Приложение 1
к Условиям дистанционного банковского обслуживания
юридических лиц и индивидуальных предпринимателей
в АО «Россельхозбанк» с использованием системы
«Банк-Клиент»/«Интернет-Клиент»
(приказ АО «Россельхозбанк» от 21.02.2017 № 97-ОД)

Регламент
предоставления, использования и обслуживания системы «Банк-Клиент»/«Интернет-Клиент» в АО «Россельхозбанк»

1. Общие положения

Настоящий Регламент устанавливает порядок подключения Клиента к Системе ДБО, порядок обращения с СКЗИ, криптографическими ключами ЭП и паролями, а также порядок передачи и обработки электронных сообщений, виды которых перечислены в Приложении 3 к Условиям.

2. Обязательства сторон

2.1. Банк обязуется:

2.1.1. Осуществлять прием от Клиента, на основе настоящего Регламента, по электронным каналам связи должным образом оформленные ЭД.

2.1.2. Принимать к исполнению ЭД только с подлинной ЭП, сформированной с использованием ключей ЭП, действующих на момент подписания ЭД.

2.1.3. Принимать к исполнению только те ЭД, которые подписаны подлинной ЭП лиц, заявленных в карточке с образцами подписей и оттиска печати Клиента в соответствии с Договором банковского счета (или иным договором).

2.1.4. В случае наличия в карточке с образцами подписей и оттиска печати Клиента более двух подписей, принимать к исполнению только те ЭД, которые подписаны определенным сочетанием ЭП Уполномоченных лиц Клиента в соответствии с Соглашением о количестве и сочетании подписей[1], содержащим информацию о количестве подписей и возможном сочетании подписей Уполномоченных лиц Клиента.

2.1.5. Осуществлять обработку и исполнение полученных ЭД Клиента в строгом соответствии с настоящим Регламентом, установленными нормами, техническими требованиями, стандартами, инструкциями Банка России и Банка.

2.1.6. Информировать Клиента о результатах проверки, обработки (или об отказе в приеме на обработку) его ЭД, исполнении его распоряжений, предусмотренных нормативными актами Банка России, путем присвоения в Системе ДБО соответствующих статусов обработки указанных ЭД и распоряжений («ЭП не верна», «Ошибка реквизитов», «Ожидает визирования», «В обработке», «Принят»/«Не принят», «Исполнен»/«Не исполнен»/«Отозван», «Принят ВК/Отказан ВК/Отказан ВК частично», «Закрыт», «Получен банком плательщика»)[2].

2.1.7. Уведомлять Клиента о частичном исполнении распоряжений о переводе денежных средств путем присвоения статуса обработки платежного документа «Исполнен частично» в Системе ДБО и представления Клиенту по его требованию выписки из его счета с приложением

[1] В соответствии с Инструкцией Банка России от 30 мая 2014 года № 153-И «Об открытии и закрытии банковских счетов, счетов по вкладам (депозитам), депозитных счетов».

[2] Присваиваемые в Системе ДБО статусы обработки платежных документов «ЭП не верна», «Ошибка реквизитов», «Не принят», «Не исполнен» означают возврат Банком распоряжений Клиента без исполнения в соответствии с Положением Банка России от 19.06.2012 № 383-П «О правилах осуществления перевода денежных средств».

платежного ордера на зачисление суммы частично списанных денежных средств со счета плательщика не позднее следующего рабочего дня после совершения операции.

2.1.8. Подготавливать и представлять Клиенту выписки по счету, содержащие сведения о совершенных по результатам обработки и исполнения ЭД Клиента операциях, а также об иных операциях, в срок до 10:00 часов (по местному времени) следующего рабочего дня в виде надлежащим образом оформленных ЭД.

2.1.9. Своевременно информировать Клиента об изменениях порядка осуществления приема/передачи ЭД и другой информации по Системе ДБО.

