|  |  |
| --- | --- |
|  | **УТВЕРЖДЕНЫ**  **Правлением Банка «Возрождение» (ПАО)**  **протокол от «26» декабря 2018 г. №96-18/П** |

**ПРАВИЛА ПОЛЬЗОВАНИЯ  
ЦЕНТРАЛИЗОВАННОЙ СИСТЕМОЙ**

**ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ**

**БАНКА «ВОЗРОЖДЕНИЕ» (ПАО)**

**Версия 3.4**

Содержание

[1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 4](#_Toc532839746)

[2. ПРЕДМЕТ РЕГУЛИРОВАНИЯ 11](#_Toc532839747)

[3. РЕГУЛИРОВАНИЕ ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ, ПОРЯДОК ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ В СИСТЕМЕ ДБО 11](#_Toc532839748)

[4. ПОРЯДОК И УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ ДОСТУПА КЛИЕНТУ К ОСУЩЕСТВЛЕНИЮ ДОКУМЕНТООБОРОТА В СИСТЕМЕ ДБО 12](#_Toc532839749)

[5. ПОРЯДОК ВСТУПЛЕНИЯ В СИЛУ НАСТОЯЩИХ ПРАВИЛ, ВНЕСЕНИЯ В НИХ ИЗМЕНЕНИЙ И ПРЕКРАЩЕНИЯ ДЕЙСТВИЯ 15](#_Toc532839750)

[6. ПОРЯДОК УВЕДОМЛЕНИЯ О ВНЕСЕНИИ ИЗМЕНЕНИЙ В ПРАВИЛА 15](#_Toc532839751)

[7. ОБЩИЕ ПОЛОЖЕНИЯ 15](#_Toc532839752)

[8. ЭЛЕКТРОННЫЙ ДОКУМЕНТ 20](#_Toc532839753)

[**8.1.** **Требования, предъявляемые к электронному документу** 20](#_Toc532839754)

[**8.2.** **Электронная подпись электронного документа** 20](#_Toc532839755)

[**8.3.** **Подлинник электронного документа** 21](#_Toc532839756)

[**8.4.** **Копии электронного документа на бумажном носителе** 21](#_Toc532839757)

[**8.5.** **Электронные документы, используемые в Системе ДБО** 21](#_Toc532839758)

[9. ОРГАНИЗАЦИЯ ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ 22](#_Toc532839759)

[**9.1.** **Обмен электронными документами** 22](#_Toc532839760)

[**9.2.** **Формирование электронного документа** 23](#_Toc532839761)

[**9.3.** **Отправка и доставка электронного документа** 23](#_Toc532839762)

[**9.4.** **Проверка подлинности доставленного электронного документа** 23](#_Toc532839763)

[**9.5.** **Подтверждение получения электронного документа** 23](#_Toc532839764)

[**9.6.** **Отзыв электронного документа** 24](#_Toc532839765)

[10. ОБЯЗАННОСТИ КЛИЕНТА 24](#_Toc532839766)

[11. ПОРЯДОК ОПЛАТЫ УСЛУГ 25](#_Toc532839767)

[12. СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 26](#_Toc532839768)

[**12.1.** **Порядок формирования криптографических профилей, ключей ЭП и СКП ЭП Клиента, организация обслуживания Клиента** 26](#_Toc532839769)

[**12.2.** **Особенности оформления пакета документов для Клиентов при подключении Системы ДБО в конфигурации «Корпоративный контроль»** 33](#_Toc532839770)

[**12.3.** **Проведение плановой замены ключей ЭП Клиента** 35](#_Toc532839771)

[**12.4.** **Порядок действий при компрометации ключей ЭП или физической порче носителя ключевой информации** 37](#_Toc532839772)

[13. ОТВЕТСТВЕННОСТЬ СТОРОН. ОБСТОЯТЕЛЬСТВА, ИСКЛЮЧАЮЩИЕ ОТВЕТСТВЕННОСТЬ СТОРОН (ФОРС-МАЖОР) 38](#_Toc532839773)

[14. ПОРЯДОК УРЕГУЛИРОВАНИЯ СПОРНЫХ СИТУАЦИЙ 39](#_Toc532839774)

[15. ПОРЯДОК ПРОТИВОДЕЙСТВИЯ ОСУЩЕСТВЛЕНИЮ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ БЕЗ СОГЛАСИЯ КЛИЕНТА С ИСПОЛЬЗОВАНИЕМ ЦС ДБО 43](#_Toc532839775)

[Приложение 1. Заявление о присоединении к Правилам пользования централизованной системой ДБО и Регламенту удостоверяющего центра (для системы ДБО BS-Client и системы ДБО Correqts с СКЗИ) 46](#_Toc532839776)

[Приложение 1а. Заявление о присоединении к Правилам пользования централизованной системой ДБО (для системы ДБО Correqts только со средством электронной подписи PayControl) 47](#_Toc532839777)

[Приложение 2. Заявление на регистрацию пользователя УЦ и выпуск сертификата ключа проверки электронной подписи для использования в ЦС ДБО (для системы ДБО BS-Client и системы ДБО Correqts с СКЗИ) 48](#_Toc532839778)

[Приложение 2а. Заявление на регистрацию пользователя и ключа проверки ЭП PayControl для использования в ЦС ДБО (для системы ДБО Correqts со средством ЭП PayControl)… 49](#_Toc532839779)

[Приложение 3. Заявление на аннулирование сертификата ключа проверки электронной подписи пользователя Удостоверяющего центра (для системы ДБО BS-Client и системы ДБО Correqts с СКЗИ) 50](#_Toc532839780)

[Приложение 3а. Заявление на аннулирование ключа проверки электронной подписи (для системы ДБО Correqts со средством электронной подписи PayControl) 51](#_Toc532839781)

[Приложение 4. Доверенность на получение ключей ЭП, документов, программного и информационного обеспечения для использования в ЦС ДБО 52](#_Toc532839782)

[Приложение 4а. Доверенность на полномочного представителя клиента для работы с СКП ЭП (для системы ДБО BS-Client в конфигурации «Корпоративный контроль» и «Мультиклиент») 53](#_Toc532839783)

[Приложение 5. Заявление на предоставление услуг, установку, настройку, восстановление системы ДБО 54](#_Toc532839784)

[Приложение 6. Акт о передаче программного обеспечения системы ДБО (для системы ДБО BS-Client) 55](#_Toc532839785)

[Приложение 6а. Акт о передаче программного обеспечения системы ДБО (для системы ДБО Correqts с СКЗИ) 57](#_Toc532839786)

[Приложение 6б. Акт о передаче программного обеспечения системы ДБО (для системы ДБО Correqts со средством электронной подписи PayControl) 58](#_Toc532839787)

[Приложение 7. Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации Клиентом АРМ системы ДБО (для системы ДБО BS-Client) 59](#_Toc532839788)

[Приложение 7а. Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации Клиентом АРМ системы ДБО (для системы ДБО Correqts с СКЗИ) 61](#_Toc532839789)

[Приложение 7б. Руководство по обеспечению безопасности использования Клиентом Мобильного устройства (для системы ДБО Correqts со средством электронной подписи PayControl) 63](#_Toc532839790)

[Приложение 8. Акт о соблюдении Клиентом требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ системы ДБО (для системы ДБО BS-Client) 65](#_Toc532839791)

[Приложение 8а. Акт о соблюдении Клиентом требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ системы ДБО (для системы ДБО Correqts с СКЗИ)……… 68](#_Toc532839792)

[Приложение 8б. Акт о соблюдении Клиентом требований Руководства по обеспечению безопасности использования клиентом Мобильного устройства (для системы ДБО Correqts со средством электронной подписи PayControl) 71](#_Toc532839793)

[Приложение 9. Анкета о результатах выполнения Клиентом требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ системы ДБО (для системы ДБО BS-Client)……….. 74](#_Toc532839794)

[Приложение 9а. Анкета о результатах выполнения Клиентом требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ системы ДБО (для системы ДБО Correqts с СКЗИ) 77](#_Toc532839795)

[Приложение 9б. Анкета о результатах соблюдении Клиентом требований Руководства по обеспечению безопасности использования клиентом Мобильного устройства (для системы ДБО Correqts со средством электронной подписи PayControl) 79](#_Toc532839796)

[Приложение 10. Акт об оказании услуг по выпуску сертификата ключа проверки электронной подписи в системе ДБО (для системы ДБО BS-Client, оформляется на бумажном носителе) 8](#_Toc532839797)1

[Приложение 10а. Акт об оказании услуг по выпуску сертификата ключа проверки электронной подписи в системе ДБО (для системы ДБО Correqts с СКЗИ, оформляется в электронном виде) 8](#_Toc532839798)2

[Приложение 10б. Акт об оказании услуг по регистрации ключа проверки электронной подписи PayControl (для системы ДБО Correqts со средством электронной подписи PayControl, оформляется на бумажном носителе) 8](#_Toc532839799)3

[Приложение 11. Перечень договоров и список лиц 8](#_Toc532839800)4

[Приложение 12. Акт об оказании услуг по установке и настройке программного обеспечения системы ДБО представителем Банка 8](#_Toc532839801)5

[Приложение 13. Правила применения простой ЭП в системе ДБО 8](#_Toc532839802)6

[Приложение 14. Акт о передаче микро-комплекта подключения к системе ДБО 9](#_Toc532839803)0

# 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.  В случае использования средства ЭП PayControl в состав АРМ Системы ДБО входит Мобильное устройство |
| Автоматизированное рабочее место разбора конфликтных ситуаций  (АРМ РКС) | Специализированное программное обеспечение (ПО) разработчика из состава ПО:   1. Удостоверяющего центра Банка для систем ДБО с СКЗИ; 2. Системы PayControl для систем ДБО со средством ЭП PayControl. |
| Аннулирование сертификата ключа проверки электронной подписи | процедура, выполняемая Банком, по прекращению действия СКП ЭП Клиента в Системе ДБО, включая аннулирование СКП ЭП Удостоверяющим центром |
| Аннулирование ключа проверки электронной подписи средства ЭП PayControl | процедура, выполняемая Банком, по прекращению действия ключа проверки электронной подписи средства ЭП PayControl Клиента в Системе ДБО |
| 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 |
| Владелец ключа проверки электронной подписи PayControl | лицо, которому в установленном Федеральным законом от 06.04.2011 № 63-ФЗ "Об электронной подписи" порядке Банк зарегистрировал ключ проверки электронной подписи PayControl |
| 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 представлении 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 о присоединении | один из следующих документов, оформленных на бумажном носителе: Заявление о присоединении (Приложение 1, 1а 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 Correqts и описан в соответствующих разделах данных Правил |
| Компрометация криптографических ключей СКЗИ | Утрата доверия к тому, что используемые криптографические ключи обеспечивают безопасность информации. К событиям, связанным с компрометацией криптографических ключей относятся, включая, но не ограничиваясь, следующие:  1. Потеря ключевых носителей.  2. Потеря ключевых носителей с их последующим обнаружением.  3. Увольнение сотрудников, имевших доступ к ключевой информации.  4. Нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа.  5. Возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи.  6. Нарушение печати на сейфе с ключевыми носителями.  7. Случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника)  Различаются два вида компрометации закрытого ключа: явная и неявная. Первые четыре события трактуются как явная компрометация ключей. Следующие три требуют специального рассмотрения в каждом конкретном случае |
| Компрометация ключей ЭП PayControl | Утрата доверия к тому, что используемые ключи средства ЭП PayControl обеспечивают безопасность информации. К событиям, связанным с компрометацией ключей PayControl относятся, включая, но не ограничиваясь, следующие:  1. Потеря Мобильного устройства Клиента с загруженными ключами регистрации и/или выработанными рабочими ключами ЭП.  2. Потеря Мобильного устройства Клиента с загруженными ключами регистрации и/или выработанными рабочими ключами ЭП с последующим обнаружением.  3. Увольнение сотрудников, имевших доступ к Мобильному устройству Клиента с загруженными ключами регистрации и/или выработанными рабочими ключами.  4. Нарушение правил хранения Мобильного устройства Клиента с загруженными ключами регистрации и/или выработанными рабочими ключами.  5. Возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи.  6. Случаи, когда нельзя достоверно установить, что произошло с мобильным устройством Клиента с загруженными и/или выработанными ключами (в том числе случаи, когда Мобильное устройство вышло из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника).  Различаются два вида компрометации закрытого ключа: явная и неявная. Первые четыре события трактуются как явная компрометация ключей. Следующие два требуют специального рассмотрения в каждом конкретном случае. |
| 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) |
| Ключи регистрации PayControl | уникальные ключи, вырабатываемые Банком для каждого Уполномоченного лица Клиента – владельца средства ЭП PayControl. Направляются Банком каждому УЛК Клиента в закодированном виде двумя частями (QR-код + SMS и/или сообщение по электронной почте) |
| Ключ ЭП PayControl | уникальный ключ, самостоятельно вырабатываемый Клиентом одновременно с ключом проверки ЭП PayControl с использованием средства ЭП PayControl при выполнении процедуры первичной выработки ключа ЭП PayControl, а так же при проведении плановой смены ключей ЭП PayControl. Однозначно соответствует ключу проверки ЭП PayControl |
| Ключ проверки ЭП PayControl | уникальный ключ, самостоятельно вырабатываемый Клиентом одновременно с ключом ЭП PayControl с использованием средства ЭП PayControl при выполнении процедуры первичной выработки ключа ЭП PayControl, а так же при проведении плановой смены ключей ЭП PayControl |
| Менеджер | работник Банка, ответственный за взаимодействие c Клиентом в рамках заключённого с ним Договора ДБО |
| Микро-комплект подключения | содержит только ключ простой ЭП. Используется в случаях предусмотренных п.12.3.12 настоящих Правил |
| Мобильное устройство | Смартфон, планшет соответствующие требованиям настоящих Правил, используемые УЛК Клиента для работы в подсистемах Мобильный Бизнес Клиент и/или Интернет-Клиент Системы Correqts. Используется как носитель ключевой информации для средства ЭП PayControl |
| Мошеннические действия | действия, квалифицируемые как «Мошенничество в сфере компьютерной информации» в соответствии со ст. 159.6. Уголовного кодекса Российской Федерации |
| Носитель ключевой информации  (НКИ) | носитель информации, предназначенный для записи, хранения, воспроизведения ключа ЭП. Включает Мобильное устройство с загруженными ключами средства ЭП PayControl |
| Плановая смена ключей для СКЗИ | процедура смены ключа ЭП и СКП ЭП в связи с окончанием срока действия СКП ЭП. Включает создание ключа ЭП, Запроса на СКП ЭП Владельцем СКП ЭП и выдачу нового СКП ЭП Владельцу |
| Плановая смена ключей PayControl | процедура смены ключей регистрации и рабочих ключей ЭП PayControl в связи с окончанием срока их действия. Включает загрузку в Мобильное устройство новых ключей регистрации PayControl, автоматизированную выработку Клиентом нового ключа ЭП PayControl, отправку и регистрацию на сервере PayControl Банка нового ключа проверки ЭП PayControl, оформление Сторонами нового Акта об оказании услуг по регистрации ключа проверки электронной подписи PayControl |
| 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 |
| 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  Средство простой ЭП PayControl не относится к СКЗИ |
| 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 |
| Средство ЭП PayControl | программный комплекс, предназначенный для подтверждения уполномоченным лицом Клиента операций в подсистемах Интернет-Клиент и/или Мобильный Бизнес Клиент системы ДБО Correqts |
| Технологический ключ ЭП 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 отправке Клиентом в Банк запроса на выпуск первого рабочего СКП ЭП |
| Технологический ключ ЭП для подсистемы Интернет-Клиент Системы Correqts | 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 подсистемы Интернет-Клиент Системы Correqts | 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  (УЦ) | Банк «Возрождение» (ПАО) |
| Уполномоченное лицо Клиента (УЛК)  Представитель Клиента | лицо, действующее от имени Клиента в силу полномочия, основанного на доверенности, указании закона либо акте уполномоченного государственного органа или органа местного самоуправления, владелец ключа ЭП |
| Централизованная система дистанционного банковского обслуживания Банка «Возрождение» (ПАО)  (Система) | 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».  Владельцем и Оператором Системы ДБО является Банк.  В Банке эксплуатируются следующие Системы ДБО:   1. Система ДБО «BS-Client» (Система BS-Client). В Систему BS-Client входят следующие подсистемы: 2. подсистема Интернет-Клиент, доступ к которой осуществляется с использованием сайта Банка в сети "Интернет"; 3. подсистема Клиент-Банк, доступ к которой осуществляется с использованием специального программного обеспечения, устанавливаемого на рабочие станции Клиента; 4. Система ДБО «BSS CORREQTS Corporate» (Система Correqts). В Систему Correqts входят следующие подсистемы: 5. подсистема Интернет-Клиент, предоставляет Клиентам Банка доступ к Системе Correqts посредством технологии "тонкий клиент" – Клиенты работают с Системой с ПК через поддерживаемые браузеры; 6. подсистема Мобильный Бизнес Клиент обеспечивает доступ клиентов к услугам системы Correqts посредством приложения Мобильный Бизнес Клиент (Mobile Business Client), устанавливаемого на Мобильном устройстве Клиента. |
| 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/ еmail 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. К SMS-информированию не относится направление SMS-сообщений, связанных с завершением отдельных этапов подключения Клиента к Системе Correqts |

