Приложение 2

к Условиям дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей   
в АО «Россельхозбанк» с использованием информационной системы «Цифровой канал обслуживания юридических лиц «Свой бизнес»

**Регламент**

**предоставления, использования и обслуживания**

**ИС Свой Бизнес** **в АО «Россельхозбанк»**

**1. Общие положения**

Настоящий Регламент устанавливает порядок подключения Клиента к ИС Свой Бизнес, порядок обращения с СКЗИ, ключами ЭП, Аутентификационными данными   
и Средствами подтверждения, а также порядок передачи и обработки ЭД.

**2. Обязательства сторон**

* 1. **Банк обязуется:**
     1. Осуществлять прием от Клиента, на основе настоящего Регламента,   
        по электронным каналам связи должным образом оформленные ЭД.
     2. Принимать к исполнению ЭД только с подлинной ЭП, действующей на момент поступления ЭД в Банк.
     3. Принимать к исполнению только те ЭД, которые подписаны подлинной ЭП лиц, заявленных в карточке с образцами подписей и оттиска печати Клиента и/или в Соглашении о количестве и сочетании подписей в соответствии с Договором банковского счета (или иным договором).
     4. В случае наличия в карточке с образцами подписей и оттиска печати Клиента более двух подписей, или отсутствии в Банке карточки с образцами подписей и оттиска печати, принимать к исполнению только те ЭД, которые подписаны определенным сочетанием ЭП Уполномоченных лиц Клиента в соответствии с Соглашением о количестве и сочетании подписей, содержащим информацию о количестве подписей и возможном сочетании подписей Уполномоченных лиц Клиента.
     5. Осуществлять обработку и исполнение ЭД, полученных от Клиента, в строгом соответствии с настоящим Регламентом, установленными нормами, техническими требованиями, стандартами, инструкциями Банка России и Банка.
     6. Информировать Клиента о результатах проверки, обработки (или об отказе   
        в приеме на обработку) его ЭД, исполнении его распоряжений, путем присвоения в ИС Свой Бизнес соответствующих статусов обработки указанных ЭД и распоряжений («Принят»/«Не принят», «Исполнен»/«Отозван», «Отказан/Отказан(приостановлен)», «Ожидает обработку сотрудником», «Обработка сотрудником», «Частично обработан», «Частично отказан», «Помещен в картотеку», «Отправлен в банк плательщика»). Указанные статусы ЭПД   
        в рублях РФ являются надлежащим уведомлением Банком Клиента о результатах проверки, обработки (или об отказе в приеме на обработку) ЭПД, исполнения распоряжений Клиентов, предусмотренных нормативными актами Банка России[[1]](#footnote-2).
     7. Уведомлять Клиента о частичном исполнении распоряжений о переводе денежных средств путем выписки по счету с приложением платежного ордера на сумму частично списанных денежных средств со счета плательщика не позднее рабочего дня, следующего за днем совершения операции.
     8. 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.
     9. Своевременно информировать Клиента об изменениях порядка осуществления приема/передачи ЭД и другой информации по ИС Свой Бизнес.
     10. В случае использования УНЭП осуществлять регистрацию СИО в УЦ РСХБ   
         и сопровождение СКП ЭП СИО в соответствии с Регламентом УЦ РСХБ.
  2. **Клиент обязуется:**
     1. Разработать и утвердить руководством организации специальные документы,   
        в которых должны быть отражены вопросы обеспечения функционирования и безопасности СКЗИ в соответствии с требованиями эксплуатационной документации на СКЗИ.
     2. Обеспечить защиту конфиденциальности ключей ЭП, Аутентификационных данных и Средств подтверждения, Мобильного устройства, Зарегистрированного номера.
     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 ключей ЭП, 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 ключей ЭП, эксплуатационной документации, и иной конфиденциальной информации, сохраняемой на материальных носителях памяти и/или бумажных носителях, 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 эксплуатационной документации на СКЗИ;

- системные блоки ЭВМ с СКЗИ должны быть оборудованы средствами контроля их вскрытия.