2.1.10. Осуществлять регистрацию уполномоченных лиц Клиента в УЦ РСХБ и управление сертификатами ключей проверки ЭП уполномоченных лиц Клиента в соответствии с Временным регламентом УЦ РСХБ.

2.2. Клиент обязуется:

2.2.1. Разработать и утвердить руководством организации специальные документы, в которых должны быть отражены вопросы обеспечения функционирования и безопасности СКЗИ с учетом эксплуатационной документации на СКЗИ.

2.2.2. Обеспечить защиту конфиденциальности ключей ЭП, составляющих коммерческую тайну Клиента.

2.2.3. Соблюдать следующие требования по размещению, специальному оборудованию, охране и режиму в помещениях, в которых размещены СКЗИ:

- размещение, специальное оборудование, охрана и режим в помещениях, в которых размещены СКЗИ (далее – помещения), должны обеспечивать безопасность информации, СКЗИ и криптографических ключей, невозможность неконтролируемого доступа к СКЗИ, просмотра процедур работы с СКЗИ посторонними лицами;
- порядок допуска в помещения определяется внутренней инструкцией, которая разрабатывается с учетом специфики и условий функционирования конкретной структуры организации;
- при расположении помещений на первых и последних этажах зданий, а также при наличии рядом с окнами балконов, пожарных лестниц и т.п. окна помещений оборудуются металлическими решетками, ставнями, охранной сигнализацией или другими средствами, препятствующими несанкционированному доступу в помещения. Эти помещения должны иметь прочные входные двери, на которые устанавливаются надежные замки;
- для хранения криптографических ключей ЭП, эксплуатационной документации, инсталляционных CD-дисков[3], помещения обеспечиваются металлическими шкафами (хранилищами, сейфами), оборудованными внутренними замками с двумя экземплярами ключей. Дубликаты ключей от хранилищ и входных дверей должны храниться в сейфе ответственного лица, назначаемого руководством организации;
- устанавливаемый руководителем организации порядок охраны помещений должен предусматривать периодический контроль технического состояния средств охранной и пожарной сигнализации и соблюдения режима охраны;
- размещение и установка СКЗИ осуществляется в соответствии с требованиями документации на СКЗИ;
- системные блоки ЭВМ с СКЗИ должны быть оборудованы средствами контроля их вскрытия.

2.2.4. Соблюдать следующие требования по обеспечению безопасности криптографических ключей ЭП:

- все отчуждаемые ФКН (для хранения криптографических ключей ЭП) и инсталляционные CD-диски должны учитываться поэкземплярно в выделенных для этих целей журналах;

[3] При подключении Клиента к Системе «Банк-Клиент» /«Интернет-Клиент» без использования ЛК.

.

- учет и хранение инсталляционных дисков, учет ФКН должны быть поручены специально выделенным работникам. Каждый владелец ключа ЭП несет персональную ответственность за его использование и сохранность;

- поэкземплярный учет сформированных уполномоченными лицами Клиента криптографических ключей ЭП и их уничтожение осуществляется Клиентом.

- хранение ФКН с криптографическими ключами ЭП, инсталляционных CD-дисков допускается в одном хранилище с другими документами при условии, исключающем их непреднамеренное разрушение или уничтожение. Использование ФКН и инсталляционных дисков для записи какой-либо другой информации категорически запрещается;

- ключи ЭП каждого уполномоченного лица Клиента должны храниться на отдельном ФКН;

- в случае отсутствия у работника (уполномоченного лица) индивидуального хранилища, ФКН с криптографическими ключами ЭП (в виде, исключающем несанкционированный доступ к ним) по окончании рабочего дня должны сдаваться лицу, ответственному за их хранение;

- уполномоченными лицами или, по поручению руководителя организации, одним из работников из числа допущенных к эксплуатации СКЗИ, должен проводиться периодический контроль сохранности входящего в состав СКЗИ оборудования, а также всего используемого программного обеспечения для предотвращения внесения программно-аппаратных закладок и вредоносного программного обеспечения.

