель Клиента

(наименование организации / ФИО ИП)

(ФИО уполномоченного представителя)

действующий на основании _____, составил настоящий акт о том, что мною получен микро-комплект подключения к Системе ДБО, состоящий из логина и пароля

(идентификатор PIN-конверта)

для уполномоченного лица Клиента – владельца сертификата ключа проверки электронной подписи (СКП ЭП)

(ФИО владельца СКП ЭП)

Личная подпись уполномоченного представителя Клиента _____
(подпись)

===== отметки Банка (заполняется работником Банка) =====

Микро-комплект подключения к Системе ДБО выдал, представленные Клиентом сведения проверил:

Уполномоченный представитель Банка

(наименование должности работника)
(фамилия и инициалы)

(подпись)

м.п.

« ____ » _____ 20 ____ г.