* + 1. Соблюдать следующие требования по обеспечению безопасности ключей ЭП:

- все отчуждаемые КН (для хранения ключей ЭП) должны учитываться поэкземплярно в выделенных для этих целей журналах;

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

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

- хранение КН, содержащих ключи ЭП, допускается в одном хранилище с другими документами при условии, исключающем их непреднамеренное разрушение или уничтожение. Использование КН для записи какой-либо другой информации категорически запрещается;

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

- в случае отсутствия у СИО (работника Клиента) индивидуального хранилища, КН с ключами ЭП (в виде, исключающем несанкционированный доступ к ним – отдельный опечатываемый СИО контейнер) 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.

* + 1. 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, ознакомленные с 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.

* + 1. 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. Выполнять требования по защите ключей ЭП, Аутентификационных данных   
       и Средств подтверждения, Мобильного устройства, Зарегистрированного номера, оформлению и защите передаваемой и получаемой по ИС Свой Бизнес информации   
       в виде ЭД.
    3. Соблюдать порядок осуществления приема и передачи ЭД и обеспечивать передачу только надлежащим образом оформленных документов.
    4. 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, или заявленных в Соглашении о количестве и сочетании подписей в случае отсутствия в Банке карточки с образцами подписей и оттиска печати.
    5. 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 ИС Свой Бизнес и смены ключей ЭП. Смена уполномоченных лиц Клиента должна сопровождаться блокировкой их доступа к ИС Свой Бизнес и при использовании Клиентом УНЭП - аннулированием СКП ЭП и регистрацией в УЦ РСХБ новых уполномоченных лиц Клиента (с последующей выдачей СКП ЭП), в соответствии с порядком, установленным Регламентом УЦ РСХБ в соответствии с настоящим Регламентом.
    6. В случае смены СИО, своевременно представлять в Подразделение Банка запрос на аннулирование СКП ЭП СИО (по форме Приложение 10 к Регламенту УЦ РСХБ)   
       и заявление о предоставлении/закрытии доступа к ИС Свой Бизнес данным СИО Клиента.
    7. В случае смены Пользователя/Представителя Клиента, своевременно представлять в Банк запрос на закрытие доступа к ИС Свой Бизнес данному Пользователю/Представителю Клиента (по форме Приложения 11 к настоящим Условиям).
    8. Обеспечивать защиту АРМ и Мобильного устройства от несанкционированного доступа, а также заражения вредоносным кодом (вирусами). В случае обнаружения неработоспособности ИС Свой Бизнес, признаков несанкционированного доступа к АРМ, КН и/или Мобильному устройству, а также признаков заражения АРМ   
       и Мобильного устройства вредоносным кодом (вирусами), не позднее следующего рабочего дня с момента обнаружения сообщить об этом Банку любым доступным способом.
    9. Исключить возможность установки и использования специализированного программного обеспечения для удаленного администрирования (например, Radmin, TeamViewer и др.) на устройстве, с которого осуществляется взаимодействие с ИС Свой Бизнес. При обнаружении специализированного программного обеспечения на устройстве,   
       с которого осуществляется взаимодействие с ИС Свой Бизнес, незамедлительно произвести удаление недопустимого программного обеспечения
    10. Устанавливать Мобильное приложение только из доверенных источников размещенное в «Play Маркет», «App Store», «Appgallery», «Galaxy Store», «RuStore»   
        и «NashStore».
    11. В случае смены уполномоченных лиц Клиента с правом акцептующей (визирующей) подписи ЭПД Контролируемой организации, своевременно представлять в Банк запрос на аннулирование СКП ЭП СИО (Приложение 10 к Регламенту УЦ РСХБ) и Заявление об изменении параметров контроля за платежами и просмотра остатков на счетах Контролируемой организации в ИС Свой Бизнес (Приложение 18 к Условиям).
  1. **Стороны взаимно обязуются:**
     1. Не осуществлять действий, наносящих ущерб другой Стороне вследствие использования ИС Свой Бизнес. Использовать для обмена ЭД согласно п.п. 2.1-2.2 настоящего Регламента только ИС Свой Бизнес.
     2. Поддерживать системное время АРМ и Мобильного устройства по местному времени с точностью до 5 минут. При обработке документов, полученных с использованием ИС Свой Бизнес, определяющим временем является текущее время по системным часам аппаратных средств Банка.
     3. При осуществлении операций, выполняемых на основании полученных по ИС Свой Бизнес ЭД, руководствоваться требованиями законодательства Российской Федерации и соглашений между Банком и Клиентом.
     4. Обеспечивать защиту ключей ЭП, Аутентификационных данных и Средств подтверждения, Мобильного устройства, Зарегистрированного номера, целостность   
        и сохранность программных средств, ЭД и информации, передаваемой и получаемой по ИС Свой Бизнес.
     5. Вести архивы документов в электронном виде и бумажных носителях, хранить их в соответствии с порядком и сроками, установленными для хранения ЭД.
     6. Представлять по запросам другой Стороны подтверждения о получении ЭД,   
        а также надлежащим образом оформленные бумажные копии ЭД.
     7. За собственный счет поддерживать в рабочем состоянии и при необходимости самостоятельно модернизировать свои помещения и технические средства, обеспечивать работоспособность вычислительной техники, средств связи, Мобильных устройств.