2.2.5. Учитывать следующие требования, предъявляемые к работникам, осуществляющим эксплуатацию и установку (инсталляцию) СКЗИ:

- к работе с СКЗИ допускаются решением руководства организации только работники, знающие правила эксплуатации СКЗИ, владеющие практическими навыками работы на ПЭВМ, ознакомленные с Временным регламентом УЦ РСХБ;

- работники, осуществляющие эксплуатацию СКЗИ, должны иметь представление о возможных угрозах информации при ее обработке, передаче, хранении, а также о методах и средствах защиты информации; руководителю организации рекомендуется организовать контроль над эксплуатацией СКЗИ.

2.2.6. Осуществлять ввод расчетных документов (и осуществлять контроль введенной информации на соответствие ее первичным расчетным документам и формирование записей) в электронный файл, соблюдая порядок подготовки документов, обеспечивая заполнение форм в соответствии с банковскими требованиями.

2.2.7. Выполнять требования по защите ключей ЭП, паролей доступа, оформлению и защите передаваемой и получаемой по Системе ДБО информации в виде ЭД.

2.2.8. Соблюдать порядок осуществления приема и передачи ЭД и обеспечивать передачу только надлежащим образом оформленных документов.

2.2.9. Направлять в Банк только те ЭД, которые подписаны ЭП лиц, заявленных в карточке с образцами подписей и оттиска печати Клиента, с соблюдением условий количества и сочетания подписей Уполномоченных лиц Клиента в соответствии с Соглашением о количестве и сочетании подписей.

2.2.10. В случае внесения изменений в карточку с образцами подписей и оттиска печати и/или Соглашение о количестве и сочетании подписей, своевременно представлять в Банк сведения, подтверждающие полномочия лиц Клиента по подписанию ЭД и способные повлиять на исполнение расчетных документов. Замена карточки и/или Соглашения о количестве и сочетании подписей, а также истечение сроков полномочий по подписанию расчетных документов у всех/одного из уполномоченных лиц Клиента, имеющих право подписи, согласно Соглашению о количестве и сочетании подписей, являются основаниями для приостановки обмена информацией с помощью Системы ДБО и смены ключей ЭП. Смена уполномоченных лиц Клиента должна сопровождаться аннулированием сертификатов ключей проверки ЭП лиц, ранее имевших право подписи, а также регистрацией в УЦ РСХБ, с последующей выдачей сертификатов ключей проверки ЭП, новых уполномоченных лиц Клиента, в соответствии с порядком, установленным Временным регламентом УЦ РСХБ.

2.2.11. В случае смены уполномоченных лиц Клиента, не имеющих права подписи расчетных документов, своевременно представлять в Банк запрос на аннулирование сертификата ключа проверки ЭП Субъекта информационного обмена (Приложение 12 к Временному регламенту УЦ РСХБ) и заявление о предоставлении/закрытии доступа к Системе ДБО уполномоченному лицу Клиента без права подписи расчетных документов (Приложение 15 к настоящим Условиям).

2.2.12. В случае смены уполномоченных лиц Клиента с правом акцептующей (визирующей) подписи платежных документов Контролируемой организации, своевременно представлять в Банк запрос на аннулирование сертификата ключа проверки электронной подписи Субъекта информационного обмена (Приложение 12 к Временному регламенту УЦ РСХБ) и Заявление об установлении/отключении функции контроля за платежами Контролируемой организации в Системе ДБО (Приложение 17 к Условиям).

2.2.13. Обеспечивать защиту клиентского модуля Системы ДБО от несанкционированного доступа, а также заражения вредоносным кодом (вирусами). В случае обнаружения неработоспособности Системы ДБО, признаков несанкционированного доступа к системе, а также признаков заражения клиентского модуля Системы ДБО вредоносным кодом (вирусами), не позднее следующего рабочего дня с момента обнаружения сообщить об этом Банку любым доступным способом.