# ПРЕДМЕТ РЕГУЛИРОВАНИЯ

* 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. Заключение Договора ДБО осуществляется в соответствии со ст. 428 ГК РФ путем присоединения Клиента к настоящим Правилам и Регламенту или только к Правилам (в зависимости от выбранной Клиентом конфигурации Системы ДБО и средства ЭП) на основании поданного в Банк Заявления на бумажном носителе. Клиент полностью и безусловно присоединяется к Правилам и Регламенту или только к 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.
  3. Банк вправе без объяснения причин отказать Клиенту в принятии (акцепте) Заявления (заключении Договора ДБО).
  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).
  5. Требования к содержанию электронных документов, порядок их исполнения не являются предметом регулирования настоящих Правил.
  6. Положения настоящих Правил применяются Сторонами при использовании Клиентом подсистем Системы Correqts или Системы BS-Client, если иное не предусмотрено законодательными или иными правовыми актами РФ, включая нормативные акты Банка России.
  7. Если специально не оговорено, что действие конкретного пункта Правил распространяется исключительно на Систему Correqts либо на Систему BS-Client, то считается, что действие пункта Правил распространяется на обе Системы ДБО, включая их подсистемы.

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

* 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.
  2. ЭД, передаваемые в Системе со стороны Клиента, в зависимости от выбранной Клиентом конфигурации Системы ДБО и средства ЭП подписываются:

1. усиленной квалифицированной ЭП (в случае, если Банк может обеспечить выпуск квалифицированных СКП ЭП);
2. усиленной неквалифицированной ЭП, соответствующей ГОСТ Р 34.10-2001/ ГОСТ Р 34.10-2012;
3. простой ЭП PayControl, в соответствии с Правилами применения простой ЭП (п. 3 [Приложения 13](#Приложение13) к настоящим Правилам);
4. простой ЭП в случаях и в порядке, установленных в настоящих Правилах и в соответствии с Правилами применения простой ЭП (пункты 1, 2 [Приложения 13](#Приложение13) к настоящим Правилам).
   1. ЭД, передаваемые в Системе со стороны Банка, подписываются усиленной квалифицированной ЭП. В случае невозможности использования усиленной квалифицированной ЭП, ЭД, передаваемые в Системе со стороны Банка, подписываются усиленной неквалифицированной ЭП.
   2. Стороны признают, что ЭД, подписанные в Системе в соответствии с пунктами 3.2, 3.3 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. Используемые в Системе ДБО для создания усиленной квалифицированной, усиленной неквалифицированной ЭП, их проверки, создания ключа усиленной квалифицированной, усиленной неквалифицированной ЭП и ключа проверки усиленной квалифицированной, усиленной неквалифицированной ЭП 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 27.12.2011 № 796, установленным в соответствии с положениями Федерального закона «Об электронной подписи» от 06.04.2011 № 63-ФЗ. 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.
   4. Используемое в Системе ДБО Correqts средство ЭП PayControl является средством простой ЭП. Стороны признают применение средства простой ЭП PayControl в системе ДБО Correqts достаточным для обеспечения целостности, авторства и неотказуемости передаваемой между Сторонами информации и невозможности ее фальсификации после момента её подписания.
   5. Клиент осознает и принимает на себя все риски, связанные с использованием Системы ДБО в сети Интернет.
   6. При использовании Клиентом аппаратно-программного СКЗИ в форм-факторе смарт-карты снижение рисков, связанных с использованием Системы ДБО, дополнительно обеспечивается средством визуализации ЭП (например, SafeTouch).

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

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

1. представления Клиентом и одобрения Банком пакета документов, необходимых для заключения Договора ДБО и выпуска СКП ЭП Представителям Клиента (если применимо) в соответствии с разделом [12.1](#Раздел_12_1) настоящих Правил;
2. оплаты Клиентом комиссии в соответствии с разделом 11 настоящих Правил;
3. создания Банком и последующей передачи Клиенту комплекта подключения для первичного входа в Систему ДБО;
4. подписания Сторонами на бумажном носителе Акта о передаче программного обеспечения, необходимого для подключения к Системе ДБО по форме [Приложение 6](#Приложение6), [6а](#Приложение6а) или [6б](#Приложение6б) к настоящим Правилам в зависимости от подсистемы систем ДБО BS-Client или Correqts, либо подтверждения Клиентом факта получения программного обеспечения в составе Заявления на предоставление комплексного обслуживания;
5. установки Клиентом на свои рабочие станции/Мобильные устройства необходимых для подключения к соответствующей подсистеме систем ДБО BS-Client или Correqts аппаратных средств и/или специального программного обеспечения, представленного Банком Клиенту;
6. приведения Клиентом своих рабочих станций/Мобильных устройств в соответствие требованиям Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ Системы ДБО (Приложение [7](#Приложение7), [7а](#Приложение7а), [7б](#Приложение7б) к настоящим Правилам в зависимости от используемой Клиентом подсистемы систем ДБО BS-Client или Correqts);
7. 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](#Приложение8), [8а](#Приложение8а), [8б](#Приложение8б) или Приложение [9](#Приложение9), [9а](#Приложение9а), [9б](#Приложение7б) к настоящим Правилам в зависимости от используемой Клиентом подсистемы систем ДБО BS-Client или Correqts);
8. создания Клиентом своих рабочих ключей электронной подписи, получения рабочих СКП ЭП/регистрации Банком ключа проверки ЭП (для средства ЭП PayControl) и подписания Клиентом Акта об оказании услуг по выпуску сертификата ключа проверки электронной подписи (Приложение [10](#Приложение10), [10а](#Приложение10а), [10б](#Приложение10б) к настоящим Правилам в зависимости от используемой Клиентом подсистемы систем ДБО BS-Client или Correqts).
   1. 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 представлены документы, необходимые для 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 обоснования соответствия операций/сделок характеру и масштабам финансово-хозяйственной деятельности Клиента;

Банку стала известна информация об отсутствии Клиента – юридического лица по адресу, указанному в Едином государственном реестре юридических лиц;

не представлены документы, позволяющие однозначно определить законность целей проведения операций и их непричастность к отмыванию преступных доходов, финансированию терроризма и финансированию распространения оружия массового уничтожения;

Клиент включен в перечень организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму, или в перечень организаций и физических лиц, в отношении которых имеются сведения об их причастности к распространению оружия массового уничтожения;

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.

* 1. 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.
  2. 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.
  3. 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 (если применимо);

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

в иных случаях по усмотрению Банка.

* 1. Клиент должен уведомить Банк о своем желании приостановить использование Системы ДБО/расторгнуть Договор ДБО в соответствии с пунктами 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.
  2. Банк уведомляет Клиента о приостановлении использования Системы ДБО в соответствии с пунктами. 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.

* 1. 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.

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

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

# ПОРЯДОК УВЕДОМЛЕНИЯ О ВНЕСЕНИИ ИЗМЕНЕНИЙ В ПРАВИЛА

* 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.
  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.

# ОБЩИЕ ПОЛОЖЕНИЯ

* 1. ЭДО в Системе ДБО регулируется действующим законодательством РФ, нормативными актами Банка России, Регламентом и настоящими Правилами.
  2. В системе ДБО Банка используются сертифицированные программные СКЗИ, аппаратно-программные СКЗИ и средство простой ЭП PayControl (только в системе Correqts). При применении программных СКЗИ Банк обеспечивает эксплуатацию данных СКЗИ в Системе ДБО с обязательным использованием в качестве носителей ключей ЭП НКИ. Представляемые Банком НКИ и аппаратно-программные СКЗИ в форм-факторах USB-ключей или смарт-карт являются персональным средством аутентификации и хранения данных.
  3. Применяемые в Системе ДБО средства ЭП в процессе их использования автоматически выполняют контроль срока действия ключей. Участник Системы ДБО не может подписать ЭД своей ЭП или произвести зашифрование информации в текущий момент времени, если к этому времени истек срок действия его ключей.

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

* 1. Ключи ЭП Клиентов для используемых в Системе ДБО средств ЭП имеют признак – «не экспортируемые» и обеспечивают невозможность копирования/экспорта/хищения ключа ЭП из одного средства ЭП в другое.
  2. Создание технологических ключей/ключей регистрации (для средства ЭП PayControl) Клиента производится работником Банка. Создание рабочих ключей ЭП производится Клиентами самостоятельно.
  3. Стороны признают, что используемые в Системе ДБО шифровальные средства обеспечивают достаточную конфиденциальность ЭДО, а применяемые средства ЭП обеспечивают авторство, целостность и неотказуемость ЭД.
  4. Клиент обязуется:

использовать со средством ЭП PayControl Мобильное устройство, приобретенное у официального продавца и сертифицированное по требованиям ГОСТ в соответствии с действующим законодательством для использования на территории Российской Федерации;

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 и/или средство ЭП PayControl;

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

* 1. Услуги Банка по изготовлению технологических ключей/ключей регистрации (для средства ЭП PayControl), предоставлению СКЗИ, НКИ, средства ЭП PayControl 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>.
  2. В процессе эксплуатации АРМ Системы ДБО/Мобильного устройства Клиент обязуется выполнять требования [Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации Клиентом АРМ Системы ДБО (Приложение 7, [7а](#Приложение7а), [7б](#Приложение7б) к настоящим Правилам в зависимости от используемых Клиентом подсистемы систем ДБО BS-Client или Correqts и средства ЭП)](#Приложение7)[[1]](#footnote-1). Подтверждение выполнения Клиентом требований Руководства по обеспечению информационной безопасности должно быть оформлено Актом либо Анкетой о соблюдении Клиентом требований Руководства по обеспечению информационной безопасности (Приложение [8](#Приложение8), [8а](#Приложение8а), [8б](#Приложение8б) или Приложение [9](#Приложение9), [9а](#Приложение9а), [9б](#Приложение7б) к настоящим Правилам в зависимости от используемых Клиентом подсистемы систем ДБО BS-Client или Correqts и средства ЭП). 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, [7а](#Приложение7а), [7б](#Приложение7б) к настоящим Правилам в зависимости от используемых Клиентом подсистемы систем ДБО BS-Client или Correqts](#Приложение7) и средства ЭП)](#Приложение7) и другие условия Правил в части использования Клиентом электронной подписи и средств электронной подписи.

* 1. Владельцами ключей ЭП в Системе ДБО являются физические лица – уполномоченные лица Клиента и Банка.

Полномочия владельцев ключей ЭП Клиента подтверждаются карточкой с образцами подписей и оттиска печати[[2]](#footnote-2), иными предусмотренными действующим законодательством документами, а также выданными данным лицам доверенностями для работы в Системе (при необходимости).

Полномочия владельцев ключей ЭП сотрудников Банка подтверждаются Приказами о назначении на должность.

* 1. ЭДО осуществляется в связи с исполнением договоров Сторон, указанных в Перечне договоров ([Приложение 11](#Приложение11) к настоящим Правилам).
  2. При изменении списка договоров, состава и полномочий Уполномоченных лиц 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](#Раздел_8_5_ЭД_используемые_в_системе), Клиент представляет новый Перечень договоров и Список лиц, имеющих доступ к Системе ДБО ([Приложение 11](#Приложение11) к настоящим Правилам). Ключи ЭП изготавливаются только новым Представителям Клиента в случае добавления их в Список лиц, имеющих доступ к Системе ДБО. Для Уполномоченных лиц Клиента, полномочия которых в соответствии с новым Списком лиц прекращены, выполняются мероприятия по аннулированию СКП ЭП/ключа проверки ЭП (для средства ЭП PayControl) в соответствии с [разделом 12.4](#Раздел_12_4) настоящих Правил, если к моменту прекращения полномочий не истек срок действия данного СКП ЭП (ключей ЭП PayControl).
  3. 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](#Приложение11) 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 проставленными полномочиями только лицам, указанным Клиентом в новом Списке лиц.

* 1. Банк обеспечивает хранение СКП ЭП (ключей проверки ЭП PayControl) Клиентов в форме ЭД и возможность получения СКП ЭП (ключей проверки ЭП PayControl) Клиентов в форме ЭД в течение всего срока действия СКП ЭП (ключей проверки ЭП PayControl).
  2. Для оповещения Клиента о принятии к исполнению Банком ЭД «Платежное поручение» используется подсистема «Сервер нотификации».

В адрес Клиента Банк направляет соответствующее уведомление на номер мобильного телефона и/или на адрес электронной почты Клиента, указанный в Заявлении на предоставление услуг, установку, настройку, восстановление Системы ДБО ([Приложение 5](#Приложение5) к настоящим Правилам).

Для оповещения Клиента о принятии к исполнению Банком ЭД «Платежное поручение» также используется услуга СМС-информирование, в случае ее подключения Клиентом в рамках Договора комплексного обслуживания.

Для оповещения Клиента о принятии к исполнению Банком ЭД «Платежное поручение» в адрес Клиента, Банк направляет соответствующее уведомление на номер мобильного телефона, указанный Клиентом в Заявлении по форме Приложения 5 к настоящим Правилам/Заявлении на подключение услуги СМС-информирования.

* 1. Подключение/изменение услуги «SMS/email информирование» проводится только в том офисе Банка, в котором Клиент оформил Заявление. SMS-сообщения и/или email сообщения будут направляться только по тем банковским счетам, которые подключены к Системе ДБО.
  2. 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.
  3. Подключение банковского счета Клиента к Системе ДБО освобождает Банк от обязанности представления выписок по счетам с приложением подтверждающих операции документов на бумажном носителе.
  4. 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.
  5. 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.
  6. 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.