**3. Условия и порядок осуществления электронных платежей**

* 1. **Общие положения**
     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, Условий настройки программно-технических средств и доступа   
        к ИС Свой Бизнес (Приложение 3 к Условиям) и Регламента УЦ РСХБ.
     2. ЭД представляют собой электронные бланки документов, заполняемые Клиентом в соответствии с банковскими требованиями и пересылаемые в Банк по каналам связи с использованием ИС Свой Бизнес для исполнения. Для удобства подготовки ЭД на экран АРМ и Мобильных устройств Клиента выводится электронный бланк, который заполняется согласно наименованиям полей и правилам, описанным в документации. Некоторые поля заполняются автоматически в соответствии со встроенными справочниками реквизитов.
     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).
     4. На этапе обработки документов банковским модулем осуществляется автоматический контроль (на подлинность ЭП/Средства подтверждения, 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/Средства подтверждения Клиента в ходе проверки документа операции по документу не проводятся, при этом документу в ИС Свой Бизнес присваивается статус «Не принят»/«Отказан» (в зависимости от вида ошибки) с указанием причин отказа в приеме ЭД на обработку.
     5. После заполнения электронной формы документа Клиентом осуществляется подписание документа ЭП и отправка ЭД в Банк с использованием ИС Свой Бизнес.
     6. В случае если Контролирующей организацией осуществляется Контроль за платежами Контролируемой организации посредством акцепта документов в электронной форме, Контролируемой организацией после заполнения электронной формы документа осуществляется подписание документа УНЭП и отправка ЭПД в Банк с использованием ИС Свой Бизнес. Документ автоматически в ИС Свой Бизнес поступает на акцепт (подтверждение) Контролирующей организацией. После акцепта Контролирующей организацией, документ, при условии отсутствия иных оснований отказа в приеме к исполнению, принимается Банком к исполнению, в случае отказа - Контролируемой организации направляется уведомление об отказе в акцепте.
     7. Активной стороной при установлении связи является Клиент.
     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;
* неоплата Клиентом в установленный срок услуг Банка по установке   
  и обслуживанию ИС Свой Бизнес в соответствии с Тарифами Банка;
* применение Банком к Клиенту мер, предусмотренных пунктом 5 статьи 7.7 Федерального закона № 115-ФЗ, а также иных мер ограничительного характера, в том числе связанных с исполнением требований 115-ФЗ;
* отсутствие Акцептующей подписи Контролирующей организации (в случае осуществления Контроля за платежами в ИС Свой Бизнес по счетам Контролируемой организации).
  + 1. 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 ошибочно и/или подлежат отзыву Клиентом, Банк производит обработку ЭД по факту поступления от Клиента скорректированных ЭД.

* 1. **Сроки обработки платежей**
     1. Работа ИС Свой Бизнес 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 официальном сайте Банка в сети Интернет по адресу:<https://www.rshb.ru>[[2]](#footnote-3).