2.3. Стороны взаимно обязуются:

2.3.1. Не осуществлять действий, наносящих ущерб другой Стороне вследствие использования Системы ДБО.

2.3.2. Поддерживать системное время ПЭВМ своего абонентского пункта Системы ДБО по местному времени с точностью до 5 минут. При обработке документов, полученных по Системе ДБО, определяющим временем является текущее время по системным часам аппаратных средств Банка.

2.3.3. При осуществлении операций, выполняемых на основании полученных по Системе ДБО ЭД, руководствоваться требованиями законодательства Российской Федерации и соглашений между Банком и Клиентом.

2.3.4. Обеспечивать защиту ключей ЭП, паролей доступа, целостность и сохранность программных средств, ЭД и другой информации, передаваемой и получаемой по Системе ДБО.

2.3.5. Вести архивы документов в электронном виде и бумажных носителях, хранить их в соответствии с порядком и сроками, установленными для хранения ЭД.

2.3.6. Представлять по запросам другой Стороны подтверждения о получении ЭД, а также надлежащим образом оформленные бумажные копии ЭД.

2.3.7. За собственный счет поддерживать в рабочем состоянии и при необходимости самостоятельно модернизировать свои помещения и технические средства, обеспечивать работоспособность вычислительной техники, средств связи, автоматизированного рабочего места, на котором установлено программное обеспечение Системы ДБО.

3. Условия и порядок осуществления электронных платежей

3.1. Общие положения

3.1.1. После подписания Сторонами Заявления о присоединении к Условиям Стороны осуществляют необходимые технические и организационные мероприятия для организации и осуществления электронного документооборота в соответствии с требованиями настоящего Регламента, Регламента установки и сопровождения клиентского модуля систем дистанционного банковского обслуживания АО «Россельхозбанк» (Приложение 2 к Условиям) и Временного регламента УЦ РСХБ.

3.1.2. ЭД представляют собой электронные бланки документов, заполняемые Клиентом в соответствии с банковскими требованиями и пересылаемые в Банк по каналам связи с использованием Системы ДБО для исполнения. Для удобства подготовки ЭД на экран ПЭВМ

Клиента выводится электронный бланк, который заполняется согласно наименованиям полей и правилам, описанным в документации на клиентский модуль. Некоторые поля заполняются автоматически в соответствии со встроенными справочниками реквизитов.

3.1.3. Заполняемые в клиентском модуле документы проходят предварительную автоматическую проверку (на дату документа, на присутствие обязательной информации в полях документа, на соответствие вводимых данных – реквизитам, записанным во встроенном справочнике, а также другую проверку в соответствии с принятой технологией).

3.1.4. На этапе обработки документов банковским модулем осуществляется автоматический контроль (на соответствие ЭП содержимому документа, на правильность указанного номера счета Клиента, на соответствие реквизитов Банка и БИК/наименование Банка получателя, установленным Банком России, а также другой контроль в соответствии с принятой технологией, в том числе получение дополнительного подтверждения подлинности и авторства ЭД). В случае выявления вышеуказанных несоответствий/компрометации, подозрения на компрометацию ключа ЭП Клиента в ходе проверки документа операции по документу не проводятся, при этом документу в Системе ДБО присваивается статус «Не принят»/«Ошибка реквизитов»/«ЭП не верна» (в зависимости от вида ошибки) с указанием причин отказа в приеме ЭД на обработку.

3.1.5. После заполнения электронной формы документа Клиентом осуществляется подписание документа ЭП и отправка ЭД в Банк с использованием Системы ДБО.

3.1.6. В случае если Контролирующей организацией осуществляется контроль за платежами Контролируемой организации посредством визирования (акцепта) документов в электронной форме (на основании заявления по форме Приложения 17 к Условиям): Контролируемой организацией после заполнения электронной формы документа осуществляется подписание документа ЭП и отправка ЭД в адрес Банка с использованием Системы ДБО[4].