# ЭЛЕКТРОННЫЙ ДОКУМЕНТ

## **Требования, предъявляемые к электронному документу**

* + 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 (если применимо).
    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.

## **Электронная подпись электронного документа**

* + 1. ЭД считается подписанным уполномоченным лицом, если он подписан ключом ЭП, для которого УЦ Банка изготовлен СКП ЭП/зарегистрирован ключ проверки ЭП при использовании средства PayControl.
    2. Замена ключей ЭП не влияет на статус ЭД, если он был подписан действующим на момент подписания ключом ЭП в соответствии с данными Правилами.
    3. У каждого Представителя Стороны имеется ключ ЭП, с использованием которого он подписывает ЭД, за исключением случая использования Клиентом подсистемы Мобильный Бизнес Клиент без PayControl.
    4. ЭД, подписанный средством PayControl, считается подписанным, если он подписан с помощью ключа ЭП, для которого Банком зарегистрирован ключ проверки ЭП. На каждое УЛК формируется собственный ключ ЭП PayControl.
    5. Режим офлайн для средства ЭП PayControl Банком не используется.

## **Подлинник электронного документа**

* + 1. ЭД может иметь неограниченное количество экземпляров.
    2. Все экземпляры ЭД являются подлинниками данного ЭД.
    3. ЭД не может иметь копий в электронном виде.
    4. 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.

## **Копии электронного документа на бумажном носителе**

* + 1. Копии ЭД могут быть изготовлены (распечатаны) на бумажном носителе и должны быть заверены собственноручной подписью лица, уполномоченного Стороной, являющейся отправителем или получателем ЭД.
    2. ЭД и его копии на бумажном носителе должны быть идентичными.

## **Электронные документы, используемые в Системе ДБО**

* + 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 подтверждающих документах;

заявление о переоформлении паспорта сделки;

заявление о закрытии паспорта сделки;

запрос выписки из лицевого счета[[3]](#footnote-3);

запрос на отзыв документа;

документы, для которых формат не установлен - произвольные документы в Банк[[4]](#footnote-4).

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.

* + 1. 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]](#footnote-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;

уведомление о поступлении валюты Российской Федерации на расчетный счет резидента;

платежное поручение в формате МТ103[[6]](#footnote-6).

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.

* + 1. Клиент признает, что в случае его отказа от подключения услуги «SMS/email информирование» Услуги СМС информирование, направление Банком выписки по счету в электронном виде по Системе ДБО в соответствии с пунктами 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».
    2. Клиент признает, что отказ от подключения Услуги «SMS/email информирование» Услуги СМС информирование предоставляемых Банком в соответствии с п. 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.

# ОРГАНИЗАЦИЯ ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ

## **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.

## **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.

## **Отправка и доставка электронного документа**

* + 1. В отношениях между отправителем и получателем ЭД считается исходящим от отправителя, если ЭД отправлен:

самим отправителем, или

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

* + 1. Документ считается доставленным получателю, если отправитель получил подтверждение о доставке.

## **Проверка подлинности доставленного электронного документа**

* + 1. Проверка ЭД включает:

проверку ЭД на соответствие формату, установленному Банком;

проверку подлинности всех электронных подписей ЭД.

* + 1. 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.
    2. 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.

## **Подтверждение получения электронного документа**

* + 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.
    2. Если иное не предусмотрено договорами, заключаемыми между Сторонами, ЭД считается неполученным Банком до тех пор, пока Клиент не получил соответствующее ЭС.
    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.

## **Отзыв электронного документа**

* + 1. Участник Системы ДБО вправе отозвать отправленный электронный документ путем отправки Банку электронного документа «Запрос на отзыв документа», подписанного ЭП Клиента.
    2. В ЭД «Запрос на отзыв документа» указываются реквизиты отзываемого ЭД и причина его отзыва.
    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 исполнен[[7]](#footnote-7).

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

# ОБЯЗАННОСТИ КЛИЕНТА

* + 1. ЭДО осуществляется в соответствии с настоящими Правилами и Регламентом (если применимо). 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.
    2. Установить необходимые для подключения к Системе ДБО аппаратные средства, клиентское программное и информационное обеспечение, а также поддерживать их в работоспособном состоянии.
    3. Выполнить всю совокупность действий, необходимых для получения допуска к осуществлению ЭДО, предусмотренных Регламентом (если применимо) 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](#Приложение7), [7а](#Приложение7а), [7б](#Приложение7б) к настоящим Правилам в зависимости от используемых Клиентом подсистемы систем ДБО BS-Client или Correqts и средств ЭП), организационно-технические требования по обеспечению безопасности информации, установленные в Регламенте и настоящих Правилах.
    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 сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра (для системы ДБО BS-Client и системы ДБО Correqts с СКЗИ), ([Приложение 3](#Приложение3) к настоящим Правилам) или Заявления на аннулирование ключа проверки электронной подписи (для системы ДБО Correqts со средством электронной подписи PayControl) ([Приложение 3а](#Приложение3а) к настоящим Правилам).
    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.
    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.
    7. При возникновении в Системе ДБО ситуаций, признаваемых чрезвычайными в соответствии с Регламентом (если применимо), Клиент признает и исполняет решения, принимаемые Банком в соответствии с Регламентом (если применимо) и настоящими Правилами.
    8. Соблюдать Порядок урегулирования спорных ситуаций и споров, установленный Регламентом (если применимо) и [разделом 14](#Раздел_14) настоящих Правил.

# ПОРЯДОК ОПЛАТЫ УСЛУГ

* + 1. До получения комплекта подключения Системы ДБО Клиент уплачивает Банку комиссионное вознаграждение за подключение к Системе ДБО / предоставление средства СКЗИ / предоставление средства ЭП для подключения к Системе (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/ предоставление средства СКЗИ / предоставление средства ЭП для подключения к Системе, 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](#Приложение6), [6а](#Приложение6а) или [6б](#Приложение6б) к настоящим Правилам, в зависимости от выбранных Клиентом подсистемы систем ДБО BS-Client или Correqts и средства ЭП, к настоящим Правилам.

* + 1. 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](#Приложение12) 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 установку Системы 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 установку Систем 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.

# СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## **Порядок формирования криптографических профилей, ключей ЭП и СКП ЭП Клиента, организация обслуживания Клиента**

* + 1. Клиент передает Менеджеру пакет заверенных надлежащим образом документов, необходимых для формирования криптографического профиля и ключей Клиента.
    2. Пакет документов включает следующие документы:
  1. Заявление о присоединении,
  2. Заявление на регистрацию пользователя Удостоверяющего центра Банка «Возрождение» (ПАО) и выпуск СКП ЭП, [Приложение 2](#Приложение2) к настоящим Правилам (для системы ДБО BS-Client и системы ДБО Correqts с СКЗИ) либо Заявление на регистрацию пользователя и ключа проверки ЭП PayControl для использования в ЦС ДБО, [Приложение 2а](#Приложение2а) (для системы ДБО Correqts со средством ЭП PayControl).
  3. Перечень договоров и Список лиц, имеющих доступ к Системе ДБО ([Приложение 11](#Приложение11) к настоящим Правилам). 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 «+». 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 ([Приложение 2](#Приложение2)), либо вторая часть Заявления на регистрацию пользователя и ключа проверки ЭП PayControl для использования в ЦС ДБО, [Приложение 2а](#Приложение2а) (для системы ДБО Correqts со средством ЭП PayControl);

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» (только для системы ДБО BS-Client). 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» (только для системы ДБО BS-Client). 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» (только для системы ДБО BS-Client) иные полномочия никому не назначаются. Отметка «+» в графе «Полномочия» указывается только в колонке «Шифрование». Данный АРМ используется только для просмотра документов.

* 1. Анкета физического лица на Представителя Клиента, на чье имя будет изготавливаться СКП ЭП Клиента/зарегистрирован ключ проверки ЭП (при использовании средства ЭП PayControl), в случае если данная анкета не представлялась в Банк ранее;
  2. 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;
  3. Доверенность на получение ключей ЭП, документов, программного и информационного обеспечения для работы с СКП ЭП ([Приложение 4](#Приложение4) к настоящим Правилам) в случае получения Комплекта подключения Клиента и эксплуатационной документации на систему ДБО Представителем Клиента, не являющимся лицом, на чье имя будет изготовлен СКП ЭП/зарегистрирован ключ проверки ЭП (при использовании средства ЭП PayControl);
  4. Заявление на предоставление услуг, установку, настройку, восстановление Системы ДБО ([Приложение 5](#Приложение5) к настоящим Правилам);
  5. Акт или Анкету о соблюдении Клиентом требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ Системы ДБО (Приложение [8](#Приложение8), [8а](#Приложение8а), [8б](#Приложение8б) или Приложение [9](#Приложение9), [9а](#Приложение9а), [9б](#Приложение7б) к настоящим Правилам в зависимости от используемых Клиентом подсистемы систем ДБО BS-Client или Correqts и средства ЭП);
  6. Учредительные документы Клиента – юридического лица (если их актуальная редакция отсутствует в Банке);
     1. В случае **первоначального подключения к** [**подсистеме Интернет-Клиент** **Системы BS-Client**](#Приложение5) 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 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](#Приложение6) к настоящим Правилам).;

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

средство визуализации электронной подписи[[8]](#footnote-8) SafeTouch.

* + 1. В случае первоначального подключения к [**подсистеме Интернет-Клиент** **Системы Correqts** **с СКЗИ**](#Приложение5) 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 Correqts;

2 бумажных экземпляра Акта о передаче комплекта подключения для Системы ДБО BSS-Correqts с СКЗИ ([Приложение 6а](#Приложение6а) к настоящим Правилам);

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

* + 1. В случае первоначального подключения к [**подсистеме Интернет-Клиент** **Системы Correqts** **с PayControl, в том числе к подсистеме «Мобильный Бизнес Клиент» с PayControl**](#Приложение5)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 PIN-конверт с уникальной парой логин-пароль УЛК для входа в систему ДБО Correqts, и получения из Банка ключей регистрации – уникальных ключей, вырабатываемых Банком для каждого УЛК – владельца средства ЭП PayControl. Направляются Банком каждому УЛК Клиента в закодированном виде (QR-код + SMS и/или сообщение по электронной почте), создания ключа ЭП и ключа проверки ЭП и регистрации Банком ключа проверки ЭП;

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

* + 1. В случае первоначального подключения к **подсистеме «Мобильный Бизнес Клиент» без PayControl** 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 PIN-конверт с уникальной парой логин-пароль УЛК для входа в систему ДБО Correqts;

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

* + 1. 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 1](#Приложение2)1 к настоящим Правилам):

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

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 ([Приложение 6](#Приложение6) к настоящим Правилам).

* + 1. Каждый комплект подключения вскрывается Менеджером Банка в присутствии представителя Клиента, после чего Сторонами подписывается Акт о передаче программного обеспечения по форме Приложения [6](#Приложение6), [6а](#Приложение6а) или [6б](#Приложение6б) к настоящим Правилам в зависимости от используемых Клиентом подсистемы систем ДБО BS-Client или Correqts и средства ЭП.
    2. 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, подписать два экземпляра Акта (Приложение 6 к настоящим Правилам) и вернуть один экземпляр Менеджеру Банка.
    3. 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 использования в ЦС ДБО ([Приложение 4](#Приложение4) к настоящим Правилам).
    4. Клиент самостоятельно проводит установку Системы ДБО на свои рабочие станции/Мобильные устройства, соответствующие требованиям Руководства по обеспечению информационной безопасности (Приложение [7](#Приложение7), [7а](#Приложение7а), [7б](#Приложение7б) 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](#Приложение8), [8а](#Приложение8а), [8б](#Приложение8б) либо [9](#Приложение9), [9а](#Приложение9а), [9б](#Приложение9б) к настоящим Правилам).

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

* + 1. 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 необходимых при подключении к Системе ДБО комиссии 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](#Приложение12) к настоящим Правилам), а также Акт о соблюдении требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи (Приложение [8](#Приложение8), [8а](#Приложение8а), [8б](#Приложение8б) к настоящим Правилам).

**Выработка рабочих ключей ЭП для систем ДБО с СКЗИ**

* + 1. **Для систем ДБО BS-Client и Correqts с СКЗИ** после установки Системы ДБО на свои рабочие станции Клиент самостоятельно вырабатывает свой ключ ЭП с записью на НКИ – USB-ключ, формирует, подписывает и отправляет в Банк запрос на СКП ЭП. С целью исключения возможности записи ключей ЭП при генерации или при перегенерации на любые другие НКИ, запрещается регистрировать на рабочих станциях Клиента какие-либо считыватели кроме считывателя смарт-карт, запрещается регистрировать все съёмные диски и реестр.
    2. 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.
    3. 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](#Приложение10) к настоящим Правилам). Акт оформляется каждому УЛК Клиента – владельцу СКП ЭП на каждый СКП ЭП.
    4. **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.
    5. **В случае использования Системы Correqts** 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 10а](#Приложение10а) 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.
    6. **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.
    7. **В случае использования Системы Correqts** 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.
    8. После ввода Банком в эксплуатацию нового СКП ЭП процедура создания ключей ЭП завершается, Клиент может приступить к работе с новым комплектом ключей ЭП.
    9. 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).
    10. 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 перегенерацию). Технологический ключ, для которого истек срок действия технологического СКП ЭП, должен быть самостоятельно удален из памяти НКИ уполномоченным представителем Клиента.
    11. 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 перегенерации). 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. Так как сертифицированный НКИ является высоконадежным носителем ключей ЭП, а сам ключ ЭП имеет признак «Не экспортируемый» создание дубликата НКИ не производится.
    13. Каждому ключу ЭП, записанному на НКИ, 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.
    14. 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.

**Выработка рабочих ключей для средства ЭП PayControl**

* + 1. Перед выработкой рабочих ключей средства ЭП PayControl Клиенту необходимо выполнить требования Руководства по обеспечению безопасности использования Клиентом Мобильного устройства (для системы ДБО Correqts со средством электронной подписи PayControl), [Приложение 7б](#Приложение7б) к настоящим Правилам, включая установку приложения PayControl из одного из официальных сервисов Google Play или App Store.
    2. Ключи регистрации средства ЭП PayControl вырабатываются Банком для каждого Уполномоченного лица Клиента – владельца средства ЭП PayControl.
    3. Первая часть ключей регистрации в виде QR-кода направляется Банком каждому УЛК по защищенному каналу подсистемы Интернет-Клиент системы ДБО Correqts и выводится на экран монитора.
    4. Вторая часть ключей регистрации направляется УЛК в виде SMS или сообщения по электронной почте.
    5. После сканирования приложением PayControl Мобильного устройства Клиента первой части ключей регистрации и ввода в приложение PayControl значения второй части из SMS/email сообщения система PayControl выполняет автоматизированную процедуру выработки рабочего ключа ЭП с сохранением его в зашифрованном виде в Мобильном устройстве, отправки в Банк значения ключа проверки ЭП и регистрации ключа проверки ЭП в Банке.
    6. Банк средствами системы ДБО Correqts формирует Акт об оказании услуг по регистрации ключа проверки электронной подписи PayControl ([Приложение 10б](#Приложение10б) к настоящим Правилам) и направляет его Клиенту средствами Системы по защищенному каналу подсистемы Интернет-Клиент Системы ДБО Correqts.
    7. Клиент просматривает полученный Акт об оказании услуг по регистрации ключа проверки электронной подписи PayControl ([Приложение 10б](#Приложение10б) к настоящим Правилам), сравнивает реквизиты Акта, включая Идентификатор пользователя и значение открытого ключа из приложения PayControl Мобильного устройства со значениями в Акте, самостоятельно распечатывает Акт в двух экземплярах с помощью текстового редактора, подписывает и передает два экземпляра Акта Менеджеру Банка.
    8. После получения, проверки и регистрации Акта в Банке процедура регистрации ключа проверки ЭП в Банке завершается и Клиенту направляется SMS/email уведомление о готовности средства ЭП PayControl Клиента к работе.