* + 1. 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 ИС Свой Бизнес после проведения процедур проверки ЭД в соответствии с положениями настоящего Регламента и Условий   
       и законодательством Российской Федерации.
    2. Списание средств на телеграфные расходы (если они указаны   
       в соответствующих реквизитах документа) производится Банком в соответствии   
       с действующими тарифами Центрального банка Российской Федерации.
  1. **Аварийный режим работы**
     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.
     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 ЭП**

* 1. Клиент обязан назначить не менее одного администратора безопасности, обязанности которого связаны с контролем за обеспечением режима конфиденциальности ключей ЭП. 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 использованием ключей ЭП в ИС Свой Бизнес, Клиенту не рекомендуется.
  2. **Порядок передачи, установки, хранения и утилизации программных средств, СКЗИ и ключей ЭП**
     1. Ответственный работник Банка передает Клиенту/Представителю Клиента:
  + для подключения к Интернет-банк Свой бизнес с применением УНЭП:   
    ПИН-конверт, КН; лицензию на использование СКЗИ;
  + для подключения к Интернет-банк Свой бизнес с применением ПЭП: логин   
    для каждого пользователя и технический (временный) пароль.
    1. Установочный комплект ИС Свой Бизнес передается Клиенту/Представителю Клиента на основании полученных от Клиента доверенности на их получение (Приложение 8 к Условиям).
    2. Факт передачи Клиенту/Представителю Клиента Установочного комплекта подтверждается подписанием Сторонами Акта приема-передачи средств для подключения   
       к ИС Свой Бизнес (по форме Приложения 5/5.1 к Условиям).
    3. **После получения Установочного комплекта и документов:**

4.2.3.1. Каждый СИО Клиента при подключении к Интернет-банк Свой бизнес   
с применением УНЭП должен создать ключи ЭП и запрос на выдачу СКП ЭП и передать   
в Банк Запрос на выдачу СКП ЭП в электронном виде и на бумажном носителе по форме Приложения 9 к Регламенту УЦ РСХБ. При подключении к Интернет-банк Свой бизнес   
с использованием ПЭП – сменить технический пароль (временный пароль) на постоянный.   
В случае использования Мобильного приложения – установить на Мобильное устройство пользователя Мобильное приложение и задать постоянный PIN-код для входа   
и подтверждения операций.

4.2.3.2. Выдача владельцу СКП ЭП осуществляется Банком в соответствии   
с Регламентом УЦ РСХБ.

4.2.3.3. Клиент и Банк переходят к эксплуатации своих ключей ЭП после внесения соответствующих СКП ЭП в реестр выданных и аннулированных СКП ЭП УЦ РСХБ.

* + 1. Инсталлированные криптографические средства, используемые СИО, должны утилизироваться в течение одного рабочего дня после минования надобности использования таких средств в ИС Свой Бизнес путем деинсталляции с АРМ.
    2. Утилизация ключей ЭП производится Клиентом самостоятельно в течение одного рабочего дня после минования надобности использования таких средств. Утилизация ключа ЭП, записанного на КН, выполняется путем надежного стирания значения ключа ЭП.
  1. **Порядок действий в случаях компрометации ключа ЭП, их плановой   
     и внеплановой смены**
     1. Ключ ЭП считается скомпрометированным в следующих случаях:
* разглашение или подозрение на разглашение содержания ключа ЭП, логина и/или пароля;
* утрата (в том числе – временная) КН;
* перевод на другую работу или увольнение работников, имеющих доступ к ключу ЭП, паролю к КН;
* 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 КН;
* случаи, когда нельзя достоверно установить, что произошло с КН (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 ЭП Клиента, без его согласия;
* иные обстоятельства, прямо или косвенно свидетельствующие о доступе или возможности доступа к содержимому КН неуполномоченных лиц. В случае компрометации ЭП владелец СКП ЭП самостоятельно принимает решение о наличии или отсутствии факта компрометации принадлежащего ему ключа ЭП.
  + 1. В случае компрометации ключа ЭП Клиента:

СИО, выявившее факт компрометации, подозрение на компрометацию своего ключа ЭП, незамедлительно сообщает о факте компрометации и необходимости приостановления действия или аннулирования СКП 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 Регламентом УЦ РСХБ;