3.1.6.1. Документ автоматически поступает на одобрение (акцепт) в Контролирующую организацию Клиента. После одобрения (акцепта)/отклонения Контролирующей организацией Клиента, документ принимается Банком к исполнению либо Контролируемой организации направляется уведомление об отказе.

3.1.7. Активной стороной при установлении связи является Клиент.

3.1.8. Основанием для отказа Банка от исполнения ЭД служат:

- отрицательный результат проверки подлинности ЭП;
- отсутствие ЭП под документами, наличие ЭП неуполномоченного лица;
- недостаток денежных средств для проведения операции на счете Клиента;
- несоответствие даты документа требуемой;
- неверно указанные реквизиты;
- проведение Клиентом сомнительных/подозрительных операций;
- отсутствие акцептующей подписи Контролирующей организации (в случае предоставления услуги по контролю за платежами Контролируемой организации в Системе ДБО);
- неоплата Клиентом в установленный срок услуг Банка по установке и обслуживанию Системы ДБО в соответствии с Тарифами Банка.

3.1.9. Клиент имеет право отозвать ЭД, переданные Банку путем создания и отправки в Банк ЭД «Запрос на отзыв документа» с указанием реквизитов отзываемого ЭД и основания отзыва. ЭД может быть отозван только в случае, если на момент поступления запроса на отзыв ЭД в Банк указанный ЭД принят, но не исполнен Банком, и у Банка имеется техническая возможность отменить его исполнение.

Если по информации, поступившей в Банк от Клиента в электронном виде, ЭД, направленные Клиентом и еще не принятые Банком для обработки, были направлены

[4] Функция контроля платежей возможна только для счетов в валюте Российской Федерации, а также при наличии системы «Интернет-Клиент» у Контролирующей организации Клиента.

ошибочно и/или подлежат отзыву Клиентом, Банк производит обработку ЭД по факту поступления от Клиента скорректированных ЭД.

3.2. Сроки обработки платежей

3.2.1. Работа Системы ДБО обеспечивается Банком в течение времени, установленного Банком для обслуживания Клиентов.

Информация о времени обслуживания Клиентов и порядке приема расчетных документов доводится до сведения Клиента путем размещения на информационных стендах в офисах Банка и web-сайте Банка в сети Интернет по адресу: http://www.rshb.ru[5].

3.2.2. Списание средств со счета Клиента производится в соответствии с условиями заключенного с Клиентом Договора банковского счета и Заявления о присоединении к Условиям на основании электронных расчетных документов Клиента, переданных им по каналам связи в Банк с использованием Системы ДБО после проведения процедур проверки ЭД в соответствии с положениями настоящего Регламента и Условий и законодательством Российской Федерации.

3.2.3. Списание средств на телеграфные расходы (если они указаны в соответствующих реквизитах документа) производится Банком в соответствии с действующими тарифами Центрального банка Российской Федерации.

3.3. Аварийный режим работы

3.3.1. При возникновении неисправности технических или программных средств Клиента или других внештатных ситуаций Клиент незамедлительно (но не позднее 18:00 часов по местному времени) должен предупредить уполномоченных работников Банка и осуществить действия по доставке в Банк надлежащим образом оформленных документов на бумажном носителе.

3.3.2. Обработка расчетных и иных документов, оформленных на бумажных носителях, осуществляется работниками операционного подразделения в соответствии с принятой в Банке технологией.