**Порядок подключения к Подсистеме Мобильный Бизнес Клиент без PayControl**

* + 1. В случае выбора Клиентом услуги «Подсистема Мобильный Бизнес Клиент без PayControl», при первоначальном подключении Клиентом в Заявлении по форме [Приложения 5](#Приложение5) указывается соответствующая отметка.
    2. При добавлении данной услуги действующим Клиентом Заявка на подключение к услуге «Мобильный Бизнес Клиент» направляется Клиентом средствами системы ДБО Correqts.

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

* + 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 офисов Банка обслуживаются счета юридического лица/основного юридического лица холдинга, а в других офисах Банка – счета обособленных подразделений юридического лица / дочерних юридических лиц холдинга.
    2. При предоставлении услуги «Корпоративный контроль» Представителям основного юридического лица холдинга или головного подразделения юридического лица, не требуется выпуск нового СКП ЭП.
    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 офисах 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).

* + 1. Для холдингов:
       1. Для предоставления Представителям основного юридического лица холдинга полномочий просмотра и визирования ЭД дочерних юридических лиц в офисе Банка, обслуживающем основное юридическое лицо холдинга, необходимо оформить следующие документы:

новый Перечень договоров ([Приложение 11](#Приложение11) к настоящим Правилам), где будут указаны все подключаемые счета дочерних юридических лиц и соответствующие полномочия для Представителей основного юридического лица;

доверенность ([Приложение 4а](#Приложение4а) 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;

* + - 1. В целях предоставления Представителем основного юридического лица холдинга полномочий визирования, дополнительно к вышеуказанным документам в офисах 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.
    1. Для Клиентов с территориально распределенной сетью обособленных подразделений:

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

новый Перечень договоров ([Приложение 11](#Приложение11) 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 офисах 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 офисах 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).

* + 1. 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.
    2. 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.

## **Проведение плановой замены ключей ЭП Клиента**

**Для систем ДБО с СКЗИ**

* + 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.
    2. Клиент самостоятельно выполняет процедуру формирования ключа ЭП (обновление ключей Клиента или удаленную перегенерацию) согласно Руководству пользователя и отправку в Банк запроса на выпуск СКП ЭП.
    3. При формировании Клиентом новых ключей ЭП замена НКИ не требуется. Новые ключи ЭП записываются на ранее полученный НКИ. Старые ключи ЭП, если таковые имеются, для которых истекли сроки действия СКП ЭП, должны быть самостоятельно удалены из памяти НКИ уполномоченным Представителем Клиента.
    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.
    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.
    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.
    7. **В случае использования Системы Correqts** 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](#Приложение10) 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.
    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.
    9. После ввода Банком в эксплуатацию нового СКП ЭП процедура создания ключей ЭП завершается, Клиент может приступить к работе с новым комплектом ключей ЭП.
    10. Новые СКП ЭП Представителей Клиента в форме документов на бумажном носителе предоставляются Клиентам в течение пятнадцати рабочих дней после получения соответствующего запроса Клиента.

**Для средства ЭП PayControl**

* + 1. Процедура плановой смены ключей ЭП средства PayControl аналогична процедуре первичной выработки рабочих ключей средства ЭП PayControl с учетом следующего:

1. Заявление на регистрацию пользователя и ключа проверки ЭП PayControl для использования в ЦС ДБО (для системы ДБО Correqts со средством ЭП PayControl), [Приложение 2а](#Приложение2а), не оформляется.
2. Основанием для проведения плановой смены ключей ЭП средства PayControl является направление Клиентом Запроса на продление ключа PayControl, направляемого Клиентом средствами системы Correqts в электронном виде.
   * 1. **Для систем ДБО с СКЗИ** в случаях:
3. истечения срока действия СКП ЭП Клиента и невозможности подписать запрос в Банк на выработку нового СКП ЭП;
4. изменения реквизитов действующего уполномоченного лица Клиента, включаемых в СКП ЭП;
5. смены уполномоченного лица Клиента (при сохранении ключевого носителя);
6. ошибочного удаления Клиентом действующего ключа электронной подписи с ключевого носителя;
7. 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 НКИ Клиенту может не предоставляться;

В случае использования Клиентом подсистем Интернет-Клиент Системы BS-Client или Системы Correqts 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](#Приложение6) к настоящим Правилам) либо отдельному Акту о передаче Микро-комплекта подключения к Системе ДБО ([Приложение 14](#Приложение14)). Для Клиента формируется новый криптографический профиль. Новые технологические ключ и СКП ЭП в данном случае Клиенту подсистемы Интернет-Клиент Системы Correqts 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](#Приложение10) 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 НКИ новый технологический ключ ЭП, а так же новый технологический СКП ЭП Клиента, Клиент должен выполнить действия, предусмотренные п. 12.1 настоящих Правил.

## **Порядок действий при компрометации ключей ЭП или физической порче носителя ключевой информации**

12.4.1. В случае Компрометации ключей ЭП или физической порче носителя ключевой 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 в рабочее время Менеджеру обслуживающего его филиала/ДО Банка или в нерабочее время 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/сотрудник горячей линии Банка выполняет ответный звонок Уполномоченному лицу Клиента. В случае положительной проверки Менеджер/сотрудник горячей линии Банка дает указание Администратору Системы ДБО заблокировать в Системе ДБО соответствующий криптографический профиль Представителя Клиента.

12.4.5 В течение того же рабочего дня (очередного рабочего дня в случае компрометации ключа ЭП в нерабочее время), когда Клиент уведомил Менеджера/сотрудника горячей линии Банка по телефону о компрометации ключа ЭП, Клиент обязан направить на имя Управляющего филиалом/Регионального управляющего ДО Заявление на аннулирование сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра (для системы ДБО BS-Client и системы ДБО Correqts с СКЗИ) ([Приложение 3](#Приложение3) к настоящим Правилам) или Заявление на аннулирование ключа проверки электронной подписи (для системы ДБО Correqts со средством электронной подписи PayControl) ([Приложение 3а](#Приложение3а) к настоящим Правилам). Заявление на аннулирование регистрируется как входящая корреспонденция в установленном в Банке порядке и обязательно помещается в юридическое дело Клиента на бумажном носителе.

12.4.6. В случае компрометации ключа ЭП Клиент должен выполнить действия, предусмотренные п.[12.](#Раздел_12_2)1 настоящих Правил с учетом следующих особенностей:

в случае использования Клиентом подсистем Интернет-Клиент Системы BS-Client и Системы Correqts с СКЗИ новый НКИ 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](#Приложение6) к настоящим Правилам) либо отдельному Акту о передаче Микро-комплекта подключения к Системе ДБО ([Приложение 14](#Приложение14));

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

в случае использования Клиентом средства подписи PayControl для доступа в ЦС ДБО Клиенту необходимо получить комплект подключения (конверт с логином и паролем) и выполнить действия согласно пункту 12.1 настоящих Правил.

12.4.7. В случае физической порчи НКИ Клиент должен выполнить действия, предусмотренные разделом 12.1 настоящих Правил.

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

# 

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

* 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/или 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](#Приложение7), [7а](#Приложение7а), [7б](#Приложение7б) к настоящим Правилам в зависимости от используемых Клиентом подсистемы систем ДБО BS-Client или Correqts и средств ЭП).
  2. Клиент осведомлен о рисках при использовании Системы ДБО и признает свою ответственность в случае использования ключей ЭП неуполномоченными на это лицами.
  3. Банк не несет ответственность за последствия исполнения распоряжений, в случаях не уведомления Клиентом Банка о фактах Компрометации ключей ЭП Представителей Клиента.
  4. Банк не несет ответственности за ущерб, причиненный Клиенту в результате использования третьими лицами ключа ЭП Представителей Клиента.
  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.
  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.
  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.
  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/Мобильного устройства, на котором установлен АРМ Системы ДБО Клиента, Банк согласовывает с Клиентом иной способ уведомления об операциях, совершенных с использованием электронных средств платежа.
  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/или 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.
  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.
  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.
  12. Обязанность доказывать существование обстоятельств непреодолимой силы лежит на Стороне, которая ссылается на их действие.
  13. По прошествии обстоятельств непреодолимой силы Стороны обязуются принять все меры для ликвидации последствий и уменьшения причиненного реального ущерба.

# ПОРЯДОК УРЕГУЛИРОВАНИЯ СПОРНЫХ СИТУАЦИЙ

* 1. В случае возникновения между Сторонами спорных ситуаций при использовании Системы ДБО, Стороны предпримут все меры для их разрешения путем переговоров.
  2. При возникновении спорной ситуации одна Сторона направляет другой Стороне соответствующую письменную претензию.
  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.
  4. Если Сторонам не удастся разрешить спорную ситуацию путем переговоров, совместным решением обеих Сторон для проведения [технической экспертизы](#техническая_экспертиз) 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.
  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 (для систем ДБО с СКЗИ);

специалисты Федеральной Службы Безопасности Российской Федерации (для систем ДБО с СКЗИ);

разработчика средства ЭП PayControl (если спорный ЭД был подписан с использованием средства ЭП PayControl).

* 1. Стороны согласны с тем, что оплачивать услуги привлеченных экспертов в области защиты информации должна Сторона, предъявившая претензию.
  2. Техническая комиссия осуществляет свою работу на территории Банка.
  3. 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.

* 1. При проведении [технической экспертизы](#техническая_экспертиз) проводится проверка соответствия АРМ Системы ДБО Клиента требованиям Руководства по обеспечению информационной безопасности (Приложение [7](#Приложение7), [7а](#Приложение7а), [7б](#Приложение7б) к настоящим Правилам в зависимости от используемых Клиентом подсистемы систем ДБО BS-Client или Correqts и средств ЭП), 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](#Приложение8), [8а](#Приложение8а), [8б](#Приложение8б) к настоящим Правилам). Акт [технической экспертизы](#техническая_экспертиз) подписывается членами комиссии.
  2. 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.
  3. Протокол составляется на бумажном носителе в двух экземплярах, имеющих одинаковую силу. Экземпляры Протокола хранятся у Банка и Клиента.
  4. 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.

* 1. Акт составляется на бумажном носителе в двух экземплярах, имеющих одинаковую силу. Экземпляры акта хранятся у Банка и Клиента.
  2. 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.
  3. Техническая комиссия проводит техническую экспертизу спорных ситуаций в соответствии с Регламентом и настоящими Правилами.

**Для систем ДБО с СКЗИ**

* 1. 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.

* 1. 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.

* 1. 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.
  2. 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.

**Для средства ЭП PayControl**

* 1. Для проведения технической экспертизы спорного ЭД техническая комиссия получает:

у Администратора Системы ДБО Банка:

специализированное ПО разработчика средства ЭП PayControl – ПО АРМ РКС;

файл спорного ЭД;

значение ЭП спорного ЭД;

в системе Юридическое досье Клиента:

Акт об оказании услуг по регистрации ключа проверки электронной подписи PayControl.

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

загрузку в АРМ РКС файла спорного ЭД;

загрузку в АРМ РКС файла со значением ЭП спорного ЭД;

проверку ЭП выгруженного файла спорного ЭД с использованием значения ключа проверки ЭП;

печать протокола работы АРМ РКС.

* 1. В случае, если:

проверяемая ЭП для данного спорного ЭД верна;

ключ проверки ЭП, отобранный для разбора конфликтной ситуации, соответствует значению ключа в Акте об оказании услуг по регистрации ключа проверки электронной подписи PayControl,

считается установленным:

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

проверяемый спорный ЭД был подписан ключом ЭП, соответствующим зарегистрированному Банком ключу проверки ЭП PayControl, использованному при проведении технической экспертизы;

владельцем ключа ЭП и ключа проверки ЭП PayControl является Представитель Клиента, зарегистрированный Банком.

* 1. Стороны признают решения технической комиссии обязательными и обязуются добровольно их исполнять.
  2. 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 исполнения решения технической комиссии, спор подлежит разрешению в Арбитражном суде г. Москвы.

# ПОРЯДОК ПРОТИВОДЕЙСТВИЯ ОСУЩЕСТВЛЕНИЮ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ БЕЗ СОГЛАСИЯ КЛИЕНТА С ИСПОЛЬЗОВАНИЕМ ЦС ДБО

* 1. Клиент в соответствии п.7.15 и п.8.5.3 настоящих Правил обязуется уведомить незамедлительно, но не позднее рабочего дня, следующего за днем выявления факта, Банк об известных ему:

попытках третьих лиц совершить действия, способные привести к нарушению целостности Системы ДБО;

сбоях в работе Системы ДБО;

выходе из строя Системы ДБО;

выходе из строя компьютера, на котором установлен АРМ Системы ДБО, либо Мобильного устройства, на котором установлено приложение PayControl или Мобильный Бизнес Клиент;

утрате компьютера, на котором установлен АРМ Системы ДБО, либо Мобильного устройства, на котором установлено средство ЭП PayControl или Мобильный Бизнес Клиент,

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.п.8.5.2 – 8.5.4 настоящих Правил.

* 1. Информирование Банка осуществляется Клиентом по телефону клиентской поддержки 8 800 775-90-09 или по региональному телефонному номеру, который используется для связи с обслуживающим филиалом.
  2. При получении от Клиента уведомления, указанного в п. 15.1. настоящих Правил, после осуществления списания денежных средств с банковского счета Клиента Банк обязан незамедлительно направить оператору по переводу денежных средств, обслуживающему получателя средств, уведомление о приостановлении зачисления денежных средств на банковский счет получателя средств или увеличения остатка электронных денежных средств получателя средств по форме и в порядке, которые установлены нормативным актом Банка России.
  3. Банк при выявлении им операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента, до осуществления списания денежных средств с банковского счета Клиента приостанавливает на срок не более двух рабочих дней исполнение распоряжения о совершении операции, соответствующей признакам осуществления перевода денежных средств без согласия Клиента. Признаки осуществления перевода денежных средств без согласия клиента устанавливаются Банком России и размещаются на его официальном сайте в информационно-телекоммуникационной сети «Интернет».
  4. Банк после выполнения действий, предусмотренных п.15.4 настоящих Правил, в обязательном порядке извещает об этом Клиента и одновременно незамедлительно запрашивает у Клиента по номеру мобильного телефона, предоставленного им Банку для этих целей или иного номера, имеющегося в Банке, подтверждение возобновления исполнения распоряжения. При этом Банк в течение одного рабочего дня осуществляет не менее двух попыток дозвона до Клиента по указанному номеру мобильного телефона. При получении от Клиента подтверждения Банк незамедлительно возобновляет исполнение распоряжения. В случае, если попытки дозвона были неуспешными, в результате чего распоряжение Клиента оказалось неподтвержденным в день получения его Банком, Банк задерживает исполнение такого распоряжения на срок не более двух рабочих дней, осуществляя попытки дозвона до клиента в течение этих двух рабочих дней по указанному номеру мобильного телефона. Если все попытки дозвона до Клиента оказались неуспешными, Банк по истечении двух рабочих дней возобновляет исполнение распоряжения Клиента.