* Уполномоченное лицо Банка, выявившее факт компрометации, подозрения   
  на компрометацию ключа ЭП СИО, выполняет операцию отказа в приеме ЭД, аналогично   
  п. 3.1.4 настоящего Регламента;
* аннулирование/приостановление действия СКП ЭП СИО, а также его внеплановая смена осуществляются в соответствии с Регламентом УЦ РСХБ;
* Клиент немедленно прекращает использование скомпрометированного ключа ЭП (блокирует соответствующий СКП ЭП). При этом документы на бумажных носителях Клиент может представлять в Банк в полном объеме без ограничений;
* возобновление действия СКП ЭП, выпущенного УЦ РСХБ, возможно только   
  в течение срока, на который ранее было приостановлено действие этого СКП ЭП;
* возобновление действия СКП ЭП осуществляется в соответствии с 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 ИС Свой Бизнес извещение Уполномоченным лицам Клиентов о факте компрометации ключа ЭП Банка, используя   
  в целях идентификации скомпрометированного ключа ЭП Банка серийный номер СКП ЭП Банка соответствующего ключу ЭП Банка, а также инициирует процедуру внеплановой смены СКП ЭП Банка в УЦ РСХБ;
* извещение о факте компрометации ключа ЭП Банка подписывается резервным ключом ЭП Банка. Аннулирование СКП ЭП Банка, а также внеплановая смена ключей ЭП Банка и соответствующего им СПК ЭП осуществляются в соответствии с Регламентом УЦ РСХБ;
* в случае если на момент получения извещения сведения о СКП ЭП Банка, соответствующем скомпрометированному ключу ЭП Банка, не содержатся в актуальном списке отозванных СКП ЭП УЦ РСХБ, Клиент должен немедленно вывести из обращения СКП ЭП Банка;
* для обмена информацией с Клиентом Банк переходит на резервные ключи ЭП   
  и соответствующий им СКП ЭП, и формирует новые резервные ключи ЭП и соответствующий им СКП ЭП.

4.3.4. Плановая и внеплановая смена ключей ЭП и соответствующего им СКП ЭП осуществляется в соответствии с Регламентом УЦ РСХБ.

**5. Порядок проведения смены пароля для ИС Свой Бизнес**

* 1. Смена пароля для входа Пользователя в ИС Свой Бизнес производится путем отправки Банком нового временного пароля на Зарегистрированный номер данного Пользователя при личном обращении Пользователя/Представителя Клиента в офис Банка.
  2. Пароль доступа к ИС Свой Бизнес считается скомпрометированным   
     в следующих случаях:
* разглашение содержания пароля;
* создание условий для разглашения пароля:
* утрата (в том числе – временная), хищение, несанкционированное копирование или подозрение на несанкционированное копирование;
* перевод на другую работу или увольнение работника, имеющего доступ к паролю;
* иные обстоятельства, прямо или косвенно свидетельствующие о доступе или возможности доступа к содержимому пароля.

**6. Порядок действий в случаях компрометации Средств подтверждения**

* 1. Средство подтверждения считается скомпрометированным в следующих случаях:
* разглашение или подозрение на разглашение содержания Средства подтверждения;
* утрата Средства подтверждения (Мобильного устройства);
* перевод на другую работу или увольнение работников, имеющих доступ   
  к Средству подтверждения (Мобильному устройству);
* несанкционированное копирование или подозрение в копировании информации содержащейся в Средстве подтверждения;
* возникновение подозрений на утечку конфиденциальной информации или ее искажение, в т.ч. подозрение на наличие вредоносного программного обеспечения, Мобильного устройства, направленного на кражу данных и мошеннические действия третьих лиц;
* случаи, когда нельзя достоверно установить, что произошло со Средством подтверждения/Мобильным устройством;
* факт или попытка несанкционированного списания денежных средств со счета Клиента с использованием Средств подтверждения;
* иные обстоятельства, прямо или косвенно свидетельствующие о доступе или возможности доступа к содержимому Средства подтверждения (Мобильному устройству) неуполномоченных лиц.
  1. Блокировка доступа Пользователя осуществляется Банком при наступлении обстоятельств, свидетельствующих о компрометации Средств подтверждения, разглашении Аутентификационных данных, а также при подозрении на несанкционированное использование ИС Свой Бизнес.
  2. Разблокировка Пользователей осуществляется по письменному заявлению клиента, после подтверждения отсутствия обстоятельств, свидетельствующих о факте компрометации, в том числе при изменении Зарегистрированного номера.

1. Присваиваемые в ИС Свой Бизнес 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 29.06.2021 № 762-П «О правилах осуществления перевода денежных средств». [↑](#footnote-ref-2)
2. Информация о режиме обслуживания Клиентов в региональном филиале Банка (его внутренних структурных подразделениях) размещается на странице соответствующего регионального филиала на официальном сайте Банка в сети Интернет. [↑](#footnote-ref-3)