4. Порядок распространения, учета, утилизации программных и криптографических средств, действий в случае компрометации ключей ЭП и пароля оповещения, плановой и внеплановой смены ключей

4.1. Клиент обязан назначить не менее одного администратора безопасности, обязанности которого связаны с контролем за обеспечением конфиденциальности ключей ЭП, а также подачей запроса на аннулирование /приостановление действия сертификатов ключей проверки ЭП Уполномоченных лиц Клиента в случае увольнения/смены указанных Уполномоченных лиц Клиента (в соответствии с порядком, определенным Временным регламентом УЦ РСХБ). Сведения об Администраторах безопасности Клиента указываются в Заявлении о присоединении к Условиям. При смене работников из числа Администраторов безопасности Клиента в Банк должно быть направлено письменное уведомление в произвольной форме с указанием сведений об исключенных и вновь назначенных Администраторах безопасности Клиента, подписанное руководителем Клиента. Совмещение одним работником Клиента обязанностей Администратора безопасности и обязанностей, связанных с применением ключей ЭП и сертификатов ключей проверки ЭП в Системе ДБО, Клиенту не рекомендуется.

4.2. Порядок передачи, установки, хранения и утилизации программных средств, СКЗИ и криптографических ключей ЭП

4.2.1. Ответственный работник Банка передает Клиенту/представителю Клиента пакет программных средств и документов, включающий:

---

[5] Информация о режиме обслуживания Клиентов в региональном филиале Банка (его внутренних структурных подразделениях) размещается на странице соответствующего регионального филиала на указанном web-сайте Банка в сети Интернет.

– компакт-диск[6], содержащий дистрибутив клиентской части программных средств, СКЗИ, рабочие и резервные сертификаты ключей проверки ЭП уполномоченных лиц Банка;

– ФКН;

– лицензию на использование СКЗИ,

– временные ключи ЭП и соответствующие им временные сертификаты ключей проверки ЭП уполномоченных лиц Клиента, записанные на ФКН[7];

– документацию по работе с системой «Банк-Клиент»/«Интернет-Клиент» и СКЗИ;

- логин и пароль для аутентификации в Личном кабинете Клиента[8].

4.2.2. Пакет программных средств и документов Системы ДБО передаются Клиенту/представителю Клиента на основании полученных от Клиента доверенностей на их получение (Приложения 11.1 и 11.2 к Условиям) в зависимости от выбранной Клиентом Системы ДБО. Сертификаты ключей проверки ЭП на ФКН передаются Клиенту/представителю Клиента в упаковке с голографической наклейкой (в случае подключения к Системе «Банк-Клиент») на основании доверенности по форме Приложения 9 к Временному регламенту УЦ РСХБ.

4.2.3. Факт передачи Клиенту/представителю Клиента ФКН и пакета средств и документов для подключения Клиента к Системе «Интернет-Клиент» с использованием Личного кабинета подтверждается подписанием Сторонами Актов приема-передачи средств для подключения к Системе «Интернет-Клиент» с использованием Личного кабинета (по форме Приложения 5.1 к настоящим Условиям).

Факт передачи Клиенту/представителю Клиента пакета программных средств и документов Системы «Банк-Клиент» и Системы «Интернет-Клиент» без использования ЛК подтверждается подписанием Сторонами Акта приема-передачи программных средств и документов Системы «Банк-Клиент»/«Интернет-Клиент» без использования Личного кабинета (по форме Приложения 5.2 к настоящим Условиям). Факт передачи Клиенту/представителю Клиента ФКН при подключении Клиента к Системе «Банк-Клиент»/«Интернет-Клиент» без использования Личного кабинета подтверждается распиской, подписанной Клиентом/представителем Клиента по форме Приложения 10 к Временному регламенту УЦ РСХБ.

4.2.3. После установки у Клиента Системы ДБО:

4.2.3.1. Каждое Уполномоченное лицо Клиента должно создать основные ключи ЭП и запрос на выдачу сертификата ключа проверки ЭП (с использованием своих временных ключей ЭП – при подключении к Системе «Банк-Клиент»/«Интернет-Клиент» без использования ЛК; с использованием функционала ЛК – при подключении к Системе «Интернет-Клиент» с использованием ЛК) и передать в Банк Запрос на выдачу сертификата ключа проверки ЭП в электронном виде и на бумажном носителе по форме Приложения 11 к Временному регламенту УЦ РСХБ.