Клиент в случае обнаружения им факта неисполнения Банком его распоряжения в установленный договором банковского счета срок вправе самостоятельно позвонить в Банк и, воспользовавшись услугой «Кодовое слово» (при условии ее подключения Клиенту), подтвердить возобновление исполнения распоряжения.

* 1. При получении Банком информации от Клиента в соответствии с п.15.1 настоящих Правил или при подтверждении Клиентом факта осуществления попытки списания денежных средств без согласия Клиента в соответствии с п.п. 15.3 – 15.5 настоящих Правил, до выяснения всех обстоятельств по инциденту Банком выполняется блокирование АРМ Клиента и перевод его на прием распоряжений на бумажном носителе.
  2. После блокирования Банком АРМ Клиента в соответствии с п. 15.6 настоящих Правил Клиент в течение трех рабочих дней обязан подать письменное заявление на приостановление действия СКП ЭП/регистрации ключа проверки ЭП PayControl. 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.
  3. 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.
  4. 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 компьютера[[9]](#footnote-9) 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.

* 1. 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](#Приложение7), [7а](#Приложение7а), [7б](#Приложение7б) к настоящим Правилам в зависимости от используемой Клиентом подсистемы систем ДБО BS-Client или Correqts).
  2. 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](#Приложение8), [8а](#Приложение8а), [8б](#Приложение8б) к настоящим Правилам).
  3. 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](#Приложение9), [9а](#Приложение9а), [9б](#Приложение9б) к настоящим Правилам).
  4. 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](#Приложение9), [9а](#Приложение9а), [9б](#Приложение9б) к настоящим Правилам) Банк вправе приостановить использование Клиентом Системы ДБО на неопределенный срок.
  5. Разблокировка АРМ Клиента осуществляется только после проведения работ согласно п.п. 15.9 и 15.10 настоящих Правил, приведения АРМ в соответствие требованиям Руководства по обеспечению информационной безопасности (Приложение [7](#Приложение7), [7а](#Приложение7а), [7б](#Приложение7б) к настоящим Правилам) и получения Банком Акта или Анкеты о соблюдении требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ Системы ДБО (Приложения [8](#Приложение8), [8а](#Приложение8а), [8б](#Приложение8б) или [9](#Приложение9), [9а](#Приложение9а), [9б](#Приложение9б) к настоящим Правилам).

# Приложение 1. Заявление о присоединении к Правилам пользования централизованной системой ДБО и Регламенту Удостоверяющего центра (для системы ДБО BS-Client и системы ДБО Correqts с СКЗИ)

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)*

|  |
| --- |
|  |

|  |  |
| --- | --- |
| 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 1а. Заявление о присоединении к Правилам пользования централизованной системой ДБО (для системы ДБО Correqts только со средством электронной подписи PayControl)

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)*

|  |
| --- |
|  |

|  |  |
| --- | --- |
| в лице |  |

*(должность, фамилия, имя, отчество)*

|  |  |
| --- | --- |
| действующего на основании |  |

в соответствии со ст. 428 ГК РФ полностью и безусловно присоединяется к 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 (для системы ДБО BS-Client и системы ДБО Correqts с СКЗИ)

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.

|  |  |
| --- | --- |
| 1. 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.

1. 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))* |

\* – отметки ❑ проставляются для Клиентов подсистемы Интернет-Клиент Системы Correqts и подсистемы Клиент-Банк Системы BS-Client

# Приложение 2а. Заявление на регистрацию пользователя и ключа проверки ЭП PayControl для использования в ЦС ДБО (для системы ДБО Correqts со средством ЭП PayControl)

**Заявление**

**на регистрацию пользователя и ключа проверки электронной подписи PayControl**

**для использования в ЦС ДБО**

Прошу:

1. Зарегистрировать меня в качестве пользователя средства ЭП PayControl системы ДБО Банка «Возрождение» (ПАО), изготовить мне ключи регистрации и зарегистрировать ключ проверки 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 в Банк «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 Банк «Возрождение» (ПАО) 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 ключа ЭП – Уполномоченное лицо Клиента |  |  |
|  | *(подпись)* | *(фамилия, имя, отчество)* |
|  | *«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_*20\_\_г. | |

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

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

уполномочивается выступать в роли пользователя средства ЭП PayControl системы ДБО Банка «Возрождение» (ПАО) и совершать действия в рамках 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 ключи регистрации, ключ электронной подписи и соответствующий ему ключ проверки электронной подписи, владельцем которого является указанное Уполномоченное лицо Клиента, 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 (для системы ДБО BS-Client и системы ДБО Correqts с СКЗИ)

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/ДО Банка.

Регистрационный № \_\_\_\_\_\_\_\_\_\_\_\_\_\_ от «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

|  |  |
| --- | --- |
| Ответственный сотрудник Банка | |
|  |  |
| *(Подпись)* | *(Фамилия, инициалы)* |
|  |  |

# Приложение 3а. Заявление на аннулирование ключа проверки электронной подписи (для системы ДБО Correqts со средством электронной подписи PayControl)

В Банк «Возрождение» (ПАО)

**Заявление**

**на аннулирование ключа проверки электронной подписи средства ЭП PayControl**

|  |
| --- |
|  |

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

|  |  |
| --- | --- |
| в лице |  |

*(должность)*

|  |
| --- |
|  |

*(фамилия, имя, отчество)*

|  |  |  |
| --- | --- | --- |
| действующего на основании | |  |
| в связи с |  | |

*(причина аннулирования сертификата)*

Просит аннулировать ключ проверки электронной подписи своего уполномоченного представителя:

|  |
| --- |
|  |

*(фамилия, имя, отчество)*

|  |
| --- |
|  |
| (Должность и Ф.И.О.) |
|  |
| (Подпись) |
| «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_ г. |
| (дата подписания заявления) |
| (м.п.) |

Заявление зарегистрировано в филиале/ДО Банка.

Регистрационный № \_\_\_\_\_\_\_\_\_\_\_\_\_\_ от «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

|  |  |
| --- | --- |
| Ответственный сотрудник Банка | |
|  |  |
| *(Подпись)* | *(Фамилия, инициалы)* |
|  |  |

# Приложение 4. Доверенность на получение ключей ЭП, документов, программного и информационного обеспечения для использования в ЦС ДБО

**Доверенность № \_\_\_\_\_\_**

|  |  |
| --- | --- |
| г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(место выдачи)* | " \_\_\_\_\_\_ " \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г. |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 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 ключи регистрации, технологические ключи ЭП и технологические СКП ЭП Уполномоченных лиц Клиента;
* получать СКП ЭП УЦ, СКП ЭП уполномоченных лиц 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 системы ДБО BS-Client в конфигурации «Корпоративный контроль» и «Мультиклиент»)

**Доверенность № \_\_\_\_\_\_**

|  |  |
| --- | --- |
| г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(место выдачи)* | " \_\_\_\_\_\_ " \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г. |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 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 до[[10]](#footnote-10) "\_\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года.

Образец подписи владельца СКП ЭП – полномочного представителя организации

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

(подпись) (Фамилия и инициалы)

Руководитель Клиента \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

(подпись) (Фамилия и инициалы)

М.П.

# Приложение 5. Заявление на предоставление услуг, установку, настройку, восстановление Системы ДБО

В Банк «Возрождение» (ПАО)

**ЗАЯВЛЕНИЕ  
на предоставление услуг, установку, настройку, восстановление Системы ДБО**

|  |
| --- |
|  |
| (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:

|  |  |  |  |
| --- | --- | --- | --- |
| **Систем Correqts** | | | **Система BS-Client** |
| ❑ **Подсистема Интернет-Клиент с СКЗИ**  В том числе в конфигурации:  ❑ **«Корпоративный Контроль»**  ❑ **«Мультиклиент»** | ❑ **Подсистема Интернет-Клиент с PayControl**  В том числе в конфигурации:  ❑ **«Мобильный Бизнес Клиент» с PayControl**  ❑ **«Корпоративный Контроль»**  ❑ **«Мультиклиент»** | ❑ **Подсистема Мобильный Бизнес Клиент без PayControl** | ❑ **Подсистема Интернет-Клиент**  В том числе в конфигурации:  ❑ **«Корпоративный Контроль»**  ❑ **«Мультиклиент** |

1. **Предоставить услуги/ установить/ настроить/ восстановить (ненужное зачеркнуть)** Систему ДБО в следующей конфигурации:

Сведения для установки Системы:

|  |  |
| --- | --- |
| Установка Системы будет произведена | ❑ Клиентом самостоятельно ❑ специалистом Банка |
| Тип НКИ (только для подсистемы Интернет-Клиент Систем Correqts с СКЗИ и BS-Client) | ❑ USB ❑ Смарт-карта, средство визуализации ЭП SafeTouch |
| Адрес места установки Системы ДБО |  |

Сведения о контактном лице Клиента, ответственном за эксплуатацию Системы ДБО

|  |  |
| --- | --- |
| (Ф.И.О.) |  |
| Телефон (ы) |  |
| Email |  |
| Время работы (перерыв) |  |

2. **Предоставить** (рекомендуется) **/ не предоставлять / отключить (ненужное зачеркнуть)** услугу по отправке SMS/email сообщений с информацией об операциях по банковским счетам Клиента[[11]](#footnote-11)):

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 |
| ❑SMS ❑Email |  |  |

|  |
| --- |
|  |
| (должность и ФИО руководителя организации или ФИО физического лица) |
|  |
| (подпись руководителя организации или физического лица) |
| «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_г. |
| (дата подписания заявления) |

# Приложение 6. Акт о передаче программного обеспечения Системы ДБО (для системы ДБО BS-Client)

Акт № - \_\_\_\_\_\_\_\_\_-BSS

**о передаче программного обеспечения Системы ДБО** **BS-Client**

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 | CD/DVD-диск № \_\_\_\_\_\_\_\_\_\_ с дистрибутивом СКЗИ, эксплуатационной документацией к нему, ПО для работы с сертифицированными НКИ, дистрибутивом АРМ Клиента и эксплуатационной документацией для клиентского АРМ Системы ДБО |  |
| 2 | Лицензия на использование СКЗИ КриптоПро CSP на бумажном носителе серийный номер – \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| 3 | НКИ в комплекте, ID \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ в форм-факторе:  ❑ - USB  ❑ - Смарт-карта, Дополнительно ❑ - SafeTouch |  |
| 4 | ПИН-конверт с логином и паролем, ID \_\_\_\_\_\_\_\_\_ для клиентского АРМ системы ДБО\*) |  |
| 5 | Информация клиенту системы дистанционного банковского обслуживания Банка «Возрождение» (ПАО) |  |
| 6 | АРМ Клиента сконфигурирован в следующей комплектации (нужное подчеркнуть)  ❑ Комплект Интернет-Клиент Системы BS-Client  ❑ Комплект Интернет-Клиент Системы BS-Client в конфигурации "Мультиклиент"  ❑ Комплект Интернет-Клиент Системы BS-Client в конфигурации "Корпоративный контроль"  ❑ Комплект Системы BS-Client "Клиент-Банк Офис" |  |

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  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(должность представителя Клиента)*  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(подпись, фамилия, инициалы представителя Клиента)* | Уполномоченный представитель Банка  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *(должность представителя Банка)*  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(подпись, фамилия, инициалы представителя Банка)* |

\*)– выдан уполномоченному лицу Клиента – владельцу СКП ЭП

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(фамилия, имя, отчество владельца СКП ЭП)

|  |
| --- |
| 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 6а. Акт о передаче программного обеспечения Системы ДБО (для системы ДБО Correqts с СКЗИ)

**Акт № - \_\_\_\_ BSS-Correqts**

**о передаче комплекта подключения для Системы ДБО Correqts с СКЗИ**

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 комплект подключения для Системы ДБО BSS-Correqts, который будет использоваться на компьютере Клиента, находящемся по адресу: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

|  |  |  |
| --- | --- | --- |
| № п/п | Переданные средства | Отметка о передаче |
| 1 | PIN-конверт № ­­\_\_\_\_\_ для уполномоченного лица Клиента – владельца СКП ЭП  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,  *(фамилия, имя, отчество будущего владельца СКП ЭП)*  содержащий ключ простой ЭП – логин и пароль для доступа в систему ДБО, а так же PIN-коды пользователя и администратора для доступа к USB-ключу |  |
| 2 | USB-ключ ID \_\_\_\_\_\_\_\_\_\_ с предустановленными PIN-кодами пользователя и администратора, содержащий ключ ЭП и соответствующий ему технологический СКП ЭП серийный № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| 3 | Информация клиенту системы дистанционного банковского обслуживания Банка «Возрождение» (ПАО) |  |

Клиент признает, что на основании Приложения № 13 Правил ДБО и данного Акта Уполномоченное лицо Клиента, указанное в п. 1, является владельцем ключа простой ЭП и технологического СКП ЭП с серийным номером, указанным в п. 2.

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  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(должность представителя Клиента)*  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(подпись, фамилия, инициалы представителя Клиента)* | Уполномоченный представитель Банка  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *(должность представителя Банка)*  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(подпись, фамилия, инициалы представителя Банка)* |

|  |
| --- |
| Инструкция по оформлению Акта о передаче комплекта подключения для Системы ДБО BSS-Correqts   1. Акт оформляется во всех случаях передачи комплекта подключения и оформляется на каждое уполномоченное лицо Клиента – владельца ключа простой ЭП, указанное в п. 1, USB-ключа с технологическим СКП ЭП, с серийным номером, указанным в п. 2. 2. В графе «Уполномоченный представитель Клиента» в нижней левой части Акта должен расписаться представитель Клиента, уполномоченный им для получения комплекта подключения. 3. Специалист Банка в присутствии уполномоченного представителя Клиента заполняет в обоих экземплярах Акта реквизиты, подлежащие ручному заполнению. 4. Один экземпляр Акта возвращается Клиенту. |

# Приложение 6б. Акт о передаче программного обеспечения Системы ДБО (для системы ДБО Correqts со средством электронной подписи PayControl)

**Акт № - \_\_\_\_ Correqts**

**о передаче комплекта подключения для Системы ДБО Correqts с PayControl**

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 комплект подключения для Системы ДБО Correqts со средством электронной подписи PayControl.

|  |  |  |
| --- | --- | --- |
| № п/п | Переданные средства | Отметка о передаче |
| 1 | PIN-конверт № \_\_\_\_\_ для уполномоченного лица Клиента – владельца технологического и рабочих ключей ЭП средства ЭП PayControl  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,  *(фамилия, имя, отчество будущего владельца ключей ЭП PayControl)*  содержащий логин и пароль для доступа в систему ДБО |  |
| 2 | Информация клиенту системы дистанционного банковского обслуживания Банка «Возрождение» (ПАО) |  |

Клиент признает, что на основании Приложения № 13 Правил ДБО и данного Акта Уполномоченное лицо Клиента, указанное в п. 1, является владельцем ключей регистрации средства ЭП PayControl.