4.2.3.2. Выдача владельцу сертификата ключа проверки ЭП осуществляется Банком в соответствии с разделом 9.2 Временного регламента УЦ РСХБ.

4.2.3.3. Банк осуществляет консультационную поддержку работников Клиента по работе с клиентской частью Системы ДБО. Клиент и Банк переходят к эксплуатации своих ключей ЭП после внесения соответствующих сертификатов ключей проверки ЭП в реестр выпущенных сертификатов ключей проверки ЭП УЦ РСХБ.

4.2.4. Инсталлированные криптографические средства, используемые Клиентом, должны утилизироваться в течение одного рабочего дня после минования надобности использования таких средств в Системе ДБО путем деинсталляции с компьютеров, на которых установлена Система ДБО.

---

[6] При подключении Клиента к Системе «Банк-Клиент».

[7] При подключении Клиента к Системе «Банк-Клиент»/«Интернет-Клиент» без использования ЛК.

[8] В случае использования Клиентом системы «Интернет-Клиент» с использованием ЛК.

4.2.5. Утилизация основных ключей ЭП производится Клиентом самостоятельно в течение одного рабочего дня после истечения срока его действия. Утилизация ключа ЭП, записанного на ФКН, выполняется путем надежного стирания значения ключа ЭП.

4.2.6. Дистрибутив клиентской части программных средств, используемый Клиентом, утилизируется Клиентом самостоятельно.

4.3. Порядок действий в случаях компрометации криптографических ключей, их плановой и внеплановой смены

4.3.1. Ключ ЭП считается скомпрометированным в следующих случаях:

- разглашение или подозрение на разглашение содержания ключа ЭП;
- утрата (в том числе – временная) ФКН;
- перевод на другую работу или увольнение работников, имеющих доступ к ключу ЭП и(или) к ФКН;
- нарушение правил хранения ключа ЭП, установленных в соответствии с п. 2.2.4 настоящего Регламента;
- несанкционированное копирование или подозрение в копировании ключей ЭП;
- несанкционированное нарушение печати на хранилище/сейфе, где хранятся ФКН;
- случаи, когда нельзя достоверно установить, что произошло с ФКН (в том числе, случаи, когда физический носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника);
- факт или попытка несанкционированного списания денежных средств со счета Клиента с использованием рабочих ключевых пар;
- иные обстоятельства, прямо или косвенно свидетельствующие о доступе или возможности доступа к содержимому ФКН неуполномоченных лиц. В случае компрометации ключа ЭП владелец сертификата ключа проверки ЭП самостоятельно принимает решение о наличии или отсутствии факта компрометации принадлежащего ему ключа ЭП.

4.3.2. В случае компрометации ключа ЭП Клиента:

- уполномоченное лицо Клиента, выявившее факт компрометации, подозрение на компрометацию своего ключа ЭП, незамедлительно сообщает о факте компрометации и необходимости приостановления действия или аннулирования сертификата ключа проверки ЭП, соответствующего скомпрометированному ключу ЭП, Администратору Центра регистрации по контактному телефону, указанному в Заявлении о присоединении к Условиям, либо работнику операционного подразделения при личном обращении в порядке, установленном Временным регламентом УЦ РСХБ;
- Представитель Клиента, выявивший факт компрометации, подозрение на компрометацию рабочего ключа ЭП уполномоченного лица Клиента/субъекта информационного обмена, в том числе после обращения работника Банка для дополнительного подтверждения подлинности и авторства ЭД, незамедлительно сообщает уполномоченному лицу Клиента о факте компрометации ключа ЭП и необходимости приостановления действия или аннулирования сертификата ключа проверки ЭП, соответствующего скомпрометированному ключу ЭП;
- Уполномоченное лицо Банка, выявившее факт компрометации, подозрения на компрометацию ключа ЭП Клиента, выполняет операцию отказа в приеме ЭД, аналогично п.3.1.4 настоящего Регламента;
- аннулирование/приостановление действия сертификата ключа проверки ЭП, а также его внеплановая смена осуществляются в соответствии с Временным регламентом УЦ РСХБ;
- Клиент немедленно прекращает использование скомпрометированного ключа ЭП (блокирует соответствующий сертификат ключа проверки ЭП). При этом документы на бумажных носителях Клиент может представлять в Банк в полном объеме без ограничений;
- возобновление действия сертификата ключа проверки ЭП, выпущенного УЦ РСХБ, возможно только в течение срока, на который ранее было приостановлено действие этого сертификата ключа проверки ЭП;

- возобновление действия сертификата ключа проверки ЭП осуществляется в соответствии с Временным регламентом УЦ РСХБ.

4.3.3. В случае компрометации ключа ЭП Банка:

- уполномоченное лицо Банка, выявившее факт компрометации, подозрение на компрометацию своего рабочего ключа ЭП, незамедлительно прекращает использование скомпрометированного ключа ЭП и рассылает с использованием Системы ДБО извещение Уполномоченным лицам Клиентов о факте компрометации ключа ЭП Банка, используя в целях идентификации скомпрометированного ключа ЭП Банка идентификатор сертификата ключа проверки ЭП Банка соответствующего ключа ЭП Банка, а также инициирует процедуру внеплановой смены сертификата ключа проверки ЭП Банка в УЦ РСХБ;

- извещение о факте компрометации ключа ЭП Банка подписывается резервным ключом ЭП Банка. Аннулирование сертификата ключа проверки ЭП Банка, а также внеплановая смена ключей ЭП Банка и соответствующего им сертификата ключей проверки ЭП осуществляются в соответствии с Временным регламентом УЦ РСХБ;

- в случае если на момент получения извещения сведения о сертификате ключа проверки ЭП Банка, соответствующем скомпрометированному ключу ЭП Банка, не содержатся в актуальном списке отозванных сертификатов ключей проверки ЭП УЦ РСХБ, Клиент должен немедленно вывести из обращения сертификат ключа проверки ЭП Банка (заблокировать соответствующий сертификат ключа проверки ЭП Банка);

- для обмена информацией с Клиентом Банк переходит на резервные ключи ЭП и соответствующий им сертификат ключа проверки ЭП, которые переводится в разряд рабочей, и формирует новые резервные ключи ЭП и соответствующий им сертификат ключа проверки ЭП.

4.3.4. Плановая и внеплановая смена ключей ЭП и соответствующего им сертификата ключа проверки ЭП осуществляется в соответствии с разделом 9.9-9.10 Временного регламента УЦ РСХБ.

5. Порядок проведения смены логина и пароля для системы «Интернет-Клиент» при их компрометации

5.1. Смена логина и пароля для системы «Интернет-Клиент» производится при их компрометации по заявлению Клиента (по форме Приложения 6 к настоящим Условиям).

5.2. Логин и/или пароль доступа к системе «Интернет-Клиент» считаются скомпрометированными в следующих случаях:

- разглашение содержания логина и/или пароля;
- создание условий для разглашения логина и/или пароля:
  - утрата (в том числе – временная), хищение, несанкционированное копирование или подозрение на несанкционированное копирование;
  - нарушение правил хранения резервных копий.
- перевод на другую работу или увольнение работника, имеющего доступ к логину и/или паролю;
- иные обстоятельства, прямо или косвенно свидетельствующие о доступе или возможности доступа к содержимому логина и/или пароля.

5.3. Логин и пароль передаются Банком Клиенту/представителю Клиента в запечатанном конверте. Факт передачи логина и пароля Клиенту/представителю Клиента подтверждается подписанием Сторонами акта приема-передачи по форме Приложения 7 к настоящим Условиям.

5.4. Смена логина и пароля производится Банком в течение 4 рабочих дней после представления Клиентом заявления, указанного в п. 5.1 настоящего Регламента.