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  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(должность представителя Клиента)*  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(подпись, фамилия, инициалы представителя Клиента)* | Уполномоченный представитель Банка  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *(должность представителя Банка)*  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(подпись, фамилия, инициалы представителя Банка)* |

|  |
| --- |
| Инструкция по оформлению Акта о передаче комплекта подключения для Системы ДБО BSS-Correqts   1. Акт оформляется во всех случаях передачи комплекта подключения и оформляется на каждое уполномоченное лицо Клиента – владельца ключей регистрации средства ЭП PayControl. 2. В графе «Уполномоченный представитель Клиента» в нижней левой части Акта должен расписаться представитель Клиента, уполномоченный им для получения комплекта подключения. 3. Специалист Банка в присутствии уполномоченного представителя 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 системы ДБО BS-Client)

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Требования по обеспечению информационной безопасности при эксплуатации Клиентом АРМ Системы ДБО** | **Признак обязательности** |
| 1 | 1. АРМ Системы ДБО обслуживается уполномоченными лицами Клиента. | ++ |
| 1. Клиентом обеспечивается контроль доступа в помещение, в котором размещен АРМ Системы ДБО. | ++ |
| 1. Администратор локальной вычислительной сети (ЛВС) и администратор безопасности (при их наличии) ознакомлены с настоящим Руководством. | ++ |
| 2 | 1. На АРМ Системы ДБО отсутствуют программы удаленного администрирования (например, RAdmin). 2. Осуществляется периодический контроль активного программного обеспечения (ПО), установленного на АРМ Системы ДБО. |  |
| 3 | 1. НКИ 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. | ++ |
| 1. По окончанию сеанса работы с Банком приложение Системы ДБО закрывается, НКИ извлекаются из АРМ, при уходе с рабочего места НКИ 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 | 1. Доступ к АРМ Системы ДБО по сети (локальной, Интернет) запрещен. | + |
| 1. Запрещен доступ неуполномоченных лиц к каталогам с установленной Системой ДБО. | ++ |
| 7 | Дистрибутив СКЗИ КриптоПро CSP получен на учтенном 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 | 1. На АРМ Системы ДБО установлены все рекомендованные производителем обновления безопасности операционной Системы. | ++ |
| 1. 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 | 1. Работа на АРМ Системы ДБО производится под учетной записью обычного пользователя. Администраторские права используются только для установки СКЗИ КриптоПро и Системы ДБО. | ++ |
| 1. Стандартная учетная запись «Гость» отключена. | ++ |
| 1. 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 | 1. 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>. | ++ |
| 1. Включены настройки антивирусного ПО, установленные разработчиком по умолчанию. Включена защита настроек паролем. | ++ |
| 1. На АРМ Системы ДБО дополнительно установлены средства защиты от спама, вредоносного ПО и злоумышленного воздействия. | \* |
| 1. Антивирусные базы обновляются в автоматическом режиме с рекомендуемым разработчиком периодом обновления. | ++ |
| 1. 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; * НКИ; * PIN-кодов к НКИ, логинов и паролей. | ++ |
| 14 | Клиенту известен установленный Банком порядок уведомления обслуживающего филиала Банка о блокировке доступа к счетам в случае утраты НКИ 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;
* пунктыРуководства, отмеченные знаком «\*», имеют рекомендательный характер.

# Приложение 7а. Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации Клиентом АРМ Системы ДБО (для системы ДБО Correqts с СКЗИ)

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Требования по обеспечению информационной безопасности при эксплуатации Клиентом АРМ Системы ДБО** | **Признак обязательности** |
| 1 | 1. АРМ Системы ДБО обслуживается уполномоченными лицами Клиента. | ++ |
| 1. Клиентом обеспечивается контроль доступа в помещение, в котором размещен АРМ Системы ДБО. | ++ |
| 1. Администратор локальной вычислительной сети (ЛВС) и администратор безопасности (при их наличии) ознакомлены с настоящим Руководством. | ++ |
| 2 | 1. На АРМ Системы ДБО отсутствуют программы удаленного администрирования (например, RAdmin). 2. Осуществляется периодический контроль активного программного обеспечения (ПО), установленного на АРМ Системы ДБО. | ++ |
| 3 | 1. НКИ 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. | ++ |
| 1. По окончанию сеанса работы с Банком приложение Системы ДБО закрывается, НКИ извлекаются из АРМ, при уходе с рабочего места НКИ и носители с PIN-кодами доступа хранятся в недоступном для посторонних месте. | ++ |
| 4 | 1. Доступ к АРМ Системы ДБО по сети (локальной, Интернет) запрещен. | + |
| 1. Запрещен доступ неуполномоченных лиц к каталогам с установленной Системой ДБО. | ++ |
| 5 | Комплект подключения получен по акту приема-передачи, подписанным сотрудником Банка и уполномоченным представителем Клиента. | ++ |
| 6 | 1. На АРМ Системы ДБО установлены все рекомендованные производителем обновления безопасности операционной Системы. | ++ |
| 1. 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. | ++ |
| 7 | 1. Работа на АРМ Системы ДБО производится под учетной записью обычного пользователя. Администраторские права используются только для установки Системы ДБО. | ++ |
| 1. Стандартная учетная запись «Гость» отключена. | ++ |
| 1. 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. | ++ |
| 8 | 1. На АРМ Системы ДБО установлено антивирусное ПО. | ++ |
| 1. Включены настройки антивирусного ПО, установленные разработчиком по умолчанию. Включена защита настроек паролем. | ++ |
| 1. На АРМ Системы ДБО дополнительно установлены средства защиты от спама, вредоносного ПО и злоумышленного воздействия. | \* |
| 1. Антивирусные базы обновляются в автоматическом режиме с рекомендуемым разработчиком периодом обновления. | ++ |
| 1. Полная проверка АРМ Системы ДБО на наличие вирусов и вредоносного ПО производится в автоматическом режиме с рекомендуемым разработчиком периодом проверки. | ++ |
| 9 | 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. | \* |
| 10 | При уходе пользователя АРМ Системы ДБО с рабочего места в течение рабочего дня АРМ блокируется пользователем, после завершения рабочего дня – выключается. | ++ |
| 11 | В случае установки на ноутбук ПО АРМ Системы ДБО, Клиентом обеспечивается раздельное хранение трех компонент:   * ноутбука; * НКИ; * PIN-кодов к НКИ, логинов и паролей. | ++ |
| 12 | Клиенту известен установленный Банком порядок уведомления обслуживающего филиала Банка о блокировке доступа к счетам в случае утраты НКИ или PIN-кода доступа к нему. | ++ |
| 13 | Клиенту известен установленный Банком порядок немедленного уведомления обслуживающего филиала Банка о блокировке доступа к счетам в случае внезапной остановки работы Системы ДБО. | ++ |
| 14 | По завершении операционного времени обслуживающего филиала Банка Клиентом контролируется состояние счета путем отправки в Банк запроса промежуточного отчета об операциях по счету. | ++ |
| 15 | 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;
* пунктыРуководства, отмеченные знаком «\*», имеют рекомендательный характер.

# Приложение 7б. Руководство по обеспечению безопасности использования Клиентом Мобильного устройства (для системы ДБО Correqts со средством электронной подписи PayControl)

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Требования по обеспечению информационной безопасности при эксплуатации Клиентом Мобильного устройства со средством электронной подписи PayControl** | **Признак обязательности** |
| 1 | Мобильное устройство, предназначенное для использования Клиентом со средством ЭП PayControl, должно быть приобретено у официального продавца и быть сертифицировано по требованиям ГОСТ в соответствии с действующим законодательством для использования на территории Российской Федерации. | ++ |
| 2 | Мобильное устройство Клиента имеет поддерживаемую средством ЭП PayControl лицензионную версию операционной системы:   1. Android 5.0 и выше, 2. iOS 10.X, 11.X. | ++ |
| 3 | Клиент не использует средство ЭП PayControl на мобильных устройствах, на которых были получены права root («рутованые» устройства) или произведён «джейлбрейк» (англ. jailbreak). | ++ |
| 4 | Для операционной системы Мобильного устройства и приложений, установленных на Мобильное устройство, Клиентом установлены максимально возможные на текущее время обновления рекомендованные производителем/разработчиком. | + |
| 5 | Клиентская часть средства ЭП PayControl – приложение PayControl самостоятельно установлена Клиентом из одного из официальных сервисов Google Play или App Store. Клиент не использовал переход к указанным сервисам и установку клиентской части средства ЭП PayControl по ссылке из других источников. | ++ |
| 6 | Если при установке клиентской части средства ЭП PayControl появились сообщения о необходимости удаления приложения/приложений, представляющих угрозу для средства ЭП PayControl, Клиент удалил представляющие угрозу приложение/приложения с Мобильного устройства | ++ |
| 7 | Для разблокировки Мобильного устройства включён максимально возможный из доступных на данном Мобильном устройстве способ защиты от несанкционированного доступа к функциям устройства и хранящихся на нём данным (в порядке убывания стойкости защиты):   1. средство распознания радужки глаза; 2. средство распознавания отпечатка пальца или лица; 3. пароль длиною не менее 6 символов (включая буквы и цифры); 4. графический ключ; 5. PIN-код.   При использовании пароля или PIN-кода Клиент запомнил их и не сохранил в памяти Мобильного устройства. | ++ |
| 8 | Мобильное устройство настроено Клиентом на автоматическую блокировку устройства по истечении определённого времени (не более 5 минут). | ++ |
| 9 | На Мобильное устройство под управлением ОС Android используется средство защиты от вредоносного кода («антивирусное программное обеспечение»). | ++ |
| 10 | На Мобильном устройстве под управлением ОС Android отключена возможность установки приложений из непроверенных источников. | ++ |
| 11 | На Мобильное устройство не установлено корневых сертификатов PKI, полученных из ненадёжных источников. | ++ |
| 12 | Мобильное устройство с принятыми из Банка ключами регистрации PayControl (направляются Банком каждому УЛК Клиента в закодированном виде: QR-код + SMS и/или сообщение по электронной почте) и самостоятельно выработанными УЛК Клиента рабочими ключами ЭП PayControl, а так же атрибуты доступа к Мобильному устройству (логин, пароль, графический ключ) никогда не передается Клиентом неуполномоченным лицам, включая Руководство организации, коллег и членов семьи Уполномоченного лица Клиента и не оставляется им без присмотра. | ++ |
| 13 | Мобильное устройство, с установленной клиентской частью средства ЭП PayControl, используется Клиентом только для посещения сайтов и установки приложений, необходимых и достаточных Клиенту для ведения его коммерческой/уставной деятельности. | ++ |
| 14 | Мобильное устройство не подключается Клиентом к компьютерам, безопасность которых:   1. обеспечение доверенной среды, 2. отсутствие удаленного управления и 3. установленных/запущенных вредоносных программ,   Клиент не может гарантировать. | ++ |
| 15 | Мобильное устройство не подключается Клиентом к общественным WI-FI сетям. Общественные WI-FI сети, как правило, плохо защищены, их настройки неизвестны и эти сети приходится делить со множеством людей вокруг, среди которых могут быть злоумышленники. | ++ |
| 16 | В случае компрометации ключей ЭП PayControl, а так же атрибутов доступа к Мобильному устройству (логин, пароль, графический ключ) Клиенту известен установленный Банком порядок уведомления обслуживающего филиала/ДО Банка о блокировке доступа к счетам. | ++ |
| 17 | По завершении операционного времени обслуживающего филиала Банка Клиентом контролируется состояние счета путем отправки в Банк запроса промежуточного отчета об операциях по счету. | ++ |
| 18 | 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.

# Приложение 8. Акт о соблюдении Клиентом требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ Системы ДБО (для системы ДБО BS-Client)

|  |  |
| --- | --- |
| «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 (для системы ДБО BS-Client)** | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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. НКИ 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 окончанию сеанса работы с Банком приложение Системы ДБО закрывается, НКИ извлекаются из АРМ, при уходе с рабочего места НКИ 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 учтенном 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; * НКИ; * PIN-кодов к НКИ, логинов и паролей. | | ++ |  |
| 14 | Клиенту известен установленный Банком порядок уведомления обслуживающего филиала Банка о блокировке доступа к счетам в случае утраты НКИ 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.

|  |  |
| --- | --- |
| Уполномоченный представитель Клиента  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (должность представителя Клиента)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись, фамилия, инициалы представителя Клиента) | Уполномоченный представитель Банка  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (должность представителя Банка)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись, фамилия, инициалы представителя Банка) |

# Приложение 8а. Акт о соблюдении Клиентом требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ Системы ДБО (для системы ДБО Correqts с СКЗИ)

|  |  |
| --- | --- |
| «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**  **(для системы ДБО Correqts с СКЗИ)** | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 | 1. АРМ Системы ДБО обслуживается уполномоченными лицами Клиента. | | ++ |  |
| 1. Клиентом обеспечивается контроль доступа в помещение, в котором размещен АРМ Системы ДБО. | | ++ |  |
| 1. Администратор локальной вычислительной сети (ЛВС) и администратор безопасности (при их наличии) ознакомлены с настоящим Руководством. | | ++ |  |
| 2 | 1. На АРМ Системы ДБО отсутствуют программы удаленного администрирования (например, RAdmin). 2. Осуществляется периодический контроль активного программного обеспечения (ПО), установленного на АРМ Системы ДБО. | | ++ |  |
| 3 | 1. НКИ 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. | | ++ |  |
| 1. По окончанию сеанса работы с Банком приложение Системы ДБО закрывается, НКИ извлекаются из АРМ, при уходе с рабочего места НКИ и носители с PIN-кодами доступа хранятся в недоступном для посторонних месте. | | ++ |  |
| 4 | 1. Доступ к АРМ Системы ДБО по сети (локальной, Интернет) запрещен. | | + |  |
| 1. Запрещен доступ неуполномоченных лиц к каталогам с установленной Системой ДБО. | | ++ |  |
| 5 | Комплект подключения получен по акту приема-передачи, подписанным сотрудником Банка и уполномоченным представителем Клиента. | | ++ |  |
| 6 | 1. На АРМ Системы ДБО установлены все рекомендованные производителем обновления безопасности операционной Системы. | | ++ |  |
| 1. 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. | | ++ |  |
| 7 | 1. Работа на АРМ Системы ДБО производится под учетной записью обычного пользователя. Администраторские права используются только для установки Системы ДБО. | | ++ |  |
| 1. Стандартная учетная запись «Гость» отключена. | | ++ |  |
| 1. 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. | | ++ |  |
| 8 | 1. На АРМ Системы ДБО установлено антивирусное ПО. | | ++ |  |
| 1. Включены настройки антивирусного ПО, установленные разработчиком по умолчанию. Включена защита настроек паролем. | | ++ |  |
| 1. На АРМ Системы ДБО дополнительно установлены средства защиты от спама, вредоносного ПО и злоумышленного воздействия. | | \* |  |
| 1. Антивирусные базы обновляются в автоматическом режиме с рекомендуемым разработчиком периодом обновления. | | ++ |  |
| 1. Полная проверка АРМ Системы ДБО на наличие вирусов и вредоносного ПО производится в автоматическом режиме с рекомендуемым разработчиком периодом проверки. | | ++ |  |
| 9 | 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. | | \* |  |
| 10 | При уходе пользователя АРМ Системы ДБО с рабочего места в течение рабочего дня АРМ блокируется пользователем, после завершения рабочего дня – выключается. | | ++ |  |
| 11 | В случае установки на ноутбук ПО АРМ Системы ДБО, Клиентом обеспечивается раздельное хранение трех компонент:   * ноутбука; * НКИ; * PIN-кодов к НКИ, логинов и паролей. | | ++ |  |
| 12 | Клиенту известен установленный Банком порядок уведомления обслуживающего филиала Банка о блокировке доступа к счетам в случае утраты НКИ или PIN-кода доступа к нему. | | ++ |  |
| 13 | Клиенту известен установленный Банком порядок немедленного уведомления обслуживающего филиала Банка о блокировке доступа к счетам в случае внезапной остановки работы Системы ДБО. | | ++ |  |
| 14 | По завершении операционного времени обслуживающего филиала Банка Клиентом контролируется состояние счета путем отправки в Банк запроса промежуточного отчета об операциях по счету. | | ++ |  |
| 15 | 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.

|  |  |
| --- | --- |
| Уполномоченный представитель Клиента  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (должность представителя Клиента)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись, фамилия, инициалы представителя Клиента) | Уполномоченный представитель Банка  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (должность представителя Банка)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись, фамилия, инициалы представителя Банка) |

Приложение 8б. Акт о соблюдении Клиентом требований Руководства по обеспечению безопасности использования Клиентом Мобильного устройства (для системы ДБО Correqts со средством электронной подписи PayControl)

|  |  |
| --- | --- |
| «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 Руководство по обеспечению безопасности использования Клиентом Мобильного устройства**  **(для системы ДБО Correqts со средством электронной подписи PayControl)** | | |

|  |  |
| --- | --- |
| 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 Мобильного устройства со средством электронной подписи PayControl | Признак обязательности | Оценка соответствия Требованиям  (Да/Нет) |
| 1 | Мобильное устройство, предназначенное для использования Клиентом со средством ЭП PayControl, должно быть приобретено у официального продавца и быть сертифицировано по требованиям ГОСТ в соответствии с действующим законодательством для использования на территории Российской Федерации. | ++ |  |
| 2 | Мобильное устройство Клиента имеет поддерживаемую средством ЭП PayControl лицензионную версию операционной системы:   1. Android 5.0 и выше, 2. iOS 10.X, 11.X. | ++ |  |
| 3 | Клиент не использует средство ЭП PayControl на мобильных устройствах, на которых были получены права root («рутованые» устройства) или произведён «джейлбрейк» (англ. jailbreak). | ++ |  |
| 4 | Для операционной системы Мобильного устройства и приложений, установленных на Мобильное устройство, Клиентом установлены максимально возможные на текущее время обновления рекомендованные производителем/разработчиком. | + |  |
| 5 | Клиентская часть средства ЭП PayControl самостоятельно установлена Клиентом из одного из официальных сервисов Google Play или App Store. Клиент не использовал переход к указанным сервисам и установку клиентской части средства ЭП PayControl по ссылке из других источников. | ++ |  |
| 6 | Если при установке клиентской части средства ЭП PayControl появились сообщения о необходимости удаления приложения/приложений, представляющих угрозу для средства ЭП PayControl, Клиент удалил представляющие угрозу приложение/приложения с Мобильного устройства | ++ |  |
| 7 | Для разблокировки Мобильного устройства включён максимально возможный из доступных на данном Мобильном устройстве способ защиты от несанкционированного доступа к функциям устройства и хранящихся на нём данным (в порядке убывания стойкости защиты):   1. средство распознавания радужки глаза; 2. средство распознавания отпечатка пальца или лица; 3. пароль длиною не менее 6 символов (включая буквы и цифры); 4. графический ключ; 5. PIN-код.   При использовании пароля или PIN-кода Клиент запомнил их не сохранил в памяти Мобильного устройства. | ++ |  |
| 8 | Мобильное устройство настроено Клиентом на автоматическую блокировку устройства по истечении определённого времени (не более 5 минут). | ++ |  |
| 9 | На Мобильное устройство под управлением ОС Android используется средство защиты от вредоносного кода («антивирусное программное обеспечение»). | ++ |  |
| 10 | На Мобильном устройстве под управлением ОС Android отключена возможность установки приложений из непроверенных источников. | ++ |  |
| 11 | На Мобильное устройство не установлено корневых сертификатов PKI, полученных из ненадёжных источников. | ++ |  |
| 12 | Мобильное устройство с принятыми из Банка ключами регистрации PayControl (направляются Банком каждому УЛК Клиента в закодированном виде: QR-код + SMS и/или сообщение по электронной почте) и самостоятельно выработанными УЛК Клиента рабочими ключами ЭП PayControl, а так же атрибуты доступа к Мобильному устройству (логин, пароль, графический ключ) никогда не передается Клиентом неуполномоченным лицам, включая Руководство организации, коллег и членов семьи Уполномоченного лица Клиента и не оставляется им без присмотра. | ++ |  |
| 13 | Мобильное устройство, с установленной клиентской частью средства ЭП PayControl, используется Клиентом только для посещения сайтов и установки приложений, необходимых и достаточных Клиенту для ведения его коммерческой/уставной деятельности. | ++ |  |
| 14 | Мобильное устройство не подключается Клиентом к компьютерам, безопасность которых:   1. обеспечение доверенное среды, 2. отсутствие удаленного управления и 3. установленных/запущенных вредоносных программ,   Клиент не может гарантировать. | ++ |  |
| 15 | Мобильное устройство не подключается Клиентом к общественным WI-FI сетям. Общественные WI-FI сети, как правило, плохо защищены, их настройки неизвестны и эти сети приходится делить со множеством людей вокруг, среди которых могут быть злоумышленники. | ++ |  |
| 16 | В случае компрометации ключей ЭП PayControl, а так же атрибутов доступа к Мобильному устройству (логин, пароль, графический ключ) Клиенту известен установленный Банком порядок уведомления обслуживающего филиала Банка о блокировке доступа к счетам. | ++ |  |
| 17 | По завершении операционного времени обслуживающего филиала Банка Клиентом контролируется состояние счета путем отправки в Банк запроса промежуточного отчета об операциях по счету. | ++ |  |
| 18 | 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;

|  |  |
| --- | --- |
| Уполномоченный представитель Клиента  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (должность представителя Клиента)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись, фамилия, инициалы представителя Клиента) | Уполномоченный представитель Банка  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (должность представителя Банка)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись, фамилия, инициалы представителя Банка) |

Приложение 9. Анкета о результатах выполнения Клиентом требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ Системы ДБО (для системы ДБО BS-Client)

|  |  |  |
| --- | --- | --- |
| **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 | 1. АРМ Системы ДБО обслуживается уполномоченными лицами Клиента. | | ++ |  |
| 1. Клиентом обеспечивается контроль доступа в помещение, в котором размещен АРМ Системы ДБО. | | ++ |  |
| 1. 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 | 1. На АРМ Системы ДБО отсутствуют программы удаленного администрирования (например, RAdmin). | | ++ |  |
| 1. Осуществляется периодический контроль активного программного обеспечения (ПО), установленного на АРМ Системы ДБО. | | ++ |  |
| 3 | 1. Электронные ключи НКИ 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. | | ++ |  |
| 1. По окончанию сеанса работы с Банком приложение Системы ДБО закрывается, НКИ извлекаются из АРМ, при уходе с рабочего места НКИ 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 | 1. Доступ к АРМ Системы ДБО по сети (локальной, Интернет) запрещен. | | + |  |
| 1. Запрещен доступ неуполномоченных лиц к каталогам с установленной Системой ДБО. | | ++ |  |
| 7 | Дистрибутив СКЗИ КриптоПро CSP получен на учтенном 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 | 1. На АРМ Системы ДБО установлены все рекомендованные производителем обновления безопасности операционной Системы. | | ++ |  |
| 1. 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 | 1. Работа на АРМ Системы ДБО производится под учетной записью обычного пользователя. Администраторские права используются только для установки СКЗИ КриптоПро и Системы ДБО. | | ++ |  |
| 1. Стандартная учетная запись «Гость» отключена. | | ++ |  |
| 1. 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 | 1. На АРМ Системы ДБО установлено антивирусное ПО в соответствии с требованиями, указанными в формуляре на применяемое СКЗИ. 2. 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». 3. Перечень средств защиты информации, сертифицированных ФСБ России: <http://clsz.fsb.ru/certification.htm>, <http://clsz.fsb.ru/files/download/sved_po_sertif.pdf>. | | ++ |  |
| 1. Включены настройки антивирусного ПО, установленные разработчиком по умолчанию. Включена защита настроек паролем. | | ++ |  |
| 1. На АРМ Системы ДБО дополнительно установлены средства защиты от спама, вредоносного ПО и злоумышленного воздействия. | | \* |  |
| 1. Антивирусные базы обновляются в автоматическом режиме с рекомендуемым разработчиком периодом обновления. | | ++ |  |
| 1. 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; * НКИ; * PIN-кодов к НКИ, логинов и паролей. | | ++ |  |
| 14 | Клиенту известен установленный Банком порядок уведомления обслуживающего филиала Банка о блокировке доступа к счетам в случае утраты НКИ 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.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / Фамилия, инициалы/

Должность представителя Клиента (подпись)

**М.П.**

Приложение 9а. Анкета о результатах выполнения Клиентом требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ Системы ДБО (для системы ДБО Correqts с СКЗИ)

|  |  |  |
| --- | --- | --- |
| **Анкета № -** |  | **-BSS** |
| **о результатах выполнения Клиентом требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ Системы ДБО**  **(для системы ДБО Correqts с СКЗИ)** | | |

|  |  |
| --- | --- |
| 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 | 1. АРМ Системы ДБО обслуживается уполномоченными лицами Клиента. | ++ |  |
| 1. Клиентом обеспечивается контроль доступа в помещение, в котором размещен АРМ Системы ДБО. | ++ |  |
| 1. Администратор локальной вычислительной сети (ЛВС) и администратор безопасности (при их наличии) ознакомлены с настоящим Руководством. | ++ |  |
| 2 | 1. На АРМ Системы ДБО отсутствуют программы удаленного администрирования (например, RAdmin). 2. Осуществляется периодический контроль активного программного обеспечения (ПО), установленного на АРМ Системы ДБО. | ++ |  |
| 3 | 1. НКИ 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. | ++ |  |
| 1. По окончанию сеанса работы с Банком приложение Системы ДБО закрывается, НКИ извлекаются из АРМ, при уходе с рабочего места НКИ и носители с PIN-кодами доступа хранятся в недоступном для посторонних месте. | ++ |  |
| 4 | 1. Доступ к АРМ Системы ДБО по сети (локальной, Интернет) запрещен. | + |  |
| 1. Запрещен доступ неуполномоченных лиц к каталогам с установленной Системой ДБО. | ++ |  |
| 5 | Комплект подключения получен по акту приема-передачи, подписанным сотрудником Банка и уполномоченным представителем Клиента. | ++ |  |
| 6 | 1. На АРМ Системы ДБО установлены все рекомендованные производителем обновления безопасности операционной Системы. | ++ |  |
| 1. 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. | ++ |  |
| 7 | 1. Работа на АРМ Системы ДБО производится под учетной записью обычного пользователя. Администраторские права используются только для установки Системы ДБО. | ++ |  |
| 1. Стандартная учетная запись «Гость» отключена. | ++ |  |
| 1. 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. | ++ |  |
| 8 | 1. На АРМ Системы ДБО установлено антивирусное ПО. | ++ |  |
| 1. Включены настройки антивирусного ПО, установленные разработчиком по умолчанию. Включена защита настроек паролем. | ++ |  |
| 1. На АРМ Системы ДБО дополнительно установлены средства защиты от спама, вредоносного ПО и злоумышленного воздействия. | \* |  |
| 1. Антивирусные базы обновляются в автоматическом режиме с рекомендуемым разработчиком периодом обновления. | ++ |  |
| 1. Полная проверка АРМ Системы ДБО на наличие вирусов и вредоносного ПО производится в автоматическом режиме с рекомендуемым разработчиком периодом проверки. | ++ |  |
| 9 | 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. | \* |  |
| 10 | При уходе пользователя АРМ Системы ДБО с рабочего места в течение рабочего дня АРМ блокируется пользователем, после завершения рабочего дня – выключается. | ++ |  |
| 11 | В случае установки на ноутбук ПО АРМ Системы ДБО, Клиентом обеспечивается раздельное хранение трех компонент:   * ноутбука; * НКИ; * PIN-кодов к НКИ, логинов и паролей. | ++ |  |
| 12 | Клиенту известен установленный Банком порядок уведомления обслуживающего филиала Банка о блокировке доступа к счетам в случае утраты НКИ или PIN-кода доступа к нему. | ++ |  |
| 13 | Клиенту известен установленный Банком порядок немедленного уведомления обслуживающего филиала Банка о блокировке доступа к счетам в случае внезапной остановки работы Системы ДБО. | ++ |  |
| 14 | По завершении операционного времени обслуживающего филиала Банка Клиентом контролируется состояние счета путем отправки в Банк запроса промежуточного отчета об операциях по счету. | ++ |  |
| 15 | 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 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.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / Фамилия, инициалы/

Должность представителя Клиента (подпись)

**М.П.**

Приложение 9б. Анкета о результатах соблюдении Клиентом требований Руководства по обеспечению безопасности использования Клиентом Мобильного устройства (для системы ДБО Correqts со средством электронной подписи PayControl)

|  |  |  |
| --- | --- | --- |
| **Анкета № -** |  | **-BSS** |
| **о результатах выполнения Клиентом требований Руководства**  **по обеспечению безопасности использования Клиентом Мобильного устройства**  **(для системы ДБО Correqts со средством электронной подписи PayControl)** | | |

|  |  |
| --- | --- |
| г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Дата «\_\_\_\_\_» «\_\_\_\_\_\_\_\_\_\_\_\_\_\_» 20\_\_ г. |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(полное наименование Клиента, включая организационно-правовую форму, ИНН)* | |

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Требования по обеспечению информационной безопасности при эксплуатации Клиентом Мобильного устройства со средством электронной подписи PayControl | Признак обязательности | Оценка соответствия Требованиям  (Да/Нет) |
| 1 | Мобильное устройство, предназначенное для использования Клиентом со средством ЭП PayControl, должно быть приобретено у официального продавца и быть сертифицировано по требованиям ГОСТ в соответствии с действующим законодательством для использования на территории Российской Федерации. | ++ |  |
| 2 | Мобильное устройство Клиента имеет поддерживаемую средством ЭП PayControl лицензионную версию операционной системы:   1. Android 5.0 и выше, 2. iOS 10.X, 11.X. | ++ |  |
| 3 | Клиент не использует средство ЭП PayControl на мобильных устройствах, на которых были получены права root («рутованые» устройства) или произведён «джейлбрейк» (англ. jailbreak). | ++ |  |
| 4 | Для операционной системы Мобильного устройства и приложений, установленных на Мобильное устройство, Клиентом установлены максимально возможные на текущее время обновления рекомендованные производителем/разработчиком. | + |  |
| 5 | Клиентская часть средства ЭП PayControl самостоятельно установлена Клиентом из одного из официальных сервисов Google Play или App Store. Клиент не использовал переход к указанным сервисам и установку клиентской части средства ЭП PayControl по ссылке из других источников. | ++ |  |
| 6 | Если при установке клиентской части средства ЭП PayControl появились сообщения о необходимости удаления приложения/приложений, представляющих угрозу для средства ЭП PayControl, Клиент удалил представляющие угрозу приложение/приложения с Мобильного устройства. | ++ |  |
| 7 | Для разблокировки Мобильного устройства включён максимально возможный из доступных на данном Мобильном устройстве способ защиты от несанкционированного доступа к функциям устройства и хранящихся на нём данным (в порядке убывания стойкости защиты):   1. средство распознавания радужки глаза; 2. средство распознавания отпечатка пальца или лица; 3. пароль длиною не менее 6 символов (включая буквы и цифры); 4. графический ключ; 5. PIN-код.   При использовании пароля или PIN-кода Клиент запомнил их не сохранил в памяти Мобильного устройства. | ++ |  |
| 8 | Мобильное устройство настроено Клиентом на автоматическую блокировку устройства по истечении определённого времени (не более 5 минут). | ++ |  |
| 9 | На Мобильное устройство под управлением ОС Android используется средство защиты от вредоносного кода («антивирусное программное обеспечение»). | ++ |  |
| 10 | На Мобильном устройстве под управлением ОС Android отключена возможность установки приложений из непроверенных источников. | ++ |  |
| 11 | На Мобильное устройство не установлено корневых сертификатов PKI, полученных из ненадёжных источников. | ++ |  |
| 12 | Мобильное устройство с принятыми из Банка ключами регистрации PayControl (направляются Банком каждому УЛК Клиента в закодированном виде: QR-код + SMS и/или сообщение по электронной почте) и самостоятельно выработанными УЛК Клиента рабочими ключами ЭП PayControl, а так же атрибуты доступа к Мобильному устройству (логин, пароль, графический ключ) никогда не передается Клиентом неуполномоченным лицам, включая Руководство организации, коллег и членов семьи Уполномоченного лица Клиента и не оставляется им без присмотра. | ++ |  |
| 13 | Мобильное устройство, с установленной клиентской частью средства ЭП PayControl, используется Клиентом только для посещения сайтов и установки приложений, необходимых и достаточных Клиенту для ведения его коммерческой/уставной деятельности. | ++ |  |
| 14 | Мобильное устройство не подключается Клиентом к компьютерам, безопасность которых:   1. обеспечение доверенное среды, 2. отсутствие удаленного управления и 3. установленных/запущенных вредоносных программ,   Клиент не может гарантировать. | ++ |  |
| 15 | Мобильное устройство не подключается Клиентом к общественным WI-FI сетям. Общественные WI-FI сети, как правило, плохо защищены, их настройки неизвестны и эти сети приходится делить со множеством людей вокруг, среди которых могут быть злоумышленники. | ++ |  |
| 16 | В случае компрометации ключей ЭП PayControl, а так же атрибутов доступа к Мобильному устройству (логин, пароль, графический ключ) Клиенту известен установленный Банком порядок уведомления обслуживающего филиала Банка о блокировке доступа к счетам. | ++ |  |
| 17 | По завершении операционного времени обслуживающего филиала Банка Клиентом контролируется состояние счета путем отправки в Банк запроса промежуточного отчета об операциях по счету. | ++ |  |
| 18 | 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 Акта;
* пункты Требований, отмеченные знаком «+», обязательны и должны быть выполнены Клиентом в течение 2-х недель после составления Акта;

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / Фамилия, инициалы/

Должность представителя Клиента (подпись)

**М.П.**

Приложение 10. Акт об оказании услуг по выпуску сертификата ключа проверки электронной подписи в Системе ДБО (для системы ДБО BS-Client, оформляется на бумажном носителе)

**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 НКИ, 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 10а. Акт об оказании услуг по выпуску сертификата ключа проверки электронной подписи в Системе ДБО (для системы ДБО Correqts с СКЗИ, оформляется в электронном виде)

**Акт**

**об оказании услуг по выпуску сертификата ключа проверки электронной подписи**

|  |
| --- |
| Я, нижеподписавшийся, уполномоченный представитель Клиента  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,  *(наименование организации / ФИО ИП)*  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,  *(ФИО представителя)*  составил настоящий акт о том, что мною самостоятельно выработан ключ электронной подписи с записью в НКИ, электронный запрос на СКП ЭП, открытый ключ  \_\_\_\_\_\_\_\_\_,  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 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Приложение 10б. Акт об оказании услуг по регистрации ключа проверки электронной подписи PayControl (для системы ДБО Correqts со средством электронной подписи PayControl, оформляется на бумажном носителе)

**Акт № -\_\_\_\_\_\_-BSS**

**об оказании услуг по регистрации ключа проверки электронной подписи PayControl**

Настоящим Актом регистрируется ключ проверки электронной подписи (ЭП), принадлежащий уполномоченному владельцу (пользователю) ключа:

|  |  |
| --- | --- |
| ФИО владельца (пользователя) ключа |  |
| Организация |  |
| Дата начала срока действия ключа |  |
| Дата окончания срока действия ключа |  |
| Ключ ЭП создан с использованием средства ЭП | PayControl |
| Идентификатор владельца (пользователя) |  |
| Значение ключа проверки ЭП |  |

Ключ проверки ЭП зарегистрирован и может использоваться для обмена сообщениями.

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

Личная подпись владельца (пользователя) ключа \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

***(подпись)***

Настоящим подтверждаю самостоятельную выработку владельцем (пользователем) ключа ЭП и ключа проверки ЭП:

***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

***(должность руководителя организации Клиента) (подпись) ФИО руководителя организации/ИП***

***М.П.***

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

Акт об оказании услуг по регистрации ключа проверки электронной подписи PayControl 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.** | **№№ счетов2,**  **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 полномочий7** | |
| **подпись 1** | **подпись 2** | **единственная подпись** | **единственная визирующая подпись** | **визирующая подпись 1** | **визирующая подпись 2** | **шифрование** | **начало** | **окончание** |
| Карточка с образцами подписей и оттиска печати | Доверенность |
|  |  | |  |  |  |  |  |  |  |  |  |  |  |
|  |  | |  |  |  |  |  |  |  |  |  |  |  |
|  |  | |  |  |  |  |  |  |  |  |  |  |  |
|  |  | |  |  |  |  |  |  |  |  |  |  |  |
|  | | 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: | |
| Оказанные услуги | |
| Программное обеспечение Системы ДБО установлено/восстановлено (нужное подчеркнуть) на компьютер(ы) Клиента, находящийся по адресу: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ представителем Банка в следующей комплектации (отметить нужное):  ❑ Комплект Интернет-Клиент Системы BS-Client  ❑ Комплект Интернет-Клиент Системы BS-Client в конфигурации "Мультиклиент"  ❑ Комплект Интернет-Клиент Системы BS-Client в конфигурации "Корпоративный контроль"  ❑ Комплект Системы BS-Client "Клиент-Банк Офис"  ❑ Комплект Интернет-Клиент Системы Correqts с СКЗИ  ❑ Комплект Интернет-Клиент Системы Correqts с СКЗИ в конфигурации "Мультиклиент"  ❑ Комплект Интернет-Клиент Системы Correqts с СКЗИ в конфигурации "Корпоративный контроль"  ❑ Комплект Интернет-Клиент Системы Correqts со средством ЭП PayControl  ❑ Комплект Мобильный Бизнес Клиент Системы Correqts со средством ЭП PayControl  ❑ Комплект Мобильный Бизнес Клиент Системы Correqts без средства ЭП PayControl | |
| 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. 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.
   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](#Приложение6) 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) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(фамилия, имя, отчество владельца СКП ЭП)* | V |

либо подписанный Сторонами Акт о передаче Микро-комплекта подключения к системе ДБО ([Приложение 14](#Приложение14) к Правилам) либо подписанное Клиентом Заявление на предоставление комплексного обслуживания.

* 1. При создании ключа простой ЭП Банк обязуются соблюдать его конфиденциальность.
  2. Клиент (ИП, лицо, занимающееся частной практикой)/Представитель Клиента, использующий ключ простой ЭП, обязан соблюдать конфиденциальность ключа простой ЭП.
  3. 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.
  4. 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.
  5. 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.
  6. 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 НКИ (сам НКИ 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](#Приложение6)) 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](#Приложение14) к Правилам).
  7. В подсистеме Клиент-Банк Системы BS-Client простая ЭП не используется.

1. Правила применения простой ЭП в подсистеме Интернет-Клиент Системы Correqts с использованием СКЗИ
   1. Ключом простой ЭП в Подсистеме Интернет-Клиент Системы Correqts 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. 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](#Приложение6) 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)* | V |

либо подписанный Сторонами Акт о передаче Микро-комплекта подключения к системе ДБО ([Приложение 14](#Приложение14)) либо подписанное Клиентом Заявление на предоставление комплексного обслуживания.

* 1. При создании ключа простой ЭП Банк обязуются соблюдать его конфиденциальность.
  2. Клиент (ИП, лицо, занимающееся частной практикой)/Представитель Клиента, использующий ключ простой ЭП, обязан соблюдать конфиденциальность ключа простой ЭП.
  3. Ключ простой ЭП используется Клиентом (ИП; лицом, занимающимся частной практикой)/ Представителем Клиента совместно с технологическим сертификатом для первого входа в Систему ДБО Correqts 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.
  4. Определение в Системе ДБО Correqts 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.
  5. 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](#Приложение6)) с отметкой о передаче в строке 5 колонки «Отметка о передаче»:

|  |  |  |
| --- | --- | --- |
| № п/п | Переданные средства | Отметка о передаче |
| 5 | Технологический ключ в НКИ и технологический СКП ЭП, ID \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, серийный № СКП ЭП \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | V |

либо подписанное Клиентом Заявление на предоставление комплексного обслуживания.

* 1. 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.

1. Правила применения простой ЭП в подсистемах Интернет-Клиент и/или Мобильный Бизнес Клиент Системы Correqts с использованием средства ЭП PayControl
   1. Средство ЭП PayControl – это программный комплекс, предназначенный для подтверждения Клиентом операций в подсистемах Интернет-Клиент и/или Мобильный Бизнес Клиент Системы Correqts.
   2. Клиентская часть программного комплекса представляет собой приложение для мобильных платформ Android 5.0 и выше, iOS 10.X, 11.X, выполняющее следующие функции:
      1. управление ключевой информацией (считывание, хранение, использование, обновление, удаление);
      2. получение информации для подтверждения от серверной части в режиме онлайн или офлайн;
      3. отображение подтверждаемой информации на экране Мобильного телефона;
      4. выработка кода подтверждения на основе данных транзакции, ключа пользователя, времени выработки и (опционально) отпечатка устройства;
      5. отправка кода подтверждения в серверную часть в режиме онлайн или отображение пользователю в режиме офлайн.
   3. В подсистемах Интернет-Клиент и/или Мобильный Бизнес Клиент Системы Correqts со средством ЭП PayControl используются следующие ключи ЭП:
      1. Ключи регистрации PayControl. Уникальные ключи, вырабатываемые Банком для каждого Уполномоченного лица Клиента – владельца средства ЭП PayControl. Направляются Банком каждому УЛК Клиента в закодированном виде (QR-код + SMS и/или сообщение по электронной почте).
      2. Рабочий ключ электронной подписи PayControl. Уникальный ключ, самостоятельно вырабатываемый Клиентом одновременно с ключом проверки ЭП с использованием средства клиентской и серверных частей программного комплекса PayControl при выполнении процедуры первичной выработки ключа ЭП, а так же при проведении плановой смены ключей ЭП. Однозначно соответствует ключу проверки электронной подписи PayControl.
      3. Рабочий ключ проверки ЭП PayControl. Уникальный ключ, самостоятельно вырабатываемый Клиентом одновременно с ключом ЭП с использованием средства ЭП PayControl при выполнении процедуры первичной выработки ключа ЭП, а так же при проведении плановой смены ключей ЭП.
   4. Срок действия всех ключей ЭП, указанных в п.3.3 установлен в 1 год.
   5. Автоматизированная процедура выработки пары рабочих ключей – ключа ЭП и ключа проверки ЭП средства ЭП PayControl начинается в клиентской части программного комплекса PayControl после ввода в Мобильное устройство Клиента ключей регистрации, полученных Клиентом путем считывания QR-кода (1-й части ключей регистрации) и ввода в Мобильное устройство SMS и/или сообщения по электронной почте (2-й части ключей регистрации).
   6. Ключ ЭП Клиента средства ЭП PayControl является не извлекаемым и никогда не покидает Мобильное устройство Клиента.
   7. Ключ проверки ЭП средства ЭП PayControl по защищенному каналу направляется на сервер PayControl Банка, где однозначно регистрируется для УЛК Клиента.
   8. Для подтверждения принадлежности рабочего ключа проверки ЭП его владельцу – уполномоченному лицу Клиента, Банк средствами системы ДБО Correqts формирует Акт об оказании услуг по регистрации ключа проверки электронной подписи PayControl ([Приложение 10а](#Приложение10а)) и направляет его Клиенту в электронном виде.
   9. Клиент, получив Акт об оказании услуг по регистрации ключа проверки электронной подписи PayControl средствами системы ДБО Correqts, распечатывает Акт в 2-х экземплярах, сравнивает атрибуты УЛК Клиента – владельца (пользователя) ключа и значение ключа проверки электронной подписи с данными в клиентской части средства ЭП PayControl. В случае совпадения атрибутов и ключа проверки электронной подписи УЛК Клиента, Клиент оформляет Акт в 2-х экземплярах со стороны Клиента и представляет 2 экземпляра Акта в обслуживающий его ДО/филиал Банка.
   10. После проверки и оформления Акта со стороны Банка менеджером обслуживающего Клиента ДО/филиала Банка рабочие ключи ЭП PayControl вводятся в действие Банком.
   11. Стороны признают, что юридически значимым доказательством принадлежности Клиенту (ИП, лицу, занимающемуся частной практикой) / конкретному Представителю Клиента рабочего ключа проверки ЭП PayControl, используемого Банком для проверки ЭП Клиента, является подписанный Сторонами и надлежащим образом оформленный Акт об оказании услуг по регистрации ключа проверки электронной подписи PayControl ([Приложение 10а](#Приложение10а)).

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) (подпись) (фамилия и инициалы)*

**М.П.**

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_г.

1. Далее – Руководство по обеспечению информационной безопасности. [↑](#footnote-ref-1)
2. Далее – КОПОП. [↑](#footnote-ref-2)
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. [↑](#footnote-ref-3)
4. Предназначенный для отправки в Банк текстового сообщения или присоединенного файла (файлов) [↑](#footnote-ref-4)
5. Направляется Банком Клиенту по запросу последнего в течение текущего операционного дня;

   не является итоговым отчетом по операциям; может отражать ошибочные сведения. [↑](#footnote-ref-5)
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 [↑](#footnote-ref-6)
7. Статус документа в системе ДБО - «Принят» [↑](#footnote-ref-7)
8. Представляется при указании данной услуги в Заявлении на предоставление услуг, установку, настройку, восстановление Системы ДБО в случае использования Клиентом НКИ в форм-факторе смарт-карты. [↑](#footnote-ref-8)
9. Далее – ПК [↑](#footnote-ref-9)
10. Срок действия доверенности не может превышать срока действия СКП ЭП, указанного в сертификате. [↑](#footnote-ref-10)
11. Перечень операций, о которых направляются сообщения, определяется настоящими Правилами. [↑](#footnote-ref-11)